National Bank of Belgium
Securities Settlement System

Annexes to the Terms and Conditions

governing the participation in the NBB-SSS

July 2021

List of annexes

1. Participation agreement of the securities settlement system managed by the NBB
   - 1.a Participant Identification Form
   - 1.b Participant List of authorized signatures
   - 1.c Participant Static data Form
3. Description X/N settlement
   - 3.1 Identification certificate - exempt account
   - 3.2 Individual certificate for the conversion of a registration by name
   - 3.3 List of beneficiaries of tax refunding
   - 3.4 Tax date correction
   - 3.5 E-mail: collection of withholding tax
4. E-mail Tenders
6. Instructions on behalf
8. Conditions of use of the RAMSES GUI
   - 8.1. Certification Practice Statement
   - 8.2 Certificate policy
     - 8.2a Certificate Policies for the ESCB/SSM users certificates
     - 8.2b Certificate Policies for the NON - ESCB/NON - SSM users certificates
   - 8.3. Trusted agents Terms and Conditions
     - 8.b. NBB-Net - Terms and Conditions
     - 8.c. NBB-Net – Terms and Conditions and Order Form
     - 8.d. Agreement on the testing of NBB - PKI
9. Description of Static data of a security account
12. Application for registration by name in the Belgian debt ledger
13. Cancellation of registration by name in the Belgian debt ledger
16. Guidelines for the use of Secure E-mail
17. Deleted
18. Power of attorney
    - 18.0 General Power of attorney
    - 18.1 Trading and settlement platforms
    - 18.2 Power of attorney for MTS Belgium
    - 18.3 Deleted
    - 18.4 Power of attorney for BrokerTec
    - 18.5 Power of attorney for MTS Spa
    - 18.6 Power of attorney EURO-MTS
    - 18.7 Power of attorney LCH
    - 18.8 Power of attorney FCA/DTA
    - 18.9 T2S Cross-Border Settlement "Already Matched" Instructions

19. Issues
    - 19.1 Fees
    - 19.2 Models of Service Agreements
        - 19.2.Service contract for the issuance of fixed income securities
        - 19.2a.Deleted
        - 19.2b.Deleted
        - 19.2c.Deleted
    - 19.3 Security information form
    - 19.4 Issuance Program summary
20. NBB-SSS link to Target2 Procedures
    - 20.0 NBB-SSS link to Target2
    - 20.1 Form SB04-Target2 RTGS account for use with NBB-SSS
    - 20.2 Form 2002 Debit Mandate for AS Settlement
    - 20.3 Contingency Procedures for Transfers DLNS
    - 20.4 Notification formats Target2 Direct Participant
    - 20.5 Notification formats Target 2 Non-Direct Participant
21. Matching rules
22. Buyer Protection Instruction
23. Information for DCP
24. Change request
25. Trade ABC between two N accounts involving investor CSD
26. Issuance overview
27. DVP In foreign currency
28. Insolvency procedure
29. Static Data for Status Eligible Counterparty CSD

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 1

PARTICIPATION AGREEMENT

of the securities settlement system managed by the National Bank of Belgium (NBB-SSS)

The undersigned institution:

.....

with BIC11-identification number:

.....

having its registered office at:

.....

.....

registration number (companies/trade register or any similar official register):

.....

being validly represented for the present purpose by (name, surname, capacity):

.....

- acknowledges that it has received a copy of the "Terms and conditions for the participation in the NBB-SSS", Annexes and sub-Annexes included (hereafter called the "Terms and conditions") and that it is fully aware of the Terms and conditions;
- acknowledges and unconditionally agrees with all the provisions of the said Terms and conditions, which will automatically and exclusively govern the transactions effected in the NBB-SSS upon instruction of the undersigned institution both for its own account and on behalf of its clients;
- commits itself to be bound by all the obligations and constraints imposed to the Participants to the NBB-SSS as described in the Terms and conditions, in particular (but not exclusively) the duty to build and maintain the operational and technical capacity required for participation to the NBB-SSS (e.g. as regards its IT and telecommunications systems) and the duty to timely pay all fees due to the NBB in retribution of the provision of the NBB-SSS services;
- irrevocably entitles the NBB with the power to effect movements in any of the Securities accounts opened in the name of the undersigned institution, either on its own behalf or on behalf of its clients, as well as in the Current accounts opened by the undersigned institution in the NBB's books, including any debit or credit entries or transactions, in accordance with the procedures described in the Terms and conditions;

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

- acknowledges and agrees that the power of attorney as referred to in the previous indent shall remain in force by operation of law as long as the undersigned institution remains Participant to the NBB-SSS, without prejudice of the provisions of Article 10.8 of the Terms and conditions;
- joins to this request Annex 1a Participant Identification Form, Annex 1b Participant List of authorized signatures and Annex 1c Participant Static data Form, for the purpose of the processing of instructions in the NBB-SSS in the name of the undersigned institution. The annexes shall remain valid until written communication of a modified annex to the NBB.

Place and date of signature:

[Signature, name and position of the person(s) entitled to validly commit the institution]

To be added:

- Annex 1a Participant Identification Form
- Annex 1b Participant List of authorized signatures
- Annex 1c Participant Static data Form

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Participant Identification Form

Annex 1a

BIC11 ----------

Name ----------

Address ----------

Postal address (if different)[1] ----------

Invoice address ----------

Legal Entity Identifier (LEI) ----------

GIIN (identifier for FATCA) ----------

Name of account-administrator[3] ----------

Department, service ----------

Language code (FR/NL/EN) ----------

Phone ----------

Fax ----------

E-mail ----------

Company number ----------

Cash account **C**

in the name of [2] ----------

[1] Mandatory if the administrator is another participant.

[2] If the cash account belongs to another participant, the latter must give his permission (to be sent to the NBB-SSS).

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Optionally: e-mail addresses for automatically generated e-mails (preferably a group address)

Domain	**E-mail address**
General notices to the participants	
Settled instructions	
Unsettled instructions	
Approved adjudications in het primary market Administration of the Treasury	
Securities shortages	
Account balances	
Unmatched instructions	
X/N-corrections	
Statements of X/N instructions	
Instructions of coupon payment and capital reimbursement (only for paying agents)	

Place and date of signature:

[Signature, name and position of the person(s) entitled to validly commit the institution]

Contacts NBB-SSS

Participant BIC11:.....

Name:.....

Domain	Name	Phone	Fax	E-mail (group addresses)
Operational				
Issues				
Euronext Brussels				
Invoices				
Cash account				
X/N				
Business Continuity (BCP)				
Alert messages				

.....,.....(place and date)

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 1b

PARTICIPANT LIST OF AUTHORISED SIGNATURES

Participant BIC11: .....

Participant Name: .....

The company declares that the persons listed below are authorized to sign, individually or jointly, without any restrictions as regards the amount or the value, all documents and endorsements, receipts, release notes, declarations and forms relating to the instructions of the NBB-SSS of the National Bank of Belgium.

Name	Authorisation	Signature

This list shall remain valid until written communication of a modified list to the NBB.

Place and date of signature:

[Signature, name and position of the person(s) entitled to validly commit the institution]

NBB - Payments and Securities Service
Securities Settlements System
Boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 36 00
sss@nbb.be

Participant Static Data Form

Annex 1c

BIC11 .....

Name .....

LEI .....

All Accounts:

SWIFT Addresses		*ISO 15022 – BIC11*	*ISO 20022 - DN*
Confirmation & Advice	*MT54x*		
Allegements	*MT578*		
Statement of Accounts - Daily	*MT535*		
Statement of Transactions	*MT536*		
Statements of Pending Transactions	*MT537*		
Corporate Actions Notifications	*MT564*		
		All Securities ☐	
		Positions Only ☐	
Corporate Actions Confirmation	*MT566*		
Message Broadcast	*MT599*		
Foreign Currency Cash Forecast (camt.052)			
Technical Address			
Inbounds			

Place and date of signature:

[Signature, name and position of the person(s) entitled to validly commit the institution]

NBB - Payments and Securities Service
Securities Settlements System
Boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 36 00
sss@nbb.be

Securities Account – Static Data – Only to be filled out when different from BIC11 Participant level

Annex 1c

Securities Account: .....

SWIFT Addresses		*ISO 15022 – BIC11*	*ISO 20022 - DN*
Confirmations & Advice	*MT54x*		
Statements of Accounts - Daily	*MT535*		
Statement of Transactions	*MT536*		
Statements of Pending Transactions	*MT537*		
Corporate Actions Notification	*MT564*		
		All Securities ☐	
		Positions Only ☐	
Corporate Actions Confirmation	*MT566*		
Foreign Currency Cash Forecast (camt.052)			

Place and date of signature:

[Signature, name and position of the person(s) entitled to validly commit the institution]

Send one form below duly signed for each securities account to NBB-SSS

		Example	Production
Securities Account	Always starts with "NBBE"	NBBE10081110178	
Category Account	Own acc.; Customer acc.; Pledge acc.	Own account	
Participant	BIC11		
Account Name	Free text		
Fiscal Policy	X or N	X	
Auto Collateralisation	Y or N	Y	
Standard DCA in EUR	Standard Cash Account	C……..	
DCA for Corporate Action Credit in EUR	Corporate Action – Credit Cash Account	C……..	
DCA for Market Claims EUR	Market Claims Cash Account	C……..	
Party Hold Indicator	Y or N / Hold Release Indicator	N	
Auction on Hold	Y or N	N	
Statement of Account EOD Only	Y or N	Y	
Statement of Transaction EOD Only	Y or N	Y	
Stripping and Reconstitution Eligibility	Y or N	N	
Customer BIC	Customer Swift	None	
Customer Name		/	
Dealer Type	Primary Dealer; Recognized Dealer; None	None	
T2S Account Type	CSDP (Participant); CSDO (Omnibus) or Issuance Account (ISSA)	CSDP	
CSD-R Account Type	Own Account (OW); Omnibus Account (OM); Individually Segregated Account (IS)	Own Account	
Opening Date			
Closing Date		31/12/2999	
Primary Market Default Account	Y or N	N	
Earmarking for Auto-Collat Restriction	Y or N	N	
Real-Time Auto-Collat Reporting	Y or N	N	

Place and date of signature:

[Signature, name and position of the person(s) entitled to validly commit the institution]

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 3

GENERAL DESCRIPTION OF THE MAIN TAX ASPECTS OF THE X/N SETTLEMENT SYSTEM

Taxation rules for the operation of the NBB-SSS mentioned in article 1.1° of the Law of 6 August 1993 on transactions in certain securities

1. APPLICATION OF THE PROVISIONS OF THE LAW OF 6 AUGUST 1993 ON TRANSACTIONS IN CERTAIN FIXED-INTEREST SECURITIES TO PARTICIPANTS IN THE NBB-SSS AND THEIR ACCOUNT-KEEPING CUSTOMERS.

1.1. By the Royal Decree of 14 June 1994[1] the NBB-SSS operated by the National Bank of Belgium (NBB) was approved as an X/N system (hereafter the "X/N system") in accordance with Article 15 of the Law of 6 August 1993 on transactions in certain securities.

Consequently, transactions in the NBB-SSS are subject to the tax provisions of the above-mentioned Law of 6 August 1993 and of its implementing decrees[2], except for those which remain subject to ordinary tax law (see below, point 2).

This annex may be amended as a result of new legal measures or regulations.

Taxation is governed solely by legal provisions and regulations and by the circulars of the Belgian Tax Authorities (Direct Tax Department). The operator of the X/N system (hereafter the "X/N operator") may give instructions to the Participants in order to ensure proper application of the tax rules and proper operation of the system.

1.2. Participants and their account–keeping customers agree that they become subject to the tax provisions of the X/N system as soon as they carry out transactions governed by the rules of the X/N system. It is incumbent on the Participants to provide their account-keeping customers with appropriate information on the operation of the X/N system and the rights and duties resulting from this participation and ensure that their account-keeping customers comply with the rules of the X/N system.

The collection and refunding of taxes in the X/N system take place solely through the participants to the X/N system. Participants expressly acknowledge and accept this responsibility as intermediary vis-à-vis their account-keeping customers and guarantee its proper performance.

1.3. The list of the securities accepted in the NBB-SSS is published on www.nbbsss.be and available in the RAMSES application.

1.4. The X/N operator is authorised to establish a scale of charges specific to the X/N system.

[1] Royal Decree of 14 June 1994 approving a settlement and clearing system in accordance with chapter 1 of the Law of 6 August 1993 on transactions in certain securities.

[2] Royal Decree of 26 May 1994 on the collection and refunding of the withholding tax in accordance with chapter 1 of the law of 6 August 1993 on transactions in certain securities, as amended from time to time.

1.5. Pursuant to Article 14 of the Royal Decree, no refund (equal to the withholding tax) is due in the case of withdrawal of securities from an X-account, when the debtor of the income remains in default on the Payment date. If the refund is postponed (until the payment of the income), the transactions will be carried out in the X/N system on the Payment date and the X/N operator will apply, on behalf of the parties, a deduction of an amount equal to the withholding tax, by creating a separate Dedicated Withholding Tax Transaction.

1.6. If a Participant fails to comply with the administrative formalities laid down by the taxation laws, the X/N operator is authorised to carry out unilaterally at the expense of the Participant the operations required by the Law of 6 August 1993, such as, inter alia, the collection of the withholding tax or the recovery of the refund equal to the withholding tax.

1.7. For all amounts due as a result of the participation in the X/N system, including tax corrections resulting therefrom (see point 9 below), the Participants accept the application of the NBB-SSS Terms and conditions, including the rules applying to Dedicated Cash Accounts, both for the transactions carried out for their own account and on behalf of third parties.

1.8. Except for the application of article 6 bis of the Royal Decree of 26 May 1994, the rules of article 6 of this Royal Decree (see below point 3.) are also valid for account-keepers established outside Belgian territory.

2. MANAGEMENT OF TRANSACTIONS IN SECURITIES.

All transactions in securities admitted in NBB-SSS are subject to the X/N system.

The X/N tax rules are applicable only from the entry of these securities in a securities account held in the NBB-SSS. When these securities circulate outside the X/N system, transactions in them are subject to ordinary tax law.

3. SECURITIES ACCOUNTS EXEMPT FROM WITHHOLDING TAX (X ACCOUNTS).

3.1 Opening of an X account.

The investors authorised to hold a securities account exempt from withholding tax are enumerated in Article 4 of the Royal Decree of 26 May 1994 on the collection and refunding of the withholding tax in accordance with chapter 1 of the Law of 6 August 1993 on transactions on certain securities (hereafter “the Royal Decree”).

When an X account is opened, the investor must send to the institution acting as account-keeper, in accordance with Article 5 of the Royal Decree, an **identification certificate** (see annex 3.1) whereby he declares that he belongs to one of the categories of investors entitled to claim exemption from the withholding tax as listed in Article 4 of the Royal Decree. This certificate must be kept by the account-keeper and held at the disposal of the Belgian Tax Authorities.

Account-keepers established outside Belgium must send the certificates to the NBB-SSS or to their Belgian participant which holds them at the disposal of the Belgian Tax Authorities.

According to Article 6 of the Royal Decree, the financial institution acting as account-keeper must also send to the NBB-SSS, at the latest on the 15th January of each year, the list of all persons and/or entities that held one or more X-account during the precedent calendar year (« the **nominative statement** »)[3]. This list must contain the names and full addresses of the holders of the X-accounts.
According to Article 6bis of the Royal Decree[4], the obligations regarding the identification certificate and the nominative statement do not apply to central securities depositaries ("CSD") as defined in Article 2, 1st paragraph, 1) of the Regulation (EU) N° 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories, provided that, as direct participant of the NBB-SSS, the CSD holds only X-accounts and is able to identify the ultimate account holders (ultimate investor or beneficial owner).

This exception is subject to the condition that the contractual arrangements between Participants acting as CSD and their customers (indirect participants) ensure that their customers (account holders) belong to one of the categories of investors listed in Article 4 of the Royal Decree.

In accordance with Article 4, last paragraph, of the Royal Decree, investors entitled to an X account can only open an X account.

Derogation: public debt securities referred to in Article 4, 10°of the Royal Decree.

For the categories of investors mentioned in Article 4, 3° and 10° of the Royal Decree, the Minister has published a notice containing a non-limitative list of the categories of investors authorised to hold an X account for the above-mentioned public debt securities[5].

Investors not included in this list but consider that they belong to one of these specific categories may apply directly to the Belgian Tax Authorities.

This derogation is optional. It is granted only following an application for the opening of a securities account by the designated owner and is valid only from this application onwards, without any possibility of regularisation for the past. If the investor was already the holder of a non-exempt account ("N account") or if he already held the securities outside the system, the withholding tax will be deducted from the incomes from movable assets accrued when the transfer to or deposit on the X account was made.

3.2 Operation of the X account

For the owners of an X account, the X/N operator executes the gross interest payments at the **due date of the coupon**. No withholding tax is collected on **accrued income** by transactions carried out between two due dates from X accounts.

A special feature with regard to the withholding tax for holders of an X account concerns the **entry** of securities into the system and the **exit** of these securities from the system.

In the case of an **entry** on an X account, the X/N operator will create a separate Dedicated Withholding Tax Transaction for withholding the tax on the accrued income. The holder of the X

[3] When the nominative statement refers to legal entities that are part of the European system of national and regional accounts (ESA) or to semi-governmental institutions for social security or assimilated institutions, the account-keeper must also mention the nominal amount of the transferable securities referred to in Article 4,10 °of the Royal Decree of 26 May 1994.
[4] As amended by the Royal Decree of 31 May 2017 amending the Royal Decree of 26 May 1994 on the collection and refunding of the withholding tax in accordance with chapter 1 of the Law of 6 August 1993 on transactions on certain securities.
[5] Notice concerning the withholding tax, Moniteur belge/Belgisch Staatsblad of 1997-02-01, page 1963.

account may recover this withholding tax in accordance with the ordinary tax law. The deposit may be made with exemption from withholding tax when the provisions of Article 13 of the Royal Decree of 26 May 1994 are applicable (see annexes 3.2a and 3.2b).

In the case of an **exit** from an X account, a refund of withholding tax is granted to the account-holder for the period of accrued income under the X/N tax law provisions. However, this refund is paid only upon the next due date for interest or upon final maturity (capitalisation bond or zero coupon). When income from movable securities is collected from securities which have been withdrawn from the system, the withholding tax will always be collected. As quickly as possible after an exit, the participant must send to the X/N operator the list of names referred to in Article 16, paragraph 1,3° of the Royal Decree (see point 7 below).

4. SECURITIES ACCOUNTS NOT EXEMPT FROM WITHHOLDING TAX (N ACCOUNTS).

4.1 Opening of an N account.

N accounts are intended for investors who cannot hold an X account. These investors are subject to individual or legal entities income tax, with the exception of the institutions referred to in article 4, 10° of the Royal Decree[6].

4.2 Operation of the N account

On the **interests payment date**, the X/N operator creates a separate Dedicated Withholding Tax Transaction for withholding the tax on the gross income paid to holders of N accounts.

For **transactions between two interests payment dates**, the withholding tax is collected from the accrued income by a separate Dedicated Withholding Tax Transaction on the N account of the holder who sells the securities, and a refund equal to the withholding tax on the accrued income is granted to the holder of the N account who buys the securities.

5. CALCULATION OF ACCRUED INCOMES FROM MOVABLE SECURITIES.

Accrued incomes from movable securities are calculated according to the rules laid down by articles 8 to 11 of the Royal Decree.

The interest rate used for the securities issued on a discount basis is the weighted average annual yield on the first issue of the securities in question and not the average of the annual yields of each issue, so that the income reported by the X/N operator to the issuer in accordance with article 16, paragraph 1, 1° of the Royal Decree may differ from the amount of the expenses that the issuer may deduct.

The yield referred to in articles 8 to 10 of the Royal Decree must be calculated on the basis of the cost for the issuer. Exceptionally, account may be taken of commissions or other expenses when they result from a written issue agreement applicable without distinction to the entire loan and to all investors or intermediaries.

If the characteristics of the securities or the conditions of issuance do not correspond to those of the cases referred to in articles 8 and 9, the Minister of Finance or his delegate will determine the calculation rules by analogy.

[6] See point 3.1 above.

The income from securities denominated in a currency which country of issuance has not adopted the euro in accordance with the Treaty establishing the European Union are, for the settlement of the withholding tax, converted into euros on the basis of the indicative rate for that currency published by the European Central Bank or the National Bank of Belgium on the Business Day before the tax date (Article 11 of the Royal Decree).

6. FORBIDDEN SPECIFIC TRANSACTIONS OF AN N ACCOUNT.

Deleted [7].

7. LATE SUBMISSION OF LISTS BY PARTICIPANTS.

With regard to the postponed refunding connected with the withdrawal of securities from the system by an investor exempt from withholding tax, the X/N operator will recover the refund if, after the granting or payment of the income, the list of names referred to in article 16, paragraph 1, 3° of the Royal Decree (see annex 3.3) is not in its possession. First, the participant will be notified of the absence of this list 15 calendar days after the due date. If, within 5 NBB-SSS business days after this notification, the list has still not been provided, the withholding tax will be automatically recovered.

Except when Article 6 bis of the Royal Decree is applicable, the X/N operator will inform the Belgian Tax Authorities if financial institutions acting as account-keepers have not sent to it the list of names of all the holders of one or more securities accounts exempt from withholding tax during the past calendar year (Article 6 of the Royal Decree – see also 3.1 above).

8. INTEREST ON ARREARS.

The provisions of article 414, paragraph 1 of the Income Tax Code 1992 with regard to arrears are applied to the withholding tax on the income paid on a due date. The amounts are settled by the Belgian Tax Authorities.

9. PROCEDURE AND FORMALITIES RELATING TO TAX CORRECTIONS.

The provisions mentioned here revoke and replace all preceding regulations concerning corrections, including those mentioned in circular 4/96.

The X/N operator is authorised to carry out the corrections which are necessary in accordance with the rules laid down by the Belgian Tax Authorities and/or at the request of participants.

Any participant may request the correction of an error by means of a correcting notification sent to the X/N operator by e-signed e-mail (see annex 3.4), providing a motivation with the data concerning the transaction(s) giving rise to the correction.

The X/N operator verifies the requested corrections, including, if necessary, with the other party. If no adequate response is received within five NBB-SSS business days to a request for additional information, or if the X/N operator considers that the information supplied is insufficient, the correction is refused and the X/N operator, if appropriate, informs the Direct Tax Department and the relevant participant(s).

When a correction concerns a transaction which has already been settled and which can no longer be rectified by means of a correcting notification and the associated “tax correction date” by e-signed e-mail, a participant who does not wish to make the correction request to the Belgian Tax

[7] Art. 11 of the law of 6 August 1993.

Authorities himself requests the X/N operator in writing to make the correction. He must motivate the request with the data concerning the transaction which has given rise to the correction.

As appropriate, he will provide additional information and/or supporting documents for this purpose.

The X/N operator will make the correction after having verified the transactions relating to the correction, in order to ensure that all related transactions are corrected in a consistent manner, with the agreement of the other parties concerned. Where appropriate, the operator will transmit the required information, especially the history of the transaction to be corrected and the necessary supporting documents, to the Belgian Tax Authorities.

When requests for corrections are refused, for whatever reason, by the Belgian Tax Authorities, the Participant will accept the reversing of the entries without being entitled to claim any compensation from the X/N operator.

10. CODING OF X/N TRANSACTIONS.

First character	Second character
Reason for transaction	Nature of transaction
1. current transaction	1. debit of N account
5. cancellation	2. credit of N account
9. correction	3. entry materialised security in X account
	4. exit materialised security from X account
	5. payment of coupon
	6. interest income on a security without coupon
	7. redemption premium.

In the e-mail giving the details of the withholding tax, this code is preceded by the letters XN.

11. CODING OF THE DETAILS OF THE WITHHOLDING TAX (SEE ANNEX 3.5).

The e-mail giving the details of the withholding tax is sent on the first bank working day following the date on which the withholding tax was paid. This e-mail consists of three parts:

A. *withholding tax paid with the settlement system transactions:*

a) Current transactions:
XN11, XN12, XN13, XN15, XN16 and XN17;

b) Deferred payments of withholding tax:
- XN14;
- XN12 in cases of lifting of suspension of a withholding tax refund;

B. *withholding tax paid outside the NBB-SSS:*

this relates to cancellations and corrections, i.e. X/N transactions which first code character begins with 5 or 9;

C. *withholding tax which is not paid immediately:*

a) withholding tax refunded on the next due date:
- XN14 and XN94;
- in cases of suspension of refunding of withholding tax: XN12 and XN14;

b) withholding tax not refunded owing to a cancellation:
   - XN12 and XN14 cancelled before payment for them has actually been made.

Each part of the e-mail (A, B and C) is sent only when one or more transactions have taken place.

In order to facilitate the internal checks of the recipients of the e-mail, the e-mail mentions, by value date and ISIN code, the year and dispatch number, the code of the X/N transaction, the nominal amount to which the transaction relates, the amount of income on which the withholding tax is calculated and the amount of the withholding tax. While the nominal amount and the amount of income are denominated in the currency of the security, the withholding tax is denominated in euros.

FPS FINANCE
Ledger service
Avenue des arts 30 - 1040 Brussels
Tel.: +32 (0)2 574 72 09 - Fax: +32 (0)2 233 70 86

Annex 3.1

IDENTIFICATION CERTIFICATE
X/N securities settlement system (movable assets)
Exempt account

Certificate drawn up pursuant to article 5 of the Royal Decree of 26 May 1994 on the collection and payment of the withholding tax on income from movable assets in accordance with chapter I of the law of 6 August 1993 on transactions in certain securities.

When an exempt account is opened, the holder shall deliver to the account-keeping institution a certificate which enables the holder or the beneficiaries of the income to be identified and makes it possible to ascertain that these belong to one of the categories of persons who can claim exemption from the withholding tax on income from movable assets.

This certificate shall be held in safekeeping by the account-keeping institution at the disposal of the Direct Tax Department. Account-keeping institutions established abroad shall transmit these certificates either to the manager of the X/N settlement system or to their Belgian participant, which shall keep these certificates at the disposal of the Department.

The holder of an exempt account shall immediately inform the account-keeping institution of any change to the data contained in the certificate. Account-keeping institutions established abroad shall immediately notify the manager or the Belgian participant of these changes.

The undersigned[1] ----------

---

acting of behalf of[2] ----------

---

address or registered head office ----------

---

1) certify/certifies that the latter belongs to one of the categories[3] of taxpayers[4] mentioned below:

1° the resident companies referred to in article 2 of the Income Tax Code 1992 (CIR 92);
2° without prejudice to the application of article 262, 1° and 5°, CIR 92, the institutions, associations or companies referred to in article 2, § 3, of the law of 9 July 1975 on the supervision of insurance companies, other than those referred to in 1° and 3°;
3° the semi-public ("parastate") social security agencies, or agencies equivalent thereto, referred to in article 105, 2°, of the royal decree implementing CIR 1992 (AR/CIR 92);
4° the non-resident savers referred to in article 105, 5° of the same decree;
5° the unit trusts referred to in article 115 of the same decree;
6° the taxpayers referred to in article 227, 2°, of CIR 92 who are subject to the tax on non-residents in accordance with article 233 of the same Code and who have used the income-producing capital for the exercise of their professional activity in Belgium;

[1] Surname(s) and forename(s) of the declarant or his agents.
[2] Exact name - only for legal persons.
[3] Categories referred to in article 4 of the Royal Decree of 26 May 1994.
[4] Delete as appropriate.

7° the Belgian State, for its investments which are exempt from the withholding tax on income from movable assets, in accordance with article 265 of CIR 92;

8° collective investment undertakings governed by foreign law which have joint assets managed by a management company on behalf of the participants, when their right of participation are not publicly issued in Belgium and are not marketed in Belgium;

9° resident companies not referred to in 1° whose sole or main activity consists in the granting of credits and loans;

10° exclusively with regard to income of securities issued by legal entities forming part of the sector of government within the meaning of the European System of national and regional accounts (ESA) for the application of the Council Regulation (EC) No 3605/93 of 22 November 1993 on the application of the Protocol on the excessive deficit procedure annexed to the Treaty establishing the European Community, the legal entities forming part of the above mentioned sector of government.

11° To be completed in the event of the extension of article 4 of the Royal Decree of 26 May 1994 to other categories of investors.

2) confirm(s) that the securities which will be booked on an exempt account exclusively belong to the holder of the account either as owner or as usufructuary, or that the holder will act solely on behalf of persons belonging to one of the categories of persons referred to in section 1;

3) undertake(s) to notify the account-keeping institution with which his/her/their account is opened of any change affecting the accuracy of this certificate[5];

4) authorise(s) the account-keeping institution and the debtor of the income to comply with the rules to which the renunciation of the collection of the withholding tax on income from movable assets is subject, especially with regard to the communication to the Direct Tax Department of the above-mentioned information and of information concerning the income produced by the said securities.

Done at ....., (date) .....

.....

Signature(s)

BOX RESERVED FOR THE ACCOUNT-KEEPING INSTITUTION

Name of the account-keeping institution: ----------

BIC11 of the participant or sub-participant: ----------

Security account opened in the applicant's name: ----------

[5] Account-keeping institutions not established in Belgium must forward the certificate and the information to NBB-SSS or to their Belgian participant via which they participate in the settlement system.

FPS FINANCE
Ledger service
Avenue des arts 30 - 1040 Brussels
Tel.: +32 (0)2 574 72 09 - Fax: +32 (0)2 233 70 86

Annex 3.2

INDIVIDUAL CERTIFICATE

FOR THE CONVERSION OF A REGISTRATION BY NAME

drawn up pursuant to Article 13 (2) of the Royal Decree of 26 May 1994 on the collecting and refunding of withholding tax in accordance with Chapter I of the Law of 6 August 1993 on transactions in certain securities.

.....

.....

.....

(full name and address of the issuer)

declares:

1. that BE.....
   (ISIN code and name) .....
   deposited on (dd/mm/yyyy) .....
   for a nominal amount of .....
   in the X/N settlement system managed by the National Bank of Belgium,
   were recorded continuously in the register of names from payment of the last coupon up to the day of deposit in the X/N system.

2. that the investor entered in that register for the amount in question
   .....
   .....
   .....
   (full name and address of the relevant investor) fulfils all the conditions for total exemption from withholding tax on income from movable assets and has the status of a person exempt from withholding tax under Article 4 of the said decree.

Done at ....., on.....

Signature(s) of the issuer's authorised representative(s)

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

Annex 3.3

List of beneficiaries of tax refunding

BIC11 ……..

Name ……..

Certificate pursuant to Art. 16 § 1, 3° of the Royal Decree of 26 May 1994 on the collection and payment of withholding tax on income from movable assets (R.V.) in accordance with Chapter I of the Law of 6 August 1993 on transactions in certain securities.

LIST OF NAMES OF BENEFICIARIES OF THE PAYMENT OF WITHHOLDING TAX ON INCOME FROM MOVABLE ASSETS ON WITHDRAWAL OF THE EXEMPT ACCOUNTS

ISIN Code: BE	Due date:		
Name and address of beneficiary	Tax date	Nominal	R.V.

Place and date of signature:

[Signature, name and position of the person(s) entitled to validly commit the institution]

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 3.4

TAX DATE CORRECTION

Participant BIC11			
Reference of incorrect instruction [1]			
Reference of amended instruction [1]			
ISIN			
Nominal value			
Value date of incorrect notification	day	month	year
Value date of corrected notification	day	month	year
Correct tax date	day	month	year

[1] Instructions before 02/02/2015: Sending Year and Number
Instructions after 02/02/2015: Participant Account Owner Reference

Reason for correcting the tax date:

Name and telephone number of the person responsible for this matter:

Participant's stamp

Signatures

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

X/N Report

Date:

Your reference:
Our reference:

Your correspondent:

Phone – Fax
sss@nbb.be

Annex 3.5

Withholding tax situation.

Normal notifications:

Fiscal date: 26.07.2006 **Security: BE0002145701 6 % OLO**

Notification	XN Code	Your reference	Nominal	Incomes	Withholding tax
2006 / 0	XN 12	2006-07-25876399	153,00 EUR	8,00 EUR	1,20
2006 / 313911	XN 12	0313911	25,50 EUR	1,33 EUR	0,20
2006 / 3173	XN 11	0313REF1	25,50 EUR	1,33 EUR	-0,20
2006 / 7643	XN 11	0313REF8	153,00 EUR	8,00 EUR	-1,20

Fiscal date: 26.07.2006 **Security: BE5962143867 TB/BT XYZ**

Notification	XN Code	Your reference	Nominal	Incomes	Withholding tax
2006 / 316111	XN 12	076399	1 000 000,00 EUR	0,00 EUR	0,00
2006 / 313881	XN 11	012563	1 000 000,00 EUR	0,00 EUR	0,00

Posted amount: **1,20**

Total: **1,20**

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

X/N Report - Corrections

NBB • boulevard de Berlaimont 14 • BE-1000 BRUSSELS
(addressee)

Date:
Your reference:
Our reference:

Your correspondent:

Phone – Fax
sss@nbb.be

Withholding tax situation.

Annulations and updates:

Fiscal date: 14.06.2006 **Security:** BE0002145701 6 % OLO

Notification	X/N Code	Your reference	Nominal	Incomes	Withholding tax
2006 / 0	XN 91	2006-07-25876399	1 000 000,00 EUR	2 199,80 EUR	329,97

Fiscal date: 26.07.2006 **Security:** BE0002145701 6 % OLO

Notification	X/N Code	Your reference	Nominal	Incomes	Withholding tax
2006 / 316111	XN 51	076399	1 000 000,00 EUR	0,00 EUR	0,00

Posted amount: 329,97

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

Primary market

Date:

Your reference:
Our reference:

Your correspondent:

Phone – Fax
sss@nbb.be

Annex 4

Tender on: 13.06.2006 **Competitive tender**
Subscriber: BE020100 ABC BANK

Waarde: BE0312620868 CERTIFICAT TRESORERIE **EUR**
Maturity date: **14.06.2007**

Following subscriptions have been accepted:

Date	Notification	Tender	Nominal amount	Cash amount in EUR	Consent (*)
13.06.2006	**1518**	11	**17 000 000,00** EUR	**12 777 741,58**	☑
	Settlement date:	**15.06.2006**			
	Securities account:	**100-8010061-99**			
			Amount payable in euro:	12 777 741,58	

Signature(s),

(*) The participant shall give his consent to subscriptions in behalf of his clients and shall return the present document duly signed to the NBB-SSS of the National Bank of Belgium before 11:00 am on the settlement day, except if any registration of your clients is not accepted.

☐ The participant gives his consent by signing in the appropriate place.

☑ The participant doesn't have to give his consent.

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 6

INSTRUCTIONS OF BEHALF

Instructions that need to be inserted into the system by NBB-SSS 'on behalf' of a participant should be sent via secured e-mail and will be charged. The Participant shall ensure that the "four eyes" principle is being guaranteed by having the Annex 6 signed by two end users who have the privileges to add and approve entering Instructions in the RAMSES GUI. Please take into account that fields marked with an "*" symbol are mandatory. "(m)", "(o)" and "(a)" mean that the field is a mandatory matching field, optional matching field, or additional matching field respectively.

Operation Type:
SecuritiesSettlementTransactionInstruction

Message Type:
sese.023.001.07

Instructing Party*:
-

Account Owner Reference*:

Securities Movement Type (m)*:
-

Common Trade Reference (o):

Payment Type (m)*:
-

Trade Date (m)*:

Cum/Ex Indicator (a):
-

Settlement Date (m)*:

Matching Status:
-

ISIN (m)*:

ISIN Description:

Face Amount (m)*:

Cash Amount (m):

Safekeeping Account*:

Cash Currency (m):
-

Securities Transaction Type*:
-

Credit Debit Indicator (m):
-

Yield to Maturity Rate:

Hold Indicator:
-

Automated Market Claim (a):
-

Hold Indicator Reason:
-

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Modification Cancellation Allowed:

-

Partial Settlement Indicator:

-

Priority:

-

Beneficial Ownership:

-

Delivering

Depository (m):

-

Party 1 (m):

-

Party 2:

SAFE Party 1 (o):

-

SAFE Party 2:

Party 1 Pledge Reference:

Party 2 Pledge Reference:

Receiving

Depository (m):

-

Party 1 (m):

-

Party 2:

SAFE Party 1 (o):

-

SAFE Party 2:

Party 1 Pledge Reference:

Party 2 Pledge Reference:

Links

Pool ID:

Current Instruction Number:

Total of Linked Instructions:

Instruction Links

Processing Position:

-

Reference Owner:

-

Account Owner Reference:

Date and Signatures:

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

Annex 8

Conditions of use of the RAMSES Graphical User Interface

Table of Contents

1.	**Scope**	**1**
2.	**Definitions**	**1**
3.	**Conditions for access to the RAMSES GUI**	**2**
4.	**Use of Certificates in order to access the RAMSES GUI and to pass valid instructions**	**3**
4.1	Applicable rules: CPS, CP	3
4.2	Respective roles and responsibilities of the involved Parties	4
4.2.1	*The BdE*	*4*
4.2.2	*The NBB*	*4*
4.2.3	*The Participant*	*5*
5.	**Change management**	**6**

1. Scope

In accordance with Article 6.2.1.1.2 of the Terms and conditions for the participation in the NBB-SSS, any Participant can send instructions manually and can send data to or receive information from the NBB-SSS in U2A modus and in pull and push mode through the RAMSES Graphical User Interface (GUI), having a connection with which is in principle mandatory for each Participant.

This document aims at defining the conditions of connection to and use of the RAMSES GUI, including the related certificates and tokens.

2. Definitions

Unless otherwise stated, the terms in this Annex shall follow the definitions as provided for in Article 2 of the "Terms and conditions for the participation in the NBB-SSS".

Furthermore, for the purpose of this Annex:

- "**BdE**" means the Banco de España, being the national central bank of the Kingdom of Spain;
- "**Certificate**" means an electronic file, issued by the BdE acting in the capacity of sole Certification authority in the framework of the RAMSES GUI and operator of the related PKI infrastructure, which binds a public key with a Certificate holder's identity and which is used for the following purposes:
  a) to verify that a public key belongs to the said Certificate holder;
  b) to electronically verify the identity of (= authenticate) the Certificate holder in order to verify his/her access rights to the NBB-SSS;
  c) to check a Certificate's holder signature.
- "**Certificate applicant**" means the physical person in favour of whom the issuance of a Certificate has been requested by the Participant to the BdE via the NBB acting in its role as Registration authority;
- "**Certificate holder**" means the physical person in favour of whom a Certificate has been issued by the BdE via the NBB acting in its role as Registration authority;
- "**Certificate user**" means either a Certificate holder or a Certificate applicant;
- "**Certification authority**" means the BdE it its capacity of entity trusted by the users of the certification services (Participants and Certificate users) to create, issue, manage, revoke and renew valid Certificates in the framework of the RAMSES GUI;
- "**CP**" stands for "Certificate Policy" and means the set of rules that define the applicability or use of a Certificate within a community of users that have a series of security requirements in common. The CP details and completes the CPS, containing the rules to which the use of the Certificates defined in this policy are subject, as well as the scope of application and the technical characteristics of this type of Certificate;
- "**CPS"** stands for "Certification practice statement" and means the set of norms and procedures that regulate the entire life-cycle of the Certificate used in the framework of the NBB-SSS, from its request to its end of subscription or revocation, as well as the relations that are established between the Participant, the NBB acting in its role as Registration authority, the Certificate applicant, the Certificate holder, the BdE acting in its role of Certification authority and the other Participants as relying parties of the said Certificate;
- "**ESCB**" means the European System of central banks, as ruled by the Treaty on the working of the European Union;
- **"Participant's member"** means a natural person who is either a member of the staff of a Participant or a member of its decision making bodies;

- "**PIN code**" means the personal identification number delivered with the Token to the Certificate user, which serves as a Token password preventing the use of the Token by another person than the Certificate holder by locking the Token after repeatedly and consecutively entering wrong PIN codes;
- "**PKI**" stands for "public key infrastructure" and means the set of individuals, policies, procedures, and computer systems necessary to provide authentication, integrity and non-repudiation services by way of public and private key cryptography and digital Certificates, used by the NBB for the secure access to and use of the RAMSES GUI by Participants;
- "**PKI services**" means the services performed by the NBB and, for a part, by the BdE on behalf of the NBB, in the framework of the proper operation and maintenance of the PKI;
- "**Public key**" means a random number which is attributed to the Certificate applicant and is made accessible to any relying party via a publicly accessible directory held by the BdE. The public key is mathematically and uniquely related, by a cryptographic technique to the private key, being another random number which is attributed to the Certificate applicant and which is not disclosed to any third parties, so that a set of data that is encrypted with a public key may only be decrypted by its corresponding private key and vice versa;
- "**PUK code**" means the personal unlock key number delivered with the Token to the Certificate user, which serves as an administration Token password allowing the Certificate holder to unlock a Token that has been locked after repeatedly and consecutively entering wrong PIN codes;
- "**Registration authority**" means the NBB in its capacity of entity trusted by the users of the certification services (Participants and Certificate users) to verify the identity of the Certificate applicant before requesting the issuance of the Certificate by the BdE acting in its role of Certification authority;
- "**Token**" means the data carrier device (including USB-devices), on which the Certificate is stored, and the use of which is conditioned by the entry of the personal identification number ("PIN code") of the Certificate holder;
- "**Trusted agent**" means the physical person who is appointed by the Participant to materially exert the competences resulting from the power of attorney entrusted by the NBB to verify on its behalf the identity of the Certificate user before physically delivering the Token to the latter.

3. Conditions for access to the RAMSES GUI

The Participant can access the RAMSES GUI if:

- it has installed and maintains a domestic IT infrastructure allowing a proper connection with the NBB-SSS;
- it has subscribed to the NBB-Net TCP/IP secured data transport network set up by the NBB in order to be connected with the NBB's IT infrastructure and networks;
- it has provided to the NBB the duly completed static data collection forms and any additional information required or deemed useful by the NBB for the Participant's registration;
- at least one Trusted agent appointed among the Participant's members has undersigned and sent to the NBB the sub-Annex 8.3 of the Terms and conditions;
- it has acquired the dedicated Tokens and Certificates in order to get authenticated and to validly and irrevocably sign instructions and notifications passed through the RAMSES GUI; and
- it has successfully passed the Participant certification tests.

The NBB shall notify the Participant of its registration for direct access to the RAMSES GUI or, as the case may be, its rejection. Any rejection decision shall be reasoned.

4. Use of Certificates in order to access the RAMSES GUI and to pass valid instructions

4.1 Applicable rules: CPS, CP

As a rule, each Participant shall be held liable in the case of breach of the obligations contained in the CPS, in the CP and, in general terms, in any mandatory legislation or regulation that should apply with regard to the possession and use of Certificates, by Certificate users or by the Trusted agent belonging to its organisation.

As the NBB-SSS makes a local use of the ESCB-wide PKI infrastructure operated by the BdE for the account of all national central banks of the Eurosystem, among which the NBB, the Participant acknowledges and agrees that in its relations with the NBB, with the BdE in its capacity of certification authority, and with all other Participants of the NBB-SSS, it shall be bound by the ESCB-PKI CPS and by the ESCB-PKI CP for the non-ESCB users' Certificates, which are fully applicable by analogy to the NBB-SSS. However, it is understood – and accepted by the Participant – that for the analogical application to the NBB-SSS of the said CPS and CP:

- the BdE shall be the sole Certification Authority, as referred to in Article 1.3.2 of the CPS, entitled to issue valid Certificates to be used in the NBB-SSS;
- the NBB shall be the sole Registration Authority, as referred to in Article 1.3.3 of the CPS, entitled to verify the identity of the Certificate applicants Certificates to be used in the NBB-SSS;
- the Participants are External Organisations for the application of the CPS;
- Certificate holders are Certificate Subscribers as referred to in Article 1.3.6.1 of the CPS; the Certificates delivered by the NBB will be advanced Certificates stored on a cryptographic device (USB-key) in the sense of Article 1.3.6.1 of the CP;
- all Participants of the NBB-SSS (including the NBB itself) are Relying Parties as referred to in Article 1.3.6.2 of the CPS;
- "the ESCB" must be understood as "the NBB" (in particular the NBB-SSS) for the application of Article 1.4 of the CPS;
- except when explicitly otherwise provided for in this Document, contacts between the Participants, the Certificate users and the BdE shall only occur through the compulsory intermediation of the NBB;
- the Articles 9.1, 9.2 and 9.7 of the CPS are not applicable, but only the relevant provisions of the Terms and conditions for the participation to the NBB-SSS relating to the same items;
- for the application of Article 3.2.3 and Article 4.2.1 of the CP, it is understood that the identity authentication of an individual Certificate applicant shall occur either through a direct face-to-face identification process of the said Certificate applicant, either through an indirect identification process based on the communication of the evidence required by the said Article 3.2.3 by the Trusted agent after a face-to-face identification of the Certificate applicant by the Trusted Agent. No Token shall be delivered to the Certificate applicant but by means of a physical handover either by the NBB or by the Trusted agent (no expedition by mail or courier);
- a query for a Certificate can only be initiated by using the ESCB-PKI web interface, not by means of the ESCB Identity Access Management as referred to Article 4.1.2.1 of the CP;
- each Participant is validly entrusted with a power of attorney to request either the issuance of a Certificate, the delivery of a Token and/or the revocation of a Certificate on behalf of any Certificate user who belongs to the said Participant.

The version 1.2 of the ESCB-PKI CPS (dated December 10, 2013) is joined as sub-Annex 8.1 of the Terms and conditions, and the version 1.1 of the ESCB-PKI CP for the non-ESCB users' Certificates (dated January 11, 2013) is joined as sub-Annex 8.2 of the Terms and conditions. The Participant explicitly acknowledges and agrees to be fully aware of the existence and of the content of the said

documents, which can be unilaterally amended from time to time without prior notice by the ESCB, in which case an actualised version is published on the website of the ECB[1] and is made available on the NBB-SSS teamsite.

4.2 Respective roles and responsibilities of the involved Parties

Without prejudice of the application of the CPS and CP as referred to in Article 4.1, which shall in any case enjoy precedence on the provisions of this Article, the following involved Parties are responsible for the provision of the following services :

4.2.1 The BdE

In its capacity of Certification authority and of Verification authority, the BdE is *e.g.* responsible for the following tasks:

- generating advanced Certificates on request of the NBB in favour of the Certificate applicants according to the CPS and the CP and informing both the NBB and the concerned Certificate applicant of this issuance;
- revoking Certificates on request of the NBB acting as Registration authority and publishing this revocation in real time via the online ESCB-PKI repository (OCSP) as well as periodically through downloadable Certificate revocation lists, as soon as possible after the revocation request has been received;
- confirming the validity of the Certificate used by the Certificate holder in order to authenticate himself or to sign an instruction;
- keeping an up-to-date directory containing all Certificates and information about their current pending, validity, expiration and revocation status.

In the execution of the said services, the BdE commits itself to:

- refrain from keeping, processing, copying, disclosing or forwarding information about the Certificate user other than strictly necessary for the provision of its PKI-related services;
- abide by the applicable personal data protection laws;
- inform the Certificate holder at least three months in advance of the expiration of the validity of his/her ongoing Certificate;
- follow the validation mechanism supplementary to the publication of the Certificate revocation lists; and
- in general, abide by all the obligations imposed by the CPS, CP and applicable legislation to any Certification authority and to any Verification authority.

Notwithstanding this list, the Participant acknowledges and agrees that the BdE only performs PKI services on behalf and in the capacity of sub-contractor of the NBB, so that no single legal boundary shall exist between the Participant and the BdE. The NBB shall therefore exclusively and solely bear any liability resulting from an evidenced non-performance of the PKI services materially performed by the BdE, however within the liability limits defined in the Terms and conditions.

4.2.2 The NBB

The NBB is *e.g.* responsible for the provision of Token Management services and Account management services toward each Certificate user.

[1] Address : http://pki.escb.eu/epkweb/en/repository.html. This hyperlink may be modified at any time without notice.

In its capacity of Registration authority, the NBB is *e.g.* responsible for the following types of services toward each Certificate user:

- adjusting its internal systems and interfaces to interoperate with the ESCB-PKI infrastructure in the framework of the RAMSES GUI;
- appointing NBB staff members in the role of PKI security officer, local identity administrator, personal Certificate requestor and registration officer before the start of operation of the RAMSES GUI and provide them with the adequate technical equipment;
- verifying the Participant's identity and its ongoing eligibility status with regard to the adherence to the NBB-SSS;
- verifying the Certificate applicant's and the Trusted agent's identity and registering their identity and other related data in the PKI;
- submitting each Certificate request to the BdE;
- registering the serial number of each delivered Token, the hereto related PIN and PUK codes, the identification data relating to the Certificate applicant on behalf of whom the Token is issued, and the identification data relating to the Participant to which the concerned Certificate applicant belongs;
- delivering, either physically, by postal mail or by courier and against written receipt, to the Certificate applicant or to the Trusted agent empowered by the NBB to verify the Certificate applicants' identity, one envelope per Certificate applicant with a view to the use of the RAMSES GUI in production environment, containing one Token, together with its initial PIN code and its PUK code, as well as the data needed to allow the download of the Certificate from the ESCB-PKI website, and;
- managing the replacement of lost, stolen, destroyed or damaged Tokens and revoking the Certificate stored on the said lost, stolen, destroyed or damaged Token;
- managing the blocking of a Token due to a loss of the PIN code or a repeated entry of a wrong PIN code;
- informing the Certificate holders about the working, functionalities, technical characteristics and requirements of the use of Certificates in the framework of the RAMSES GUI; and
- providing the service desk technical assistance to the Certificate holders via a single point of contact (SPOC), in case of an incident impeding or affecting a Participant's access to the NBB-SSS, which is not imputable to either SWIFT, the NBB-Net or the Participant's network service provider.

4.2.3 The Participant

The NBB shall validly rely on any information or message authenticated by a Certificate delivered to a Certificate holder who is a Participant's member and shall lawfully carry out instructions and settle transactions signed with such a Certificate in the name of the said Participant on its own behalf or on behalf of the Participant's clients. The Participant hereby acknowledges and agrees that it shall irrevocably, fully and definitely be bound by information, messages, instructions carried out and transactions settled by the NBB-SSS that are authenticated or signed with a Certificate delivered on behalf of one of the Participant's members and, therefore, that it bears full and exclusive responsibility and liability toward other Participants and third Parties, if any, for any misuse of the Token after its handover by the NBB to the Certificate applicant or the Trusted agent.

Furthermore, the Participant acknowledges and agrees that the "four-eye principle" is applicable to the signature of instructions so that two electronic signatures are required for the validation of the creation, the modification or the cancellation of each individual instruction.

The use of a Certificate shall be strictly personal to the Certificate holder and may not be shared with third parties, whether being Participant's members or not. No Certificate may be used as a group or entity-bound Certificate. The Participant shall take all security measures in order to prevent such an abuse of the Certificate. Any Certificate may be immediately revoked without prior warning or notice by the NBB if the latter becomes aware of such an abuse of the Certificate.

The Participant shall appoint at least one (preferably two or more) Trusted agent among the Participant's members in order to materially exert on the basis of a power of attorney delivered by the NBB, the competence to verify the identity of the Certificate user on behalf of the NBB before physically delivering to the said Certificate user the Token, together with the initial PIN code and the PUK code relating to the delivered Token and the associated user identification data linked with each delivered Token. The Participant shall verify that the Trusted agent has signed the "Terms and conditions relating to Trusted agents", joined as sub-Annex 8.3 of the Terms and conditions, and shall send the duly signed form to the NBB. Together with the Trusted agent, the Participant shall be responsible for the performance of the said identity verification and Token delivery tasks by the Trusted agent and bears the exclusive responsibility for the use of the said Tokens in order to send instructions and sign transactions in the Participant's name as soon as the Trusted agent has delivered to the NBB a signed receipt of the concerned Tokens. Therefore, the NBB shall not incur any liability for any damage resulting from a possible misuse of the said Tokens as from the same moment in time.

Without prejudice to the provisions of Article 6.2.1.2 of the Terms and conditions, each Participant shall design, test and implement adequate business continuity and contingency procedures and practicable IT-roundabouts in order to manage any denial of service or hampered operation of the RAMSES GUI.

The Participant shall implement adequate security controls in order to protect and prevent the RAMSES GUI from unauthorised access. The Participant shall ensure the adequate protection of the confidentiality, integrity and availability of its own IT systems.

The Participant shall inform the NBB of any security-related incident in its technical infrastructure and, where appropriate, security-related incidents that occur in the technical infrastructure of third party providers which may have an impact on the confidentiality, integrity and availability of the RAMSES GUI. The NBB may request further information about the incident and, if necessary, request that the Participant takes appropriate measures to prevent a recurrence of such an event. The NBB may also impose additional security requirements on the Participant.

The Participant shall inform the Certificate applicants of:

- the processing by the NBB, and by the BDE acting as sub-contractor on behalf of the NBB, of relevant personal data with the sole purpose of identifying the Certificate applicants in order to link the Token, and the Certificate stored on it, to the concerned Certificate applicant's identity;
- the personal data which are processed, being the Certificate applicant's name, surname, place and date of birth which are extracted from the copy of the Certificate applicant's identity documents joined as an annex to the certificate application form;
- the fact that the NBB is the sole responsible entity for the said processing of personal data;
- the NBB's complete address;
- the Certificate applicants' personal rights to consult and correct the above mentioned personal data processed by the NBB;
- the fact that these personal data shall be irrecoverably removed from the NBB's files one year after the revocation of the latest Certificate issued by BDE in the name of the Certificate user.

5. Change management

As the PKI makes use of the ESCB-PKI infrastructure, new ESCB-PKI features and functionalities, as well as changes to the ESCB-PKI's existing features and functionalities, may be implemented by the NBB in the PKI without prior notice. The NBB shall inform as soon as possible the Participants of the changes that may have a material impact on the provision of the PKI services or the procedures to be followed in this framework.

NBB - Securities
boulevard de Berlaimont 14
BE-1000 Brussels (Belgium)
Phone: +32 (0)2 221 22 14
Fax: + 32 (0)2 221 31 19
E-mail: sss@nbb.be

BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI SERVICES

OID: 0.4.0.127.0.10.1.2.1

CERTIFICATION PRACTICE STATEMENT

VERSION 1.3

1 June 2015

Table of Contents

CONTENT, RIGHTS AND OBLIGATIONS ESTABLISHED IN THIS CERTIFICATION PRACTICE STATEMENT *10*

1 Introduction *11*

1.1 Overview **11**

1.2 Document Name and Identification **12**

1.3 ESCB-PKI Participants **13**

1.3.1 The Policy Approval Authority 13

1.3.2 Certification Authority 13

1.3.3 Registration Authorities 15

1.3.4 Validation Authority 16

1.3.5 Key Archive 16

1.3.6 Users 17

1.4 Certificate Usage **18**

1.4.1 Appropriate certificate use 18

1.4.2 Certificate usage constraints and restrictions 18

1.5 Policy Approval **19**

1.5.1 The governing bodies of the ECB 19

1.5.2 Contact Person 19

1.5.3 Establishment of the suitability of a CPS from an External CA as regards the ESCB-PKI Certificate Policies 19

1.5.4 Approval Procedure for this CPS 19

1.6 Definitions and Acronyms **19**

1.6.1 Definitions 19

1.6.2 Acronyms 21

2 Publication and Repository Responsibilities *23*

2.1 Repositories **23**

2.2 Publication of Certification Data, CPS and CP **23**

2.3 Publication Timescale or Frequency **24**

2.4 Repository Access Controls **24**

3 Identification and Authentication (I&A) *25*

3.1 Naming **25**

3.1.1 Types of names 25

3.1.2 The need for names to be meaningful 25

3.1.3 Rules for interpreting various name formats 25

3.1.4 Uniqueness of names 25

3.1.5 Name dispute resolution procedures 25

3.1.6 Recognition, authentication, and the role of trademarks 25

3.2 Initial Identity Validation **25**

3.2.1 Means of proof of possession of the private key 25

3.2.2 Identity authentication for an entity 25
3.2.3 Identity authentication for an individual 26
3.2.4 Non-verified applicant information 26
3.2.5 Validation of authority 26
3.2.6 Criteria for operating with external CAs 26

3.3 Identification and Authentication for Re-key Requests 26
3.3.1 Identification and authentication requirements for routine re-key 26
3.3.2 Identification and authentication requirements for re-key after certificate revocation 27

4 Certificate Life Cycle Operational Requirements 28

4.1 Certificate Application 28
4.1.1 Who can submit a certificate application? 28
4.1.2 Enrolment process and applicants' responsibilities 28

4.2 Certificate Application Processing 28
4.2.1 Performance of identification and authentication procedures 28
4.2.2 Approval or rejection of certificate applications 28
4.2.3 Time limit for processing the certificate applications 29

4.3 Certificate Issuance 29
4.3.1 Actions performed by the CA during the issuance of the certificate 29
4.3.2 CA notification to the applicants of certificate issuance 29

4.4 Certificate Acceptance 29
4.4.1 Form of certificate acceptance 29
4.4.2 Publication of the certificate by the CA 29
4.4.3 Notification of certificate issuance by the CA to other Authorities 30

4.5 Key Pair and Certificate Usage 30
4.5.1 Certificate subscribers' use of the private key and certificate 30
4.5.2 Relying parties' use of the public key and the certificate 30

4.6 Certificate Renewal 30
4.6.1 Circumstances for certificate renewal with no key changeover 30

4.7 Certificate Re-key 30
4.7.1 Circumstances for certificate renewal with key changeover 30
4.7.2 Who may request certificate renewal? 30
4.7.3 Procedures for processing certificate renewal requests with key changeover 31
4.7.4 Notification of the new certificate issuance to the certificate subscriber 31
4.7.5 Manner of acceptance of certificates with changed keys 31
4.7.6 Publication of certificates with the new keys by the CA 31
4.7.7 Notification of certificate issuance by the CA to other Authorities 31

4.8 Certificate Modification 31
4.8.1 Circumstances for certificate modification 31

4.9 Certificate Revocation and Suspension 32
4.9.1 Circumstances for revocation 32
4.9.2 Who can request revocation? 32
4.9.3 Procedures for requesting certificate revocation 33
4.9.4 Revocation request grace period 33
4.9.5 Time limit for the CA to process the revocation request 33

4.9.6 Requirements for revocation verification by relying parties 33
4.9.7 CRL issuance frequency 34
4.9.8 Maximum latency between the generation of CRLs and their publication 34
4.9.9 Online certificate revocation status checking availability 34
4.9.10 Online revocation checking requirements 34
4.9.11 Other forms of revocation alerts available 34
4.9.12 Special requirements for the revocation of compromised keys 34
4.9.13 Causes for suspension 34
4.9.14 Who can request the suspension? 34
4.9.15 Procedure for requesting certificate suspension 35
4.9.16 Suspension period limits 35

4.10 Certificate Status Services 35
4.10.1 Operational characteristics 35
4.10.2 Service availability 35
4.10.3 Additional features 35

4.11 End of Subscription 35

4.12 Key Escrow and Recovery 35
4.12.1 Key escrow and recovery practices and policies 35
4.12.2 Session key protection and recovery policies and practices 36

5 Facility Management, and Operational Controls 37

5.1 Physical SecurityControls 37
5.1.1 Site location and construction 37
5.1.2 Physical access 37
5.1.3 Power and air-conditioning 37
5.1.4 Water exposure 37
5.1.5 Fire prevention and protection 37
5.1.6 Storage system 38
5.1.7 Waste disposal 38
5.1.8 Offsite backup 38

5.2 Procedural Controls 38
5.2.1 Roles responsible for PKI control and management 38
5.2.2 Number of individuals required to perform each task 40
5.2.3 Identification and authentication of each user 40
5.2.4 Roles that require separation of duties 40

5.3 Personnel Controls 40
5.3.1 Requirements concerning professional qualification, knowledge and experience 40
5.3.2 Background checks and clearance procedures 41
5.3.3 Training requirements 41
5.3.4 Retraining requirements and frequency 41
5.3.5 Frequency and sequence for job rotation 41
5.3.6 Sanctions for unauthorised actions 41
5.3.7 Requirements for third party contracting 41
5.3.8 Documentation supplied to personnel 41

5.4 Audit Logging Procedures 41
5.4.1 Types of events recorded 41

5.4.2 Frequency with which audit logs are processed ... 42
5.4.3 Period for which audit logs are kept ... 42
5.4.4 Audit log protection ... 42
5.4.5 Audit log back up procedures ... 42
5.4.6 Audit data collection system ... 43
5.4.7 Notification to the subject who caused the event ... 43
5.4.8 Vulnerability assessment ... 43

5.5 Records Archival ... 43
5.5.1 Types of records archived ... 43
5.5.2 Archive retention period ... 43
5.5.3 Archive protection ... 44
5.5.4 Archive backup procedures ... 44
5.5.5 Requirements for time-stamping records ... 44
5.5.6 Audit data archive system (internal vs. external) ... 44
5.5.7 Procedures to obtain and verify archived information ... 44

5.6 Key Changeover ... 44

5.7 Compromise and Disaster Recovery ... 44
5.7.1 Incident and compromise handling procedures ... 44
5.7.2 Corruption of computing resources, software, and/or data ... 45
5.7.3 Action procedures in the event of compromise of an Authority's private key ... 45
5.7.4 Installation following a natural disaster or another type of catastrophe ... 45

5.8 CA or RA Termination ... 45
5.8.1 Certification Authority ... 45
5.8.2 Registration Authority ... 46

6 Technical Security Controls ... 47

6.1 Key Pair Generation and Installation ... 47
6.1.1 Key pair generation ... 47
6.1.2 Delivery of private keys to certificate subscribers ... 47
6.1.3 Delivery of the public key to the certificate issuer ... 47
6.1.4 Delivery of the CA's public key to relying parties ... 47
6.1.5 Key sizes ... 47
6.1.6 Public key generation parameters and quality checks ... 47
6.1.7 Accepted key usage (KeyUsage field in X.509 v3) ... 47

6.2 Private Key Protection and Cryptographic Module Engineering Controls ... 48
6.2.1 Cryptographic module standards ... 48
6.2.2 Private key multi-person (k out of n) control ... 48
6.2.3 Escrow of private keys ... 48
6.2.4 Private key backup copy ... 48
6.2.5 Private key archive ... 49
6.2.6 Private key transfer into or from a cryptographic module ... 49
6.2.7 Private key storage in a cryptographic module ... 49
6.2.8 Private key activation method ... 49
6.2.9 Private key deactivation method ... 49
6.2.10 Private key destruction method ... 49
6.2.11 Cryptographic module classification ... 49

6.3 Other Aspects of Key Pair Management 49
6.3.1 Public key archive 49
6.3.2 Operational period of certificates and usage periods for key pairs 49
6.4 Activation Data 50
6.4.1 Generation and installation of activation data 50
6.4.2 Activation data protection 50
6.4.3 Other activation data aspects 50
6.5 Computer Security Controls 50
6.5.1 Specific security technical requirements 50
6.5.2 Computer security evaluation 50
6.6 Life Cycle Security Controls 50
6.7 Network Security Controls 51
6.8 Timestamping 51
7 Certificate, CRL, and OCSP Profiles 52
7.1 Certificate Profile 52
7.1.1 Version number 52
7.1.2 Certificate extensions 52
7.1.3 Algorithm Object Identifiers (OID) 53
7.1.4 Name formats 53
7.1.5 Name constraints 53
7.1.6 Certificate Policy Object Identifiers (OID) 53
7.1.7 Use of the "PolicyConstraints" extension 53
7.1.8 Syntax and semantics of the “PolicyQualifier 53
7.1.9 Processing semantics for the critical “Certificate Policy” extension 54
7.2 CRL Profile 54
7.2.1 Version number 54
7.2.2 CRL and extensions 54
7.3 OCSP Profile 54
7.3.1 Version number(s) 54
7.3.2 OCSP Extensions 54
8 Compliance Audit and Other Assessment 55
8.1 Frequency or Circumstances of Controls for each Authority 55
8.2 Identity/Qualifications of the Auditor 55
8.3 Relationship between the Assessor and the Entity being Assessed 55
8.4 Aspects Covered by Controls 55
8.5 Actions Taken as a Result of Deficiencies Found 55
8.6 Notification of the Results 56
9 Other Business and Legal Matters 57
9.1 Fees 57
9.1.1 Certificate issuance or renewal fees 57
9.1.2 Certificate access fees 57

9.1.3 Revocation or status information fees 57
9.1.4 Fees for other services, such as policy information 57
9.1.5 Refund policy 57
9.2 Financial Responsibility 57
9.2.1 Insurance 57
9.2.2 Other assets 57
9.2.3 Insurance or warranty coverage for end-entities 57
9.3 Confidentiality of Business Information 57
9.3.1 Scope of confidential information 58
9.3.2 Non-confidential information 58
9.3.3 Duty to maintain professional secrecy 58
9.4 Privacy of Personal Information 58
9.4.1 Personal data protection policy 58
9.4.2 Information considered private 59
9.4.3 Information not classified as private 59
9.4.4 Responsibility to protect personal data 59
9.4.5 Notification of and consent to the use of personal data 59
9.4.6 Disclosure within legal proceedings 59
9.4.7 Other circumstances in which data may be made public 59
9.5 Intellectual Property Rights 59
9.6 Representations and Warranties 60
9.6.1 Obligations of the CA 60
9.6.2 Obligations of the RA 61
9.6.3 Obligations of certificate subscribers 62
9.6.4 Obligations of relying parties 62
9.7 Disclaimers of Warranties 63
9.7.1 ESCB-PKI liabilities 63
9.7.2 Scope of liability coverage 63
9.8 Limitations of Liability 63
9.9 Indemnities 64
9.10 Term and Termination 64
9.10.1 Term 64
9.10.2 CPS substitution and termination 64
9.10.3 Consequences of termination 64
9.11 Individual notices and communications with participants 65
9.12 Amendments 65
9.12.1 Amendment procedures 65
9.12.2 Notification period and mechanism 65
9.12.3 Circumstances in which the OID must be changed 65
9.13 Dispute Resolution Procedures 65
9.14 Governing Law 65
9.15 Compliance with Applicable Law 66

9.16 Miscellaneous Provisions 66
9.16.1 Entire agreement clause 66
9.16.2 Independence 66
9.16.3 Resolution through the courts 66
9.17 Other Provisions 66

Control Sheet

	Title	Certification Practice Statement
	Author	ESCB-PKI Service Provider
	Version	1.3
	Date	11.05.2015

RELEASE NOTES

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column "Release number" refer to the current version of the document.

Release number	Status	Date	Change Reason
0.1	Draft	07.04.2011	First draft
0.2	Draft	27.05.2011	BdE revision
0.3	Draft	15.06.2011	BdE revision
0.4	Draft	17.06.2011	BdE revision. Validate Compliance with RFC
0.5	Draft	14.07.2011	BdE revision
0.6	Draft	22.07.2011	BdE revision
0.7	Draft	26.07.2011	Added CA fingerprint
0.8	Draft	02.09.2011	Update after SRM-WG and PKI-AB revision
1.0	Final	19.10.2011	Update after ITC approval.
1.1	Final	11.01.2013	GovC approval.
1.2	Final	10.12.2013	New ESCB users' certificate types for mobile devices, shared mailbox, administrator and provisional.
1.3	Final	01.06.2015	Hashing algorithm update Scope extension to ESCB/SSM.

CONTENT, RIGHTS AND OBLIGATIONS ESTABLISHED IN THIS CERTIFICATION PRACTICE STATEMENT

This section provides an overview of the content, rights and obligations established in this Certification Practice Statement (CPS). Its content must be supplemented with the corresponding Certificate Policy (CP), applicable to the certificate requested or being used.
It is recommended that this CPS be read fully, as well as the applicable CPs, in order to understand the purposes, specifications, regulations, rights, obligations and responsibilities governing the provision of the certification service.

- This CPS and the related documentation regulate the entire life-cycle of electronic certificates, from their request to their end of subscription or revocation, as well as the relations that are established between the certificate applicant, the certificate subscriber, the Certification Authority and the relying parties. It takes into consideration the requirements for certificates foreseen in Directive 1999/93/EC of the European Parliament and of the Council[1], and Regulation (EU) No 910/2014 of the European Parliament and of the Council[2].
- The European System of Central Banks PKI issues different types of certificates for which there are specific Certificate Policies (CP). Consequently, when requesting any kind of certificate and in order to request and use them correctly, those applying must be aware of the content of this CPS and, as appropriate, the applicable CP.
- The following Certificate Policies are available: i) the Certificate Policies for the ESCB/SSM users' certificates, governing the personal certificates issued by the ESCB-PKI Certification Authority for ESCB/SSM users (i.e. users that belong to ESCB Central Banks or SSM National Competent Authorities) and ii) the Certificate Policies for the non-ESCB/non-SSM users' certificates, governing the personal certificates issued by the ESCB-PKI Certification Authority for non-ESCB/non-SSM users (i.e. users that belong to external organisations outside the ESCB and the SSM)
- The CPS and the CPs set out the scope of liabilities for the different parties involved, as well as their limits as regards possible damages.
- The CPS and the CPs are available to certificate applicants, certificate subscribers and relying parties on the website http://pki.escb.eu/policies
- Certificate subscribers shall make appropriate use of certificates and shall be solely responsible for any use other than that specified in the CPS and corresponding CP.
- Certificate subscribers shall notify the relevant Registration Authority of any modification or variation in the personal data provided to obtain the certificate, regardless of whether or not said data is included on the certificate itself.
- Safekeeping of the private key by certificate subscribers is an essential requirement for the security of the system. Therefore, the Registration Authority must immediately be informed of the existence of any of the causes established in the CPS for revocation/suspension of certificate validity, thus enabling suspension/revocation of the compromised certificate to prevent its illegal use by unauthorised third parties.

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).
2 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (OJ L 257, 28.8.2014, p. 73).

- Persons who wish to rely on a certificate are responsible for verifying, using the information sources provided, that the certificate and the rest of the certificates in the chain of trust are valid and have not expired or been suspended or revoked.

For more information, consult the website established for this purpose at http://pki.escb.eu/ or contact the Certification Authority by e-mail at escb-pki@pki.escb.eu, or your respective Registration Authority.

1 Introduction

1.1 Overview

This Certification Practice Statement (CPS) describes the certification practices for the functioning and operations of the Public Key Infrastructure (hereinafter referred to as 'PKI') of the European System of Central Banks (hereinafter referred to as 'ESCB-PKI'). It has been drafted in compliance with the **Decision ECB/2013/1 of the European Central Bank**[1].

This document is intended for the use of all the participants related to the ESCB-PKI hierarchy, including the Certification Authority (CA), Registration Authorities (RA), certificate applicants, certificate subscribers and relying parties, among others.
This CPS has been structured in accordance with the guidelines of the PKIX work group in the IETF (Internet Engineering Task Force) in its reference document RFC 3647 (approved in November 2003) "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". In order to give the document a uniform structure and facilitate its reading and analysis, all the sections established in RFC 3647 have been included. Where nothing has been established for a given section the phrase "No stipulation" will appear. Furthermore, when drafting its content, European standards have been taken into consideration, among which the most significant are:

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
- ETSI TS 101 862: Qualified Certificate Profile.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

Likewise, the following relevant legal framework has been considered:

- Decision (EU) 2015/XX (ECB/2015/XX)[2];
- Directive 95/46/EC of EC of the European Parliament and of the Council[3]; Directive 1999/93/EC of the European Parliament and of the Council[1]; Regulation (EU) No 910/2014 of

[1] Decision ECB/2013/1of the European Central Bank of 11 January 2013 laying down the framework for a public key infrastructure for the European System of Central Banks (OJ L 74, 16.3.2013, p. 30).
[2] Decision (EU) 2015/[XX] of [date, month] 2015 on the access and use of SSM electronic applications, systems, platforms and services by the European Central Bank and the national competent authorities of the Single Supervisory Mechanism (ECB/2015/XX), not yet published in the Official Journal of the European Union.
[3] Directive 95/46/EC of EC of the European Parliament and of the Council of 24 October 1994 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

the European Parliament and of the Council[2];Spanish Law 59/2003, of 19 December, the Electronic Signature Act (Spanish Official Journal, 20 December).[3]

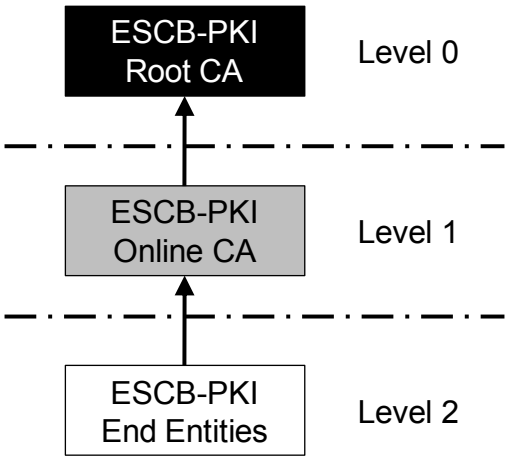
- Spanish Organic Law 15/1999, of 13 December 1999, on the protection of personal data
- Spanish Royal Decree 1720/2007, of 21 December2007, approving the Regulations for the development of Spanish Organic Law 15/1999.
- National legislation transposing Directive 95/46/EC and the Directive 99/93/EC applicable to the ESCB central banks and SSM national competent authorities acting as Registration Authorities.

This CPS sets out the services policy, as well as a statement on the level of guarantee provided, by way of description of the technical and organisational measures established to guarantee the PKI's level of security.

The CPS includes all the activities for managing electronic certificates throughout their life cycle, and serves as a guide for the relations between ESCB-PKI and its users. Consequently, all the PKI participants (see section 1.3) must be aware of the content of the CPS and adapt their activities to the stipulations therein.

This CPS assumes that the reader is conversant with PKI, certificate and electronic signature concepts. If not, readers are recommended to obtain information on the aforementioned concepts before they continue reading this document.

The general architecture of the ESCB-PKI, in hierarchic terms, is as follows:



1.2 Document Name and Identification

Document name	Certification Practice Statement for the European System of Central Banks Public Key Infrastructure (ESCB-PKI)
Document version	1.3
Document status	Final

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

2 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (OJ L 257, 28.8.2014, p. 73).

[3]Spanish legislation is also considered owed to the fact that Banco de España, the Service Provide, is established at Spain

Date of issue	11.05.2015
OID (Object Identifier)	0.4.0.127.0.10.1.2.1
CPS location	http://pki.escb.eu/policies

1.3 ESCB-PKI Participants

The participating entities and persons are:

- The Eurosystem Central Banks and the ECB, as the owners of the ESCB-PKI
- The governing bodies of the ECB as the Policy Approval Authority
- Banco de España, as the Service Provider, has the overall responsibility on the technical components that provide all PKI services:
    - The CA.
    - The RAs.
    - The Validation Authority.
    - The Key Archive.
- Banco de España, as the Service Provider, has also the responsibilities assigned in this document to the Certification Authority, Validation Authority and Key Archive.
- The ESCB Central Banks, including Banco de España, and the SSM National Competent Authorities, acting as Registration Authorities.
- The users of the certificates issued by the ESCB-PKI.

1.3.1 The Policy Approval Authority

The Policy Approval Authority (PAA) is the governing bodies of the ECB. The PAA approves the ESCB-PKI Certification Practice Statement (CPS) and related Certificate Policies (CP), as well as oversees the regular revision of the aforementioned documents with the assistance of the Information Technology Committee (ITC).

1.3.2 Certification Authority

The CA is the authority trusted by the users of the certification services (i.e. certificate subscribers as well as relying parties) to create and assign certificates. The CA is identified in the certificate as the issuer and its private key is used to sign certificates. The CA is in charge of issuing both private and public key certificates and revocation lists, and generating key pairs associated with specific certificates (i.e. those that require key recovery). The CA signs and manages public key certificates.

The CA relies on other parties to provide parts of the certification service (i.e. the CA relies on the Registration Authorities to identify the certificate applicants). However, the CA always maintains overall responsibility and ensures that the policy requirements identified in the present document are met.

The CA includes all individuals, policies, procedures and computer systems entrusted with issuing the electronic certificates and assigning them to their certificate subscribers.

This role is assigned to Banco de España.

The Certification Authority includes two technical components:

- **The Root ESCB-PKI Certification Authority**: First-level Certification Authority. This CA only issues certificates for itself and its Subordinate CAs. It will only be in operation whilst carrying out the operations for which it is established. Its most significant data are:

SHA-1 certificate[1]:

Distinguished Name	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial Number	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Distinguished Name of Issuer	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity Period	From 21-06-2011 11:58:26 to 21-06-2041 11:58:26
Message Digest (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Message Digest (SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Cryptographic algorithms	SHA-1 / RSA 4096

SHA-256 certificate:

Distinguished Name	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial Number	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8
Distinguished Name of Issuer	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity Period	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
Message Digest (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message Digest (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Cryptographic algorithms	SHA-256 / RSA 4096

- The Online ESCB-PKI Certification Authority: Certification Authority subordinated to the ESCB-PKI Root CA. It is responsible for issuing the ESCB-PKI end entities[2] certificates. Its most significant data are:

SHA-1 certificate[3]:

Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial Number	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished Name of Issuer	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU

[1] This certificate will be used only in systems that do not support higher algorithms.

[2] In this CPS the term end entity is used to represent users in general including their roles as subscribers and relying parties.

[3] This certificate will be used only in systems that do not support higher algorithms.

Validity Period	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message Digest (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Message Digest (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Cryptographic algorithms	SHA-1 / RSA 4096

SHA-256 certificate:

Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial Number	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Distinguished Name of Issuer	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity Period	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message Digest (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message Digest (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Cryptographic algorithms	SHA-256 / RSA 4096

1.3.3 Registration Authorities

A Registration Authority (RA) includes individuals, policies, procedures and computer systems entrusted with verifying the identity of those applying for electronic certificate and, when appropriate, of the attributes associated with them.

RAs shall identify those applying for certificates pursuant to the rules established in this CPS and the corresponding CP; the relations between both parties will be governed by this CPS and the applicable CP.

1.3.3.1 Registration Authorities' roles

RA roles, which shall be performed in accordance with this CPS and the relevant CPs, are the following:

The following roles shall be performed by all the Eurosystem Central Banks and the ECB, as well as by the Central Banks outside the Euro area and the SSM National Competent Authorities that join the ESCB-PKI:

- **Registration Officers for External Organisations**: Registration Officers for External Organisations (RO4EO) are a particular type of Registration Officers, described below. They belong to an ESCB Central Bank or a SSM National Competent Authority and are in charge of managing electronic certificates for persons and technical components that belong to external organisations, typically (but not always) from the same country where the Central Bank or National Competent Authority is located.

- **Registration Officers**: Registration Officers (ROs) are the people responsible for identifying certificate applicants, validating the documentation required during the identification process,

gathering all the information necessary to issue the public key certificate and finally allowing the user to retrieve the certificate. They interact with the ESCB-PKI Registration Authority subsystem.
ROs are in charge of managing electronic certificates for persons that belong to their Central Bank or SSM National Competent Authority. It will be up to each Central Bank and National Competent Authority to decide the legal binding within the group of people that it will manage (i.e. just internal employees, subcontractors, etc.)

- **Trusted Agent**: they are the people authorised to act as a representative of a Registration Authority in providing face to face identification of certificate applicants during the registration process. Trusted Agents will not have automated interfaces with the RA. It will be up to each Registration Authority to decide the legal binding with the Trusted Agent.

- **Registration Officers for Technical Components**: The Registration Officer for Technical Components (RO4TC) is a specific type of Registration Officer that is in charge of managing technical certificates by approving or rejecting certification requests from technical certificate applicants.

- **Key Recovery Officers**: This role is performed by the ESCB Central Banks and SSM National Competent Authorities that decide to use the Key Recovery service. Key Recovery Officers (KROs) participate during the recovery of encryption key pairs from the Key Archive (see section 1.3.5), when the owner of the key pair is not present. Four-eye principle will always be required to recover any key pair. This role shall only be available at those Central Banks and National Competent Authorities that decide to use the Key Archive service.

- **Shared Mailbox Administrator**: The Shared Mailbox Administrator (SMA) role is in charge of defining in the ESCB-PKI system the attributes of those shared mailboxes that require an electronic certificate.

1.3.4 Validation Authority

The Validation Authority (VA) is in charge of providing online information about revocation status and is responsible for verifying the status of the certificates issued by the ESCB-PKI, by way of the *Online Certificate Status Protocol* (OCSP), which determines the current status of an electronic signature at the request of a relying party, without the need to access the Certificate Revocation Lists.
This role is assigned to Banco de España.
This validation mechanism is supplementary to the publication of the Certificate Revocation Lists (CRL).

1.3.5 Key Archive

The Certificate Policies may establish the existence of a Key Archive (KA) that will be in charge of storing a copy of specific key pairs that need to be recovered in case of loss. A KA encompasses a computer system, together with the corresponding policies and procedures, that enables the archiving and recovery of the private keys belonging to certificate subscribers of the certificates regulated under said policies. The Key Archive must guarantee the confidentiality of the private keys and their recovery must require the intervention of at least two people. The CP must regulate the request and processing procedures for key recovery.
Under no circumstances will private keys linked to electronic signature certificates be archived.

1.3.6 Users

This section describes the end user roles, i.e. users without responsibilities in managing certificates for other users.

1.3.6.1 Certificate Subscribers

A certificate subscriber is an individual who is the subject of an electronic certificate and has been issued an electronic certificate and/or a technical component manager who has accepted an electronic certificate issued for a technical component by the ESCB-PKI Certification Authority.

Certificate entitlement becomes effective once the certificate has been issued by the CA and the certificate applicant has accepted the required terms and conditions application form.

The population of certificate subscribers that can hold each type of certificate will be defined and limited in the related CP.

Certificates subscribers have, among others, the following obligations:

- Provide accurate, complete and truthful information regarding the data requested to carry out the registration process;
- To inform the corresponding RA of any modification to said data;
- Take the necessary security measures in order to avoid loss, modification or unauthorised use of the cryptographic card issued;
- The process to obtain the certificates requires the personal selection of a control PIN for the cryptographic token. The certificate subscriber is responsible for keeping the PIN and PUK numbers secret;
- Request the revocation of the certificates in the event of detecting any inaccuracy in the information contained therein or becoming aware of or suspecting any reduction in the reliability of the private key corresponding to the public key contained in a certificate and due, among other causes, to loss, theft, or knowledge by third parties of the PIN and/or PUK;
- Fulfil any other obligation derived from the CPS and the Certificate Policies;
- Understand and accept the terms and conditions for using certificates and, specifically, those contained in the applicable CPS and CPs (the more relevant information is included in this section and in sections 4.1.2, 4.5 and 9.6.3).

The certificate subscriber will be held responsible in case of non-compliance with her/his obligations and in case of wrongful use of the certificate, or the untruthfulness or inaccuracy of the information submitted at the certificate request to the Registration Authority.

The certificate subscriber shall abide to what is established in this CPS and the corresponding CPs.

In case of shared mailbox certificates, the certificate subscriber will be the person responsible for the shared mailbox.

The types of entities that can hold the ESCB-PKI certificates are defined and limited in each CP. In general terms, without prejudice to the CP in each case, the following chart shows some of the types of ESCB-PKI certificate subscribers:

Certification Authority	Certificate subscribers
Online CA	Users from ESCB Central Banks or SSM National Competent Authorities (ESCB/SSM users) Users from external organisations non-ESCB/non-SSM users) Individuals in charge of the ESCB/SSM applications and technical components that use the certificate ESCB-PKI entities

1.3.6.2 Relying Parties

A relying party is an individual or an entity other than a certificate subscriber that decides to accept and rely on a certificate. That is, relying parties understand the linkage between the public key contained in a certificate and the identity of the subscriber, in order to verify the integrity of a digitally signed message, recognise the creator of a message or establish confidential communications with the certificate subscriber.

Relying parties must make use of the information contained in the certificate (such as the certificate policy identifiers) to determine the suitability of the certificate for a particular use.The following are the responsibilities of the relying parties that trust in ESCB-PKI certificates:

- Check the public key of the Service Provider's certificate before trusting any certificate issued by ESCB-PKI;
- Check the certificates chain of trust, from the root CA to the last subordinate CA, through queries to the CRLs or through OCSP;
- Check and take into account all restrictions for the use of a given certificate that are stated in the corresponding CPs;
- Notify either any Registration Authority or Banco de España, as the Certification Authority, about any anomaly related to a certificate which is deemed to be a cause for its revocation.

1.4 Certificate Usage

1 Certificates issued by the ESCB-PKI may only be used within the scope of the ESCB/SSM by:

- **a** Users from the ESCB/SSM
- **b** External users to interact with the ESCB/SSM
- **c** ESCB/SSM applications and technical components

2 Within the scope of the paragraph above, certificates issued by ESCB-PKI may be used for financial activities.

1.4.1 Appropriate certificate use

The appropriate use of each certificate is established in the Certificate Policies corresponding to each type of certificate. It is not the purpose of this CPS to determine that usage.

1.4.2 Certificate usage constraints and restrictions

The certificates must be used in accordance with the functions and purposes defined in their corresponding CP and may not be used for activities or purposes not included therein.

Likewise, the certificates must be used solely in accordance with the applicable legislation.
Unless otherwise specified in the CP, the certificates may not be used to act as RAs or CA, or for signing public key certificates of any kind or Certificate Revocation Lists (CRL).
The certification services provided by ESCB-PKI have not been designed nor are they authorised for use in high risk activities or those that require fail-safe operations, such as those related to the running of hospital, nuclear or air or rail traffic control facilities, or any other where failure could lead to death, personal injury or serious environmental damage.
The CPs corresponding to each certificate may establish additional certificate usage constraints or restrictions. It is not the purpose of this CPS to establish those additional constraints and restrictions.

1.5 Policy Approval

1.5.1 The governing bodies of the ECB

This CPS is approved by the Governing Council, with the assistance of the Eurosystem/ESCB Committees, in particular the Information Technology Committee (ITC).

1.5.2 Contact Person

This CPS is managed by the Policy Approval Authority (PAA) for ESCB-PKI:

Name	Banco de España
E-mail address	escb-pki@pki.escb.eu
Postal Address	Information Systems Department C/Alcala, 522. 28027 - Madrid (Spain)

1.5.3 Establishment of the suitability of a CPS from an External CA as regards the ESCB-PKI Certificate Policies

In the event of having to evaluate the possibility of an external CA interoperating with ESCB-PKI, the ITC will determine whether or not the CPS of the external CA is suitable for the CP in question. The procedures for establishing suitability are included in the CP that contemplates the possibility of operating with other CAs.

1.5.4 Approval Procedure for this CPS

The Service Provider (Banco de España) will elaborate the new versions of this CPS and the CPs. The Governing Council, with the assistance of the Eurosystem/ESCBCommittees, in particular the Information Technology Committee (ITC) will approve the documents.

1.6 Definitions and Acronyms

1.6.1 Definitions

Within the scope of this CPS the following terms are used:

Authentication: the process of confirming the identity of a certificate subscriber.
Identification: the process of verifying the identity of those applying for a certificate.

Eurosystem Central Bank: means either an NCB of a Member State whose currency is the euro or the ECB.
Non-euro area NCB: means an NCB of a Member State whose currency is not the euro.
ESCB Central Bank: means either a Eurosystem Central Bank or a non-euro area NCB**.**
Central Bank: In this CPS the term "Central Bank" is used to refer to any Central Bank belonging to the European System of Central Banks (ESCB)/Eurosystem, including the ECB, that has agreed to use the ESCB-PKI.
National Competent Authority or SSM National Competent Authority: means any National Competent Authority (NCA) belonging to the Single Supervisory Mechanism (SSM) that has agreed to use the ESCB-PKI.
ESCB/SSM user: user that belongs to an ESCB Central Bank or SSM National Competent Authority.
External or non-ESCB/non-SSM Organisation: public or private organisation that do not belong to the European System of Central Banks (ESCB) or the Single Supervisory Mechanism (SSM).
Non-ESCB/non-SSM user: user that belongs to a non-ESCB/non-SSM organisation.
Electronic certificate or certificate: electronic file, issued by a certification authority, that binds a public key with a certificate subscriber's identity and is used for the following: to verify that a public key belongs to a certificate subscriber; to authenticate a certificate subscriber; to check a certificate's subscriber signature; to encrypt a message addressed to a certificate subscriber; or to verify a certificate subscriber's access rights to ESCB/SSM electronic applications, systems, platforms and services. Certificates are held on data carrier devices, and references to certificates include such devices.
Public key and private key: the asymmetric cryptography on which the PKI is based employs a key pair in which what is enciphered with one key of this pair can only be deciphered by the other, and vice versa. One of these keys is "public" and is included in the electronic certificate, whilst the other is "private" and is only known by the certificate subscriber and, when appropriate, by the Keys Archive (KA).
Session key: a key established to encipher communication between two entities. The key is established specifically for each communication, or session, and its utility expires upon termination of the session.
Key agreement: a process used by two or more technical components to agree on a session key in order to protect a communication.
Technical component (or simply, "component"): refers to any software or hardware device that may use electronic certificates, for its own use, for the purpose of its identification or for exchanging signed or enciphered data with relying parties.
Directory: a data repository that is accessed through the LDAP protocol.
User identifier: a set of characters that are used to uniquely identify the user of a system.
Public Key Infrastructure: the set of individuals, policies, procedures, and computer systems necessary to provide authentication, encryption, integrity and non-repudiation services, by way of public and private key cryptography and electronic certificates.
ESCB-PKI Certification Authority: means the entity, trusted by users, to issue, manage, revoke and renew certificates in accordance with the ESCB certificate acceptance framework, as amended from time to time, including in relation to the SSM.
Trust hierarchy: the set of certification authorities that maintain a relationship of trust by which a CA of a higher level guarantees the trustworthiness of one or several lower level CAs. In the case of ESCB-PKI, the hierarchy has two levels: the Root CA at the top level guarantees the trustworthiness of its subordinate CAs, one of which is the Online CA.

Certification Service Provider (CSP): entity or a legal person who issues certificates or provides other services related to electronic signatures.
Registration Authority: means an entity trusted by the users of the certification services which verifies the identity of individuals applying for a certificate before the issuance of the certificate by the ESCB-PKI Certification Authority.
Certificate applicants: the individuals who request the issuance of certificates for themselves or for a technical component.
Certificate subscribers: an individual who is the subject of an electronic certificate and has been issued an electronic certificate and/or a technical component manager who has accepted an electronic certificate issued for a technical component by the ESCB-PKI certification authority.
Relying parties: an individual or entity other than a certificate subscriber that decide to accept and rely on a certificate issued by ESCB-PKI.
Providing Central Bank or **service provider:** means the NCB appointed by the Governing Council to develop the ESCB-PKI and to issue, manage, revoke and renew electronic certificates on behalf and for the benefit of the Eurosystem central banks.
Repository: a part of the content of the ESCB-PKI website where relying parties, certificate subscribers and the general public can obtain copies of ESCB-PKI documents, including but not limited to this CPS and CRLs.

Secure e-mail gateway: computer system that improves the security of electronic mail systems by adding digital signature and encryption to the message content.

Shared mailbox: an electronic mailbox that can be accessed by multiple users. Technically it is equivalent to a personal mailbox but instead of identifying a specific individual it is linked to a business task (e.g. HR secretary)

Validation Authority: means an entity trusted by the users of the certification services which provides information about the revocation status of the certificates issued by the ESCB-PKI Certification Authority.

1.6.2 Acronyms

C: (Country). Distinguished Name (DN) attribute of an object within the X.500 directory structure
CA: Certification Authority
CAF: Certificate Acceptance Framework
CB: Central Bank that uses the ESCB-PKI
CDP: CRL Distribution Point
CEN: Comité Européen de Normalisation
CN: Common Name Distinguished Name (DN) attribute of an object within the X.500 directory structure
CP: Certificate Policy
CPS: Certification Practice Statement
CRL: Certificate Revocation List
CSP: Certification Service Provider
CSR: Certificate Signing Request: set of data that contains the public key and its electronic signature using the companion private key, sent to the CA for the issue of an electronic signature that contains said public key
CWA: CEN Workshop Agreement
DN: Distinguished Name: unique identification of an entry within the X.500 directory structure
ECB: European Central Bank

ESCB: European System of Central Banks
ESCB-PKI: European System of Central Banks Public Key Infrastructure: means the public key infrastructure developed by the providing central bank on behalf of and for the benefit of the Eurosystem Central Banks which issues, manages, revokes and renews certificates in accordance with the ESCB certificate acceptance framework – as amended from time to time including in relation to SSM -
ETSI: European Telecommunications Standard Institute
FIPS: Federal Information Processing Standard
HSM: Hardware Security Module: cryptographic security module used to store keys and carry out secure cryptographic operations
IAM: Identity and Access Management
IETF: Internet Engineering Task Force (internet standardisation organisation)
ITC: Information Technology Committee
LDAP: Lightweight Directory Access Protocol
NCA: National Competent Authority
NCB: National Central Bank
O: Organisation. Distinguished Name (DN) attribute of an object within the X.500 directory structure
OCSP: Online Certificate Status Protocol: this protocol enables online verification of the validity of an electronic certificate
OID: Object Identifier
OU: Organisational Unit. Distinguished Name (DN) attribute of an object within the X.500 directory structure
PAA: Policy Approval Authority
PIN: Personal Identification Number: password that protects access to a cryptographic card
PKCS: Public Key Cryptography Standards: internationally accepted PKI standards developed by RSA Laboratories
PKI: Public Key Infrastructure
PKIX: Work group within the IETF (Internet Engineering Task Group) set up for the purpose of developing PKI and internet specifications
PUK: PIN UnlocK Code: password used to unblock a cryptographic card that has been blocked after repeatedly and consecutively entering the wrong PIN
RA: Registration Authority
RO: Registration Officer
RO4EO: Registration Officer for External Organisations
RFC: Request For Comments (Standard issued by the IETF)
SMA: Shared Mailbox Administrator
SSCD: Secure Signature Creation Device
SSM: Single Supervisory Mechanism
T&C: Terms and conditions application form
UID: User identifier
VA: Validation Authority

2 Publication and Repository Responsibilities

2.1 Repositories

The ESCB-PKI repositories are listed below:

Root CA CRLs distribution point:

- ESCB-PKI Directory Service (LDAP):
  ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20Root %20CA,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList? base?objectclass=cRLDistributionPoint
- ESCB-PKI website (HTTP):
  http://pki.escb.eu/crls/rootCA.crl

Online CA CRLs distribution point:

- ESCB-PKI Directory Service (LDAP):
  ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20CA,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList? base?objectclass=cRLDistributionPoint
- ESCB-PKI website (HTTP):
  http://pki.escb.eu/crls/subCA.crl

Online validation service that implements the OCSP protocol:

- http://ocsp-pki.escb.eu

RootCA certificate distribution point:

- ESCB-PKI website (HTTP):
  http://pki.escb.eu/crls/rootCA.crt

Online CA certificate distribution point:

- ESCB-PKI website (HTTP):
  http://pki.escb.eu/crls/subCA.crt

For CPSs and CPs:

- ESCB-PKI website (HTTP): http://pki.escb.eu/policies

ESCB-PKI repository does not contain any information of a confidential nature.

2.2 Publication of Certification Data, CPS and CP

This CPS is public and is available on the ESCB-PKI website referred to in Section 2.1. *Repositories*, in PDF format.

The Certificate Policies are public and are available on the ESCB-PKI website referred to in Section 2.1. *Repositories*, in PDF format.

The ESCB-PKI Certificate Revocation Lists (CRLs) are public and are available, in CRL v2 format, on the repository and on the ESCB-PKI website referred to in Section 2.1 Repositories.

The Certificate Revocation Lists will be signed electronically by the ESCB-PKI CA that issued them.

The information about certificate status can be obtained by accessing the CRL directly or via the available online validation service that implements the OCSP protocol.

The electronic certificates issued by the ESCB-PKI CA are published in an internal LDAP directory located at the service provider's premises only available to ESCB/SSM systems on a need-to-know basis.

2.3 Publication Timescale or Frequency

The CPS and the CPs are published as they are created, as well as when any modification to them is approved. Modifications are made public on the website referred to in Section 2.1 *Repositories*.

The CA will add revoked certificates to the corresponding CRL during the period of time established under point 4.9.7 Issue Frequency of CRLs.

2.4 Repository Access Controls

Reading access to the CPS and CP is public. However, only Banco de España, as service provider of the ESCB-PKI is authorised to modify, substitute or eliminate information from its repository or website. For this purpose, Banco de España has established controls that prevent unauthorised individuals from manipulating the information contained in the repositories.

3 Identification and Authentication (I&A)

3.1 Naming

3.1.1 Types of names

All the electronic certificates issued by the ESCB-PKI Certification Authority must have a distinguished name pursuant to the X.500 standard.

The procedure for distinguished name assignment is determined in the policy drawn up for this purpose, developed and described in the CP corresponding to the certificate in question. This policy must be in line with the general guidelines described in this chapter of the CPS.

3.1.2 The need for names to be meaningful

In all cases, it is recommended that certificate subscribers' distinguished names be meaningful.

In any case, the procedure for making distinguished names meaningful is determined in the policy drawn up for this purpose, developed and described in the CP corresponding to the certificate in question.

3.1.3 Rules for interpreting various name formats

The rule applied by ESCB-PKI for the interpretation of the distinguished names for certificate subscribers it issues is the ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

3.1.4 Uniqueness of names

The whole made up of the combination of the distinguished name plus the KeyUsage extension content must be unique and unambiguous to ensure that certificates issued for two different certificate subscribers will have different distinguished names.

The procedures to guarantee uniqueness are established in the Certificate Policies.

3.1.5 Name dispute resolution procedures

Any dispute concerning ownership of names will be resolved as stipulated in point 9.13 *Claims and Jurisdiction* in this CPS.

3.1.6 Recognition, authentication, and the role of trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Means of proof of possession of the private key

Each CP will establish the procedure to be used as means of proof of possession of the private key.

3.2.2 Identity authentication for an entity

When applicable, each CP will establish the identity authentication procedure for entities.

3.2.3 Identity authentication for an individual

The CP applicable to each type of certificate will define the identification procedure for an individual.

Each CP establishes the data to be provided by the applicant, determining, among others, the following aspects:

- Types of identity documents valid for identification.
- RA procedures to identify the individual.
- Whether or not in-person identification is required.
- Means of proof of belonging to a specific organisation.

3.2.4 Non-verified applicant information

Each CP will establish which part of the information provided in the application for a certificate shall not necessarily be verified.

3.2.5 Validation of authority

For issuance of technical component certificates, verification of the authority of the person responsible for the application for those certificates will be established in the specific CP.

3.2.6 Criteria for operating with external CAs

Before establishing interoperation with external CAs, their suitability to meet certain requirements must be established. The minimum criterion to consider a CA suitable to interoperate with ESCB-PKI, which may be extended in each case by the ITC is to be compliant with the ESCB Certificate Acceptance Framework (CAF) – as amended from time to time including in relation to SSM -, thus accomplishing the main following requirements:

- The external CA must provide a security level in its certificates management, and throughout their entire life cycle, equal, at least, to that of ESCB-PKI security level. This requirement shall be included in the corresponding CPS and CP and in their fulfilment by the CA.
- It must comply with the ETSI TS 102 042: *Policy requirements for certification authorities issuing public key certificates* or equivalent.
- It must provide an audit report from an independent Authority of recognised prestige regarding its operations, as a means of verifying the existing security level. The ITC may waive this requirement for CAs belonging to Public Administrations.
- It must establish a collaboration agreement that sets out the commitments given as regards the security of the certificates included in the interoperation.

Even when the CA fulfils the aforementioned requirements, the ITC may refuse the application for interoperation without the need to give any justification.

Interoperation may be carried out by way of cross-certification, unilateral certification or by other means.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication requirements for routine re-key

The identification and individual authentication process is defined in the CP applicable to each type of certificate.

3.3.2 Identification and authentication requirements for re-key after certificate revocation

The identification and individual authentication processes are defined in the CP applicable to each type of certificate, and they must be at least as strict as those applied at the initial certificate application.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Each CP establishes who can apply for a certificate and the information to be supplied in the application. Furthermore, the CP establishes the steps required to carry out this process.

4.1.2 Enrolment process and applicants' responsibilities

The ESCB-PKI Registration Authority is responsible for establishing the suitability of the type of certificate to the characteristics of the applicants' duties, as established in the CP in each case. The Registration Authority may authorise or refuse the certificate application.

Certificate applications, once completed shall be submitted by the Registration Officer to the CA.

As a rule, all applicants who seek a certificate must:

- Complete the terms and conditions application form with all the information requested by ESCB-PKI to issue those certificates. It should be noted that not all the information requested will appear on the certificate, and that information will be kept confidential by the CA, pursuant to the applicable legislation on personal data protection.
- Deliver the certificate application, which includes the public key, to the corresponding RA, in the event that the key pair has been generated by the applicant and the certificate is generated directly based on that request. The procedure for delivery will be established in the corresponding CP.

The existence of the terms and conditions application form and, in general, of the enrolment procedure for ESCB-PKI certificates are defined in the CP corresponding to each certificate.

4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

The individual identification process is defined in the CP applicable to each type of certificate.

In order to guarantee that this identification is done with the same legal assurance in spite of the actual Registration Authority performing the identification of the user, the ESCB-PKI Certificate Policies shall define the documentation required to complete this process. Identification and authentication requirements shall include the following:

- The certificate applicant shall provide for verification a proof of identity: a valid passport, a national identity card, driving licence or any other document having a legal validity in the country
- The Registration Authority shall verify the authenticity and validity of the provided identity proof

4.2.2 Approval or rejection of certificate applications

Certificates will be issued once the Registration Authority has completed the verifications necessary to validate the certificate application.

The Registration Authority may refuse to issue a certificate to any applicant based exclusively on its own criteria and without leading to any liability whatsoever for any consequences that may arise from that refusal.

4.2.3 Time limit for processing the certificate applications

The Certification Authority shall not be held liable for any delays that may arise in the period between application for the certificate, publication in the ESCB-PKI repository (when appropriate), and its delivery. In any case, the minimum deadlines for processing certificate applications will be established in the corresponding CPs.

4.3 Certificate Issuance

4.3.1 Actions performed by the CA during the issuance of the certificate

Issuance of the certificate signifies final approval of the application by the CA.

When the CA issues a certificate pursuant to a certificate application, it will make the notifications established under point 4.3.2 of this chapter.

All certificates will become effective upon issue. The period of validity is subject to possible early, temporary or permanent termination in the event of circumstances that give cause to the suspension or revocation of the certificate.

All stipulations in this section are subject to the different Certificate Policies regarding the issue of certificates covered by those policies.

4.3.2 CA notification to the applicants of certificate issuance

Each CP will establish the manner in which applicants must be informed of the issuance of their certificates.

4.4 Certificate Acceptance

4.4.1 Form of certificate acceptance

Certificate acceptance signifies commencement of the certificate applicants' obligations in relation to ESCB-PKI.

Certificates that require identification in person shall carry certificate applicants' explicit acceptance and acknowledgement that they are in agreement with the terms and conditions contained in the terms and conditions acceptance form for the certification services provided by the ESCB-PKI, which govern the rights and obligations assumed between ESCB-PKI and certificate applicants. Likewise it shall also carry express declaration that the certificate applicants are aware of the existence of this CPS, which sets out the technology and operations of the electronic certificate services provided by ESCB-PKI. The certificates applicants shall sign the terms and conditions application form.

For online renewals, terms and conditions acceptance may be carried out by way of electronic signature.

The corresponding CP may detail or extend the manner in which certificates are accepted.

4.4.2 Publication of the certificate by the CA

Publication of certificates in the ESCB-PKI repository shall be established in each CP.

4.4.3 Notification of certificate issuance by the CA to other Authorities

When theCA issues a certificate pursuant to a certificate application processed through an RA, it shall send a copy of the same to the RA that forwarded the application.

4.5 Key Pair and Certificate Usage

4.5.1 Certificate subscribers' use of the private key and certificate

The responsibilities and constraints relating to the use of key pairs and certificates will be established in the corresponding CP.

Certificate subscribers may only use the private key and the certificate for the uses authorised in the CP and in accordance with the 'Key Usage' and 'Extended Key Usage' fields of the certificate. Likewise, certificate subscribers may only use the key pair and the certificate once they have accepted the terms and conditions of use established in the CPS and CP, and only for that which is stipulated therein.

Following certificate end-of-life or revocation, certificate subscribers must discontinue the use of the private key.

4.5.2 Relying parties' use of the public key and the certificate

Relying parties may only rely on the certificates as stipulated in the corresponding CP and in accordance with the 'Key Usage' field of the certificate.

Relying parties are obliged to check the status of a certificate using the mechanisms established in this CPS and the corresponding CP. Likewise, they accept the obligations regarding the conditions of use set forth in those documents.

4.6 Certificate Renewal

4.6.1 Circumstances for certificate renewal with no key changeover

All certificate renewals covered by this CPS shall be carried out with change of keys. Consequently, the remaining points in section 4.6 (4.6.2 to 4.6.7) established in RFC 3647 are not included and, therefore, for the purposes of this Statement, their content is "no stipulation".

4.7 Certificate Re-key

4.7.1 Circumstances for certificate renewal with key changeover

The certificate renewal procedure shall depend on the CP applicable to each type of certificate.

A certificate may be renewed for the following reasons, among others:

- End of the validity period
- Modification of the data contained in the certificate.
- When the keys are compromised or are no longer fully reliable.
- Change of format.

All certificate renewals covered by this CPS shall be carried out with change of keys.

4.7.2 Who may request certificate renewal?

Renewal must be requested by certificate subscribers, although not all certificates include this option. Each CP will establish who may request a certificate renewal.

4.7.3 Procedures for processing certificate renewal requests with key changeover

During the renewal process, the RA will check that the information used to verify the identity and attributes of the certificate subscriber is still valid. If any of the certificate subscriber's data have changed, they must be verified and registered with the agreement of the certificate subscriber.

In any case, certificate renewal is subject to:

- The request being made in due time and manner, following the instructions and regulations established by ESCB-PKI specifically for this purpose.
- The RA or CA not having certain knowledge of the existence of any cause for the revocation / suspension of the certificate.
- The request for the renewal of the provision of services being for the same type of certificate as the one initially issued.

4.7.4 Notification of the new certificate issuance to the certificate subscriber

Each CP shall establish the manner in which applicants will be informed that the corresponding certificate has been issued in their name.

4.7.5 Manner of acceptance of certificates with changed keys

Each CP shall establish the manner of acceptance.

4.7.6 Publication of certificates with the new keys by the CA

Each CP shall establish, as appropriate, the procedure for publishing the certificates in the ESCB-PKI repository.

4.7.7 Notification of certificate issuance by the CA to other Authorities

When an ESCB-PKI CA issues a certificate pursuant to a certificate application processed through an RA, it shall send a copy of the same to the RA that forwarded the application.

4.8 Certificate Modification

4.8.1 Circumstances for certificate modification

Certificate modification takes place when a new certificate is issued due to changes in the certificate information, not related to its public key or end-of-life of the certificate.

Certificate modification may be due to causes such as:

- Change of name.
- Change of duties within the organisation.
- Reorganisation resulting in a change in the DN.

All certificate modifications carried out within the scope of this CPS will be treated as certificate renewals and, therefore, the previous points in this respect shall be applicable.

Consequently, the remaining points in section 4.8 (4.8.2 to 4.8.7) established in RFC 3647 are not included, meaning that, for the purpose of this Statement, they are not regulated.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

Certificate revocation is the action that renders a certificate invalid prior to its expiry date. Certificate revocation produces the discontinuance of the certificate's validity, rendering it permanently inoperative as regards its inherent uses and, therefore, discontinuance of the provision of certification services. Revocation of a certificate prevents its legitimate use by the certificate subscriber.

The revocation request process is defined in the CP applicable to each type of certificate.

Revocation of a certificate entails its publication on the public-access Certificate Revocation Lists (CRL). Once the period of validity of a revoked certificate has expired, it is removed from the CRL.

Causes for revocation:

Notwithstanding the applicable legislation, a certificate may be revoked in the following cases:

- Loss, disclosure, modification or any other circumstance that compromises the certificate subscriber's private key or when suspicion of such compromise exists.
- Deliberate misuse of keys and certificates, or failure to observe or infringement of the operational requirements contained on the Acceptance Form for the terms and conditions of the certification services provided by the ESCB-PKI CA, in the associated CP or in this CPS.
- The certificate subscriber ceases to belong to the group, when that membership granted the certificate subscriber the right to hold the certificate.
- ESCB-PKI ceases its activity.
- Defective issue of a certificate due to:
    1. Failure to comply with the material requirements for certificate issuance.
    2. Reasonable belief that basic information related to the certificate is or could be false.
    3. The existence of a data entry error or any other processing error.
- The key pair generated by the certificate subscriber has been found to be "weak".
- The information contained in a certificate or used for the application becomes inaccurate.
- By order of the certificate subscriber or an authorised third party.
- The certificate of a higher RA or CA in the certificate trust hierarchy is revoked.
- The existence of any other cause specified in this CPS or in the corresponding Certificate Policies established for each type of certificate.

The main effect of revocation as regards the certificate is the immediate and early termination of its term of validity, with which the certificate becomes invalid. Revocation shall not affect the underlying obligations created or notified by this CPS, nor shall its effects be retroactive.

4.9.2 Who can request revocation?

The CA or any of the RAs may, at their own initiative, request the revocation of a certificate if they become aware or suspect that the certificate subscriber's private key has been compromised, or in the event of any other determining factor that recommends taking such action.

Additionally, certificate subscribers or, in the case of component certificates, component managers may also request revocation of their certificates, which must be carried out in accordance with the conditions specified in point 4.9.3.

The identification policy for revocation requests may be the same as that of the initial registration. The authentication policy shall accept revocation requests signed electronically by

the certificate subscriber, as long as it is done using a valid certificate other than the one for which the revocation is requested.
The different Certificate Policies may establish other identification procedures of a stricter nature.

4.9.3 Procedures for requesting certificate revocation

The revocation request procedure for each type of certificate shall be established in the corresponding CP.
In general, notwithstanding the CP:

- Certificate subscribers shall be notified of the revocation of their certificates by e-mail. Following certificate revocation, certificate subscribers must discontinue use of the private key pertaining to that certificate.
- In the case of certificates belonging to individuals, revocation of an authentication certificate revokes the rest of the certificates linked to the certificate subscriber.
- Certificate revocation requests received after the date of expiry will be not be processed.

The information required to request certificate revocation shall be established at the expense of that specified in the corresponding CP.

4.9.4 Revocation request grace period

Revocation shall be carried out immediately following the processing of each request that is verified as valid. Therefore, the process will not include a grace period during which the revocation request may be cancelled.

4.9.5 Time limit for the CA to process the revocation request

Each CP shall establish the maximum time allowed for processing revocation requests. Notwithstanding the aforementioned, it is hereby established that, as a general rule, that time shall will be less than 1 hour.

4.9.6 Requirements for revocation verification by relying parties

Verification of revocations, whether by directly consulting the CRL or using the OCSP protocol, is mandatory for each use of the certificates by relying parties.
Relying parties must check the validity of the CRL prior to each use and download the new CRL from the ESCB-PKI repository when the one they hold expires. Certificate Revocation Lists stored in cache[1] memory, even when not expired, do not guarantee availability of updated revocation data.
Optionally, unless the applicable CP establishes otherwise, the VA may be used for revocation verification.
When the CP accepts other forms of revocation data publication, the requirements for checking data will be specified in the CP itself.

[1]Cache memory: memory that stores the necessary data for the system to operate faster, as it does not have to obtain this data from the source for every operation. Use of cache memory could entail the risk of operating with outdated data.

4.9.7 CRL issuance frequency

ESCB-PKI shall publish a new CRL in its repository whenever a revocation occurs. In any case, ESCB-PKI shall publish a new CRL in its repository at least every 24 hours for Subordinated CAs and at least every 6 months for the Root CA, even when the CRL has not been modified; that is, even when no certificate has been revoked since the previous publication.
The CRL lifetime will ≤72 hours for the Subordinate CAs and ≤6 months for the Root CA.

4.9.8 Maximum latency between the generation of CRLs and their publication

Each CP will establish the maximum time allowed between generation of the CRLs and their publication in the repository.

4.9.9 Online certificate revocation status checking availability

ESCB-PKI provides a repository on which it publishes the CRLs for verification of the status of the certificates it issues. Additionally, there is a VA that, via OCSP protocol, enables certificate status verification.
The web addresses for access to the CRLs and the VA are set out in point 2.1 *Repositories*.

4.9.10 Online revocation checking requirements

When using the VA, relying parties must have software capable of operating with the OCSP protocol to obtain the certificate information.

4.9.11 Other forms of revocation alerts available

Some CPs may accept other forms of revocation alerts.

4.9.12 Special requirements for the revocation of compromised keys

There are no variations to the aforementioned clauses for revocation due to private key compromise.

4.9.13 Causes for suspension

Suspension of certificate validity shall be applied (when said operation is included in the corresponding CP), in the following cases, among others:

- Temporary change of any of the certificate subscribers' circumstances that make it advisable to suspend the certificates for the duration of said change. Upon return to the initial situation, the certificate suspension will be lifted. The characteristics of and requirements for the suspension will be established in the corresponding CP.
- Notification by certificate subscribers of the possible compromise of their keys. In the event that the suspicion, due to the level of certainty, does not warrant immediate revocation, the certificates of the certificate subscriber in question will be suspended until the possible compromise of the keys has been established. Once the study has been completed, a determination will be made as to whether the certificates are to be revoked or the suspension lifted.
- Legal or administrative decisions that so order.

4.9.14 Who can request the suspension?

Requests may be submitted by the certificate subscriber or the person established by the corresponding CP.

4.9.15 Procedure for requesting certificate suspension

Each CP may establish the procedure for requesting certificate suspension.

4.9.16 Suspension period limits

Each CP may establish suspension period limits.

Expiry or request for revocation of a certificate during the period of suspension shall have the same effect as in the case of expiry or request for revocation of non-suspended certificates.

4.10 Certificate Status Services

4.10.1 Operational characteristics

ESCB-PKI has at least two services that provide information on the status of certificates issued by its CA:

- Publication of Certificate Revocation Lists (CRL). Access to CRLs can be obtained via the ESCB-PKI Directory Service (LDAP) or the ESCB-PKI Website (HTTP).
- Online validation service that implements the RFC 2560 Online Certificate Status Protocol. Using this protocol, the current status of an electronic certificate can be determined without using the CRLs. An OCSP client sends a certificate status request to the VA, which in turn, after consulting the CRLs it has available, sends a reply regarding the certificate status via HTTP.

4.10.2 Service availability

The service, in its two varieties, is available permanently, every day of the year, for both ESCB-PKI internal relying parties and external relying parties.

4.10.3 Additional features

To use the online validation service, relying parties must have an RFC 2560 compliant OCSP client.

4.11 End of Subscription

Certificate subscription may be ended due to the following causes:

- Certificate revocation due to any of the causes established in point 4.9.1.
- End of the certificate validity period.

If certificate renewal is not requested, the end of the subscription will terminate the relationship between the certificate subscriber and the CA.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery practices and policies

The policies and practices for key registration and recovery shall be identified in each CP that establishes private key escrow.

No private key for any certificate in which the non-repudiation electronic signature functionality has been authorised shall be escrowed. This can be verified by checking whether or not the 'Key Usage' code is “1” in the 'nonRepudiation' field.

4.12.2 Session key protection and recovery policies and practices

When appropriate, the corresponding CP will identify the policies and practices for the protection and recovery of session keys.

5 Facility Management, and Operational Controls

5.1 Physical SecurityControls

The aspects related to security controls are set out in detail in the documentation drawn up for this purpose by the ESCB-PKI Service Provider (Banco de España). This chapter establishes the most significant measures taken.

5.1.1 Site location and construction

The building in which the ESCB-PKI infrastructure is located has access control security measures that permit only duly authorised personnel to access the building.

All ESCB-PKI critical operations are carried out in physically secure facilities, with specific levels of security for the most critical elements.

The Service Provider (Banco de España) facilities meet the following physical requirements:

a They are distant from smoke ventilation points to avoid possible damage from fires on other floors.

b Absence of windows to the outside of the building.

c Surveillance cameras in restricted access areas.

d Access control based on card and PIN code.

e Fire protection and prevention systems: detectors, extinguishers, personnel training on what steps to take in the event of fire, etc.

f Transparent partitions that delimit the different zones and enable observation of the rooms from the access passageways, in order to detect intrusions or illicit activity inside.

g Cabling, both for data transmission and telephony, protected against damage and interception.

5.1.2 Physical access

There is a complete system to control physical access by individuals at the entry and exit, comprising various levels of security. All sensitive operations are carried out within a physically secure facility with different levels of security required to access critical machinery and applications.

Loading and unloading areas are isolated and under permanent surveillance, by human and technical means.

5.1.3 Power and air-conditioning

The rooms in which ESCB-PKI infrastructure equipment is located have suitable power supply and air-conditioning for the requirements of the equipment installed in them. The infrastructure is protected against power failures or any other electricity supply anomaly. Systems that so require have permanent power supply units as well as a generator.

5.1.4 Water exposure

Appropriate measures have been taken to prevent exposure of the equipment and cables to water.

5.1.5 Fire prevention and protection

The rooms have the suitable means (detectors) to protect their content against fire.

Cabling is installed under a false floor or above a false ceiling and the appropriate means (detectors in the floor and ceilings) have been installed to protect them against fire.

5.1.6 Storage system

ESCB-PKI has established all the necessary procedures to make backup copies of all its productive infrastructure data.
ESCB-PKI has organised backup copy plans for all the sensitive data and those considered necessary for activity continuity.

5.1.7 Waste disposal

Waste management measures has been adopted that guarantee destruction of any material that could contain information, as well as management measures for removable media.

5.1.8 Offsite backup

ESCB-PKI has backup copies in two of its own premises, which have the necessary security measures in place and are suitably physically separated.

5.2 Procedural Controls

Banco de España, as service provider of the ESCB-PKI, endeavours to ensure that all management, related to both operational and administrative procedures, is carried out in a secure manner, pursuant to the guidelines in this document, carrying out periodic audits. (See Chapter 8 *Performing audits and other conformity controls*).
Additionally, duties have been divided to prevent a single person from obtaining control of the entire infrastructure.

5.2.1 Roles responsible for PKI control and management

The PKI system is the core infrastructure required to provide public key services such as key pair generation, public key certificate issuance and life cycle management, CRL generation, issuance of OCSP tokens, etc.
The list of the subsystems that are part of the PKI System is the following:

- CA: in charge of issuing public key certificates and revocation lists, and generating key pairs associated with specific certificates (e.g. those that require key recovery);
- Registration Authority: in charge of managing certificates for the whole population of users and obtaining the required information to be included in the certificates;
- VA: in charge of providing online information about revocation status by implementing the Online Certificate Status Protocol (OCSP);
- Key Archive: in charge of storing a copy of specific key pairs that need to be recovered in case of loss.

The following responsibilities are established for control and management of the system:

HSM Administration and Operation.Different functions are established for Hardware Security Module (HSM) administration and operation at Banco de España premises:

- *HSM Administrators*: Four eyes principle has been established on HSM administration. The HSM Administrators are responsible for carrying out the following operations:

1 Recovery of cryptographic hardware functionality in the event of HSM failure.

2 Key recovery in the event of accidental deleting.

3 Replacement of a set of administrator cards. This operation only needs to be carried out when increasing or reducing the number of administrator cards.

4 Replacement of a set of operator cards. This operation only needs to be carried out when increasing or reducing the number of operator cards or to replace the existing one due to deterioration

5 Increase in the number of HSM integrated in the infrastructure.

6 Given that operation is carried out in FIPS140-2 Level 3 mode, authorisation for the generation of operator and keys sets. This operation is only required during the CA's key generation protocol.

- *HSM Operators*: Four eyes principle has been established on HSM operation. The HSM Operators are responsible for carrying out the following operations:

1 Key activation for their use. This means that each initiation of a CA requires the insertion of the operator cards linked to the keys.

2 Authorisation for application key generation, although this authorisation may also be carried out by an Administrator. This operation is only required during the CA's key generation protocol.

3 Starting the CA configuration interface and those of the other entities that make up the PKI. Through this interface, the operator can modify the certificate templates and define the CA's remote administrators.

Operations carried out by operators are more frequent than those carried out by Administrators, as they must intervene whenever the CA needs to be reconfigured or when one of the processes involved in ESCB-PKI needs to be rebooted.

System Administrator: System Administrators, belonging to Banco de España, are authorised to install, configure and maintain the PKI system, but have no access to security-related information.

Security Officer: PKI Security Officers, belonging to Banco de España, have overall responsibility for administering the implementation of the security policies and practices. For-eyes principle is required to change relevant policies of the PKI (e.g. modify or add certificate profiles).

System Auditor: System Auditors, belonging to Banco de España, are authorised to view the PKI system archives and audit logs.

Registration Officers: ESCB-PKI Registration Officers are responsible for the approval of certificate generation, revocation and suspension, using the Registration Authority services for this purpose. There are two types of ESCB-PKI registration officers:

- PKI System Registration Officers. They belong to Banco de España asService Provider and are in charge of managing certificates for the PKI subsystems (CA, RA, VA and KA);
- Registration Officers are nominated by the Central Banks and are in charge of managing end user certificates.

Trusted Agents: delegated at the Central Banks, National Competent Authorities or non-ESCB/non-SSM organisations. They act as a representative of a Registration Authority only for user identification.

System Operators: System Operators, belonging to Banco de España, are responsible for operating the PKI system on a day-to-day basis. They are authorised to perform system backup and recovery procedures.

5.2.2 Number of individuals required to perform each task

A minimum of 2 people with sufficient professional capacity are required to perform the tasks of HSM Administration and Operation set out under point 5.2.1 *Roles responsible for PKI control and management*.

5.2.3 Identification and authentication of each user

The HSM Administrators and Operators are identified and authenticated in the HSMs by way of shared secrecy techniques in specific HSM cryptographic cards.
The rest of the ESCB-PKI authorised users are identified by way of electronic certificates issued by the PKI and authenticated by way of cryptographic tokens.

5.2.4 Roles that require separation of duties

Banco de España personnel assignment shall be done according to the following incompatibility matrix:

	PKIsecurity Officers	**PKIsystem Registration Officers**	**System Admin.**	**SystemOperators**	**System Auditors**
PKI security Officers			✘		✘
PKI system Registration Officers					✘
System Admin.	✘				✘
System Operators					✘
SystemAuditors	✘	✘	✘	✘	

✘ = roles that cannot be held by the same person

5.3 Personnel Controls

5.3.1 Requirements concerning professional qualification, knowledge and experience

All personnel working in the ESCB-PKI environment must have sufficient knowledge, experience and training for optimum performance of their assigned duties.
Therefore, Banco de España as the service provider carries out the personnel selection processes it considers necessary to ensure that the professional profiles of personnel are the most suitable to the features inherent to the tasks to be carried out.

5.3.2 Background checks and clearance procedures

In accordance with personnel selection procedures established by the Service Provider (Banco de España) background checks and clearance procedures are performed.

5.3.3 Training requirements

In accordance with the procedures established by the Service Provider (Banco de España) training requirements are checked.

Specifically, personnel related to PKI operations will receive the necessary training to ensure the correct performance of their duties. The following aspects are included in the training:

- Delivery of a copy of the Certification Practices Statement.
- Awareness programmes for physical, logical, and technical security.
- Operation of the software and hardware corresponding to each specific role.
- Security procedures corresponding to each specific role.
- Operational and administrative procedures for each specific role.
- Procedures for PKI operations recovery in the event of catastrophe.

5.3.4 Retraining requirements and frequency

Banco de España´s procedures on retraining requirements and frequency procedures shall be apply

5.3.5 Frequency and sequence for job rotation

No stipulation.

5.3.6 Sanctions for unauthorised actions

Unauthorised action shall be classified as a work offence, sanctioned pursuant to Banco de España's Labour Regulations and in the Spanish Workers' Statute, without prejudice to the liabilities of any other kind that may be incurred.

5.3.7 Requirements for third party contracting

Banco de España's general regulations shall be applied to contracting.

5.3.8 Documentation supplied to personnel

Access will be given to the mandatory security regulations together with this CPS and those contained in the Certificate Policies.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

The operations are divided into events, so data on one or more events are logged for each relevant operation. The events recorded include, at least, the following data:

Category: Indicates the importance of the event.

- Information: the events in this category contain data on operations carried out successfully.
- Mark: every time an administration session is initiated or terminated, an event of this category is recorded.

- Alert: indicates that an unusual occurrence was detected during the operation, but it did not cause an operation failure (for example a refused batch request).
- Error: indicates an operation failure due to a predictable error (for example, a batch that was not processed because the RA requested a certificate template for which it was not authorised).
- Fatal Error: indicates that there was an exceptional occurrence during an operation (for example, failure to access a database table).

Date: Date and time of the event.
Author: Distinguished Name of the Authority that generated the event.
Role: Type of Authority that generated the event.
Event Type: Identifies the type of event, differentiating between, among others, cryptographic, user interface or library events.
Event ID: Number that uniquely identifies an event among a group of events of the same type, generated by the same module.
Module: Identifies the module that generated the event.
Level: Number that indicates the level at which the event is located. The events produced by some operations are organised hierarchically, so an event may group other events from a lower level, depending on the complexity of the operation. For level-one events, this field will indicate a value of 1. For second and successive level events, it will indicate the corresponding value. Events to which this characteristic is not applicable will be assigned a value of 0.
Remarks: Textual representation of the event. For some events the description is followed by a list of parameters, the values of which will vary depending on the data on which the operation was carried out.

Some examples of parameters that are included for the description of the "Generated Certificate" event are: the serial number, the distinguished name of the certificate subscriber issued and the certificate template applied.
The events registered in the database may be subject to certificate types, specified in the CP.

5.4.2 Frequency with which audit logs are processed

Logs are analysed manually when necessary. No frequency for this process has been established.

5.4.3 Period for which audit logs are kept

The information generated in the audit logs is kept online until it is archived. Once archived, audit logs are kept for at least 5 years.

5.4.4 Audit log protection

Events logged by the ESCB-PKI are protected by encipherment in such a way that they can only be accessed by the event viewing applications and with the appropriate access controls.

5.4.5 Audit log back up procedures

Backup copies of audit logs are made in accordance with the standard measures established by ESCB-PKI for Central Computer Database backup copies.

5.4.6 Audit data collection system

The ESCB-PKI's system for compiling audit data is a combination of automatic and manual processes carried out by the ESCB-PKI technical components. All the CA and RA logs are stored in ESCB-PKI internal systems managed by the service provider.

The most significant audit logs in ESCB-PKI are accumulated in a database associated to the CA. The security control procedures employed by ESCB-PKI are based on the construction technology used in the database.

The system's features are as follows:

- It enables verification of database integrity; that is, it detects any possible fraudulent manipulation of the data.
- It ensures non-repudiation by the authors of operations carried out on the data. This is achieved using electronic signatures.
- It keeps a historical log of data updating; that is, it stores successive versions of each log resulting from the different operations carried out. This makes it possible to log the operations carried out and prevent loss of electronic signatures carried out previously by other users when the data is updated.

5.4.7 Notification to the subject who caused the event

No automatic notification of audit log file actions to the subject who caused the event has been established.

5.4.8 Vulnerability assessment

Vulnerability assessment performed shall be pursuant to ESCB Vulnerability and Patch management policy – as amended from time to time including in relation to SSM -.

5.5 Records Archival

5.5.1 Types of records archived

The CAstores, for the established periods, all the information related to the operations carried out with certificates and keeps an events log.

Logged operations include those carried out by the administrators who use the ESCB-PKI element administration applications, as well as all the data related to the registration process.

The types of data or files archived include, among others:

- Data related to certificate application and registration processes.
- Those specified under point 5.4.1.
- Keys historical archive.

5.5.2 Archive retention period

All the electronic information related to certificates is held by Banco de Espana and the terms and conditions application form is held by the CBs and NCAs as Registration Authorities. The retention period is defined in each CP.

For audit logs, point 5.4.3 shall apply, always taking into account any specific particularity of the CP for the certificate corresponding to the data involved.

5.5.3 Archive protection

Log archives are protected by encipherment in such a way that they can only be accessed by the event viewing applications and with the appropriate access controls.

5.5.4 Archive backup procedures

Backup copies of log archives are made in accordance with the standard measures established by ESCB-PKI for Central Computer Database backup copies.

5.5.5 Requirements for time-stamping records

The information systems employed by ESCB-PKI guarantee logging of the time at which the log entries were made. The moment in time in the systems comes from a secure source that establishes the date and time. Specifically, the clock signal comes from:

- The atomic clock in Braunschweig, Germany (PhysikalischTechnischeBundesanstalt), which represents the official time within Eurosystem.

5.5.6 Audit data archive system (internal vs. external)

Data collection is internal to the Authority and corresponds to ESCB-PKI.

5.5.7 Procedures to obtain and verify archived information

Events logged by the ESCB-PKI are protected by encipherment in such a way that they can only be accessed by the event viewing and management applications.

This verification must be carried out by the Audit Administrator, who must have access to the verification and integrity control tools for the ESCB-PKI events log.

5.6 Key Changeover

The procedures to provide certificate subscribers and relying parties of the certificates of the former with a new CA public key, in the event of key changeover, are the same as those used to provide the current public key. Consequently, the new key will be published in the ESCB-PKI repository (see point 2.1).

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

ESCB-PKI has established a Contingency Plan that sets out the actions to be taken, resources to be used and personnel to be employed in the case of a deliberate or accidental event that renders useless or deteriorates the resources or certification services provided by ESCB-PKI.

The Contingency Plan deals with the following aspects, among others:

- Redundancy of the most critical components.
- Start-up of an alternative backup centre.
- Complete and periodic checks of the backup copy service.

In the event of any compromise of the signature verification data of the CA, ESCB-PKI shall inform all certificate subscribers and relying parties known that all the certificates and revocation lists of certificates signed with that data are no longer valid. Service will be re-established as soon as possible.

5.7.2 Corruption of computing resources, software, and/or data

If computing resources, software, and/or data are corrupted or suspected to be corrupted, ESCB-PKI operations will be halted until the environment's security has been re-established, with the incorporation of new components, the suitability of which can be accredited. At the same time, an audit will be carried out to identify the cause of the corruption and ensure it does not reoccur.
In the event that issued certificates are affected, the users of the same will be notified and new certificates issued.

5.7.3 Action procedures in the event of compromise of an Authority's private key

If an Authority's private key is compromised, it will be revoked immediately. The corresponding CRL will then be generated and published and the Authority's activity ceased, carrying out the generation, certification and start-up of a new Authority with the same name as the eliminated one and with a new key pair.
In the event that the Authority affected is the CA, its revoked certificate shall remain accessible in the ESCB-PKI repository in order to continue verifying the certificates issued whilst it was operational.
The Authorities that make up ESCB-PKI that are dependent on the CA will be informed of the situation and urged to request new certification by the CA with its new key.
All the affected Authorities will be notified that the certificates and revocation data, supplied with CA's compromised key, cease to be valid from the moment of notification, so they must use the CA's new public key to verify data validity.
Certificates signed by the Authorities dependent on the CA during the period between key compromise and the corresponding certificate revocation will likewise be revoked, notifying their certificate subscribers of this circumstance and issuing new certificates.

5.7.4 Installation following a natural disaster or another type of catastrophe

The ESCB-PKI system can be reconstructed in the event of disaster. Carrying out this reconstruction requires:

- A system with hardware, software and a Security Cryptographic Hardware device similar to that which existed prior to the disaster.
- Administrator cards for all the ESCB-PKI.
- A backup copy of the system disks prior to the disaster.

With these elements it is possible to reconstruct the system as it was at the time the backup copy was made and, therefore, recover the CA, including its private keys.
Storage, both of the CA Administrator access cards and of the copies of the CA's system disks is carried out in a different place, sufficiently distant and protected in order to avoid, as far as possible, concurrence of simultaneous disasters in the production and recovery element systems.

5.8 CA or RA Termination

5.8.1 Certification Authority

In the event of termination of activities of the CA, Banco de España as the service provider will ensure that the potential problems for its certificate subscribers and relying parties are kept to a minimum, as well as ensuring maintenance of the records required to provide certified proof of the certificates for legal purposes.

In the event of termination of the activities of the CA, Banco de España as the service provider will notify the certificate subscribers and relying parties, by any means that guarantee sending and receipt of said notifications and with a minimum notice of 2 months prior to the termination of activities, that it intends to have the corresponding CA discontinue its activities as certification services provider.

In the event the ESCB-PKI's owners decide to transfer the activity to another Certification Services Provider, it shall notify their certificate subscribers regarding the transfer agreements. For this purpose, ESCB-PKI's owners shall send a document explaining the transfer terms and conditions and the characteristics of the Provider to which it proposes to transfer certificate management. This notification shall be carried out by any means that guarantees sending and receipt of the notification, at least two months prior to the effective termination of its activities.

The ESCB-PKI infrastructure is located in Spain therefore, in accordance with the Spanish legislation, Banco de España as the service provider shall notify the Spanish Ministry of Industry, Trade and Tourism, with the advance notice indicated in the previous paragraph, of the termination of its activities and the destination of the certificates, specifying whether their management is to be transferred and to whom, or whether their validity is to be terminated.

Likewise, it shall report any other relevant circumstance that could prevent activity continuity.

Banco de España as the service provider shall send the Spanish Ministry of Industry, Trade and Tourism, prior to final termination of its activity, the data related to the certificates for which validity has been terminated, so that it can take custody of them for the purposes established under Section 20.1.f of the Spanish Electronic Signature Act.

The certificates will be revoked once the two months period has elapsed without any transfer agreement having been drawn up.

5.8.2 Registration Authority

If any of the Central Banks acting as Registration Authority ceases to carry out its duties, it shall transfer the records it holds to Banco de España, as the Certification Authority, or any other Registration Authority, when the obligation subsists to maintain the information on file; otherwise, the information shall be destroyed.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Key pairs for internal ESCB-PKI components, specifically RootCA and OnlineCA, are generated in cryptographic hardware modules with FIPS 140-2 Level 3 certification, installed in their respective systems. The hardware and software systems used are compliant with the CWA 14167-1 and CWA 14167-2 standards.

The key pairs for the rest of the certificate subscribers are generated as stipulated in the applicable CP for each certificate.

The hardware and software devices to be used in the generation of keys for each type of certificate issued by ESCB-PKI are determined by the applicable CP.

6.1.2 Delivery of private keys to certificate subscribers

The method used to deliver private keys to their certificate subscribers depends on each certificate and is established in the CP corresponding to each certificate.

6.1.3 Delivery of the public key to the certificate issuer

The method used to deliver the public key to the issuer when it is generated by the certificate subscriber will depend on each certificate and will be established in the CP corresponding to each certificate.

6.1.4 Delivery of the CA's public key to relying parties

The public key of the Root CA and the Online CA are made available to relying parties in the ESCB-PKI repository (see point 2.1), notwithstanding the possibility of the CP establishing additional mechanisms for the delivery of these keys.

6.1.5 Key sizes

The Root CA key size is 4096 bits. The Online CA key size is 4096 bits.

The size of the keys for each type of certificate issued by ESCB-PKI is defined in the applicable CP.

6.1.6 Public key generation parameters and quality checks

RootCA and OnlineCA keys are encoded pursuant to RFC 3280 and PKCS#1. The key generation algorithm is the RSA.

The key generation parameters for each type of certificate issued by ESCB-PKI are determined in the applicable CP.

The procedures and means of checking the quality of the key generation parameters for each type of certificate issued by ESCB-PKI are determined in the applicable CP.

6.1.7 Accepted key usage (KeyUsage field in X.509 v3)

The accepted key usage for each type of certificate issued by ESCB-PKI is defined in the applicable CP.

All certificates issued by ESCB-PKI contain the *Key Usage* extension defined under the X.509 v3 standard, which is classified as critical. Additional constraints may be established through the *Extended Key Usage* extension.
It should be noted that the efficiency of constraints based on certificate extensions can sometimes depend on the operational characteristics of computer applications that have not been designed by ESCB-PKI.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

The modules used to create keys used by RootCA and OnlineCA comply with FIPS 140-2 Level 3 certification.
Start-up of each one of the Certification Authorities, taking into account that a Hardware Security cryptographic Module (HSM) is used, involves the following tasks:

a HSM module status boot up.
b Creation of administration and operator cards.
c Generation of the CA keys.

ESCB-PKI uses hardware and software cryptographic modules available commercially, developed by third parties. ESCB-PKI only uses cryptographic modules with FIPS 140-2 Level 3 certification that comply with the following standards:

- FCC: CRFA47, Section 15, Subsection B, Class A
- EC: EN 55022 Class A, EN 55024-1, EN 60950

As regards the cryptographic cards, they comply with the CC EAL4+ security level, although the equivalent ITSEC E3 or FIPS 140-2 Level 2 certifications are also acceptable.

6.2.2 Private key multi-person (k out of n) control

Both the Root CA and OnlineCA private keys are under multi-person control[1]. This is realised by means of booting the CA software requiring a minimum amount of operators from the CA. This is the only method available to activate said private key.
A certain number 'K' of HSM operators (where K≥2), out of a total of 'N', are necessary to activate and use the ESCB-PKI Root CA and Online CA private keys.

6.2.3 Escrow of private keys

Escrow of the private keys for the certificates is carried out by their certificate subscribers. The ESCB-PKI encipherment private keys are only escrowed by archiving them.
The private keys of the CA are housed in cryptographic hardware devices with FIPS-2 Level 3 certification linked to each of the CAs.

6.2.4 Private key backup copy

The private keys of the CA are archived under the protection of the HSMs belonging to each of them and to which only the administrators and operators of the CA have access.

[1] Multi-person control: control by more than one person, normally a subgroup 'k' of a total of 'n' people. This guarantees that no one has individual control of the critical activities and, at the same time, it facilitates availability of the necessary people.

6.2.5 Private key archive

Private keys for signature certificates of individuals are never archived in order to guarantee non-repudiation.

Encipherment certificates private keys are archived and their recovery procedures are established in their CP.

6.2.6 Private key transfer into or from a cryptographic module

Private keys can only be transferred between cryptographic modules (HSM) and require the intervention of a certain number 'K' of HSM administrators (where K≥2), out of a total of 'N'.

6.2.7 Private key storage in a cryptographic module

Private keys are generated in the cryptographic module when each ESCB-PKI Authority that makes use of that module is created, and they are stored enciphered.

6.2.8 Private key activation method

As stipulated under point 6.2.2 above (*Private key multi-person control*) the private keys of both the Root CA and the Online CA are activated by booting the CA software using a certain number 'K' of HSM operators (where K≥2) of the corresponding CA, out of a total of 'N'. This is the only method to activate that private key.

Activation of the keys of the rest of the certificate subscribers is determined in the applicable Certificate Policies.

6.2.9 Private key deactivation method

The System Administrator, with authorisation from two HSM Administrators, can deactivate ESCB-PKI CA's keys by halting the computer application of the corresponding CA.

6.2.10 Private key destruction method

No stipulation.

6.2.11 Cryptographic module classification

The cryptographic modules used comply with the FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archive

ESCB-PKI maintains an archive of all the certificates issued, which include the public keys, for a period of fifteen (15) years. The administrator of the CA is responsible for controlling this register.

The archive has the appropriate means to protect the information it contains against tampering.

6.3.2 Operational period of certificates and usage periods for key pairs

The ESCB-PKI RootCA certificate and key pair are valid for thirty (30) years and those of the ESCB-PKI Online CA for fifteen (15) years.

The active lifetime for the rest of the certificates is established in the CP applicable to each one.

6.4 Activation Data

6.4.1 Generation and installation of activation data

To establish a CA, cryptographic cards must be created to be used for recovery and operational activities. The CA has two operational roles, each of which requires their corresponding cryptographic cards:

- The set of *administrator cards*. These cards will be required to recover the HSM status in the event of a disaster or to transfer the keys to another module.
- The set of *operator cards*. These cards are used to protect the CAs keys. There must be a minimum number of operators present and they must indicate the PINs for their respective cards to carry out any operation with the CA, regardless of whether or not it involves the use of the CA keys.

If one or more cards are lost or damaged, or the administrator forgets the PIN or ceases to use it for any reason, the whole set of cards must be regenerated as soon as possible, using all of the security cards.

6.4.2 Activation data protection

Only authorised personnel, in this case the PKI Operators corresponding to the CA, hold cryptographic cards capable of CA activation and know the PINs and passwords to access the activation data.

6.4.3 Other activation data aspects

No stipulation.

6.5 Computer Security Controls

The information under this section is confidential. Access to this information is limited to those who can prove a need to know, such as in the case of external or internal inspection audits.
The system will comply with the relevant ESCB/SSM policies.

6.5.1 Specific security technical requirements

The information under this section is confidential. Access to this information is limited to those who can prove a need to know.

6.5.2 Computer security evaluation

ESCB-PKI permanently evaluates its level of security to identify any possible weaknesses and establish the corresponding corrective measures, through internal and external audits, as well as continuously carrying out security checks.

6.6 Life Cycle Security Controls

The information under this section is confidential. Access to this information is limited to those who can prove a need to know.
The system will comply with all the relevant ESCB/SSM policies.

6.7 Network Security Controls

The information under this section is confidential. Access to this information is limited to those who can prove a need to know.

The system will be compliant with the relevant ESCB/SSM policies on network security.

6.8 Timestamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version number

All the ESCB-PKI certificates are compliant with X.509 Version 3 (X.509 v3) certificates.

7.1.2 Certificate extensions

The certificate extensions used generically are:

- *KeyUsage*. Classified as critical.
- *BasicConstraints*. Classified as critical.
- *CertificatePolicies*. Classified as non-critical.
- *SubjectAlternativeName*. Classified as non-critical.
- *CRLDistributionPoint*. Classified as non-critical.
- *Subject Key Identifier*. Classified as non-critical.
- *Authority Key Identifier*. Classified as non-critical.
- *extKeyUsage*. Classified as critical.
- *Auth. Information Access*. Classified as non-critical.

ESCB-PKI Certificate Policies may establish variations in the set of extensions used for each type of certificate.

The *SubjectAlternativeName* extension allows the following ESCB-PKI proprietary fields:

OID	Concept	Description
0.4.0.127.0.10.1.1.1	Personal Name	Name and surname of the certificate subscriber
0.4.0.127.0.10.1.1.2	Personal Middle Name	
0.4.0.127.0.10.1.1.3	Personal Surnames	
0.4.0.127.0.10.1.1.4	Personal Secondary Surname	
0.4.0.127.0.10.1.1.10	Personal First Surname	
0.4.0.127.0.10.1.1.5	Employee number	Employee or contracted personnel no.
0.4.0.127.0.10.1.1.6	External employee number	External employee or contracted personnel no.
0.4.0.127.0.10.1.1.7	ESCB user identifier (UID)	User identifier (UID) in the ESCB user repositories
0.4.0.127.0.10.1.1.8	National identifier Number	National ID document, Passport ID, etc.
0.4.0.127.0.10.1.1.9	ESCB/SSM Application code	Identifier of the ESCB/SSM application
0.4.0.127.0.10.1.1.11	ESCB/SSM Application description	Display name of the ESCB/SSM application or shared mailbox

ESCB-PKI has established a policy for assigning OIDs within its private numbering scale under which the OID for all the proprietary extensions for the ESCB-PKI certificates begin with the prefix 0.4.0.127.0.10.1.3.
ESCB-PKI has established the following proprietary extensions:

OID	Concept	Description
0.4.0.127.0.10.1.3.1	escbUseCertType	This extension provides the certificate purpose information. The allowed values are listed below: • SIGNATURE • AUTHENTICATION • ENCRYPTION • MOBILE DEVICE • SECURE EMAIL GATEWAY • PROVISIONAL • ADMINISTRATOR • SHARED MAILBOX

7.1.3 Algorithm Object Identifiers (OID)

Cryptographic algorithm objects identifiers (OID):
SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

7.1.4 Name formats

Certificates issued by ESCB-PKI contain the X.500 distinguished name of the certificate issuer and that of the subject in the issuer name and subject name fields, respectively.

7.1.5 Name constraints

The names contained in the certificates are restricted to X.500 distinguished names, which are unique and unambiguous.

7.1.6 Certificate Policy Object Identifiers (OID)

To be established in each CP.
ESCB-PKI has established a policy for assignment of OIDs within its private enumeration scale under which the OID for all the ESCB-PKI Policy Certificates begin with the prefix 0.4.0.127.0.10.1.2.

7.1.7 Use of the "PolicyConstraints" extension

No stipulation.

7.1.8 Syntax and semantics of the "PolicyQualifier

The Certificate Policies extension contains the following Policy Qualifiers:
- URL CPS: contains the URL to the CPS and the CP that govern the certificate.

7.1.9 Processing semantics for the critical "Certificate Policy" extension

The extension will be classified as *nonCritical*. This is done following the recommendations for the standard applications for secure e-mail, S/MIME [RFC 2632], and web authentication, SSL/TLS [RFC 2246]. The fact that the extension is not critical does not prevent the applications from using the information contained in said extension.

7.2 CRL Profile

7.2.1 Version number

ESCB-PKI supports and uses X.509 version 2 (v2) CRLs.

7.2.2 CRL and extensions

No stipulation.

7.3 OCSP Profile

7.3.1 Version number(s)

The profile is defined in RFC 2560.

7.3.2 OCSP Extensions

The VA supports signed requests and the NONCE extension.

8 Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Controls for each Authority

ESCB-PKI will be audited at least once every 3 year, in accordance with the ESCB Certificate Acceptance Framework – as amended from time to time including in relation to SSM -. This guarantees that its functioning and operations are in accordance with the stipulations included in this CPS and the CPs.

8.2 Identity/Qualifications of the Auditor

Audits to the ESCB-PKI may be entrusted to external auditors or, as specified in the ESCB Audit Policy – as amended from time to time including in relation to SSM -, to the ESCB Internal Auditors Committee (IAC) according to the annual audit program.

All teams or the person designated to carry out a security audit on ESCB-PKI must fulfil the following requirements:

- Appropriate training and experience in PKI, security, cryptographic technology and audit procedures.
- Independence at the organisational level from the ESCB-PKI Authority (RA, CA, KA or VA) being audited.

8.3 Relationship between the Assessor and the Entity being Assessed

Regardless of the purpose of the audit, the auditor and the audited party (ESCB-PKI) shall not have any kind of relationship that could derive in a conflict of interests. In the case of audits entrusted to the IAC, the auditors may not have any operational relationship with the area being audited.

8.4 Aspects Covered by Controls

The audit shall determine whether or not the ESCB-PKI services are in accordance with this CPS and the applicable CPs. It shall also determine whether and to what degree there is a risk of the operations failing to conform to what is established in those documents.

The scope of the audit activities shall include, at least:

- Security and privacy policy
- Physical security
- Technological evaluation
- Management of the CA's services
- Personnel selection
- Applicable CPS and CPs
- Sufficient level of staffing and skills
- Contracts

8.5 Actions Taken as a Result of Deficiencies Found

Corrective measures shall be taken upon identification of deficiencies found as a result of the audit. The ESCB-PKI Owner (Eurosystem Central Banks), in collaboration with the auditor, shall be responsible for establishing them.

In the event of observing serious deficiencies, the ITC may make, among others, the following decisions: temporary suspension of operations until the deficiencies are corrected, revocation of certificates issued to the assessed entity, suggest changes in the personnel involved, invocation of the liabilities policy and more frequent overall audits.

8.6 Notification of the Results

The audit team shall notify the results of the audit to the ESCB-PKI Owner (Eurosystem Central Banks and the ECB), the ESCB-PKI Security Manager, as well as the ESCB-PKI administrators and those of the Authority in which incidents were detected.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The fees for the issuance and renewal of each certificate are specified in the applicable CP.

9.1.2 Certificate access fees

The fees for certificate access are specified in the applicable CP.

9.1.3 Revocation or status information fees

The fees for access to the information on the status or revocation of each certificate are specified in the applicable CP

9.1.4 Fees for other services, such as policy information

No fees shall be applied for supplying information on this CPS or the CPs managed by ESCB-PKI or for any other additional service that may be known at the time of drawing up this document.

This provision may be modified by the CP applicable in each case.

9.1.5 Refund policy

Should any CP specify any fee applicable for certification or revocation services provided by ESCB-PKI for the type of certificate it defines, the corresponding refund policy must be established.

9.2 Financial Responsibility

9.2.1 Insurance

The ESCB-PKI has subscribed an insurance policy covering the risks identified with respect to the services provided. The coverage of the insurance is described in section 9.7.2.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of Business Information

Concerning the ESCB-PKI CA and RA duty to maintain the confidentiality of data and information it obtains in the course of its activities, the following confidentiality scheme is set up for data related to ESCB-PKI:

9.3.1 Scope of confidential information

All information not considered by ESCB-PKI as public shall be of a confidential nature and access may only be granted to those with an official need-to-know in order to perform their official duties related to the ESCB-PKI. The nature of confidential information is expressly given to:

- The ESCB-PKI Certification Authorities private keys.
- The private keys that ESCB-PKI holds in escrow.
- The information related to operations carried out by ESCB-PKI.
- The information referring to security, control and audit procedure parameters.
- Personal data provided by certificate applicants to ESCB-PKI during the registration process.

Personal data is protected pursuant to that established in the personal data protection laws and their implementation regulations.

9.3.2 Non-confidential information

The following information is considered public information and, therefore, available to third parties:

- The content of this CPS.
- The Certificate Policies.
- The list of certificates suspended or revoked.

The electronic certificates issued by the ESCB-PKI CA are published in an internal LDAP directory located at the service provider's premises only available to ESCB/SSM systems on a need-to-know basis.

9.3.3 Duty to maintain professional secrecy

All personnel who takes part in any activities inherent to or derived from ESCB-PKI are committed to maintaining professional secrecy and, therefore, are subject to the applicable legal provisions, in particular, Article 37 of the Statute of the European System of Central Banks and of the European Central Bank and the corresponding national provisions applicable to the ESCB national central banks and national competent authorities.

Likewise, contracted personnel that takes part in any ESCB-PKI activities or operations are subject to the duty of professional secrecy within the framework of their contractual obligations with ESCB-PKI CA and RA.

9.4 Privacy of Personal Information

9.4.1 Personal data protection policy

The procedures and operation of the ESCB-PKI, this CPS and each CP are in line with the national legislation applicable to the ESCB Central Banks and National Competent Authorities implementing the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1994 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regards to the processing of personal data by the Community institutions and bodies and of free movement of such a data[2].

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.

9.4.2 Information considered private

All data corresponding to individuals is personal data for the purposes of the ESCB-PKI personal data protection policy and shall be considered private, unless otherwise specified in this CPS or the relevant CP, in accordance with section 9.4.3 below.

9.4.3 Information not classified as private

Each CP shall establish the personal data to be included in the personal certificates. Acceptance by the applicants of the certificates issued in their name constitutes their consent to publication.

9.4.4 Responsibility to protect personal data

The Eurosystem Central Banks (as the owners of the ESCB-PKI), Banco de España (as the Service Provider) and the non-Eurosystem Central Banks and the National Competent Authorities that use the ESCB-PKI are co-controllers for ESCB-PKI data protection purposes, and in accordance with the allocation of roles and responsibilities, comply with and apply the legal, technical and management measures required by the respective national legislation transposing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1994 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The ECB processes personal data in accordance with Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regards to the processing of personal data by the Community institutions and bodies and of free movement of such a data.

9.4.5 Notification of and consent to the use of personal data

Each CP shall establish the mechanisms to notify certificate applicants and, when appropriate, obtain their consent for the processing of their personal data.

9.4.6 Disclosure within legal proceedings

Personal data may only be disclosed to third parties, without the consent of the person affected, to the extent permitted under the applicable personal data protection law.

9.4.7 Other circumstances in which data may be made public

No stipulation.

9.5 Intellectual Property Rights

The ESCB-PKI Service Provider has obtained all the necessary licenses regarding all intellectual property rights related to the electronic certificates issued by the ESCB-PKI for individuals and technical components, the certificate revocation lists, the content of this CPS and the CPs as well as all intellectual property rights related to any other electronic or any other kind of document, protocol, computer program and hardware, file, directory, database and consultation service that may be required to carry out the ESCB-PKI activities.

The object identifiers (OIDs) are property of Eurosystem central banks and have been registered with the European Telecommunications Standards Institute (ETSI) under the itu-t.identified-organization.etsi.reserved.etsi-identified-organization 0.4.0.127.0-ETSI identified organizations

section, having been assigned the number **0.4.0.127.0.10** (ESCB-PKI). This may be consulted and verified at the document ETSI EG 200 351 (downloadable from http://www.etsi.org).
Unless express agreement from ESCB-PKI, no OID assigned to ESCB-PKI may be partially or fully used, except for the specific uses included in the Certificate or Directory.

9.6 Representations and Warranties

9.6.1 Obligations of the CA

The ESCB-PKI CA has the following obligations:

CAO.1	To carry out its operations in accordance with this CPS. To provide CA services in accordance with the practices in this CPS.
CAO.2	To protect the private keys.
CAO.3	To issue certificates in accordance with the applicable CP.
CAO.4	Following receipt of a valid certificate application, to issue certificates in accordance with the practices in this CPS and the the X.509 v3 standard and the requirements of the application.
CAO.5	To issue certificates that are in accordance with the information known at the time of their issue, and free from data recording errors.
CAO.6	To publish the certificates to interoperate with other users or computer systems that so require.
CAO.7	To revoke the certificates in the terms of point *4.4 Certificate Revocation and Suspension* and publish revoked certificates in the CRL and in the directory and web services referred to under point *4.9.7 Issue Frequency of CRLs*
CAO.8	To publish this CPS and the applicable CPs on the website referred to under point *2.1 Repositories*.
CAO.9	To notify changes to this CPS and the CPs as established under point 9.*10.2 Notification Period and Mechanism*
CAO.10	To guarantee the availability of the CRLs, pursuant to point 4.9.9 in this CPS.
CAO.11	In the event that the CA revokes a certificate, to notify this to the certificate users in accordance with the applicable CP.
CAO.12	To operate in accordance with the applicable legislation and specifically with: - Spanish Law 59/2003, of 19 December 2009, on electronic signature. - Spanish Organic Law 15/1999, of 13 December 1999, on the protection of personal data.
CAO.13	To protect the keys in its custody, if any.
CAO.14	Not to store, under any circumstances, the signature creation data, the private key, of the certificate subscribers issued for the purpose of using them for electronic signature *(key usage = nonrepudiation)*, whether acknowledged or not.

CAO.15	In the event of ceasing its activity, to report this at least two months in advance to the certificate subscribers issued by the CA and to the Spanish Ministry of Industry, Trade and Tourism, as stipulated under point 5.8.1.
CAO.16	To keep a record of all the information related to a qualified certificate for a period of fifteen years.
CAO.17	Guaranteeing that the data for the creation and verification of the digital signature is complementary
CAO.18	To provide CA services 7 days a week, 24 hours per day with the stipulation that it is not a warranty of 100% availability (availability may be affected by systemic maintenance, system repair, or by factors outside the control of the CA).
CAO.19	To ensure corrective actions to deficiencies identified by an audit.
CAO.20	By delivering the certificate to the subscriber, the ESCB-PKI CA certifies it has issued a certificate to the named subscriber; and that the information stated in the certificate was verified in accordance with this CPS; and the subscriber has accepted the certificate

9.6.2 Obligations of the RA

The ESCB-PKI RAs shall fulfil the following obligations:

RAO.1	To properly verify the identity of the certificate subscribers and/or applicants and the organisations they represent, in accordance with the procedures established in this CPS and CP specific to each type of certificate, employing any legally approved means.
RAO.2	To inform the certificate applicant and/or subscriber of the terms and conditions for the use of the certificate. Bring to the attention of their certificate applicants and/or subscribers all relevant information pertaining to the rights and obligations of the CA, RA, certificate applicants and certificate subscribers contained in this CPS, the terms and conditions for the use of the certificate, and any other relevant document outlining the terms and conditions of use.
RAO.3	To formalise the issuance of the certificates to the certificate subscribers in the terms and conditions established in the CP.
RAO.4	To submit to the CA complete, accurate, valid and duly authorised certificate applications.
RAO.5	To store in a secure manner and for the period indicated in section 5.5.2 of the relevant Certificate Policies the documentation provided in the certificate issuance process and in its suspension/revocation process, including a copy of the terms and conditions accepted by the certificate applicants in which they acknowledge that they have understood their obligations and rights, consent to the use of their personal data by the CA and confirm that the information provided is correct.
RAO.6	To carry out any duties that may correspond, through the personnel necessary in each case, as established in this CPS.

9.6.3 Obligations of certificate subscribers

The certificate subscribers issued under this CPS shall have the following obligations:

CSO.1	Provide accurate, full and truthful information regarding the data requested by those entrusted with their verification in order to carry out the registration process.
CSO.2	To inform the corresponding RA of any modification to said data.
CSO.3	To understand and accept the terms and conditions of use of the certificates and, specifically, those contained in this CPS and the applicable CPs, as well as any modifications thereto.
CSO.4	To restrict and condition the use of the certificates to that permitted under the corresponding CP and this CPS.
CSO.5	To take reasonable precautions for the safekeeping of their cryptographic card, preventing its loss, modification or unauthorised use.
CSO.6	The process to obtain the certificates requires the personal selection of a control PIN for the cryptographic card and activation of the private keys and a PUK for unlocking. The subscriber is responsible for keeping the PIN and PUK numbers secret.
CSO.7	To immediately request the RA the revocation or suspension of a certificate upon detecting any inaccuracy in the information contained therein or upon becoming aware of or suspecting any compromise of the private key corresponding to the public key contained in the certificate due, among other causes, to: loss, theft, potential compromise, knowledge by third parties of the PIN and/or PUK. The procedure for requesting certificate revocation and suspension are described in sections 4.9.3 and 4.9.15 of the corresponding CP.
CSO.8	Not monitor, manipulate or carry out any reverse engineering on the technical implementation (hardware and software) of the certification services.
CSO.9	Not to transfer or delegate to third parties their obligations pertaining to a certificate assigned to them.
CSO.10	Any other obligation under this CPS or the CP.

9.6.4 Obligations of relying parties

Third parties who accept and rely on certificates issued by ESCB-PKI shall have the following obligations:

RPO.1	To limit reliability on the certificates to the uses that they allow, pursuant to the certificate extensions and the corresponding CP and this CPS.
RPO.2	To verify the validity of the certificates by checking that the certificate is valid and has not expired or been suspended or revoked.
RPO.3	To assume the responsibility for correct verification of the electronic signatures, including the verification of the validity of the signer's certificate.

RPO.4	To assume responsibility for checking the validity as well as the revocation or suspension status of the certificates they accept and rely on.
RPO.5	To be aware of the guarantees and responsibilities derived from acceptance of the certificates on which they rely and accept that they are subject to them.
RPO.6	To notify any anomalous event or circumstance pertaining to the certificate, which could be considered cause for its revocation.
RPO.7	Trust and make use of certificates only if a valid certificate chain is established between the relying party and the certificate subject.

9.7 Disclaimers of Warranties

9.7.1 ESCB-PKI liabilities

The Eurosystem Central Banks, the Banco de España and the non-Eurosystem CBs and the NCAs that use the ESCB-PKI shall be held liable according to their liabilities pursuant to Decision ECB/2013/1 and to Decision (EU) 2015/XX (ECB/2015/XX)

The Liability of Eurosystem central banks towards users is foreseen in Article 10 of the Decision ECB/2013/1. Particularly, Banco de España as the Certification Authority, will be liable in case of damages to the certificate subscriber or bona fide relying parties in case of lack or delay while including certificates in the revocation information service; unless Banco de España can prove that it has not acted negligently.

9.7.2 Scope of liability coverage

ESCB-PKI has taken out civil liability insurance coverage in the amount of €3,000,000 to cover any risks of liability for damages that may be caused by the use of qualified certificates issued by ESCB-PKI. Since Banco de España acts as CA for the ESCB-PKI, that civil liability insurance coverage fully complies with the requirements laid down in Spanish Law 59/2003, of 19 December 2009, on electronic signature.

9.8 Limitations of Liability

Article 10 of Decision ECB/2013/1 sets out the liability of the Eurosystem central banks towards users.

Except those stipulated in the provisions of this CPS or in the applicable CP and in the applicable legislation, the ESCB central banks and national competent authorities shall accept no other liability regarding certificate subscribers or relying parties in the event of losses or damages:

LIAB.1	Related to services it provides, in the event of war, natural disaster or any other kind of accidental or force majeure circumstances: public disorder, transport strike, loss of power and/or telephone service, computer viruses, deficiencies in telecommunication services or compromise in the asymmetric keys derived from an unforeseeable technological hazard.
LIAB.2	Incurred during the period between certificate application and delivery to the certificate subscriber.

LIAB.3	Caused by certificate usage that exceeds the limitations established in the same, the corresponding CP and this CPS.
LIAB.4	Caused by misuse of the information contained in the certificate.
LIAB.5	Caused by improper or fraudulent use of certificates or the CRLs issued by ESCB-PKI CA.
LIAB.6	ESCB-PKI CA and RAs shall not be held liable in any way whatsoever for the use of certificates issued by its CA and the private/public key pair linked to certificate subscribers for any activity not specified in the CPS or in the corresponding CPs
LIAB.7	ESCB-PKI CA and RAs, shall not be held liable for the content of documents signed using its certificates, nor for any other use of its certificates, such as message or communication encipherment processes.
LIAB.8	ESCB-PKI CA and RAs shall not be held liable for any indirect, incidental, consequential or any other kind of damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates, digital signatures, or other transactions or services contemplated by the present CPS.

9.9 Indemnities

ESCB-PKI assumes no financial responsibility for improperly used certificates, CRLs, etc.

9.10 Term and Termination

9.10.1 Term

This CPS shall come into force from the moment it is published in the ESCB-PKI repository.
This CPS shall remain valid until such time as it is expressly terminated due to the issue of a new version, or upon re-key of the Root CA keys, at which time a new version shall be drawn up.

9.10.2 CPS substitution and termination

If this CPS is substituted, it shall be substituted for a new version, regardless of the importance of the changes carried out therein. Accordingly, it shall always be applicable in its entirety.
If the CPS is terminated, it shall be withdrawn from the ESCB-PKI public repository, though a copy thereof shall be held for 15 years.

9.10.3 Consequences of termination

The obligations established under this CPS, referring to audits, confidential information, ESCB-PKI obligations and liabilities that came into being whilst it was in force shall continue to prevail following its termination or substitution , in this latter case, only with respect to those terms which are not contrary to the new version.

9.11 Individual notices and communications with participants

All notifications, demands, applications or any other type of communication required in the practices described in this CPS shall be carried out by electronic message or in writing, by registered post, addressed to any of the addresses contained in point 1.5 above (Policy Administration). Electronic notifications shall be effective upon receipt by the recipients to which they are addressed.

9.12 Amendments

9.12.1 Amendment procedures

The authority empowered to carry out and approve amendments to this CPS and the CPs is the Policy Approval Authority (PAA). The PAA's contact details can be found under point 1.5 above (Policy Administration).

9.12.2 Notification period and mechanism

Should the PAA deem that the amendments to this CPS or a CP could affect the acceptability of the certificates for specific purposes, it shall request the ESCB-PKI service provider to notify the users of the certificates corresponding to the amended CP or CPS that an amendment has been carried out and that they should consult the new CPS in the relevant repository. When, in the opinion of the PAA, the changes do not affect the acceptability of the certificates, the changes shall not be notified to the users of the certificates.

9.12.3 Circumstances in which the OID must be changed

In case of amendment, when numbering the new version of the CPS or the relevant CP:

- If the PAA deems that the amendments could affect the acceptability of the certificates for specific purposes, the highest version number of the document shall be changed and its lowest number reset to zero. The last two numbers of the Object Identifier (OID), which match those of the lower version number, will also be modified.
- If the PAA deems that the amendments do not affect the acceptability of the certificates for specific purposes, the lowest version number of the document will be increased as well as the last number of the Object Identifier (OID) that represents it, maintaining the highest version number of the document, as well as the rest of the associated OID.

9.13 Dispute Resolution Procedures

Resolution of any dispute between users and the ESCB-PKI that may arise shall be submitted to the courts of the city where the registered address of the national central bank which acted or would have acted as RA is located/ for the ECB the European Court of Justice, the parties waiving any other jurisdiction to which they may have a right.

9.14 Governing Law

The Decision of the European Central Bank of 11 January 2013 (ECB/2013/1) governs the operations and functioning of the ESCB-PKI, as well as this CPS and the applicable CP for each type of certificate.

Since Banco de España acts as CA for the ESCB-PKI, certificates are issued in accordance with Spanish Law 59/2003, of 19 December 2003, on electronic signature, and are fully recognised

within the European Union in accordance with the national laws and regulations implementing Directive 1999/93/EC of the European Parliament and of 13 December 1999 on a Community framework for electronic signature and Regulation (EU) No 910/2014 of the European Parliament and of the Council[1].

The CA, the RAs and the VA shall comply with the following EU legislation and where applicable with the relevant national laws and/or internal rules and, in particular, with those implementing:

- Directive 95/46/EC of EC of the European Parliament and of the Council[2];
- .
- Directive 1999/93/EC of the European Parliament and of 13 December 1999 on a Community framework for electronic signature
- Regulation (EU) No 910/2014 of the European Parliament and of the Council.
- Decision (EU) 2015/XX (ECB/2015/XX)[3]The ECB processes personal data in accordance with Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regards to the processing of personal data by the Community institutions and bodies and of free movement of such a data.

9.15 Compliance with Applicable Law

ESCB-PKI Participants are responsible for ensuring compliance with the applicable legislation.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement clause

All the users and relying parties accept the content of the latest version of this CPS and the applicable CPs in their entirety.

9.16.2 Independence

Should any of the provisions of this CPS be declared invalid, null or legally unenforceable, it shall be deemed as not included, unless said provisions were essential in such a way that excluding them from the CPS would render the latter without legal effect.

9.16.3 Resolution through the courts

No stipulation.

9.17 Other Provisions

No stipulation.

---

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

[2] Directive 95/46/EC of EC of the European Parliament and of the Council of 24 October 1994 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[3] Decision (EU) 2015/[XX] of [date, month] 2015 on the access and use of SSM electronic applications, systems, platforms and services by the European Central Bank and the national competent authorities of the Single Supervisory Mechanism (ECB/2015/XX), not yet published in the Official Journal of the European Union.

NBB - Securities
boulevard de Berlaimont 14
BE -1000 Brussels (Belgium)
Phone: + 32 (0)2 221 22 14
Fax: + 32 (0)2 221 31 19
E-mail: sss@nbb.be

BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI SERVICES

OIDS: 0.4.0.127.0.10.1.2.2.0

CERTIFICATE POLICIES FOR THE ESCB/SSM USERS' CERTIFICATES

VERSION 1.3

11 May 2015

Table of Contents

1 Introduction 8

1.1 Overview 8

1.2 Document Name and Identification 9

1.3 ESCB-PKI Participants 10

1.3.1 The Policy Approval Authority 10
1.3.2 Certification Authority 10
1.3.3 Registration Authorities 10
1.3.4 Validation Authority 11
1.3.5 Key Archive 11
1.3.6 Users 11

1.4 Certificate Usage 12

1.4.1 Appropriate certificate use 12
1.4.2 Certificate Usage Constraints and Restrictions 13

1.5 Policy Approval 13

1.6 Definitions and Acronyms 13

1.6.1 Definitions 13
1.6.2 Acronyms 14

2 Publication and Repository Responsibilities 16

2.1 Repositories 16

2.2 Publication of Certification Data, CPS and CP 16

2.3 Publication Timescale or Frequency 16

2.4 Repository Access Controls 16

3 Identification and Authentication (I&A) 17

3.1 Naming 17

3.1.1 Types of names 17
3.1.2 The need for names to be meaningful 17
3.1.3 Rules for interpreting various name formats 17
3.1.4 Uniqueness of names 17
3.1.5 Name dispute resolution procedures 18
3.1.6 Recognition, authentication, and the role of trademarks 18

3.2 Initial Identity Validation 18

3.2.1 Means of proof of possession of the private key 18
3.2.2 Identity authentication for an entity 18
3.2.3 Identity authentication for an individual 19
3.2.4 Non-verified applicant information 19
3.2.5 Validation of authority 19
3.2.6 Criteria for operating with external CAs 19

3.3 Identification and Authentication for Re-key Requests 19

3.3.1 Identification and authentication requirements for routine re-key 19

3.3.2 Identification and authentication requirements for re-key after certificate revocation 20

4 Certificate Life-Cycle Operational Requirements 21

4.1 Certificate Application 21

4.1.1 Who can submit a certificate application? 21

4.1.2 Enrolment process and applicants' responsibilities 21

4.2 Certificate Application Processing 26

4.2.1 Performance of identification and authentication procedures 26

4.2.2 Approval or rejection of certificate applications 26

4.2.3 Time limit for processing the certificate applications 26

4.3 Certificate Issuance 26

4.3.1 Actions performed by the CA during the issuance of the certificate 26

4.3.2 CA notification to the applicants of certificate issuance 26

4.4 Certificate Acceptance 26

4.4.1 Form of certificate acceptance 26

4.4.2 Publication of the certificate by the CA 26

4.4.3 Notification of certificate issuance by the CA to other Authorities 26

4.5 Key Pair and Certificate Usage 26

4.5.1 Certificate subscribers' use of the private key and certificate 26

4.5.2 Relying parties' use of the public key and the certificate 27

4.6 Certificate Renewal 27

4.7 Certificate Re-key 27

4.7.1 Circumstances for certificate renewal with key changeover 27

4.7.2 Who may request certificate renewal? 27

4.7.3 Procedures for processing certificate renewal requests with key changeover 27

4.7.4 Notification of the new certificate issuance to the certificate subscriber 27

4.7.5 Manner of acceptance of certificates with changed keys 27

4.7.6 Publication of certificates with the new keys by the CA 28

4.7.7 Notification of certificate issuance by the CA to other Authorities 28

4.8 Certificate Modification 28

4.8.1 Circumstances for certificate modification 28

4.9 Certificate Revocation and Suspension 28

4.9.1 Circumstances for revocation 28

4.9.2 Who can request revocation? 28

4.9.3 Procedures for requesting certificate revocation 28

4.9.4 Revocation request grace period 28

4.9.5 Time limit for the CA to process the revocation request 28

4.9.6 Requirements for revocation verification by relying parties 29

4.9.7 CRL issuance frequency 29

4.9.8 Maximum latency between the generation of CRLs and their publication 29

4.9.9 Online certificate revocation status checking availability 29

4.9.10 Online revocation checking requirements 29

4.9.11 Other forms of revocation alerts available 29

4.9.12 Special requirements for the revocation of compromised keys 29

4.9.13 Causes for suspension 29

4.9.14 Who can request the suspension? ... 30
4.9.15 Procedure for requesting certificate suspension ... 30
4.9.16 Suspension period limits ... 30
4.10 Certificate Status Services ... 30
4.11 End of Subscription ... 30
4.12 Key Escrow and Recovery ... 30
4.12.1 Key Archive and recovery practices and policies ... 30
4.12.2 Session key protection and recovery policies and practices ... 31
5 Facility, Management, and Operational Controls ... 32
5.1 Physical Security Controls ... 32
5.2 Procedural Controls ... 32
5.3 Personnel Controls ... 32
5.4 Audit Logging Procedures ... 32
5.5 Records Archival ... 32
5.5.1 Types of records archived ... 32
5.5.2 Archive retention period ... 32
5.5.3 Archive protection ... 32
5.5.4 Archive backup procedures ... 32
5.5.5 Requirements for time-stamping records ... 32
5.5.6 Audit data archive system (internal vs. external) ... 32
5.5.7 Procedures to obtain and verify archived information ... 32
5.6 Key Changeover ... 32
5.7 Compromise and Disaster Recovery ... 33
5.8 CA or RA Termination ... 33
6 Technical Security Controls ... 34
6.1 Key Pair Generation and Installation ... 34
6.1.1 Key pair generation ... 34
6.1.2 Delivery of private keys to certificate subscribers ... 35
6.1.3 Delivery of the public key to the certificate issuer ... 36
6.1.4 Delivery of the CA's public key to relying parties ... 37
6.1.5 Key sizes ... 37
6.1.6 Public key generation parameters and quality checks ... 37
6.1.7 Key usage purposes (KeyUsage field in X.509 v3) ... 37
6.2 Private Key Protection and Cryptographic Module Engineering Controls ... 37
6.2.1 Cryptographic module standards ... 37
6.2.2 Private key multi-person (k out of n) control ... 37
6.2.3 Escrow of private keys ... 38
6.2.4 Private key backup copy ... 38
6.2.5 Private key archive ... 38
6.2.6 Private key transfer into or from a cryptographic module ... 38
6.2.7 Private key storage in a cryptographic module ... 38
6.2.8 Private key activation method ... 39

6.2.9 Private key deactivation method 39
6.2.10 Private key destruction method 39
6.2.11 Cryptographic module classification 39
6.3 Other Aspects of Key Pair Management 39
6.3.1 Public key archive 39
6.3.2 Operational period of certificates and usage periods for key pairs 39
6.4 Activation Data 39
6.5 Computer Security Controls 40
6.6 Life Cycle Security Controls 40
6.7 Network Security Controls 40
6.8 Timestamping 40
7 Certificate, CRL, and OCSP Profiles 41
7.1 Certificate Profile 41
7.1.1 Version number 41
7.1.2 Certificate extensions 41
7.1.3 Algorithm Object Identifiers (OID) 60
7.1.4 Name formats 60
7.1.5 Name constraints 60
7.1.6 Certificate Policy Object Identifiers (OID) 60
7.1.7 Use of the "PolicyConstraints" extension 60
7.1.8 Syntax and semantics of the “PolicyQualifier 60
7.1.9 Processing semantics for the critical “CertificatePolicy” extension 61
7.2 CRL Profile 61
7.3 OCSP Profile 61
8 Compliance Audit and Other Assessment 62
9 Other Business and Legal Matters 63
9.1 Fees 63
9.1.1 Certificate issuance or renewal fees 63
9.1.2 Certificate access fees 63
9.1.3 Revocation or status information fees 63
9.1.4 Fees for other services, such as policy information 63
9.1.5 Refund policy 63
9.2 Financial Responsibility 63
9.3 Confidentiality of Business Information 63
9.3.1 Scope of confidential information 63
9.3.2 Non-confidential information 63
9.3.3 Duty to maintain professional secrecy 63
9.4 Privacy of Personal Information 63
9.4.1 Personal data protection policy 63
9.4.2 Information considered private 64
9.4.3 Information not classified as private 64
9.4.4 Responsibility to protect personal data 64

9.4.5 Notification of and consent to the use of personal data 64
9.4.6 Disclosure within legal proceedings 64
9.4.7 Other circumstances in which data may be made public 64
9.5 Intellectual Property Rights 64
9.6 Representations and Warranties 64
9.7 Disclaimers of Warranties 64
9.8 Limitations of Liability 64
9.9 Indemnities 64
9.10 Term and Termination 64
9.10.1 Term 64
9.10.2 CP substitution and termination 65
9.10.3 Consequences of termination 65
9.11 Individual notices and communications with participants 65
9.12 Amendments 65
9.13 Dispute Resolution Procedures 65
9.14 Governing Law 65
9.15 Compliance with Applicable Law 65
9.16 Miscellaneous Provisions 65
9.16.1 Entire agreement clause 65
9.16.2 Independence 65
9.16.3 Resolution through the courts 65
9.17 Other Provisions 65

Control Sheet

	Title	Certification Policy for the ESCB/SSM users' certificates
	Author	ESCB-PKI Service Provider
	Version	1.3
	Date	11.05.2015

RELEASE NOTES

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column "Release number" refer to the current version of the document.

Release number	Status	Date	Change Reason
0.1	Draft	27.05.2011	BdE revision
0.2	Draft	15.06.2011	BdE revision
0.3	Draft	14.07.2011	BdE revision
0.4	Draft	22.07.2011	BdE revision
0.5	Draft	26.07.2011	Add CA Fingerprint
0.6	Draft	15.09.2011	Revision of certificate profiles
1.0	Final	19.10.2011	Update after ITC approval.
1.1	Final	11.01.2013	GovC approval
1.2	Final	10.12.2013	New certificate types for mobile devices, shared mailbox, administrator and provisional
1.3	Final	11.05.2015	Hashing algorithm update

1 Introduction

1.1 Overview

This document sets out the Certificate Policy (CP) governing the personal certificates issued to ESCB/SSM users (i.e. users that belong to ESCB Central Banks or SSM National Competent Authorities) by the Public Key Infrastructure (hereinafter referred to as PKI) of the European System of Central Banks (hereinafter referred to as ESCB-PKI). It has been drafted in compliance with the **Decision ECB/2013/1 of the European Central Bank**[1].

This document is intended for the use of all the participants related to the ESCB-PKI hierarchy, including the Certification Authority (CA), Registration Authorities (RA), certificate applicants, certificate subscribers and relying parties, among others.

From the perspective of the X.509 v3 standard, a CP is a set of rules that define the applicability or use of a certificate within a community of users, systems or specific class of applications that have a series of security requirements in common.

This CP details and completes the "Certification Practice Statement" (CPS) of the ESCB-PKI, containing the rules to which the use of the certificates defined in this policy are subject, as well as the scope of application and the technical characteristics of this type of certificate.

This CP has been structured in accordance with the guidelines of the PKIX work group in the IETF (Internet Engineering Task Force) in its reference document RFC 3647 (approved in November 2003) "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". In order to give the document a uniform structure and facilitate its reading and analysis, all the sections established in RFC 3647 have been included. Where nothing has been established for any section the phrase “No stipulation” will appear.

Furthermore, when drafting its content, European standards have been taken into consideration, among which the most significant are:

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
- ETSI TS 101 862: Qualified Certificate Profile.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

The following legislation has been considered:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1994[2].
- Directive 1999/93/EC of the European Parliament and of the Council [3].
- Regulation (EU) No 910/2014 of the European Parliament and the Council[4].
- Spanish Law 59/2003, of 19 December, the Electronic Signature Act (Spanish Official Journal, 20 December).[5]
- Spanish Organic Law 15/1999, of 13 December 1999, on the protection of personal data

[1] Decision ECB/2013/1of the European Central Bank of 11 January 2013 laying down the framework for a public key infrastructure for the European System of Central Banks (OJ L 74, 16.3.2013, p. 30).

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1994 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

[4] Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

[5]Spanish legislation is also considered owed to the fact that Banco de España, the Service Provide, is established at Spain

- Spanish Royal Decree 1720/2007, of 21 December2007, approving the Regulations for the development of Spanish Organic Law 15/1999.

National legislation transposing Directive 95/46/EC and the Directive 99/93/EC applicable to the ESCB central banks and SSM national competent authorities acting as Registration Authorities.

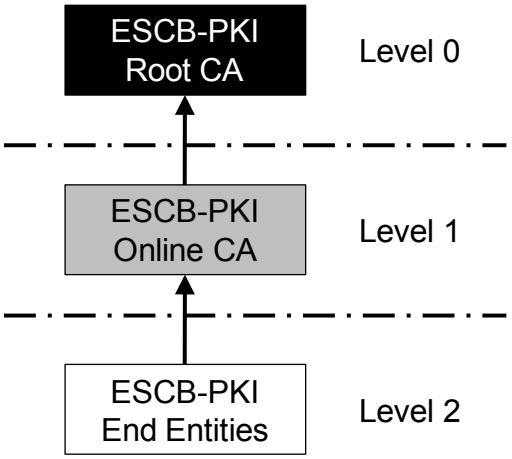
- Decision (EU) 2015/XX (ECB/2015/XX)[6].

This CP sets out the services policy, as well as a statement on the level of guarantee provided, by way of description of the technical and organisational measures established to guarantee the PKI's level of security.

The CP includes all the activities for managing the ESCB/SSM users' certificates throughout their life cycle, and serves as a guide for the relations between ESCB-PKI and its users. Consequently, all the PKI participants (see section 1.3) must be aware of the content of the CP and adapt their activities to the stipulations therein.

This CP assumes that the reader is conversant with the PKI, certificate and electronic signature concepts. If not, readers are recommended to obtain information on the aforementioned concepts before they continue reading this document.

The general architecture, in hierarchic terms, of ESCB-PKI is as follows:



1.2 Document Name and Identification

Document name	Certificate Policy (CP) for the ESCB/SSM users' certificates
Document version	1.3
Document status	Final
Date of issue	11.05.2015
OID (Object Identifiers)	0.4.0.127.0.10.1.2.2.0: Certificate policies for the ESCB/SSM users' certificates (this document) 0.4.0.127.0.10.1.2.2.1: Certificate Policy of Advanced Authentication certificate for ESCB/SSM

[6] Decision (EU) 2015/[XX] of [date, month] 2015 on the access and use of SSM electronic applications, systems, platforms and services by the European Central Bank and the national competent authorities of the Single Supervisory Mechanism (ECB/2015/XX), not yet published in the Official Journal of the European Union.

	users 0.4.0.127.0.10.1.2.2.2: Certificate Policy of Archived Encryption certificate for ESCB/SSM users 0.4.0.127.0.10.1.2.2.3: Certificate Policy of Non-Archived Encryption certificate for ESCB/SSM users 0.4.0.127.0.10.1.2.2.4: Certificate Policy of Advanced Signature certificate based on a SSCD for ESCB/SSM users 0.4.0.127.0.10.1.2.2.5: Certificate Policy of Advanced Signature certificate for ESCB/SSM users 0.4.0.127.0.10.1.2.2.6: Certificate Policy of Standard Authentication certificate for ESCB/SSM users 0.4.0.127.0.10.1.2.2.7: Certificate Policy of Mobile Device certificate for ESCB/SSM users 0.4.0.127.0.10.1.2.2.8: Certificate Policy of Secure E-mail Gateway certificate for ESCB/SSM users 0.4.0.127.0.10.1.2.2.9: Certificate Policy of Provisional certificate for ESCB/SSM users 0.4.0.127.0.10.1.2.2.10: Certificate Policy of Administrator certificate for ESCB/SSM users 0.4.0.127.0.10.1.2.2.11: Certificate Policy of Shared Mailbox certificate for ESCB/SSM users 0.4.0.127.0.10.1.2.2.12: Certificate Policy of Archived Encryption certificate recoverable in software for ESCB/SSM users
CPS location	http://pki.escb.eu/policies
Related CPS	Certification Practice Statement of ESCB-PKI OID 0.4.0.127.0.10.1.2.1

1.3 ESCB-PKI Participants

As specified in the ESCB-PKI CPS.

1.3.1 The Policy Approval Authority

As specified in the ESCB-PKI CPS.

1.3.2 Certification Authority

As specified in the ESCB-PKI CPS.

1.3.3 Registration Authorities

As specified in the ESCB-PKI CPS.

1.3.3.1 Registration Authorities' roles

From the list of Registration Authorities' roles described in the CPS the ones required to manage ESCB/SSM users' certificates are the following:

- **Registration Officers**
- **Trusted Agents**
- **Key Recovery Officers**
- **Shared Mailbox Administrators**

1.3.4 Validation Authority

As specified in the ESCB-PKI CPS.

1.3.5 Key Archive

The Key Archive service, defined in the ESCB-PKI CPS, is only applicable for the archived encryption certificate, as well as the related encryption private key. Thus, no other private keys will be archived.

1.3.6 Users

As specified in the ESCB-PKI CPS.

1.3.6.1 Certificate Subscribers

Certificate subscribers are defined in accordance with the ESCB-PKI CPS.

The categories of persons who may be certificate subscribers of ESCB/SSM users's certificates issued by the ESCB-PKI Online CA are limited to those included in the following chart:

Certification Authority	**Certificate subscribers**
Online CA	Users from ESCB Central Banks or SSM National Competent Authorities (ESCB/SSM users) It will be up to each CB or NCA to decide the legal binding with the group of people that will be certificate subscribers of ESCB/SSM users's certificates (i.e. just internal employees, subcontractors, etc.)

Certificate subscribers will be able to receive any of the following certificate packages:

- Advanced certificate package, where all the following certificates will be stored in a smartcard or other cryptographic token (e.g. USB device):

- Advanced authentication certificate. The corresponding key pair will be generated inside the cryptographic token.
- Advanced signature certificate or advanced signature certificate based on a SSCD depending upon if the cryptographic token has got a SSCD certification or not. In both cases, the corresponding private key will be generated inside the cryptographic token.
- One of the following encryption certificates: i) advanced encryption certificate without key archive, ii) advanced encryption certificate with archived private key only recoverable in a token, or iii) standard encryption certificate with archived private key recoverable in software format or in a token. In the first case, the key pair will be

generated inside the cryptographic token and no other copy will be archived. In the second and third cases, the key pair will be generated by the ESCB-PKI Subordinate CA and afterwards stored in the cryptographic device and another copy in the Key Archive service. The archived copies of the private key will be recoverable only in a token (second case) or in software format or in a token (third case)

- **Standard certificates**, where the private key will be generated by the CA and stored in a software device. The standard certificate will be mainly valid for authentication, although signature and encryption is also allowed.
- **Mobile device certificates**, where the private key will be generated by the CA and stored in a software keystore with the aim of being imported into a mobile device. This certificate is mainly valid for authentication, although signature is also allowed.
- **Secure e-mail gateway certificates**, where the private key will be generated by the CA and stored in a software keystore with the aim of being imported into a secure e-mail gateway. This certificate is valid for e-mail signing and encryption.
- **Administrator certificates**, where the private key will be generated and stored in a smartcard or other cryptographic token (e.g. USB device). This certificate is oriented for those subscribers that have got an administrator account to access IT or business services with special privileges. The certificate is mainly valid for authentication, although signature is also allowed.
- **Provisional certificates**, where the private key will be generated and stored in a smartcard or other cryptographic token (e.g. USB device). This certificate is oriented for those subscribers of advanced or administrator certificates that have forgotten their smartcard and need to access IT or business services that require two-factor authentication. The certificate has a limited lifetime (less or equal to 31 days) and is mainly valid for authentication, although signature is also allowed.
- **Shared mailbox certificates**, where the private key will be generated by the CA and stored in a software keystore so that each person that needs to access the shared mailbox has a copy of the keys. This certificate is oriented to protecting information exchanged by a shared mailbox. The certificate is mainly valid for e-mail signing and encryption, although authentication is also allowed.

1.3.6.2 Relying Parties

As specified in the ESCB-PKI CPS.

1.4 Certificate Usage

1.4.1 Appropriate certificate use

1 Certificates issued by ESCB-PKI in the scope of this CP may only be used within the scope of the ESCB/SSM by users from any of the ESCB Central Banks or National Competent Authorities.

2 Within the scope of the paragraph above, certificates issued by ESCB-PKI may be used for financial activities.

The certificates regulated by this CP shall be used for personal authentication, signing and/or encipherment purposes, depending on the corresponding keyUsage extension and OID attribute in the *certificatePolicies* extension.

1.4.2 Certificate Usage Constraints and Restrictions

Any other use not included in the previous point shall be excluded.

1.5 Policy Approval

As specified in the ESCB-PKI CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

Within the scope of this CP the following terms are used:

Authentication: the process of confirming the identity of a certificate subscriber.

Identification: the process of verifying the identity of those applying for a certificate.

Eurosystem Central Bank: means either an NCB of a Member State whose currency is the euro or the ECB.

Non-euro area NCB: means an NCB of a Member State whose currency is not the euro.

ESCB Central Bank: means either a Eurosystem Central Bank or a non-euro area NCB**.**

Central Bank: In this CP the term "Central Bank" is used to refer to any Central Bank belonging to the European System of Central Banks(ESCB)/Eurosystem, including the ECB.

National Competent Authority or SSM National Competent Authority: means any National Competent Authority (NCA) belonging to the Single Supervisory Mechanism (SSM) that has agreed to use the ESCB-PKI.

ESCB/SSM user: user that belongs to an ESCB Central Bank or to a SSM National Competent Authority.

Electronic certificate or certificate: electronic file, issued by a certification authority, that binds a public key with a certificate subscriber's identity and is used for the following: to verify that a public key belongs to a certificate subscriber; to authenticate a certificate subscriber; to check a certificate's subscriber signature; to encrypt a message addressed to a certificate subscriber; or to verify a certificate subscriber's access rights to ESCB/SSM electronic applications, systems, platforms and services. Certificates are held on data carrier devices, and references to certificates include such devices.

Public key and private key: the asymmetric cryptography on which the PKI is based employs a key pair in which what is enciphered with one key of this pair can only be deciphered by the other, and vice versa. One of these keys is "public" and is included in the electronic certificate, whilst the other is "private" and is only known by the certificate subscriber and, when appropriate, by the Keys Archive (KA).

Session key: a key established to encipher communication between two entities. The key is established specifically for each communication, or session, and its utility expires upon termination of the session.

Key agreement: a process used by two or more technical components to agree on a session key in order to protect a communication.

Directory: a data repository that is usually accessed through the LDAP protocol.

User identifier: a set of characters that are used to uniquely identify the user of a system.

Public Key Infrastructure: the set of individuals, policies, procedures, and computer systems necessary to provide authentication, encryption, integrity and non-repudiation services, by way of public and private key cryptography and electronic certificates.

ESCB-PKI Certification Authority: means the entity, trusted by users, to issue, manage, revoke and renew certificates in accordance with the ESCB certificate acceptance framework.

Trust hierarchy: the set of Certification Authorities that maintain a relationship of trust by which a CA of a higher level guarantees the trustworthiness of one or several lower level CAs. In the case of ESCB-PKI, the hierarchy has two levels: the Root CA at the top level guarantees the trustworthiness of its subordinate CAs, one of which is the Online CA.

Certification Service Provider (CSP): entity or a legal person who issues certificates or provides other services related to electronic signatures.

Registration Authority: means an entity trusted by the users of the certification services which verifies the identity of individuals applying for a certificate before the issuance of the certificate by the ESCB-PKI Certification Authority.

Certificate applicants: the individuals who request the issuance of certificates.

Certificate subscribers: the individuals for which an electronic certificate is issued and by whom it is accepted.

Relying parties: individuals or entities, other than certificate subscribers, that decide to accept and rely on a certificate issued by ESCB-PKI.

Providing Central Bank or **service provider:** means the NCB appointed by the Governing Council to develop the ESCB-PKI and to issue, manage, revoke and renew electronic certificates on behalf and for the benefit of the Eurosystem central banks.

Repository: a part of the content of the ESCB-PKI website where relying parties, certificate subscribers and the general public can obtain copies of ESCB-PKI documents, including but not limited to this CP and CRLs.

Secure e-mail gateway: computer system that improves the security of electronic mail systems by adding digital signature and encryption to the message content.

Shared mailbox: an electronic mailbox that can be accessed by multiple users. Technically it is equivalent to a personal mailbox but instead of identifying a specific individual it is linked to a business task (e.g. HR secretary)

Validation Authority: means an entity trusted by the users of the certification services which provides information about the revocation status of the certificates issued by the ESCB-PKI Certification Authority.

1.6.2 Acronyms

C: (Country). Distinguished Name (DN) attribute of an object within the X.500 directory structure

CA: Certification Authority

CAF: Certificate Acceptance Framework

CB: Central Bank that uses the ESCB-PKI

CDP: CRL Distribution Point

CEN: Comité Européen de Normalisation

CN: Common Name Distinguished Name (DN) attribute of an object within the X.500 directory structure.

CP: Certificate Policy

CPS: Certification Practice Statement

CRL: Certificate Revocation List

CSP: Certification Service Provider

CSR: Certificate Signing Request: set of data that contains the public key and its electronic signature using the companion private key, sent to the CA for the issue of an electronic signature that contains said public key

CWA: CEN Workshop Agreement

DN: Distinguished Name: unique identification of an entry within the X.500 directory structure

ECB: European Central Bank

ESCB: European System of Central Banks

ESCB-PKI: European System of Central Banks Public Key Infrastructure: means the public key infrastructure developed by the providing central bank on behalf of and for the benefit of the Eurosystem Central Banks which issues, manages, revokes and renews certificates in accordance with the ESCB certificate acceptance framework - as amended from time to time including in relation to SSM -

ETSI: European Telecommunications Standard Institute

FIPS: Federal Information Processing Standard

HSM: Hardware Security Module: cryptographic security module used to store keys and carry out secure cryptographic operations

IAM: Identity and Access Management

IETF: Internet Engineering Task Force (internet standardisation organisation)

ITC: Information Technology Committee

LDAP: Lightweight Directory Access Protocol

NCA: National Competent Authority

NCB: National Central Bank

O: Organisation. Distinguished Name (DN) attribute of an object within the X.500 directory structure

OCSP: Online Certificate Status Protocol: this protocol enables online verification of the validity of an electronic certificate

OID: Object Identifier

OU: Organisational Unit. Distinguished Name (DN) attribute of an object within the X.500 directory structure

PAA: Policy Approval Authority

PIN: Personal Identification Number: password that protects access to a cryptographic card

PKCS: Public Key Cryptography Standards: internationally accepted PKI standards developed by RSA Laboratories

PKI: Public Key Infrastructure

PKIX: Work group within the IETF (Internet Engineering Task Group) set up for the purpose of developing PKI and internet specifications

PUK: PIN UnlocK Code: password used to unblock a cryptographic card that has been blocked after repeatedly and consecutively entering the wrong PIN

RA: Registration Authority

RO: Registration Officer

RFC: Request For Comments (Standard issued by the IETF)

SMA: Shared Mailbox Administrator

SSCD: Secure Signature Creation Device

SSM: Single Supervisory Mechanism

T&C: Terms and conditions application form

UID: User identifier

VA: Validation Authority

2 Publication and Repository Responsibilities

2.1 Repositories

As specified in the ESCB-PKI CPS.

2.2 Publication of Certification Data, CPS and CP

As specified in the ESCB-PKI CPS.

Moreover, a copy of the ESCB/SSM users' certificates is published in the directory of the ESCB Identity and Access Management (IAM) service.

2.3 Publication Timescale or Frequency

As specified in the ESCB-PKI CPS.

2.4 Repository Access Controls

As specified in the ESCB-PKI CPS.

3 Identification and Authentication (I&A)

3.1 Naming

3.1.1 Types of names

The certificates issued by ESCB-PKI contain the Distinguished Name (or DN) X.500 of the issuer and that of the certificate subject in the fields *issuer name* and *subject name*, respectively. The CN (Common Name) attribute of the DN contains a prefix that identifies the certificate usage, and the following are accepted:

- [AUT:S] → Standard Authentication certificate
- [AUT:A] → Advanced Authentication certificate
- [SIG:A] → Advanced Signature certificate based on a token without SSCD certification
- [SIG:Q] → Advanced Signature certificate based on a token with SSCD certification
- [ENC:A] → Advanced Encryption certificate without private key archive
- [ENC:K] → Advanced Encryption certificate with private key archive only recoverable in a token
- [ENC:S] → Encryption certificate with private key archive recoverable in software
- [MOB:S] → Mobile Device certificate
- [EGW:S] → Secure E-mail Gateway certificate
- [TMP:A] → Provisional certificate
- [ADM:A] → Administrator certificate
- [SHM:S] → Shared mailbox certificate

This prefix will be followed by the name, middle name and surnames of the certificate subscribers but in the case of shared mailbox certificates where it will be followed by the shared mailbox's display name.

Additionally, the following field is used:

- PS (OID: 2.5.4.65)= <User identifier at ESCB/SSM level>

The rest of the DN attributes shall have the following fixed values:

- C [Country where the Registration Authority is located]
- O EUROPEAN SYSTEM OF CENTRAL BANKS
- OU Central Bank or National Competent Authority to which the certificate subscriber belongs to

3.1.2 The need for names to be meaningful

In all cases the distinguished names of the certificates are meaningful because they are subject to the rules established in the previous point in this respect.

3.1.3 Rules for interpreting various name formats

As specified in the ESCB-PKI CPS.

3.1.4 Uniqueness of names

The whole made up of the combination of the distinguished name plus the KeyUsage extension content must be unique and unambiguous to ensure that certificates issued for two different certificate subscribers will have different distinguished names.

Certificate DNs must not be repeated. The use of the user identifier at ESCB/SSM level guarantees the uniqueness of the DN.

3.1.5 Name dispute resolution procedures

As specified in the ESCB-PKI CPS.

3.1.6 Recognition, authentication, and the role of trademarks

As specified in the ESCB-PKI CPS.

3.2 Initial Identity Validation

3.2.1 Means of proof of possession of the private key

Depending on the specific certificate type, the means of proof of private key possession will be different:

- [AUT:S] → standard authentication certificate: the key pair will be created by the ESCB-PKI Online CA, so this section does not apply.
- [AUT:A] → advanced authentication certificate: the key pair will be created by the subject in the private zone into his cryptographic token and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [SIG:A] → advanced signature certificate (no SSCD token): the key pair will be created by the subject in the private zone into his cryptographic token and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [SIG:Q] → advanced Signature certificate based on a SSCD token: the key pair will be created by the subject in the SSCD zone of a secure signature creation device and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [ENC:A] → advanced encryption without key archive: the key pair will be created by the subject in the private zone into his secure signature creation device and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [ENC:K] → advanced encryption with key archive: Advanced Encryption certificate key pair will be created by the ESCB-PKI Online CA so this section does not apply.
- [ENC:S] → encryption with key archive recoverable in software: the key pair will be created by the ESCB-PKI Online CA so this section does not apply.
- [MOB:S] → mobile device certificate: the key pair will be created by the ESCB-PKI Online CA so this section does not apply.
- [EGW:S] → secure e-mail gateway: the key pair will be created by the ESCB-PKI Online CA so this section does not apply.
- [TMP:A] → provisional certificate: the key pair will be created by the subject in the private zone into his secure signature creation device and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [ADM:A] → administrator certificate: the key pair will be created by the subject in the private zone into his secure signature creation device and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [SHM:S] → shared mailbox certificate: the key pair will be created by the ESCB-PKI Online CA so this section does not apply.

3.2.2 Identity authentication for an entity

This CP does not consider the issuance of certificates for entities.

3.2.3 Identity authentication for an individual

Evidence of the subject's identity is checked against a physical person.

Validation of the individual

The certificate applicant shall provide evidences of, at least, the following information:

- Full name, and
- Date and place of birth, or reference to a nationally recognized identity document, or other attributes which may be used to distinguish the person from others with the same name.

To validate the previous information the certificate applicant must present a document as proof of identity. The acceptable documents are:

- Passport, or
- National Identity Card, or
- Any other legal document accepted by the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority to dully identify an individual.

If the case of shared mailbox certificates the certificate applicant will be the person responsible for the shared mailbox.

If the certificate applicant has already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the employee identification card is accepted as sufficient to identify the certificate applicant.

The validation of the identity will be performed by a Registration Officer or by a Trusted Agent.

Validation of the organisation

To prove his relation with the CB the certificate applicant must present his employee identification card.

3.2.4 Non-verified applicant information

All the information stated in the previous section must be verified.

3.2.5 Validation of authority

As specified in the ESCB-PKI CPS.

3.2.6 Criteria for operating with external CAs

As specified in the ESCB-PKI CPS.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication requirements for routine re-key

The same process as for initial identity validation is used.

3.3.2 Identification and authentication requirements for re-key after certificate revocation

The same process as for initial identity validation is used.

4 Certificate Life-Cycle Operational Requirements

This chapter contains the operational requirements for the life cycle of ESCB/SSM users's certificates issued by the ESCB-PKI CA. Despite the fact that these certificates might be stored on cryptographic tokens, it is not the purpose of the CP to regulate the management of said tokens and, therefore, it is also assumed that the certificate applicants have previously obtained their cryptographic tokens.

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Certificates for ESCB/SSM users will be managed by a Registration Officer (RO). ROs will be able to request certificate types mentioned in section 1.3.6.

In case of shared mailbox certificates the attributes required to identify the shared mailbox will be entered by a Shared Mailbox Administrator (SMA).

Application for a certificate does not mean it will be obtained if the applicant does not fulfil the requirements established in the CPS or in this CP for ESCB/SSM users' certificates (e.g. if the certificate applicant does not provide the RO with the documents necessary for his/her identification)

4.1.2 Enrolment process and applicants' responsibilities

Advanced certificate package (cryptographic token-based)

This process is carried out to obtain a certificate package consisting on three certificates: authentication, encryption and signature certificates. The certificate package will be stored in a cryptographic token. The procedure is the same independently on the type of token (with or without SSCD certification) to be used.

The procedure is as follows:

1. Cryptographic token-based certificate requests for an ESCB/SSM user can be initiated:
    a. either using ESCB Identity Access Management (IAM) interfaces,
    b. or using ESCB-PKI web interface;
2. The certificate applicant must explicitly accept the terms and conditions of the application form (T&C) by his/her hand-written signature of the term and conditions. The T&C will incorporate the following data:
    a. the attributes to be included in the certificate: first name, middle name (if any), surname, name of the central bank or national competent authority, user identifier and e-mail address;
    b. the attributes required to distinguish the person from others with the same name (see Section 3.2.3), namely, the number of a national recognized identity document according to the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority, or the date and place of birth, or, if the certificate applicant has already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the number of the employee identification card or the employee number if this is printed on the employee identification card;

c. the serial number of the certificate applicant's cryptographic token.

3. In the case that a Trusted Agent is in charge of identifying and authenticating the certificate applicant, he/she will add his hand-written signature to the T&C;
4. The RO must validate the information included in the certificate request against the documentation provided by the certificate applicant (see Section 3.2.3) including the T&C. In the case that the certificate applicant is not in front of him/her, the RO will also validate that a valid Trusted Agent has signed the T&C;
5. The RO, using the ESCB-PKI web interface, will either:
    a. Start the issuance of the certificates
    b. Approve a remote download

   In both cases the certificate applicant must hold his/her cryptographic token and, when requested, must insert it and type his/her personal PIN to generate the keys and store the certificates
6. The RO must securely archive all the following documentation during the retention period described in Section 5.5.2 of this CP:
    a. the terms and conditions application form signed by both, the certificate applicant and the person who identified and authenticated him/her (i.e. the Trusted Agent or the RO himself/herself)
    b. if the certificate applicant has not already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, a copy of the identification document used to validate the certificate applicant's identity or, if this were not legally feasible, a copy of other identification document, preferable with the certificate applicant's photography, under the conditions and limitations of the applicable law

Standard certificates (software-based)

This process is carried out to obtain a single certificate valid for authentication that will be stored in a software keystore (i.e. a password protected file).

The procedure is as follows:

1. Software-based certificate requests for a ESCB/SSM user can be initiated:
    a. either using ESCB Identity Access Management (IAM) interfaces,
    b. or using ESCB-PKI web interface;
2. The certificate applicant must explicitly accept the terms and conditions of the application form (T&C) by his/her hand-written signature of the term and conditions. The T&C will incorporate the following data:
    a. the attributes to be included in the certificate: first name, middle name (if any), surname, name of the central bank or national competent authority, user identifier and e-mail address;
    b. the attributes required to distinguish the person from others with the same name (see Section 3.2.3), namely, the number of a national recognized identity document according to the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority, or the date and place of birth, or, if the certificate applicant has already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the number

of the employee identification card or the employee number if this is printed on the employee identification card.

3. In the case that a Trusted Agent is in charge of identifying and authenticating the certificate applicant, he will add his/her hand-written signature to the T&C;
4. The RO must validate the information included in the certificate request against the documentation provided by the certificate applicant (see Section 3.2.3) including the T&C. In the case that the certificate applicant is not in front of him/her, the RO will also validate that a valid Trusted Agent has signed the T&C;
5. The RO, using the ESCB-PKI web interface, will either:
    a. Start the issuance of the certificate.
    b. Approve a remote download

   In both cases the certificate applicant will be requested to type a password to protect the keystore (file) to be generated with the certificate and its corresponding private key;
6. The RO must securely archive all the following documentation during the retention period described in Section 5.5.2 of this CP:
    a. the terms and conditions application form signed by both, the certificate applicant and the person who identified and authenticated him/her (i.e. the Trusted Agent or the RO himself/herself)
    b. if the certificate applicant has not already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, a copy of the identification document used to validate the certificate applicant's identity or, if this were not legally feasible, a copy of other identification document, preferable with the certificate applicant's photography, under the conditions and limitations of the applicable law

Mobile device certificates (software-based)

The same applies as in case of standard certificates.

Secure e-mail gateway certificates (software-based)

The same applies as in the case of standard certificates.

Administrator certificates (token-based)

The process will be similar to the process for advanced certificates. The only difference is that only one certificate, valid for authentication and signature, will be generated instead of three certificates.

Provisional certificates (token-based)

This process is carried out to obtain a certificate stored in a cryptographic token. This certificate will be only used in case that the subscriber of an advanced certificate package or an administrator certificate has forgotten his token. The provisional certificate lifetime will be less or equal to 31 days.

The procedure is as follows:

1. Only requests for provisional certificates coming from users that have already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity and that are subscribers of advanced (token-based) or administrator certificates will be accepted;
2. Provisional certificate requests for a ESCB/SSM user can be initiated:

   a. either using ESCB Identity Access Management (IAM) interfaces,
   b. or using ESCB-PKI web interface;
3. The certificate applicant must explicitly accept the terms and conditions of the application form (T&C) by hand-written signature of the T&C. The T&C will incorporate the following data:
   a. the attributes to be included in the certificate: first name, middle name (if any), surname, name of the central bank or national competent authority, user identifier and e-mail address;
   b. the attributes required to distinguish the person from others with the same name (see Section 3.2.3), namely, the number of a national recognized identity document according to the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority, or the date and place of birth, or, if the certificate applicant has already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the number of the employee identification card or the employee number if this is printed on the employee identification card;
   c. the serial number of the provisional cryptographic token where the subscriber will download the provisional certificate;
4. In the case that a Trusted Agent is in charge of identifying and authenticating the certificate applicant, he/she will also sign the T&C;
5. The RO must validate the information included in the certificate request against the documentation provided by the certificate applicant (see Section 3.2.3) including the T&C. Alternatively, in order to deal with the situation in which the user has not got any identification document (e.g. he has forgotten his wallet) the RO will be allowed to identify the user by means of a local directory with photograph;

   In the case that the certificate applicant is not in front of him/her, the RO will also validate that a valid Trusted Agent has signed the T&C. In this case, in order to expedite the process, the Trusted Agent will be allowed to anticipate a scanned copy of the T&C document by fax or e-mail so that the RO can process the request as soon as possible. In any case, the original copy of the T&C document has to be sent to the RO for archival;
6. The RO, using the ESCB-PKI web interface, will decide how long the certificate will be valid (less or equal than 31 days). Afterwards he will either:
   a. Start the issuance of the certificate
   b. Approve a remote download

   In both cases the certificate applicant must hold his/her cryptographic token and, when requested, must insert it and type his/her personal PIN to generate the keys and store the certificate;
7. The RO must securely archive all the following documentation during the retention period described in Section 5.5.2 of this CP:
   a. the terms and conditions application form signed by both, the certificate applicant and the person who identified and authenticated him/her (i.e. the Trusted Agent or the RO himself/herself)

Shared mailbox certificates (software-based)

This process is carried out to obtain a certificate for a mailbox shared by several users. In this case there must be a physical person responsible for the certificate and carrying out the role of the applicant.

The procedure is as follows:

1. Shared mailbox certificate requests for a ESCB/SSM user can be initiated:
    a. either using ESCB Identity Access Management (IAM) interfaces,
    b. or using ESCB-PKI web interface;
2. A Shared Mailbox Administrator (SMA) will participate in the process to enter or complement the attributes of the shared mailbox or the person that is acting as the certificate subscriber;
3. The certificate applicant must explicitly accept the terms and conditions of the application form (T&C) by hand-written signature of the T&C. The T&C will incorporate the following data:
    a. the shared mailbox attributes to be included in the certificate: display name, name of the central bank or national competent authority, user identifier and e-mail address;
    b. the attributes to identify the certificate subscriber, that will not be included in the certificate: first name, middle name (if any), surname, e-mail address and the attributes required to distinguish the person from others with the same name (see Section 3.2.3), namely, the number of a national recognized identity document according to the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority, or the date and place of birth, or, if the certificate applicant has already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the number of the employee identification card or the employee number if this is printed on the employee identification card.
4. In the case that a Trusted Agent is in charge of identifying and authenticating the certificate applicant, he/she will also sign the T&C;
5. The RO must validate the information included in the certificate request against the documentation provided by the certificate applicant (see Section 3.2.3) including the T&C. In the case that the certificate applicant is not in front of him/her, the RO will also validate that a valid Trusted Agent has signed the T&C;
6. The RO, using the ESCB-PKI web interface, will approve the certificate download;
7. The SMA, using the ESCB-PKI web interface, will download the certificate. For this, it will be required to type a password to protect the keystore (file) that will be generated with the certificate and its corresponding private key;
8. The SMA will deliver the certificate file to the certificate subscriber by means of local procedures (e.g. by means of a USB stick);
9. The RO must securely archive all the following documentation during the retention period described in Section 5.5.2 of this CP:
    a. the terms and conditions application form signed by both, the certificate applicant and the person who identified and authenticated him/her (i.e. the Trusted Agent or the RO himself/herself)
    b. if the certificate applicant has not already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, a copy of the identification document used to validate the certificate applicant's identity or, if this were not legally feasible, a copy of other identification document, preferable with the certificate applicant's photography, under the conditions and limitations of the applicable law

4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

The validation of certificate requests will require face-to-face authentication of the certificate applicant or using means which provide equivalent assurance to physical presence.

A Registration Officer or a Trusted Agent will perform the certificate applicant's identification and authentication and will ensure that all the information provided is correct at the time of registration. The identification and authentication process will be done as specified in section 3.2.3 of this CP.

4.2.2 Approval or rejection of certificate applications

As specified in the ESCB-PKI CPS.

4.2.3 Time limit for processing the certificate applications

The Certification Authority shall not be held liable for any delays that may arise in the period between application for the certificate, publication in the ESCB-PKI repository and its delivery. As far as possible, the Certification Authority will process requests within 24 hours.

4.3 Certificate Issuance

4.3.1 Actions performed by the CA during the issuance of the certificate

As specified in the ESCB-PKI CPS.

4.3.2 CA notification to the applicants of certificate issuance

Applicants will be advised of the availability of the certificates via e-mail.

4.4 Certificate Acceptance

4.4.1 Form of certificate acceptance

Certificate applicants must confirm acceptance of the ESCB/SSM users' certificates and of its conditions by way of a hand-written signature of the terms and conditions application form.

4.4.2 Publication of the certificate by the CA

The ESCB-PKI CA publishes a copy of the ESCB/SSM user's certificates: i) in an internal LDAP directory located at the service provider's premises, only available to ESCB/SSM systems on a need-to-know basis, and ii) in the directory of the ESCB Identity and Access Management (IAM) service.

4.4.3 Notification of certificate issuance by the CA to other Authorities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Certificate subscribers' use of the private key and certificate

The certificates regulated by this CP may be used only to provide the following security services:

- Authentication certificates: authentication of the subscriber.
- Encryption certificates: encryption of email messages and files.
- Signature certificates: digital signature of transactions, email messages and files.

4.5.2 Relying parties' use of the public key and the certificate

As specified in ESCB-PKI CPS.

4.6 Certificate Renewal

As specified in ESCB-PKI CPS.

4.7 Certificate Re-key

4.7.1 Circumstances for certificate renewal with key changeover

As specified in ESCB-PKI CPS.

Provisional certificates cannot be renewed. Every time that a user requires a provisional certificate a new one will be generated.

4.7.2 Who may request certificate renewal?

Renewals must be requested by certificate subscribers.

4.7.3 Procedures for processing certificate renewal requests with key changeover

During the renewal process, the RO will check that the information used to verify the identity and attributes of the certificate subscriber is still valid. If any of the certificate subscriber's data have changed, they must be verified and registered with the agreement of the certificate subscriber.

If any of the conditions established in this CP have changed, the certificate subscriber must be made aware of this and agree to it.

In any case, certificate renewal is subject to:

- Renewal must be requested in person at the places of registration, as established for initial issuance, as established in 4.1.2.
- Renewal of certificates may only be requested within the last 100 days of its lifetime.
- The CA not having knowledge of the existence of any cause for the revocation / suspension of the certificate.
- The request for the renewal of the provision of services being for the same type of certificate as the one initially issued.

4.7.4 Notification of the new certificate issuance to the certificate subscriber

They are notified by e-mail.

4.7.5 Manner of acceptance of certificates with changed keys

As in the initial certificate issuance, they must sign the terms and conditions application form as a manner of acceptance of the certificates.

4.7.6 Publication of certificates with the new keys by the CA

The ESCB-PKI CA publishes a copy of the ESCB/SSM user's certificates: i) in an internal LDAP directory located at the service provider's premises, only available to ESCB/SSM systems on a need-to-know basis, and ii) in the directory of the ESCB Identity and Access Management (IAM) service.

4.7.7 Notification of certificate issuance by the CA to other Authorities

As specified in the ESCB-PKI CPS.

4.8 Certificate Modification

4.8.1 Circumstances for certificate modification

As specified in ESCB-PKI CPS.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

As specified in ESCB-PKI CPS.
Additionally, revoked ESCB/SSM users' certificates will be eliminated from the directories in which they are published.

4.9.2 Who can request revocation?

The CA or any of the RAs may, at their own initiative, request the revocation of a certificate if they become aware or suspect that the certificate subscriber's private key has been compromised, or in the event of any other factor that recommends taking such action.
Likewise, certificate subscribers may also request revocation of their certificates, which they must do in accordance with the conditions established under point 4.9.3.
The identification policy for revocation requests will be the same as that of the initial registration.

4.9.3 Procedures for requesting certificate revocation

The certificate subscribers or individuals requesting the revocation must appear before the RO, identifying themselves and indicating the reason for the request.
The RO shall always process the revocation requests submitted by its assigned certificate subscribers. The request is made via an authenticated web Interface.
Apart from this ordinary procedure, PKI System registration officers may immediately revoke any certificate upon becoming aware of the existence of any of the causes for revocation.

4.9.4 Revocation request grace period

As specified in ESCB-PKI CPS.

4.9.5 Time limit for the CA to process the revocation request

Requests for revocation of certificates must be processed as quickly as possible, and in no case may said processing take more than 1 hour.

4.9.6 Requirements for revocation verification by relying parties

Verification of revocations, whether by directly consulting the CRL or using the OCSP protocol, is mandatory for each use of the certificates by relying parties.

Relying parties must check the validity of the CRL prior to each use and download the new CRL from the ESCB-PKI repository when the one they hold expires. CRLs stored in cache[7] memory, even when not expired, do not guarantee availability of updated revocation data.

For ESCB/SSM users' certificates, the ordinary validity verification procedure for a certificate shall be carried out with the ESCB-PKI Validation Authority, which shall indicate, through the OCSP protocol, the status of the certificate.

4.9.7 CRL issuance frequency

As specified in ESCB-PKI CPS.

4.9.8 Maximum latency between the generation of CRLs and their publication

The maximum time allowed between generation of the CRLs and their publication in the repository is 1 hour.

4.9.9 Online certificate revocation status checking availability

As specified in ESCB-PKI CPS.

4.9.10 Online revocation checking requirements

As specified in ESCB-PKI CPS.

4.9.11 Other forms of revocation alerts available

No stipulation.

4.9.12 Special requirements for the revocation of compromised keys

As specified in ESCB-PKI CPS.

4.9.13 Causes for suspension

Certificate suspension is the action that renders a certificate invalid for a period of time prior to its expiry date. Certificate suspension produces the discontinuance of the certificate's validity for a limited period of time, rendering it inoperative as regards its inherent uses and, therefore, discontinuance of the provision of certification services. Suspension of a certificate prevents its legitimate use by the certificate subscriber.

Suspension of a certificate entails its publication on the public-access Certificate Revocation Lists (CRL).

The main effect of suspension as regards the certificate is that certificates become invalid until they are again reactivated. Suspension shall not affect the underlying obligations created or notified by this CP, nor shall its effects be retroactive.

ESCB/SSM users' certificates may be suspended due to:

- Certificate subscriber's request, under suspicion of key compromise.

[7]Cache memory: memory that stores the necessary data for the system to operate faster, as it does not have to obtain this data from the source for every operation. Its use could entail the risk of operating with outdated data.

4.9.14 Who can request the suspension?

The subscribers of ESCB/SSM users' certificates and Registration Officers

4.9.15 Procedure for requesting certificate suspension

Certificate subscribers may immediately suspend his certificates via an authenticated Web Interface. Access will be granted by means of one of the following mechanisms:

- an authentication certificate;
- an user ID and password for the ESCB Identity and Access Management (IAM) system;
- a suspension code (secret shared with the ESCB-PKI system)

4.9.16 Suspension period limits

The CA shall ensure that a certificate is not kept suspended for longer than is necessary to confirm its status.

Revocation will be processed immediately after receiving the certificate subscriber confirmation for revocation (see 4.9).

4.10 Certificate Status Services

As specified in ESCB-PKI CPS.

4.11 End of Subscription

As specified in ESCB-PKI CPS.

4.12 Key Escrow and Recovery

4.12.1 Key Archive and recovery practices and policies

The Key Recovery service for ESCB-PKI encryption certificates (and the associated private key) will be available only to those CBs that demand this service. For these CBs, the CA will send a copy of any user encryption key pair to the Key Archive, as to allow key recovery in case of cryptographic token loss or replacement.

4.12.1.1 Key recovery with the participation of the certificate subscriber

Certificate subscribers will be able to download a copy of the key encryption pair contained in previous cryptographic tokens.

The procedure will be the following:

- The certificate subscriber accesses a Web interface using his authentication certificate;
- The certificate subscriber downloads and installs the encryption his pair in the cryptographic token. In case that the encryption certificate is enabled for recovery in software format (name starting with [ENC:S]), the certificate subscriber will able to chose between installing the recovered keys in a cryptographic token, or downloading a software keystore protected with a password previously entered by the subscriber.

4.12.1.2 Key recovery without the participation of the certificate subscriber

Key Recovery Officers (KROs) participate during the recovery of encryption key pairs from the Key Archive when the owner of the key pair is not available. There shall be at least two KROs at each CB as to carry away the process of "Key recovery without the participation of the certificate subscriber". The KROs shall assume one or more of the following interim roles (see incompatibility matrix) for every key recovery operation:

- The Requestor KRO will request the key recovery of an encryption key pair that belongs to a particular certificate subscriber from that CB (i.e. he will trigger "Key recovery without the participation of the certificate subscriber" process).
- The Approver KROs are in charge of endorsing the recovery Request placed by the Requestor KRO.
- The Operator KRO recovers the key pair and stores it in a blank cryptographic token.

Key recovery process

Recovery of encryption certificates requested by someone else than the certificate subscriber will involve the participation of, at least, K different Key Recovery Officers of the total N KROs available at the certificate subscriber's CB.

The precise values for K and N will be determined individually at each CB. Four-eye principle will always be complied with, i.e. K will always be equal or greater than 2.

The procedure will be the following:

- One of the N KROs available at the CB, acting as a Requestor KRO, requests the key recovery of an encryption key pair that belongs to a particular certificate subscriber from that CB;
- The ESCB-PKI randomly generates a password and uses it to encrypt the key pair;
- A secret-sharing scheme is applied for the password: it is split into N pieces in such a way that any K pieces are required to reconstruct the password;
- The certificate subscriber receives an informative e-mail;
- All the N KROs from the CB receive an e-mail with one of the N pieces of the shared secret. It is required the participation of at least K KROs to get access to the encryption certificate. These K KROs will act as Approver KROs;
- One of the N KROs, acting as the Operator KRO (cannot be the same that the Requestor KRO) accesses a Web interface available through CoreNet;
- The Operator KRO introduces his/her piece of the shared secret and other K-1 Approver KROs introduce theirs;
- The Operator KRO recovers the key pair and stores it in a blank cryptographic token.

4.12.2 Session key protection and recovery policies and practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

As specified in the ESCB-PKI CPS.

5.2 Procedural Controls

As specified in the ESCB-PKI CPS.

5.3 Personnel Controls

As specified in the ESCB-PKI CPS.

5.4 Audit Logging Procedures

As specified in the ESCB-PKI CPS.

5.5 Records Archival

5.5.1 Types of records archived

As specified in the ESCB-PKI CPS.

5.5.2 Archive retention period

The retention period for records related to ESCB/SSM users' certificates is 15 years, which is the legally mandated period according to the Spanish legislation.

5.5.3 Archive protection

As specified in the ESCB-PKI CPS.

5.5.4 Archive backup procedures

As specified in the ESCB-PKI CPS.

5.5.5 Requirements for time-stamping records

As specified in the ESCB-PKI CPS.

5.5.6 Audit data archive system (internal vs. external)

As specified in the ESCB-PKI CPS.

5.5.7 Procedures to obtain and verify archived information

As specified in the ESCB-PKI CPS.

5.6 Key Changeover

As specified in the ESCB-PKI CPS.

5.7 Compromise and Disaster Recovery

As specified in the ESCB-PKI CPS.

5.8 CA or RA Termination

As specified in the ESCB-PKI CPS.

6 Technical Security Controls

Technical security controls for internal ESCB-PKI components, and specifically those controls for Root CA and Online CA, during certificate issue and certificate signature processes, are described in the ESCB-PKI CPS.
In this paragraph technical security controls for the issuance of certificates under this CP are covered.

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Keys for ESCB/SSM users' certificates issued by the Online CA are generated under the following circumstances, depending on the certificate type:

- **Advanced certificate package**, where all the following certificates will be stored in a smartcard or other cryptographic token:
  - Advanced authentication certificate. The corresponding key pair will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent.
  - Advanced signature certificate. The corresponding private key will be generated inside the cryptographic token pursuant to the FIPS 140-2 level 3 or CC EAL4+ specification or equivalent.
  - Advanced signature certificate based on a SSCD. The corresponding private key will be generated inside the cryptographic token pursuant to the FIPS 140-2 level 3 or CC EAL4+ specification or equivalent and to the SSCD (CWA 14169) specification.
  - Advanced encryption certificate without key archive. The key pair will be generated inside the cryptographic token pursuant to the FIPS 140-2 level 3 or CC EAL4+ specification or equivalent, and no other copy will be archived.
  - Advanced encryption certificate with key archive recoverable only in a token. The key pair will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification. Once generated, the key pair will be stored in the Key Archive service that will use a cryptographic module with the same requirements, and another copy will be stored in the cryptographic token pursuant to the CC EAL 4+ specification or equivalent.
  - Standard encryption certificate with key archive recoverable in software format or in a token. The key pair will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification. Once generated, the key pair will be stored in the Key Archive service that will use a cryptographic module with the same requirements, and another copy will be stored in the cryptographic token pursuant to the CC EAL 4+ specification or equivalent.
- **Standard certificates**, where the private key will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification.
- **Mobile devices certificates**, where the private key will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification.
- **Secure e-mail gateway certificates**, where the private key will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification.

- **Administrator certificates**, where the corresponding private key will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent.
- **Provisional certificates**, where the corresponding private key will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent.
- **Shared mailbox certificates**, where the private key will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification.

6.1.2 Delivery of private keys to certificate subscribers

6.1.2.1 Advanced certificate package

With the exception of the advanced encryption certificates with key archive and the encryption certificates with archived keys recoverable in software format, the private keys will be generated directly by the certificate subscribers in their secure token and, therefore, no delivery is required.

Delivery of the private key for advanced encryption certificates with key archive:

- As mentioned in section 6.1.1, the private keys are generated by the Online CA in a file pursuant to the PKCS#12 specification.
- The PKCS#12 file will be delivered to:
  a) The certificate subscriber, in the case of:
     - The habitual certificate package delivery process, next to the authentication and signature certificates. The RA application will force to download the PKCS#12 file in a cryptographic token.
     - In case that the certificate subscriber requires to retrieve a copy of the encryption key pair from the KA (e.g. in case of substitution of the cryptographic token). The certificate subscriber will use a specific authenticated web interface that will force to download the PKCS#12 file in a cryptographic token.
  b) The required number of Key Recovery Officers nominated by the CB. This will be case when the certificate subscriber is not available. Four-eye principle will be required to recover a key pair in this case. KROs will use a specific authenticated web interface that will force to download the PKCS#12 file in a cryptographic token.
- To guarantee delivery security, the availability of the generation and subsequent downloading of the certificate shall be notified by e-mail to the certificate subscriber.

Delivery of the private key for encryption certificates with archived keys recoverable in software format:

- As mentioned in section 6.1.1, the private keys are generated by the Online CA in a file pursuant to the PKCS#12 specification.
- The PKCS#12 file will be delivered to:
  a) The certificate subscriber, in the case of:
     - The habitual certificate package delivery process, next to the authentication and signature certificates. The RA application will force to download the PKCS#12 file in a cryptographic token.
     - In case that the certificate subscriber requires to retrieve a copy of the encryption key pair from the KA (e.g. in case of substitution of the cryptographic token). The certificate subscriber will use a specific

authenticated web interface that will allow downloading the PKCS#12 file in a software keystore procted with a password selected by the subscriber, or in a cryptographic token.

b) The required number of Key Recovery Officers nominated by the CB. This will be case when the certificate subscriber is not available. Four-eye principle will be required to recover a key pair in this case. KROs will use a specific authenticated web interface that will force to download the PKCS#12 file in a cryptographic token.

To guarantee delivery security, the availability of the generation and subsequent downloading of the certificate shall be notified by e-mail to the certificate subscriber.

6.1.2.2 Standard certificates

For standard certificates, the delivery of the private key to the certificate subscriber will be performed by means of an authenticated web interface. The certificate subscriber will receive the key pair in a file pursuant to the PKCS#12 specification protected with a password selected by him/her.

6.1.2.3 Mobile device certificates

For mobile device certificates, the delivery of the private key to the certificate subscriber will be performed by means of an authenticated web interface. The certificate subscriber will receive the key pair in a file pursuant to the PKCS#12 specification protected with a password selected by him/her.

6.1.2.4 Secure e-mail gateway certificates

For secure e-mail gateway certificates, the delivery of the private key to the certificate subscriber will be performed by means of an authenticated web interface. The certificate subscriber will receive the key pair in a file pursuant to the PKCS#12 specification protected with a password selected by him/her.

6.1.2.5 Administrator certificates

For administrator certificates, the private keys will be generated directly by the certificate subscribers in their secure token and, therefore, no delivery is required.

6.1.2.6 Provisional certificates

For provisional certificates, the private keys will be generated directly by the certificate subscribers in their secure token and, therefore, no delivery is required.

6.1.2.7 Shared mailbox certificates

For shared mailbox certificates, the delivery of the private key to the shared mailbox administrator will be performed by means of an authenticated web interface. The shared mailbox administrator will receive the key pair in a file pursuant to the PKCS#12 specification protected with a password selected by him/her.

6.1.3 Delivery of the public key to the certificate issuer

In case of advanced encryption certificates with key archive and standard authentication certificates, public keys are generated by the ESCB-PKI Online CA, and therefore delivery to the certificate issuer is not applicable.

In the other cases, the public keys are generated by certificate subscribers on their cryptographic tokens and then delivered to the ESCB-PKI Online CA within the process required to obtain the certificate.

6.1.4 Delivery of the CA's public key to relying parties

The ESCB-PKI Online CA public key is included in the certificate of that CA. The ESCB-PKI Online CA certificate is not included in the certificate package generated for the certificate subscriber. The ESCB-PKI Online CA certificate must be obtained from the repository specified in this document where it is available by certificate subscribers and relying parties to carry out any type of verification.

6.1.5 Key sizes

The key size of any ESCB/SSM users' certificate is 2048 bits.

6.1.6 Public key generation parameters and quality checks

Public keys are encoded pursuant to RFC 3280 and PKCS#1. The key generation algorithm is the RSA.

6.1.7 Key usage purposes (KeyUsage field in X.509 v3)

The 'Key Usage' and 'Extended Key Usage' fields of the certificates included in this CP are described in the 7.1.2.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

The Hardware Security Module (HSM) used for the creation of keys used by ESCB-PKI Online CA is pursuant to FIPS 140-2 Level 3.
Start-up of each of the Certification Authorities, taking into account that a HSM is used, involves the following tasks:

a HSM module status boot up.
b Creation of administration and operator cards.
c Generation of the CA keys.

As regards the cryptographic token, they will be pursuant to the FIPS 140-2 level 3 or CC EAL4+ specification or equivalent. In the case of advanced signature certificates based on a SSCD, they will be also pursuant to the SSCD specification (CWA 14169).

6.2.2 Private key multi-person (k out of n) control

The private key, both for Root CA as for Subordinate CA, is under multi-person control; its activation is done through CA software initialisation by means of a combination of CA and HSM operators. This is the only activation method for said private key.
There is no multi-person control established for accessing the private keys of the certificates issued under this CP. When key archive service is requested by the CB, the recovery process will be as described in section 4.12.1

6.2.3 Escrow of private keys

Only advanced encryption certificates with key archive are escrowed. See sections 4.12.1 and 6.1.1.

6.2.4 Private key backup copy

Advanced certificates

The certificate subscribers cannot backup their certificates because the keys cannot be exported outside of the cards and these cannot be cloned. When key archive service is requested by the CB the certificate subscriber belongs to, the encryption private keys are subject to key archive as described in section *4.12.1Key Archive and recovery practices and policies.*

Standard certificates

The certificate subscribers will have to keep the PKCS#12 file and corresponding protection password as a backup copy.

6.2.5 Private key archive

Advanced certificates

The private keys of the authentication and signature certificates are generated on cryptographic cards, they are not exported under any circumstances, and access to operations with said cards is protected by a PIN code.

The private keys of the encryption certificate are stored on cryptographic cards held by their certificate subscribers, they are not exported under any circumstances, and access to operations with said cards is protected by a PIN. When key archive service is requested by the CB the certificate subscriber belongs to, the encryption private keys are subject to key archive as described in section *4.12.1Key Archive and recovery practices and policies.*

Standard certificates

ESCB-PKI will not keep any archive of the private key associated to standard certificates.

6.2.6 Private key transfer into or from a cryptographic module

Advanced certificates

Provided that the private key is generated inside the cryptographic token there is no transmission of this key to or from any cryptographic module.

Standard certificates

No stipulated

6.2.7 Private key storage in a cryptographic module

Advanced certificates

Private keys of authentication, signature and encryption certificates without key archive are created on the cryptographic token and are stored there. Private keys of encryption certificates with key archive are generated by the CA's cryptographic module and afterwards stored in the KA's cryptographic module and in cryptographic token.

Standard certificates

Private keys are created in the ESCB-PKI Online CA's cryptographic module, but they are not subsequently saved.

6.2.8 Private key activation method

Advanced certificates

Private keys are stored in a cryptographic token protected with a PIN code that is required to activate the keys.

Standard certificates

Private keys are delivered in a PKCS#12 file, protected by a password. The password is required to activate the private key.

6.2.9 Private key deactivation method

Advanced certificates

Private keys can be deactivated by removing the card from the reader.

Standard certificates

No stipulation.

6.2.10 Private key destruction method

Advanced certificates

Private keys can be destroyed by destroying the cryptographic token.

Standard certificates

No stipulation.

6.2.11 Cryptographic module classification

The cryptographic modules used by ESCB-PKI technical components comply with the FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archive

As specified in the ESCB-PKI CPS.

6.3.2 Operational period of certificates and usage periods for key pairs

All certificates and their linked key pair have a lifetime of 3 years, although the ESCB-PKI Online CA may establish a shorter period at the time of their issue.

6.4 Activation Data

As specified in the ESCB-PKI CPS.

6.5 Computer Security Controls

As specified in the ESCB-PKI CPS.

6.6 Life Cycle Security Controls

As specified in the ESCB-PKI CPS.

6.7 Network Security Controls

As specified in the ESCB-PKI CPS.

6.8 Timestamping

As specified in the ESCB-PKI CPS.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version number

Certificates for the ESCB/SSM users are compliant with the X.509 version 3 (X.509 v3) standard.

7.1.2 Certificate extensions

The certificate extensions used generically are:

- *Subject Key Identifier*. Classified as non-critical.
- *Authority Key Identifier*. Classified as non-critical.
- *KeyUsage*. Classified as critical.
- *extKeyUsage*. Classified as non-critical.
- *CertificatePolicies*. Classified as non-critical.
- *SubjectAlternativeName*. Classified as non-critical.
- *BasicConstraints*. Classified as critical.
- *CRLDistributionPoint*. Classified as non-critical.
- *Auth. Information Access*. Classified as non-critical.
- escbUseCertType *(0.4.0.127.0.10.1.3.1)*. Classified as non-critical.

For understanding purposes, all ESCB-PKI OID attributes references are made under the [OID ESCBPKI] mark, which corresponds to 0.4.0.127.0.10.1.

7.1.2.1 Advanced authentication certificate

Advanced authentication certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which user is member* *User identifier (UID)* [AUT:A] *Name Middle name Surnames*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature[8] Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 0 0 1 0 0	Yes
extKeyUsage	 clientAuth (1.3.6.1.5.5.7.3.2) smartCardLogon (1.3.6.1.4.1.311.20.2.2) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies Policy Identifier	 *[OID ESCBPKI]*.2.2.1	

[8] This usage is allowed in the scenarios where a digital signature is generated to authenticate the certificate subscriber

URL CPS	*[CPS-URL]*	
Subject Alternative Names RegisteredID UPN (1.3.6.1.4.1.311.20.2.3) rfc822 RegisteredID (*[OID ESCBPKI]*.1.1.1) RegisteredID (*[OID ESCBPKI]*.1.1.2) RegisteredID (*[OID ESCBPKI]*.1.1.3) RegisteredID (*[OID ESCBPKI]*.1.1.10) RegisteredID (*[OID ESCBPKI]*.1.1.4) RegisteredID (*[OID ESCBPKI]*.1.1.7)	 *User Principal Name (if available)* *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers Ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbUseCertType	AUTHENTICATION	

7.1.2.2 Advanced signature certificate and advanced signature certificate based on a SSCD

Advanced signature certificate and advanced signature certificate based on a SSCD		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which user is member* *User identifier (UID)* [SIG:Q] *Name Middle name Surnames* *OR* [SIG:A] *Name Middle name Surnames*[9]	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 0 1 0 0 0 0 0	Yes
extKeyUsage	 emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	

[9] *[SIG:Q]* in case of advanced signature certificates based on a SSCD
[SIG:A] in case of advanced signature certificates

Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.4 OR *[OID ESCBPKI]*.2.2.5[10] *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1.1) RegisteredID (*[OID ESCBPKI]*.1.1.2) RegisteredID (*[OID ESCBPKI]*.1.1.3) RegisteredID (*[OID ESCBPKI]*.1.1.10) RegisteredID (*[OID ESCBPKI]*.1.1.4) RegisteredID (*[OID ESCBPKI]*.1.1.7)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers Ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
qcStatements	 id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) Id-etsi-qcs-QcSSCD[11] (0.4.0.1862.1.4)	
[ESCB] Extensions		
escbUseCertType	SIGNATURE	

[10] *[OID ESCBPKI]*.2.2.4 in case of advanced signature certificates based on a SSCD.
[OID ESCBPKI].2.2.5 in case of advanced signature certificates.
[11] Only in the case of advanced signature certificates based on a SSCD.

7.1.2.3 Standard encryption certificate with and without key archive

Standard encryption certificate with and without key archive		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which user is member* *User identifier (UID)* [ENC:K] *Name Middle name Surnames* [ENC:A] *Name Middle name Surnames* [ENC:S] *Name Middle name Surnames* [12]	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 0 0 1 1 0 0 0	Yes
extKeyUsage	 emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	

[12] *[ENC:K]* in case of advanced encryption certificates with key archive recoverable only in a token
[ENC:A] in case of advanced encryption certificates without key archive
[ENC:S] in case of encryption certificates with key archive recoverable in software

Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.2 *[OID ESCBPKI]*.2.2.3 *[OID ESCBPKI]*.2.2.12 [13] *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1.1) RegisteredID (*[OID ESCBPKI]*.1.1.2) RegisteredID (*[OID ESCBPKI]*.1.1.3) RegisteredID (*[OID ESCBPKI]*.1.1.10) RegisteredID (*[OID ESCBPKI]*.1.1.4) RegisteredID (*[OID ESCBPKI]*.1.1.7)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbUseCertType	ENCRYPTION	

[13] *[OID ESCBPKI]*.2.2.2 in case of advanced encryption certificates with key archive recoverable only in a token
[OID ESCBPKI].2.2.3 in case of advanced encryption certificates without key archive
[OID ESCBPKI].2.2.12 in case of encryption certificates with key archive recoverable in software

7.1.2.4 Standard authentication certificate

Standard authentication certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which user is member* *User identifier (UID)* [AUT:S] *Name Middle name Surnames*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature[14] Non Repudiation Key Encipherment[15] Data Encipherment[12] Key Agreement Key Certificate Signature CRL Signature	 1 0 1 1 1 0 0	Yes
extKeyUsage	 clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies		

[14] This usage is allowed in the scenarios where a digital signature is generated to authenticate the certificate subscriber

[15] keyEncipherment and dataEncipherment are allowed for emailProtection only. The private key is never stored in the Key Archive.

Policy Identifier URL CPS	*[OID ESCBPKI]*.2.2.6 *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4) RegisteredID (*[OID ESCBPKI]*.1.7)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	AUTHENTICATION	

7.1.2.5 Mobile device certificate

Mobile device certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which user is member* *User identifier (UID)* [MOB:S] *Name Middle name Surnames*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 0 0 1 0 0	Yes
extKeyUsage	 clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.7 *[CPS-URL]*	
Subject Alternative Names		

rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4) RegisteredID (*[OID ESCBPKI]*.1.7)	*Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	MOBILE DEVICE	

7.1.2.6 Secure e-mail gateway certificate

Secure e-mail gateway certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which user is member* *User identifier (UID)* [EGW:S] *Name Middle name Surnames*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 1 1 0 0 0	Yes
extKeyUsage	 emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.8 *[CPS-URL]*	
Subject Alternative Names rfc822	 *Subject's Email*	

RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4) RegisteredID (*[OID ESCBPKI]*.1.7)	*Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	SECURE EMAIL GATEWAY	

7.1.2.7 Provisional certificate

Provisional certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*Maximum 1 month*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which user is member* *User identifier (UID)* [TMP:A] *Name Middle name Surnames*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 0 0 1 0 0	Yes
extKeyUsage	 emailProtection (1.3.6.1.5.5.7.3.4) clientAuth (1.3.6.1.5.5.7.3.2) smartCardLogon (1.3.6.1.4.1.311.20.2.2) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.9 *[CPS-URL]*	

Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4) RegisteredID (*[OID ESCBPKI]*.1.7)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	PROVISIONAL	

7.1.2.8 Administrator certificate

Administrator certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which user is member* *User identifier (UID)* [ADM:A] *Name Middle name Surnames*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 0 0 1 0 0	Yes
extKeyUsage	 emailProtection (1.3.6.1.5.5.7.3.4) clientAuth (1.3.6.1.5.5.7.3.2) smartCardLogon (1.3.6.1.4.1.311.20.2.2) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.10 *[CPS-URL]*	

Subject Alternative Names		
RegisteredID UPN (1.3.6.1.4.1.311.20.2.3)	*User Principal Name (if available)*	
rfc822	*Subject's Email*	
RegisteredID (*[OID ESCBPKI]*.1.1)	*Subject's Name*	
RegisteredID (*[OID ESCBPKI]*.1.2)	*Subject's Middle Name (if any)*	
RegisteredID (*[OID ESCBPKI]*.1.3)	*Subject's Surname*	
RegisteredID (*[OID ESCBPKI]*.1.10)	*Subject's First surname*	
RegisteredID (*[OID ESCBPKI]*.1.4)	*Subject's Secondary surname (if any)*	
RegisteredID (*[OID ESCBPKI]*.1.7)	*ESCB user identifier (UID)*	
Basic Constraints		Yes
CA	FALSE	
Path Length Constraint	*Not used*	
CRL Distribution Points		
Private Extensions		
Authority Information Access		
caIssuers	*[HTTP URI Root CA]*	
caIssuers	*[HTTP URI Sub CA]*	
ocsp	*[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	ADMINISTRATOR	

7.1.2.9 Shared mailbox certificate

Shared mailbox certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority of the shared mailbox* *ESCB user identifier (UID)* [SHM:S] *Display Name*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 1 1 1 0 0	Yes
extKeyUsage	 emailProtection (1.3.6.1.5.5.7.3.4) clientAuth (1.3.6.1.5.5.7.3.2) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.11 *[CPS-URL]*	
Subject Alternative Names		

rfc822 RegisteredID (*[OID ESCBPKI]*.1.11) RegisteredID (*[OID ESCBPKI]*.1.7)	*Subject's Email* *Shared mailbox display name* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	SHARED MAILBOX	

7.1.3 Algorithm Object Identifiers (OID)

Cryptographic algorithm object identifiers (OID):
SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

7.1.4 Name formats

Certificates issued by ESCB-PKI contain the X.500 distinguished name of the certificate issuer and that of the subject in the issuer name and subject name fields, respectively.

7.1.5 Name constraints

See section 3.1.1.

7.1.6 Certificate Policy Object Identifiers (OID)

The OIDs for this CP are the following:

[OID ESCBPKI].2.2.0.X.Y: Certificate policies for the ESCB/SSM users' certificates (this document)

[OID ESCBPKI].2.2.1.X.Y: Certificate Policy of Advanced Authentication certificate for ESCB/SSM users

[OID ESCBPKI].2.2.2.X.Y: Certificate Policy of Archived Encryption certificate recoverable in token for ESCB/SSM users

[OID ESCBPKI].2.2.3.X.Y: Certificate Policy of Non-Archived Encryption certificate for ESCB/SSM users

[OID ESCBPKI].2.2.4.X.Y: Certificate Policy of Advanced Signature certificate based on a SSCD for ESCB/SSM users

[OID ESCBPKI].2.2.5.X.Y: Certificate Policy of Advanced Signature certificate for ESCB/SSM users

[OID ESCBPKI].2.2.6.X.Y: Certificate Policy of Standard Authentication certificate for ESCB/SSM users

[OID ESCBPKI].2.2.7.X.Y: Certificate Policy of Mobile Device certificate for ESCB/SSM users

[OID ESCBPKI].2.2.8.X.Y: Certificate Policy of Secure E-mail Gateway certificate for ESCB/SSM users

[OID ESCBPKI].2.2.9.X.Y: Certificate Policy of Provisional certificate for ESCB/SSM users

[OID ESCBPKI].2.2.10.X.Y: Certificate Policy of Administrator certificate for ESCB/SSM users

[OID ESCBPKI].2.2.11.X.Y: Certificate Policy of Shared Mailbox certificate for ESCB/SSM users

[OID ESCBPKI].2.2.12.X.Y: Certificate Policy of Archived encryption certificate for ESCB/SSM users

Where:

- [OID ESCBPKI]: represents the OID 0.4.0.127.0.10.1
- X.Y indicate the version.

7.1.7 Use of the "PolicyConstraints" extension

As specified in the ESCB-PKI CPS.

7.1.8 Syntax and semantics of the "PolicyQualifier

The Certificate Policies extension contains the following Policy Qualifiers:

- URL CPS: contains the URL to the CPS and to the CP that govern the certificate.

The content for certificates regulated under this policy can be seen in point *7.1.2 Certificate extensions*.

7.1.9 Processing semantics for the critical "CertificatePolicy" extension

As specified in the ESCB-PKI CPS.

7.2 CRL Profile

As specified in the ESCB-PKI CPS.

7.3 OCSP Profile

As specified in the ESCB-PKI CPS.

8 Compliance Audit and Other Assessment

As specified in the ESCB-PKI CPS.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

ESCB-PKI will not charge any direct fee to the certificate subscribers for the issuance or renewal of ESCB/SSM users' certificates.

9.1.2 Certificate access fees

Access to certificates issued under this Policy is free of charge and, therefore, no fee is applicable to them.

9.1.3 Revocation or status information fees

Access to information on the status or revocation of the certificates is open and free of charge and, therefore, no fees are applicable.

9.1.4 Fees for other services, such as policy information

No fee shall be applied for information services on this policy, nor on any additional service that is known at the time of drawing up this document.

9.1.5 Refund policy

Not applicable.

9.2 Financial Responsibility

As specified in the ESCB-PKI CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

As specified in the ESCB-PKI CPS.

9.3.2 Non-confidential information

As specified in the ESCB-PKI CPS. Moreover, a copy of the ESCB/SSM users' certificates is published in the directory of the ESCB Identity and Access Management (IAM) service.

9.3.3 Duty to maintain professional secrecy

As specified in the ESCB-PKI CPS.

9.4 Privacy of Personal Information

As specified in the ESCB-PKI CPS.

9.4.1 Personal data protection policy

As specified in the ESCB-PKI CPS.

9.4.2 Information considered private

As specified in the ESCB-PKI CPS.

9.4.3 Information not classified as private

As specified in the ESCB-PKI CPS.

9.4.4 Responsibility to protect personal data

As specified in the ESCB-PKI CPS.

9.4.5 Notification of and consent to the use of personal data

The mechanisms to notify certificate applicants and, when appropriate, obtain their consent for the processing of their personal data is the terms and conditions application form.

9.4.6 Disclosure within legal proceedings

As specified in the ESCB-PKI CPS.

9.4.7 Other circumstances in which data may be made public

As specified in the ESCB-PKI CPS.

9.5 Intellectual Property Rights

As specified in the ESCB-PKI CPS.

9.6 Representations and Warranties

As specified in the ESCB-PKI CPS.

9.7 Disclaimers of Warranties

As specified in the ESCB-PKI CPS.

9.8 Limitations of Liability

As specified in the ESCB-PKI CPS.

9.9 Indemnities

As specified in the ESCB-PKI CPS.

9.10 Term and Termination

9.10.1 Term

This CP shall enter into force from the moment it is approved by the PAA and published in the ESCB-PKI repository.

This CP shall remain valid until such time as it is expressly terminated due to the issue of a new version, or upon re-key of the Corporate CA keys, at which time it is mandatory to issue a new version.

9.10.2 CP substitution and termination

This CP shall always be substituted by a new version, regardless of the importance of the changes carried out therein, meaning that it will always be applicable in its entirety.
When the CP is terminated, it will be withdrawn from the ESCB-PKI public repository. Nevertheless, it will be kept for 15 years.

9.10.3 Consequences of termination

The obligations and constraints established under this CP, referring to audits, confidential information, ESCB-PKI obligations and liabilities that came into being whilst it was in force shall continue to prevail following its substitution or termination with a new version in all terms which are not contrary to said new version.

9.11 Individual notices and communications with participants

As specified in the ESCB-PKI CPS.

9.12 Amendments

As specified in the ESCB-PKI CPS.

9.13 Dispute Resolution Procedures

As specified in the ESCB-PKI CPS.

9.14 Governing Law

As specified in the ESCB-PKI CPS.

9.15 Compliance with Applicable Law

As specified in the ESCB-PKI CPS.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement clause

As specified in the ESCB-PKI CPS.

9.16.2 Independence

Should any of the provisions of this CP be declared invalid, null or legally unenforceable, it shall be deemed as not included, unless said provisions were essential in such a way that excluding them from the CP would render the latter without legal effect.

9.16.3 Resolution through the courts

As specified in the ESCB-PKI CPS.

9.17 Other Provisions

As specified in the ESCB-PKI CPS.

NBB - Securities
boulevard de Berlaimont 14
BE -1000 Brussels (Belgium)
Phone: + 32 (0)2 221 22 14
Fax: + 32 (0)2 221 31 19
E-mail: sss@nbb.be

BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI SERVICES

OIDS: 0.4.0.127.0.10.1.2.3.0

CERTIFICATE POLICIES FOR THE NON-ESCB/NON-SSM USERS' CERTIFICATES

VERSION 1.2

11 May 2015

Table of Contents

1 Introduction 8

1.1 Overview 8

1.2 Document Name and Identification 9

1.3 ESCB-PKI Participants 10

1.3.1 The Policy Approval Authority 10
1.3.2 Certification Authority 10
1.3.3 Registration Authorities 10
1.3.4 Validation Authority 10
1.3.5 Key Archive 11
1.3.6 Users 11

1.4 Certificate Usage 11

1.4.1 Appropriate certificate use 11
1.4.2 Certificate Usage Constraints and Restrictions 12

1.5 Policy Approval 12

1.6 Definitions and Acronyms 12

1.6.1 Definitions 12
1.6.2 Acronyms 13

2 Publication and Repository Responsibilities 16

2.1 Repositories 16

2.2 Publication of Certification Data, CPS and CP 16

2.3 Publication Timescale or Frequency 16

2.4 Repository Access Controls 16

3 Identification and Authentication (I&A) 17

3.1 Naming 17

3.1.1 Types of names 17
3.1.2 The need for names to be meaningful 17
3.1.3 Rules for interpreting various name formats 17
3.1.4 Uniqueness of names 17
3.1.5 Name dispute resolution procedures 17
3.1.6 Recognition, authentication, and the role of trademarks 17

3.2 Initial Identity Validation 18

3.2.1 Means of proof of possession of the private key 18
3.2.2 Identity authentication for an entity 18
3.2.3 Identity authentication for an individual 18
3.2.4 Non-verified applicant information 19
3.2.5 Validation of authority 19
3.2.6 Criteria for operating with external CAs 19

3.3 Identification and Authentication for Re-key Requests 19

3.3.1 Identification and authentication requirements for routine re-key 19
3.3.2 Identification and authentication requirements for re-key after certificate revocation 19

4 Certificate Life-Cycle Operational Requirements 20

4.1 Certificate Application 20
4.1.1 Who can submit a certificate application? 20
4.1.2 Enrolment process and applicants' responsibilities 20

4.2 Certificate Application Processing 22
4.2.1 Performance of identification and authentication procedures 22
4.2.2 Approval or rejection of certificate applications 22
4.2.3 Time limit for processing the certificate applications 22

4.3 Certificate Issuance 22
4.3.1 Actions performed by the CA during the issuance of the certificate 22
4.3.2 CA notification to the applicants of certificate issuance 22

4.4 Certificate Acceptance 23
4.4.1 Form of certificate acceptance 23
4.4.2 Publication of the certificate by the CA 23
4.4.3 Notification of certificate issuance by the CA to other Authorities 23

4.5 Key Pair and Certificate Usage 23
4.5.1 Certificate subscribers' use of the private key and certificate 23
4.5.2 Relying parties' use of the public key and the certificate 23

4.6 Certificate Renewal 23

4.7 Certificate Re-key 23
4.7.1 Circumstances for certificate renewal with key changeover 23
4.7.2 Who may request certificate renewal? 23
4.7.3 Procedures for processing certificate renewal requests with key changeover 23
4.7.4 Notification of the new certificate issuance to the subscriber 24
4.7.5 Manner of acceptance of certificates with changed keys 24
4.7.6 Publication of certificates with the new keys by the CA 24
4.7.7 Notification of certificate issuance by the CA to other Authorities 24

4.8 Certificate Modification 24
4.8.1 Circumstances for certificate modification 24

4.9 Certificate Revocation and Suspension 24
4.9.1 Circumstances for revocation 24
4.9.2 Who can request revocation? 24
4.9.3 Procedures for requesting certificate revocation 25
4.9.4 Revocation request grace period 25
4.9.5 Time limit for the CA to process the revocation request 25
4.9.6 Requirements for revocation verification by relying parties 25
4.9.7 CRL issuance frequency 25
4.9.8 Maximum latency between the generation of CRLs and their publication 25
4.9.9 Online certificate revocation status checking availability 25
4.9.10 Online revocation checking requirements 26
4.9.11 Other forms of revocation alerts available 26
4.9.12 Special requirements for the revocation of compromised keys 26

4.9.13 Causes for suspension 26
4.9.14 Who can request the suspension? 26
4.9.15 Procedure for requesting certificate suspension 26
4.9.16 Suspension period limits 26
4.10 Certificate Status Services 26
4.11 End of Subscription 27
4.12 Key Escrow and Recovery 27
5 Facility, Management, and Operational Controls 28
5.1 Physical Security Controls 28
5.2 Procedural Controls 28
5.3 Personnel Controls 28
5.4 Audit Logging Procedures 28
5.5 Records Archival 28
5.5.1 Types of records archived 28
5.5.2 Archive retention period 28
5.5.3 Archive protection 28
5.5.4 Archive backup procedures 28
5.5.5 Requirements for time-stamping records 28
5.5.6 Audit data archive system (internal vs. external) 28
5.5.7 Procedures to obtain and verify archived information 28
5.6 Key Changeover 28
5.7 Compromise and Disaster Recovery 29
5.8 CA or RA Termination 29
6 Technical Security Controls 30
6.1 Key Pair Generation and Installation 30
6.1.1 Key pair generation 30
6.1.2 Delivery of private keys to subscribers 30
6.1.3 Delivery of the public key to the certificate issuer 30
6.1.4 Delivery of the CA's public key to relying parties 31
6.1.5 Key sizes 31
6.1.6 Public key generation parameters and quality checks 31
6.1.7 Key usage purposes (KeyUsage field in X.509 v3) 31
6.2 Private Key Protection and Cryptographic Module Engineering Controls 31
6.2.1 Cryptographic module standards 31
6.2.2 Private key multi-person (k out of n) control 31
6.2.3 Escrow of private keys 32
6.2.4 Private key backup copy 32
6.2.5 Private key archive 32
6.2.6 Private key transfer into or from a cryptographic module 32
6.2.7 Private key storage in a cryptographic module 32
6.2.8 Private key activation method 32
6.2.9 Private key deactivation method 33

6.2.10 Private key destruction method 33
6.2.11 Cryptographic module classification 33
6.3 Other Aspects of Key Pair Management 33
6.3.1 Public key archive 33
6.3.2 Operational period of certificates and usage periods for key pairs 33
6.4 Activation Data 33
6.5 Computer Security Controls 33
6.6 Life Cycle Security Controls 33
6.7 Network Security Controls 33
6.8 Timestamping 33
7 Certificate, CRL, and OCSP Profiles 34
7.1 Certificate Profile 34
7.1.1 Version number 34
7.1.2 Certificate extensions 34
7.1.3 Algorithm Object Identifiers (OID) 43
7.1.4 Name formats 43
7.1.5 Name constraints 43
7.1.6 Certificate Policy Object Identifiers (OID) 43
7.1.7 Use of the "PolicyConstraints" extension 43
7.1.8 Syntax and semantics of the “PolicyQualifier 43
7.1.9 Processing semantics for the critical “CertificatePolicy” extension 44
7.2 CRL Profile 44
7.3 OCSP Profile 44
8 Compliance Audit and Other Assessment 45
9 Other Business and Legal Matters 46
9.1 Fees 46
9.1.1 Certificate issuance or renewal fees 46
9.1.2 Certificate access fees 46
9.1.3 Revocation or status information fees 46
9.1.4 Fees for other services, such as policy information 46
9.1.5 Refund policy 46
9.2 Financial Responsibility 46
9.3 Confidentiality of Business Information 46
9.3.1 Scope of confidential information 46
9.3.2 Non-confidential information 46
9.3.3 Duty to maintain professional secrecy 46
9.4 Privacy of Personal Information 46
9.4.1 Personal data protection policy 47
9.4.2 Information considered private 47
9.4.3 Information not classified as private 47
9.4.4 Responsibility to protect personal data 47

9.4.5 Notification of and consent to the use of personal data 47
9.4.6 Disclosure within legal proceedings 47
9.4.7 Other circumstances in which data may be made public 47
9.5 Intellectual Property Rights 47
9.6 Representations and Warranties 47
9.7 Disclaimers of Warranties 47
9.8 Limitations of Liability 47
9.9 Indemnities 47
9.10 Term and Termination 48
9.10.1 Term 48
9.10.2 CP substitution and termination 48
9.10.3 Consequences of termination 48
9.11 Individual notices and communications with participants 48
9.12 Amendments 48
9.13 Dispute Resolution Procedures 48
9.14 Governing Law 48
9.15 Compliance with Applicable Law 48
9.16 Miscellaneous Provisions 48
9.16.1 Entire agreement clause 48
9.16.2 Independence 49
9.16.3 Resolution through the courts 49
9.17 Other Provisions 49

Control Sheet

	Title	Certification Policy for the non-ESCB/non-SSM users' certificates
	Author	ESCB-PKI Service Provider
	Version	1.2
	Date	11.05.2015

RELEASE NOTES

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column "Release number" refer to the current version of the document.

Release number	Status	Date	Change Reason
0.1	Draft	27.05.2011	BdE revision
0.2	Draft	15.06.2011	BdE revision
0.3	Draft	14.07.2011	BdE revision
0.4	Draft	22.07.2011	BdE revision
0.5	Draft	26.07.2011	Add CA Fingerprint
0.6	Draft	15.09.2011	Revision of certificate profiles
1.0	Final	19.10.2011	Update after ITC approval.
1.1	Final	11.01.2013	GovC approval
1.2	Final	11.05.2015	Hashing algorithm update

1 Introduction

1.1 Overview

This document sets out the Certificate Policy (CP) governing the personal certificates issued to non-ESCB/non-SSM users (i.e. users that belong to organisations external to ESCB Central Banks and SSM National Competent Authorities) by the Public Key Infrastructure (hereinafter referred to as PKI) of the European System of Central Banks (hereinafter referred to as ESCB-PKI). It has been drafted in compliance with the **Decision ECB/2013/1 of the European Central Bank**[1].

This document is intended for the use of all the participants related to the ESCB-PKI hierarchy, including the Certification Authority (CA), Registration Authorities (RA), certificate applicants, certificate subscribers and relying parties, among others.

From the perspective of the X.509 v3 standard, a CP is a set of rules that define the applicability or use of a certificate within a community of users, systems or specific class of applications that have a series of security requirements in common.

This CP details and completes the "Certification Practice Statement" (CPS) of the ESCB-PKI, containing the rules to which the use of the certificates defined in this policy are subject, as well as the scope of application and the technical characteristics of this type of certificate.

This CP has been structured in accordance with the guidelines of the PKIX work group in the IETF (Internet Engineering Task Force) in its reference document RFC 3647 (approved in November 2003) "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". In order to give the document a uniform structure and facilitate its reading and analysis, all the sections established in RFC 3647 have been included. Where nothing has been established for any section the phrase "No stipulation" will appear.

Furthermore, when drafting its content, European standards have been taken into consideration, among which the most significant are:

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
- ETSI TS 101 862: Qualified Certificate Profile.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

The following legislation has been considered:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1994[2].
- Directive 1999/93/EC of the European Parliament and of the Council [3].
- Regulation (EU) No 910/2014 of the European Parliament and the Council[4].
- Spanish Law 59/2003, of 19 December, the Electronic Signature Act (Spanish Official Journal, 20 December).[5]

[1] Decision ECB/2013/1of the European Central Bank of 11 January 2013 laying down the framework for a public key infrastructure for the European System of Central Banks (OJ L 74, 16.3.2013, p. 30).

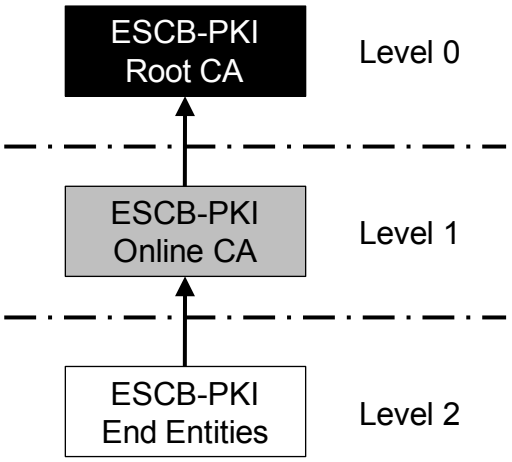
[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1994 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

[4] Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

- Spanish Organic Law 15/1999, of 13 December 1999, on the protection of personal data
- Spanish Royal Decree 1720/2007, of 21 December2007, approving the Regulations for the development of Spanish Organic Law 15/1999.
- National legislation transposing Directive 95/46/EC and the Directive 99/93/EC applicable to the ESCB central banks and SSM national competent authorities acting as Registration Authorities.
- Decision (EU) 2015/XX (ECB/2015/XX)[6].

This CP sets out the services policy, as well as a statement on the level of guarantee provided, by way of description of the technical and organisational measures established to guarantee the PKI's level of security.
The CP includes all the activities for managing the non-ESCB/non-SSM users' certificates throughout their life cycle, and serves as a guide for the relations between the Online CA and its users. Consequently, all the PKI participants (see section 1.3) involved must be aware of the content of the CP and adapt their activities to the stipulations therein.
This CP assumes that the reader is conversant with the PKI, certificate and electronic signature concepts. If not, readers are recommended to obtain information on the aforementioned concepts before they continue reading this document.
The general architecture, in hierarchic terms, of ESCB-PKI is as follows:



1.2 Document Name and Identification

Document name	Certificate Policy (CP) for the non-ESCB/non-SSM users' certificates
Document version	1.2
Document status	Final
Date of issue	11.05.2015

[5]Spanish legislation is also considered owed to the fact that Banco de España, the Service Provide, is established at Spain
[6] Decision (EU) 2015/[XX] of [date, month] 2015 on the access and use of SSM electronic applications, systems, platforms and services by the European Central Bank and the national competent authorities of the Single Supervisory Mechanism (ECB/2015/XX), not yet published in the Official Journal of the European Union.

OID (Object Identifiers)	0.4.0.127.0.10.1.2.3.0: Certificate policies for the non-ESCB/non-SSM users' certificates (this document) 0.4.0.127.0.10.1.2.3.1: Certificate Policy of Advanced Authentication certificate for non-ESCB/non-SSM users 0.4.0.127.0.10.1.2.3.2: Certificate Policy of Advanced Encryption certificate for non-ESCB/non-SSM users 0.4.0.127.0.10.1.2.3.4: Certificate Policy of Advanced Signature certificate based on a SSCD for non-ESCB/non-SSM users 0.4.0.127.0.10.1.2.3.5: Certificate Policy of Advanced Signature certificate for non-ESCB/non-SSM users 0.4.0.127.0.10.1.2.3.6: Certificate Policy of Standard Authentication certificate for non-ESCB/non-SSM users
CPS location	http://pki.escb.eu/policies
Related CPS	Certification Practice Statement of ESCB-PKI OID 0.4.0.127.0.10.1.2.1

1.3 ESCB-PKI Participants

As specified in the ESCB-PKI CPS.

1.3.1 The Policy Approval Authority

As specified in the ESCB-PKI CPS.

1.3.2 Certification Authority

As specified in the ESCB-PKI CPS.

1.3.3 Registration Authorities

As specified in the ESCB-PKI CPS.

1.3.3.1 Registration Authorities' roles

From the list of Registration Authorities' roles described in the CPS the ones required to manage ESCB/SSM users' certificates are the following:

- **Registration Officers for External Organisations**
- **Trusted Agents**

1.3.4 Validation Authority

As specified in the ESCB-PKI CPS.

1.3.5 Key Archive

No applicable.

1.3.6 Users

As specified in the ESCB-PKI CPS.

1.3.6.1 Certificate Subscribers

Certificate subscribers are defined in accordance with the ESCB-PKI CPS.
The categories of persons who may be certificate subscribers of non-ESCB/non-SSM users' certificates issued by the ESCB-PKI Online CA are limited to those included in the following chart:

Certification Authority	Certificate subscribers
Online CA	Users from non-ESCB/non-SSM organisations that need to communicate with ESCB/SSM applications (as non-ESCB/non-SSM users)

Certificate subscribers will be able to receive any of the following certificate packages:

- **Advanced certificates**, where all the following certificates will be stored in a smartcard or other cryptographic token (e.g. USB device):
  - Advanced authentication certificate. The corresponding key pair will be generated inside the cryptographic token.
  - Advanced signature certificate or advanced signature certificate based on a SSCD depending upon if the cryptographic token has got a SSCD certification or not. In both cases, the corresponding private key will be generated inside the cryptographic token.
  - Advanced encryption certificate without key archive. The key pair will be generated inside the cryptographic token and no other copy will be archived.
- **Standard certificates**, where the private key will be generated by the CA and stored in a software device. The only type of standard certificate described in this CP is the authentication certificate.

1.3.6.2 Relying Parties

As specified in the ESCB-PKI CPS.

1.4 Certificate Usage

1.4.1 Appropriate certificate use

1 Certificates issued by ESCB-PKI in the scope of this CP may only be used within the scope of the ESCB/SSM by users from external organisations.

2 Within the scope of the paragraph above, certificates issued by ESCB-PKI may be used for financial activities.

The certificates regulated by this CP shall be used for personal authentication, signing and/or encipherment purposes, depending on the corresponding keyUsage extension and OID attribute in the *certificatePolicies* extension.

1.4.2 Certificate Usage Constraints and Restrictions

Any other use not included in the previous point shall be excluded.

1.5 Policy Approval

As specified in the ESCB-PKI CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

Within the scope of this CPS the following terms are used:

Authentication: the process of confirming the identity of a certificate subscriber.
Identification: the process of verifying the identity of those applying for a certificate.
Eurosystem Central Bank: means either an NCB of a Member State whose currency is the euro or the ECB.
Non-euro area NCB: means an NCB of a Member State whose currency is not the euro.
ESCB Central Bank: means either a Eurosystem Central Bank or a non-euro area NCB**.**
Central Bank: In this CP the term "Central Bank" is used to refer to any Central Bank belonging to the European System of Central Banks/Eurosystem, including the ECB.
National Competent Authority or SSM National Competent Authority: means any National Competent Authority (NCA) belonging to the Single Supervisory Mechanism (SSM) that has agreed to use the ESCB-PKI.
External or non-ESCB/non-SSM Organisation: public or private organisation that do not belong to the European System of Central Banks (ESCB) or to the Single Supervisory Mechanism (SSM).
Non-ESCB/non-SSM user: user that belongs to a non-ESCB/non-SSM organisation.
Electronic certificate or certificate: electronic file, issued by a certification authority, that binds a public key with a certificate subscriber's identity and is used for the following: to verify that a public key belongs to a certificate subscriber; to authenticate a certificate subscriber; to check a certificate's subscriber signature; to encrypt a message addressed to a certificate subscriber; or to verify a certificate subscriber's access rights to ESCB/SSM electronic applications, systems, platforms and services. Certificates are held on data carrier devices, and references to certificates include such devices.
Public key and private key: the asymmetric cryptography on which the PKI is based employs a key pair in which what is enciphered with one key of this pair can only be deciphered by the other, and vice versa. One of these keys is "public" and is included in the electronic certificate, whilst the other is "private" and is only known by the certificate subscriber.
Session key: a key established to encipher communication between two entities. The key is established specifically for each communication, or session, and its utility expires upon termination of the session.

Key agreement: a process used by two or more technical components to agree on a session key in order to protect a communication.
Directory: a data repository that is usually accessed through the LDAP protocol.

User identifier: a set of characters that are used to uniquely identify the user of a system.
Public Key Infrastructure: the set of individuals, policies, procedures, and computer systems necessary to provide authentication, encryption, integrity and non-repudiation services, by way of public and private key cryptography and electronic certificates.
ESCB-PKI Certification Authority: means the entity, trusted by users, to issue, manage, revoke and renew certificates in accordance with the ESCB certificate acceptance framework.
Trust hierarchy: the set of Certification Authorities that maintain a relationship of trust by which a CA of a higher level guarantees the trustworthiness of one or several lower level CAs. In the case of ESCB-PKI, the hierarchy has two levels: the Root CA at the top level guarantees the trustworthiness of its subordinate CAs, one of which is the Online CA.
Certification Service Provider (CSP): entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.
Registration Authority: means an entity trusted by the users of the certification services which verifies the identity of individuals applying for a certificate before the issuance of the certificate by the ESCB-PKI Certification Authority.
Certificate applicants: the individuals who request the issuance of certificates.
Certificate subscribers: the individuals for which an electronic certificate is issued and accepted by said individuals.
Relying parties: individuals or entities, other than certificate subscribers, that decide to accept and rely on a certificate issued by ESCB-PKI.
Providing Central Bank or **service provider:** means the NCB appointed by the Governing Council to develop the ESCB-PKI and to issue, manage, revoke and renew electronic certificates on behalf and for the benefit of the Eurosystem central banks.
Repository: a part of the content of the ESCB-PKI website where relying parties, certificate subscribers and the general public can obtain copies of ESCB-PKI documents, including but not limited to this CP and CRLs.

Validation Authority: means an entity trusted by the users of the certification services which provides information about the revocation status of the certificates issued by the ESCB-PKI Certification Authority.

1.6.2 Acronyms

C: (Country). Distinguished Name (DN) attribute of an object within the X.500 directory structure
CA: Certification Authority
CAF: Certificate Acceptance Framework
CB: Central Bank that uses the ESCB-PKI
CDP: CRL Distribution Point
CEN: Comité Européen de Normalisation
CN: Common Name Distinguished Name (DN) attribute of an object within the X.500 directory structure
CP: Certificate Policy
CPS: Certification Practice Statement
CRL: Certificate Revocation List

CSP: Certification Service Provider
CSR: Certificate Signing Request: set of data that contains the public key and its electronic signature using the companion private key, sent to the CA for the issue of an electronic signature that contains said public key
CWA: CEN Workshop Agreement
DN: Distinguished Name: unique identification of an entry within the X.500 directory structure
ECB: European Central Bank
ESCB: European System of Central Banks
ESCB-PKI: European System of Central Banks Public Key Infrastructure: means the public key infrastructure developed by the providing central bank on behalf of and for the benefit of the Eurosystem Central Banks which issues, manages, revokes and renews certificates in accordance with the ESCB certificate acceptance framework - as amended from time to time including in relation to SSM -
ETSI: European Telecommunications Standard Institute
FIPS: Federal Information Processing Standard
HSM: Hardware Security Module: cryptographic security module used to store keys and carry out secure cryptographic operations
IAM: Identity and Access Management
IETF: Internet Engineering Task Force (internet standardisation organisation)
ITC: Information Technology Committee
LDAP: Lightweight Directory Access Protocol
NCA: National Competent Authority
NCB: National Central Bank
O: Organisation. Distinguished Name (DN) attribute of an object within the X.500 directory structure
OCSP: Online Certificate Status Protocol: this protocol enables online verification of the validity of an electronic certificate
OID: Object Identifier
OU: Organisational Unit. Distinguished Name (DN) attribute of an object within the X.500 directory structure
PAA: Policy Approval Authority
PIN: Personal Identification Number: password that protects access to a cryptographic card
PKCS: Public Key Cryptography Standards: internationally accepted PKI standards developed by RSA Laboratories
PKI: Public Key Infrastructure
PKIX: Work group within the IETF (Internet Engineering Task Group) set up for the purpose of developing PKI and internet specifications
PUK: PIN UnlocK Code: password used to unblock a cryptographic card that has been blocked after repeatedly and consecutively entering the wrong PIN
RA: Registration Authority
RO: Registration Officer
RO4EO: Registration Officer for External Organisations
RFC: Request For Comments (Standard issued by the IETF)
SSCD: Secure Signature Creation Device
SSM: Single Supervisory Mechanism
T&C: Terms and conditions application form
UID: User identifier
VA: Validation Authority

2 Publication and Repository Responsibilities

2.1 Repositories

As specified in the ESCB-PKI CPS.

2.2 Publication of Certification Data, CPS and CP

As specified in the ESCB-PKI CPS.

Moreover, a copy of the non-ESCB/non-SSM users' certificates is published in the directory of the ESCB Identity and Access Management (IAM) service.

2.3 Publication Timescale or Frequency

As specified in the ESCB-PKI CPS.

2.4 Repository Access Controls

As specified in the ESCB-PKI CPS.

3 Identification and Authentication (I&A)

3.1 Naming

3.1.1 Types of names

The certificates issued by ESCB-PKI contain the Distinguished Name (or DN) X.500 of the issuer and that of the certificate subject in the fields *issuer name* and *subject name*, respectively.
The CN (Common Name) attribute of the DN contains a prefix that identifies the certificate usage, and the following are accepted:

- [AUT:S] → Standard Authentication certificate
- [AUT:A] → Advanced Authentication certificate
- [SIG:A] → Advanced Signature certificate based on a token without SSCD certification
- [SIG:Q] → Advanced Signature certificate based on a token with SSCD certification
- [ENC:A] → Advanced Encryption certificate without private key archive

This prefix will be followed by the name, middle name and surnames of the certificate subscribers.

Additionally, the following field is used:

- PS (OID: 2.5.4.65)= <User identifier at ESCB/SSM level>

The rest of the DN attributes shall have the following fixed values:

- C [Country where the Registration Authority is located]
- O EUROPEAN SYSTEM OF CENTRAL BANKS
- OU Non-ESCB/non-SSM organisation to which the subscriber belongs to

3.1.2 The need for names to be meaningful

In all cases the distinguished names of the certificates are meaningful because they are subject to the rules established in the previous point in this respect.

3.1.3 Rules for interpreting various name formats

As specified in the ESCB-PKI CPS.

3.1.4 Uniqueness of names

The whole made up of the combination of the distinguished name plus the KeyUsage extension content must be unique and unambiguous to ensure that certificates issued for two different certificate subscribers will have different distinguished names.
Certificate DNs must not be repeated. The use of the user identifier at ESCB/SSM level guarantees the uniqueness of the DN.

3.1.5 Name dispute resolution procedures

As specified in the ESCB-PKI CPS.

3.1.6 Recognition, authentication, and the role of trademarks

As specified in the ESCB-PKI CPS.

3.2 Initial Identity Validation

3.2.1 Means of proof of possession of the private key

Depending on the specific certificate type, the means of proof of private key possession will be different:

- [AUT:S] → standard authentication certificate: the key pair will be created by the ESCB-PKI Online Certification Authority, so this section does not apply.
- [AUT:A] → advanced authentication certificate: the key pair will be created by the subject in the private zone into his cryptographic token and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [SIG:A] → advanced signature certificate (no SSCD token): the key pair will be created by the subject in the private zone into his cryptographic token and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [SIG:Q] → advanced Signature certificate based on a SSCD token: the key pair will be created by the subject in the SSCD zone of a secure signature creation device and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [ENC:A] → advanced encryption without key archive: the key pair will be created by the subject in the private zone into his secure signature creation device and the public key will be provided to the ESCB-PKI Online CA for its certification.

3.2.2 Identity authentication for an entity

This CP does not consider the issuance of certificates for entities.

3.2.3 Identity authentication for an individual

Evidence of the subject's identity is checked against a physical person.

Validation of the individual

Unless the certificate applicant has already been identified previously by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process with the same requirements, the certificate applicant shall provide evidences of, at least, the following information:

- Full name, and
- Date and place of birth, or reference to a nationally recognized identity document, or other attributes which may be used to distinguish the person from others with the same name.

To validate the previous information the certificate applicant must present a document as proof of identity. The acceptable documents are:

- Passport, or
- National Identity Card, or
- Any other legal document accepted by the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority to dully identify an individual.

The validation of the identity will be performed by a Registration Officer for External Organisations or by a Trusted Agent delegated at the external organisation.

Validation of the non-ESCB/non-SSM organisation

Unless the non-ESCB/non-SSM organisation to which the certificate applicant belongs has already been validated previously by the Central Bank or National Competent Authority through a process with the same requirements, the following information must be provided:

1. To validate the non-ESCB/non-SSM organisation:
- Recent constitutive act of the non-ESCB/non-SSM organisation, or
- Recent extract of the national commercial register, or
- Any equivalent document accepted by the applicable national legislation to dully identify an Organisation, and

2. To prove the applicant's relations with the non-ESCB/non-SSM organisation
- An authorisation of one of the physical persons who are a legal representative of the non-ESCB/non-SSM organisation, to request non-ESCB/non-SSM users' certificates to be used in the communication between the ESCB/SSM and the Organisation
- A copy of the identity evidence (National Identity card, Passport or any other legal document accepted by the applicable national legislation) of the physical person who is the legal representative of the Organisation; in case this person cannot be physically present, the copy must be certified by a competent authority according to the national legislation.

3.2.4 Non-verified applicant information

All the information stated in the previous section must be verified.

3.2.5 Validation of authority

As specified in the ESCB-PKI CPS.

3.2.6 Criteria for operating with external CAs

As specified in the ESCB-PKI CPS.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication requirements for routine re-key

The same process as for initial identity validation is used.

3.3.2 Identification and authentication requirements for re-key after certificate revocation

The same process as for initial identity validation is used.

4 Certificate Life-Cycle Operational Requirements

This chapter contains the operational requirements for the life cycle of non-ESCB/non-SSM users' certificates issued by the ESCB-PKI CA. Despite the fact that these certificates might be stored on cryptographic tokens, it is not the purpose of the Certificate Policy to regulate the management of said tokens and, therefore, it is also assumed that the certificate applicants have previously obtained their cryptographic tokens.

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Certificates for non-ESCB/non-SSM users will be managed by a Registration Officer for External Organisations (RO4EO). RO4EOs will be able to request certificate types mentioned in section 1.3.6.

Application for a certificate does not mean it will be obtained if the applicant does not fulfil the requirements established in the CPS or in this CP for non-ESCB/non-SSM users' certificates (e.g. if the certificate applicant does not provide the RO4EO with the documents necessary for his/her identification)

4.1.2 Enrolment process and applicants' responsibilities

Advanced certificates (cryptographic token-based)

This process is carried out to obtain a certificate package consisting on three certificates: authentication, encryption and signature certificates. The certificate package will be stored in a cryptographic token. The procedure is the same independently on the type of token (with or without SSCD certification) to be used.

The procedure is as follows:

1. Cryptographic token-based certificate requests for a non-ESCB/non-SSM user can be initiated:
    a. either using ESCB Identity Access Management (IAM) interfaces,
    b. or using ESCB-PKI web interface;
2. The certificate applicant must explicitly accept the terms and conditions application form (T&C) by his/her hand-written signature of the term and conditions. The T&C will incorporate the following data:
    a. the attributes to be included in the certificate: first name, middle name (if any), surname, name of the organisation that the user belongs to, user identifier and e-mail address;
    b. the serial number of the certificate applicant's cryptographic token;
    c. under the conditions and limitations of the applicable data protection law, central banks may require that the certificate applicant provides on the T&C the attributes required to distinguish the person from others with the same name (see Section 3.2.3), namely, the number of a national recognized identity document according to the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority, or the date and place of birth.

3. In the case that a Trusted Agent is in charge of identifying and authenticating the certificate applicant, he/she will add his/her hand-written signature to the T&C;
4. The RO4EO must validate the information included in the certificate request against the documentation provided by the certificate applicant, including the T&C. In the case that the certificate applicant is not in front of him/her, the RO4EO will also validate that a valid Trusted Agent has signed the T&C;
5. The RO4EO, using the ESCB-PKI web interface, will either:
    a. Start the issuance of certificates
    b. Approve a remote download

   In both cases the certificate applicant must hold his/her token and, when requested, must insert it and type his/her personal PIN to generate the keys and store the certificates,
6. The RO4EO must securely archive all the documentation during the retention period described in section 5.5.2 of this CP:
    a. the terms and conditions application form signed by both, the certificate applicant and the person who identified and authenticated him/her (i.e. the Trusted Agent or the RO4EO himself/herself)
    b. under the conditions and limitations of the applicable data protection law, the central bank may choose to ask their RO4EO to retain a copy of the official identification document used to validate the certificate applicant's identity or, if this were not legally feasible, a copy of other identification document, preferable with the certificate applicant's photography;

Standard certificates (software-based)

This process is carried out to obtain a single certificate valid for authentication that will be stored in a software keystore (i.e. a password protected file).
The procedure is as follows:

1. Software-based certificate requests for a non-ESCB/non-SSM user can be initiated:
    a. either using ESCB Identity Access Management (IAM) interfaces,
    b. or using ESCB-PKI web interface;
2. The certificate applicant must explicitly accept the terms and conditions application form (T&C) by his/her hand-written signature of the terms and conditions. The T&C will incorporate the following data:
    a. the attributes to be included in the certificate: first name, middle name (if any), surname, name of the organisation that the user belongs to, user identifier and e-mail address;
    b. under the conditions and limitations of the applicable data protection law, central banks may require that certificate applicant provides on the T&C the attributes required to distinguish the person from others with the same name (see Section 3.2.3), namely, the number of a national recognized identity document, according to the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority, or the date and place of birth.
3. In the case that a Trusted Agent is in charge of identifying and authenticating the certificate applicant, he/she will add his/her hand-written signature to the T&C;
4. The RO4EO must validate the information included in the certificate request against the documentation provided by the certificate applicant, including the T&C. In the case that

the certificate applicant is not in front of him/her, the RO4EO will also validate that a valid Trusted Agent has signed the T&C;

5. The RO4EO, using the ESCB-PKI web interface, will either:
    a. Start the issuance of the certificate.
    b. Approve a remote download

   In both cases the certificate applicant will be requested to type a password to protect the keystore (file) to be generated with the certificate and its corresponding private key;
6. The RO4EO must securely archive all the documentation during the retention period described in section 5.5.2 of this CP:
    a. the terms and conditions application form signed by both, the certificate applicant and the person who identified and authenticated him/her (i.e. the Trusted Agent or the RO4EO himself/herself)
    b. under the conditions and limitations of the applicable data protection law, the Central Bank or National Competent Authority may choose to ask their RO4EO to retain a copy of the official identification document used to validate the certificate applicant's identity or, if this were not legally feasible, a copy of other identification document, preferable with the certificate applicant's photography;

4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

The validation of certificate requests will require face-to-face authentication of the certificate applicant or using means which provide equivalent assurance to physical presence.

The Registration Officer for External Organisations or a Trusted Agent will perform the certificate applicant's identification and authentication and will ensure that all the information provided is correct at the time of registration. The identification and authentication process will be done as specified in section 3.2.3 of this CP.

4.2.2 Approval or rejection of certificate applications

As specified in the ESCB-PKI CPS.

4.2.3 Time limit for processing the certificate applications

The Certification Authority shall not be held liable for any delays that may arise in the period between application for the certificate, publication in the ESCB-PKI repository and its delivery. As far as possible, the Certification Authority will process requests within 24 hours.

4.3 Certificate Issuance

4.3.1 Actions performed by the CA during the issuance of the certificate

As specified in the ESCB-PKI CPS.

4.3.2 CA notification to the applicants of certificate issuance

Applicants will be advised of the availability of the certificates via e-mail.

4.4 Certificate Acceptance

4.4.1 Form of certificate acceptance

Certificate applicants must confirm acceptance of the non-ESCB/non-SSM users' certificates and of its conditions by way of a hand-written signature of the terms and conditions application form.

4.4.2 Publication of the certificate by the CA

The ESCB-PKI CA publishes a copy of the non-ESCB/non-SSM user's certificates: i) in an internal LDAP directory located at the service provider's premises, only available to ESCB/SSM systems on a need-to-know basis, and ii) in the directory of the ESCB Identity and Access Management (IAM) service.

4.4.3 Notification of certificate issuance by the CA to other Authorities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Certificate subscribers' use of the private key and certificate

The certificates regulated by this CP may be used only to provide the following security services:

- Authentication certificates: authentication against ESCB/SSM applications.
- Encryption certificates: encryption of email messages and files.
- Signature certificates: digital signature of transactions, email messages and files.

4.5.2 Relying parties' use of the public key and the certificate

As specified in ESCB-PKI CPS.

4.6 Certificate Renewal

As specified in ESCB-PKI CPS.

4.7 Certificate Re-key

4.7.1 Circumstances for certificate renewal with key changeover

As specified in ESCB-PKI CPS.

4.7.2 Who may request certificate renewal?

Renewals must be requested by certificate subscribers.

4.7.3 Procedures for processing certificate renewal requests with key changeover

During the renewal process, the RO4EO will check that the information used to verify the identity and attributes of the certificate subscriber is still valid. If any of the certificate subscriber's data have changed, they must be verified and registered with the agreement of the certificate subscriber.

If any of the conditions established in this CP have changed, the certificate subscriber must be made aware of this and agree to it.
In any case, certificate renewal is subject to:

- Renewal must be requested in person at the places of registration, as established for initial issuance, as established in 4.1.2.
- Renewal of certificates may only be requested within the last 100 days of its lifetime.
- The CA not having certain knowledge of the existence of any cause for the revocation / suspension of the certificate.
- The request for the renewal of the provision of services being for the same type of certificate as the one initially issued.

4.7.4 Notification of the new certificate issuance to the subscriber

They are notified by e-mail.

4.7.5 Manner of acceptance of certificates with changed keys

As in the initial certificate issuance, they must sign the terms and conditions application form as a manner of acceptance of the certificates.

4.7.6 Publication of certificates with the new keys by the CA

The ESCB-PKI CA publishes a copy of the non-ESCB/non-SSM user's certificates: i) in an internal LDAP directory located at the service provider's premises, only available to ESCB/SSM systems on a need-to-know basis, and ii) in the directory of the ESCB Identity and Access Management (IAM) service.

4.7.7 Notification of certificate issuance by the CA to other Authorities

As specified in the ESCB-PKI CPS.

4.8 Certificate Modification

4.8.1 Circumstances for certificate modification

As specified in ESCB-PKI CPS.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

As specified in ESCB-PKI CPS.
Additionally, revoked ESCB/SSM users' certificates will be eliminated from the directories in which they are published.

4.9.2 Who can request revocation?

The CA or any of the RAs may, of their own initiative, request the revocation of a certificate if they become aware or suspect that the certificate subscriber's private key has been compromised, or in the event of any other factor that recommends taking such action.

Likewise, certificate subscribers may also request revocation of their certificates, which they must do in accordance with the conditions established under point 4.9.3.
The identification policy for revocation requests will be the same as that of the initial registration.

4.9.3 Procedures for requesting certificate revocation

The certificate subscribers or individuals requesting the revocation must appear before the RO4EO, identifying themselves and indicating the reason for the request.
The RO4EO shall always process the revocation requests submitted by its assigned subscribers. The request is made via an authenticated web Interface.
Apart from this ordinary procedure, PKI System registration officers may immediately revoke any certificate upon becoming aware of the existence of any of the causes for revocation.

4.9.4 Revocation request grace period

As specified in ESCB-PKI CPS.

4.9.5 Time limit for the CA to process the revocation request

Requests for revocation of certificates must be processed as quickly as possible, and in no case may said processing take more than 1 hour.

4.9.6 Requirements for revocation verification by relying parties

Verification of revocations, whether by directly consulting the CRL or using the OCSP protocol, is mandatory for each use of the certificates by relying parties.
Relying parties must check the validity of the CRL prior to each use and download the new CRL from the ESCB-PKI repository when the one they hold expires. CRLs stored in cache[7] memory, even when not expired, do not guarantee availability of updated revocation data.
For non-ESCB/non-SSM users' certificates, the ordinary validity verification procedure for a certificate shall be carried out with the ESCB-PKI Validation Authority, which shall indicate, through the OCSP protocol, the status of the certificate.

4.9.7 CRL issuance frequency

As specified in ESCB-PKI CPS.

4.9.8 Maximum latency between the generation of CRLs and their publication

The maximum time allowed between generation of the CRLs and their publication in the repository is 1 hour.

4.9.9 Online certificate revocation status checking availability

As specified in ESCB-PKI CPS.

[7]Cache memory: memory that stores the necessary data for the system to operate faster, as it does not have to obtain this data from the source for every operation**.** Its use could entail the risk of operating with outdated data.

4.9.10 Online revocation checking requirements

As specified in ESCB-PKI CPS.

4.9.11 Other forms of revocation alerts available

No stipulation.

4.9.12 Special requirements for the revocation of compromised keys

As specified in ESCB-PKI CPS.

4.9.13 Causes for suspension

Certificate suspension is the action that renders a certificate invalid for a period of time prior to its expiry date. Certificate suspension produces the discontinuance of the certificate's validity for a limited period of time, rendering it inoperative as regards its inherent uses and, therefore, discontinuance of the provision of certification services. Suspension of a certificate prevents its legitimate use by the subscriber.

Suspension of a certificate entails its publication on the public-access Certificate Revocation Lists (CRL).

The main effect of suspension as regards the certificate is that certificates become invalid until they are again reactivated. Suspension shall not affect the underlying obligations created or notified by this CP, nor shall its effects be retroactive.

Non-ESCB/non-SSM users' certificates may be suspended due to:

- Certificate subscriber's request, under suspicion of key compromise.

4.9.14 Who can request the suspension?

The subscribers of Non-ESCB/non-SSM users' certificates and Registration Officers for External Organisations.

4.9.15 Procedure for requesting certificate suspension

Certificate subscribers may immediately suspend his certificates via an authenticated Web Interface. Access will be granted by means of by means of one of the following mechanisms:

- an authentication certificate;
- an user ID and password for the ESCB Identity and Access Management (IAM) system;
- a suspension code (secret shared with the ESCB-PKI system)

4.9.16 Suspension period limits

The CA shall ensure that a certificate is not kept suspended for longer than is necessary to confirm its status.

Revocation will be processed immediately after receiving the certificate subscriber confirmation for revocation (see 4.9).

4.10 Certificate Status Services

As specified in ESCB-PKI CPS.

4.11 End of Subscription

As specified in ESCB-PKI CPS.

4.12 Key Escrow and Recovery

Not applicable.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

As specified in the ESCB-PKI CPS.

5.2 Procedural Controls

As specified in the ESCB-PKI CPS.

5.3 Personnel Controls

As specified in the ESCB-PKI CPS.

5.4 Audit Logging Procedures

As specified in the ESCB-PKI CPS.

5.5 Records Archival

5.5.1 Types of records archived

As specified in the ESCB-PKI CPS.

5.5.2 Archive retention period

The retention period for records related to non-ESCB/non-SSM users' certificates is 15 years, which is the legally mandated period according to the Spanish legislation.

5.5.3 Archive protection

As specified in the ESCB-PKI CPS.

5.5.4 Archive backup procedures

As specified in the ESCB-PKI CPS.

5.5.5 Requirements for time-stamping records

As specified in the ESCB-PKI CPS.

5.5.6 Audit data archive system (internal vs. external)

As specified in the ESCB-PKI CPS.

5.5.7 Procedures to obtain and verify archived information

As specified in the ESCB-PKI CPS.

5.6 Key Changeover

As specified in the ESCB-PKI CPS.

5.7 Compromise and Disaster Recovery

As specified in the ESCB-PKI CPS.

5.8 CA or RA Termination

As specified in the ESCB-PKI CPS.

6 Technical Security Controls

Technical security controls for internal ESCB-PKI components, and specifically those controls for Root CA and Online CA, during certificate issue and certificate signature processes, are described in the ESCB-PKI CPS.
In this paragraph technical security controls for the issuance of certificates under this CP are covered.

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Keys for non-ESCB/non-SSM users' certificates issued by the Online CA are generated under the following circumstances, depending on the certificate type:

- **Advanced certificates**, where all the following certificates will be stored in a smartcard or other cryptographic token:
  - Advanced authentication certificate. The corresponding key pair will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent.
  - Advanced signature certificate. The corresponding private key will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent.
  - Advanced signature certificate based on a SSCD. The corresponding private key will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent and to the SSCD (CWA 14169) specification.
  - Advanced encryption certificate without key archive. The key pair will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent, and no other copy will be archived.
- **Standard certificates**, where the private key will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification.

6.1.2 Delivery of private keys to subscribers

6.1.2.1 Advanced certificates

The private keys will be generated directly by the subscribers in their secure token and, therefore, no delivery is required.

6.1.2.2 Standard certificates

For standard certificates, the delivery of the private key to the certificate subscriber will be performed by means of an authenticated web interface. The certificate subscriber will receive the key pair in a file pursuant to the PKCS#12 specification protected with a password selected by him/her.

6.1.3 Delivery of the public key to the certificate issuer

In case of standard authentication certificates, public keys are generated by the ESCB-PKI Online CA, and therefore delivery to the certificate issuer is not applicable.

In the other cases, the public keys are generated by certificate subscribers on their cryptographic tokens and then delivered to the ESCB-PKI Online CA within the process required to obtain the certificate.

6.1.4 Delivery of the CA's public key to relying parties

The ESCB-PKI Online CA public key is included in the certificate of that CA. The ESCB-PKI Online CA certificate is not included in the certificate generated by the certificate subscriber. The ESCB-PKI Online CA certificate must be obtained from the repository specified in this document where it is available by certificate subscribers and relying parties to carry out any type of verification.

6.1.5 Key sizes

The key size of any non-ESCB/non-SSM users' certificate is 2048 bits.

6.1.6 Public key generation parameters and quality checks

Public keys are encoded pursuant to RFC 3280 and PKCS#1. The key generation algorithm is the RSA.

6.1.7 Key usage purposes (KeyUsage field in X.509 v3)

The 'Key Usage' and 'Extended Key Usage' fields of the certificates included in this CP are described in the 7.1.2.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

The Hardware Security Module (HSM) used for the creation of keys used by ESCB-PKI Online CA is pursuant to FIPS 140-2 Level 3.
Start-up of each one of the Certification Authorities, taking into account that a HSM is used, involves the following tasks:

a HSM module status boot up.
b Creation of administration and operator cards.
c Generation of the CA keys.

As regards the cryptographic token, they will be pursuant to the FIPS 140-2 level 3 or CC EAL4+ specification or equivalent. In the case of advanced signature certificates based on a SSCD, they will be also pursuant to the SSCD specification (CWA 14169).

6.2.2 Private key multi-person (k out of n) control

The private key, both for Root CA as for Subordinate CA, is under multi-person control; its activation is done through CA software initialisation by means of a combination of CA and HSM operators. This is the only activation method for said private key.
There is no multi-person control established for accessing the private keys of the certificates issued under this CP.

6.2.3 Escrow of private keys

Not applicable

6.2.4 Private key backup copy

Advanced certificates

The certificate subscribers cannot backup their certificates because the keys cannot be exported outside of the cards and these cannot be cloned.

Standard certificates

The certificate subscribers will have to keep the PKCS#12 file and corresponding protection password as a backup copy.

6.2.5 Private key archive

Advanced certificates

The private keys are generated on cryptographic cards, they are not exported under any circumstances, and access to operations with said cards is protected by a PIN code.

Standard certificates

ESCB-PKI will not keep any archive of the private key associated to standard certificates.

6.2.6 Private key transfer into or from a cryptographic module

Advanced certificates

Provided that the private key is generated inside the cryptographic token there is no transmission of this key to or from any cryptographic module.

Standard certificates

No stipulated

6.2.7 Private key storage in a cryptographic module

Advanced certificates

Private keys are created on the cryptographic token and are stored there

Standard certificates

Private keys are created in the ESCB-PKI Online CA's cryptographic module, but they are not subsequently saved.

6.2.8 Private key activation method

Advanced certificates

Private keys are stored in a cryptographic token protected with a PIN code that is required to activate the keys.

Standard certificates

Private keys are delivered in a PKCS#12 file, protected by a password. The password is required to activate the private key.

6.2.9 Private key deactivation method

Advanced certificates

Private keys can be deactivated by removing the card from the reader.

Standard certificates

No stipulation.

6.2.10 Private key destruction method

Advanced certificates

Private keys can be destroyed by destroying the cryptographic token.

Standard certificates

No stipulation.

6.2.11 Cryptographic module classification

The cryptographic modules used by ESCB-PKI technical components comply with the FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archive

As specified in the ESCB-PKI CPS.

6.3.2 Operational period of certificates and usage periods for key pairs

All certificates and their linked key pair have a lifetime of 3 years, although the ESCB-PKI Online CA may establish a shorter period at the time of their issue.

6.4 Activation Data

As specified in the ESCB-PKI CPS.

6.5 Computer Security Controls

As specified in the ESCB-PKI CPS.

6.6 Life Cycle Security Controls

As specified in the ESCB-PKI CPS.

6.7 Network Security Controls

As specified in the ESCB-PKI CPS.

6.8 Timestamping

As specified in the ESCB-PKI CPS.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version number

Certificates for the non-ESCB/non-SSM users are compliant with the X.509 version 3 (X.509 v3) standard.

7.1.2 Certificate extensions

The certificate extensions used generically are:

- *Subject Key Identifier*. Classified as non-critical.
- *Authority Key Identifier*. Classified as non-critical.
- *KeyUsage*. Classified as critical.
- *extKeyUsage*. Classified as non-critical.
- *CertificatePolicies*. Classified as non-critical.
- *SubjectAlternativeName*. Classified as non-critical.
- *BasicConstraints*. Classified as critical.
- *CRLDistributionPoint*. Classified as non-critical.
- *Auth. Information Access*. Classified as non-critical.
- escbUseCertType *(0.4.0.127.0.10.1.3.1)*. Classified as non-critical.

For understanding purposes, all ESCB-PKI OID attributes references are made under the [OID ESCBPKI] mark, which corresponds to 0.4.0.127.0.10.1.

7.1.2.1 Advanced authentication certificate

Advanced authentication certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 [Registration Organisation Country] EUROPEAN SYSTEM OF CENTRAL BANKS Organisation within which user is member User identifier (UID) [AUT:A] Name Middle name Surnames	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature[8] Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 0 0 1 0 0	Yes
extKeyUsage	 clientAuth (1.3.6.1.5.5.7.3.2) smartCardLogon (1.3.6.1.4.1.311.20.2.2) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies Policy Identifier	 *[OID ESCBPKI]*.2.3.1	

[8] This usage is allowed in the scenarios where a digital signature is generated to authenticate the certificate subscriber

URL CPS	*[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4) RegisteredID (*[OID ESCBPKI]*.1.7)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers Ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbUseCertType	AUTHENTICATION	

7.1.2.2 Advanced signature certificate and advanced signature certificate based on a SSCD

Advanced signature certificate and SSCD signature certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Organisation within which user is member* *User identifier (UID)* [SIG:Q] *Name Middle name Surnames* *OR* [SIG:A] *Name Middle name Surnames* [9]	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 0 1 0 0 0 0 0	Yes
extKeyUsage	 emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	

[9] *[SIG:Q]* in case of advanced signature certificates based on a SSCD
[SIG:A] in case of advanced signature certificates

Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.3.4 OR *[OID ESCBPKI]*.2.3.5[10] *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4) RegisteredID (*[OID ESCBPKI]*.1.7)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers Ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
qcStatements	 id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) Id-etsi-qcs-QcSSCD[11] (0.4.0.1862.1.4)	
[ESCB] Extensions		
escbUseCertType	SIGNATURE	

[10] *[OID ESCBPKI]*.2.3.4 in case of advanced signature certificates based on a SSCD.
[OID ESCBPKI].2.3.5 in case of advanced signature certificates.
[11] Only in the case of advanced signature certificates based on a SSCD.

7.1.2.3 Advanced encryption certificate

Advanced encryption certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Organisation within which user is member* *User identifier (UID)* [ENC:A] *Name Middle name Surnames*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 0 0 1 1 0 0 0	Yes
extKeyUsage	 emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.3.2 *[CPS-URL]*	
Subject Alternative Names rfc822	 *Subject's Email*	

RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4) RegisteredID (*[OID ESCBPKI]*.1.7)	*Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbUseCertType	ENCRYPTION	

7.1.2.4 Standard authentication certificate

Standard authentication certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before the publication of this document) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Organisation within which user is member* *User identifier (UID)* [AUT:S] *Name Middle name Surnames*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature[12] Non Repudiation Key Encipherment[13] Data Encipherment[10] Key Agreement Key Certificate Signature CRL Signature	 1 0 1 1 1 0 0	Yes
extKeyUsage	 clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) anyExtendedKeyUsage (2.5.29.37.0)	
Certificate Policies		

[12] This usage is allowed in the scenarios where a digital signature is generated to authenticate the certificate subscriber
[13] keyEncipherment and dataEncipherment are allowed for emailProtection only. The private key is never stored in the Key Archive.

Policy Identifier URL CPS	*[OID ESCBPKI]*.2.3.6 *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4) RegisteredID (*[OID ESCBPKI]*.1.7)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	AUTHENTICATION	

7.1.3 Algorithm Object Identifiers (OID)

Cryptographic algorithm object identifiers (OID):
SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

7.1.4 Name formats

Certificates issued by ESCB-PKI contain the X.500 distinguished name of the certificate issuer and that of the subject in the issuer name and subject name fields, respectively.

7.1.5 Name constraints

See section 3.1.1.

7.1.6 Certificate Policy Object Identifiers (OID)

The OIDs for this CP are the following[14]:

[OID ESCBPKI].2.3.0.X.Y: Certificate policies for the non-ESCB/non-SSM users' certificates (this document)

[OID ESCBPKI].2.3.1.X.Y: Certificate Policy of Advanced Authentication certificate for non-ESCB/non-SSM users

[OID ESCBPKI].2.3.2.X.Y: Certificate Policy of Advanced Encryption certificate for non-ESCB/non-SSM users

[OID ESCBPKI].2.3.4.X.Y: Certificate Policy of Advanced Signature certificate based on a SSCD for non-ESCB/non-SSM users

[OID ESCBPKI].2.3.5.X.Y: Certificate Policy of Advanced Signature certificate for non-ESCB/non-SSM users

[OID ESCBPKI].2.3.6.X.Y: Certificate Policy of Standard Authentication certificate for non-ESCB/non-SSM users

Where:

- [OID ESCBPKI]: represents the OID 0.4.0.127.0.10.1
- X.Y indicate the version.

7.1.7 Use of the "PolicyConstraints" extension

As specified in the ESCB-PKI CPS.

7.1.8 Syntax and semantics of the "PolicyQualifier

The Certificate Policies extension contains the following Policy Qualifiers:

- URL CPS: contains the URL to the CPS and to the CP that govern the certificate.

The content for certificates regulated under this policy can be seen in point *7.1.2 Certificate extensions*.

[14] The OID [OID ESCBPKI].2.3.3 y not used

7.1.9 Processing semantics for the critical "CertificatePolicy" extension

As specified in the ESCB-PKI CPS.

7.2 CRL Profile

As specified in the ESCB-PKI CPS.

7.3 OCSP Profile

As specified in the ESCB-PKI CPS.

8 Compliance Audit and Other Assessment

As specified in the ESCB-PKI CPS.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

ESCB-PKI will not charge any direct fee to the certificate subscribers for the issuance or renewal of non-ESCB/non-SSM users' certificates.

9.1.2 Certificate access fees

Access to certificates issued under this Policy is free of charge and, therefore, no fee is applicable to them.

9.1.3 Revocation or status information fees

Access to information on the status or revocation of the certificates is open and free of charge and, therefore, no fees are applicable.

9.1.4 Fees for other services, such as policy information

No fee shall be applied for information services on this policy, nor on any additional service that is known at the time of drawing up this document.

9.1.5 Refund policy

Not applicable.

9.2 Financial Responsibility

As specified in the ESCB-PKI CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

As specified in the ESCB-PKI CPS.

9.3.2 Non-confidential information

As specified in the ESCB-PKI CPS. Moreover, a copy of the non-ESCB/non-SSM users' certificates is published in the directory of the ESCB Identity and Access Management (IAM) service.

9.3.3 Duty to maintain professional secrecy

As specified in the ESCB-PKI CPS.

9.4 Privacy of Personal Information

As specified in the ESCB-PKI CPS.

9.4.1 Personal data protection policy

As specified in the ESCB-PKI CPS.

9.4.2 Information considered private

As specified in the ESCB-PKI CPS.

9.4.3 Information not classified as private

As specified in the ESCB-PKI CPS.

9.4.4 Responsibility to protect personal data

As specified in the ESCB-PKI CPS.

9.4.5 Notification of and consent to the use of personal data

The mechanisms to notify certificate applicants and, when appropriate, obtain their consent for the processing of their personal data is the terms and conditions application form.

9.4.6 Disclosure within legal proceedings

As specified in the ESCB-PKI CPS.

9.4.7 Other circumstances in which data may be made public

As specified in the ESCB-PKI CPS.

9.5 Intellectual Property Rights

As specified in the ESCB-PKI CPS.

9.6 Representations and Warranties

As specified in the ESCB-PKI CPS.

9.7 Disclaimers of Warranties

As specified in the ESCB-PKI CPS.

9.8 Limitations of Liability

As specified in the ESCB-PKI CPS.

9.9 Indemnities

As specified in the ESCB-PKI CPS.

9.10 Term and Termination

9.10.1 Term

This CP shall enter into force from the moment it is approved by the PAA and published in the ESCB-PKI repository.

This CP shall remain valid until such time as it is expressly terminated due to the issue of a new version, or upon re-key of the Corporate CA keys, at which time it is mandatory to issue a new version.

9.10.2 CP substitution and termination

This CP shall always be substituted by a new version, regardless of the importance of the changes carried out therein, meaning that it will always be applicable in its entirety.

When the CP is terminated, it will be withdrawn from the ESCB-PKI public repository; nevertheless it will be kept for 15 years.

9.10.3 Consequences of termination

The obligations and constraints established under this CP, referring to audits, confidential information, ESCB-PKI obligations and liabilities that came into being whilst it was in force shall continue to prevail following its substitution or termination with a new version in all terms which are not contrary to said new version.

9.11 Individual notices and communications with participants

As specified in the ESCB-PKI CPS.

9.12 Amendments

As specified in the ESCB-PKI CPS.

9.13 Dispute Resolution Procedures

As specified in the ESCB-PKI CPS.

9.14 Governing Law

As specified in the ESCB-PKI CPS.

9.15 Compliance with Applicable Law

As specified in the ESCB-PKI CPS.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement clause

As specified in the ESCB-PKI CPS.

9.16.2 Independence

Should any of the provisions of this CP be declared invalid, null or legally unenforceable, it shall be deemed as not included, unless said provisions were essential in such a way that excluding them from the CP would render the latter without legal effect.

9.16.3 Resolution through the courts

As specified in the ESCB-PKI CPS.

9.17 Other Provisions

As specified in the ESCB-PKI CPS.

NBB - Payments and Securities Service
Securities Settlement System
boulevard de Berlaimont 14
1000 Brussels (Belgium)
Phone: + 32 (0)2 221 36 00
sss@nbb.be

Sub-Annex 8.3

Trusted agent for the NBB-SSS Registration Authority: Terms and conditions

1. Scope

In accordance with Article 6.2.1.1.2 of the "Terms and conditions for the participation in the NBB-SSS", any Participant can send instructions manually and can send data to or receive information from the NBB-SSS in U2A modus and in pull and push mode through the RAMSES GUI, having a connection with which is in principle mandatory for each Participant.

The conditions of use of the RAMSES GUI, including the related certificates and tokens, are described in Annex 8 of the Terms and conditions. Article 4.2.2 of the said Annex 8 provides that the NBB, in its role of verification authority, needs to deliver the Tokens against written receipt, either physically, by postal mail or by courier. In principle, the Token should be directly delivered by the NBB to the Certificate applicant, but in many cases such physical delivery raises practical problems or appears materially impossible. In such cases, the Token needs to be delivered, either physically, by postal mail or by courier, by the NBB to a Participant's member entrusted, in the framework of the Participant's organisation, to verify the identity of the Certificate user before physically delivering the Token to the latter on behalf of the NBB acting as verification authority in accordance with the CPS and the CP. For this reason, Article 4.2.3 of Annex 8 provides that each Participant needs to appoint at least one (preferably two or more) Trusted agent among the Participant's members in order to materially exert, on the basis of a power of attorney delivered by the NBB, the competence to verify the identity of the Certificate user on behalf of the NBB before physically delivering the Token to the said Certificate user.

This sub-Annex 3 defines the terms and conditions of the power of attorney delivered by the NBB to the Trusted agent appointed by the Participant for the above mentioned purpose.

2. Definitions

Unless otherwise stated, the terms in this sub-Annex shall follow the definitions as provided for in Article 2 of the Terms and conditions, in Article 2 of Annex 8 and in the sub-Annexes 8.1 and 8.2 of the Terms and conditions.

3. Terms and conditions

3.1 Principle

In the framework of the operation of the RAMSES GUI, the NBB relies on the ESCB-PKI certificates and services. When carrying out the tasks of the NBB acting as Registration authority as described in Annex 8 of the Terms and conditions, the CPS and the CP, the Trusted agent shall similarly comply with the terms of Annex 8, the CPS and the CP.

Trusted agents will not have automated interfaces with the NBB acting as Registration authority.

3.2 Roles and responsibilities of the Participant and of the Trusted agent

The Participant and the Trusted agent shall carry out all the tasks and assume all the responsibilities corresponding to their role as Trusted agent as defined above and as described in more detail in the CPS and the CP. In performing their obligations under these terms and conditions, the Participant and the Trusted agent shall be bound by the CPS, the CP and any security measure implemented and required by the NBB. They shall fulfil their obligations in accordance with the applicable national laws and regulations and shall take the utmost care to mitigate any loss or damage.

The Participant shall verify that the Trusted agent has signed the present sub-Annex 8.3 of the Terms and conditions, and shall send the duly signed form to the NBB.

The Trusted Agent shall:

a) deliver to the NBB a written receipt for the Tokens received from the NBB;
b) identify each Certificate applicant by physically checking their identity against a physical person;
c) validate the documentation required during the identification process by requesting the submission by the Certificate's applicant of any official document that evidences the Certificate applicant's identity, at least on the basis of a Certificate applicant's recent photography, and that has legal validity in Belgium. Hence, the acceptable documents must be either a valid and not expired passport or national identity card,
d) countersign the Certificate application form signed by the Certificate applicant;
e) deliver to the duly identified Certificate applicant the envelope containing one Token, its initial PIN code and its PUK code, as well as the data needed for the Certificate applicant to download its certificate from the ESCB-PKI website.

Together with the Trusted agent, the Participant shall be responsible for the performance of the above mentioned identity verification and Token delivery tasks by the Trusted agent and bears the exclusive responsibility for the use of the said Tokens in order to sign and send instructions in the Participant's name as soon as the Trusted agent has delivered to the NBB a signed receipt of the concerned Tokens.

3.3 Liability

The Participant shall be liable toward other Participants and third parties, if any, for any misinformation, mistakes, losses or damages arising as a result of any deliberate or negligent action and/or omission of the Trusted agent in the performance of its obligations under these terms and conditions as soon as the Trusted agent has delivered to the NBB a signed receipt of the concerned Tokens. Therefore, the NBB shall not incur any liability for any damage resulting from a possible misuse of the said Tokens as from the same moment in time.

3.4 Confidentiality and personal data protection

3.4.1 Confidentiality protection

The Participant and the Trusted agent shall keep confidential all sensitive, secret or confidential information or know-how (whether such information is of a commercial, financial, regulatory, technical or other nature) that is marked as such and belongs to the ESCB-PKI and/or the NBB or which the ESCB-PKI and/or the NBB has a lawful right to use, and shall not disclose such matters to any third party without the express, prior and written consent of the ESCB-PKI and/or the NBB.

The Participant shall restrict access to the information or know-how referred to in the previous paragraph to the appointed Trusted Agent, and such access shall only be permitted in cases of explicit operational need. The Participant shall take all appropriate measures to prevent access to such confidential information or know-how by persons other than the appointed trusted agent.

The duty of confidentiality under this Article does not apply where disclosure is:

a) warranted by the defence of the Participant's legitimate interests in court proceedings, arbitration or similar legal proceedings; or

b) required by law.

3.4.2 Personal data protection

The Trusted Agent hereby acknowledges:

- the processing by the NBB of the following personal data with the sole purpose of identifying the Trusted Agent: name, surname, e-mail address, and identity of the Participant by which it is appointed as Trusted Agent;
- the fact that the NBB is the sole responsible entity for the said processing of personal data;
- the NBB's complete address, as mentioned in the header of this form;
- the Trusted Agent's personal rights to consult and correct the above mentioned personal data processed by the NBB;
- the fact that these personal data shall be irrecoverably removed from the NBB's files one year after the revocation by the Participant of the Trusted Agent's appointment;
- the transmission to the NBB of a copy of a valid and not expired identity document (passport, national identity card, or equivalent official document) evidencing the Trusted agent's identification, which clearly and readably mentions the Trusted Agent's name and surname.

Access to the above mentioned personal data shall be granted only to those with an official need to know.

4. Identification data

Representative entitled to validly commit the NBB
First name:
Surname:
Title or capacity:
Participant's data
Organisation's name:
BIC11:
Address:

Representative(s) entitled to validly commit the Participant
First name:
Surname:
Title or capacity:

Trusted agent's data
First name:
Surname:
E-mail address:

By signing this document, the representative entitled to validly commit the Participant and the Trusted Agent irrevocably agree to the Terms and conditions, the terms of Annex 8 thereof, the CPS, the CP and the present terms and conditions.

Made in Brussels on ..... in two original versions, one intended for the NBB and one intended for the Participant.

Name and signature of the NBB's representative	Name and signature of the Participant's representative

Name and signature of the Participant's Trusted agent

Please attach to this document copies of the appointed Trusted Agent's valid passport or national identity card (or equivalent official document).

NBB-NET

TERMS AND CONDITIONS

1. DEFINITIONS

For the purpose of this document:

- "**Customer**" means any person needing to have a remote access to specific IT-applications or platforms hosted and operated by the NBB as a consequence either of its membership of a non-profit association in the financial sector, of a co-operation agreement scheme set up by the NBB or to which the NBB adheres, of a legal obligation or of any other professional reason;
- "**NBB**" means the NATIONAL BANK OF BELGIUM, a public limited company by shares created by law, having its registered office at de Berlaimontlaan 14, B-1000 Brussels, registered in the legal entities repository of Brussels under the enterprise number 0203.201.340, VAT number BE 0203.201.340;
- "**NBB-Net**" means a TCP/IP secured data transport network set up by the NBB with the aim to provide for a state-of-the-art connection channel between the NBB and its professional clients over the Internet, a private MPLS cloud[1] or a legacy leased line[2], including the services provided by the NBB in order to set up, operate and maintain this network;
- "**Starter Box**" means an encryption device (router) composed of both hardware[3] and software components that is initially pre-configured and further managed by the NBB in function of the technical environment of the Customer in such a way that the said device is ready for use by the client ("plug and play");
- "**Terms and conditions**" means the present terms and conditions on the provision by the NBB of the NBB-Net, as well as the most recent version of all documents to which this document specifically refers, even if they are not materially attached as an annex to this document;
- "**Turn key**" means a managed solution owned and maintained by NBB up to the encryption box at the Customer's premises. The transport network used with this solution is the private MPLS cloud.

2. SCOPE

The scope of these Terms and conditions is strictly limited to NBB-Net and ancillary services like "Turn key" and "Starter". Therefore, this scope does not extend to:

- the use of the IT-applications or platforms to which access is granted through the NBB-Net connection, which is covered by specific terms and conditions,
- Customer's use of a legacy leased line agreed upon with Belgacom or Colt, or of a broad bandwidth connection with the internet via a provider freely selected by the Customer. The Customer is exclusively responsible for the implementation and maintenance at his own cost of

---

1 MPLS stands for « Multi Protocol Label Switching ». The private MPLS cloud for NBB-Net is currently provided and operated by Colt.

2 This solution, deprecated by the NBB, is no longer available for new connections with NBB-Net.

3 Currently : Cisco router, model CISCO881-K9. The choice of the devices can be modified at any time by the NBB in order to stick with the technical evolution and state-of-the-art.

such a leased line or of such an access to the internet[4]. Therefore, the NBB shall not overtake any technical, contractual, financial and/or legal constraint whatsoever regarding the leased line or the internet access services subscribed by the Customer and shall not be bound by the terms, conditions, technical features and limitations whatsoever agreed with the Customer's concerned service provider.

2.1. NBB-NET

The technical documentation about NBB-Net is available on the website of the NBB, at the following address: http://www.nbb.be/doc/EL/NBB-Net.pdf. This technical documentation is an integral part of the Terms and conditions and its respect by the Customer is mandatory.

The technical features of NBB-Net may be unilaterally modified by NBB at any time in order to stick with the technical evolution and state-of-the-art, operational experience, feedback and enhancement proposals provided by the Customers. However, major changes that may have a substantial impact on the Customers' IT infrastructure shall only be implemented after due notification to the Customers.

Encryption is mandatory for all transport of data via NBB-Net.

NBB-Net makes use of one of the following, TCP/IP-based connectivity media:

- Colt MPLS network,
- legacy leased lines, or
- a broad bandwidth connection over the internet.

2.1.1. COLT MPLS NETWORK

The physical underlying transport channel of the Colt MPLS network is a Virtual Private network provided via optical fibres[5] throughout Europe by the network operator Colt, which has been appointed by the NBB via a public procurement procedure. Although it provides for the data transport network, Colt is a sub-contractor of the NBB and is no Party to the present Terms and conditions. Therefore, the NBB assumes alone all contractual and legal aspects of the MPLS solution. This means that the Customer needs in all cases to contact the NBB for any issue regarding the MPLS solution, including troubleshooting and incidents, and is therefore not allowed to directly contact Colt for such matters, even with regard to his locally installed loop(s).

The optional « Turn key » solution (see below, Clause 2.2) is only available for Customers making use of the Colt MPLS Network.

The MPLS infrastructure set up at NBB-side is dedicated to NBB-Net and is thus not shared with other IT-solutions.

2.1.2. LEGACY LEASED LINES

The physical underlying transport channel is a specific leased line installed by Belgacom or Colt. No new leased lines will be installed with the NBB, so that this service is only performed in favour of Customers who dispose of a legacy leased line already used previously in the frame of the remote access to NBB applications and platforms.

The leased line infrastructure set up at NBB-side is dedicated to NBB-Net and is thus not shared with other IT-solutions.

2.1.3. BROAD BANDWIDTH CONNECTION OVER THE INTERNET

The physical underlying transport channel is an internet access provided by an Internet provided selected by the Customer under his responsibility and at his own costs.

---

4 It goes without saying that the NBB is exclusively responsible for the implementation and maintenance of its own access to the internet, which goes via two different internet service providers.

5 Excepted the last mile to the Customer's premises, which can be in copper cable.

The optional « Starter » solution (see below, Clause 2.3) is only available for Customers making use of such a broad bandwidth connection over the internet.

The broad bandwidth Internet connections set up at NBB-side are not exclusively dedicated to NBB-Net but are shared with other NBB IT-solutions and applications such as NBB-mails, internet site, access to public NBB-applications, etc.).

2.2. "TURN KEY"

"Turn key" is an optional service provided by the NBB on top of the Colt MPLS Network as NBB-Net connectivity medium.

"Turn key" consists of the NBB taking on its account the procurement, installation, monitoring and possible debugging of the Colt MPLS infrastructure and the encryption devices (routers) needed for the setup of the connection with NBB-Net. The NBB sub-contractor for the management of the encryption devices is currently Belgacom. The NBB is also responsible for reporting possible incidents to Colt and/or Belgacom for the incident solving (relating to software as well as hardware), however within the limits of its technical possibilities and available knowledge of the Colt MPLS network, and for the operation of a Single Point of Contact (SPOC) in case of incident or fallout of the MPLS network or encryption devices.

"Turn key" is an ancillary service of NBB-Net that is provided on explicit request of the Customer. It is not available outside the framework of the NBB-Net service.

2.3. "STARTER"

"Starter" is an optional service provided by the NBB to Customers having selected a broad bandwidth connection over the Internet as NBB-Net connectivity medium.

"Starter" consists in the delivery by the NBB to the Customer of one or more[6] pre-configured Starter Boxes as well as the automated pro-active monitoring[7], the further technical assistance by phone and by e-mail for installation completion, the provision, as far as reasonably possible[8], of a remote intervention by the NBB on a Starter Box that is not working properly, and its replacement by a new Service box in accordance with Clause 5.2. The Customer is informed in advance of a possible remote intervention carried out by the NBB and of the period during which this intervention can take place. Automated pro-active monitoring shall be performed by NBB until the Customer notifies to the NBB its wish to terminate this specific provision of service.

The technical assistance of the NBB ceases as soon as the configuration setup has been completed successfully or if the Customer unilaterally modifies the initial configuration of the Starter Box, which requires the communication by the NBB on demand of the Customer of the password locking the configuration of the Starter Box.

The NBB provides, on a case by case-basis, a prior advice to the Customer relating to the optimal number of Starter Boxes to be delivered. However, this number is defined by the Customer self, under its own responsibility.

"Starter" is an ancillary service of NBB-Net that is provided on explicit request of the Customer. It is not available outside the framework of the NBB-Net service.

---

6 If deemed necessary, the Customer may order a spare Starter Box in order to allow faster recovery from failure of an operational Starter box.

7 SNMP polling, sending of traps to NBB and periodic backup of the software configuration.

8 Indeed, the possibility of a remote technical intervention by NBB on the Starter Box is rather limited due to the fact that the NBB has no physical access, and even no logical access, to the Customer's Starter Box or IT-infrastructure.

3. ORDER

The Customer places an order by sending back to the NBB the duly completed and signed Order form available on the internet site of the NBB, at the following address: http://www.nbb.be/doc/EL/NBB-Net_Order_form.pdf.

By sending back a duly completed and signed Order form, the Customer acknowledges his full adherence with the present Terms and conditions, which become applicable as from the date of their signature by the Customer.

4. FINANCIAL REGIME

4.1. FEES

The NBB charges fees to the Customer in retribution of the basic and optional NBB-Net services. These fees reflect the NBB actual costs (NBB internal costs, network operators' or subcontractors' expenses and costs entailed by other third parties' provisions of services) and are therefore updated each year, in principle on the 1st of January, in order to be adjusted to the NBB's actual cost level.

The yearly actualised list of tariffs is available on the website of the NBB, at the following address: http://www.nbb.be/doc/EL/NBB-Net_tariffs.pdf.

4.1.1. NBB-NET

The retribution of the NBB-Net services provided by the NBB consists of:

a) a periodic fee calculated per physical connection channel (*i.e.* per leased line, per MPLS end point and per Internet connectivity) and per half year; in some cases (MPLS network, leased line), the level of such fee depends of the maximum data transfer capacity requested by the Customer;
b) "one-shot" installation costs in the case of the MPLS network, the amount of which is calculated by Colt in view of the Customer's specific situation.

4.1.2. "TURN KEY"

The retribution of the optional "Turn key" services provided by the NBB consists of:

a) a periodic fee calculated per encryption device and per half year;
b) "one-shot" installation costs of the encryption device.

4.1.3. "STARTER"

The retribution of the optional "Starter" services provided by the NBB consists of a periodic fee calculated per delivered Starter Box and per half year.

4.2. INVOICING

The fees shall be invoiced to the Customer:

- immediately after the performance of the concerned services, when they relate to installation costs ("one shot" costs, see Clause 4.1 above),
- in June and in December of each civil year, when they relate to recurrent provisions of services which are charged on a half-yearly basis (see Clause 4.1 above). The invoice issued in June refers to the provision of services during the first semester of the running civil year, the invoice issued in December during the second semester of the running civil year. If the Customer subscribes to NBB-Net, and possibly the ancillary services "Turn key" or "Starter" in the course of a semester, the fee relating to the said semester shall be calculated on a *pro rata temporis* basis.

4.3. PAYMENT

Invoiced amounts must be paid by the Customer in euro within thirty (30) days after their issuance, on the bank account number mentioned on these invoices, whereby all costs related to this payment will be exclusively borne by the Customer. In case of delayed payment, penalties are due in accordance

with the Belgian law d.d. 2 August 2002 regarding the fight against belated payments of commercial transactions.

Any tax and right applicable to the services performed by the NBB in accordance with the national law of any of the Parties, including the VAT, shall be exclusively borne by the Customer.

5. LIABILITY REGIME

5.1. GENERAL LIABLITY REGIME

The Parties shall carry out their obligations arising out of the Terms and conditions in good faith. In performing their respective obligations under the Terms and conditions, the Parties shall be bound by a general duty of reasonable care in relation to each other. Each Party shall take all reasonable and practical measures to mitigate possible loss or damage to the other Party.

The NBB warrants that it shall deliver professional, state-of-the-art services to the Customer, however without any warranty regarding mandatory results to be reached.

The NBB shall be liable to reimburse to and/or indemnify the Customer for any evidenced loss, liability and/or expense incurred by the Customer which has been caused by the NBB's misconduct or negligence, whereby the burden of evidencing the invoked misconduct or negligence lays on the Customer. However, excepted in case of wilful misconduct or negligence:

- the NBB shall not be liable towards the Customer for indirect, incidental, special or consequential damage, including but not limited to: harm to the level of services provided by Customer, loss of business, loss of profit, loss of data, reputational damage, etc. arising out of or in connection with the NBB-Net services or the ancillary "Turn key" and "Starter" services,
- without prejudice to Clause 5.2, the total amount of the reimbursement and/or indemnification to be paid by the NBB to the Customer for damages occurred during a given civil year shall under no circumstance whatsoever exceed the amount of the fees paid by the said Customer to the NBB during the said civil year.

Moreover, the NBB shall not be liable for delay in performing or failure to perform any of its obligations under the Terms and conditions if the delay or failure results from a slight misconduct or negligence, or from events or circumstances outside its reasonable control. For the application of this rule:

- "slight misconduct or negligence" is understood as any misconduct or negligence that can reasonably be expected still to take place in spite of the normal care and precaution expected from a professional provider of IT-services,
- "circumstances outside its reasonable control" are understood as *force majeure*, mandatory regulation passed or actions carried out by the public authority, and the unpredictable actions or negligence of a third party, including the NBB's sub-contractors. In particular, no liability shall be vested with the NBB when the delay in performing or failure to perform its obligations results from an action, omission, delay, failure or denial of service of the Customer's internet access provider in the performance of its own obligations towards the Customer. Each Party shall inform the other Party without delay of any such actual or imminent failure, and use its best efforts to solve it as soon as reasonably possible. Furthermore, as regards the Colt MPLS network, the NBB cannot grant further terms of services than those granted by Colt itself to NBB.

Any Customer seeking indemnification by the NBB of any damage shall explicitly request the reimbursement and/or indemnity in writing by means of a registered postal mail, and shall add to its claim the evidence relating to both the misconduct or the negligence and of the invoked damage. No claim, regardless of form, arising out of the Terms & Conditions may be validly introduced by the Customer more than two (2) years after the cause of action became known to the Customer.

5.2. SPECIFIC LIABLITY REGIME FOR THE "STARTER" SERVICE

As an exception to Clause 5.1, the total amount of the reimbursement and/or indemnification to be paid by the NBB to the Customer for damages occurred during a given civil year which are entailed by a misconduct or negligence in the provision of the Starter service shall under no circumstance

whatsoever exceed the amount of the fees paid by the Customer to the NBB during the said civil year for the provision of the Starter service.

The NBB shall replace, as soon as reasonably possible, a Starter Box which does not work, or does not work properly anymore, despite possible remote interventions performed by the NBB as referred to in Clause 2.3. In such case, the Customer may need:

a) to install the second, properly pre-configured Starter Box at its disposal and deploy it in production environment, in order to keep the connection with NBB-Net running, and

b) to send a formal notice of the falldown of the Starter Box to the NBB and to send the faulty Starter Box to the NBB at its own cost. Upon receipt of the faulty Starter Box, the NBB sends at its own cost a new pre-configured Starter Box to the Customer with a fast shipping company;

6. OWNERSHIP AND INTELLECTUAL PROPERTY RIGHTS

The present Terms and conditions do not result in any transfer of property right or any other right whatsoever in any tangible of intangible asset of NBB or its agents and subcontractors to the Customer. However, the NBB grants to the Customer, to the extent feasible under applicable legislation, all licences regarding the intellectual property rights required to enable the Customer to use the NBB-Net service and the ancillary "Turn key" and "Starter" services, in particular the Starter Box and its software components.

The Starter Box remains the sole property of the NBB and is fully dedicated to the NBB-Net connection. It may not be recycled, destroyed, sold, leased, alienated or used by the Customer for any other purpose without prior written agreement of the NBB.

7. EFFECTIVENESS, DURATION AND TERMINATION

In accordance with Clause 3, these Terms and conditions become effective from the date of their signature by the Customer of the Order form.

The NBB-Net service and the ancillary services "Turn key" and "Starter" are concluded for an undefined period of time, but shall encompass a minimum duration of one full calendar year.

Subject to the mandatory respect of the said minimum duration, each Party shall be entitled to terminate the NBB-Net service, or to terminate the "Turn key" or "Starter" service while continuing the NBB-Net service, at the end of any civil year, without need of any justification and without indemnification but subject to the sending of a termination notice to the other Party, at least six months in advance. Such termination notice shall be sent to the other Party by means of a registered postal mail in order to be legally valid and shall specify whether the termination concerns the NBB-Net service as a whole or only the "Turn key" or the "Starter" service.

The extraordinary right of a Party to terminate the provision of the services if the other Party does not fulfil its own contractual duties pursuant to Article 1184 of the *Belgian Civil Code* shall remain unaffected.

The Customer having subscribed to the "Starter" service must send back the Starter Boxes in his possession to the NBB or its agent not later than the first working week following the termination date, at its own cost. The NBB is empowered as by law and without prior notification to replace the Starter Boxes which have not been received from the Customer within two weeks after the termination date, by purchasing a new encryption device for each Starter Box that have not been received, at the exclusive cost of the Customer that shall refund the said cost on first demand of the NBB.

The termination of the NBB-Net service for any reason whatsoever shall not affect provisions on the following items:
(a) Clause 5: Liability
(b) Clause 6: Ownership and property rights, and
(c) Clause 9: Applicable law and dispute resolution.

8. MISCELLANEOUS PROVISIONS

8.1. NOTICES

Without prejudice to specific diverging provisions in these Terms and conditions, any notice sent by the Parties shall be in writing (fax, post, or any other durable means of communication, including e-mail) and in English.

8.2. WAIVER

A failure or delay in exercising any right or remedy under the Terms and conditions shall not operate as a waiver of, and accordingly shall not preclude or limit any future exercise of, that right or remedy.

8.3. SEVERABILITY AND SURVIVAL

Should a provision of the Terms and conditions be or become invalid, illegal or unenforceable, the other provisions of the Terms and conditions shall remain valid, legal and enforceable.

8.4. TRANSFER OF RIGHTS OR OBLIGATIONS TO THIRD PARTIES

The Customer may only transfer or assign its rights and obligations under the Terms and conditions to a third party with the express, prior and written consent of, and subject to the conditions agreed with, the NBB.

The NBB is not allowed to transfer or assign its rights and obligations under the Terms and conditions to a third party, but is explicitly allowed to outsource the execution of its obligations under the Terms and conditions to sub-contractors.

8.5. REVISION

The Terms and conditions constitute the complete agreement between the Parties regarding the provision of NBB-Net, “Turn key” and “Starter” services and supersede any prior written or oral agreement concluded between the Parties regarding the same subject.

Any amendment or modification of the Terms and conditions shall be made in writing, shall be notified by registered postal mail to the Customer and shall enter into force on the date as specified in the relevant amendment or modification. If the Customer does not agree with the amendment or modification of the Terms and conditions proposed by the NBB, and notwithstanding the Clause 7, the Customer is allowed to unsubscribe to the NBB-Net service and/or the ancillary “Turn key” or “Starter” services at the end of the running semester, without indemnification but subject to the sending of a termination notice to the NBB. Such termination notice shall be sent to the NBB by means of a registered postal mail in order to be legally valid and shall specify the reason for the termination and whether the termination concerns the NBB-Net service as a whole or only the “Turn key” or the “Starter” service.

9. APPLICABLE LAW AND DISPUTE RESOLUTION

These Terms and conditions shall be governed by, and construed in accordance with, the laws of Belgium.

Any dispute between the Parties concerning the interpretation, application or execution of these Terms and conditions shall be settled, if possible, in an amicable and equitable manner within a reasonable period of time. If the dispute cannot be settled in an amicable and equitable manner, the matter in dispute shall be finally settled exclusively by the judicial courts of Brussels.

10. APPROVAL

Signed in …… on …….. 20 …..:

Name, 1st surname :	……..	Name, 1st surname :	……..
Title :	……..	Title :	……..
Signature :		Signature :	
	……..		……..

The signature of this document entails that the signee fully acknowledges and agrees with the Terms and conditions regarding the 'NBB-Net' service and the ancillary 'Turn key' and 'Starter' services.

Please return this duly completed and signed order form to:

NATIONAL BANK of BELGIUM, Secretary IT Operations and Infrastructure (IO), de Berlaimontlaan 14, B-1000 Brussels.

Fax: +32 2 221 31 35 E-mail: NBB-Net@nbb.be

NBB-Net

Starter services for Nbb-Net connection over Internet

Terms & Conditions and Order Form

2014

NBB-NET

TERMS AND CONDITIONS

1. DEFINITIONS

For the purpose of this document:

- "**Customer**" means any person needing to have a remote access to specific IT-applications or platforms hosted and operated by the NBB as a consequence either of its membership of a non-profit association in the financial sector, of a co-operation agreement scheme set up by the NBB or to which the NBB adheres, of a legal obligation or of any other professional reason;
- "**NBB**" means the NATIONAL BANK OF BELGIUM, a public limited company by shares created by law, having its registered office at de Berlaimontlaan 14, B-1000 Brussels, registered in the legal entities repository of Brussels under the enterprise number 0203.201.340, VAT number BE 0203.201.340;
- "**NBB-Net**" means a TCP/IP secured data transport network set up by the NBB with the aim to provide for a state-of-the-art connection channel between the NBB and its professional clients over the Internet, a private MPLS cloud[1] or a legacy leased line[2], including the services provided by the NBB in order to set up, operate and maintain this network;
- "**Starter Box**" means an encryption device (router) composed of both hardware[3] and software components that is initially pre-configured and further managed by the NBB in function of the technical environment of the Customer in such a way that the said device is ready for use by the client ("plug and play");
- "**Terms and conditions**" means the present terms and conditions on the provision by the NBB of the NBB-Net, as well as the most recent version of all documents to which this document specifically refers, even if they are not materially attached as an annex to this document;
- "**Turn key**" means a managed solution owned and maintained by NBB up to the encryption box at the Customer's premises. The transport network used with this solution is the private MPLS cloud.

2. SCOPE

The scope of these Terms and conditions is strictly limited to NBB-Net and ancillary services like "Turn key" and "Starter". Therefore, this scope does not extend to:

- the use of the IT-applications or platforms to which access is granted through the NBB-Net connection, which is covered by specific terms and conditions,
- Customer's use of a legacy leased line agreed upon with Belgacom or Colt, or of a broad bandwidth connection with the internet via a provider freely selected by the Customer. The Customer is exclusively responsible for the implementation and maintenance at his own cost of

---

1 MPLS stands for « Multi Protocol Label Switching ». The private MPLS cloud for NBB-Net is currently provided and operated by Colt.

2 This solution, deprecated by the NBB, is no longer available for new connections with NBB-Net.

3 Currently : Cisco router, model CISCO881-K9. The choice of the devices can be modified at any time by the NBB in order to stick with the technical evolution and state-of-the-art.

such a leased line or of such an access to the internet[4]. Therefore, the NBB shall not overtake any technical, contractual, financial and/or legal constraint whatsoever regarding the leased line or the internet access services subscribed by the Customer and shall not be bound by the terms, conditions, technical features and limitations whatsoever agreed with the Customer's concerned service provider.

2.1. NBB-NET

The technical documentation about NBB-Net is available on the website of the NBB, at the following address: http://www.nbb.be/doc/EL/NBB-Net.pdf. This technical documentation is an integral part of the Terms and conditions and its respect by the Customer is mandatory.

The technical features of NBB-Net may be unilaterally modified by NBB at any time in order to stick with the technical evolution and state-of-the-art, operational experience, feedback and enhancement proposals provided by the Customers. However, major changes that may have a substantial impact on the Customers' IT infrastructure shall only be implemented after due notification to the Customers.

Encryption is mandatory for all transport of data via NBB-Net.

NBB-Net makes use of one of the following, TCP/IP-based connectivity media:

- Colt MPLS network,
- legacy leased lines, or
- a broad bandwidth connection over the internet.

2.1.1. COLT MPLS NETWORK

The physical underlying transport channel of the Colt MPLS network is a Virtual Private network provided via optical fibres[5] throughout Europe by the network operator Colt, which has been appointed by the NBB via a public procurement procedure. Although it provides for the data transport network, Colt is a sub-contractor of the NBB and is no Party to the present Terms and conditions. Therefore, the NBB assumes alone all contractual and legal aspects of the MPLS solution. This means that the Customer needs in all cases to contact the NBB for any issue regarding the MPLS solution, including troubleshooting and incidents, and is therefore not allowed to directly contact Colt for such matters, even with regard to his locally installed loop(s).

The optional « Turn key » solution (see below, Clause 2.2) is only available for Customers making use of the Colt MPLS Network.

The MPLS infrastructure set up at NBB-side is dedicated to NBB-Net and is thus not shared with other IT-solutions.

2.1.2. LEGACY LEASED LINES

The physical underlying transport channel is a specific leased line installed by Belgacom or Colt. No new leased lines will be installed with the NBB, so that this service is only performed in favour of Customers who dispose of a legacy leased line already used previously in the frame of the remote access to NBB applications and platforms.

The leased line infrastructure set up at NBB-side is dedicated to NBB-Net and is thus not shared with other IT-solutions.

2.1.3. BROAD BANDWIDTH CONNECTION OVER THE INTERNET

The physical underlying transport channel is an internet access provided by an Internet provided selected by the Customer under his responsibility and at his own costs.

---

4 It goes without saying that the NBB is exclusively responsible for the implementation and maintenance of its own access to the internet, which goes via two different internet service providers.

5 Excepted the last mile to the Customer's premises, which can be in copper cable.

The optional « Starter » solution (see below, Clause 2.3) is only available for Customers making use of such a broad bandwidth connection over the internet.

The broad bandwidth Internet connections set up at NBB-side are not exclusively dedicated to NBB-Net but are shared with other NBB IT-solutions and applications such as NBB-mails, internet site, access to public NBB-applications, etc.).

2.2. "TURN KEY"

"Turn key" is an optional service provided by the NBB on top of the Colt MPLS Network as NBB-Net connectivity medium.

"Turn key" consists of the NBB taking on its account the procurement, installation, monitoring and possible debugging of the Colt MPLS infrastructure and the encryption devices (routers) needed for the setup of the connection with NBB-Net. The NBB sub-contractor for the management of the encryption devices is currently Belgacom. The NBB is also responsible for reporting possible incidents to Colt and/or Belgacom for the incident solving (relating to software as well as hardware), however within the limits of its technical possibilities and available knowledge of the Colt MPLS network, and for the operation of a Single Point of Contact (SPOC) in case of incident or fallout of the MPLS network or encryption devices.

"Turn key" is an ancillary service of NBB-Net that is provided on explicit request of the Customer. It is not available outside the framework of the NBB-Net service.

2.3. "STARTER"

"Starter" is an optional service provided by the NBB to Customers having selected a broad bandwidth connection over the Internet as NBB-Net connectivity medium.

"Starter" consists in the delivery by the NBB to the Customer of one or more[6] pre-configured Starter Boxes as well as the automated pro-active monitoring[7], the further technical assistance by phone and by e-mail for installation completion, the provision, as far as reasonably possible[8], of a remote intervention by the NBB on a Starter Box that is not working properly, and its replacement by a new Service box in accordance with Clause 5.2. The Customer is informed in advance of a possible remote intervention carried out by the NBB and of the period during which this intervention can take place. Automated pro-active monitoring shall be performed by NBB until the Customer notifies to the NBB its wish to terminate this specific provision of service.

The technical assistance of the NBB ceases as soon as the configuration setup has been completed successfully or if the Customer unilaterally modifies the initial configuration of the Starter Box, which requires the communication by the NBB on demand of the Customer of the password locking the configuration of the Starter Box.

The NBB provides, on a case by case-basis, a prior advice to the Customer relating to the optimal number of Starter Boxes to be delivered. However, this number is defined by the Customer self, under its own responsibility.

"Starter" is an ancillary service of NBB-Net that is provided on explicit request of the Customer. It is not available outside the framework of the NBB-Net service.

---

6 If deemed necessary, the Customer may order a spare Starter Box in order to allow faster recovery from failure of an operational Starter box.

7 SNMP polling, sending of traps to NBB and periodic backup of the software configuration.

8 Indeed, the possibility of a remote technical intervention by NBB on the Starter Box is rather limited due to the fact that the NBB has no physical access, and even no logical access, to the Customer's Starter Box or IT-infrastructure.

3. ORDER

The Customer places an order by sending back to the NBB the duly completed and signed Order form available on the internet site of the NBB, at the following address: http://www.nbb.be/doc/EL/NBB-Net_Order_form.pdf.

By sending back a duly completed and signed Order form, the Customer acknowledges his full adherence with the present Terms and conditions, which become applicable as from the date of their signature by the Customer.

4. FINANCIAL REGIME

4.1. FEES

The NBB charges fees to the Customer in retribution of the basic and optional NBB-Net services. These fees reflect the NBB actual costs (NBB internal costs, network operators' or subcontractors' expenses and costs entailed by other third parties' provisions of services) and are therefore updated each year, in principle on the 1st of January, in order to be adjusted to the NBB's actual cost level.

The yearly actualised list of tariffs is available on the website of the NBB, at the following address: http://www.nbb.be/doc/EL/NBB-Net_tariffs.pdf.

4.1.1. NBB-NET

The retribution of the NBB-Net services provided by the NBB consists of:

a) a periodic fee calculated per physical connection channel (*i.e.* per leased line, per MPLS end point and per Internet connectivity) and per half year; in some cases (MPLS network, leased line), the level of such fee depends of the maximum data transfer capacity requested by the Customer;
b) "one-shot" installation costs in the case of the MPLS network, the amount of which is calculated by Colt in view of the Customer's specific situation.

4.1.2. "TURN KEY"

The retribution of the optional "Turn key" services provided by the NBB consists of:

a) a periodic fee calculated per encryption device and per half year;
b) "one-shot" installation costs of the encryption device.

4.1.3. "STARTER"

The retribution of the optional "Starter" services provided by the NBB consists of a periodic fee calculated per delivered Starter Box and per half year.

4.2. INVOICING

The fees shall be invoiced to the Customer:

- immediately after the performance of the concerned services, when they relate to installation costs ("one shot" costs, see Clause 4.1 above),
- in June and in December of each civil year, when they relate to recurrent provisions of services which are charged on a half-yearly basis (see Clause 4.1 above). The invoice issued in June refers to the provision of services during the first semester of the running civil year, the invoice issued in December during the second semester of the running civil year. If the Customer subscribes to NBB-Net, and possibly the ancillary services "Turn key" or "Starter" in the course of a semester, the fee relating to the said semester shall be calculated on a *pro rata temporis* basis.

4.3. PAYMENT

Invoiced amounts must be paid by the Customer in euro within thirty (30) days after their issuance, on the bank account number mentioned on these invoices, whereby all costs related to this payment will be exclusively borne by the Customer. In case of delayed payment, penalties are due in accordance

with the Belgian law d.d. 2 August 2002 regarding the fight against belated payments of commercial transactions.

Any tax and right applicable to the services performed by the NBB in accordance with the national law of any of the Parties, including the VAT, shall be exclusively borne by the Customer.

5. LIABILITY REGIME

5.1. GENERAL LIABLITY REGIME

The Parties shall carry out their obligations arising out of the Terms and conditions in good faith. In performing their respective obligations under the Terms and conditions, the Parties shall be bound by a general duty of reasonable care in relation to each other. Each Party shall take all reasonable and practical measures to mitigate possible loss or damage to the other Party.

The NBB warrants that it shall deliver professional, state-of-the-art services to the Customer, however without any warranty regarding mandatory results to be reached.

The NBB shall be liable to reimburse to and/or indemnify the Customer for any evidenced loss, liability and/or expense incurred by the Customer which has been caused by the NBB's misconduct or negligence, whereby the burden of evidencing the invoked misconduct or negligence lays on the Customer. However, excepted in case of wilful misconduct or negligence:

- the NBB shall not be liable towards the Customer for indirect, incidental, special or consequential damage, including but not limited to: harm to the level of services provided by Customer, loss of business, loss of profit, loss of data, reputational damage, etc. arising out of or in connection with the NBB-Net services or the ancillary "Turn key" and "Starter" services,
- without prejudice to Clause 5.2, the total amount of the reimbursement and/or indemnification to be paid by the NBB to the Customer for damages occurred during a given civil year shall under no circumstance whatsoever exceed the amount of the fees paid by the said Customer to the NBB during the said civil year.

Moreover, the NBB shall not be liable for delay in performing or failure to perform any of its obligations under the Terms and conditions if the delay or failure results from a slight misconduct or negligence, or from events or circumstances outside its reasonable control. For the application of this rule:

- "slight misconduct or negligence" is understood as any misconduct or negligence that can reasonably be expected still to take place in spite of the normal care and precaution expected from a professional provider of IT-services,
- "circumstances outside its reasonable control" are understood as *force majeure*, mandatory regulation passed or actions carried out by the public authority, and the unpredictable actions or negligence of a third party, including the NBB's sub-contractors. In particular, no liability shall be vested with the NBB when the delay in performing or failure to perform its obligations results from an action, omission, delay, failure or denial of service of the Customer's internet access provider in the performance of its own obligations towards the Customer. Each Party shall inform the other Party without delay of any such actual or imminent failure, and use its best efforts to solve it as soon as reasonably possible. Furthermore, as regards the Colt MPLS network, the NBB cannot grant further terms of services than those granted by Colt itself to NBB.

Any Customer seeking indemnification by the NBB of any damage shall explicitly request the reimbursement and/or indemnity in writing by means of a registered postal mail, and shall add to its claim the evidence relating to both the misconduct or the negligence and of the invoked damage. No claim, regardless of form, arising out of the Terms & Conditions may be validly introduced by the Customer more than two (2) years after the cause of action became known to the Customer.

5.2. SPECIFIC LIABLITY REGIME FOR THE "STARTER" SERVICE

As an exception to Clause 5.1, the total amount of the reimbursement and/or indemnification to be paid by the NBB to the Customer for damages occurred during a given civil year which are entailed by a misconduct or negligence in the provision of the Starter service shall under no circumstance

whatsoever exceed the amount of the fees paid by the Customer to the NBB during the said civil year for the provision of the Starter service.

The NBB shall replace, as soon as reasonably possible, a Starter Box which does not work, or does not work properly anymore, despite possible remote interventions performed by the NBB as referred to in Clause 2.3. In such case, the Customer may need:

a) to install the second, properly pre-configured Starter Box at its disposal and deploy it in production environment, in order to keep the connection with NBB-Net running, and

b) to send a formal notice of the falldown of the Starter Box to the NBB and to send the faulty Starter Box to the NBB at its own cost. Upon receipt of the faulty Starter Box, the NBB sends at its own cost a new pre-configured Starter Box to the Customer with a fast shipping company;

6. OWNERSHIP AND INTELLECTUAL PROPERTY RIGHTS

The present Terms and conditions do not result in any transfer of property right or any other right whatsoever in any tangible of intangible asset of NBB or its agents and subcontractors to the Customer. However, the NBB grants to the Customer, to the extent feasible under applicable legislation, all licences regarding the intellectual property rights required to enable the Customer to use the NBB-Net service and the ancillary “Turn key” and “Starter” services, in particular the Starter Box and its software components.

The Starter Box remains the sole property of the NBB and is fully dedicated to the NBB-Net connection. It may not be recycled, destroyed, sold, leased, alienated or used by the Customer for any other purpose without prior written agreement of the NBB.

7. EFFECTIVENESS, DURATION AND TERMINATION

In accordance with Clause 3, these Terms and conditions become effective from the date of their signature by the Customer of the Order form.

The NBB-Net service and the ancillary services “Turn key” and “Starter” are concluded for an undefined period of time, but shall encompass a minimum duration of one full calendar year.

Subject to the mandatory respect of the said minimum duration, each Party shall be entitled to terminate the NBB-Net service, or to terminate the “Turn key” or “Starter” service while continuing the NBB-Net service, at the end of any civil year, without need of any justification and without indemnification but subject to the sending of a termination notice to the other Party, at least six months in advance. Such termination notice shall be sent to the other Party by means of a registered postal mail in order to be legally valid and shall specify whether the termination concerns the NBB-Net service as a whole or only the “Turn key” or the “Starter” service.

The extraordinary right of a Party to terminate the provision of the services if the other Party does not fulfil its own contractual duties pursuant to Article 1184 of the *Belgian Civil Code* shall remain unaffected.

The Customer having subscribed to the “Starter” service must send back the Starter Boxes in his possession to the NBB or its agent not later than the first working week following the termination date, at its own cost. The NBB is empowered as by law and without prior notification to replace the Starter Boxes which have not been received from the Customer within two weeks after the termination date, by purchasing a new encryption device for each Starter Box that have not been received, at the exclusive cost of the Customer that shall refund the said cost on first demand of the NBB.

The termination of the NBB-Net service for any reason whatsoever shall not affect provisions on the following items:
(a) Clause 5: Liability
(b) Clause 6: Ownership and property rights, and
(c) Clause 9: Applicable law and dispute resolution.

8. MISCELLANEOUS PROVISIONS

8.1. NOTICES

Without prejudice to specific diverging provisions in these Terms and conditions, any notice sent by the Parties shall be in writing (fax, post, or any other durable means of communication, including e-mail) and in English.

8.2. WAIVER

A failure or delay in exercising any right or remedy under the Terms and conditions shall not operate as a waiver of, and accordingly shall not preclude or limit any future exercise of, that right or remedy.

8.3. SEVERABILITY AND SURVIVAL

Should a provision of the Terms and conditions be or become invalid, illegal or unenforceable, the other provisions of the Terms and conditions shall remain valid, legal and enforceable.

8.4. TRANSFER OF RIGHTS OR OBLIGATIONS TO THIRD PARTIES

The Customer may only transfer or assign its rights and obligations under the Terms and conditions to a third party with the express, prior and written consent of, and subject to the conditions agreed with, the NBB.

The NBB is not allowed to transfer or assign its rights and obligations under the Terms and conditions to a third party, but is explicitly allowed to outsource the execution of its obligations under the Terms and conditions to sub-contractors.

8.5. REVISION

The Terms and conditions constitute the complete agreement between the Parties regarding the provision of NBB-Net, “Turn key” and “Starter” services and supersede any prior written or oral agreement concluded between the Parties regarding the same subject.

Any amendment or modification of the Terms and conditions shall be made in writing, shall be notified by registered postal mail to the Customer and shall enter into force on the date as specified in the relevant amendment or modification. If the Customer does not agree with the amendment or modification of the Terms and conditions proposed by the NBB, and notwithstanding the Clause 7, the Customer is allowed to unsubscribe to the NBB-Net service and/or the ancillary “Turn key” or “Starter” services at the end of the running semester, without indemnification but subject to the sending of a termination notice to the NBB. Such termination notice shall be sent to the NBB by means of a registered postal mail in order to be legally valid and shall specify the reason for the termination and whether the termination concerns the NBB-Net service as a whole or only the “Turn key” or the “Starter” service.

9. APPLICABLE LAW AND DISPUTE RESOLUTION

These Terms and conditions shall be governed by, and construed in accordance with, the laws of Belgium.

Any dispute between the Parties concerning the interpretation, application or execution of these Terms and conditions shall be settled, if possible, in an amicable and equitable manner within a reasonable period of time. If the dispute cannot be settled in an amicable and equitable manner, the matter in dispute shall be finally settled exclusively by the judicial courts of Brussels.

NBB-NET

ORDER FORM

1. CUSTOMER'S DATA

1.1. OFFICIAL INCORPORATION ADDRESS

Customer's address:
• *Name/firm* : .....
• *Legal form* : .....
• *Contact person* : .....
• *Street* : .....
• *Number* : .....
• *Zip code and city* : .....
• *Country* : .....
• *E-mail address* : .....
Customer's VAT number
.....
Customer's accounting reference (to be mentioned in any communication)
.....
Reserved to NBB : NBB accounting reference
.....

1.2. INVOICING DATA *(only when invoicing address is different from official address)*

Customer's invoicing address:
• *Contact person* : .....
• *Street* : .....
• *Number* : .....
• *Zip code and city* : .....
• *Country* : .....
• *E-mail address* : .....

1.3. CONNECTED SITE LOCATION *(one for each connected site):*

Location of site 1:
• *Contact person* : ..... • *Street* : ..... • *Number* : ..... • *Zip code and city* : ..... • *Country* : ..... • *E-mail address* : ..... • *TCP/IP address* : .....
Reserved to NBB : link reference
.....

Location of site 2, if any:
• *Contact person* : ..... • *Street* : ..... • *Number* : ..... • *Zip code and city* : ..... • *Country* : ..... • *E-mail address* : ..... • *TCP/IP address* : .....
Reserved to NBB : link reference
.....

Location of site 3, if any:
• *Contact person* : ..... • *Street* : ..... • *Number* : ..... • *Zip code and city* : ..... • *Country* : ..... • *E-mail address* : ..... • *TCP/IP address* : .....
Reserved to NBB : link reference
.....

2. ORDER FORM

Site 1	*Reserved to NBB: tariff*
☐ **NBB-net**	
○ **- Colt MPLS Network:** *requested nominal data transfer speed: …….. bps*	Installation costs: …….. € Subscription: per ½ year: …….. €
☐ **- Optional: Turn key service**	Installation costs: …….. € Subscription: per ½ year: …….. €
○ **- Legacy leased line:** *requested nominal data transfer speed: …….. bps*	Subscription: per ½ year: …….. €
○ **- Internet VPN:**	Subscription: per ½ year: …….. €
☐ **- Optional: Starter service:** *number of Starter Boxes: ……..*	Subscription: per ½ year: …….. €
Reserved to NBB: Total half-yearly fee for this site (outside installation costs):	…….. **€**

Site 2	*Reserved to NBB: tariff*
☐ **NBB-net**	
○ **- Colt MPLS Network:** *requested nominal data transfer speed: …….. bps*	Installation costs: …….. € Subscription: per ½ year: …….. €
☐ **- Optional: Turn key service**	Installation costs: …….. € Subscription: per ½ year: …….. €
○ **- Legacy leased line:** *requested nominal data transfer speed: …….. bps*	Subscription: per ½ year: …….. €
○ **- Internet VPN:**	Subscription: per ½ year: …….. €
☐ **- Optional: Starter service:** *number of Starter Boxes: ……..*	Subscription: per ½ year: …….. €
Reserved to NBB: Total half-yearly fee for this site (outside installation costs):	…….. **€**

Site 3	*Reserved to NBB: tariff*
☐ **NBB-net**	
○ **- Colt MPLS Network:** *requested nominal data transfer speed: …….. bps*	Installation costs: …….. € Subscription: per ½ year: …….. €
☐ **- Optional: Turn key service**	Installation costs: …….. € Subscription: per ½ year: …….. €
○ **- Legacy leased line:** *requested nominal data transfer speed: …….. bps*	Subscription: per ½ year: …….. €
○ **- Internet VPN:**	Subscription: per ½ year: …….. €
☐ **- Optional: Starter service:** *number of Starter Boxes: ……..*	Subscription: per ½ year: …….. €
Reserved to NBB: Total half-yearly fee for this site (outside installation costs):	…….. **€**

NBB RAMSES GUI – VPN STARTER BOX - SETUP PROFILE and configuration data.

General Company Details

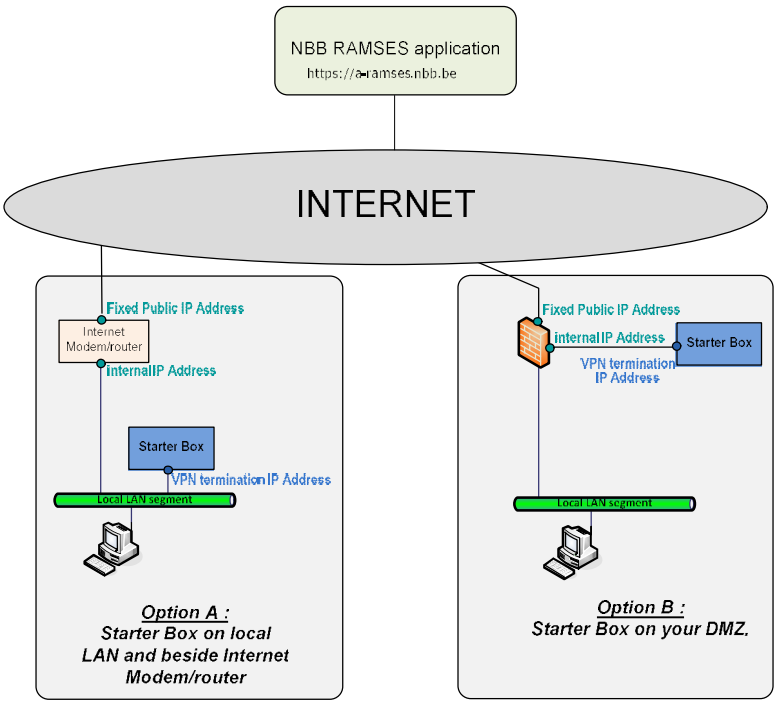
Technical Company Details

Please fill in Contact Details

NBB Contact Information			
IT Helpdesk	Call center	+32 (0) 2 221 40 60	Servicedesk@nbb.be
Business Helpdesk	Organisation	+32 (0) 2 221 37 27	T2s.Sss@nbb.be
Technical specialists	NBB-Net Team		Nbb-net@nbb.be
PARTNER Contact Information			
IT Helpdesk			
Business Helpdesk			
Technical specialists			

Partner Infrastructure Option

Please choose option



General Connection Details

Please fill in Connection Details

	Partner
Internet Provider	
Option (ref. infrastructure drawing)	
Modem/router type (ex: Bbox, router, modem, firewall)	
Modem/router Internet Fixed Public IP Address	
Modem/router Internal IP Address	
VPN termination IP address	
Firewall : Yes or No.	

Dataflow:

Please fill in Dataflow Details

Source side	**Source (local lan segment)**	**Destination**	**Service**
Partner		https://a-ramses.nbb.be	https

3. APPROVAL

Signed in …… on …….. 20 …..:

Name, 1st surname :	……..	Name, 1st surname :	……..
Title :	……..	Title :	……..
Signature :		Signature :	
	……..		……..

The signature of this document entails that the signee fully acknowledges and agrees with the Terms and conditions regarding the 'NBB-Net' service and the ancillary 'Turn key' and 'Starter' services.

Please return this duly completed and signed order form to:

NATIONAL BANK of BELGIUM, Secretary IT Operations and Infrastructure (IO), de Berlaimontlaan 14, B-1000 Brussels.

Fax: +32 2 221 31 35 E-mail: NBB-Net@nbb.be

AGREEMENT ON THE TESTING OF NBB-PKI

BETWEEN

(1) […], a […] under […] law, having its registered office at […]; further referred to as the "**Certificate User**";

AND

(2) Nationale Bank van België / Banque Nationale de Belgique, a limited liability company by shares under Belgian law, having its registered office at de Berlaimontlaan 14, 1000 Brussels, Belgium, registered in the legal entities repository of Brussels under the enterprise number 0203.201.340; further referred to as "**NBB**";

Hereinafter collectively referred to as "**the Parties**" and individually as "**a Party**";

IT HAS BEEN CONSIDERED AS FOLLOWS:

(1) NBB imposes on the participants to its central securities depository ("NBB-SSS") RAMSES application the use of identification, strong authentication and signature tools based on electronic certificates. This initiative is part of the NBB-public key infrastructure.

(2) As part of the RAMSES deployment, the Certificate User will test and evaluate the suitability of the NBB-public key infrastructure, including Tokens and Certificates provided by NBB.

THEREFORE THE PARTIES HAVE AGREED AS FOLLOWS:

ARTICLE 1. DEFINITIONS

For the purpose of this agreement:

- "**Agreement**" means this agreement on the testing of Tokens and related tools and its Annexes, as well as all other documents to which this agreement specifically refers, even if they are not materially attached as an Annex to this agreement;
- "**Certificate**" means an electronic file which binds a public key with a Certificate User's identity and is used for the following purposes: (a) to verify that a public key belongs to the said Certificate User; (b) to electronically verify the identity of (= authenticate) the Certificate User; (c) to check a Certificate User's signature; (d) to encrypt a message by a Certificate User and (e) to verify a certificate User's access rights to electronic applications, systems, platforms and services operated by the NBB-SSS;
- " **PIN code**" means the personal identification number delivered with the Token to the Certificate User, which serves as a password preventing the use of the token by another person than the Certificate User;
- "**NBB-PKI**" stands for "NBB-public key infrastructure" and means the set of individuals, policies, procedures, and computer systems necessary for NBB to provide authentication, encryption, integrity and non-repudiation services, in particular in the operation of the NBB-SSS, by way of public and private key cryptography and electronic certificates;

- "**Token**" means the data carrier device USB-stick Safenet5100, on which the certificate is stored, and the use of which is conditioned by the entry of the personal identification number ("PIN code") of the Certificate User;
- "**Trusted person**" means the physical person who is legally entrusted by the Certificate User, on the basis of a power of attorney validly issued and not revoked by the Certificate User, to request either the issuance of a certificate, the delivery of a token and/or the revocation of a certificate on behalf of the Certificate User.

ARTICLE 2. OBJECT AND PURPOSE OF THE AGREEMENT

(1) NBB agrees to provide to the Certificate User access to the test environment of the NBB-PKI, including through the delivery of Tokens and the provision of Certificates, and the Certificate User accepts, subject to the terms of this Agreement. The Certificate User agrees to test and evaluate the NBB-PKI, including the Tokens and Certificates, as provided herein.

(2) The Certificate User acknowledges and agrees that it will use the NBB-PKI, including the Tokens and Certificates, for testing purposes only and that they may not and shall not be used for identification, authentication or signature of actual transactions or communications, in the NBB-SSS production environment in particular or vis-à-vis the NBB in general.

ARTICLE 3. START OF OPERATION OF THE NBB-PKI IN TEST ENVIRONMENT

The NBB-PKI shall start to operate in test environment on 2 January 2014.

ARTICLE 4. DELIVERY AND VALIDITY OF TOKENS

(1) As from the date of execution of this Agreement, the NBB shall physically deliver Tokens to the Trusted person with the purpose of testing the NBB-PKI, together with the initial PIN code as well as the associated Certificate User identification data linked with each delivered token.

(2) Each Token shall have a validity of three years as from the date on which they are physically delivered to the Trusted person. NBB shall inform the Certificate Users of the expiration of this validity three months in advance.

ARTICLE 5. FEE

The Tokens and certificates are provided against payment by the Certificate User of a flat fee of EUR 200 per Token for the full validity period of the Token. No refund of this fee shall be granted, even in case of loss, damage etc.

ARTICLE 6. LIABILITY

(1) In performing their respective obligations under the Agreement, the Parties shall be bound by a general duty of reasonable care in relation to each other. Each Party shall take all reasonable and practical measures to mitigate loss or damage.

(2) The Parties shall bear the burden of proof of demonstrating that they have not breached their duty of reasonable care in performing their respective obligations under the Agreement, including in the operating of technical facilities thereof.

ARTICLE 7. CONFIDENTIALITY

(1) The Parties shall keep confidential all sensitive, restricted, confidential or secret information or know-how (whether such information is of a commercial, financial, regulatory, technical or other nature) that is marked as such and belongs to the other Party or which the other Party

has a lawful right to use, and shall not disclose such matters to any third party without the express, prior and written consent of the other Party.

(2) The duty of confidentiality under this Article does not apply where disclosure is:

(a) warranted by the defence of a Party's legitimate interests in court proceedings, arbitration or similar legal proceedings; or

(b) required by law.

Each Party shall inform the other Parties about any disclosure of confidential information in the context of such court proceedings, arbitration or similar legal proceedings.

ARTICLE 8. REPORTING

The Certificate User shall report without delay to NBB any matter that has a material impact on the operation of the NBB-PKI and any perceived defect in the Token. Following the discovery of any defect to the Token, the Certificate User shall terminate its use of the Token.

ARTICLE 9. MISCELLANEOUS PROVISIONS

A. NOTICES

Any notice sent under this Agreement shall be in writing (fax, post, or any other durable means of communication, including e-mail).

B. WAIVER

A failure or delay in exercising any right or remedy under the Agreement shall not operate as a waiver of, and accordingly shall not preclude or limit any future exercise of, that right or remedy.

C. SEVERABILITY AND SURVIVAL

Should a provision of the Agreement be or become invalid, illegal or unenforceable, the other provisions of the Agreement shall remain valid, legal and enforceable. The Parties shall negotiate as soon as possible a valid, legal and enforceable provision to replace the invalid, illegal or unenforceable one, the legal effect of the new provision being as close as possible as the intent of the invalid, illegal or unenforceable provision.

D. REVISION OF THE AGREEMENT

(1) The Agreement constitutes the complete agreement between the Parties regarding the testing of NBB-PKI and supersedes any prior written or oral agreement concluded between the Parties regarding the same subject.

(2) Any amendment or modification of the Agreement shall be made in writing, shall be executed by both Parties and shall enter into force on the date as specified in the relevant amendment or modification.

ARTICLE 10. APPLICABLE LAW AND DISPUTE RESOLUTION

This Agreement shall be construed and enforced according to the laws of the Kingdom of Belgium and any dispute under this Agreement must be brought in the Commercial Court of Brussels and no other.

ARTICLE 11. EFFECTIVENESS, DURATION AND TERMINATION

(1) The Agreement shall become effective on the date of signature.

(2) The Agreement is concluded for an indefinite period of time.

(3) The extraordinary right of a Party to terminate the Agreement if the other Party does not fulfil its own contractual duties pursuant to Article 1184 of the *Belgian Civil Code* shall remain unaffected.

(4) Termination of the Agreement for any reason whatsoever shall not affect provisions on the following items:
   (a) ARTICLE 6. : Liability
   (b) ARTICLE 7. : Confidentiality
   (d) ARTICLE 10. : Applicable law and dispute resolution.

In Witness whereof, the parties have executed this Agreement.

_____ _____

Certificate User NBB

_____

Date

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

Annex 9

Description of Static data of a security account

Any Participant can define the following Static data for each of his securities accounts:

- “securities account name”;
- “hold” indicator: this flag allows that all settlement instructions entered for the securities account are set on “party hold”;
- “market claims” indicator: this flag allows deactivating the market claim processing. Hence, instructions are enriched with the “no market claim” flag before submitted for matching;
- “market claims on hold”: this flag allows setting market claims when they are generated by the NBB-SSS on “party hold” whatever the hold status of the underlying instruction;
- “primary market operation on hold”: this flag allows setting all primary market operations generated by the Belgian Debt Agency related to the securities account on “party hold”;
- “BIC11 of the underlying client”: this information is used to optimize the primary market operation entered by the Belgian Debt Agency;
- “dealer type”: when the account is linked to a primary or recognized dealer;
- “start date” and “end date”;
- ‘partial settlement not allowed”: this flag allows that partial settlement instructions entered for the securities account are systematically rejected;
- “X/N”: for the purposes of the X/N tax rules, each securities account needs to be identified either as X-account (exempted from withholding tax) or N-account (non-exempted from withholding tax).

FPS FINANCE
Ledger service
Avenue des arts 30 - 1040 Brussels
Tel.: +32 (0)2 574 72 09 - Fax: +32 (0)2 233 70 86

Annex 12

APPLICATION FOR REGISTRATION BY NAME IN THE BELGIAN DEBT LEDGER

via a financial institution

www.grootboeken.be

To be handed to your FINANCIAL INTERMEDIARY
who will forward it to:
National Bank of Belgium – Payments and Securities service
boulevard de Berlaimont 14 - 1000 Brussels
tel.: 32 (0)2 221 27 14 - fax: 32 (0)2 221 31 96

I, the undersigned (surname, first name, full address) (if a company: name and position of representatives)

request registration in the State Debt Ledger.

ISIN code: BE

Name of the loan:

Nominal capital €:

IN THE NAME OF (surname, first name, full address):

National number/Holder's date of birth

The holder claims exemption from withholding tax on income from movable assets: YES/NO [1]

- If yes, for individuals attach: non-resident saver's certificate or form EUR 276
- for companies, attach: CERTIFICATE or identification certificate

The interest and the capital will be paid into:

Account number[2]:

In the name of:

Done in: on:

SIGNATURE(S)

[1] Delete as applicable.
[2] IBAN and BIC for a non-Belgian account.

FPS FINANCE
Ledger service
Avenue des arts 30 - 1040 Brussels
Tel.: +32 (0)2 574 72 09 - Fax: +32 (0)2 233 70 86

Annex 13

CANCELLATION OF REGISTRATION BY NAME

IN THE BELGIAN DEBT LEDGER

via a financial institution

www.grootboeken.be

Send this form to: in the case of "TRANSFER" **National Bank of Belgium** **Payments and Securities** **boulevard de Berlaimont 14 - 1000 Brussels** Tel.: 32 (0)2 221 27 14 Fax: 32 (0)2 221 31 96	Send this form to: in the case of "SALE": **Federal Public Service Finance** **LEDGER SERVICE** **Avenue des arts 30 - 1040 Brussels** Tel.: 32 (0)2 574 72 09 Fax: 32 (0)2 233 70 86

The undersigned (surname, first name, full address) (if a company: name and position of representatives)

ISIN code: BE

Name of the loan:

Nominal capital €:

Ledger file no.:

Ledger registration no.:

IN THE NAME OF (holder(s) or company:

TRANSFER

declares (declare) **the transfer of** capital of €:

to the National Bank of Belgium securities account number :

in the name of: value date: notification no.:

SALE

instructs (instruct) the Minister of Finance, represented by the Ledger Service, to **sell** the securities at the day's stock market price for a capital sum of €:
The proceeds from the sale and the outstanding interest will be paid into:

Bank account number IBAN:
BIC:

In the name of:

Done in: on:

SIGNATURE(S)
(**LEGALISATION mandatory for individuals)**

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 16

GUIDELINES FOR THE USE OF SECURE E-MAIL

1. Definition and conditions

Participants can use e-mail to send information to the NBB-SSS. In that case the e-mail must be secured.

The secure e-mail:

- must be signed in such a way that integrity and authenticity can be verified;
- must not be encrypted;
- must be certified with at least a category 2 certificate. The ESCB-PKI certificates on the NBB-SSS Ramses tokens are also valid for e-signing your e-mails. The full list is available on the website of the European Commission, EU Trusted Lists of Certification Service Providers: https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers

2. First use

New users of secure e-mail can send a test e-mail by contacting the NBB-SSS via SSS@nbb.be.

3. Alternative

If for some reason the participant is not able to send secure e-mail, he can request the NBB-SSS for permission to send the request by MT599 and announce the MT599 by common e-mail.

4. Liability

Without prejudice to the provisions of Article 7 of the Terms and conditions governing the participation in the NBB-SSS, the Bank cannot be held liable for any loss incurred by participants as a result of fraudulent or unlawful use of the e-mails.

Participants must take all necessary measures to guard against such incidents.

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 17

Special provisions concerning transactions with foreign SSS

(art. 5.2.1.4. of the Terms and conditions governing the participation in the NBB-SSS)

DELETED

NBB – Payment and Securities
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Tel.: +32 (0)2 221 36 00
sss@nbb.be

Annex 18.0

POWER OF ATTORNEY

The company .....
having its registered office at .....
hereafter represented by .....
participant in the NBB-SSS of the National Bank of Belgium ("the Bank")
with BIC11:
hereafter "the participant";

The company .....
having its registered office at .....
hereafter represented by .....
with BIC11:

hereafter "the instructing party";

WHEREAS:

The participant or, when the occasion arises, one or more establishments for the account on which the participant holds securities in the NBB-SSS, have authorised [the instructing party] for sending to the NBB-SSS/T2S, by means of SWIFT messages or through the NBB-SSS Ramses GUI / T2S GUI, the instruction required for the settlement of the transactions from [instructing party] such participant or these establishment(s);

THE PARTICIPANT NOTIFIES THE NBB AS FOLLOWS:

1. The Participant authorises the NBB to accept instructions by the participant itself or by an establishment for the account of which the participant holds securities in the NBB-SSS which are validly addressed on its behalf to the NBB-SSS / T2S by [the instructing party] pursuant to the mandate referred to in the preamble, and to deal with such instructions in the NBB-SSS / T2S in accordance with the provisions of the terms and conditions governing the participation in the NBB-SSS ("the Terms and Conditions"). The participant recognises that such instructions are binding it vis-à-vis the NBB and third parties just as if they had been issued by the participant itself (including, but not exclusively, for the purposes of article 8.2 of the Terms and Conditions).

The instructions referred to in the first paragraph shall only relate to:

all accounts

positions on the following securities accounts for which the mandate is exclusively valid and starts from the accompanying date:
NBBE ....
NBBE ....
NBBE ....
NBBE ....
NBBE ....

2. The instructions referred to in the first paragraph shall always mention a securities account number of the participant and shall be transmitted by the SWIFT network or through the NBB-SSS Ramses GUI / T2S GUI in accordance with the provisions laid down in the Rules for those means of communication.

The instructing party will either use:
the following BIC11 (ISO 15022):.....

or DN (ISO 20022): .....….....….....

to send its instructions to the NBB-SSS and/or T2S.

If the SWIFT network or the NBB-SSS Ramses GUI should be unavailable, even temporarily, the NBB may, however, accept instructions transmitted by other means in the cases and under the conditions that the NBB shall determine at its own discretion.

The participant shall retain the right to cancel the settlement notifications referred to in the first paragraph, subject to the conditions laid down by the Terms and Conditions.

The participant authorises the NBB to communicate to [the instructing party] any information of any kind relating to the receipt, acceptance, matching and cancellation, if appropriate, of the instructions referred to in the first paragraph, and to the settlement of the transactions notified that way.

2. Furthermore, the participant undertakes:

a) to take the necessary internal measures to ensure the settlement of all the instructions entered in the NBB-SSS / T2S by [the instructing party];

b) to indemnify the NBB against any adverse consequences (except in so far as such consequences are due to the NBB's own negligence, or the negligence of its employees or persons made responsible by the Bank for the execution of tasks, rendering the NBB liable in accordance with article 7.3 of the Terms and Conditions) arising directly from the execution of the instructions referred to in section 1, in particular (but not exclusively) any disputes between it and [the instructing party], its counterparties, clients or any third parties whatsoever. The NBB's obligations shall be limited strictly, for the application of the present power of attorney, to checking that the notifications received from [the instructing party] are conform to the instructions issued by the NBB-SSS / T2S to the participants, the Terms and Conditions and the rules governing the operation of the SWIFT system and rejecting any such instructions which do not conform. For the fulfilment of those obligations, the NBB shall be subject to the provisions on liability defined by article 7.3 of the Terms and Conditions;

c) to inform the NBB in writing, without delay, of any withdrawal of the authorisation given to the NBB in section 1 of this document. The participant recognises that such withdrawal shall, however, only take effect, and thus entail an obligation on the NBB to refuse instructions sent by [the instructing party], in the case of instructions sent on or after the NBB-SSS working day following the date on which the NBB receives instruction of the said withdrawal.

The present power of attorney shall be governed by Belgian law.

Done at ……., on……..

Authorised signature(s)

NBB – Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Tel.: +32 (0)2 221 22 17 - Fax: +32 (0)2 221 31 19
sss@nbb.be

Annex 18.1

Trading and settlement platforms that can be authorised to send instructions in the name and on behalf of a participant

- EuroMTS Limited – BIC11 EMTSGB2LXXX
- MTS Associated Markets NV/SA – BIC11 BMTSBEBBXXX
- MTS S.p.A. – BIC11 MTSCITRRXXX

- BrokerTec – BIC11 BTECGB2LXXX

- LCH.Clearnet Ltd – BIC11 LCHLGB2XXXX
- LCH.Clearnet SA – BIC11 BACPFRPPXXX – BACPFRPPEQ1

NBB – Payments and Securities Service
Securities Settlement System
Boulevard de Berlaimont 14
BE-1000 Brussels
Tel.: +32 (0)2 221 36 00
sss@nbb.be

Annex 18.2

POWER OF ATTORNEY MTS ASSOCIATED MARKETS NV/SA

The company .....
having its registered office at .....
hereafter represented by .....
participant in the NBB-SSS of the National Bank of Belgium ("the Bank")
with BIC11:
hereafter "the participant";

WHEREAS:

The participant or, when the occasion arises, one or more establishments for the account on which the participant holds securities in the NBB-SSS, acting as member(s) of MTS Associated Markets NV/SA, wishes/wish to conclude on the MTS Belgium platform transactions involving delivery versus payment of dematerialised securities of the Belgian public debt admitted to the MTS Belgium platform;

Settlement of transactions concluded that way takes place in the NBB-SSS in accordance with the rules which govern the operation of that system.

Moreover, by a separate deed, the participant or, when the occasion arises, one or more establishments for the account of which the participant holds securities in the NBB-SSS, have authorised MTS Associated Markets NV/SA for sending to the NBB-SSS, by means of SWIFT messages or through the Ramses GUI, the instructions required for the settlement of the transactions concluded on the MTS Belgium platform by such participant or these establishment(s);

However, instructions relating to transactions concluded between two clients of the participant settled exclusively in the same client securities account of that participant opened in the NBB-SSS are addressed directly to that participant by the MTS Belgium platform;

THE PARTICIPANT NOTIFIES THE BANK AS FOLLOWS:

1. The participant expressly authorises the Bank to accept settlement instructions and cancellation relating to transactions in dematerialised securities of the Belgian public debt concluded on the MTS Belgium platform by the participant itself or by an establishment for the account of which the participant holds securities in the NBB-SSS which are validly addressed to the NBB-SSS by the company

MTS Associated Markets NV/SA,
Rue des Comédiens 22
1000 Bruxelles

pursuant to the mandate referred to in the preamble, and to deal with such instructions in the NBB-SSS in accordance with the provisions of the regulations governing the operation of the NBB-SSS ("the regulations"). The participant expressly recognises that such instructions are binding it in relation to the Bank and third parties just as if they had been issued by the participant.

The instructions referred to in the first paragraph shall only relate to positions on the following securities accounts for which the mandate is exclusively valid and starts from the accompanying date:
NBBE ....
NBBE ....
NBBE ....
NBBE ....
NBBE ....

The instructions referred to in the first paragraph shall mention either the own account number or the trading account number of the participant in the case of transactions which it concludes for its own account as a member of MTS Associated Markets NV/SA or, depending on the case, the

NBB – Payments and Securities Service
Securities Settlement System
Boulevard de Berlaimont 14
BE-1000 Brussels
Tel.: +32 (0)2 221 36 00
sss@nbb.be

omnibus client account or that of one of the segregated client accounts in the case of transactions concluded by members of MTS Associated Markets NV/SA for whose account the participant holds securities in the NBB-SSS of the Bank.

The instructions referred to in the first paragraph shall be transmitted through the SWIFT network or the Ramses GUI in accordance with the rules laid down in the regulations for that means of communication. If the SWIFT network and the Ramses GUI should be unavailable, even temporarily, the Bank may, however, accept instructions transmitted by other means in the cases and under the conditions that the Bank shall determine at its own discretion.

The participant shall retain the right to cancel the settlement instructions referred to in the first paragraph, subject to the conditions laid down by the regulations.

The participant authorises the Bank to communicate to MTS Associated Markets NV/SA any information of any kind relating to the receipt, acceptance, matching and cancellation, if appropriate, of the instructions referred to in the first paragraph, and to the settlement of the transactions notified that way.

2. Furthermore, the participant undertakes:

a) to take the necessary internal measures to ensure delivery versus payment, in its books, of the securities forming the subject of transactions concluded on the MTS Belgium platform between two establishments for the account of which it holds securities registered in the same client account in the NBB-SSS, for which instructions have been addressed to it directly by the MTS Belgium platform;

b) to indemnify the Bank against any adverse consequences (except in so far as such consequences are due to the Bank's own negligence, or the negligence of its employees or persons made responsible by the Bank for the execution of tasks, rendering the Bank liable in accordance with article 7 of the regulations) arising directly from the execution of the instructions referred to in section 1, in particular (but not exclusively) any disputes between it and MTS Associated Markets NV/SA, its counterparties, clients or any third parties whatsoever. The Bank's obligations shall be limited strictly, for the application of the present power of attorney, to checking that the instructions received from MTS Associated Markets NV/SA are conform to the instructions issued by the NBB-SSS to the participants, the NBB-SSS regulations and the rules governing the operation of the SWIFT system (those rules being replaced, in cases where the last sentence in the third paragraph of section 1 applies, by the conditions determined by the Bank in accordance with that same sentence) and rejecting any such instructions which do not conform. For the fulfilment of those obligations, the Bank shall be subject to the rules on liability defined by article 7 of the regulations;

c) to inform the Bank in writing, without delay, of any withdrawal of the authorisation given to the Bank in section 1 of this document. The participant recognises that such withdrawal shall, however, only take effect, and thus entail an obligation on the Bank to refuse instructions sent by MTS Associated Markets NV/SA, in the case of instructions sent on or after the NBB-SSS working day following the date on which the Bank receives notification of the said withdrawal.

Present power of attorney shall be governed by Belgian law.

Done at ……., on……..

Authorised signature(s)

NBB – Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: +32 (0)2 221 22 17
sss@nbb.be

Annex 18.3

POWER OF ATTORNEY LCH.Clearnet Ltd

DELETED

NBB – Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Tel.: +32 (0)2 221 36 00
sss@nbb.be

Annex 18.4

POWER OF ATTORNEY BROKERTEC

The company .....
having its registered office at .....
hereafter represented by .....

participant in the NBB-SSS of the National Bank of Belgium ("the Bank")

with BIC11:
hereafter "the participant";

WHEREAS:

The participant or, when the occasion arises, one or more establishments for the account of which the participant holds securities in the NBB-SSS, acting as member(s) of the Brokertec system, wishes/wish to conclude on Brokertec transactions involving delivery versus payment of dematerialised securities of the Belgian public debt admitted to Brokertec;

Settlement of transactions concluded that way takes place in the NBB-SSS in accordance with the rules which govern the operation of that system.

Moreover, by a separate deed, the participant or, when the occasion arises, one or more establishments for the account of which the participant holds securities in the NBB-SSS, have authorised Brokertec for sending to the NBB-SSS, by means of SWIFT messages or through the Ramses GUI, the instructions required for the settlement of the transactions concluded in the Brokertec system by such participant or these establishment(s);

However, instructions relating to transactions concluded between two clients of the participant settled exclusively in the same client securities account of that participant opened in the NBB-SSS are addressed directly to that participant by Brokertec;

THE PARTICIPANT NOTIFIES THE BANK AS FOLLOWS:

1. The participant expressly authorises the Bank to accept settlement instructions and cancellation relating to transactions in dematerialised securities of the Belgian public debt concluded in the Brokertec system by the participant itself or by an establishment for the account of which the participant holds securities in the NBB-SSS which are validly addressed to the NBB-SSS by the company

BrokerTec Europe Ltd,
2 Broadgate
London EC2M 7UR

pursuant to the mandate referred to in the preamble, and to deal with such instructions in the NBB-SSS in accordance with the provisions of the regulations governing the operation of the NBB-SSS ("the regulations"). The participant expressly recognises that such instructions are binding it in relation to the Bank and third parties just as if they had been issued by the participant.

The instructions referred to in the first paragraph shall only relate to positions on the following securities accounts for which the mandate is exclusively valid and starts from the accompanying date:
NBBE ....
NBBE ....
NBBE ....
NBBE ....
NBBE ....

The instructions referred to in the first paragraph shall mention either the own account number or the trading account number of the participant in the case of transactions which it concludes for its own account as a member of Brokertec or, depending on the case, the

NBB – Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Tel.: +32 (0)2 221 36 00
sss@nbb.be

omnibus client account or that of one of the segregated client accounts in the case of transactions concluded by members of Brokertec for whose account the participant holds securities in the NBB-SSS of the Bank.

The instructions referred to in the first paragraph shall be transmitted through the SWIFT network or the Ramses GUI in accordance with the rules laid down in the regulations for that means of communication. If the SWIFT network and the Ramses GUI should be unavailable, even temporarily, the Bank may, however, accept instructions transmitted by other means in the cases and under the conditions that the Bank shall determine at its own discretion.

The participant shall retain the right to cancel the settlement instructions referred to in the first paragraph, subject to the conditions laid down by the regulations.

The participant authorises the Bank to communicate to Brokertec any information of any kind relating to the receipt, acceptance, matching and cancellation, if appropriate, of the instructions referred to in the first paragraph, and to the settlement of the transactions notified that way.

2. Furthermore, the participant undertakes:

a) to take the necessary internal measures to ensure delivery versus payment, in its books, of the securities forming the subject of transactions concluded in the Brokertec system between two establishments for the account of which it holds securities registered in the same client account in the NBB-SSS, for which instructions have been addressed to it directly by Brokertec;

b) to indemnify the Bank against any adverse consequences (except in so far as such consequences are due to the Bank's own negligence, or the negligence of its employees or persons made responsible by the Bank for the execution of tasks, rendering the Bank liable in accordance with article 7 of the regulations) arising directly from the execution of the instructions referred to in section 1, in particular (but not exclusively) any disputes between it and Brokertec, its counterparties, clients or any third parties whatsoever. The Bank's obligations shall be limited strictly, for the application of the present power of attorney, to checking that the instructions received from Brokertec are conform to the instructions issued by the NBB-SSS to the participants, the NBB-SSS regulations and the rules governing the operation of the SWIFT system (those rules being replaced, in cases where the last sentence in the third paragraph of section 1 applies, by the conditions determined by the Bank in accordance with that same sentence) and rejecting any such instructions which do not conform. For the fulfilment of those obligations, the Bank shall be subject to the rules on liability defined by article 7 of the regulations;

c) to inform the Bank in writing, without delay, of any withdrawal of the authorisation given to the Bank in section 1 of this document. The participant recognises that such withdrawal shall, however, only take effect, and thus entail an obligation on the Bank to refuse instructions sent by Brokertec, in the case of instructions sent on or after the NBB-SSS working day following the date on which the Bank receives notification of the said withdrawal.

Present power of attorney shall be governed by Belgian law.

Done at ……, on……..

Authorised signature(s)

NBB – Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Tel.: +32 (0)2 221 36 00
sss@nbb.be

Annex 18.5

POWER OF ATTORNEY MTS S.P.A.

The company .....
having its registered office at .....
hereafter represented by .....
participant in the NBB-SSS of the National Bank of Belgium ("the Bank")
with BIC11:
hereafter "the participant";

WHEREAS:

The participant or, when the occasion arises, one or more establishments for the account on which the participant holds securities in the NBB-SSS, acting as member(s) of MTS S.p.A. , wishes/wish to conclude on the MTS Italy platform transactions involving delivery versus payment of dematerialised securities of the Belgian public debt admitted to the MTS Italy platform;

Settlement of transactions concluded that way takes place in the NBB-SSS in accordance with the rules which govern the operation of that system.

Moreover, by a separate deed, the participant or, when the occasion arises, one or more establishments for the account of which the participant holds securities in the NBB-SSS, have authorised MTS S.p.A. for sending to the NBB-SSS, by means of SWIFT messages or through the Ramses GUI, the instructions required for the settlement of the transactions concluded on the MTS Spa platform by such participant or these establishment(s);

However, instructions relating to transactions concluded between two clients of the participant settled exclusively in the same client securities account of that participant opened in the NBB-SSS are addressed directly to that participant by MTS Italy;

THE PARTICIPANT NOTIFIES THE BANK AS FOLLOWS:

1. The participant expressly authorises the Bank to accept settlement instructions and cancellation relating to transactions in dematerialised securities of the Belgian public debt concluded on the MTS Italy platform by the participant itself or by an establishment for the account of which the participant holds securities in the NBB-SSS which are validly addressed to the NBB-SSS by the company

MTS S.p.A.
Via Tomacelli, 146
Rome 00186
(Italy)

pursuant to the mandate referred to in the preamble, and to deal with such instructions in the NBB-SSS in accordance with the provisions of the regulations governing the operation of the NBB-SSS ("the regulations"). The participant expressly recognises that such instructions are binding it in relation to the Bank and third parties just as if they had been issued by the participant.

The instructions referred to in the first paragraph shall only relate to positions on the following securities accounts for which the mandate is exclusively valid and starts from the accompanying date:
NBBE ....
NBBE ....
NBBE ....
NBBE ....
NBBE ....

The instructions referred to in the first paragraph shall mention either the own account number or the trading account number of the participant in the case of transactions which it concludes for its own account as a member of MTS S.p.A. or, depending on the case, the

NBB – Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Tel.: +32 (0)2 221 36 00
sss@nbb.be

omnibus client account or that of one of the segregated client accounts in the case of transactions concluded by members of MTS S.p.A. for whose account the participant holds securities in the NBB-SSS of the Bank.

The instructions referred to in the first paragraph shall be transmitted through the SWIFT network or the Ramses GUI in accordance with the rules laid down in the regulations for that means of communication. If the SWIFT network and the Ramses GUI should be unavailable, even temporarily, the Bank may, however, accept instructions transmitted by other means in the cases and under the conditions that the Bank shall determine at its own discretion.

The participant shall retain the right to cancel the settlement instructions referred to in the first paragraph, subject to the conditions laid down by the regulations.

The participant authorises the Bank to communicate to MTS S.p.A. any information of any kind relating to the receipt, acceptance, matching and cancellation, if appropriate, of the instructions referred to in the first paragraph, and to the settlement of the transactions notified that way.

2. Furthermore, the participant undertakes:

a) to take the necessary internal measures to ensure delivery versus payment, in its books, of the securities forming the subject of transactions concluded on the MTS Italy platform between two establishments for the account of which it holds securities registered in the same client account in the NBB-SSS, for which instructions have been addressed to it directly by MTS Italy;

b) to indemnify the Bank against any adverse consequences (except in so far as such consequences are due to the Bank's own negligence, or the negligence of its employees or persons made responsible by the Bank for the execution of tasks, rendering the Bank liable in accordance with article 7 of the regulations) arising directly from the execution of the instructions referred to in section 1, in particular (but not exclusively) any disputes between it and MTS S.p.A., its counterparties, clients or any third parties whatsoever. The Bank's obligations shall be limited strictly, for the application of the present power of attorney, to checking that the instructions received from MTS S.p.A. are conform to the instructions issued by the NBB-SSS to the participants, the NBB-SSS regulations and the rules governing the operation of the SWIFT system (those rules being replaced, in cases where the last sentence in the third paragraph of section 1 applies, by the conditions determined by the Bank in accordance with that same sentence) and rejecting any such instructions which do not conform. For the fulfilment of those obligations, the Bank shall be subject to the rules on liability defined by article 7 of the regulations;

c) to inform the Bank in writing, without delay, of any withdrawal of the authorisation given to the Bank in section 1 of this document. The participant recognises that such withdrawal shall, however, only take effect, and thus entail an obligation on the Bank to refuse instructions sent by MTS S.p.A., in the case of instructions sent on or after the NBB-SSS working day following the date on which the Bank receives notification of the said withdrawal.

Present power of attorney shall be governed by Belgian law.

Done at ……., on……..

Authorised signature(s)

NBB – Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Tel.: +32 (0)2 221 36 00
sss@nbb.be

Annex 18.6

POWER OF ATTORNEY EUROMTS LIMITED

DELETED

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 18.7

LCH SA
POWER OF ATTORNEY
Securities clearing activities

The undersigned,

_____
[DENOMINATION OF THE PARTICIPANT]

with a share capital of_____having its registered office at _____
_____

registered with the registry of legal entities of _____(Country) with the number: _____

hereby represented by : _____

Mr/Ms _____

[NAME _____

[TITLE _____

and

Mr/Ms _____

[NAME _____

[TITLE _____

hereafter referred to as the "Participant";

Please return one original copy to Membership Department –
LCH SA – 18, rue du Quatre Septembre 75002 Paris
(a scanned copy will be sent to the National Bank of Belgium)

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 18.7

Participant of the securities settlement system of National Bank of Belgium, a *Société Anonyme* incorporated under the laws of Belgium, having its registered office at Boulevard de Berlaimont 14, 1000 Bruxelles, Belgium, registered with the registry of legal entities of Belgium under the number 0203.201.340 and having a capital of 10 000 000,00 euros" (hereafter referred to as the "NBB"):

□ Is a Clearing Member Firm (hereafter referred to as the "CMF")

or,

□ Acts in capacity of Settlement Agent of the following CMF:

Name of the CMF: _____

with a share capital of_____having its registered office at :_____

registered with the registry of legal entities of : _____(Country)

with the number : _____

CMF BIC 11: _____

CMF Account number: _____

hereby represented by:

Mr/Ms _____

[NAME _____

[TITLE _____

and

Mr/Ms _____

[NAME _____

[TITLE _____

Please return one original copy to Membership Department –
LCH SA – 18, rue du Quatre Septembre 75002 Paris
(a scanned copy will be sent to the National Bank of Belgium)

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 18.7

The Participant hereby grants a power of attorney to:

Banque Centrale de Compensation SA, "Société Anonyme" acting as a Clearing House as defined by Article L.440-1 of the French Monetary and Financial Code (*Code Monétaire et Financier*), with a share capital of 113 066 860,26 €, having its registered office at 18 rue du Quatre Septembre – 75002 Paris, France, registered with the registry of legal entities of Paris under the number 692 032 485, with the Bank Identifier Code (BIC) : BACPFRPPXXX (or any other Bank Identifier as may be notified by LCH SA to NBB from time to time) and herein referred to as "LCH SA";

- to send to T2S/NBB-SSS by means of SWIFT messages or through the T2S GUI / NBB-SSS RAMSES GUI settlement instructions to debit and credit the following Securities Account(s) opened in NBB in order to comply with the settlement obligations deriving from the Cleared Transactions carried out on Belgian bonds settled in NBB.

- to cancel any registered settlement instruction, in order to manage a buy-in, a default or service closure, pursuant to the conditions set out in the Clearing Rules of LCH SA, or for any other technical reason which requires doing so (to the extent such request for cancellation is not in contradiction with the Terms and Conditions of the NBB and the moment of irrevocability and enforceability of settlement "SF III" has not been reached yet).

The termination of this power of attorney must be notified in writing to NBB in accordance with the provisions of the NBB Terms and Conditions.

This power of attorney is governed by the laws of Belgium.

Drawn up and duly executed in __ original copies at_____ on _____, each party declares having received an original.

_____

[NAME OF THE PARTICIPANT]

Please return one original copy to Membership Department –
LCH SA – 18, rue du Quatre Septembre 75002 Paris
(a scanned copy will be sent to the National Bank of Belgium)

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Name:	Name:
Title:	Title:

Contact Person:
Address:
Tel:
Email:

[NAME OF THE CLEARING MEMBER FIRM]

Name:	Name:
Title:	Title:

Contact Person:
Address:
Tel:
Email:

Please return one original copy to Membership Department –
LCH SA – 18, rue du Quatre Septembre 75002 Paris
(a scanned copy will be sent to the National Bank of Belgium)

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 18.7

ANNEX

LCH SA
POWER OF ATTORNEY
Securities clearing activities

Denomination of the Participant: _____

Denomination of the CMF (if different from the Participant): _____

_____

CSD	Participant BIC 11	SAC in T2S
NBB		

Please return one original copy to Membership Department –
LCH SA – 18, rue du Quatre Septembre 75002 Paris
(a scanned copy will be sent to the National Bank of Belgium)

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 18.8

POWER OF ATTORNEY

Foreign currency Cash Account (FCA) – Dedicated Transfer Account (DTA)

The company .....
having its registered office at .....
hereafter represented by .....
Participant in the securities settlement system operated by the National Bank of Belgium ("the NBB-SSS")
with BIC11:
hereafter "the Participant";

The company .....
having its registered office at .....
hereafter represented by .....
Hereafter "the Foreign currency cash Provider" or "the Participant's Foreign currency cash Provider";

The National Bank of Belgium incorporated under the laws of Belgium having its registered office at Boulevard de Berlaimont 14, BE-1000 Brussels, registered with the registry of legal entities of Belgium under the number 0203.201.340,
Hereafter "the NBB";

WHEREAS

The Participant has opted for the Foreign currency financial service offered by the NBB-SSS in accordance with the Terms and conditions governing the participation in the NBB-SSS (the "NBB-SSS Terms and Conditions");

When opted for by the Participant, the NBB shall support the settlement of the cash leg in Foreign currencies relating to securities denominated in Foreign currencies registered in the NBB-SSS (the "NBB-SSS Foreign currency financial service"): the NBB shall facilitate the settlement of the cash leg in Foreign currencies eligible for DVP transactions, including the settlement of Corporate Actions;

For DVP transactions in Foreign currencies, cash debits and credits entailed by the settlement in the NBB-SSS of securities denominated in Foreign currencies shall be registered on the Participant's Foreign currency Cash Account. When the Participant acts as a buyer of securities denominated in

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Foreign currencies, the Participant shall entitle the NBB with the power to instruct debits in any of the designated FCA in accordance with the NBB-SSS Terms and Conditions;

The settlement of Corporate Actions shall be processed on the Financial currency Cash Account (FCA) and on the Dedicated Transfer Account (DTA) of the Participant acting as Paying Agent. When the Participant acts as Paying Agent, the Participant shall entitle the NBB with the power to instruct debits in any of the designated FCA and in any of the designated DTA in accordance with the NBB-SSS Terms and Conditions.

IN CONSIDERATION THEREOF:

1. The Participant acting as a buyer of securities denominated in Foreign currencies authorises the NBB which accepts, to instruct the Participant's Foreign currency cash Provider to debit any of the designated FCA to be used for the cash leg in Foreign currency in accordance with the NBB-SSS Terms and Conditions and the procedure set out in Annex 27.

2. The Participant acting as Paying Agent (the Foreign currency Paying Agent) authorises the NBB which accepts, to instruct the Participant's Foreign currency cash Provider to debit any of the designated FCA to be used for the cash leg in Foreign currency. The Foreign currency Paying Agent authorises also the NBB which accepts, to instruct the Participant's Foreign currency cash Provider to debit any of the designated DTA in accordance with the NBB-SSS Terms and Conditions and the procedure set out in Annex 27.

3. The Participant recognises that such instructions to debit a designated FCA and a designated DTA are binding it vis-à-vis its Foreign currency cash Provider, the NBB and third parties just as if they had been issued by the Participant itself (including, but not exclusively for the purpose of Article 8.2 of the NBB-SSS Terms and Conditions).

4. The Participant authorises its Foreign currency cash Provider to accept instructions by the NBB itself which are validly addressed on its behalf and to deal with such instructions.

   The instructions by the NBB to debit an FCA shall only relate to the following designated FCAs for which the mandate is exclusively valid and starts from the accompanying date:

   Foreign currency Cash Account: .....
   Foreign currency cash Provider: .....
   Start Date: .....

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

5. The instructions by the NBB to debit a DTA shall only relate to the following designated DTAs for which the mandate is exclusively valid and starts from the accompanying date:

   Dedicated Transfer Account: .....
   Foreign currency cash Provider: .....
   Starting Date: .....

   The instructions referred to above shall always mention a Securities Account number of the Participant and shall be transmitted by the SWIFT network or through the NBB-SSS Ramses GUI / T2S GUI in accordance with the provisions laid down in the NBB-SSS Terms and Conditions for those means of communication.

   The instructing party will either use:
   the following BIC11 (ISO 15022): .....
   or DN (ISO 20022): .....
   to send its instructions to the NBB-SSS and/or T2S.

   If the SWIFT network or the NBB-SSS Ramses GUI should be unavailable, even temporarily, the NBB may, however, accept instructions transmitted by other means in the cases and under the conditions that the NBB shall determine at its own discretion.

6. Furthermore, the Participant undertakes:

   a. to take the necessary internal measures to ensure that sufficient funds are available on designated FCAs to allow the settlement of the transaction in Foreign currency on the Intended settlement date;
   b. to indemnify the NBB against any adverse consequences (except in so far as such consequences are due to the NBB's own negligence, or the negligence of its employees or persons made responsible by the Bank for the execution of tasks, rendering the NBB liable in accordance with article 7.3 of the NBB-SSS Terms and Conditions) arising directly from the execution of the instructions referred to above, in particular (but not exclusively) any disputes between it and its Foreign currency cash Provider, the NBB, or any third parties whatsoever. The NBB’s obligations shall be limited strictly, for the application of the present power of attorney, to support the settlement of the cash leg in eligible Foreign currencies relating to securities denominated in Foreign currencies and registered in the NBB-SSS For the fulfilment of those obligations, the NBB shall be subject to the provisions on liability defined by article 7.3 of the Terms and Conditions;

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

c. to inform the NBB-SSS in writing by e-signed e-mail, without delay, of any changes relating to the designated FCAs and/or DTAs;
d. to inform the NBB-SSS in writing by e-signed e-mail, without delay of the withdrawal of this power of attorney. The Participant recognises that such withdrawal shall, however, take effect after the NBB-SSS Business day following the date on which the NBB receives the writing confirmation of the said withdrawal. The withdrawal may never take effect before the final settlement of all transactions in Foreign currencies initiated by the Participant in accordance with the NBB-SSS Terms and Conditions.

The present power of attorney shall be governed by Belgian law.

Done at ....., on .....

Authorised signature(s)

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 18.9

T2S CROSS-BORDER SETTLEMENT

"Already Matched" Instructions

This form is to be completed if you intend to receive and set-up cross-border instructions with the flag "already matched" with a Participant in a CSD linked to NBB-SSS. With this order you confirm that a power of attorney ("POA") for "already matched" cross-border instructions is maintained on the T2S platform.

1. Receive: The associated rights enable the counterparty ("POA Grantee") at the receiver CSD[1] to perform instruction management on selected SAC(s) from the NBB-SSS Participant ("POA Grantor").
2. Set-up: The associated rights allow the NBB-SSS Participant to perform instruction management for a SAC in a CSD linked to NBB-SSS.

Please note that the NBB-SSS Participant and the counterparty at the linked CSD must instruct both involved CSDs to maintain the related POA with the associated rights ("privileges") on T2S. A cross-border instruction with the flag "already matched" can only be successfully created, modified or cancelled if the rights have been granted by both mandated CSDs. NBB-SSS can only set up the configuration of the SAC(s) maintained at NBB-SSS.

NBB-SSS BIC11: NBBEBEBB216
NBB-SSS Participant BIC11 (Grantor): .....
NBB-SSS Participant Name: .....
NBB-SSS Participant SAC(s): .....
.....
.....

Receiving CSD BIC11: .....
Receiving CSD Participant BIC11: .....
Receiving CSD Participant Name (Grantee): .....
Receiving CSD Participant SAC(s)[2]: .....
.....
.....

[1] Receiver CSDs with a link to NBB-SSS: https://www.nbb.be/nl/list-nbb-investor-icsds
[2] Optional.

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Date "From"[3]: .....

We, the undersigned NBB-SSS Participant, hereby request the NBB-SSS to maintain the configuration for cross-border instructions with the flag "already matched" at the receiving CSD.

Contact person (first name and surname): .....

Telephone: .....

E-mail: .....

Signature:

[3] It is recommended to test the requested set-up prior to deployment in production.

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 19.1

ISSUANCE FEES

The following table lists the tariffs (excluding VAT) used to determine the issuance fee, which is payable by the Issuer to the NBB for each service agreement, unless otherwise specified in the agreement or in the NBB-SSS T&C Art. 8.1.6[1].

This fee shall be charged by automatically debiting the cash account of the Issuer or when represented by a Paying Agent, by automatically debiting the latter's cash account.

I. HANDLING CHARGES	**Tariff**	**Due**
1. One-off fee for each service agreement. These fees apply when the issuance is 'plain vanilla', ➢ €1000 Treasury certificates, Deposit certificates, general Dematerialised securities ➢ €2750 Securities with bond factors Depending on the administrative work by the NBB in preparation for the agreement, the handling charges may be increased.	Min. € 1.000	After signing the contract.
II. DATA CREATION		
1. One-off fee per ISIN code for its creation.	€ 100	After establishment of the ISIN code in NBB-SSS.
2. If the coupon rates are not the same for all the coupons of a security and/or require a manual creation of the coupons by an NBB-SSS operator.	€ 50	After creation of the coupon in NBB-SSS.
3. One-off fee for all coupons for their creation, if all necessary details of all coupons are known prior to the issue.	€ 100	After creation of the coupons in NBB-SSS.
4. One-off fee per ISIN code for which bond factors are provided.	€ 250	After establishment of the ISIN code in NBB-SSS.
5. One-off fee per bond factor for its creation.	€ 100	After creation of the bond factor in NBB-SSS.
6. Fee for booking out securities in order to carry out a partial circulation reduction which is not feasible by means of a bond factor.	€250	After the repayment settlement date.
7. Fee for booking out securities in order to carry out a complete cancellation of the circulation which is not feasible through the settlement system's existing automatic standard procedures.	€250	After the cancellation settlement date.
8. One-off fee per cash distribution for its creation	€100	After creation of the cash distribution in NBB-SSS

[1] Green, Social and Sustainability Bonds will not be subject to Issuance fees in the NBB-SSS

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

III. FINANCIAL SERVICE	Tariff	Due
1. ISIN code for the capital reimbursement in T2S currency or foreign currency on its final due date.	€100	At reimbursement.
2. Fee per coupon for payment of the outstanding interest.	€100	After the coupon due date.
4. One-off fee per bond factor for the partial repayment of capital on the day on which the bond factor becomes effective.	€100	After the day on which the bond factor becomes effective.
5. Fee for carrying out the cash part of a partial capital repayment which is not feasible through a bond factor.	€250	After the repayment settlement date.
6. Fee for carrying out the cash part of a full capital reimbursement which is not feasible through the settlement system's existing automatic standard procedures.	€250	After the repayment settlement date.
7. Fee for Cash distribution	€100	At cash distribution date
IV. CUSTODY		
1. Annual fee per ISIN code for physical securities.	€250	The fee is payable after the issue date, and after each anniversary of the latter, for as long as the security has not reached its final due date.

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

V. VARIOUS SERVICES		
1. Fee for various services which may have to be provided under the agreement within the framework of the issue by the NBB, and which are not described elsewhere in the table.	€ 50 / for each initial hour	Determined on a case-by-case basis.
2. Contribution as CSD to the labelling process for the STEP label and supply of statistical data as SSS to the ECB for labelled issue programmes.	free of charge	Contribution as CSD to the labelling process for the STEP label and supply of statistical data as SSS to the ECB for labelled issue programmes.
3. Periodic fee per successive period of 12 months during which there has been no circulation within the framework of a service agreement.	€250	After the relevant period.
4. Fee on an annual percentage basis on the nominal average circulation (adjusted, if required, for the bond factor) of an ISIN code.		After each anniversary of the ISIN code issue date, for as long as the security has not reached its final due date, and after the due date following maturity.
circulation ≤ € 0.5 billion		0.0005% of the circulation
€ 0.5 billion < circulation ≤ € 1 billion		€ 2 500
€ 1 billion < circulation ≤ € 2 billion		€ 3 000
€ 2 billion < circulation ≤ € 3 billion		€ 3 500
€ 3 billion < circulation ≤ € 5 billion		€ 4 000
€ 5 billion < circulation ≤ €10 billion		€ 5 000
€ 10 billion < circulation		€ 7 000

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 19.2

SERVICE CONTRACT

For the Issuance of Fixed-Income Securities

Between

NATIONALE BANK VAN BELGIË N.V.,
having its registered office at Boulevard de Berlaimont 14, 1000 Brussels,
represented for the purposes of this contract by
.....
.....
hereafter “the NBB”, of the one part

and

.....
having its registered office at .....
with Legal Entity Identifier .....
represented for the purposes of this contract by
.....
.....
hereafter “the Issuer”

and

.....
having its registered office at .....
represented for the purposes of this contract by
.....
.....
hereafter “the Paying Agent”, of the other part.

The NBB, the Issuer and the Paying Agent are referred to hereafter jointly as “the Parties”.

IT IS HEREBY AGREED AS FOLLOWS:

Article 1 – Subject

1.1. The Issuer commissions the NBB, which hereby agrees, to provide central securities depository services relating to (*make a choice by ticking the relevant box*):

- ☐ dematerialised treasury certificates and certificates of deposit, governed by the Law of 22 July 1991;
- ☐ dematerialised bonds governed by the Belgian company Code;
- ☐ other fixed-income securities held under the system provided for in the Royal Decree n°62 of 10 November 1967 on the deposit of fungible financial instruments and the settlement of transactions involving such instruments such as e.g. collective bearer securities (collective bonds);

described below, being securities issued by the Issuer

.....[1]

denominated in (make a choice by ticking the relevant box(es)):

- ☐ euro;
- ☐ currencies other than the euro and the Danish krone, for which the European Central Bank publishes the daily reference exchange rates against the euro ("Foreign currencies", see Article 7):
  - □ the Issuer and its Paying Agent opt in for the NBB-SSS Foreign currency financial service for corporate according to Article 7.2.1.
  - □ the Issuer and its Paying Agent opt out for the NBB-SSS Foreign currency financial service for corporate according to Article 7.2.2.

1.2. The Issuer enters into a Paying Agent contract with a direct Participant in the Bank's securities settlement system (hereafter the "NBB-SSS"). A Paying Agent contract is not required if the Issuer is a direct Participant in the NBB-SSS.

The Paying Agent commits to complying with the conditions laid down in this contract.

The commitments and rights of the Issuer specified in this contract shall be implemented in the NBB-SSS by or with respect to the Paying Agent in its capacity as the Issuer's agent.

If the Paying Agent is replaced by another Paying Agent or if the Paying Agent ceases for any reason to be a direct Participant in the NBB-SSS, the Issuer shall immediately appoint a new Paying

[1] Subject of the issue to be specified. If this is not an issue programme, the ISIN code of the bonds must be stated.

Agent and notify the NBB-SSS in writing. An annex to this contract will then be drawn up with the new Paying Agent. The new Paying Agent must be a direct Participant in the NBB-SSS. A Paying Agent which gives up its duties for any circumstance must continue to perform its duties until the new Paying Agent is able to take them over in full.

1.3. Capitalised terms which are not defined in this service contract shall have the same meaning as referred to in the Terms and Conditions governing the participation in the NBB-SSS.

Article 2 - Representation by the Issuer

2.1. The Issuer confirms that the execution of this service contract complies with the Issuer's articles of association.

2.2. The NBB reserves the right to suspend the execution of the contract in case of breach of this representation. Such a suspension shall be immediately notified in writing or by e-signed mail to the Issuer and the Participants. The settlement of transactions on the securities can be temporarily suspended until measures necessary to remedy the breach have been taken.

Article 3 - Information and documents to be supplied to the NBB-SSS

3.1. The Issuer shall supply the following data and documents to the NBB-SSS at least one week before the start of the issue programme:

1° the terms and conditions governing the issue and the prospectus, and all other documents required by the law and implementing decrees applying to the issue, and in general all documents intended for the investors;

2° the characteristics specific to each security series and any information relevant for the administration of the issue by NBB-SSS, including the following documents:

- the Issuance Program (IP) summary (see Annex 19.4).
- the Issuer Information Sheet (in case it concerns a new Issuer - see Annex 19.3a).

The Issuer must ensure that the status of its Legal Entity Identifier (LEI) is either "Issued", "Pending Transfer" or "Pending Archival". In all cases, it shall immediately notice the CSD of any change related to the LEI. In the absence of a valid LEI of the Issuer, the NBB-SSS shall not accept the Issuance.

3° the executed copy of this service contract, signed by authorized representatives of the Issuer and of the Paying Agent.

If the data and documents referred to in this provision are not submitted within two Business days before the start of the issue, the NBB-SSS may decide to delay the start of the issue.

For the purpose of this contract, "Business day" means an NBB-SSS opening day as referred to in the Terms and Conditions governing the participation in the NBB-SSS.

3.2. If the service contract concerns the issue of dematerialised treasury certificates, the Issuer shall submit the following data as soon as they are published:

- supplements to the prospectus;
- the updated versions and the half-yearly reports and tables concerning the activities and results which Issuers of treasury certificates are required to produce in accordance with Article 2 and Article 5, §2 and 3 of the Law of 22 July 1991 and Article 22 of the Royal Decree of 14 October 1991 on treasury certificates and certificates of deposit, or the latest half-yearly report published in accordance with the provisions of the Royal Decree of 14 November 2007 on the obligations upon Issuers of financial instruments admitted to trading on a regulated market.

3.3. Communication of information and documents as referred to in Article 3.1 and 3.2 are intended to inform the NBB-SSS of the terms and conditions of the issue and of the rights attached to the issued securities. It does not relieve the Issuer of the obligation to provide the investors with the information stipulated by law and by the regulations for the issue of the concerned securities, and in general, to ensure that the issue complies with any conditions laid down by law, regulation or administrative provision, applicable to the issue.

The NBB-SSS will notify its Participants of the admission to the system of each new issue and of the principal rights attached to the issued securities.

3.4. The NBB is not required to examine whether the Issuer fulfils the conditions laid down by the Law and its implementing regulation for the issue. The Issuer and the Paying Agent jointly and severally guarantee the Bank that no issue will take place if one or more of those conditions are not fulfilled.

Article 4 - Conduct of the issue

4.1. In addition to the data and documents supplied in accordance with Article 3.1, the Issuer shall communicate the following data to NBB-SSS as soon as possible and in any event no later than 11:00 CET on the subscription settlement day:

- the Security information form (see Annex 19.3b), including the following information:
  - the ISIN code assigned to the securities;
  - the currency of issue;
  - the nominal amount of securities actually subscribed to be entered in the Securities Accounts;
  - the subscription price;
  - the redemption price;
  - the subscription settlement date;
  - the redemption date;
  - the interest rate and, if appropriate, the yield on the securities with a view to determine the accrued interest on those securities in accordance with Articles 8 and 9 of the Royal Decree

of 26 May 1994 on the deduction and payment of withholding tax on income from movable assets in accordance with Chapter 1 of the Law of 6 August 1993 on transactions in certain securities, as amended from time to time; and,

- the interest payment details.

- In the case of securities with a variable interest rate, the data referred to in the last two indents above must be communicated no later than 11:00 CET on the Business day preceding the first day of each interest period.

The securities are identified in the NBB-SSS by their ISIN code. It is the responsibility of the Issuer to provide the NBB-SSS with the ISIN code of the security as soon as possible and in accordance with Article 4.1. No security can be issued and no instruction can be accepted by the NBB-SSS as long as the ISIN code of the security has not yet been communicated by the Issuer. The NBB-SSS cannot be held responsible for any rejected instruction due to late communication of the ISIN code.

Information relating to the characteristics of the securities communicated by the Issuer in accordance with Article 4.1 or in accordance with any other service contract for the issuance of fixed-Income Securities entered into by the Issuer with the NBB may be published by the NBB on the NBB-SSS website and updated during the lifetime of the issued securities. The Issuer agrees that such information shall include the outstanding amount (e.g., the outstanding amount of an ISIN is the initial amount of the ISIN including updates from early partial redemptions, tapping, pool factor, etc.), including in circumstances where it could constitute sensitive information. The data are published for information purposes only.

4.2. In case of an issue of dematerialised treasury certificates, certificates of deposit or dematerialised bonds, the NBB-SSS shall on the subscription settlement date credit the securities account of the Issuer or of his Paying Agent in accordance with the conditions laid down in the Terms and Conditions governing the participation in the NBB-SSS.

For collective bonds: the Issuer or the Paying Agent acting on behalf of the Issuer shall hand over to the NBB-SSS by no later than 11:00 CET on the issue settlement date, a collective bearer security representing the bonds issued. That security, duly authenticated by the Issuer, shall conform to the law governing the security and shall represent all the issue rights. The NBB-SSS shall credit the Securities Account of the Issuer or of his Paying Agent, with the nominal amount of the securities represented by the collective bearer security that the Issuer or his Paying Agent has handed over to the NBB-SSS. That amount shall be credited on the subscription settlement date following the issue of the collective security in accordance with the conditions laid down in the Terms and Conditions governing the participation in the NBB-SSS (see also Article 5 below).

4.3. The Issuer or his Paying Agent shall then by no later than the subscription settlement date allocate the securities issued among the institutions which maintain the subscribers' securities accounts in accordance with the Terms and Conditions governing the participation in the NBB-SSS.

4.4. In case of issuance of dematerialised bonds, on the subscription settlement date, the Issuer shall enter the total of the dematerialised securities in circulation in the register of registered securities ("registre des titres nominatifs"/"register van de effecten op naam") in the name of the NBB-SSS in accordance with Article 7:35 of the Code of Companies and Associations. The Issuer shall make the necessary amendments in the register when dematerialised securities are subsequently repaid, converted to registered securities or created as a result of the conversion of registered securities.

4.5. The NBB performs the issue according to the Terms and Conditions governing the NBB-SSS and following the instructions provided by the Issuer in accordance with Articles 3.1, 2° and 4.1 and provided that those instructions are compatible with the Terms and Conditions governing the NBB-SSS. The NBB shall not verify whether these instructions comply with the Terms and Conditions governing the issue, the prospectus or all other documents applicable to the issue of the securities.

The NBB can never be held liable in relation to the Issuer, his Paying Agent or any third person on account of

- book entries which have formed the subject of the communication to the NBB-SSS in accordance with Articles 3.1,2°. and 4.1 (including but not exclusively in cases where the amount specified for the programme in the issue prospectus has been exceeded), or
- errors or omissions committed by the Issuer in connection with the communications referred to in Articles 3.1,2° and 4.1.

Article 5 – Custody, entry in accounts and deposit of securities issued under the fungibility regime

5.1. The NBB shall act as custodian of the collective security representing the individual debt securities (collective bearer bond) or shall act as nominee (registered securities) for the account of the Participants in the NBB-SSS, for each Participant in the sum of the nominal amount of the securities recorded on its Securities Account.

The collective security representing the entries on the Securities Accounts shall constitute a single deposit held in accordance with the fungibility principle.

The NBB is entitled to entrust the collective security to a sub-depository.

5.2. Within ten Business Days of the reimbursement of the securities, the NBB or its agent shall deliver, against a certificate of receipt, the collective bearer security to the Issuer or its agent. The collective bearer security shall be perforated to indicate its cancellation.

Article 6 - Payment of interests and of refundable principal on securities denominated in euro

6.1. The interest on securities denominated in euro is payable by the NBB-SSS to the Participants at the intervals indicated by the Issuer and based on the Interest payment date and the annual interest rate communicated by the Issuer in accordance with Article 4.1.

6.2. On the Interest payment date of the securities (for the purposes of this contract, "Interest payment date" means the date on which the Issuer must pay the amount of interest in accordance with the instructions given to the NBB-SSS by the Issuer or, if that date is not a Business day, the next Business day), the NBB-SSS shall execute the cash debits and credits as follows:

1° the NBB-SSS automatically debits the total amount of the interest from the Dedicated Cash Account of the Issuer or of his Paying Agent in the NBB's or another central bank's books during the night-time settlement window and in accordance with the conditions specified in the Terms and Conditions governing the participation in the NBB-SSS;

2° subject to the debit described under 1°, the NBB-SSS automatically credits the amount of the net interest (determined on the basis of the securities accounts balances at the end of the Business day preceding the interest payment date) on the Dedicated Cash Account of the Participants having a position in the concerned security, and creates a separate dedicated withholding tax transaction on income from movable assets when applicable. That interest is credited during the night-time settlement window after debiting the total amount as described in 6.2.1. and in accordance with the conditions specified in the Terms and Conditions governing the participation in the NBB-SSS.

The interest is calculated as follows:

- the amount of interest debited in accordance with paragraph 1, 1° shall be calculated by applying the interest rate to the total interest-bearing amount of the issuance, the outcome being rounded down to the nearest cent;
- the amounts of interest to be credited to each of the beneficiary and for each account in accordance with paragraph 1, 2° shall be calculated by applying the interest rate to the interest-bearing amount of the concerned securities held in account, the outcome being rounded down to the nearest cent;
- When calculating the interest to be paid, if necessary, the NBB-SSS takes the "Bond factor" into account, which is the percentage of the capital outstanding over the interest period in relation to the original amount issued. The fraction made up by the Bond factor is expressed in a number with twelve decimals. The Bond factor to be applied for any new interest period shall be notified to the NBB at the latest by 15:00 CET on the second Business day preceding each interest period.

6.3. On the Principal reimbursement date of the securities, the NBB-SSS shall execute the cash debits and credits as follows:

1° the NBB-SSS automatically debits the amount of the refundable principal from the Dedicated Cash Account of the Issuer or of his Paying Agent in the NBB's or other central bank's books during the night-time settlement window and in accordance with the conditions specified in the Terms and Conditions governing the participation in the NBB-SSS;

2° subject to the debit described under 1°, the NBB-SSS automatically credits on the Dedicated Cash Accounts of the Participants having a position in the concerned security the amount of the refundable principal (determined on the basis of the securities accounts balances at the end of the Business day preceding the Principal reimbursement date), and creates a separate dedicated withholding tax transaction on income from movable assets when applicable. The reimbursements are credited during the night-time settlement window after debiting the total amount as described in 6.3.1. and in accordance with the conditions specified in the Terms and Conditions governing the participation in the NBB-SSS.

For the purposes of this contract, "Principal reimbursement date" means the date on which the Issuer must reimburse the principal in accordance with the instructions given to the NBB-SSS by the Issuer or, if that date is not a Business day, the next Business day.

On the Principal reimbursement date for final redemption of the securities, the Participants' Securities Accounts shall be debited in order to cancel the amount of the reimbursed securities.

6.4. A collective bearer security has no coupons.

The NBB-SSS is exempt from presenting this security to the Issuer in order to obtain payment of interests or payment of the refundable principal.

6.5. The Issuer undertakes, if appropriate via his Paying Agent, to have sufficient funds available to be able to pay the amounts due by way of capital and interest on the due date.

Article 7 - Payment of interests and of the refundable capital on dematerialised securities denominated in Foreign currencies

7.1. The following provisions govern exclusively the securities denominated in Foreign currencies which are not participating in T2S. For the purpose of this contract, "T2S" stands for "TARGET2-Securities" and means the Eurosystem's single technical settlement solution enabling CSDs and national central banks to provide core, borderless and neutral securities settlement services in central bank money in Europe. The securities denominated in Foreign currencies participating in T2S, i.e. DKK, are handled in accordance with Article 6.

7.2. Without prejudice to the application of the tax rules, the Issuer or its Paying Agent may opt (Article 1.1) for the NBB-SSS Foreign currency financial service. The NBB-SSS Foreign currency financial service provides settlement through the system of the cash leg in eligible foreign currencies for

Corporate Actions (i.e. payment of interests and of the refundable capital) relating to securities denominated in Foreign currencies. The NBB-SSS Foreign currency financial service shall be provided by the NBB-SSS in accordance with the conditions specified in the Terms and Conditions governing the participation in the NBB-SSS.

7.2.1. When the Issuer and its Paying Agent opt in for the NBB-SSS Foreign currency financial service, the Paying Agent and each Participant having a position in the relevant securities ('investor participant') shall have a Foreign currency Cash Account (FCA) in accordance with the conditions specified in the Terms and Conditions governing the participation in the NBB-SSS. Each Paying Agent shall entitle the NBB-SSS with the power to instruct any debits movements on its designated FCA.

The Paying Agent shall also have a Dedicated Transfer Account (DTA) at the Foreign currency cash Provider of its choice in accordance with the Terms and Conditions governing the participation in the NBB-SSS. The Paying Agent shall provide a Power of Attorney (Annex 18.7) to the NBB to allow the NBB debiting the Dedicated Transfer Account for the Corporate actions. The Paying Agent shall ensure that sufficient funds are available on the FCA to allow the settlement of the Corporate action on the Intended settlement date. The DTA shall only be used for crediting the full amount paid out by the Paying Agent towards Participants having a position in the relevant securities and subsequently debiting all amounts due to Participants having a position in the relevant securities.

The interest on securities denominated in Foreign currencies is payable by the NBB-SSS to the Participants at the intervals indicated by the Issuer on the basis of the Interest payment date and the annual interest rate communicated by the Issuer in accordance with Article 4.1. The interest payments are generated based on the End Of Day positions in the T2S Day Schedule (between 18:00 – 18:45 CET) on the Participants securities accounts on Record Date. Consequently, securities transfers between different Participants shall be allowed during the Business day preceding an interest payment date or a reimbursement date (no "frozen day").

On the Interest payment date, the NBB-SSS shall execute the cash debits and the cash credits as follows, in accordance with the Terms and Conditions governing the participation in the NBB-SSS:

1° the NBB-SSS automatically debits the total amount of the interests from the Foreign currency Cash Account of the Paying Agent and shall credit this amount on the DTA designated by the Paying Agent;

2° subject to the debit described under 1°, the NBB-SSS automatically debits the amount of net interest (determined on the basis of the securities accounts balances at the end of the Business day preceding the Interest payment date) from the DTA and credits this

amount on the FCA of Participants having a position in the concerned security, and create a separate dedicated withholding tax transaction on income from movables assets when applicable.

The interest is calculated as described in Article 6.2.

On the Principal reimbursement date of the securities, the NBB-SSS shall execute the cash debits and credits as follows, in accordance with the Terms and Conditions governing the participation in the NBB-SSS:

1° the NBB-SSS automatically debits the amount of the refundable principal from the FCA of the Paying Agent and shall credit this amount on the DTA designated by the Paying Agent;

2° subject to the debit described under 1°, the NBB-SSS automatically debits the amount of the refundable principal (determined on the basis of the securities accounts balances at the end of the Business day preceding the Principal reimbursement date) from the DTA and credits this amount on the FCA of Participants having a position in the concerned security, and create a separate dedicated withholding tax transaction on income from movables assets when applicable.

On the principal reimbursement date for final redemption, of the securities, the Participants' Securities Accounts shall be debited in order to cancel the amount of the reimbursed securities.

Payments of interests shall always be processed separately from the reimbursement of the principal even if the Interest payment date and the Principal reimbursement date coincide.

7.2.2. When the Issuer and its Paying Agent opt out for the NBB-SSS Foreign currency financial service, and without prejudice to the application of the tax rules, the NBB-SSS shall not intervene in the payment of the interests and in the reimbursement of the principal of the concerned securities. Such amounts shall be paid by the Issuer or, when applicable, his Paying Agent outside the NBB-SSS to the Participants.

The NBB-SSS shall notify at the event "Start of Day" in the T2S Day Schedule " (between 18:45 and 20:00 CET) of the Business day preceding the Interest payment date or the Principal reimbursement date, the nominal amount of the concerned securities, as recorded in Securities Accounts held in the name of Participants at the end of the second Business day preceding the Interest payment date or the Principal reimbursement date, to the Issuer or his Paying Agent. This notification shall form the basis for the interest and principal payments (outside NBB-SSS) to Participants by the Issuer or his Paying Agent. Consequently, no securities transfers between different Participants shall be allowed during the Business day preceding an interest payment date or a reimbursement date ("frozen day").

On the Interest payment date or the Principal reimbursement date, the Dedicated Cash Account of the Participants having a position in the concerned securities shall be debited in euro with the cash amount of the withholding tax due to the Treasury in accordance with Article 8 of the law of August 6, 1993 concerning transactions in certain securities (as amended from time to time) with its implementing provision governing the conversion to euro of income from securities denominated in monetary units of countries which have not adopted the euro, and with Council Regulation no. 1103/97/EC of June 13, 1997.

On the Principal reimbursement date for final redemption of the securities, the Participants' securities accounts shall be debited in order to cancel the amount of the reimbursed securities, without the NBB checking whether the Paying Agent has performed the corresponding cash payments or not.

Article 8 – Early reimbursement of the issue

The Issuer shall inform the NBB-SSS as soon as possible and no later than five Business days before the early reimbursement date of the exercise of its right the effect an early redemption of the securities. The NBB-SSS shall advise the Participants of the exercise of that right.

Article 9 – Fees payable to the Bank

In payment for the services provided for in this contract, the Issuer shall pay to the NBB a fee which is calculated and collected in accordance with Article 8.1.6. of the Terms and Conditions governing the participation in the NBB-SSS and annex 19.1, including any amendments thereto.

If the Paying Agent opts at a later stage to apply the Bond factor, an additional administrative charge will be levied.

The handling charge in accordance with point I.1 of Annex 19.1 to the Terms and Conditions governing the participation in the NBB-SSS is EUR ……. (excl. VAT) and is payable to the NBB after signature of the contract.

Article 10 – Default by the Issuer

10.1. In the event of default by the Issuer or by his Paying Agent, i.e. in the occurrence of one of the events referred to in Article 10.2.2. of the Terms and Conditions governing the participation in the NBB-SSS, and in the case of a shortage of funds, any reimbursement on the due date or payment of interest due shall be automatically suspended without notice of default until the Issuer or his Paying Agent has executed valid payment of the total capital or the total interests.
The Paying Agent shall inform the NBB-SSS upon receipt of information regarding the opening of Insolvency proceedings against an Issuer.

10.2. If the Issuer is represented by a Paying Agent, the latter must notify the Bank of the Issuer's default or the shortage of funds as early as possible and always before 15:00 CET on the Business day preceding the Principal reimbursement date or the Interest payment date.

After that deadline has elapsed, the Paying Agent is deemed to have approved the execution of the repayments or the interest payments on the due date, and its account will therefore be debited.

The notification to the NBB by the Paying Agent shall be done by e-signed e-mail or, alternatively, by SWIFT (message type MT599) with confirmation within 24 hours by registered mail with a return receipt.

Article 11 – Tax system

The securities registered with the NBB-SSS are subject to the tax rules laid down by the Law of 6 August 1993 on transactions in certain securities and its implementing regulations, particularly with regards to the formulas applicable for the calculation of interests.

With regards to the tax liabilities of the NBB-SSS, the Issuer, the Participants and clients, reference is made to the laws and regulations in force.

Article 12 – Applicable law – Competence

12.1. This service contract, as well as the transactions settled on their basis, shall be governed by and construed in accordance with the laws of Belgium.

12.2. In the event of any dispute arising in connection with the interpretation or execution of this service contract, the Parties shall endeavour to amicably settle it within a reasonable period of time following the invitation thereto by the most diligent Party. If the Parties do not succeed in finding a solution or reaching an agreement in order to settle the dispute, the latter shall be submitted by the most diligent Party to the jurisdiction of the Courts of Brussels.

12.3. In relation to the Issuer and the Paying Agent, the NBB is subject to no obligations or conditions relating to exercise of a right concerning the issued securities other than those specified in this service contract or in the applicable Belgian regulations.

The provisions of this service contract take precedence over any provision to the contrary in the prospectus or in any contract document relating to the issue.

This service contract does not affect the rights of the Issuer or of the Paying Agent in its capacity as an NBB-SSS Participant.

12.4. The Terms and Conditions governing the participation in the NBB-SSS and the regulations and administrative guidelines adopted by the NBB pursuant to the tax rules, including any future amendments, apply wherever no express provision is made in this contract.

12.5. The undersigned Parties to this contract agree that, under the service contract concluded between them on ....., it will no longer be possible to effect new issues from ..... [2].

Article 13 – Electronic signature

In order to electronically execute this service contract, the Parties shall use either a qualified electronic signature within the meaning of the Regulation (UE) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the " e-IDAS Regulation") or the advanced electronic signature generated by the ESCB-PKI token. When using this latter, the Parties acknowledge and agree that the advanced certificate issued by Banco de España in the framework of the ESCB-PKI shall have the same characteristics and probative force than a qualified certificate in the meaning of Article 28 of the e-IDAS Regulation, hereby including the reversal of the burden of proof regarding the authenticity of the signature generated by it.

Article 14 – Entry into force

This Agreement shall enter into force on the date of its signature by the last signing Party.

Done [in three originals[3]] in Brussels, whereby each Party recognizes to have received one original version.

For the Issuer, on .....

For the Paying Agent, on .....

For the National Bank of Belgium, on .....

[2] Dates to be entered. This clause should only be included if this contract refers to a current issue programme for which a contract already exists with the same Paying Agent.

[3] If handwritten signature only.

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 19.2a

SERVICE CONTRACT CONCERNING THE ISSUE OF DEMATERIALISED TREASURY CERTIFICATES AND CERTIFICATES OF DEPOSIT

DELETED

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 19.2b

SERVICE CONTRACT
CONCERNING THE ISSUE OF
DEMATERIALISED BONDS

DELETED

NBB – Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: +32 (0)2 221 22 17
sss@nbb.be

Annex 19.2c

SERVICE CONTRACT CONCERNING THE ISSUE OF COLLECTIVE BONDS

DELETED

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

Annex 19.3a

ISSUER'S INFORMATION SHEET

Issuer (1) .....

Name .....

Department name .....

Legal Entity Identifier .....

Address .....
.....
.....

Contact person .....

Telephone .....

Fax .....

e-mail addresses
* normal address: .....
* notice of coupon payments: .....
* notice of capital repayments: .....

Company number .....

VAT liable (2)	yes	no

Language (2)	Dutch	French	English

This sheet must be sent to NBB-SSS at least two business days before the commencement of the issue(s).

Kindly send us a copy of your official list of legally-binding signatures as well.

Date: .....

Authentic signatures: Company stamp:

---

(1) This space reserved for the NBB
(2) Delete as applicable.

NBB – Payments and Securities Service
Securities Settlement System
Boulevard de Berlaimont 14
BE-1000 Brussels
Phone + 32 (0)2 221 22 17
isin@nbb.be

SECURITY INFORMATION FORM

-Select Applicable-

ISIN Code: BE ..... **CFI:** D..... **Program Nr:** .....

Type: -Select Applicable-

Issuer Number: ..... Issuer Name: .....

Paying Agent BIC: ..... Paying Agent Name: .....

Currency: ..... **ISSU Amount:** ..... Amortisation (Bond Factor): -Select Applicable-

Issuance Date: ..... **Maturity Date:** .....

Issuance Price[1]: ..... % **Redemption Price**[1]: ..... %

Interest:

☐ **Discount:** - Weighted Average Rate[1]: .....%

- Day Count Fraction: -Select Applicable-

☐ **Coupon(s):** - Interest Rate[1]: -Select Applicable- ..... %

- Coupon Periodicity:

☐ Regular unadjusted: - Day Count Fraction: -Select Applicable-

- Periodicity: -Select Applicable-

Regular unadjusted and only one coupon irregular: -Select Applicable-

☐ Regular adjusted: - Day Count Fraction: -Select Applicable-

☐ Irregular adjusted: - Day Count Fraction: -Select Applicable-

- Maturity date first coupon: .....

- Capitalisation Options:

☐ Capitalisation of Coupon: Actual Yield (Art. 9 RD 26/05/94) [1]: ..... %

☐ Payment in Kind: Actual Yield (Art. 9 RD 26/05/94) [1]:..... %

☐ **Zero Coupon:** - Actual Yield (Art. 9 RD 26/05/94)[1]: ..... %

Minimum per transaction: ..... Multiple: .....

Regime in X/N: -Select Applicable-

Remarks: .....

.....

Name(s) and Authorized Signature(s): **Date:**

Box Reserved for NBB	Program n°:	Formula:	Coupon Periodicity:.....
	Category:		

[1] *9 digits after decimal point.*

This form shall be sent to the NBB-SSS as soon as possible and in any event no later than 11:00 CET on the issuance date.

P
I
A
2
1

NBB – Payments and Securities Service
Securities Settlement System
Boulevard de Berlaimont 14
BE-1000 Brussels
Phone + 32 (0)2 221 36 00
sss@nbb.be

COUPON FORM

ISIN Code: BE..... Currency: - Select -

ISIN Start Date: ..... ISIN Maturity Date (Calculation Date): .....

Program Nr.: ..... Paying Agent: - Select -

Issuer Nr. / Name: ..... / .....

Period from ..... to .....

Payment Date: .....

Day Count Fraction: - Select -

Rate: ..... %

Cash Value: ..... - Select -

Corporate Action ID (Reserved for NBB): BE..... / .....

Remarks:

Date:	Name and Authorized Signature:

This form shall be sent to the NBB-SSS as soon as possible and in any event no later than 11:00 CET on the business day preceding the coupon payment date.

P
I
A
2
1

NBB – Payments and Securities Service
Securities Settlement System
Boulevard de Berlaimont 14
BE-1000 Brussels
Phone + 32 (0)2 221 36 00
sss@nbb.be

NBB-SSS ISSUANCE PROGRAM (IP) SUMMARY

Documented on Page(s):

Nature: - Select - .....

Issuer: ....

Start Date: ..... **End Date:** ....

Program Size: ....

Currency: ☐ EUR ☐ GBP ☐ USD ☐ Other .....

Term: ☐ Short Term **(**Money Market) ☐ Long Term (Capital Market) .....

Type of Program: - Select - .....

Place of Listing: - Select - .....

Governing Law: - Select - .....

Foreign Currency Corporate Action Management by NBB-SSS[1]: - Select - .....

ADDITIONAL SPECIFICATIONS

X/N Status[2]: - Select - .....

Interest: ☐ Fixed ☐ Variable .....

- Select - .....

☐ Capitalisation of Interest .....

☐ Index-Linked .....

DCF if Money Market: ACT/360 ACT/365 .....

DCF if Capital Market: ACT/360 ACT/ACT 30/360 .....

Coupon Periodicity: - Select - .....

Amortization (bond factor): - Select - .....

Secondary market amount per transaction: Minimum ....
Multiple ....

Additional ISSU[2]: - Select - .....

Options[2]: ☐ Put 1st possible put date ....

☐ Call 1st possible call date ....

Tefra D: - Select - .....

[1] Corporate actions in T2S currencies will be managed by NBB-SSS. Non-T2S currencies can be managed optionally and require additional static data.

[2] Precautions in formula not to surpass 0,75% increase in yield (RD of 26/05/94 art.2 § 3).

This form shall be added to the prospectus and sent to NBB-SSS at least one week before the start of the inscription period.

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 21

MATCHING RULES

From phase 1 of the migration NBB-SSS will use the future T2S rules for matching instructions in its system.

The following types of instructions can be sent to NBB-SSS:

- DvP (Delivery versus Payment) instructions
- FoP (Free of Payment) instructions
- PFoD (Payment Free of Delivery) instructions
- DwP (Delivery with Payment) instructions

Matching of these instructions is done by comparing the different matching fields. T2S matching rules use 3 types of matching fields, each with their implications for the matching process.

Mandatory matching field	Both parties must fill in these fields in order to have a matched instruction.
Additional matching field	If one party fills in an additional matching field, its counterparty must fill in the same data as well, in order to have a matched instruction.
Optional matching field	➢ If one of the two counterparties fills in this field, while the other does not, instructions will match. ➢ If both counterparties fill in this field, they have to fill in the same data for the instructions to match.

NBB-SSS accepts already matched instructions if the participant has ownership or PoA on the accounts mentioned in the already matched instruction.

Power of Attorney (PoA) at account level is introduced: MT541 or MT543 with the 25D:MTCH/MACH at the end of the sequence TRADDET will be accepted and processed.

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

For instructions sent by two counterparties to match, the values of the different fields, when filled in (except for optional matching fields which can match against empty fields), must be identical or sometimes opposed to each other.

However, with respect to settlement amounts (cash), tolerance levels are set. Deviations in the instructed amounts smaller than € 25 are admitted if the settlement amounts exceed €100,000. For settlement amounts up to €100,000 a € 2 variation is acceptable. For settlement Instructions in Foreign currencies, the tolerance level per instruction shall be of equivalent amount based on the official exchange rates published by the ECB."

If more than one potentially matching Settlement Instruction is found by the system, it chooses the one with the smallest difference in settlement amount. If multiple potentially matching Settlement Instructions have the same settlement amount, the system chooses the instruction with the closest entry time.

In case the system matches settlement instructions with a difference in the settlement amount, the settlement amount of the delivering party of the securities is used for settlement.

Herewith an overview of the different matching fields and to which matching field type they belong.

Mandatory matching field	Additional matching field	Optional matching field
• Payment type • Securities movement type • ISIN code • Trade date • Settlement quantity • Intended settlement date • Delivering party BIC • Receiving party BIC • CSD of the counterparty • Currency (1) • Settlement amount (1) • Credit/Debit (1)	• OPT-Out ISO transaction condition indicator (3) • Cum/Ex indicator (4)	• Common trade reference • Client delivering CSD participant (BIC of Proprietary Format) (5) • Client receiving CSD participant (BIC of Proprietary Format) (5) • Securities account of the delivering party • Securities account of the receiving party

(1) Currency, settlement amount and credit/debit indicator are mandatory matching fields for DVP instructions. Euro FOP instructions are understood to not use these fields at all. If they do, they are considered to match as well.

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Foreign currency DVP instructions will be sent to T2S as FOP instructions containing the foreign currency, settlement amount and credit/debit indicator. In this case these fields are considered mandatory matching fields. These fields will refer to the amounts in GBP/USD that NBB-SSS will receive from the buyer and credit the seller through cash accounts outside T2S.

(3) If 'Y', no market claims generation or transformation, otherwise ' ': 'N' does not exist in the ISO standard.

(4) It is expected that, since NBB-SSS only settles in nominal, this field will always mention 'CUM', resulting in the non-consideration of this field in NBB-SSS's processes (i.e. withholding taxes). The NBB-SSS recommends avoiding the usage of this field.

(5) NBB-SSS recommends usage of BIC to identify the client in the light of cross-border settlement in T2S as of phase 2.

Since NBB-SSS will no longer match on the instruction type, the participants are advised to provide a common trade reference or one of the other optional matching fields in their instructions, in order to avoid cross-matching issues.

After arrival of the first instruction, the NBB-SSS provides the MITI (Market Infrastructure Transaction Identification). On arrival of the second, matching, instruction, the second instruction receives the same MITI. The MITI does not change when the transaction is recycled. The MITI will contain the T2S reference of the instruction.

The matching reference provided by T2S will only be available for the participant working with MX messages.

Settlement Finality 2 ("moment of irrevocability") is reached when the matched status is given by T2S to the instruction.

Buyer Protection Instruction (BPI)	
BPI Reference:	*This is the buyers reference which easily identifies their election.*
Date of issuance (dd-mm-yy):	*This is the date in which the BPI is created and sent to the counterparty.*
Security Name:	*Name of the security in which the Corporate Action is taken place and the trade/loan has been executed on.*
ISIN:	*The International Securities Identification Number of the above security*
Market Deadline Date and Time:	*DD-MM-YY: HH-MI (time zone GMT/CET etc)*
CA Event Type (CAEV):	*ISO code*
Official Corporate Action Reference (COAF):	*This should be the COAF which is announced by the Issuer. Should a COAF not exist then this filed must be left blank.*
CSD	*This is the name of the CSD which the trade will be settling in*

Corporate Action Details:		**Default Indicator**	
Option 1:	*Ratio's should be on a per share ration to allow for counterparties to potentially use Excel to format their calculations.*		
Option 2:	*ISO definition*		
Option 3:	*ISO definition*		

Pending Transaction Details:

RvP / FoP	Transaction Ref	Quantity	Cash Amount	Trade Date	Intended Settlement Date
		UNIT / FAMT Delete where appropriate		dd-mm-yy	dd-mm-yy

Election Details:					**Expected Outturn:**		
Entitled Nominal/Quantity	**Transaction Ref (as per the details above)**	**Election Quantity**	**Option No (as per the details above)**	**Total Unelected Amount**	**ISIN**	**Cash**	**Currency**
				0			
				0			
				0			
				0			
				0			

As per standards 20 to 22 of the Market Standards for Buyer Protection being part of the Market Standards for Corporate Actions Processing, version 2012,:
1) We shall **allow settlement** until end of settlement on the date of the Buyer Protection Deadline.
2) Should the trade(s) **settle in full** on or before the Buyer Protection Deadline, this instruction **is void**.
3) Should the trade(s) remain unsettled on the Buyer Protection Deadline, we shall cancel and reinstruct the trade(s) according to the option chosen above. The trade(s) shall not be allowed to settle after the Buyer

Should partial settlement occur after the Buyer Protection has been issued the following will apply:
4) If the above election is a split election on the same trade ref this Buyer Protection is **void** and the buyer should re-instruct with a new election(s).
5) If the above election is **not** a split election then the election will **remain** on the pending quantity.

Please confirm receipt and agreement of the above protection by return mail.

Name:	Telephone Number:	Email Address:
Mr Smith	++ 44 207 *******	Jsmith@CAJWG.eu

Buyer Protection Instruction (BPI)

BPI Reference:	BS00123
Date of issuance (dd-mm-yy):	20/11/2013
Security Name:	Banco Santander
ISIN:	ES0113900J37 Ords / ES06139009G0 Rights
Market Deadline Date and Time:	22/11/2013 15:00 CET
CA Event Type (CAEV):	EXRI
Official Corporate Action Reference (CORP):	*Banco6987858*
CSD	Iberclear

Corporate Action Details:			Default Indicator
Option 1:	NOAC		Y
Option 2:	CASH	€ 0.53	N
Option 3:	SECU	0.024390244	N

Pending Transaction Details:

RvP / FoP	Transaction Ref	Quantity	Cash Amount	Trade Date	Intended Settlement Date
RvP	123456	10,000	EUR 15,000.00	18/11/2013	21/11/2013
RvP	987654	4,000	EUR 7,500	15/11/2013	20/11/2013

Election Details:

Expected Outturn:

Entitled Nominal/Quantity	Transaction Ref (as per the details above)	Election Quantity	Option No. (as per the details above)	Total Unelected Amount	ISIN	Quantity - Cash / Stock	Currency
10,000	123456	10,000	002	0	n/a	€ 5,300.00	EUR
4,000	987654	4,000	003	0	ES0113900J37	97	n/a

As per standards 20 to 22 of the Market Standards for Buyer Protection being part of the Market Standards for Corporate Actions Processing, version 2012,:

1) We shall **allow settlement** until end of settlement on the date of the Buyer Protection Deadline.
2) Should the trade(s) **settle in full** on or before the Buyer Protection Deadline, this instruction **is void**.
3) Should the trade(s) remain unsettled on the Buyer Protection Deadline, we shall cancel and reinstruct the trade(s) according to the option chosen above. The trade(s) shall not be allowed to settle after

Should partial settlement occur after the Buyer Protection has been issued the following will apply:

4) If the above election is a split election on the same trade ref this Buyer Protection is **void** and the buyer should re-instruct with a new election(s).
5) If the above election is **not** a split election then the election will **remain** on the pending quantity.

Please confirm receipt and agreement of the above protection by return mail.

Name:	Telephone Number:	Email Address:
Mr Smith	++ 44 207 *******	Jsmith@CAJWG.eu

Buyer Protection Instruction (BPI)						
BPI Reference:	BS00123					
Date of issuance (dd-mm-yy):	20/11/2013					
Security Name:	Banco Santander					
ISIN:	ES0113900J37 Ords / ES06139009G0 Rights					
Market Deadline Date and Time:	22/11/2013 15:00 CET					
CA Event Type (CAEV):	EXRI					
Official Corporate Action Reference (CORP):	*Banco6987858*					
CSD	Iberclear					

Corporate Action Details:			Default Indicator
Option 1:	NOAC		Y
Option 2:	CASH	€ 0.53	N
Option 3:	SECU	0.024390244	N

Pending Transaction Details:

RvP / FoP	Transaction Ref	Quantity	Cash Amount	Trade Date	Intended Settlement Date
RvP	123456	10,000	EUR 15,000.00	18/11/2013	21/11/2013
RvP	987654	4,000	EUR 7,500	15/11/2013	20/11/2013

Election Details:					Expected Outturn:		
Entitled Nominal/Quantity	Transaction Ref (as per the details above)	Election Quantity	Option No. (as per the details above)	Total Unelected Amount	ISIN	Quantity - Cash / Stock	Currency
10,000	123456	8,500	002	0	n/a	€ 4,505.00	EUR
		1,500	003	0	ES0113900J37	36	n/a
4,000	987654	2,580	002	0	n/a	€ 1,367.40	EUR
		1,420	003	0	ES0113900J37	34	n/a

As per standards 20 to 22 of the Market Standards for Buyer Protection being part of the Market Standards for Corporate Actions Processing, version 2012,:

1) We shall **allow settlement** until end of settlement on the date of the Buyer Protection Deadline.
2) Should the trade(s) **settle in full** on or before the Buyer Protection Deadline, this instruction **is void**.
3) Should the trade(s) remain unsettled on the Buyer Protection Deadline, we shall cancel and reinstruct the trade(s) according to the option chosen above. The trade(s) shall not be allowed to settle

Should partial settlement occur after the Buyer Protection has been issued the following will apply:

4) If the above election is a split election on the same trade ref this Buyer Protection is **void** and the buyer should re-instruct with a new election(s).
5) If the above election is **not** a split election then the election will **remain** on the pending quantity.

Please confirm receipt and agreement of the above protection by return mail.

Name:	Telephone Number:	Email Address:
Mr Smith	++ 44 207 *******	Jsmith@CAJWG.eu

NBB-SSS
Information for DCP

Information document for stakeholders
May 2015 – Version 1.0

National Bank OF BELGIUM
Eurosystem

© National Bank of Belgium

All rights reserved.
Reproduction for educational and non-commercial purposes is permitted
provided that the source is acknowledged.

Contents

1 NBB-SSS Information for DCP 3
1.1 General 3
1.2 Overview of roles and responsibilities of T2S Actors 3
1.3 Communication tools 6
2 T2S settlement day 8
2.1 Introduction to the T2S settlement day 8
2.2 T2S change of the settlement day 10
2.3 T2S queuing during weekends and T2S closing days 10
2.4 Schedule of T2S Settlement Day 10
3 Operational issues and applicable operational procedures 18
3.1 Delay start of D + 1 settlement day in case of RTGS delay 20
3.2 Processing of the CMS data feed 21
3.3 Night-time algorithms processing during RTS 22
3.4 T2S delay 23
3.5 T2S processing with limited liquidity 26
3.6 Opening T2S on weekends for settlement 27
3.7 Technical disconnection of a participant using abnormally the system 28
3.8 Blocking one or more party technical addresses to keep T2S outgoing messages on hold 29
3.9 Handling of information security events (e.g. cyber-attack) 30
3.10 Communication on opening and closing DCA accounts 31
4 Incident Management 33
5 Access Management 35
5.1 Purpose and scope of Access Management 35
5.2 Overview of customer facing ACM activities 35
5.3 Requesting access rights 35
5.3.1 DCP Requests 36
5.3.2 DCP privileges 38
6 Service Continuity Management 39
6.1 Purpose and Scope of Service Continuity Management 39
6.2 T2S Service Continuity 39
6.2.1 Major Failure 40

6.2.2 Regional Disaster 41
6.2.3 Rebuilding Process 42
6.3 Information Required by CSD / DCP of CSD in case of RAD 43
6.4 Service Continuity Testing 44

Annex 1- T2S Direct: Access Rights (T2S privileges) required by DCPs..... 46

1 NBB-SSS INFORMATION FOR DCP

1.1 GENERAL

The NBB-SSS Information for DCP is a guide for T2S operational procedures which may involve the Directly Connected Parties (DCPs).

Such general communication with DCPs is under the control of CSDs, hence DCPs will receive fairly similar information from those CSD in which they maintain securities accounts.

1.2 OVERVIEW OF ROLES AND RESPONSIBILITIES OF T2S ACTORS

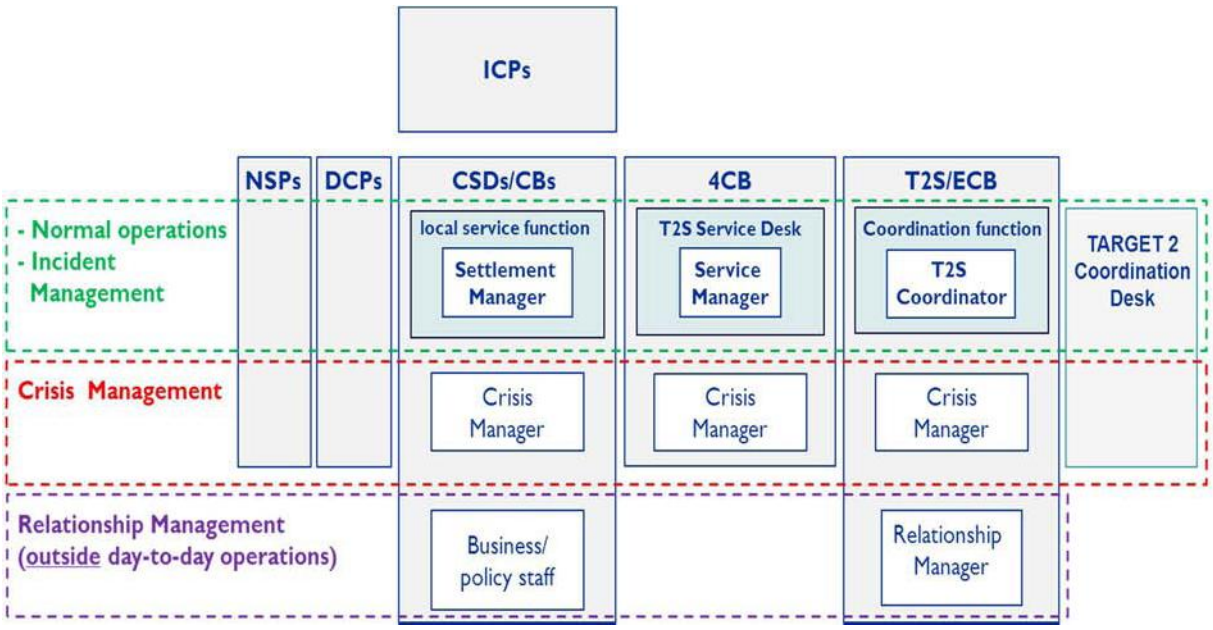


Figure 1 - T2S Actors and other relevant players

As each CSD and Central Bank remains fully responsible for the business relations with its respective participants, T2S has been designed in a way that allows the CSDs/ Central Banks to meet t he administrative and regulatory requirements in terms of service monitoring and service control.

The CSD Settlement Managers are responsible for:

- all contacts with, and provision of business support to, their participants, including the management of the relevant Static Data;
- daily operational management;
- monitoring of the settlement activities of their participants (e.g. settlement flows) and the technical and operational monitoring of any local technical components;
- handling of local contingency arrangements and abnormal situations which are covered by this document and do not explicitly require the involvement of the Crisis Managers;
- close interaction with the T2S Coordination function and the T2S Service Desk.

The CSD Crisis Managers are called to deal with events which explicitly require their involvement or are escalated to them by the Settlement Managers. To address any unforeseen situation impacting T2S Operations, the 4CB Crisis Managers are reachable 24x7.

The T2S Service Desk at the so-called 4CB (four Central Banks which operate the T2S infrastructure on behalf of the Eurosystem) provides a single point of contact for the DCPs and the NSPs for handling all incidents, queries and requests concerning T2S operational, functional or technical issues. The role of the T2S Service Desk covers as well the authorisation of the subscription to the T2S Closed Group of Users (CGUs) of the licenced NSPs.

The T2S Service Desk is reachable over phone (different numbers for production and test services) and signed e-mail.

The signed e-mail refers to e-mails bearing digital signatures of authorised signatories for relevant functions. The e-mail used is similarly S-MIME (Secure Multipurpose Internet Mail Extensions) and /or TLS (Transport Layer Security) when communicating with other relevant T2S Actors. The digital signatures are done using certificates as issued by authorised Certificate Authorities[1]. The NBB-SSS RAMSES GUI certificates (Certification Authority Banco de España on behalf of ESCB PKI) can be used for this purpose.

All communication is conducted in English.

The standard response time (time from the start of the contact until logging in the TMS) during standard support hours is 15 minutes. Service Requests during non-standard support hours (signed e-mail only) are logged and answered during the standard support hours on the next T2S settlement day.

---

[1] See the website of the European Commission, EU Trusted Lists of Certification Service Providers: https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers

The requests should be submitted to the T2S Service Desk by users authorised by the T2S Actors (excluding ICPs). Authorised users are entitled to contact the Service Desk. In case of doubt, the local help desk or the Settlement Manager of the relevant T2S Actor (excluding ICPs) can be contacted in order to verify the identity of the requestor or to check if the request is authorised.

Contact details T2S Service Desk for PRODUCTION environment:

T2S@target-ssp.eu

Phone numbers: +4969968640266 or +390620663266

Contact details T2S Service Desk for TEST environments

t2s-test@bancaditalia.it and t2s-test@bundesbank.de : use both in every e-mail !

Phone numbers: +49 69 968 640 222 or +390620663222

Players	Role	Availability	Type of support
4CB	T2S Service Desk T2S Service Manager	6:30 - 19:30 CET	On-site
ECB	T2S Coordination Function: T2S Coordinator	6:30 - 19:30 CET	On-site

Table 1 - Support and availability of T2S Service Desk

A DCP is a T2S User which is authorised by its CSD to access T2S directly for using T2S Services, i.e. without the need for the CSD to act as a technical interface. A DCP:

- subscribes the T2S Closed User Group (CGU) of one of the NSPs (SWIFT or SIA/Colt);
- communicates with T2S Platform via the Application-to-Application (A2A) and/or User-to-Application (A2A).

A DCP can participate in the T2S day-to-day operations as follows:

- All DCPs can contact the T2S Service Desk related to technical enquiries concerning their connection to T2S.

- A DCP can inform the T2S Service Desk directly if it faces incidents related to technical connectivity, which prevents the proper usage of T2S; the T2S Service Desk must then inform the relevant CSD without undue delay.
- In order to ensure smooth communication with DCPs, the CSDs shall provide the T2S Coordination function with contact details of their DCPs.
- DCPs are not directly involved in Incident and Crisis Management activities; it is for the respective CSD to ensure that the DCP is appropriately informed about on-going incidents and Crisis. They will be invited in Crisis Manager's conference call if related to the cause of the crisis.

1.3 COMMUNICATION TOOLS

The T2S Information System (T2S-info) provides up-to-date information on the operational status of the T2S Services to news agencies (such as Reuters, Bloomberg) and the T2S website. T2S-info informs about normal operations (start of day/end of day) and abnormal situations.

The T2S GUI allows the T2S Service Desk to send broadcast messages to the CSDs which in turn can also send broadcast messages to their DCPs.

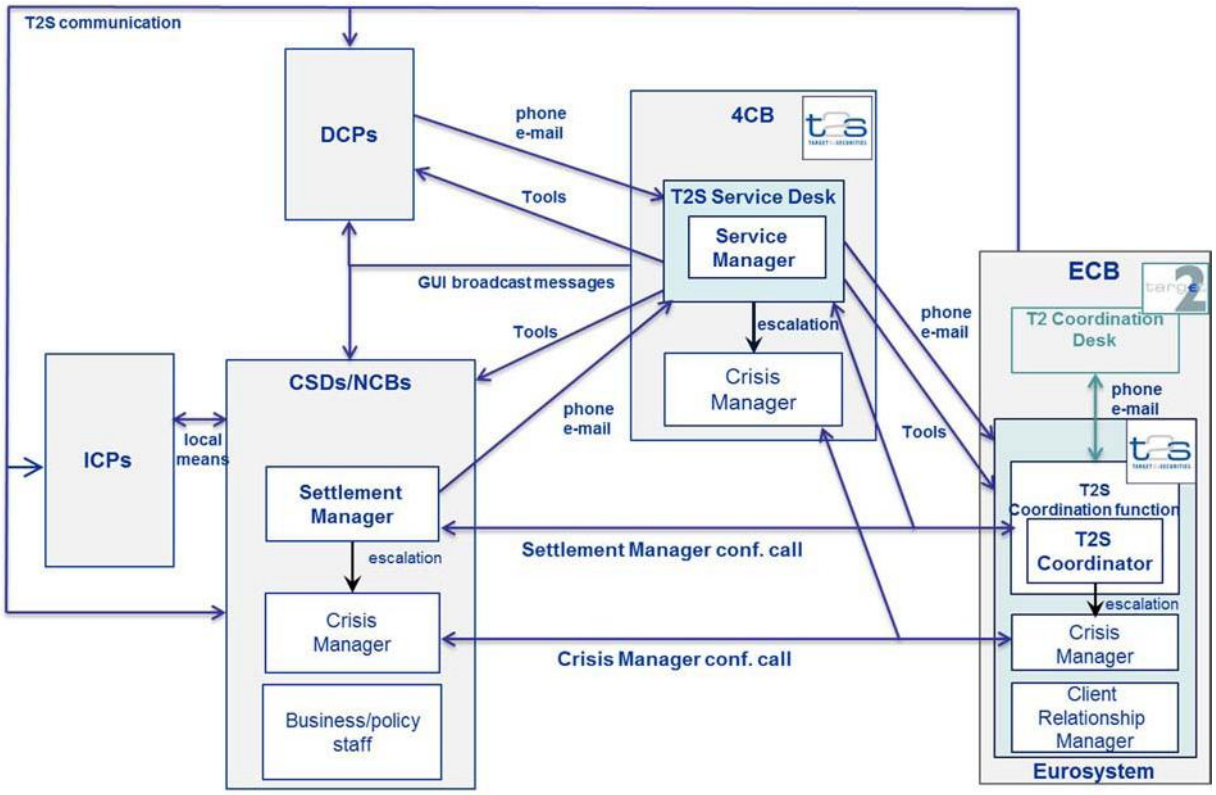


Figure 2 - Communication Tools Overview

The T2S Operational Directory is maintained on a secure part of the T2S website. It provides the current contact information for T2S Actors (excluding ICPs) as well as the T2S Service Desk and the T2S Coordination function. Changes are communicated by respective T2S Actors (excluding ICPs) to T2S Coordination function, who keeps it updated. Additionally, the T2S Coordination function revalidates the contact information every three months. The T2S Coordination function is in charge of maintaining the T2S Operational Directory and provides all T2S Actors (excluding ICPs) with passwords for accessing the secure Web pages.

The T2S Trouble Management System (TMS) supports most of the activities of the T2S Service Desk related to the Service Management processes. The T2S Service Desk uses the TMS to track all interactions (such as incidents, service requests) with CSD and Central Bank Settlement Managers as well as with the NSPs and DCPs.

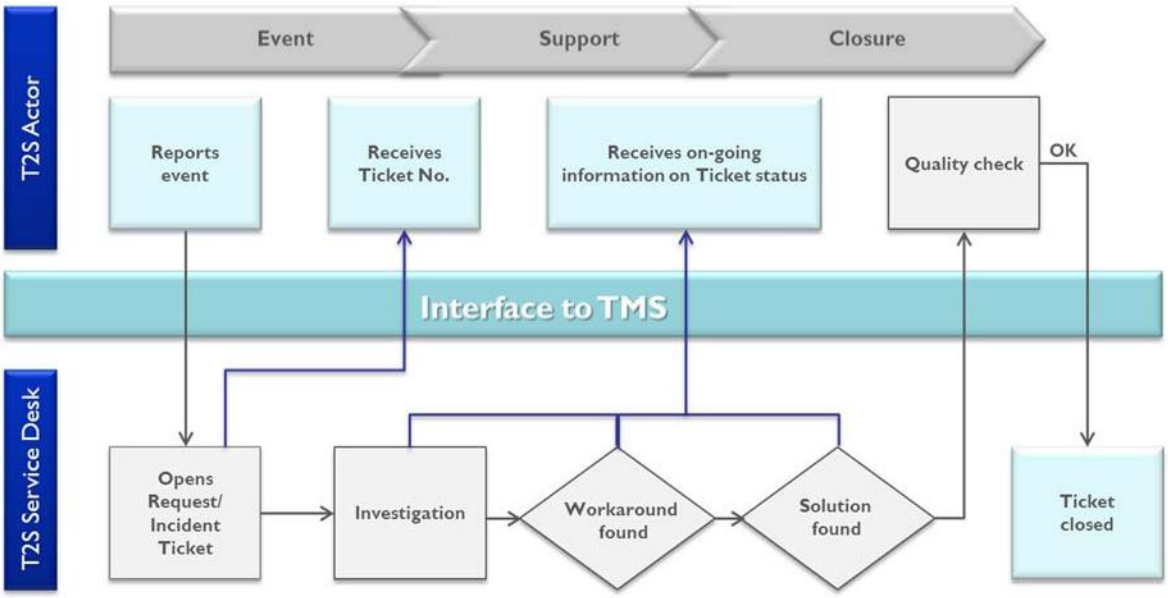


Figure 3 - TMS Overview

The CSD and Central Bank Settlement Managers as well as DCPs have read access to the TMS through its Graphical User Interface (GUI).

2 T2S SETTLEMENT DAY

2.1 INTRODUCTION TO THE T2S SETTLEMENT DAY

T2S facilitates securities settlement in CeBM, according to the calendar of the relevant RTGS system. The T2S Operator maintains a T2S operating day calendar by currency, which includes the opening days and closing days for all T2S settlement currencies (see *UDFS V2.0 Section 1.4.1 - T2S Calendar*).

A detailed description of the T2S settlement day is available at *T2S UDFS V2.0, Section 1.4.4*. The tasks related to the T2S settlement day management, business and operations monitoring are described in the *T2S UDFS V2.0, Section 1.5.3 and 1.5.4*.

The T2S settlement day, i.e. Start of Day, Night Time Settlement, Maintenance Window, Real Time Settlement, and End of Day specific events from an operational point of view and generic procedures for T2S operations, are illustrated in this chapter.

The overview of the T2S settlement day is described in Figure 4, highlighting the key T2S activities and the key interactions between external systems (e.g. TARGET2) and T2S in different phases of the T2S settlement day. Key interactions included in the figure are those interactions that have a specific deadline. In case such a deadline is not met, it would affect the normal T2S settlement day, as described in the subsequent section.

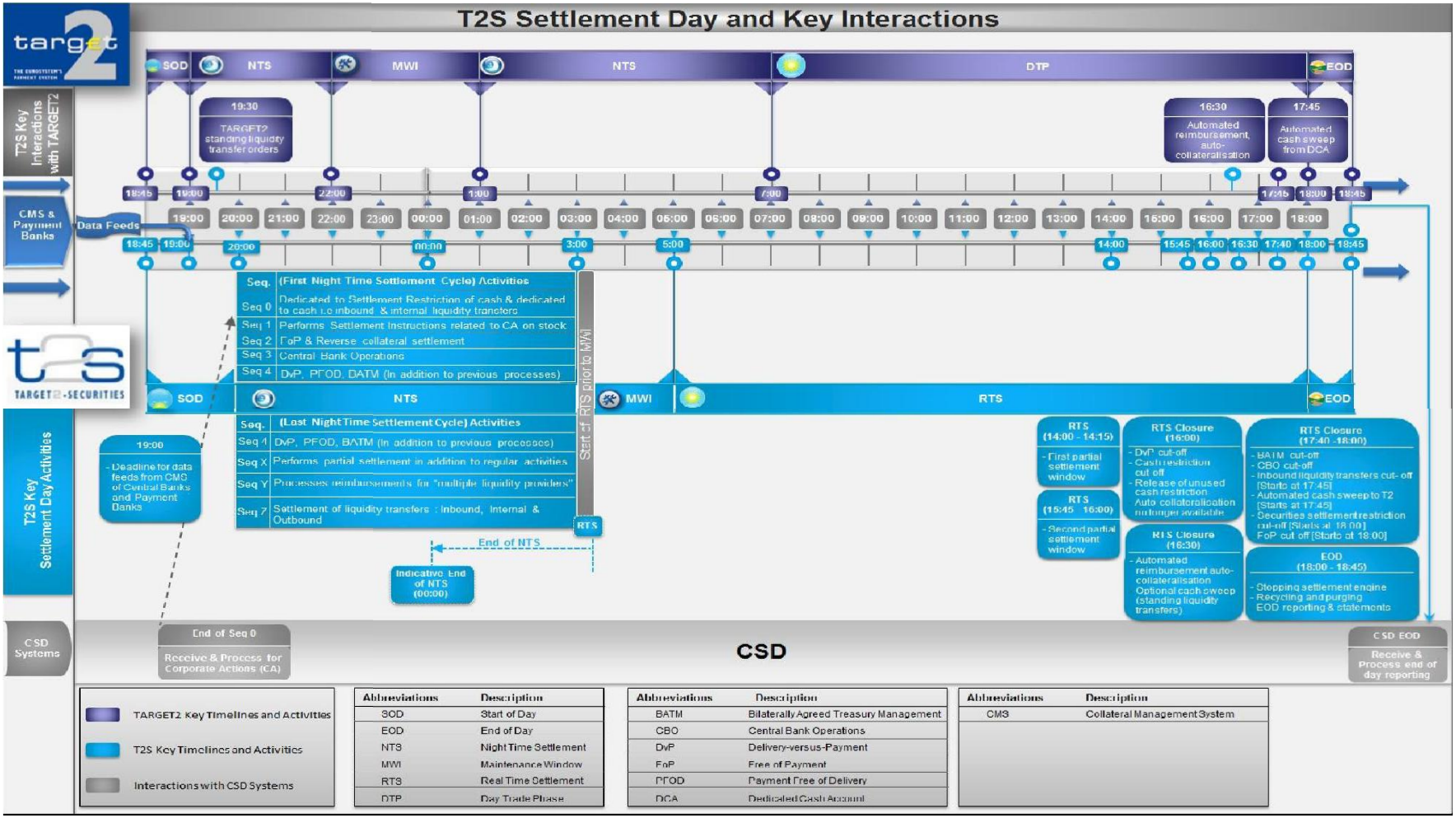


Figure 4 - T2S Settlement Day

2.2 T2S CHANGE OF THE SETTLEMENT DAY

The first action of the start-of-day process is the move to the next T2S settlement day according to the T2S Calendar, which occurs at **18.45 CET**.

On Fridays at **18:45 CET**, T2S moves the settlement date to the next T2S settlement day, i.e. Monday, and processing continues until Saturday at 03.00 CET. On Monday at 05:00 CET, T2S starts performing the schedule with the preparation of the real-time settlement as the continuation of the settlement day.

On the day before a T2S closing day, T2S moves the settlement date to the next settlement day (the first T2S settlement day after the T2S closing day, e.g. 2 January) and processing continues until 03.00 CET on the day of the T2S closing day. On the day after the T2S closing day at 05:00 CET, T2S starts the schedule with the preparation of the real-time settlement as the continuation of the settlement day.

2.3 T2S QUEUING DURING WEEKENDS AND T2S CLOSING DAYS

During weekends and T2S closing days, T2S interfaces and processes are unavailable due to the regularly executed technical maintenance activities, unless other planned activities take place (e.g. release deployments, business continuity tests). Therefore, T2S does not queue the messages. However, the Application-to-Application (A2A) communication will be queued by the NSPs until T2S is available again *(see Section Maintenance Window (03:00 CET – 05:00 CET)*.

2.4 SCHEDULE OF T2S SETTLEMENT DAY

The T2S settlement day is made up of a series of scheduled events. These events define the various processing steps and cut-offs, which are to be carried out during the system's operations. The default schedule for each settlement day is loaded automatically by the system upon each settlement date change on the basis of static data. The events which have to imperatively be triggered in the predefined sequence are linked to each other with a predecessor- successor relationship (see *T2S UDFS V2.0, Section 1.4.3*).

In case of an incident lasting through the settlement day occurs, it is possible to adjust the schedule and reschedule events following the Incident Management and/or Crisis Management procedures. The T2S Operator will implement changes manually on the current T2S settlement day schedule at runtime in exceptional situations.

The schedule of a T2S settlement day constitutes the major periods as listed below:

- start of day (SOD);
- night-time settlement (NTS);
- maintenance window (MWI);
- real-time settlement (RTS);
- end of day (EOD).

The following sections describe the procedural tasks during a normal operational day.

2.4.1.1 Start of day (18:45 CET – 20:00 CET)

The SOD process is launched at **18:45 CET.** This is confirmed via the "Status of the T2S settlement day Notification" message, an entry in the T2S GUI "Daily Schedule" screen and "T2S Diary Response" query response message.

The SOD period includes:

- changing of settlement date in T2S;
- preparing the NTS:
  - Revalidating settlement and maintenance instructions that failed to settle or to be executed as of their Intended Settlement Date (ISD);
  - Accepting data feeds from Collateral Management Systems (CMS) and Payment/ Settlement Banks received continuously throughout the day. However, 19:00 CET is the final deadline to accept data feeds (e.g. auto-collateralisation, client-collateralisation) effective for the current settlement date;
- Valuation of securities positions;
- Valuation of collateral eligible Settlement Instructions.

During this period settlement does not take place. This period is used by the T2S Actors (excluding ICPs) to prepare for NTS (e.g. corporate actions (CA) processing). Settlement instructions for processing in the NTS can be submitted during this period.

2.4.1.2 Night-time settlement (20:00 CET– 03:00 CET)

The NTS starts after the successful completion of the SOD period and is followed by the MWI and the RTS periods. This is confirmed via the "Status of the T2S settlement day Notification" message, an entry in the T2S GUI "Daily Schedule" screen and the "T2S Diary Response" query response message (messages are available to the T2S Actors (excluding ICPs) upon subscription).

In case NTS completes before **03:00 CET** RTS begins immediately after the NTS completion, before the scheduled start of the MWI at **03:00 CET.** The target completion time of NTS is **00:00 CET**. The target completion time of the first NTS cycle is at **22:20 CET**.

During the NTS, T2S processes the settlement instructions, settlement restrictions and liquidity transfers in two settlement cycles, according to an automatic predefined order called "sequence". A Settlement Cycle consists of more than one sequence (for settlement of different types of settlement instructions, settlement restrictions and liquidity transfers).

The NTS sequences in T2S include processing of

- new settlement instructions, settlement restrictions and liquidity transfers received before the start of the sequence which are eligible for settlement during this sequence (e.g. for the sequence 0 those received in T2S before **20:00**);
- pending settlement instructions not settled during previous sequences.

T2S validates and accepts the static data maintenance instructions and other maintenance instructions (e.g. cancellation instructions, amendment instructions or hold/release instructions during the NTS period on a continuous basis. However, these updates are only processed in between the different sequences, unless these updates do not impact the settlement (see *UDFS V2.0, Section 1.6.3).* T2S sends the information on the status of the static data maintenance instructions and maintenance instructions immediately after the end of their processing (i.e. acceptance, execution).

For all static data updates, i.e. immediate updates and updates with future date, T2S also performs a validation of all settlement instructions and settlement restrictions to ensure that they are valid for the intended static data update.

In case a maintenance instruction was created for a settlement instruction or a settlement restriction, but the underlying settlement instruction or settlement restriction has been cancelled during revalidation, the maintenance instruction execution will be denied, but the maintenance instruction will not be cancelled.

Queries related to securities positions and cash account balances, received and validated during a settlement sequence, are processed by the T2S with a query response back to the sending party after completion of the sequence. All other queries are processed immediately.

Once the processing of an NTS sequence is completed, T2S sends the messages that were queued during the execution of the settlement sequence, i.e. settlement advice, settlement confirmation, posting notification, etc.

At the end of each NTS sequence, T2S generates full or delta reports as per report configuration setup of the respective CSD, Central Bank or DCP.

During the NTS, T2S performs the processes in two different settlement cycles, as document in the following table.

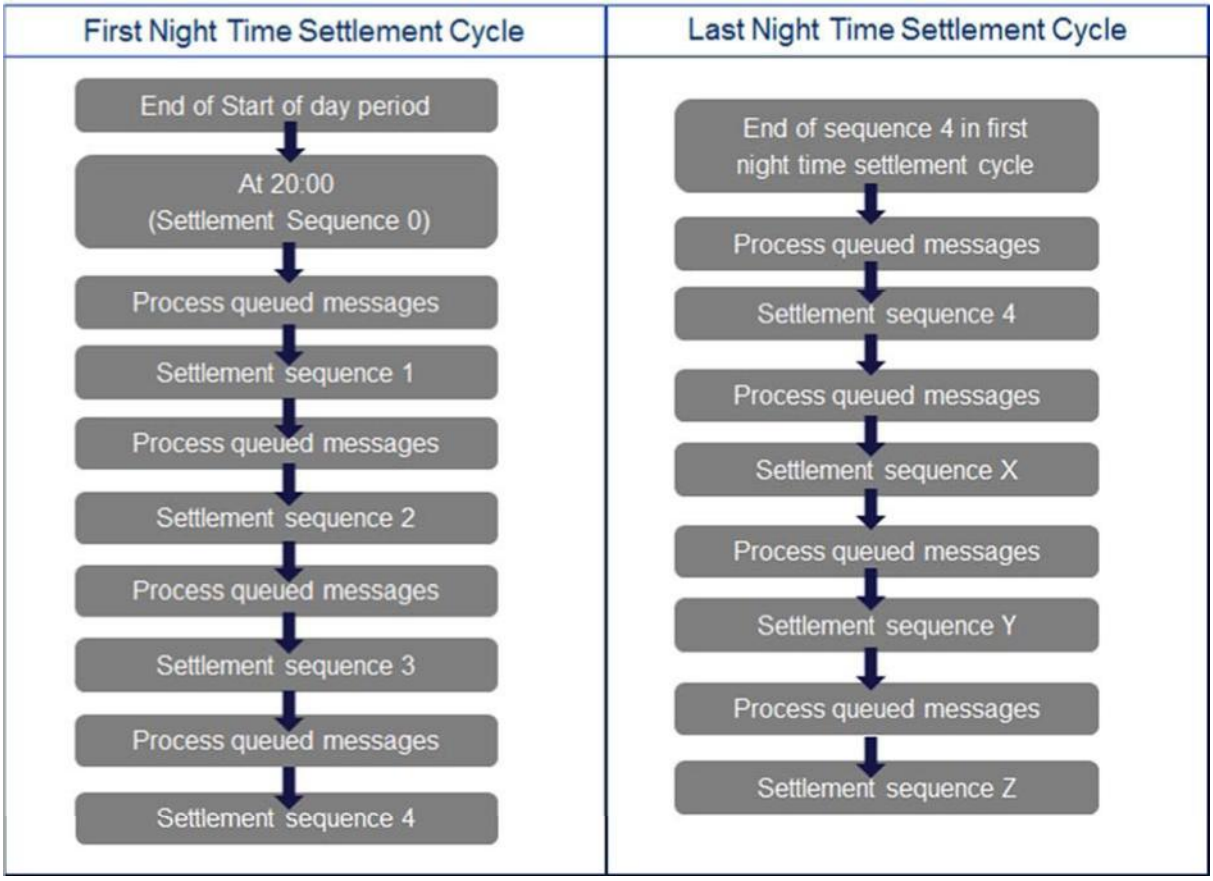


Figure 5 - T2S settlement cycles

Generally, NTS sequences perform the same activities. However, certain sequences in the NTS are dedicated to specific activities and processing specific set of messages. These sequences are described below:

- Sequence 0 is dedicated to cash i.e. inbound liquidity transfers, internal liquidity transfers and other cash settlement restrictions. T2S reattempts the inbound liquidity transfers and cash settlement restrictions in subsequent sequences in case it is unable to process in sequence 0.
- Sequence 1 performs settlement of instructions related to CA on stock new liquidity transfers, new cash Settlement Restrictions and all cash Settlement Restrictions not settled in the previous sequence.
- Sequence X performs partial settlement in addition to regular activities. T2S applies partial settlement to all fails due to lack of securities or cash which are eligible for submission to partial settlement processing.

- Sequence Y processes reimbursements for "multiple liquidity providers". This reimbursement procedure involves the execution of a series of outbound liquidity transfers from a DCA (of a payment/ settlement bank in T2S) to RTGS accounts in accordance to a pre-set sequence of reimbursement.

The end of the NTS is confirmed via an entry in the T2S GUI "Daily Schedule" screen and the "T2S Diary Response" query response messages, which are available to CSDs, Central Banks and DCPs upon request.

2.4.1.3 Maintenance Window (03:00 CET – 05:00 CET)

The MWI is scheduled from 03:00 CET until 05:00 CET after the completion of the NTS period. The start of maintenance window is reported via "Status of the T2S settlement day Notification" (messages are available to T2S Actors (excluding ICPs) upon subscription).

During the maintenance window and with the exception of the T2S interface application process, all T2S processes are unavailable. The interface application process starts the queuing of all requests received in A2A mode. This is followed by a technical validation (i.e. format validation) of the incoming A2A store and forward messages (or files).The U2A communication as well as A2A real time messages are not queued during the MWI.

2.4.1.4 Real-time settlement (05:00 CET – 18:00 CET)

The RTS starts after the end of the NTS[2] and is followed by the EOD.

The RTS period includes:

I. Preparing the real-time settlement;
II. Performing the real time settlement with the two partial settlement windows to optimise maximum value and volumes of settlement transactions;
III. Closing the real time settlement with different cut-offs for settlement instructions, settlement restrictions and liquidity transfers categories.

I. Preparing real-time settlement

The start of the RTS is confirmed via the "Status of the T2S settlement day Notification" message, an entry in the T2S GUI "Daily Schedule" screen and "T2S Diary Response" query response messages, which are available to the T2S Actors (excluding ICPs) upon request.

T2S identifies and processes static data maintenance instructions received in the A2A.

2 Following the indicative timing for the completion of the NTS the start of RTS could be already at 00:00 CET.

T2S identifies new settlement instructions, maintenance instructions and liquidity transfers available for the current settlement day. T2S identifies all settlement and maintenance instructions, not settled and/or executed during the NTS period, and recycle them for RTS. The recycling takes place after the revalidation of the s ettlement instructions and se ttlement restrictions, subject to a static data change.

II. Performing the real-time settlement

RTS attempts to pro cess all new settlement instructions, maintenance instructions and newly received liquidity transfers intraday in T2S and all previous unsettled settlement instructions after the arrival of new securities and/or cash resources.

T2S also performs the execution of static data maintenance instructions. Additionally, T2S revalidates all settlement instructions and all se ttlement restrictions, subject to static data updates. Moreover, T2S generates reports triggered by business or time events.

The RTS also includes the following two partial settlement windows:

- First partial settlement window **(14:00 CET– 14:15 CET);**
- Second partial settlement window **(15:45 CET- 16:00 CET), 15 minutes before the beginning of the DVP cut-off time.**
  - During the pa rtial settlement windows, T2S takes care of: Par tial settlement of new settlement instructions arriving into T2S in this period, eligible for partial settlement.
  - Settlement of previously unprocessed or partially processed settlement instructions, eligible for partial settlement.

All processes available during the real time settlement are also available during both the partial settlement windows.

III. Closing real-time settlement

The process starts after the completion of the second partial settlement window. It does not start before 16:00 CET. The following processes are executed sequentially:

TIME (CET)	T2S settlement day events / processes
16:00	DVP cut-off
16:00	Cash restriction cut-off
	Release of unused cash restriction
16:30	Automatic reimbursement
	Recommended: Optional cash sweep (standing liquidity transfers)
17:40	Bilaterally Agreed Treasury Management (BATM) cut-off
17:40	Central Bank Operations (CBO) cut-off
17:45	Inbound liquidity transfers cut-off
	Automated cash sweep
18:00	Securities restriction cut-off
18:00	FOP cut-off

Table 2 - Sequential settlement day event

The cut-offs are confirmed via an entry in the T2S GUI "Daily Schedule" screen and the "T2S Diary Response" query response messages, which can be available to the T2S Actors (excluding ICPs) upon request.

2.4.1.5 End of day (18:00 CET – 18:45 CET)

T2S settlement day closes at **18:00 CET**. The EOD processing starts after the successful completion of the RTS period, when settlement no longer takes place. It is followed by the SOD period of the next settlement day.

Following the cut off and until **18:45 CET**, the following events take place:

- Stopping settlement engine;
- Recycling and purging;
- End of day reporting and sending statements.

T2S generates all the EOD reports as per the agreed prioritisation and sends them to the subscribing T2S Actors (excluding ICPs). The agreed prioritisation is:

- Statement of holdings
- Settled settlement instructions

- Pending settlement instructions
- Statement of Account
- Statement of Settlement Allegement
- Statement of settled intra-balance movements
- Statement of pending intra-balance movements

The execution of the EOD process is confirmed via the "Status of the T2S settlement day Notification" message, an entry in the T2S GUI "Daily Schedule" screen and "T2S Diary Response" query response messages, which are available to the T2S Actors (excluding ICPs) upon request.

3 OPERATIONAL ISSUES AND APPLICABLE OPERATIONAL PROCEDURES

This section maps operational issues and related applicable operational procedures, and subsequently describes the operational procedures in detail. The application of such operational procedures is triggered via Incident and /or Crisis Management.

T2S settlement day consists of established processes and activities. Table 3 provides a non-exhaustive overview of possible operational issues during the different periods of the T2S settlement day with the mapping to the applicable operational procedure.

#	Phase	Key Activities	Relevant Operational Issues	Applicable Operational Procedures
1	SOD 18:45CET – 20:00 CET	Change of settlement date in T2S	RTGS not able to start new settlement day	Delay start of D + 1 settlement day in case of RTGS delay
		Preparation for Night Time Settlement	CMS data feed unavailable in T2S by 19:00	Processing of the CMS data feed
			T2S Platform failure does not allow SOD	**Error! Reference source not found.**
			CMS unable to update auto-collateralisation limit	**Error! Reference source not found.**
			T2S revalidation of instructions against Static Data updates leads to unexpected results	**Error! Reference source not found.**
			One or more T2S Actors' impossibility to access T2S	**Error! Reference source not found.**
2	NTS 20:00 CET– 03:00 CET	First night time cycle with reporting and processing of Static Data maintenance instructions at the end of each sequence	T2S has a delay to start the Night Time Settlement	**Error! Reference source not found.**
			T2S has not received the liquidity transfers	T2S processing with limited liquidity
			CSD/ Central Bank request delay (later start of NTS)	**Error! Reference source not found.**
		Last night time cycle with reporting and processing of Static Data maintenance instructions at the end of each sequence, including partial settlement	One or more T2S Actors' impossibility to access T2S	**Error! Reference source not found.**

#	Phase	Key Activities	Relevant Operational Issues	Applicable Operational Procedures
3	MWI 03:00 CET – 05:00 CET	MWI	System maintenance delay	**Error! Reference source not found.**
4	RTS 05:00 CET – 18:00 CET	RTS	RTGS failure	T2S processing with limited liquidity
			General network failure	**Error! Reference source not found.**
			One or more T2S Actors' impossibility to access T2S	**Error! Reference source not found.**
			T2S is down close to (e.g. half an hour or 15 minutes before) the start of the cut-offs	**Error! Reference source not found.**
			Reception of big volumes during real time (special sub-case when the volumes arrive just before the related cut-off)	Night-time algorithms processing during RTS
		Real Time Settlement closure	Delay in DVP cut-off	**Error! Reference source not found.**
			Delay in automatic reimbursement (rebalancing and/ or relocation)	**Error! Reference source not found.**
			Delay in other cut-offs	**Error! Reference source not found.**
			Delay in automated cash sweep	**Error! Reference source not found.**
			Request for T2S delayed closing	**Error! Reference source not found.**
		Stop settlement engine	T2S failure in EOD procedures	**Error! Reference source not found.**
		Recycling and purging		
5	EOD 18:00 CET – 18:45 CET	End of day reporting and statements	CSD identifies an issue while reconciling the statement or processing its CA	**Error! Reference source not found.**
			RTGS (e.g. TARGET2 for the euro) delayed closure of their settlement day (D)	Delay start of D + 1 settlement day in case of RTGS delay
			One or more T2S Actors' impossibility to access T2S	**Error! Reference source not found.**

Table 3 - Operational Issues and Procedures

3.1 DELAY START OF D + 1 SETTLEMENT DAY IN CASE OF RTGS DELAY

Issue Description

The RTGS system (e.g. TARGET2) either (i) has not yet closed its previous business day due to a delay or due to some unexpected incapability[3] or (ii) is not capable of starting the new business day.

Issue Resolution

If the RTGS Operator (TARGET2 Coordinator) realises that it is not possible to close the RTGS system in time or the RTGS system is not able to change to the next business day, then the RTGS Operator will immediately inform the T2S Coordinator. The T2S Coordinator initiates the T2S Incident Management process.

T2S settles against cash on DCAs that receive funds from RTGS accounts. At the end of the day, liquidity is reimbursed to these RTGS accounts. Moreover, T2S is supporting auto-collateralisation features in a fully harmonised way, allowing settlements to take place without injecting additional cash.[4]

In case of a RTGS delay, T2S Operator following Incident/Crisis Management can either (i) delay the start of settlement of the given currency in T2S for the next T2S settlement day, (ii) delay the start of T2S, or (iii) start the normal T2S processing, including for the currency of delayed RTGS system

The T2S decision depends on different aspects such as:

- reason (technical or operational) and status (is the current business day closed or not) for the RTGS delay;
- expected duration of the RTGS delay;
- expected liquidity situation;
- impact of prolonged T2S delay or T2S start on financial stability and financial markets.

In case the RTGS has not yet closed the current business day, the preferred solution is (i) to delay the start of settlement for the delayed currency or ii) to delay the start of T2S for the next T2S

---

3 The relevant TARGET2 procedures are described in the Information Guide for TARGET2 users.

4 It should be noted that the collateralisation techniques and the set-up for auto-collateralisation is not uniform among the central banks.

settlement day. To prevent the currency from settling on the DCAs for the next T2S settlement day a specific restriction on the Party Central Bank will be set.[5]

Alternatively, specifically when the RTGS has closed the current business day, it will be possible to start settlement for the next T2S settlement day in T2S without liquidity and rely on auto-collateralisation.

3.2 PROCESSING OF THE CMS DATA FEED

Issue description

The data feed for the list of eligible collateral and collateral valuation prices from the Collateral Management Systems (CMSs) is not available at 19:00 CET.

Central Banks that offer auto-collateralisation and Payment Banks that offer client-collateralisation in T2S are responsible for the setup and maintenance of the auto-collateralisation feature in T2S, including the configuration of static data. This information (data feed) will be provided directly via the respective CMS.

The CMS data feed related to the list of eligible securities for auto-collateralisation is communicated by the CMS to T2S when changes occur. With regards to the valuations of the eligible securities, the valuation is expected to be provided to T2S on a daily basis. CMS data feeds (complete set of securities valuation coefficient, delta of eligible assets, and eligible links) can be provided throughout the day; however, the data for the respective settlement day is only activated at 19:00, during the Start of Day processes.

Once the preparation of the Night-Time Settlement starts during the Start of Day process, T2S performs a check to confirm that CMS data feeds, effective for the current settlement day, have been processed in T2S. A check is also performed to confirm that for each eligible security for auto-collateralisation a valuation has been provided to T2S.

The unavailability of the data could be because:

- CMS data feeds are not yet received by T2S;
- Data feeds supplied by CMSs are not valid (i.e. cannot be processed by T2S);
- CMSs supplied the data feed before 19:00 but they are blocked at the T2S Interface.

[5] The restriction applies to all the currencies associated to the Central Bank.

Issue resolution

In case of unavailability in T2S of the necessary data feeds from one or several CMSs, as a general procedure, the settlement day processing is blocked and a predefined alert is raised to the T2S Service Desk. The T2S Service Desk manually resumes the T2S settlement day allowing the system to use the previous available data for the missing valuation of eligible securities[6] unless the NCB (its own or on behalf of their Payment Bank) triggers Incident Management process.

In case the issue is on the side of T2S and there is a risk that the prices are not processed in time, the T2S Service Desk will contact the involved Central Bank(s) to ask for an authorisation to proceed with the operational day.

If there is a need to wait for the missing data feeds (e.g. because certain assets need to be deleted or a workaround is needed), the T2S delay procedure will be activated.

3.3 NIGHT-TIME ALGORITHMS PROCESSING DURING RTS

Issue description

There is abnormally low successful settlement rate during NTS.

Issue resolution

When the number of transactions might overload the RTS Algorithms' capability to process all the transactions a technical analysis is performed and the T2S Service Manager may propose to run the OBM (Optimisation Batch Manager). The OBM is a special algorithm to manage unexpected high volumes during RTS to increase the number and value of transactions settled in T2S.

- The T2S Service Manager will initiate the Incident and Crisis Management process. A Settlement Managers' conference call will be initiated to inform the Settlement Managers[7] about the possibility to run an OBM and to agree on the timing.
- A broadcast via T2S GUI will be sent to all T2S Actors (excluding ICPs) in order to inform about the changed settlement pattern and to ensure provisioning of sufficient resources. The T2S Operator starts the OBM at the agreed time, closely monitors the situation and informs the T2S Coordinator if the situation is resolved.
- After the volumes are normalised, according to the standard Incident Management process, the T2S Service Manager will inform the T2S Coordinator about the situation who will initiate a Settlement Managers' conference call followed by Crisis Managers' conference call (if deemed necessary) in order to decide to de-activate the OBM and to proceed with normal processing.

---

6 Alternatively some workarounds can be applied e.g. setting zero price for unavailable data, manually revoking eligibility prior to 19:00, manually setting the auto-collateralisation limits to zero, or restricting the provision of auto-collateralisation.

7 The view of the TARGET2 Coordinator should be taken into account as the business day phase of TARGET2 and liquidity aspects may play a role in the decision-making.

- A broadcast via T2S GUI to all T2S Actors (excluding ICPs) is sent accordingly.

3.4 T2S DELAY

Issue description

During the T2S settlement day different situations may occur which require the postponement of one or more phases of the T2S settlement day or even a delay of the closure of the settlement day. This may, on the one hand happen in case T2S itself is, due to different reasons (e. g. a software bug), unable to continue with the phases of the T2S settlement day as scheduled. On the other hand, also issues outside T2S may impact the T2S Schedule.

The following non-exhaustive list of causes might lead to a delay:

- T2S failure;
- settlement and liquidity management services failure;
- static data services failure;
- information services failure;
- connectivity services failure;
- CSD failure;
- RTGS failure;
- CMS services failure;
- Other reasons.

Issue resolution

IV. Overview

The decision to delay the start of the night time settlement phase or to postpone any other phase of the T2S settlement day is always made by the Crisis Managers. A delayed closing is requested to T2S Service Desk and the T2S Coordinator is informed by the T2S Service Desk. The T2S Coordinator will initiate a Settlement Managers' conference call to inform about the request and to schedule a Crisis Managers' conference call immediately. The Crisis Managers shall decide on T2S delay at the latest 15 minutes before the cut-off time.

In case of a T2S failure that t riggers the failover to another site or region, there is no other possibility than to wait until the platform recovers and to delay the closing/ postponing the phase. Meanwhile, the Crisis Managers will be informed.

The T2S Coordinator shall inform the T2S Actors as early as possible about the possible duration of the delay/ postponement. As long as this cannot be anticipated, regular updates of the situation will be provided.

V. Timing of the decisions

Decisions on delays and/or postponement of cut-offs shall be taken as early as possible to reassure the markets that they have sufficient time to process all their business.

The first information is exchanged at the Settlement Manager level together with the collection of facts. Due to a possibly tight time frame it is of extreme importance that the conference calls (information collection and impact analysis) are done in a structured way.

VI. Collection of information

The information about the incident and when possible the impact shall be collected at the level of the Settlement Managers.

Collection of in formation during Settlement Managers' conference call should ideally (i.e. if known at this point in time, lack of known information must not delay the process here) comprise:

- short description of the event including a clear request for a delayed closing;
- expected time required (how long to delay);
- impact on CSDs/ Central Banks with values and volumes at stake;
- special days in CSDs' business (e.g. end of year, special CA processing);
- impact on TARGET2 an d other RTGS systems (incl. mentioning of special days like end of minimum reserve period, end of quarter).

Information not available at the time of the Settlement Managers' conference call, but likely to be there when the Crisis Managers have their conference call shall be clearly identified and mentioned.

The acceptance or rejection of a request for delay by the Crisis Managers is based on the following criteria:

- time of the day;
- length of the delay;
- possible systemic impacts if the delay is not accepted or if the delay is accepted.

In the event of a T2S failure, there is no alternative but to wait for the recovery of the T2S Platform and to provide the necessary time for the CSDs and Central Banks to finish their processing.

At the end of the conference call, the T2S Coordinator will summarise the conclusion of the conference call preferably with an agreed recommendation to be presented for decision to the Crisis Managers, with the following structure:

- reason for the delay;
- impact of the delay;
- proposal to accept or reject the request;
- impact in case of rejection;
- available options and impact in case of acceptance.

Immediate after the Settlement Managers' conference call, the Crisis Managers' conference call will be initiated, and the Crisis Management process applies.

VII. Minimum length of the T2S Settlement Day and minimum duration of the operational day phases

In order to help the evaluation of the impact of a delay and to speed up the decision making it is useful to identify the minimum duration of each phase and, consequently, the minimum duration of a whole settlement day. The following table illustrates for each main phase of the T2S settlement day the standard times and the minimum times needed to complete the activities from T2S and from CSD/ NCB side.

T2S settlement day phase	Standard time	Minimum duration (indicative)
Start of Day (18:45 to 20:00)	75 minutes	75 minutes
Night Time Settlement (20:00 to 3:00)	7 hours	4 hours
Maintenance Window (3:00 to 5:00)	2 hours	0
Real Time Settlement (first part 5.00 to 16.00)	11 hours	4 hours
Real Time Settlement (second part 16.00 to 18.00)	2 hours	2 hours
End of Day (18:00 – 18:45)	45 minutes	45 minutes
Total	24 hours	12 hours

Table 4 - Minimum Duration of Each Phase and Minimum Time to Complete Activities

The table is a tool in the hand of the T2S Coordinator and the CSD's/ Central Bank's Settlement Manager and Crisis Managers to quickly evaluate the impact of a delay on the operational day. For example after a recovery of the T2S Platform the information present in the table will help to identify how much time would be needed to complete the settlement day without delaying of the EOD/ SOD, or in case of prolonged outage what is the impact on the following settlement day. Tools will be available to the participants of the Settlement Managers' and Crisis Managers'

conference call to visualize the effect of the delay on the current and following T2S settlement days and on the interconnected systems.

VIII. Prolonged T2S outage

Such scenario covers the unlikely situations that, despite all the efforts (normally after several subsequent delays) T2S cannot start the new T2S settlement day without impacting the timely closure of the next T2S settlement day. As, declaring the next day as non T2S settlement day, would cause the system to reject instructions with that Intended Settlement Date, the only solution is to run one or more "special" T2S settlement days skipping the maintenance window and where possible reducing the duration of certain settlement phases to catch up with the processing and to resume the normal settlement day as soon as possible. For such decision the Crisis Management process will be followed.

3.5 T2S PROCESSING WITH LIMITED LIQUIDITY

Issue description

A situation might occur that while T2S is able to open and start the settlement day, no or only some liquidity transfers have been received. This situation can occur due to the following reasons:

- RTGS is running, but there is a failure of liquidity transfer processing in the RTGS;
- failure of communication between the RTGS system and T2S ;
- RTGS had closed the previous business day for payment processing (and T2S has opened), however, the RTGS has a failure during its subsequent phases i.e. Start of Day, Night Time Settlement, or Real Time processing.

Any of the above failures affect the Inbound Liquidity Transfers (from an RTGS account to a DCA) which are initiated in the relevant RTGS System and cannot be triggered in T2S. It concerns Immediate, Predefined and Standing Liquidity Transfer Orders equally, which execution is possible during the NTS sequences and the RTS period.

Issue resolution

If only some Liquidity Transfers are missing, the T2S Operator monitors and checks the issue with the RTGS Operator and the relevant T2S Actors (excluding ICPs).

T2S can settle without injecting additional cash due to its auto-collateralisation features. Therefore, in case of an RTGS failure, T2S can continue processing without RTGS liquidity provision or with limited liquidity available from auto-collateralisation and settle FOP transactions. The Incident Management will be launched and a Settlement Managers' conference call will be initiated on the T2S side whereas the RTGS Operator will monitor and handle the failed Liquidity Transfers, and initiate its own contingency measures.

If disruption in the RTGS System is so severe that it cannot be solved for a prolonged time and the liquidity situation is not expected to improve in the T2S system, the T2S Crisis Managers may decide to delay the actual settlement phase in T2S.

3.6 OPENING T2S ON WEEKENDS FOR SETTLEMENT

Description

In addition to the procedure to open T2S during weekends for trial purposes (i.e. business continuity related tests), in specific situations T2S could be opened during a weekend for settlement in the following cases:

- A large issuance in a direct holding country;
- Major releases deployment on the side of the CSDs and Central Banks ;
- Major T2S release deployment.

The purpose of requesting T2S to open during weekends for settling real instructions (i.e. no code words required) allows to identify and solve potential problems (in case of a release deployment) or settle potential large volumes (e.g. large issuance in a direct holding country) on Saturday instead of Monday morning.

T2S would be open for these activities and would provide all services as available on a normal settlement day, except liquidity transfers as the RTGS systems would not be available at that time. Transactions executed during the weekend activities would have a settlement date of Monday since they are executed after the Start of Day event.

The above listed activities are expected to be performed outside the Maintenance Window of the NSP, which has a different duration across weekends (as a standard from 17:00 CET on Saturday to 08:00 CET on the following Sunday). In case this is not feasible, a request should be sent to the NSPs following the rules defined in the NSP's User documentation.

Operational procedure

Two different options are available to open T2S for settlement during weekend:

- The NTS cycles are completed and T2S would open for RTS settlement on Saturday after a shortened Maintenance Window (MWI) at a time to be agreed on a case by case basis depending on the activities to be concretely performed as well as on the duration of the release and deployment management activities. In such case the RTS would remain open until Monday at 5:00 (normal RTS beginning after the week-end) and even continues until Monday start of EOD;

- The T2S Start of Day event (standard time 18:45) and the following NTS and MWI phases are postponed to Saturday morning. They will start after the T2S or CSD and/ or NCB major release deployment phase is completed

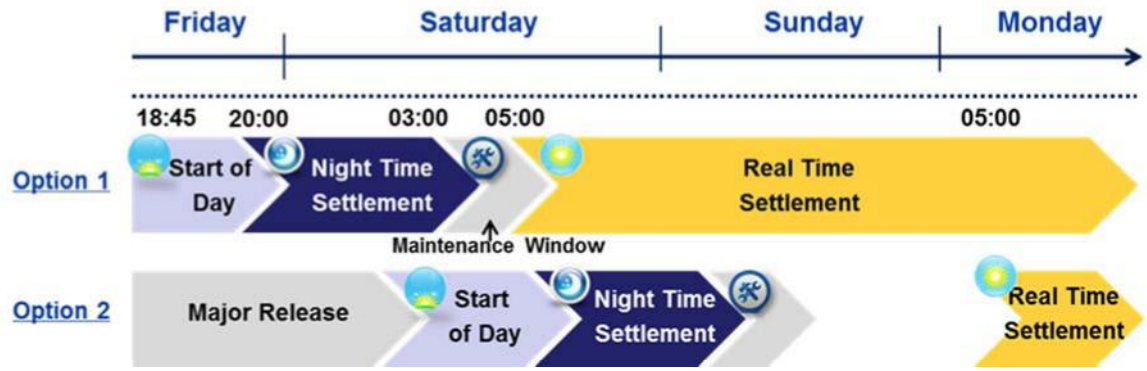


Figure 6 - T2S Operation during Weekend for Settlement

Regarding option 1 the request to open T2S during weekends for settlement is submitted to the T2S Service Desk via e-mail at least three months in advance. The T2S Service Desk will inform the T2S Coordinator accordingly. After the feasibility check, the agreement is requested from the whole community via e-mail to Settlement Managers. The Se ttlement Managers can provide agreement/ disagreement within next 5 days. Only in case of need (e.g. diverging views or different organisational needs to be accommodated) a Settlement Managers' conference call will be organized.

Option 2 is planned in advance according to the T2S release plan that includes time plan of major releases from CSDs and Central Banks.

3.7 TECHNICAL DISCONNECTION OF A PARTICIPANT USING ABNORMALLY THE SYSTEM

Description

T2S Actors (excluding ICPs), accessing the T2S Platform through NSPs, are registered in the CGU. The CGU shall restrict access to the connectivity services only to the identified and authorised users. The registration process to the CGU is arranged via the NSP.

T2S has implemented a number of technical measures to avoid that abnormal behaviour of a T2S Actor (excluding ICP) in the technical infrastructure or application can hamper the stability of the system or have an impact on other users.

Operational Procedure

In the unlikely event that the measures referred above are not effective and there is evidence that the system's integrity is at stake, the T2S Service Desk shall:

- Contact the concerned T2S Actor (excluding ICPs), asking them to stop the abnormal behaviour without delay;
- Verify, in cooperation with T2S Actor (excluding ICPs) and the NSP, if technical measures on T2S' or NSP's side are available to return to a normal situation;
- Ask the NSP to withdraw the involved T2S Actor (excluding ICPs) from the CGU in case the threat to the stability of the platform with impact on other service users is still present and no other measures have been proven effective.

The T2S Coordinator is informed and a Settlement Managers'/ Crisis Managers' conference call is initiated prior to withdrawal of the CSD/ Central Bank or DCP.

The T2S Coordinator, in accordance with the Article 36 of the FA, will consult the Relevant Competent Authorities.

The NSP shall withdraw the T2S Actor(s) (excluding ICPs) from the CGU within one hour. The withdrawal can be requested for the U2A access, the A2A access, or both depending on the nature of the incident.

The suspension from the CGU remains effective until the T2S Actor (excluding ICP) has declared to the T2S Service Desk that the threat no longer exists.

3.8 BLOCKING ONE OR MORE PARTY TECHNICAL ADDRESSES TO KEEP T2S OUTGOING MESSAGES ON HOLD

Issue description

The Party Technical Address (PTA) is the parameter allowing each T2S Actor (excluding ICPs) directly connected to T2S to receive messages from the T2S central application. After the definition, each PTA has to be linked to the relevant network services(s).

If at any moment during the settlement day the T2S Actor (excluding ICPs) experiences disturbances at the level of its local application interfacing T2S, this T2S Actor might require to temporarily block some or all the messages T2S is sending. Needless to say, should the T2S Actor (excluding ICP) be in a position to intercept its incoming messages before they reach their local application or any other way to avoid interferences in its incident resolution procedures, the below described procedure does not need to be activated.

Operational procedure

At any moment during the settlement day, a T2S Actor (excluding ICP's) directly connected to T2S can request the T2S Service Desk to intraday temporarily block one or more of its PTAs;

- Such request has to be provided via signed e-mail listing all the PTAs whose temporary blockage is being requested;
- The T2S Service Desk treats the request immediately;
- After the provisional blockage is implemented, the T2S Service Desk sends a return signed e-mail to the requesting T2S Actor (excluding ICPs) to confirm the execution;
- The messages whose routing normally happens through the blocked PTAs are held at the level of the central T2S application. They are anyway visible via the standard screens.

Once the requesting T2S Actor (excluding ICPs) decides the messages holding is no longer necessary:

- It sends another signed e-mail to the T2S Service Desk as a reply to the latter's confirmation to the original request, where the unblocking of the PTAs is requested;
- A partial unblocking is also possible. In such case, the list of the ones to be unblocked has to be clearly and explicitly provided. Failing such detail, all the previously blocked PTAs are unblocked;
- After the T2S Service Desk executes the partial or complete unblocking request, it returns via signed e-mail to the requesting T2S Actor (excluding ICPs) to confirm the unblocking is done;
- The held messages are released and from that moment the normal process is restored.

3.9 HANDLING OF INFORMATION SECURITY EVENTS (E.G. CYBER-ATTACK)

Description

Information Security management is not static. The business environment is constantly changing and new threats and vulnerabilities can occasionally emerge. Systemically important financial market infrastructures like T2S may be targeted by attackers for various reasons. In this context, both proactive and reactive information security controls must be in place to protect T2S from a wide range of threats that, despite all measures taken, do materialise.

Operational procedure

The aim of the present procedure is to address how significant information security events should be handled in a manner whereby potential damages caused to T2S stakeholders' interests are limited to a minimum.

The T2S Operator relies on a set of technical monitoring features and operational processes aiming at proactively detecting potentially harmful events and patterns at different levels of the application and technical components of the T2S Platform. More particularly, all incoming connections established with the T2S Platform over external network will be under constant monitoring.

If for whatever reason there is evidence that the system's security is at stake, the T2S Service Desk shall take any relevant measures, including one or more of the following:

- Contact the respective T2S Actor (excluding ICP), requesting them to take measures against the attack without delay;
- Verify, in cooperation with the respective T2S Actor (excluding ICPs) and the NSP, if technical measures on T2S' or NSP's side are available to return to a normal situation;
- Revoke user certificates or suspend user accesses; or, in last resort,
- Request the NSP to withdraw the involved T2S Actor (excluding ICPs) from the CGU in case the threat to the security of the platform with impact on other T2S Actors (excluding ICPs) is still present and no other measures have been proven effective.

The T2S Coordinator will be kept informed during the whole process, and a conference call of the Settlement Managers /Crisis Managers shall be initiated in case the withdrawal of the CSD/ NCB or DCP is deemed necessary or if global coordination is required to address the situation.

In case after two hours the cause of the disruption is not removed the T2S Coordinator according to the Crisis Management process will launch another Crisis Managers' conference call in order to assess the situation.

Where relevant:

- The T2S Operator shall suspend user accesses within one hour and ask Certification Authorities to revoke user certificates at the earliest opportunity;
- The NSP shall withdraw the T2S Actor(s) (excluding ICPs) from the CGU within one hour. The withdrawal can be requested for the U2A access, the A2A access, or both depending on the nature of the incident. The suspension from the CGU remains effective till the respective T2S Actor has declared to the T2S Service Desk that the threat no longer exists.

3.10 COMMUNICATION ON OPENING AND CLOSING DCA ACCOUNTS

Description

In case a payment bank wants to create or close/delete a dedicated cash account it has to request this through the NCB.

Operational procedure

The creation, closure and deletion of a DCA is performed by the responsible NCB. The NCB opens, closes and deletes DCA accounts on the request of payment banks.

The opening of DCA accounts is using a two-step approach:

- The payment bank request the NCB to open the DCA;
- Once the DCA has been opened the payment bank contacts its CSD(s) to complete the set up and perform the link of the DCA to securities account(s). The CSD(s) links the DCA to the securities account(s) in order to specify the cash account used for the settlement of the cash leg of transactions.

Should a payment bank wish to close/ delete a DCA, this is also done following a two-step process:

- The payment bank request its CSD(s) to remove the link(s) between the DCA and the securities account(s);
- Once all the link(s) have been removed the payment bank requests the NCB to close the DCA. Once the DCA has been closed it cannot be used anymore for cash settlements and liquidity transfers.
- The DCA can be deleted by the NCB. Before the deletion of a DCA T2S performs an automatic check that no links to securities account(s) exist.

Payment banks will request the respective CSDs to create or remove the link(s) of the DCA to the securities account(s) when requesting the opening or closure/deletion of the DCA, consequently the CSD will be involved in the process and is made aware of created and closed/deleted DCA accounts.

In special situations such as the insolvency of a participant, where an NCB may decide to block a DCA, the NCB informs the CSD(s) using T2S broadcasts.

4 INCIDENT MANAGEMENT

An incident is defined as an unplanned interruption or a reduction in the quality of an agreed service.

The Incident Management process manages the lifecycle of all incidents, i.e. it identifies and resolves the incidents while providing updated information of the status of the relevant incident(s) to all T2S Actors (excluding ICPs) involved in day-to-day operations. This process coordinates all tasks to restore the services as quickly as possible and minimises the adverse impact of the incident on business operations within the limits of the agreed Service Levels as specified in the FA/ CPA Schedule 6 and the relevant T2S legal framework.

This chapter provides the high level ptinciples as relevant for those involved in d ay-to-day operations.

The T2S Actors are shown in the Figure below:

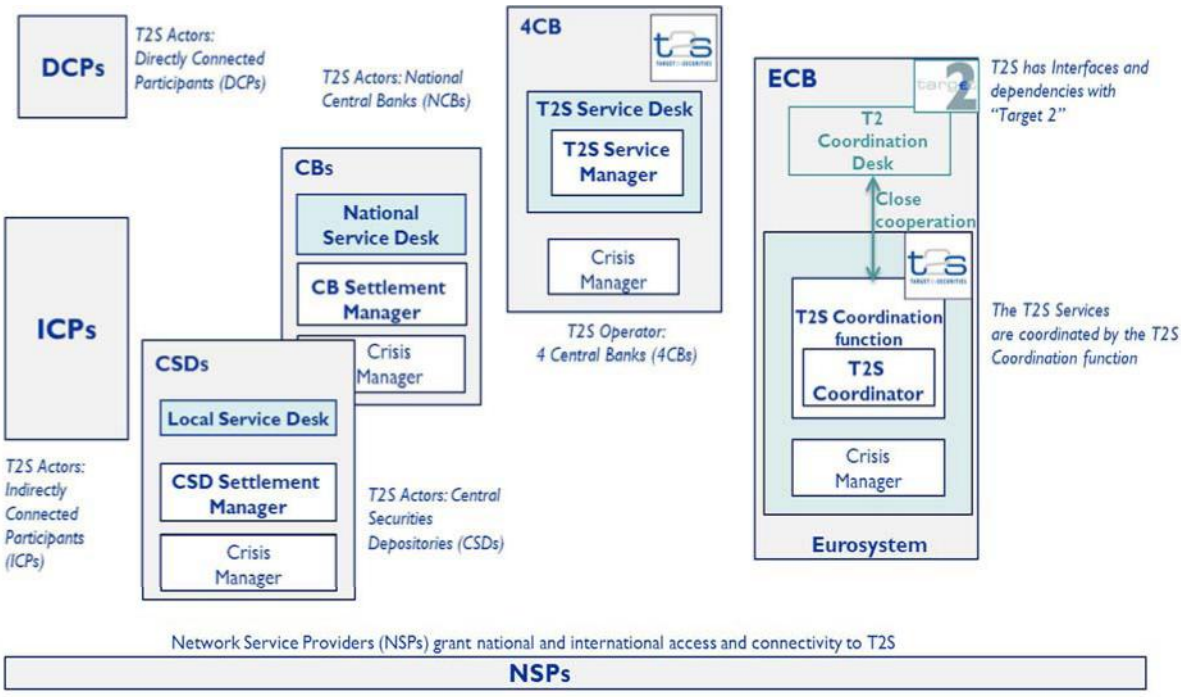


Figure 7 - T2S Actors and the NSPs

There are five pre-defined incident scenarios, depending on at which level the incident occurs. The five pre-defined scenarios are as follows:

1. Scenario 1: Incident at the level of the T2S Platform (at 4CB as T2S Operator);
2. Scenario 2: Incident at the level of TARGET2/ RTGS;
3. Scenario 3: Incident at the level of one or more CSDs;
4. Scenario 4: Incident at the level of DCPs or ICPs;
5. Scenario 5: Incident at the level of NSP.

The incident scenarios 1-5 are based on the general Incident Management process flow, although steps might differ from scenario. The processes shown in ***Error! Reference source not found.*** might have additional interfaces with other processes. In such case, the relevant processes are triggered.

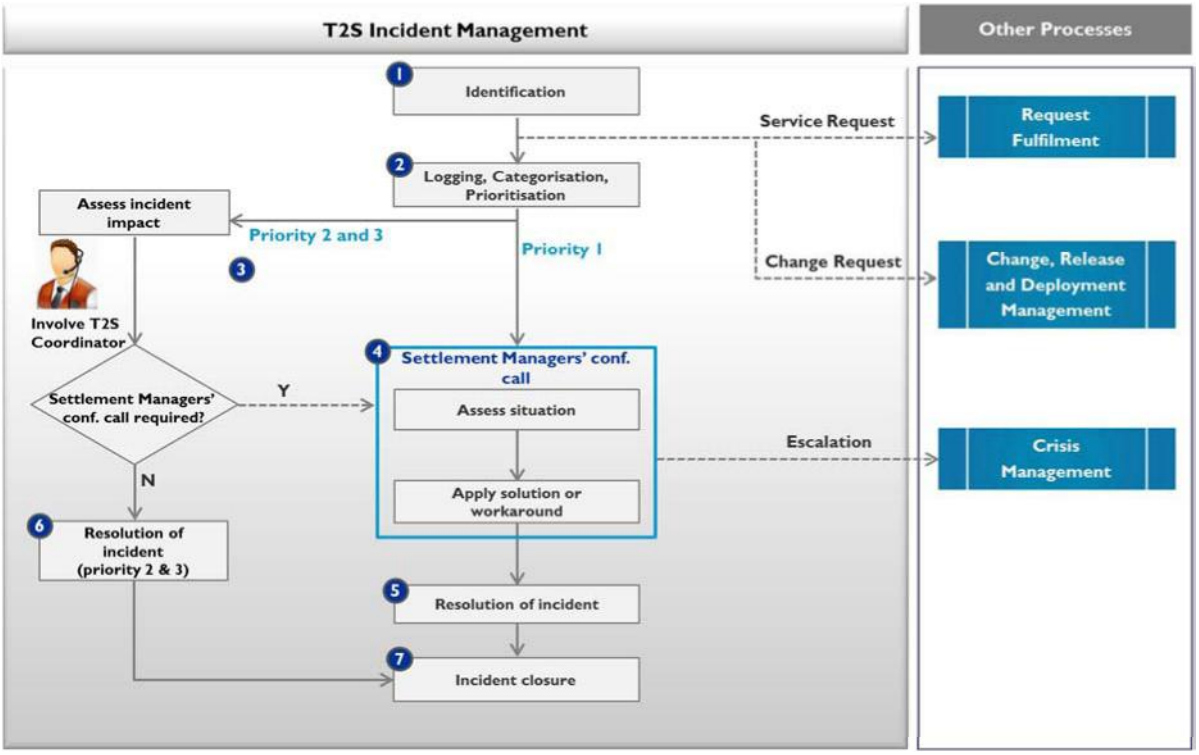


Figure 8 - General Incident Management process flow

An incident logged with the T2S Service Desk might be reprioritised during its life cycle, since at the initial stage the full picture of the impact might not be visible. The reprioritisation could be either upgrading the priority level from the originally logged or it may be reducing the priority level based on impact reassessment. The reprioritisation can be requested by any T2S Actor (excluding ICP) requesting the T2S Coordinator based on the re-assessed impact.

Incidents will be categorised in the following priorities:

Incident Priority	Severity	Impact
Priority 1	Critical	- Complete unavailability of all T2S Services (see FA/ CPA Schedule 6) - Complete unavailability of one or more services for which no work-around is available
Priority 2	Urgent	Unavailability of a service, but a work-around is available
Priority 3	Medium	All services are available, but some are experiencing performance issues
Priority 4	Low	Query or Service Request

Table 5 - Incident Priority

5 ACCESS MANAGEMENT

5.1 PURPOSE AND SCOPE OF ACCESS MANAGEMENT

The purpose of Access Management (ACM) is to grant authorised DCPs the right to use T2S Services, while preventing access to non-authorised users. ACM is designed to:

- Manage access to T2S Services; efficiently respond to requests for granting DCPs access to T2S Services, change access rights or remove access, ensure that the rights being provided or changed are properly granted;
- Monitor access to T2S Services and ensure that the rights provided to DCPs are not improperly used.

5.2 OVERVIEW OF CUSTOMER FACING ACM ACTIVITIES

DCPs can access the T2S Services through a NSP which, in addition to connectivity services, provides CGU management, Public Key Infrastructure (PKI) services, access control and non-repudiation of messages sent. While the biggest part of all activities to manage accesses end-to-end lies within the T2S providing organisations (4CB, Eurosystem) and within the licensed NSPs (SWIFT, SIA/Colt), in this chapter only the part relevant for DCPs is described.

The DCPs' relevant ACM activities are listed below:

- Requesting access rights;
- Requesting changes to existing access rights;
- Requesting removal of access rights;
- Monitoring access to T2S Services.

Prior to requesting access to T2S Services, DCPs need to inform the CSD/ Central Bank of their intention to connect directly with T2S. DCPs can request U2A access for their internal end-users and A2A access for their applications.

5.3 REQUESTING ACCESS RIGHTS

In order to get access to T2S Services, a DCP needs to follow the following steps to obtain:

- Digital Certificates used for authentication and signing purposes;
- The technical configuration of the NSP services;

- The proper configuration of T2S Static Data (Parties, Securities and Accounts).

Step	Action
1	Select the NSP of choice and join the related services
2	Select the NSP's offer and related products
3	Subscribe to the NSP's Services for T2S (e.g. inclusion into the CGU)
4	Request for the NSP digital certificates
5	Connectivity setup with NSP
6	NBB-SSS: Create the Party in T2S Static Data according to the T2S registration procedure
7	NBB-SSS: Link the Party to the Network Service of choice in Static Data
8	Create the users, set up the related Certificate-DN links, and assign role/ privileges to them according to their functions
9	Set up statements and reports in Static Data
10	Connectivity test with T2S

Table 6 - Steps for Granting T2S Access to DiCoAs

5.3.1 DCP REQUESTS

Step 1 Select the NSP of choice and join the related services

- Please see the NSP documentation and licence agreement.

Step 2 Select the NSP's offer and related products

- Please see the NSP documentation and visit the NSP website.

Step 3 Subscribe to the NSP's Services for T2S (e.g. Inclusion into the CGU)

- Via the VA-NSP website, select the appropriate scenario and the environment(s) for which access is requested. Please see the NSP documentation. Access can be requested to each of the licensed NSP either for the T2S production environment for processing T2S Live Operations, or at once for all the relevant T2S test environments. Two registration scenarios are possible:

T2S Actor	CGU (2 scenarios)	Environment(s)
DCP	U2A only	Test
		Production
	U2A + A2A	Test
		Production

Table 7 - Environments Available to T2S Actors

- This step requires the dual approval of the NBB-SSS and of the T2S Operator;
- The requester is informed via e-mail of any change in the status of the request. If the request is rejected, the rejection cause is provided. If it is accepted, a final confirmation is provided to the requestor once the implementation date is defined;
- If a DCP is customer of more than one CSD/ Central Banks this step must be performed only once. Upon request the T2S Service Desk can confirm to the NBB-SSS if a DCP is already registered to the T2S Connectivity Services.

Step 4 Request for the NSP digital certificates

- The NSP Certificate Authority can issue certificates:
  - on USB token for the U2A access of end-users; or
  - on HSM for the A2A access of applications.

Please see the NSP documentation.

Step 5 Connectivity setup with the NSP

- On the implementation date, the NSP performs service provisioning activities according to the request form, after which a final confirmation is sent to the requester.

Step 6 NBB-SSS: Create the Party in T2S Static Data according to the T2S registration procedure

- The NBB-SSS will create the DCP in T2S;
- T2S Registration Guide and UHB V2.0 *Section 3.8 "Party Management"; UDFS V2.0 Sections 1.2 "Configuration of Parties, Securities and Accounts" and 1.3 "Access to T2S"*

Step 7 NBB:SSS: Link the Party to the Network Service of choice in Static Data

- UHB V2.0 Sections 3.8.1 "Administration of Participants" and 3.17. 1 "Configuration of a Technical Address" to configure one or more technical addresses and create technical address service links.

Step 8 Create the users, set up the related Certificate-DN links, and assign role/ privileges to them according to their functions

- Only registered users have access to the T2S GUI, therefore registration in T2S reference data and to the network is necessary prior to the first GUI access;
- UHB V2.0 Section 3.2 "Access Rights". See also *UDFS V2.0 Sections 1.2 "Configuration of Parties, Securities and Accounts" and 1.3 "Access to T2S"*;

- In order to create the users, set up the related certificate-DN links, see the UHB V2.0 Section 3.2.4 “Configuration of a User” and follow the procedure described in the T2S Connectivity Guide Section 4.3 “Setting up Parties and Users”;
- In order to assign roles and privileges according to the parties’ and users’ functions, see the UHB V2.0 Sections 3.2.1.3 “Assign a Role to a User” and 3.2.1.4 “Assign a Role to a Party”.

Step 9 Set up statements and reports in Static Data

- see UHB V2.0 Sections 3.7 “Cash and Settlement Monitoring” and 3.9 “Report”.

Step 10 Connectivity test with T2S

- see User Testing documentation and to the T2S Connectivity Guide.

5.3.2 DCP PRIVILEGES

In the hierarchical party model structure of T2S the NBB-SSS can grant all available privileges to the DCP. The DCP can inherit system privileges only via the responsible CSD, i.a. the NBB-SSS.

The DCP would typically have Admin users and Business users segregated although T2S does not prevent assigning “business” privilege to admin user.

The set of privileges which promote a standard user to admin user is the following:

- ARM_AdministerParty,
- ARM_GrantPrivilege,
- ARM_GrantRole,
- ARQ_GrantedSysPrivilegesListQuery,
- ARQ_GrantObjectPrivilegesListQuery,
- ARQ_GrantedRolesListQuery.

Based on this configuration the Admin user will inherit all the privileges granted at party level and can propagate the privileges to other users within their party.

The full list of privileges is attached in annex 1.

6 SERVICE CONTINUITY MANAGEMENT

6.1 PURPOSE AND SCOPE OF SERVICE CONTINUITY MANAGEMENT

According to the FA/ CPA, the terms "business continuity" and "disaster recovery" mean the set of rules and procedures aimed at resuming normal T2S Services in compliance with the Service Levels as described in FA Schedule 6 (T2S Service Level Agreement), after the occurrence of an incident which triggers a Crisis or disaster, as well as at mitigating the impact of such an incident.

In terms of ITIL® V3, Business Continuity Management (BCM) deals with the analysis, mitigation and prevention of risks, which may lead to an interruption in the business process regardless of what root-cause (e.g. non-IT issues as earth quakes, or IT-related service breakdowns).

BCM aims to reduce the probability of down-time risks of critical business processes to an acceptable level and to devise measures to ensure that business processes can be resumed within a previously determined period of time and scope. The Service Continuity Management (SCM) is a component of the BCM process and focuses on restoring and protecting the required T2S services. While BCM is a holistic management process of the Eurosystem which goes beyond T2S, the real SCM tasks, which focus on the T2S Services, are provided by the 4CB. The Service Continuity Management assures that T2S Services Provider (4CB) undertakes all means to implement and maintain service assets that will provide the agreed level of contingency and recovery. The T2S Services have to be supported through major failures or disruptive events in order to return to normal operations after a Crisis event. Continuity is assured primarily through redundancy and providing alternative resources that are dedicated to delivering services during contingencies and that are not impacted by the original event.

6.2 T2S SERVICE CONTINUITY

Like in TARGET2, the architecture of the T2S core system is based on the concept of "2 regions/ 4 sites". The four sites are fully equivalent and each of them is equipped with the same technical resources: processor, storage, network interface, software, etc. The two sites in each region are located at a distance that is sufficient to have a distinct risk profile. The two regions are located at geographical distance of several hundreds of kilometres.

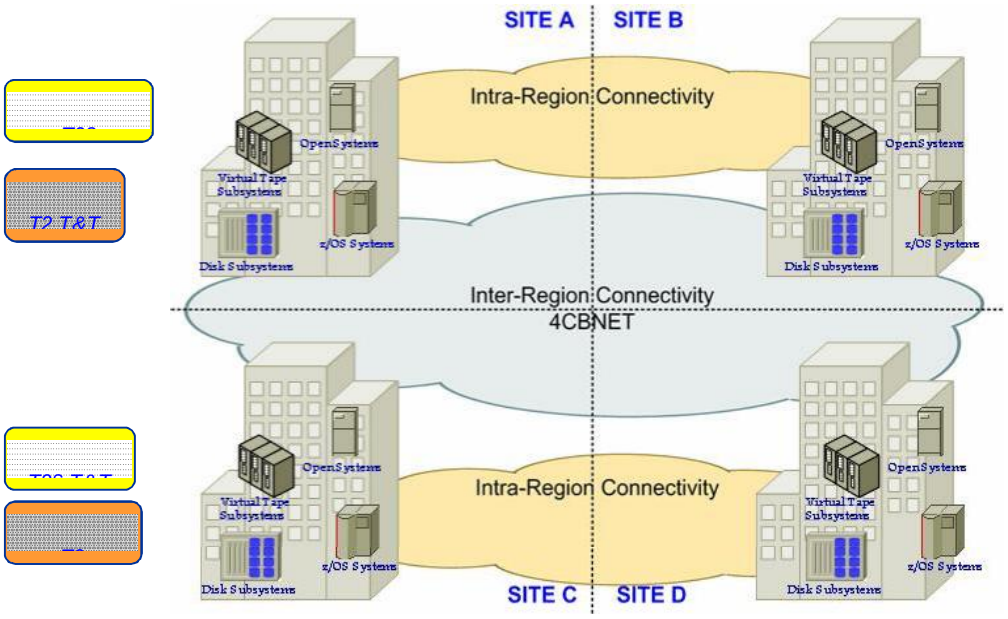


Figure 9 - T2S service continuity

The service continuity design involves different levels of the overall architecture requiring various technical solutions. A detail description of the technical solution can be found in the document T2S General Technical Specifications v2.2.0.

6.2.1 MAJOR FAILURE

Each region has the capability of a local recovery; the two sites in each region are located at a distance of a few kilometres from each other. The recovery within a region is assured by Synchronous Remote Copy (SRC) activated on the whole environment between the two sites of the same region. The SRC guarantees real time data updates in both sites; i.e. each write operation is completed only when both sites are updated. Major failure or disaster is meant to indicate a serious service interruption which is solved by relocation of T2S operations to a second site (intra-region failover), physically separate from the primary site. As a synchronous mode is applied, the databases at both sites are exactly the same, and no reconciliation is required after a failover.

An intra-region failover can be conducted by the 4CB if they decide so following an appropriate technical assessment. Both the problem identified and its envisaged solution must be reported to the T2S Coordinator as a priority 1 incident, and will follow standard Incident and Crisis Management process.

Figure 10 - Communication flow during Crisis: initiating Crisis Managers' conference call

An intra-region failover ensures the continuation of normal business within a maximum of one hour.

The processing is interrupted during the failover, but the T2S Actors are encouraged to keep on sending messages/ files, which will be queued, to the T2S System and processed when the System restart. The GUI interface is unavailable during the recovery.

The activation of the intra-region recovery on the TARGET2 System will cause the unavailability of the T2S test environments, resuming will be done on a best effort basis.

6.2.2 REGIONAL DISASTER

Recovery from a regional disaster is based on the presence of an alternate region located at a long distance away from the primary one (hundreds of kilometres). Due to the long distance, the recovery from one region to the other is only possible by Asynchronous Remote Copy (ARC), activated on the whole environment. The ARC cannot guarantee real time updates in both regions. As write operations in the remote region are asynchronous, it is possible that some data updates are lost if a regional disaster occurs. The amount of lost updates depends on the workload. The databases in the two regions show the processing status with a time discrepancy of a maximum of two minutes.

The recourse to inter-region recovery may be triggered by a number of events, including a wide-area disaster having a high impact on the region operating T2S; to be effective even in a worst-case scenario, the plan for recovering the operating region avoids any dependency (decisional, personnel, technical, etc.) from that region; i.e. the alternate region is able to take over the operation without relying at all on the impacted region.

If both sites within Region 1 become unavailable at the same time or if the asynchronous copy facility has problems, then, a loss of data would occur. In such a situation, there is no alternative but failing over to Region 2 and reconciling the missing traffic. Still the resumption of the business in Region 2 should be enabled within two hours in Region 1, excluding the time between informing service users and the service users' response, i.e. the time they need to reconcile the lost data.

Should the type of incident (e.g. in case of the so-called rolling disaster) allow an orderly and progressive external connections closure so to complete smoothly the asynchronous copy towards Region 2, the inter-region failover and the resumption of operations in Region 2 would result in no loss of data and it will be done within two hours.

Not just processing, even access to GUI may also be interrupted during a failover. The users should not send new traffic to the system during a failover.

Given the severe circumstances leading to an inter-region failover, both the Settlement and Crisis Managers will be kept informed all through the process, and accompanying conference calls will be held. More precisely, communication in the event of an inter-region failover is as follows:

- Regular reporting of the incident from detection onwards to the T2S Coordination function with a Settlement Managers' conference call and subsequent a Crisis Managers' conference call;
- After the successful failover a Crisis Managers' conference call is held to discuss next steps or approve the opening of the system for normal processing; afterwards there is a Settlement Managers' conference call to execute decisions taken by the Crisis Managers.

Figure 11 - Communication flow during Crisis: initiating Crisis Managers' conference call

The activation of the intra-region recovery on the TARGET2 System could cause the unavailability of the T2S test environments, resuming will be done on a best effort basis.

6.2.3 REBUILDING PROCESS

In case of regional disaster with loss of data, the rebuilding process is conducted by the T2S Actors (excluding ICPs) that have submitted instructions via every channel in the last 10 minutes before the consistency point with the support of the T2S Service Desk.

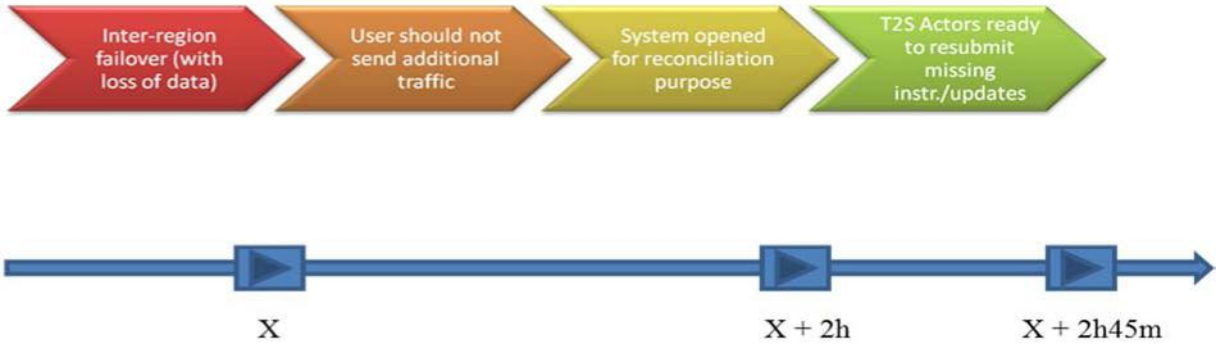


Figure 121- Rebuilding after Crisis

Rebuilding process:

In such case the T2S Actors (excl. ICPs) need to perform a reconciliation of instructions the respective T2S Actor has recorded as transmitted against the instructions present in T2S and identify which instructions have been lost during the disaster.

CSD/ Central Bank/ DCP can use T2S queries (U2A or A2A) to retrieve the information related to the instructions they have already transmitted to T2S, which may have lost during the regional disaster period. DCPs that have instructed liquidity transfers during this period should also inform their respective Central Banks.

6.3 INFORMATION REQUIRED BY CSD / DCP OF CSD IN CASE OF RAD

Once the system is opened for the purpose of reconciliation, meaning that it will not be possible to send new instructions in A2A mode (technically enforced), the users have to avoid to send new instructions in U2A mode (not technically enforced). Nevertheless, with regards to instructions, that would have been transmitted using the GUI during the time period affected by the regional disaster, the NBB-SSS can either ask its DCPs to inform of these instructions (GUI users to perform their own reconciliation), or these can be identified and reinstructed at a later stage by the participants, as this step is likely to be time consuming and only affect a limited number of messages.

To avoid receiving new instructions via U2A mode, the NBB-SSS will communicate and instruct its DCPs not to use the T2S GUI to submit new instructions. CSDs can proceed for the reconciliation process using the standard query tool (both in U2A and in A2A). CSDs can use real-time T2S queries to retrieve information on demand. The information provided in a query response is always based on the latest data available in T2S. As queries are sent and answered in real-time, the query response in general consist of only one XML message with result.

The NBB-SSS would need to perform reconciliation for the last 10 minutes on the following:

- Verify the settlement instructions processed information;
- Verify the Intra-Position Movement information;
- Verify the Amendment Instruction information for Settlement Instructions or Settlement Restrictions on Securities Position and;
- Verify the Cancellation Instruction information for Settlement Instructions or Settlement Restrictions on Securities Position.

T2S includes in a query result all securities account owned by all the participants of the NBB-SSS. For a query on the level of the participant, T2S includes all the securities of the participant. Nonetheless, depending on the search criteria which are specified in the query message, the query response is grouped by the specified search criteria. For example, if the NBB-SSS queries for all the Settlement Instructions at the level of securities account owner or securities account then the Settlement Instructions within the query response is grouped by securities account owner or securities account respectively.

Therefore, there are two approaches for reconciliation:

- The NBB-SSS can process reconciliation for its own instructions (and ICPs') and DCP instructions separately to T2S or;
- The NBB-SSS can process reconciliation for settlement instructions or settlement restrictions sent by their DCPs altogether, as they cover all securities account owned by the NBB-SSS including DCP's securities accounts.

The NBB-SSS will provide the reconciliation information to its DCPs. After reconciliation, once the confirmation that everyone is in a position to submit the possibly missing instructions given, the system is reopened in full mode, i.e. including instructions and updates processing. In resubmitting instructions the T2S Actors (excluding ICPs) have to ensure, to the maximum possible extent, that this is done using the same business reference as before (in Region 1) but not the same network reference. This would allow the standard double-entry check at T2S central system level to properly discriminate possible duplicated messages and to consequently avoid double bookings/ updates. When the internal evidences of all impacted T2S Actors (excluding ICPs) have been re-established as they were in Region 1, the system can be again used for normal operations.

6.4 SERVICE CONTINUITY TESTING

DCPs are subject to service continuity testing procedures.

For the tests to be effective, they are either performed in the production environment or, where this is not considered appropriate due to the additional operational risk, in a test environment as similar as possible to the production environment. The testing of the business continuity procedures of the NSPs do not fall within the scope of this document and their testing requirements are described in the NSP User Documentation.

Service continuity measures aim to ensure that failures of T2S components at any level do not cause a disruption to the overall functioning of the system.

DCPs need to first rely on their own backup measures. T2S and the NBB-SSS offer only limited contingency arrangements to overcome interruptions happening at the side of the DCPs in the connection with the T2S System, aiming at processing a limited number of transactions.

The NBB-SSS will collect test reports from its DCPs and send the reports to the T2S Coordinator, in principle on a yearly basis. It is expected that the test participants will perform a limited number of business transactions from the secondary site. Test results should be classified as either successful or unsuccessful. When the test objectives are not met, the test result should be seen as unsuccessful. For unsuccessful tests a repetition of the test is expected to be performed within 3 months.

Annex 1

T2S Direct: Access Rights (T2S privileges) required by DCPs

The list of privileges is based on the one published by the ECB on 29.9.14. http://www.ecb.europa.eu/paym/t2s/about/keydocs/html/index.en.html

Class of Privileges	Privilege	Privilege type	object type	PrivilegeShortName - New	Usage	CSD	Privileges can be given to DCPs (Y/N)
Access Rights Management	Administer Party	System	n/a	ARM_AdministerParty	U2A	Y	Y
Dynamic Data Queries	Allegement Query	Object	Party	DDQ_AllegementQuery	U2A	Y	Y
Settlement CSD	Amend Process Indicator of a non-modifiable Settlement Instruction on behalf of the Instructing Party of the underlying instruction	Object	Party	SIC_ANMBI	Both	Y	Y
Settlement General	Amend Process Indicator of a Settlement Instruction/Settlement Restriction on Securities either on a Securities Account or on Behalf of the CSD in T2S or on Behalf of an external CSD	Object	Securities Account Party	SIG_AMNPI	Both	Y	Y
Dynamic Data Queries	Amendment Instruction for Intra-Position Movement or Settlement Instruction Audit Trail Details Query	Object	Securities Account	DDQ_AmdInsIntrPosMovSetInsAudTrDe	U2A	Y	Y
Dynamic Data Queries	Amendment Instruction for Intra-Position Movement or Settlement Instruction Audit Trail List Query	Object	Securities Account	DDQ_AmdInsIntrPosMovSetInsAudTrLis	U2A	Y	Y
Dynamic Data Queries	Amendment Instruction Query for Intra-Position Movements and Settlement Instructions	Object	Securities Account	DDQ_AmendInstrQIntraPosMov+SetInst	Both	Y	Y
MSA Data Queries	Attribute Domain Details Query	System	n/a	MSA_AttributeDomainDetailsQuery	U2A	Y	yes, but no visibility
MSA Data Queries	Attribute Domain List Query	System	n/a	MSA_AttributeDomainListQuery	U2A	Y	yes, but no visibility
MSA Data Queries	Attribute Reference Details Query	System	n/a	MSA_DisplayAttribDomainRefDetQuery	U2A	Y	yes, but no visibility
MSA Data Queries	Attribute Reference List Query	System	n/a	MSA_DisplayAttribDomainRefListQuery	U2A	Y	yes, but no visibility
Dynamic Data Queries	Broadcast Query	System	n/a	DDQ_BroadcastQuery	U2A	Y	Y
Settlement CSD	Cancel Non-modifiable Instructions on behalf of the Instructing party of the Underlying Settlement Instruction	Object	Party	SIC_CNMBI	Both	Y	Y
Settlement General	Cancel Settlement Instruction / Settlement Restriction on Securities either on a Securities Account or on Behalf of the CSD in T2S, on Behalf on external CSD or on Behalf of an Administering Party	Object	Securities Account Party	SIG_CANCI	Both	Y	Y
Dynamic Data Queries	Cancellation Instruction for Intra-Balance Movement Audit Trail Details Query	Object	T2S Dedicated Cash Acco	DDQ_CancInstrIntraBalanMovAudTrDetQ	U2A	Y	Y
Dynamic Data Queries	Cancellation Instruction for Intra-Position Movement or Settlement Instruction Audit Trail Details Query	Object	Securities Account	DDQ_CancInstrIntraPosMovAudTrDetQ	U2A	Y	Y
Dynamic Data Queries	Cancellation Instruction for Intra-Position Movement or Settlement Instruction Audit Trail List Query	Object	Securities Account	DDQ_CancInstrIntraPosMovAudTrLisQ	U2A	Y	Y
Dynamic Data Queries	Cancellation Instruction Query for Intra-position Movements and Settlement Instructions	Object	Securities Account	DDQ_CancInstrForSI+IntraPosMovQuer	Both	Y	Y
Access Rights Queries	Certificate Query	System	n/a	ARQ_CertificateDNQuery	U2A	Y	Y
Scheduling Queries	Closing Day Query	System	n/a	SCQ_ClosingDayQuery	U2A	Y	Y
SAC Data Queries	CMB Securities Account Link List Query	System	n/a	SAQ_DisplayCMBSecAccLinkListQuery	U2A	Y	Y
Dynamic Data Queries	Collateral Value of a Security Query	System	n/a	DDQ_CollatValue-of-SecurityQuery	Both	Y	Y
Dynamic Data Queries	Collateral Value per T2S Dedicated Cash Account Query	System	n/a	DDQ_CollatValuePerT2SDCAQuery	Both	Y	Y
MSA Data Queries	Conditional Security Delivery Rule List Query	System	n/a	MSA_ConditSecDeliveryRuleQuery	U2A	Y	Y
MSA Data Queries	Conditional Security Delivery Rule Set Query	System	n/a	MSA_ConditSecDeliveryRuleSetQuery	U2A	Y	Y
Static Data Queries	Country Query	System	n/a	SDQ_CountryQuery	U2A	Y	Y
Market Specific Configuration	Create Attribute Domain	System	n/a	MSC_CreateAttributeDomain	U2A	Y	N
Market-Specific Configuration	Create Attribute Reference	System	n/a	MSC_CreateAttributeReference	U2A	Y	N
Access Rights Management	Create Certificate Distinguish Name	System	n/a	ARM_CreateCertificateDN	U2A	Y	Y
Securities Account Data Manager	Create CMB Securities Account Link	System	n/a	SAC_CreateCMBSecuritiesAccountLink	Both	Y	Y

34	Market-Specific Configuration	Create Conditional Security Delivery Rule	System	n/a	MSC_CreateConditSecurDelivRule	U2A	Y	N
35	Market-Specific Configuration	Create Conditional Security Delivery Rule Set	System	n/a	MSC_CreateConditSecurDelivRuleSet	U2A	Y	N
36	Securities Account Data Manager	Create CSD Account Link	System	n/a	SAC_CreateCSDAccountLink	U2A	Y	N
37	Security Data Management	Create Eligible Counterpart CSD Link	System	n/a	SDM_CreateEligibleCounterpCSDLink	Both	Y	N
38	Market-Specific Configuration	Create Market-Specific Attribute	System	n/a	MSC_CreateMarket-SpecificAttribute	U2A	Y	N
39	Message Subscription	Create Message Subscription Rule	System	n/a	MSU_CreateMessageSubscriptionRule	U2A	Y	Y
40	Message Subscription	Create Message Subscription Rule Set	System	n/a	MSU_CreateMessSubsRuleSet	U2A	Y	Y
41	Party Data Management	Create Party	Object	Party	PDM_CreateParty	Both	Y	Y
42	Report Configuration	Create Report Configuration	System	n/a	RCO_CreateReportConfiguration	U2A	Y	Y
43	Market-Specific Configuration	Create Restriction Type	System	n/a	MSC_CreateRestrictionType	U2A	Y	N
44	Market-Specific Configuration	Create Restriction Type Rule	System	n/a	MSC_CreateRestrictionTypeRule	U2A	Y	N
45	Access Rights Management	Create Role	System	n/a	ARM_CreateRole	U2A	Y	N
46	Network Configuration	Create Routing	System	n/a	NCO_CreateRouting	U2A	Y	Y
47	Access Rights Management	Create Secured Group	System	n/a	ARM_CreateSecuredGroup	U2A	Y	N
48	Securities Account Data Manager	Create Securities Account	Object	Party	SAC_CreateSecuritiesAccount	Both	Y	Y
49	Security Data Management	Create Security	Object	Party	SDM_CreateSecurity	Both	Y	Y
50	Security Data Management	Create Security CSD Link	System	n/a	SDM_CreateSecurityCSDLink	Both	Y	N
51	Network Configuration	Create Technical Address Network Service Link	System	n/a	NCO_CreateTechnAddressNetServLink	U2A	Y	N
52	Access Rights Management	Create User	System	n/a	ARM_CreateUser	U2A	Y	Y
53	Access Rights Management	Create User Certificate Distinguish Name Link	System	n/a	ARM_CreateUserCertificDNLink	U2A	Y	Y
54	SAC Data Queries	CSD Account Link Query	System	n/a	SAQ_CSDAccountLinkQuery	U2A	Y	yes, but no visibility
55	Settlement CSD	CSD Hold Settlement Instruction either on a Securities Account or on Behalf of the CSD in T2S	Object	Securities Account Party	SIC_CSDHI	Both	Y	Y
56	Billing Queries	Cumulative Billing Data List Query	Object	Party	BIQ_CumulativeBillDataListQuery	U2A	Y	Y
57	Billing Queries	Cumulative billing data query	Object	Party	BIQ_CumulativeBillDataDetailsQuery	Both	Y	Y
58	Static Data Queries	Currency Query	System	n/a	SDQ_CurrencyQuery	U2A	Y	Y
59	Scheduling Queries	Current Status of the T2S Settlement Day	System	n/a	SCQ_CurrStatusOfT2SSettlDay	Both	Y	Y
60	Dynamic Data Queries	Data Changes of a Business Object Details Query	System	n/a	DDQ_DataChan-BusinessObjDetailQue	U2A	Y	Y
61	Dynamic Data Queries	Data Changes of a Business Object List Query	System	n/a	DDQ_DataChan-BusinessObjListQuery	U2A	Y	Y
62	Scheduling Queries	Default Event Schedule Details Query	System	n/a	SCQ_DefaultEventSchedDetailsQuery	U2A	Y	Y
63	Market-Specific Configuration	Delete Attribute Domain	System	n/a	MSC_DeleteAttributeDomain	U2A	Y	N
64	Market-Specific Configuration	Delete Attribute Reference	System	n/a	MSC_DeleteAttributeReference	U2A	Y	N
65	Access Rights Management	Delete Certificate Distinguish Name	System	n/a	ARM_DeleteCertificateDN	U2A	Y	Y
66	Securities Account Data Manager	Delete CMB Securities Account Link	System	n/a	SAC_DeleteCMBSecuritiesAccountLink	U2A	Y	Y
67	Market-Specific Configuration	Delete Conditional Security Delivery Rule	System	n/a	MSC_DeleteConditSecurDelivRule	U2A	Y	N
68	Market-Specific Configuration	Delete Conditional Security Delivery Rule Set	System	n/a	MSC_DeleteConditSecurDelivRuleSet	U2A	Y	N
69	Securities Account Data Manager	Delete CSD Account Link	System	n/a	SAC_DeleteCSDAccountLink	U2A	Y	N
70	Security Data Management	Delete Eligible Counterpart CSD Link	System	n/a	SDM_DeleteEligibleCounterpCSDLink	U2A	Y	N
71	Market-Specific Configuration	Delete Market-Specific Attribute	System	n/a	MSC_DeleteMarket-SpecificAttribute	U2A	Y	N
72	Message Subscription	Delete Message Subscription Rule	System	n/a	MSU_DeleteMessageSubscriptionRule	U2A	Y	N
73	Message Subscription	Delete Message Subscription Rule Set	System	n/a	MSU_DeleteMessSubscriptionRuleSet	U2A	Y	N
74	Party Data Management	Delete Party	Object	Party	PDM_DeleteParty	Both	Y	Y
75	Report Configuration	Delete Report Configuration	System	n/a	RCO_DeleteReportConfiguration	U2A	Y	Y
76	Market-Specific Configuration	Delete Restriction Type	System	n/a	MSC_DeleteRestrictionType	U2A	Y	N
77	Market-Specific Configuration	Delete Restriction Type Rule	System	n/a	MSC_DeleteRestrictionTypeRule	U2A	Y	N
78	Access Rights Management	Delete Role	System	n/a	ARM_DeleteRole	U2A	Y	N

79	Network Configuration	Delete Routing	System	n/a	NCO_DeleteRouting	U2A	Y	Y
80	Access Rights Management	Delete Secured Group	System	n/a	ARM_DeleteSecuredGroup	U2A	Y	N
81	Securities Account Data Manager	Delete Securities Account	Object	Securities Account	SAC_DeleteSecuritiesAccount	Eoth	Y	Y
82	Security Data Management	Delete Security	Object	Security	SDM_DeleteSecurity	Eoth	Y	Y
83	Security Data Management	Delete Security CSD Link	System	n/a	SDM_DeleteSecurityCSDLink	U2A	Y	N
84	Network Configuration	Delete Technical Address Network Service Link	System	n/a	NCO_DeleteTechnAddressNetServLink	U2A	Y	N
85	Access Rights Management	Delete User	System	n/a	ARM_DeleteUser	U2A	Y	Y
86	Access Rights Management	Delete User Certificate Distinguish Name Link	System	n/a	ARM_DeleteUserCertificDNLink	U2A	Y	Y
87	Security Data Queries	Eligible Counterpart CSD Details Query	System	n/a	SEQ_EligibleCounterpCSDDetailsQuery	U2A	Y	yes, but no visibility
88	Security Data Queries	Eligible Counterpart CSD List Query	System	n/a	SEQ_EligibleCounterpCSD_istQuery	U2A	Y	yes, but no visibility
89	Scheduling Queries	Event Type Details Query	System	n/a	SCQ_EventTypeDetailsQuery	U2A	Y	Y
90	Scheduling Queries	Event Type List Query	System	n/a	SCQ_EventTypeListQuery	U2A	Y	Y
91	Access Rights Management	Grant privilege	System	n/a	ARM_GrantPrivilege	U2A	Y	Y
92	Access Rights Management	Grant/Revoke Role	System	n/a	ARM_GrantRole	U2A	Y	Y
93	Access Rights Queries	Granted Object Privileges List Query	System	n/a	ARQ_GrantObjectPrivilegesListQuery	U2A	Y	Y
94	Access Rights Queries	Granted Roles List Query	System	n/a	ARQ_GrantedRolesListQuery	U2A	Y	Y
95	Access Rights Queries	Granted System Privileges List Query	System	n/a	ARQ_GrantedSysPrivilegesListQuery	U2A	Y	Y
96	Settlement CSD	Hold Non-modifiable Instructions on behalf of the Instructing party of the Underlying Settlement Instruction	Object	Party	SIC_HNMBI	Eoth	Y	Y
97	Dynamic Data Queries	Hold/Release Instruction Audit Trail Details Query	Object	Securities Account	DDQ_HoldReleInstrAuditTrailDetQuery	U2A	Y	Y
98	Dynamic Data Queries	Hold/Release Instruction Audit Trail List Query	Object	Securities Account	DDQ_HoldReleInstrAuditTrailListQuery	U2A	Y	Y
99	Dynamic Data Queries	Inbound Files Details Query	System	n/a	DDQ_InboundFilesDetailsQuery	U2A	Y	Y
100	Dynamic Data Queries	Inbound Files List Query	System	n/a	DDQ_InboundFilesListQuery	U2A	Y	Y
101	Dynamic Data Queries	Inbound Message Details Query	System	n/a	DDQ_InboundMessDetailsQuery	U2A	Y	Y
102	Dynamic Data Queries	Inbound Message List Query	System	n/a	DDQ_InboundMessListQuery	U2A	Y	Y
103	Dynamic Data Queries	Intra-Position Movement Audit Trail Details Query	Object	Securities Account	DDQ_IntraPosMovAuditTrailDetQuery	U2A	Y	Y
104	Dynamic Data Queries	Intra-Position Movement Audit Trail List Query	Object	Securities Account	DDQ_IntraPosMovAuditTrailListQuery	U2A	Y	Y
105	Dynamic Data Queries	Intra-Position Movements Query	Object	Securities Account	DDQ_IntraPosMovQuery	Eoth	Y	Y
106	Security Data Queries	ISIN List Query	System	n/a	SEQ_ISINListQuery	Eoth	Y	Y
107	Billing Queries	Itemised Billing Data List Query	Object	Party	BIQ_ItemisedBillDataListQuery	U2A	Y	Y
108	Billing Queries	Itemised Billing Data Query	Object	Party	BIQ_ItemisedBillDataDetailsQuery	Eoth	Y	Y
109	T2S Dedicated Cash Account Dat	Limit Query	System	n/a	DCQ_LimitQuery	Eoth	Y	Y
110	Dynamic Data Queries	Limit Utilisation Journal Query	System	n/a	DDQ_LimitUtilisationJournalQuery	Eoth	Y	Y
111	Dynamic Data Queries	Limit Utilisation Query	System	n/a	DDQ_LimitUtilisationQuery	Eoth	Y	Y
112	Settlement General	Link to an Instruction/Pool Reference belonging to a specific Party	Object	Party	SIG_LIPRP	Eoth	Y	Y
113	Dynamic Data Queries	Maintenance for Intra-Position Movements and Settlement Instructions Query	Object	Securities Account	DDQ_MaintForIntraPosMov-SettlInstrQ	Eoth	Y	Y
114	MSA Data Queries	Market-Specific Attribute Detail Query	System	n/a	MSA_Market-SpecAttributeDetailQuery	U2A	Y	Y
115	MSA Data Queries	Market-Specific Attribute List Query	System	n/a	MSA_Market-SpecAttributeQuery	U2A	Y	Y
116	MSA Data Queries	Market-Specific Restriction List Query	System	n/a	MSA_Market-SpecRestrictListQuery	U2A	Y	Y
117	MSA Data Queries	Market-Specific Restriction Type Rule Detail Query	System	n/a	MSA_Market-SpecRestrictDetailQuery	U2A	Y	Y

118	MSA Data Queries	Market-Specific Restriction Type Rule Parameter Details Query	System	n/a	MSA_MarkSpecRestrTypeRuleParamDe	U2A	Y	Y
119	MSA Data Queries	Market-Specific Restriction Type Rule Set List Query	System	n/a	MSA_MarkSpecRestrTypeRuleSetListQu	U2A	Y	Y
120	Message Subscription Queries	Message Subscription Rule List Query	System	n/a	MSQ_MessSubscrRuleListQuery	U2A	Y	Y
121	Message Subscription Queries	Message Subscription Rule Set Details Query	System	n/a	MSQ_MessSubscrRuleSetDetailQuery	U2A	Y	Y
122	Message Subscription Queries	Message Subscription Rule Set List Query	System	n/a	MSQ_MessSubscrRuleSetListQuery	U2A	Y	Y
123	Network Configuration Queries	Network Service List Query	System	n/a	NCQ_NetworkServiceListquery	U2A	Y	Y
124	Message Management	New Broadcast	System	n/a	MMA_New Broadcast	U2A	Y	Y
125	Scheduling Queries	Operating Day Type Details Query	System	n/a	SCQ_OperatingDayTypeDetailsQuery	U2A	Y	N
126	Scheduling Queries	Operating Day Type List Query	System	n/a	SCQ_OperatingDayTypeListQuery	U2A	Y	N
127	Dynamic Data Queries	Outbound Files Details Query	System	n/a	DDQ_OutboundFilesDetailsQuery	U2A	Y	Y
128	Dynamic Data Queries	Outbound Files List Query	System	n/a	DDQ_OutboundFilesListQuery	U2A	Y	Y
129	Dynamic Data Queries	Outbound Message Details Query	System	n/a	DDQ_OutboundMessDetailsQuery	U2A	Y	Y
130	Dynamic Data Queries	Outbound Message List Query	System	n/a	DDQ_OutboundMessListQuery	U2A	Y	Y
131	Static Data Queries	Partial Settlement Threshold Query	System	n/a	SDQ_PartialSettlThresholdQuery	U2A	Y	Y
132	Party Data Queries	Party Audit Trail Query	Object	Party	PDQ_PartyAudTrailQuery	Both	Y	Y
133	Settlement General	Party Hold Settlement Instruction on a Securities Account or on Behalf of an external CSD	Object	Securities Account Party	SIG_PTYHI	Both	Y	Y
134	Party Data Queries	Party List Query	Object	Party	PDQ_PartyListQuery	Both	Y	Y
135	Party Data Queries	Party Reference Data Query	Object	Party	PDQ_PartyReferDataQuery	Both	Y	Y
136	Access Rights Queries	Privilege Query	System	n/a	ARQ_PrivilegeQuery	U2A	Y	Y
137	Settlement CSD	Release CoSD Hold Settlement Instruction on Behalf of an Administering Party	Object	Party	SIC_RCOSD	Both	Y	Y
138	Settlement CSD	Release CSD Hold Settlement Instruction either on a Securities Account or on Behalf of the CSD in T2S	Object	Securities Account Party	SIC_RCSDH	Both	Y	Y
139	Settlement CSD	Release CSD Validation Hold Settlement Instruction either on a Securities Account or on Behalf of the CSD in	Object	Securities Account Party	SIC_RCSDV	Both	Y	Y
140	Settlement CSD	Release Non-modifiable Instructions on behalf of the Instructing party of the Underlying Settlement Instruction	Object	Party	SIC_RNMBI	Both	Y	Y
141	Settlement General	Release Party Hold Settlement Instruction on a Securities Account or on Behalf of an external CSD	Object	Securities Account Party	SIG_RPTYH	Both	Y	Y
142	Report Configuration Queries	Report Configuration Details Query	System	n/a	RCO_ReportConfigDetailQuery	U2A	Y	Y
143	Report Configuration Queries	Report Configuration List Query	System	n/a	RCO_ReportConfigListQuery	U2A	Y	Y
144	Report Queries	Report Details Query	System	n/a	RCO_ReportDetailsQuery	Both	Y	Y
145	Report Queries	Report List Query	System	n/a	RCO_ReportListQuery	U2A	Y	Y
146	Message Management	Resend Communication	Object	Party	MMA_Resend Communication	Both	Y	Y
147	Static Data Queries	Residual Static Data Audit Trail Query	System	n/a	SDQ_ResidualStaticDataAudTrailQuery	U2A	Y	Y
148	Party Data Queries	Restricted Party Query	Object	Party	PDQ_RestrictedPartyQuery	Both	Y	Y
149	Access Rights Management	Revoke privilege	System	n/a	ARM_RevokePrivilege	U2A	Y	Y
150	Access Rights Queries	Role List Query	System	n/a	ARQ_RoleListQuery	U2A	Y	Y
151	Network Configuration Queries	Routing List Query	System	n/a	NCQ_RoutingListQuery	U2A	Y	Y
152	Access Rights Queries	Secured Group Details Query	System	n/a	ARQ_SecuredGroupDetailsQuery	U2A	Y	yes, but no visibility
153	Access Rights Queries	Secured Group List Query	System	n/a	ARQ_SecuredGroupListQuery	U2A	Y	yes, but no visibility
154	SAC Data Queries	Securities Account Audit Trail Query	Object	Securities Account	SAQ_SecuritiesAccAudTrailQuery	Both	Y	Y
155	SAC Data Queries	Securities Account List Query	Object	Party	SAQ_SecuritiesAccountListQuery	Both	Y	Y
156	Dynamic Data Queries	Securities Account Position Query	Object	Securities Account	DDQ_SecuritiesAccountPositionQuery	Both	Y	Y
157	SAC Data Queries	Securities Account Reference Data Query	Object	Securities Account	SAQ_SecuritiesAccReferenceDataQuery	Both	Y	Y

158	Security Data Queries	Securities Audit Trail Query	Object	Security	SEQ_SecuritiesAudTrailQuery	Both	Y	Y
159	Security Data Queries	Securities CSD Link Query	System	n/a	SEQ_SecuritiesCSDLinkQuery	Both	Y	yes, but no visibility
160	Security Data Queries	Securities Deviating Nominal Query	System	n/a	SEQ_SecuritiesDeviatNominQuery	Both	Y	Y
161	Dynamic Data Queries	Securities Position Detailed Restriction Details Query	Object	Securities Account	DDQ_SecurPosDetailedRestrDetailsQu	U2A	Y	Y
162	Dynamic Data Queries	Securities Posting Query	Object	Securities Account	DDQ_SecuritiesPostingQuery	U2A	Y	Y
163	Security Data Queries	Securities Reference Data Query	System	n/a	SEQ_SecuritiesReferDataQuery	Both	Y	Y
164	Settlement General	Send new instruction using a specific Instructing Party	Object	Party	SIG_SIUIP	Both	Y	Y
165	Settlement General	Send New Settlement Instruction/Settlement Restriction on Securities either on a Securities Account or on Behalf of an external CSD	Object	Securities Account Party	SIG_SNDSI	Both	Y	Y
166	Settlement CSD	Send Settlement Instruction with non-modifiable flag activated	System	n/a	SIC_SINMF	Both	Y	Y
167	Billing Queries	Service Item Details Query	System	n/a	BIQ_ServiceItemDetailsQuery	U2A	Y	Y
168	Billing Queries	Service Item List Query	System	n/a	BIQ_ServiceItemListQuery	U2A	Y	Y
169	Dynamic Data Queries	Settlement instruction audit trail query	Object	Securities Account	DDQ_SettlInstructAuditTrailQuery	Both	Y	Y
170	Dynamic Data Queries	Settlement Instruction Current Status Query	Object	Securities Account	DDQ_SettlInstructCurrentStatusQuery	Both	Y	Y
171	Dynamic Data Queries	Settlement Instruction Query	Object	Securities Account	DDQ_SettlInstructQuery	Both	Y	Y
172	Dynamic Data Queries	Settlement Instruction Status Audit Trail Query	Object	Securities Account	DDQ_SettlInstructStatusAuditTrailQu	Both	Y	Y
173	Static Data Queries	System Entity Query	System	n/a	SDQ_SystemEntityQuery	U2A	Y	Y
174	Network Configuration	T2S BIC Query	System	n/a	NCQ_T2SBICQuery	U2A	Y	Y
175	Scheduling Queries	T2S Calendar Query	System	n/a	SCQ_T2SCalendarQuery	Both	Y	Y
176	Scheduling Queries	T2S Diary Query	System	n/a	SCQ_T2SDiaryQuery	Both	Y	Y
177	Access Rights Queries	T2S System User Link Query	System	n/a	ARQ_UserCertifDNLinkQuery	U2A	Y	Y
178	Access Rights Queries	T2S System User Query (T2S Actor Query)	System	n/a	ARQ_T2SSysUserQueryT2SActorQuery	U2A	Y	Y
179	Network Configuration Queries	Technical Address Network Service Link Details Query	System	n/a	NCQ_DisplayTechAddressNetSerLink	U2A	Y	Y
180	Message Management	Third party receipt	Object	Party	MMA_Third party receipt	Both	Y	Y
181	Static Data Queries	Tolerance Amount Query	System	n/a	SDQ_ToleranceAmountQuery	U2A	Y	Y
182	Dynamic Data Queries	Total Collateral Value per T2S Dedicated Cash Account Query	System	n/a	DDQ_TotalCollatValuePerT2SDCAQuery	Both	Y	Y
183	Settlement CSD	Unblock CoSD Securities Blocking related to cancelled CoSD Settlement Instructions on Behalf of the relevant CSD in T2S	Object	Party	SIC_USBBI	Both	Y	Y
184	Market-Specific Configuration	Upcate Attribute Domain	System	n/a	MSC_UpdateAttributeDomain	U2A	Y	N
185	Market-Specific Configuration	Upcate Attribute Reference	System	n/a	MSC_UpdateAttributeReference	U2A	Y	N
186	Securities Account Data Manager	Upcate CMB Securities Account Link	System	n/a	SAC_UpdateCMBSecuritiesAccountLink	Both	Y	Y
187	Market-Specific Configuration	Upcate Conditional Security Delivery Rule	System	n/a	MSC_UpdateConditSecurDelivRule	U2A	Y	N
188	Market-Specific Configuration	Upcate Conditional Security Delivery Rule Set	System	n/a	MSC_UpdateConditSecurDelivRuleSet	U2A	Y	N
189	Securities Account Data Manager	Upcate CSD Account Link	System	n/a	SAC_UpdateCSDAccountLink	U2A	Y	N
190	Security Data Management	Upcate Eligible Counterpart CSD Link	System	n/a	SDM_UpdateEligibleCounterpCSDLink	U2A	Y	N

191	Market-Specific Configuration	Update Market-Specific Attribute	System	n/a	MSC_UpdateMarket-SpecificAttribute	U2A	Y	N
192	Message Subscription	Update Message Subscription Rule	System	n/a	MSU_UpdateMessageSubscriptionRule	U2A	Y	Y
193	Message Subscription	Update Message Subscription Rule Set	System	n/a	MSU_UpdateMessSubscriptionRuleSet	U2A	Y	Y
194	Party Data Management	Update Party	Object	Party	PDM_UpdateParty	Both	Y	Y
195	Report Configuration	Update Report Configuration	System	n/a	RCO_UpdateReportConfiguration	U2A	Y	Y
196	Market-Specific Configuration	Update Restriction Type	System	n/a	MSC_UpdateRestrictionType	U2A	Y	N
197	Market-Specific Configuration	Update Restriction Type Rule	System	n/a	MSC_UpdateRestrictionTypeRule	U2A	Y	N
198	Access Rights Management	Update Role	System	n/a	ARM_UpdateRole	U2A	Y	N
199	Network Configuration	Update Routing	System	n/a	NCO_UpdateRouting	U2A	Y	Y
200	Access Rights Management	Update Secured Group	System	n/a	ARM_UpdateSecuredGroup	U2A	Y	N
201	Securities Account Data Manager	Update Securities Account	Object	Securities Account	SAC_UpdateSecuritiesAccount	Both	Y	Y
202	Security Data Management	Update Security	Object	Security	SDM_UpdateSecurity	Both	Y	Y
203	Security Data Management	Update Security CSD Link	System	n/a	SDM_UpdateSecurityCSDLink	Both	Y	N
204	Network Configuration	Update Technical Address Network Service Link	System	n/a	NCO_UpdateTechnAddressNetServLink	U2A	Y	N
205	Access Rights Management	Update User	System	n/a	ARM_UpdateUser	U2A	Y	Y
206	Settlement ISO Codes	Use ISO transaction code AUTO (auto-collateralisation)	System	n/a	SII_UAUTO	Both	Y	Y
207	Settlement ISO Codes	Use ISO transaction code BSBK (buy sell back)	System	n/a	SII_UBSBK	Both	Y	Y
208	Settlement ISO Codes	Use ISO transaction code CLAI (market claim)	System	n/a	SII_UCLAI	Both	Y	Y
209	Settlement ISO Codes	Use ISO transaction code CNCB (central bank collateral operation)	System	n/a	SII_UCNCB	Both	Y	Y
210	Settlement ISO Codes	Use ISO transaction code COLI (collateral in)	System	n/a	SII_UCOLI	Both	Y	Y
211	Settlement ISO Codes	Use ISO transaction code COLO (collateral out)	System	n/a	SII_UCOLO	Both	Y	Y
212	Settlement ISO Codes	Use ISO transaction code CONV (depository receipt conversion)	System	n/a	SII_UCONV	Both	Y	Y
213	Settlement ISO Codes	Use ISO transaction code CORP (corporate action)	System	n/a	SII_UCORP	Both	Y	Y
214	Settlement ISO Codes	Use ISO transaction code ETFT (exchange traded funds)	System	n/a	SII_UETFT	Both	Y	Y
215	Settlement ISO Codes	Use ISO transaction code FCTA (factor update)	System	n/a	SII_UFCTA	Both	Y	Y
216	Settlement ISO Codes	Use ISO transaction code INSP (move of stock)	System	n/a	SII_UINSP	Both	Y	Y
217	Settlement ISO Codes	Use ISO transaction code ISSU (Issuance)	System	n/a	SII_UISSU	Both	Y	Y
218	Settlement ISO Codes	Use ISO transaction code MKDW (mark down)	System	n/a	SII_UMKDW	Both	Y	Y
219	Settlement ISO Codes	Use ISO transaction code MKUP (mark up)	System	n/a	SII_UMKUP	Both	Y	Y
220	Settlement ISO Codes	Use ISO transaction code NETT (netting)	System	n/a	SII_UNETT	Both	Y	Y
221	Settlement ISO Codes	Use ISO transaction code NSYN (non syndicated)	System	n/a	SII_UNSYN	Both	Y	Y
222	Settlement ISO Codes	Use ISO transaction code OWNE (external account transfer)	System	n/a	SII_UOWNE	Both	Y	Y
223	Settlement ISO Codes	Use ISO transaction code OWNI (internal account transfer)	System	n/a	SII_UOWNI	Both	Y	Y
224	Settlement ISO Codes	Use ISO transaction code PAIR (pair off)	System	n/a	SII_UPAIR	Both	Y	Y
225	Settlement ISO Codes	Use ISO transaction code PLAC (placement)	System	n/a	SII_UPLAC	Both	Y	Y
226	Settlement ISO Codes	Use ISO transaction code PORT (portfoliomove)	System	n/a	SII_UPORT	Both	Y	Y
227	Settlement ISO Codes	Use ISO transaction code REAL (realignment)	System	n/a	SII_UREAL	Both	Y	Y
228	Settlement ISO Codes	Use ISO transaction code REDI (withdrawal)	System	n/a	SII_UREDI	Both	Y	Y
229	Settlement ISO Codes	Use ISO transaction code REDM (redemption)	System	n/a	SII_UREDM	Both	Y	Y

230	Settlement ISO Codes	Use ISO transaction code RELE (depository receipt release cancellation)	System	n/a	SII_URELE	Both	Y	Y
231	Settlement ISO Codes	Use ISO transaction code REPU (repo)	System	n/a	SII_UREPU	Both	Y	Y
232	Settlement ISO Codes	Use ISO transaction code RODE (return delivery without matching)	System	n/a	SII_URODE	Both	Y	Y
233	Settlement ISO Codes	Use ISO transaction code RVPO (reverse repo)	System	n/a	SII_URVPO	Both	Y	Y
234	Settlement ISO Codes	Use ISO transaction code SBBK (sell buy back)	System	n/a	SII_USBBK	Both	Y	Y
235	Settlement ISO Codes	Use ISO transaction code SBRE (borrowing reallocation)	System	n/a	SII_USBRE	Both	Y	Y
236	Settlement ISO Codes	Use ISO transaction code SECB (securities borrowing)	System	n/a	SII_USECB	Both	Y	Y
237	Settlement ISO Codes	Use ISO transaction code SECL (securities lending)	System	n/a	SII_USECL	Both	Y	Y
238	Settlement ISO Codes	Use ISO transaction code SLRE (lending reallocation)	System	n/a	SII_USLRE	Both	Y	Y
239	Settlement ISO Codes	Use ISO transaction code SUBS (subscription)	System	n/a	SII_USUBS	Both	Y	Y
240	Settlement ISO Codes	Use ISO transaction code SYND (syndicate underwriters)	System	n/a	SII_USYND	Both	Y	Y
241	Settlement ISO Codes	Use ISO transaction code TBAC (TBA closing)	System	n/a	SII_UTBAC	Both	Y	Y
242	Settlement ISO Codes	Use ISO transaction code TRAD (trade)	System	n/a	SII_UTRAD	Both	Y	Y
243	Settlement ISO Codes	Use ISO transaction code TRPO (triparty repo)	System	n/a	SII_UTRPO	Both	Y	Y
244	Settlement ISO Codes	Use ISO transaction code TRVO (triparty reverse repo)	System	n/a	SII_UTRVO	Both	Y	Y
245	Settlement ISO Codes	Use ISO transaction code TURN (turnaround)	System	n/a	SII_UTURN	Both	Y	Y

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone.: + 32 (0)2 221 22 17
sss@nbb.be

Annex 24

General Information		
Request raised by:		**Date raised:** DD/MM/YYYY (*to be filled in by NBB-SSS*
Request title:		**Request ref. no:** (*to be filled in by NBB-SSS*)
Request type: Common CR		**Urgency:** (Normal, Fast-track) (*to be filled in by NBB-SSS*)
1. Legal/business importance parameter: (H, M, L)		**2. Market implementation efforts parameter:** (H, M, L)
3. Operational/Technical risk parameter: (H, M, L)		**4. Financial impact parameter:** (H, M, L) (*to be filled in by NBB-SSS*)
Requestor Category: (NBB-SSS, NBB, Participant)		**Status:** (Registered, Under Preliminary assessment, Pending with CRG…) (*to be filled in by NBB-SSS*)

Reason for change and expected benefits/business motivation:

Description of requested change:

Related documents:

Proposed wording for the Change request:

High level description of Impact:

Outcome/Decisions:

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

Annex 25

TRADE ABC BETWEEN TWO N ACCOUNTS: 1 IN NBB-SSS (BUYER) 1 IN INVESTOR CSD

General procedure:
If a transaction is using a investor CSD N-account, NBB-SSS will create an unmatched WT inx between Belgian Debt Agency and Investor CSD participant, linked "Info" with the REAL instruction and placed on CSDHold. The REAL instruction will remain blocked (CVAL) until the WTX instruction(s) has (have) been matched. The moment (any) settlement of the REAL takes place, the CSD Hold on the WTX is lifted so the WTX transaction can settle.

The procedure is described in detail hereafter.

1) Detectable in NBB-SSS :
- 1 a) Instruction BUY of the NBB-SSS participant (buyer)
- 1 b) REAL instruction (already matched) between an omnibus N-account and N-account NBB-SSS participant

2) T2S-rule sets this REAL instruction on CVAL

Ramses creates unmatched 3a) WTXinx1 to
- debet seller[1] with WTX (DCA blanc) and
- credit NBBEBEBBWTX - SPF FINANCES - FOD FINANCIEN)

3b) WTX inx1 is linked INFO to REAL
3c) WTX inx1 i on CSDHold

Ramses creates already matched 4a) WTXinx2 to
- credit buyer with WTX and
- debet NBBEBEBBWTX - SPF FINANCES - FOD FINANCIEN)

4b) WTX inx2 is linked AFTE with inx BUY

5) seller / or seller's CSD receives allegement of WTXinx1

6) seller / or seller's CSD matches WTX instruction with PFOD (containing DCA of seller)

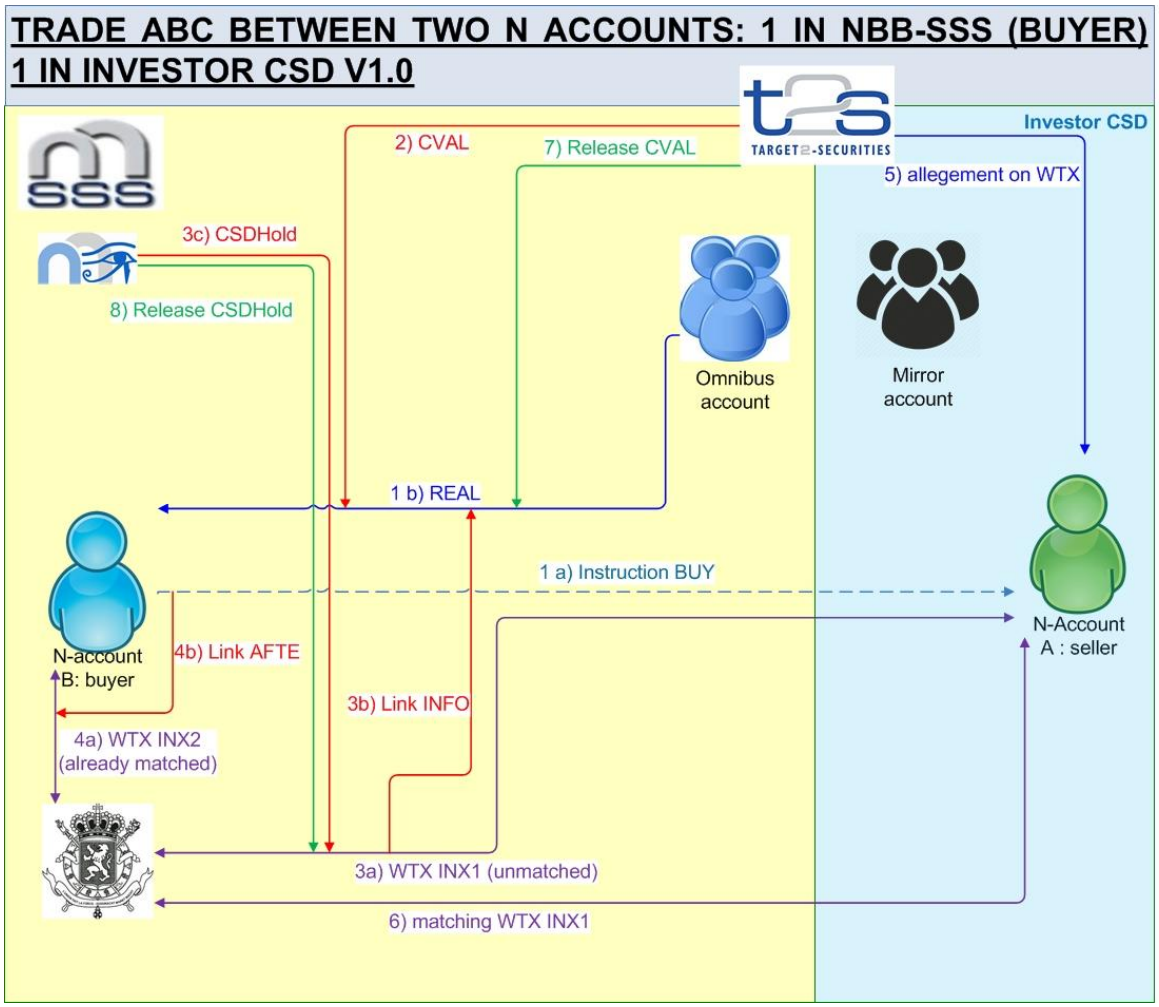
7) On matching of this WTX inx the REAL CVAL is released.

If the REAL settles completely[2]:
- 8) Ramses removes the CSDHold on the WTXinx2
- If the WT doesn't settle:
  - fine to CSD seller

If the transaction + REAL is canceled
- WTXinx2 is cancelled automatically with underlying transaction's cancelation
- CSDHold remains
- Ramses cancels the NBB-SSS part of the WTXinx1 (unmatched)
- seller receives allegement of cancelation of WTXinx1

[1] Deducted from inx BUY
[2] partial settlement is not possible, as partialling is not possible on linked inx (and inx BUY is linked with WT inx2)

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be



TRADE GHI BETWEEN TWO N ACCOUNTS: 1 IN NBB-SSS (SELLER) 1 IN INVESTOR CSD

1) Detectable in NBB-SSS :

- 1 a) An instruction SELL of the NBB-SSS participant (seller)
- 1 b) A REAL instruction (already matched) between an omnibus N-account and N-account NBB-SSS participant

2) A T2S-rule sets this REAL instruction on CVAL

Ramses creates already matched 3a) WTXinx1 to

- debet seller with WTX (DCA of seller) and
- credit NBBEBEBBWTX - SPF FINANCES - FOD FINANCIEN)

3b) WTX instruction 1 is

- linked AFTE with inx SELL

Ramses creates unmatched 4a) WTXinx2 to

- credit buyer CSD with WTX (DCA blanc) and
- debet NBBEBEBBWTX - SPF FINANCES - FOD FINANCIEN)
- 4b) linked INFO to REAL
- 4c) on CSDHold

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

5) buyer or buyer's CSD receives allegement of WTXinx2

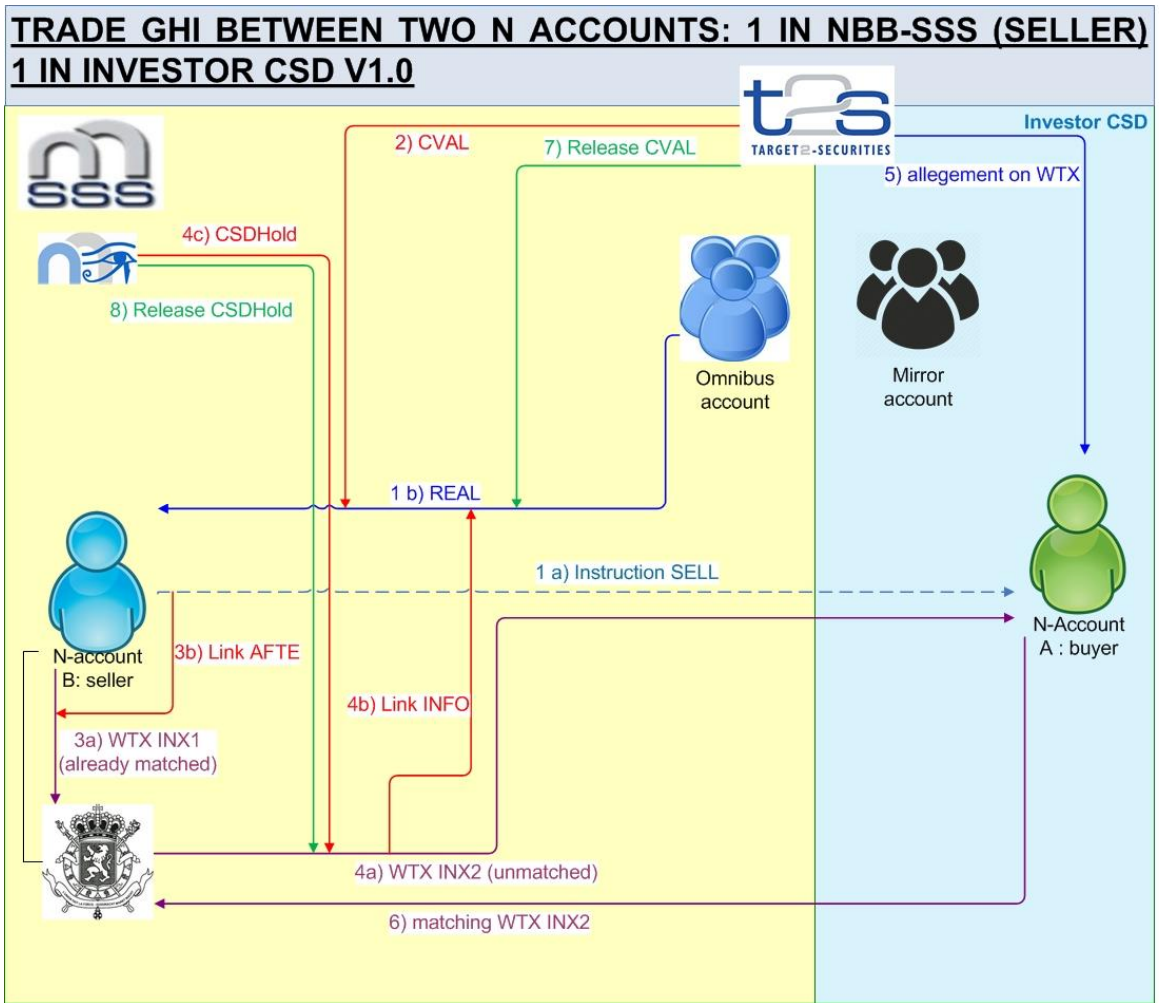
6) buyer or the buyer's CSD matches WTX instruction with PFOD containing DCA of participant buyer

7) On matching of this WTX inx the REAL CVAL is released.

If the REAL settles completely[3]:
8) Ramses removes the CSDHold on the WTXinx

If the REAL is canceled

- CSDHold remains
- Ramses cancels WTXinx1 completely
- Ramses cancels the NBB-SSS part of the WTXinx2
- CSD buyer receives allegement of cancelation of WTXinx2



[3] partial settlement is not possible, as partialling is not possible on linked inx (and inx sell is linked with WT inx2)

NBB - Payments and Securities Service
Securities settlement system
boulevard de Berlaimont 14
BE-1000 Brussels
Phone: + 32 (0)2 221 22 17
sss@nbb.be

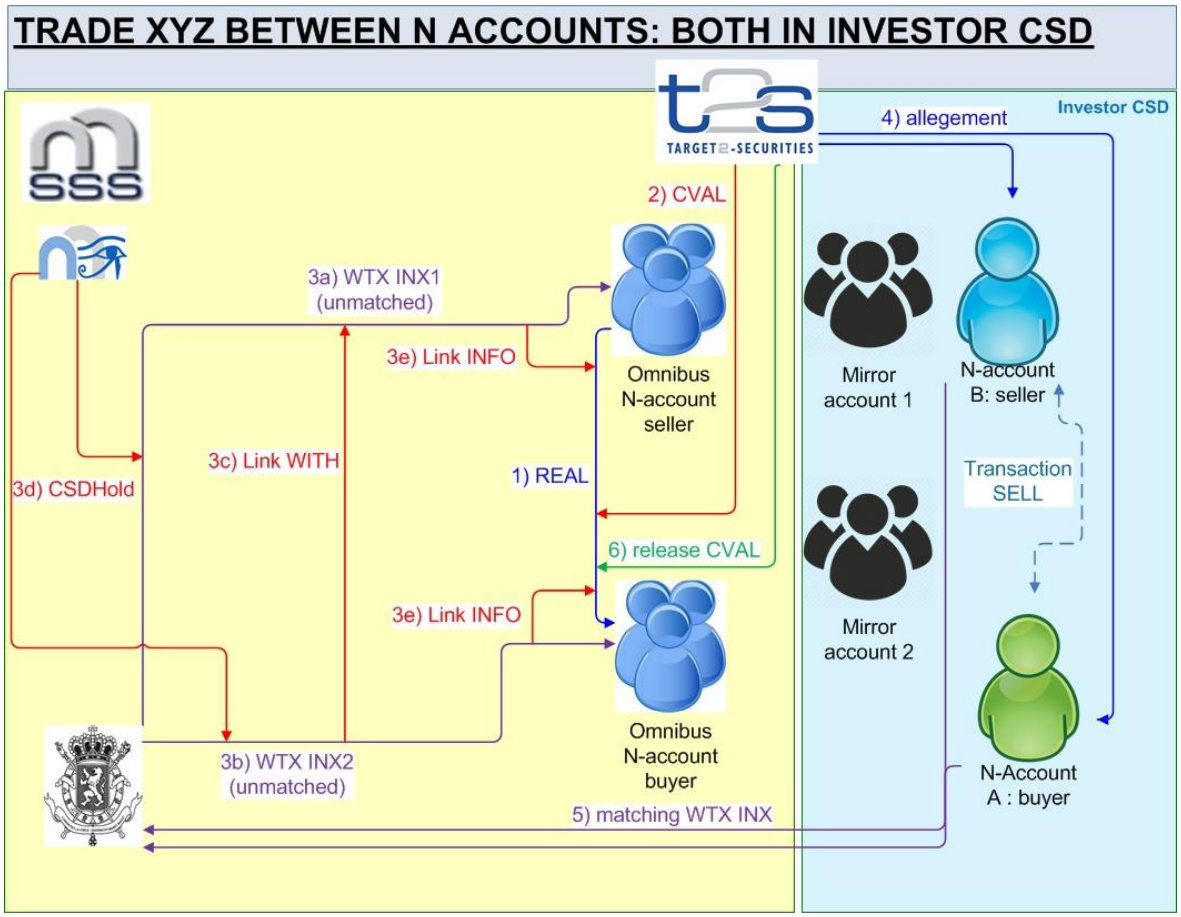
Annex 25

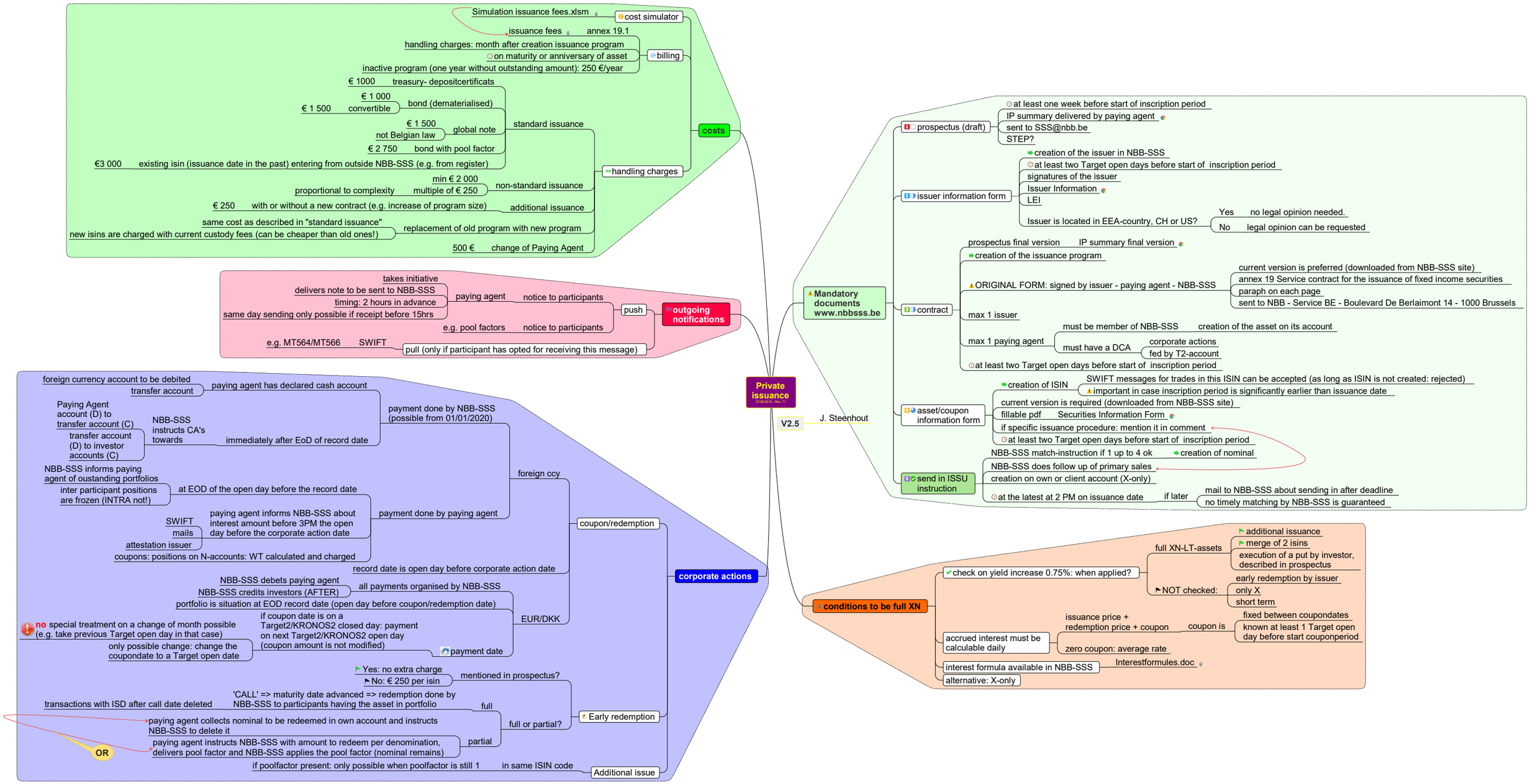
TRADE XYZ BETWEEN TWO INVESTOR CSD N ACCOUNTS: 1 IN EF (SELLER) 1 IN EF CLIENT (BUYER)

Detectable in NBB-SSS :
1) REAL instruction (already matched) between two omnibus N-accounts.
NO information on buyer
NO information on seller

2) A T2S-rule sets this REAL instruction on CVAL
3a) Create unmatched WTX inx between BDA and investor CSD seller
3b) Create unmatched WTX inx between BDA and investor CSD buyer
3c) Both inx linked 'with'
3d) Both inx on CSD hold
3e) Both inx linked 'info' to real.
4) Investor CSD (or its participants) get allegement
5) Investor CSD (or its participants) match the WTX instructions
6) release CVAL of REAL
IF REAL settles (even partially): remove CSD hold
IF REAL is cancelled:

- CSDHold remains
- Ramses cancels the NBB-SSS part of the WTXinx1
- Ramses cancels the NBB-SSS part of the WTXinx2
- CSD participants receive allegement of cancelation of WTXinxs





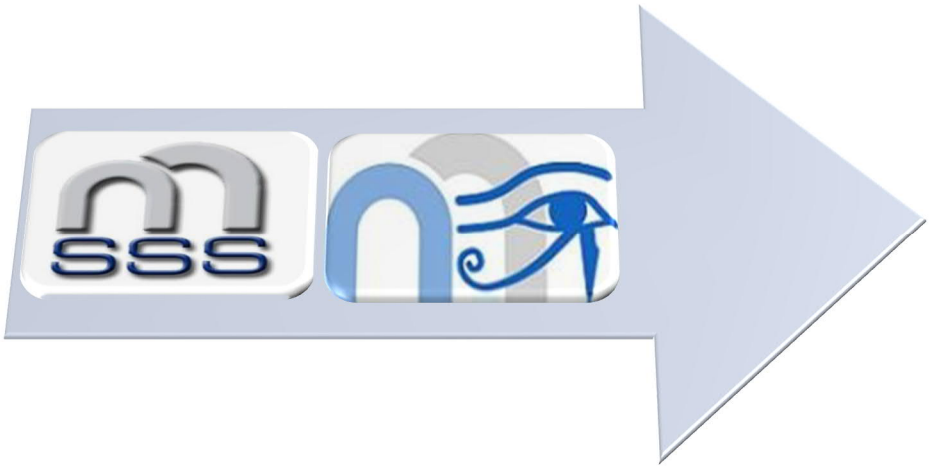
Private issuance
V2.5
J. Steenhout
Mandatory documents www.nbbsss.be
prospectus (draft)
at least one week before start of inscription period
IP summary delivered by paying agent
sent to SSS@nbb.be
STEP?
issuer information form
creation of the issuer in NBB-SSS
at least two Target open days before start of inscription period
signatures of the issuer
Issuer Information
LEI
Issuer is located in EEA-country, CH or US?
Yes
no legal opinion needed.
No
legal opinion can be requested
contract
prospectus final version
IP summary final version
creation of the issuance program
ORIGINAL FORM: signed by issuer - paying agent - NBB-SSS
current version is preferred (downloaded from NBB-SSS site)
annex 19 Service contract for the issuance of fixed income securities
paraph on each page
sent to NBB - Service BE - Boulevard De Berlaimont 14 - 1000 Brussels
max 1 issuer
max 1 paying agent
must be member of NBB-SSS
creation of the asset on its account
must have a DCA
corporate actions
fed by T2-account
at least two Target open days before start of inscription period
asset/coupon information form
creation of ISIN
SWIFT messages for trades in this ISIN can be accepted (as long as ISIN is not created: rejected)
important in case inscription period is significantly earlier than issuance date
current version is required (downloaded from NBB-SSS site)
fillable pdf
Securities Information Form
if specific issuance procedure: mention it in comment
at least two Target open days before start of inscription period
send in ISSU instruction
NBB-SSS match-instruction if 1 up to 4 ok
creation of nominal
NBB-SSS does follow up of primary sales
creation on own or client account (X-only)
at the latest at 2 PM on issuance date
if later
mail to NBB-SSS about sending in after deadline
no timely matching by NBB-SSS is guaranteed
conditions to be full XN
check on yield increase 0.75%: when applied?
full XN-LT-assets
additional issuance
merge of 2 isins
execution of a put by investor, described in prospectus
NOT checked:
early redemption by issuer
only X
short term
accrued interest must be calculable daily
issuance price + redemption price + coupon
coupon is
fixed between coupondates
known at least 1 Target open day before start couponperiod
zero coupon: average rate
interest formula available in NBB-SSS
Interestformules.doc
alternative: X-only
costs
cost simulator
Simulation issuance fees.xlsm
issuance fees
annex 19.1
billing
handling charges: month after creation issuance program
on maturity or anniversary of asset
inactive program (one year without outstanding amount): 250 €/year
handling charges
standard issuance
€ 1000
treasury- depositcertificats
€ 1 000
bond (dematerialised)
€ 1 500
convertible
€ 1 500
global note
not Belgian law
€ 2 750
bond with pool factor
€3 000
existing isin (issuance date in the past) entering from outside NBB-SSS (e.g. from register)
non-standard issuance
min € 2 000
multiple of € 250
proportional to complexity
additional issuance
€ 250
with or without a new contract (e.g. increase of program size)
replacement of old program with new program
same cost as described in "standard issuance"
new isins are charged with current custody fees (can be cheaper than old ones!)
500 €
change of Paying Agent
outgoing notifications
push
paying agent
notice to participants
takes initiative
delivers note to be sent to NBB-SSS
timing: 2 hours in advance
same day sending only possible if receipt before 15hrs
e.g. pool factors
notice to participants
pull (only if participant has opted for receiving this message)
e.g. MT564/MT566
SWIFT
corporate actions
coupon/redemption
foreign ccy
payment done by NBB-SSS (possible from 01/01/2020)
paying agent has declared cash account
transfer account
NBB-SSS instructs CA's towards
Paying Agent account (D) to transfer account (C)
transfer account (D) to investor accounts (C)
immediately after EoD of record date
payment done by paying agent
at EOD of the open day before the record date
NBB-SSS informs paying agent of oustanding portfolios
inter participant positions are frozen (INTRA not!)
paying agent informs NBB-SSS about interest amount before 3PM the open day before the corporate action date
SWIFT
mails
attestation issuer
coupons: positions on N-accounts: WT calculated and charged
record date is open day before corporate action date
EUR/DKK
all payments organised by NBB-SSS
NBB-SSS debets paying agent
NBB-SSS credits investors (AFTER)
portfolio is situation at EOD record date (open day before coupon/redemption date)
payment date
if coupon date is on a Target2/KRONOS2 closed day: payment on next Target2/KRONOS2 open day (coupon amount is not modified)
only possible change: change the coupondate to a Target open date
no special treatment on a change of month possible (e.g. take previous Target open day in that case)
Early redemption
mentioned in prospectus?
Yes: no extra charge
No: € 250 per isin
full or partial?
full
'CALL' => maturity date advanced => redemption done by NBB-SSS to participants having the asset in portfolio
transactions with ISD after call date deleted
partial
paying agent collects nominal to be redeemed in own account and instructs NBB-SSS to delete it
paying agent instructs NBB-SSS with amount to redeem per denomination, delivers pool factor and NBB-SSS applies the pool factor (nominal remains)
OR
Additional issue
in same ISIN code
if poolfactor present: only possible when poolfactor is still 1

National Bank of Belgium - Securities Settlement System

NBB - SSS

Banque Nationale Bank
DE BELGIQUE VAN BELGIË
Eurosystem

Foreign currencies:
DVP Transactions and Corporate Actions
End user Manual



June 2020

V2.1

Table of content

1 Introduction 4

1.1 Eligible Foreign currencies 4

1.1.1 For DVP transactions 4

1.1.2 For Corporate actions 4

1.2 FOP with cash part 4

1.3 Different process Foreign currency cash Transactions (DVP in Foreign currency) / Corporate actions 5

1.3.1 DVP in Foreign currency vs DVP in T2S settlement currency 5

1.3.2 Corporate actions in Foreign currency vs corporate actions in T2S settlement currency 5

1.4 UETR 7

2 Methods 8

2.1 DVP Transaction in Foreign currency 8

2.2 Corporate Action in Foreign currency 12

2.2.1 Corporate action payments via a Paying Agent's Dedicated Transfer Account (DTA) – Standard Procedure 12

2.2.2 Corporate action payments without the use of a Dedicated Transfer Account (DTA) – Exceptional procedure upon Paying Agent's request 19

2.2.3 Pros and Cons of usage of DTA versus no DTA 26

3 Reconciliation across messages 27

3.1 DVP Transaction in Foreign currency 27

3.2 Corporate action (CA) in Foreign currency 31

3.2.1 With a Dedicated Transfer Account (DTA) 31

3.2.2 Without Dedicated Transfer account 40

4 Actions required from the Participant 47

4.1 Declaring Foreign Currency Cash account (FCA) and Dedicated Transfer Account (DTA) 47

4.2 Foreign currency cash Provider and Foreign currency cash account at different levels 48

4.3 Corporate actions 48

4.3.1 Unique reference ASRF 48

4.3.2 Generation of Corporate actions on Record Date 48

4.4 End of Day functions 50

4.4.1 Cash Forecast 50
4.5 Administrative fines 51
4.5.1 Timing 51
4.5.2 MONY 51
4.5.3 LACK 51
5 Annexes 52
5.1 Annex 1 – currencies of which exchange rates are published by the ECB 52
5.2 Annex 2 – ASRF compilation 52
5.3 Annex 3 - Overview of used swift messages: equivalent MT vs MX 53
5.4 Annex 4 - Examples 54
5.4.1 DVP in foreign Currencies 54
5.4.2 Corporate actions in Foreign currency (with transferaccount DTA) 91
5.4.3 Corporate actions in Foreign currency (without transferaccount) 97
5.4.3

Version Control

Version	Date	Author	Distribution	Modifications
2.1	03/01/2020	Steenhout J	all	If buyer/seller – Paying agent/investor (in scenario of CA without DTA) have defined the same FCA, there is no MT202 created, hence no UETR in MT566.
				MT564 will not contain ASRF or UETR
				WT inx will not contain ASRF but refer to CMONID of the transaction it's linked AFTER
				SESE.023 in case of a redemption, will in first stage not mention the cash amount.
				Textual changes

1 Introduction

The current End user Manual describes the procedure followed by the NBB-SSS when providing the Foreign currency financial service in accordance with the Terms and Conditions governing the participation in the NBB-SSS. This Manual is intended for:

- DVP transactions in Foreign currencies
- Corporate actions in Foreign currencies if the Issuer or the Paying Agent opts for the NBB-SSS' Foreign currency financial service.

The NBB-SSS shall support the settlement of the cash leg in a Foreign currency relating to securities denominated in Foreign currencies registered in the NBB-SSS from Q2 2020 onwards.

This manual will mainly refer to the currently most common messages, being the MT or ISO15022 messages. In case the MX equivalent should be needed, reference is made towards Annex 3, where the comparison between MT and MX messages is listed out.

1.1 Eligible Foreign currencies

1.1.1 For DVP transactions

Foreign currencies for which the ECB publishes the exchange rate are eligible. They are listed in annex 1.1.

1.1.2 For Corporate actions

Foreign currencies for which the ECB publishes the exchange rate and which are supported by the Paying Agent's Foreign currency cash Provider are eligible for Corporate actions.

1.2 FOP with cash part

The DVP instructions in Foreign currency are sent to T2S as FOP with 3 cash fields in the cash part:

- Currency
- Cash amount
- Debit/credit

T2S treats these cash fields as additional matching fields. This means that, if one participant communicates the cash fields, they must be filled out as well by the counterparty. The currency and the field debit/credit must correspond in both instructions. The amounts can be slightly different, depending on the allowed tolerance amounts for each currency. These tolerance amounts are determined yearly by T2S.

If these fields do not match, the instructions will not match and there is no transaction.

1.3 Different process Foreign currency cash Transactions (DVP in Foreign currency) / Corporate actions

1.3.1 DVP in Foreign currency vs DVP in T2S settlement currency

DVP (delivery versus payment) transactions in Foreign currency do not follow the same process as DVP transactions in T2S settlement currencies. The cash debits and credits for DVP transactions in T2S settlement currencies are executed on the Participants' DCAs (Dedicated Cash Accounts). In case of DVP transactions in Foreign currencies, cash debits and credits entailed by the settlement in the NBB-SSS of securities transactions denominated in Foreign currencies are registered on the Participant's Foreign currency Cash Account (FCA) (see Article 4.3 of the NBB-SSS Terms and Conditions).

1.3.2 Corporate actions in Foreign currency vs corporate actions in T2S settlement currency

Corporate actions in T2S settlement currencies are executed on the T2S platform through Payment Free of Deliveries (PFODs) or, in case of redemption, DVP transactions. All these transactions are instructed between the paying agent/investor's DCA on one side and NBB-SSS' Dedicated Transfer account on the other.

Corporate actions in Foreign currencies shall be executed on the FCA and on the Dedicated Transfer Account (DTA) of the Participants acting as Paying agent and on the FCA of the Participants having a position in the relevant securities. All accounts are declared and maintained in the NBB-SSS application Ramses.

1.3.2.1 Redemption

- Paying Agent:
  - T2S settlement currencies:
    - PFOD (Payment free of delivery) between Paying Agent's account and issuance account
    - MT564
    - MT566/seev.036
  - Foreign currencies without NBB-SSS Foreign currency financial services:
    - Nothing (a FOP with 0 nominal and cash is not allowed in T2S)
    - MT564
    - MT566
    - Extra frozen day before redemption date
  - Foreign currencies with NBB-SSS Foreign currency financial services:
    - Nothing (a FOP with 0 nominal and cash is not allowed in T2S)
    - MT564
    - MT566
- Investor:
  - T2S settlement currencies:
    - DVP between investor's account (DELI) and issuance account
    - MT564
    - MT566

- Foreign currencies without NBB-SSS Foreign currency financial services:
  - FOP DELI with the nominal position of the investor
  - MT564
  - MT566
  - Extra frozen day before redemption date

- Foreign currencies with NBB-SSS Foreign currency financial services:
  - FOP DELI with the nominal position of the investor and cash
  - MT564
  - MT566

1.3.2.2 Coupon/poolfactor

- Paying Agent:
  - T2S settlement currencies:
    - PFOD (Payment free of delivery) between Paying Agent's account and issuance account
    - MT564
    - MT566

  - Foreign currencies without NBB-SSS Foreign currency financial services:
    - Nothing (a FOP with 0 nominal and cash is not allowed in T2S)
    - MT564
    - Extra frozen day before Corporate action date

  - Foreign currencies with NBB-SSS Foreign currency financial services:
    - Nothing (a FOP with 0 nominal and cash is not allowed in T2S)
    - MT564
    - MT566

- Investor
  - T2S settlement currencies:
    - PFOD (Payment free of delivery) between investor's account (DELI) and issuance account
    - MT564
    - MT566

  - Foreign currencies without NBB-SSS Foreign currency financial services:
    - Nothing (a FOP with 0 nominal and cash is not allowed in T2S)
    - MT564
    - Extra frozen day before Corporate action date

  - Foreign currencies with NBB-SSS Foreign currency financial services:
    - Nothing (a FOP with 0 nominal and cash is not allowed in T2S)
    - MT564
    - MT566

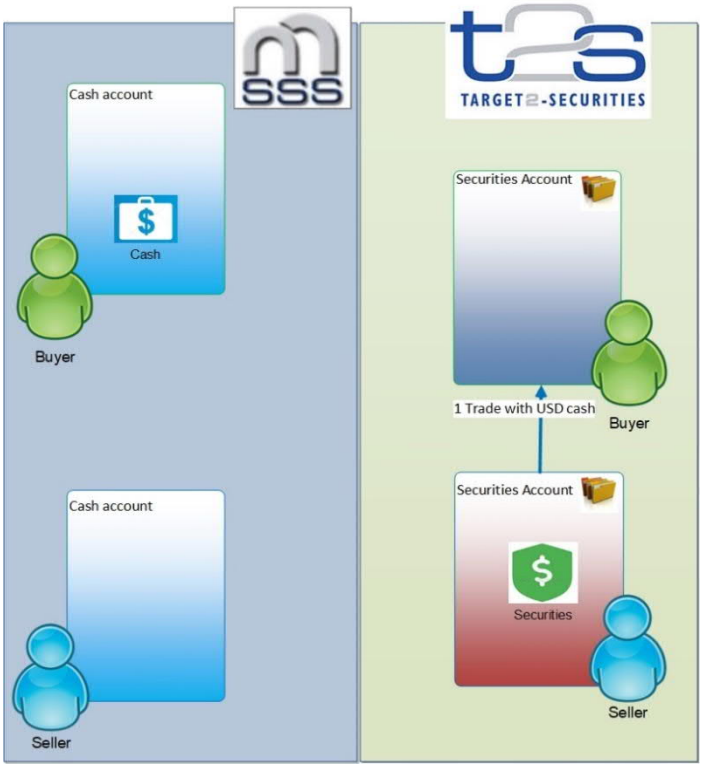
1.4 UETR

The unique end-to-end transaction reference (UETR) is a reference in the SWIFT GPI initiative that allows the user to track a payment from debited to credited party over the SWIFT network. NBB-SSS will implement the UETR code in messages where possible. As this specificity was added to the project at a later stage, some of the UETR implementations may not be active as from to go live in Q2 2020. They will be delivered on best effort basis and, when absent, may be added at a later stage.

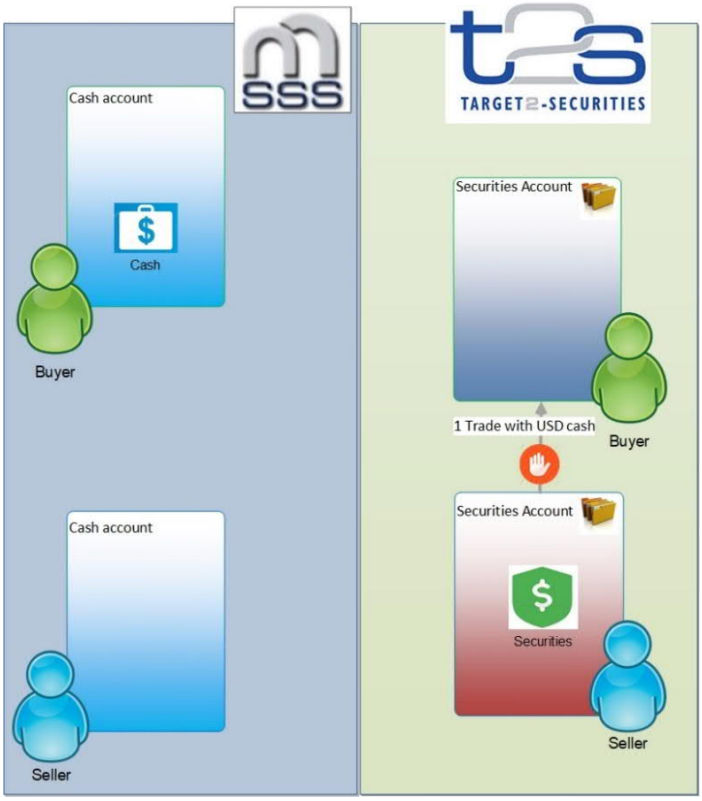
2 Methods

2.1 DVP Transaction in Foreign currency

1. The system detects a trade with Foreign currency cash amount.



An automated rule will immediately set the trade on hold.



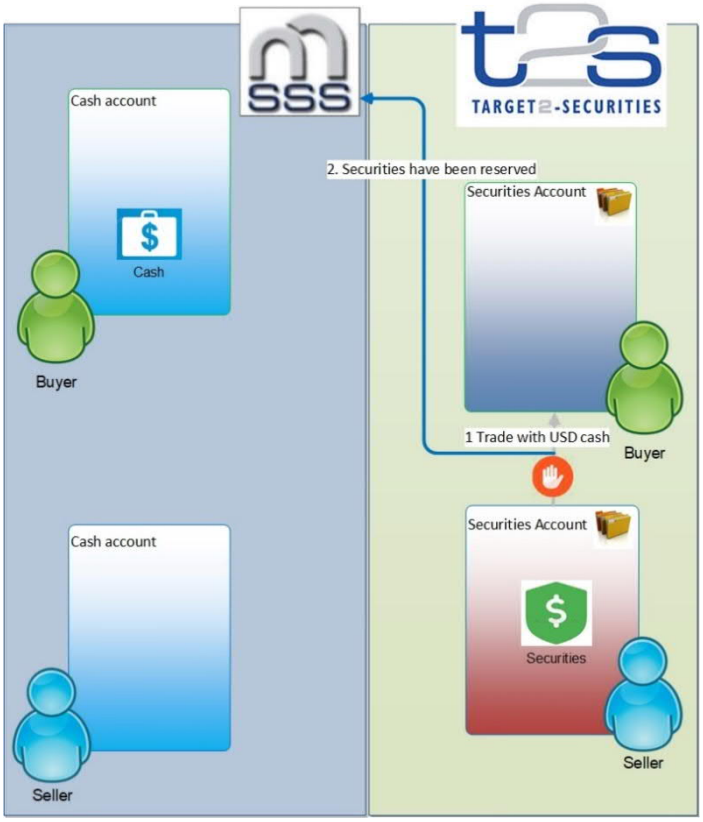
If the instruction is in a Foreign currency that is not accepted by T2S, T2S rejects it immediately.

Ifthe transaction is not eligible for FCA treatment, it is released immediately.

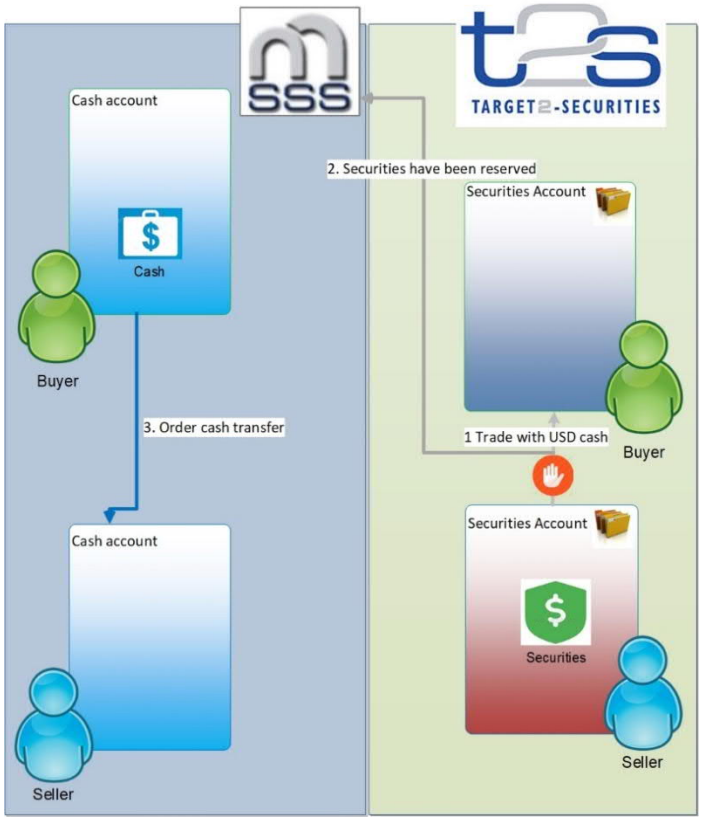
Reasons for non-eligibility:

- The FCA of the buyer and the seller are the same.
- The currency is a T2S currency

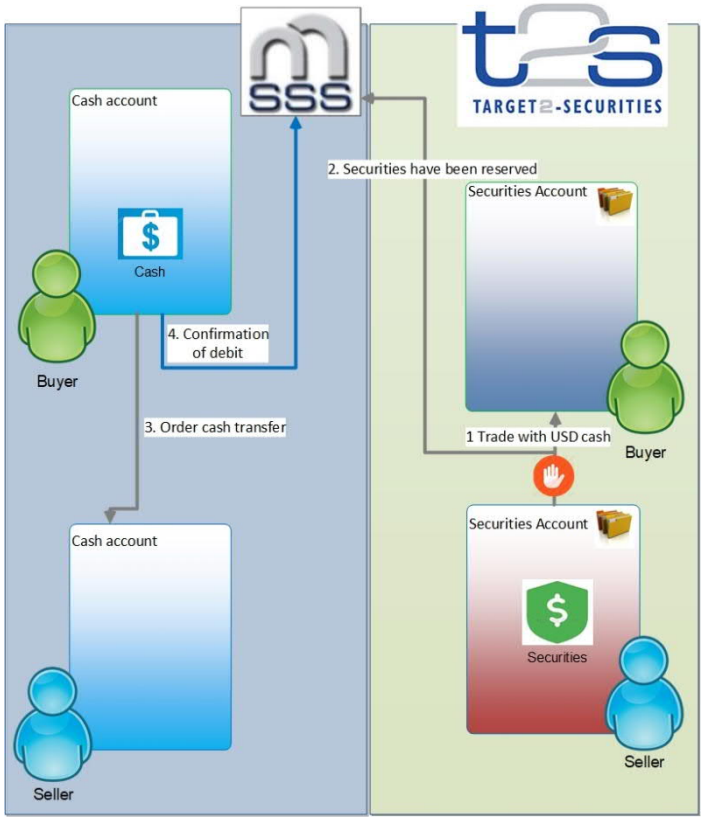
2. T2S informs NBB-SSS when the position has been reserved.



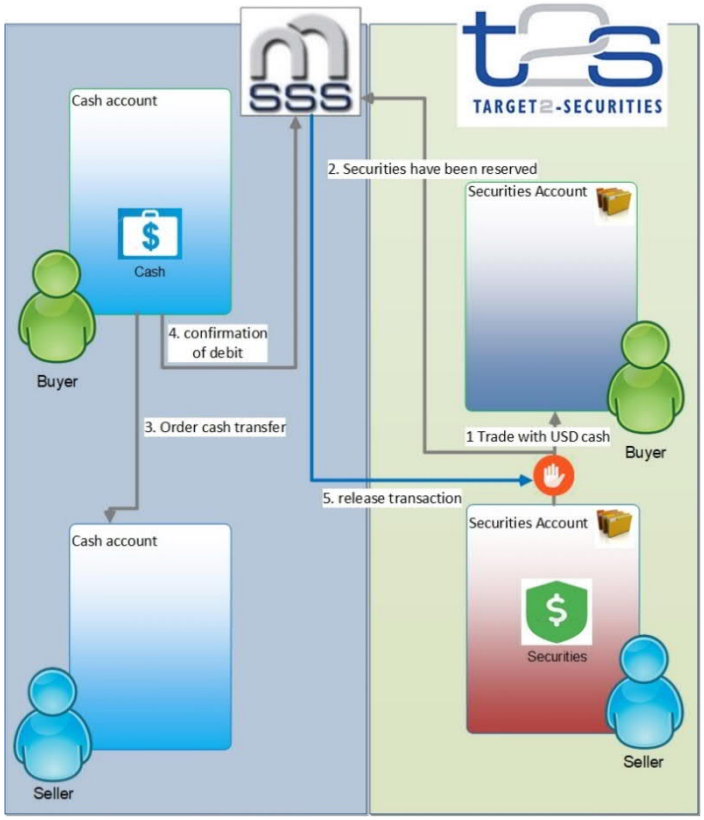
3. NBB-SSS instructs the debit of the buyer's FCA (MT202)



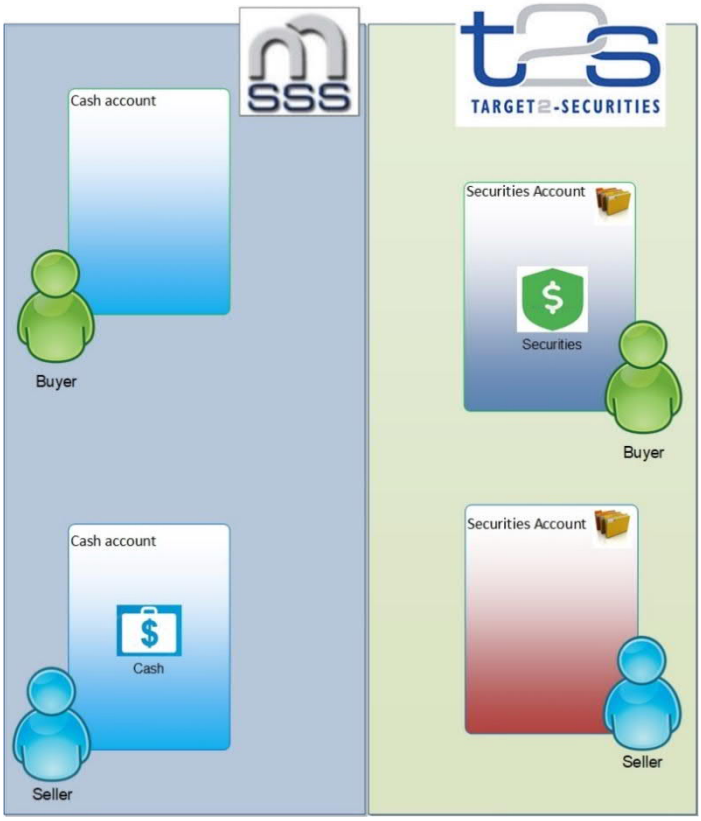
4. NBB-SSS receives confirmation of debit (MT900).



5. NBB-SSS releases the transaction in T2S.



6. DVP completed. Both securities and cash have been delivered.



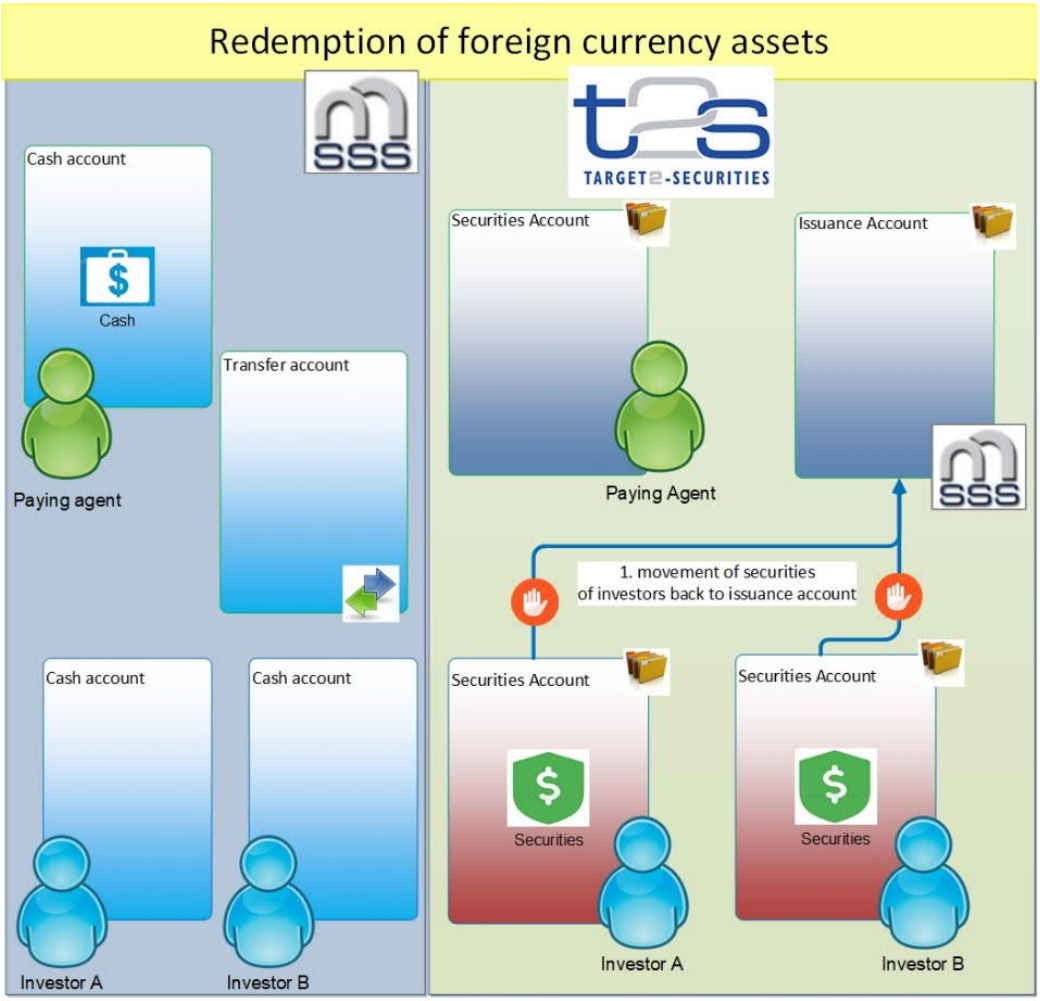
2.2 Corporate Action in Foreign currency

2.2.1 Corporate action payments via a Paying Agent's Dedicated Transfer Account (DTA) – Standard Procedure

The payment of Corporate actions in Foreign currencies (when the NBB-SSS provides the Foreign currency financial service) shall be executed on the FCA and the DT of the Participant acting as Paying Agent and on the FCA of Participants having a position in the relevant securities.

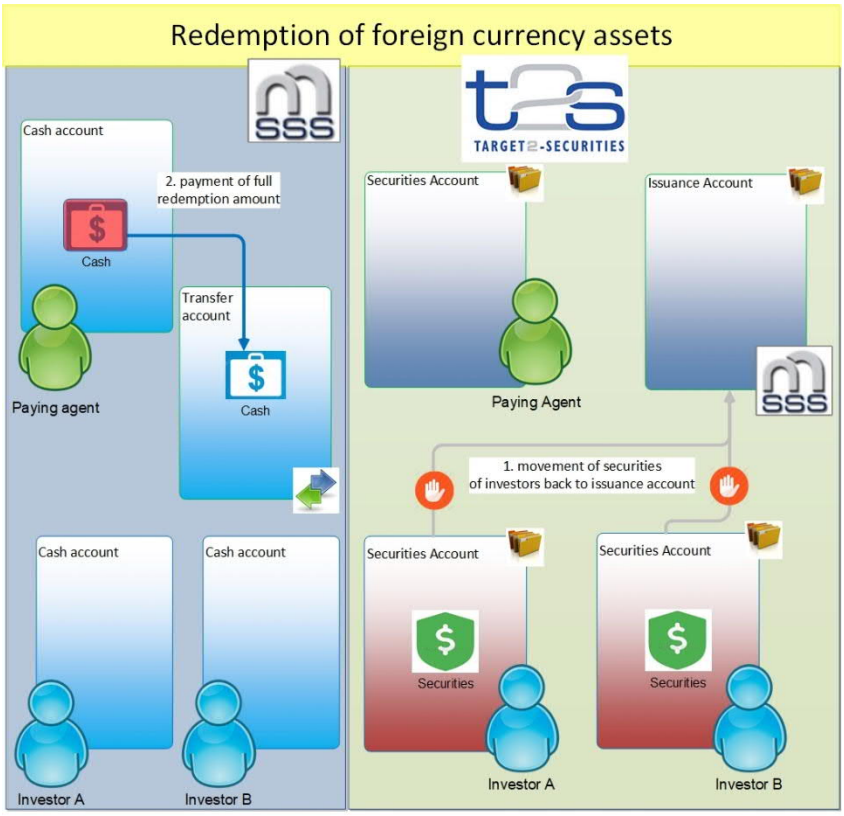
2.2.1.1 Redemptions

1. The system detects a corporate action in Foreign currencies provided the Paying Agent has opted in. The transactions delivering the position from investor's securities account to issuance account[1] are put on hold.

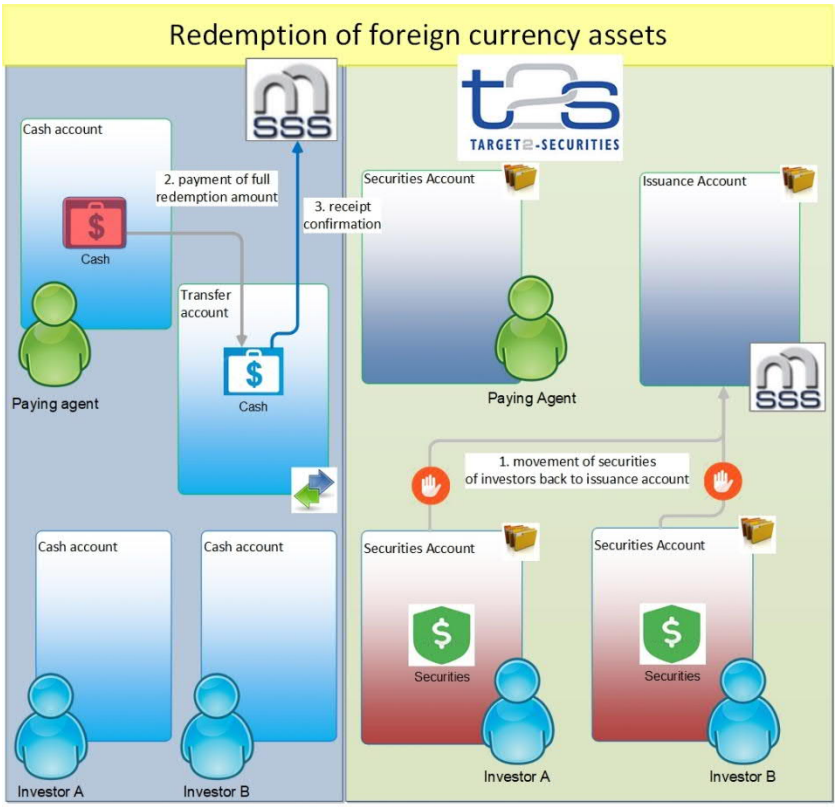


[1] In a later phase, this sese.023 will contain the cash amount

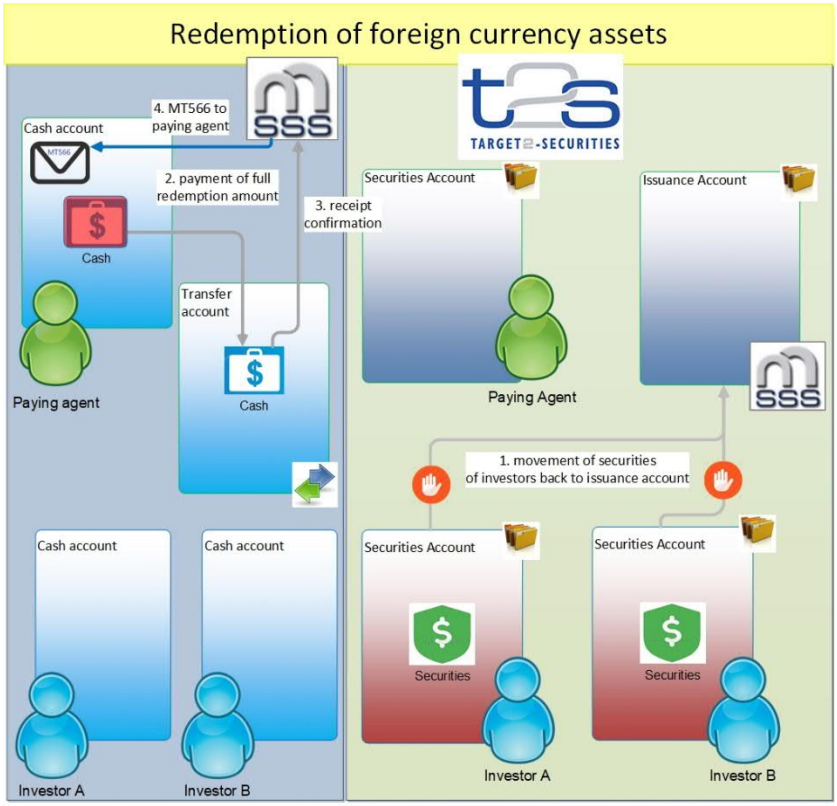
2. Cash transfer debiting the Paying Agent's FCA and crediting the Paying Agent's DTA is sent by NBB-SSS (MT202).



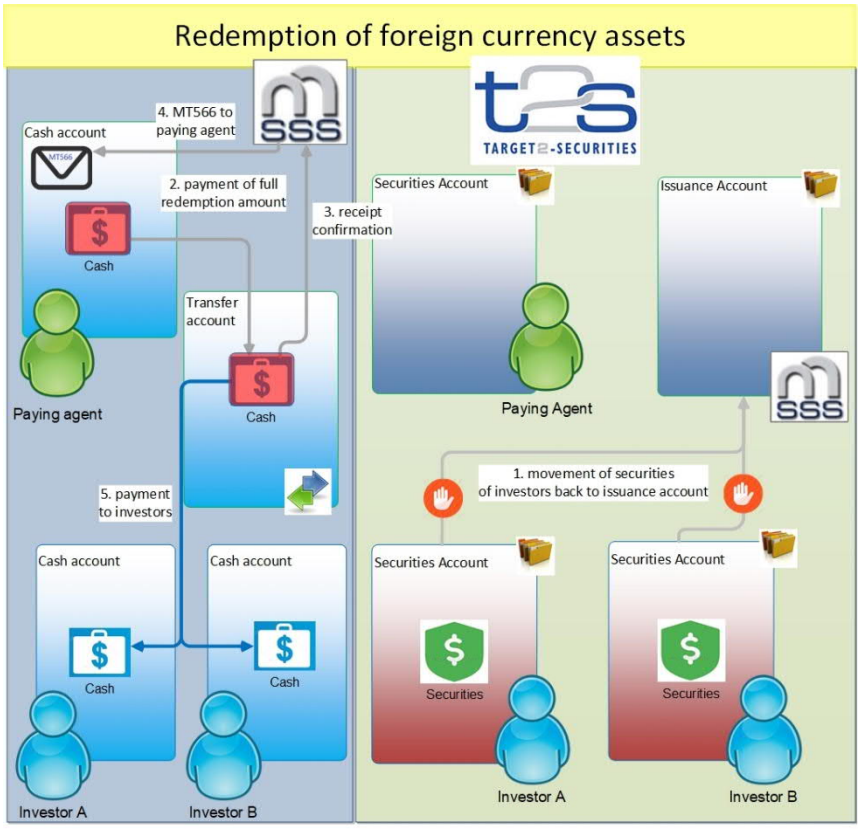
3. NBB-SSS receives the confirmation of the credit of the Paying Agent's DTA (MT910).



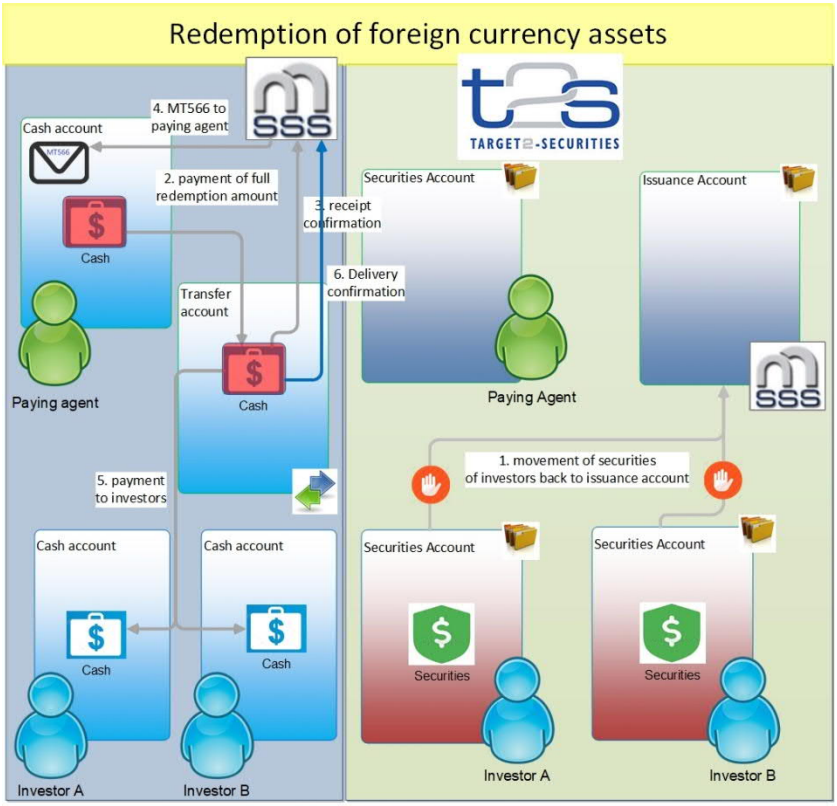
4. NBB-SSS sends the Corporate action confirmation (MT566) to the Paying Agent.



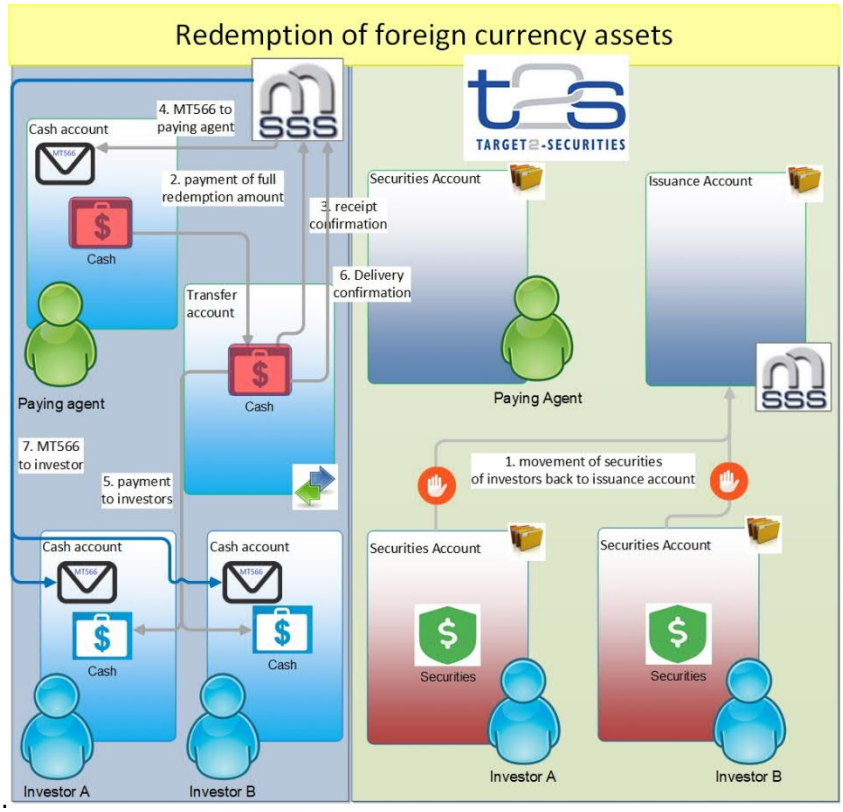
5. Cash transfer debiting the Paying Agent's DTA and crediting FCA of Participants having a position in the securities is sent (MT202).



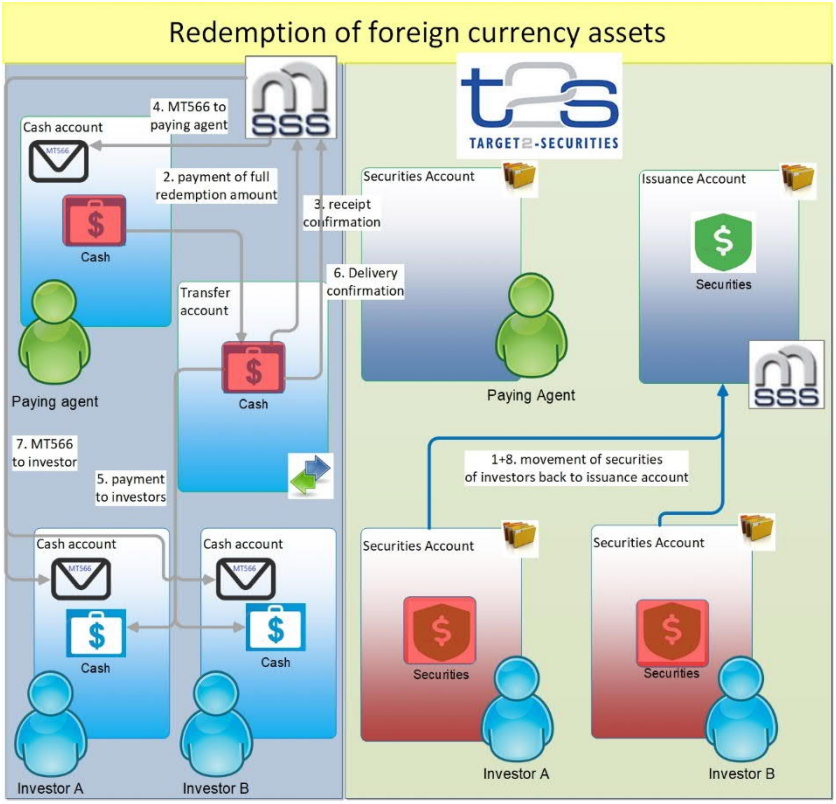
6. NBB-SSS receives the debit confirmation for the Paying Agent's DTA (MT900).



7. NBB-SSS sends the corporate action confirmation (MT566) to the Participants having a position in the securities.

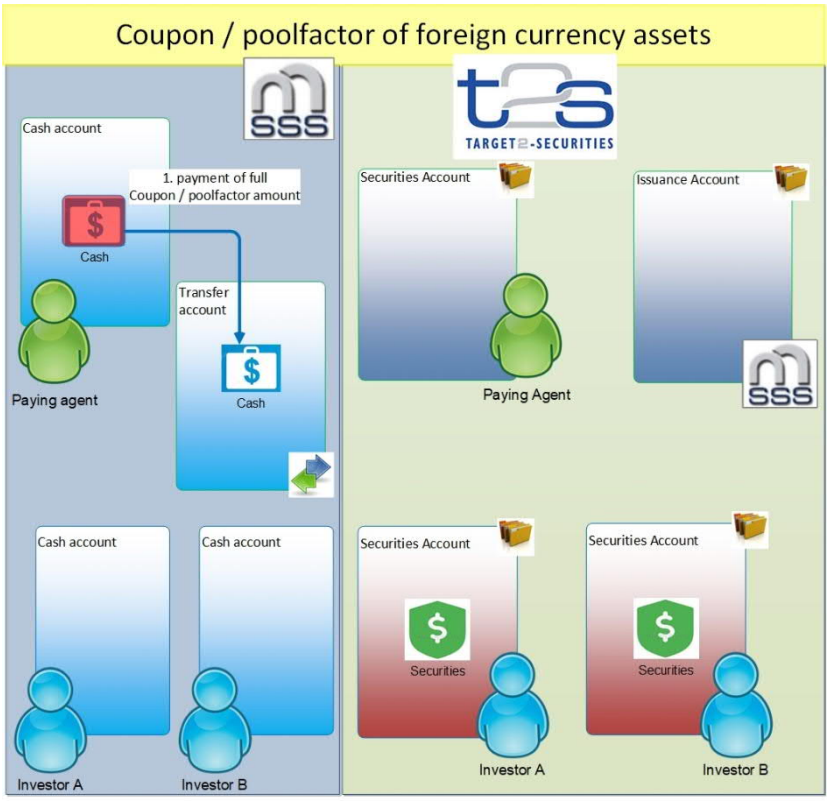


8. The Release of the transaction (type “CORP”) that moves the position of Participants having a position in the securities to the issuance account is executed.

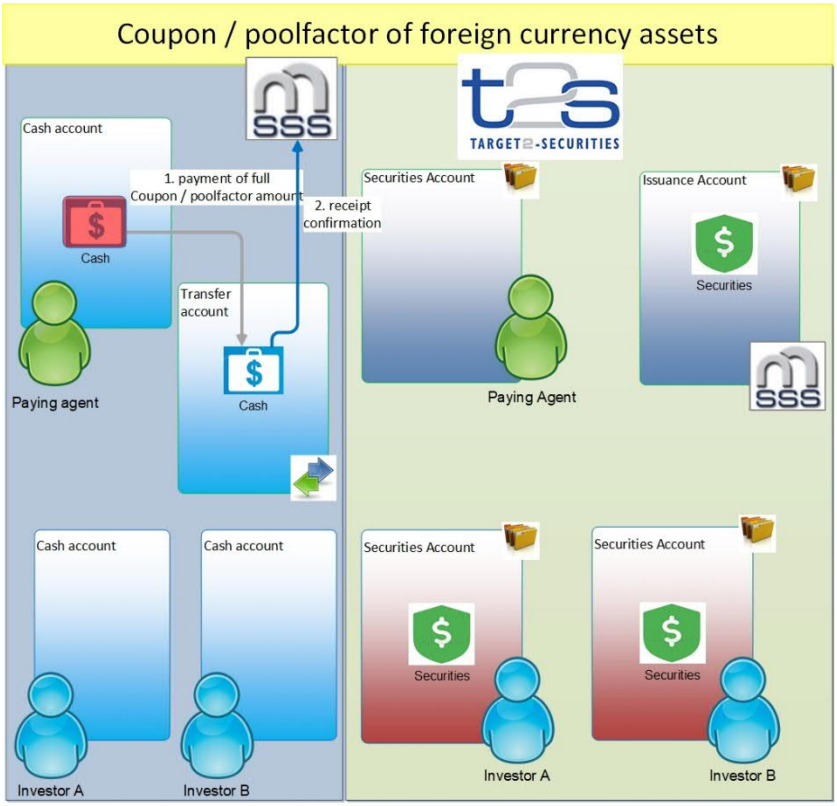


2.2.1.2 Coupons and poolfactors

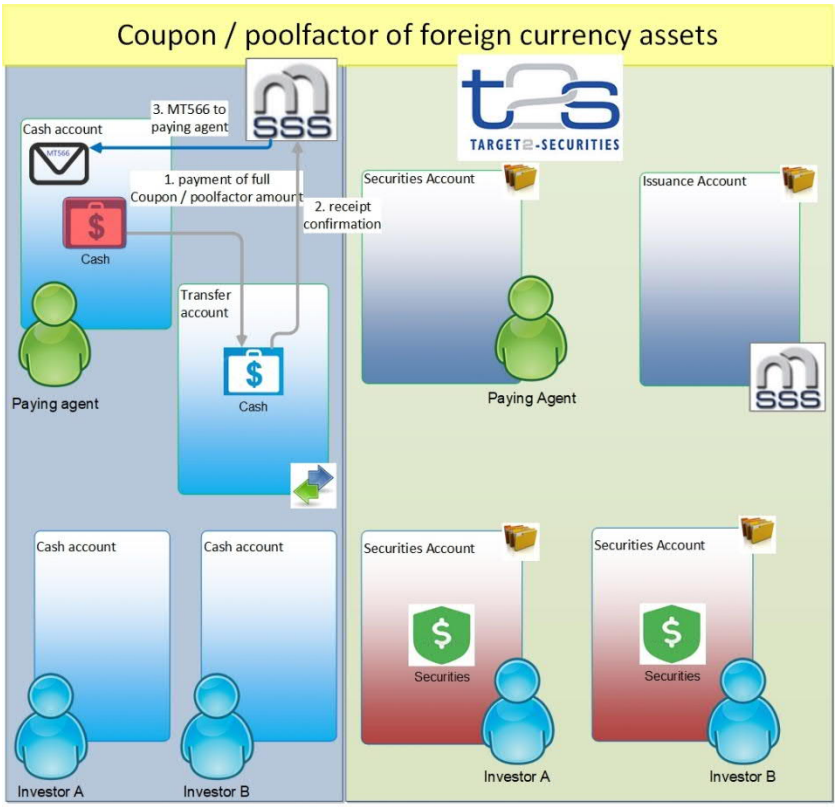
1. The cash transfer debiting the Paying Agent’s FCA and crediting Paying Agent DTA is sent (MT202).



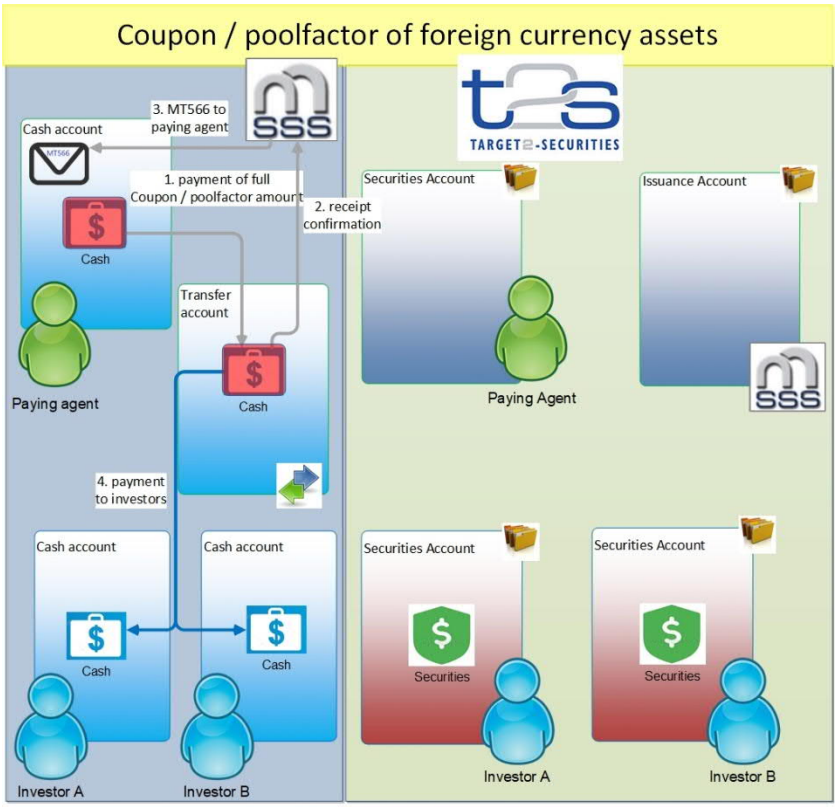
2. The NBB-SSS receives the confirmation of credit for the Paying Agent's DTA (MT910).



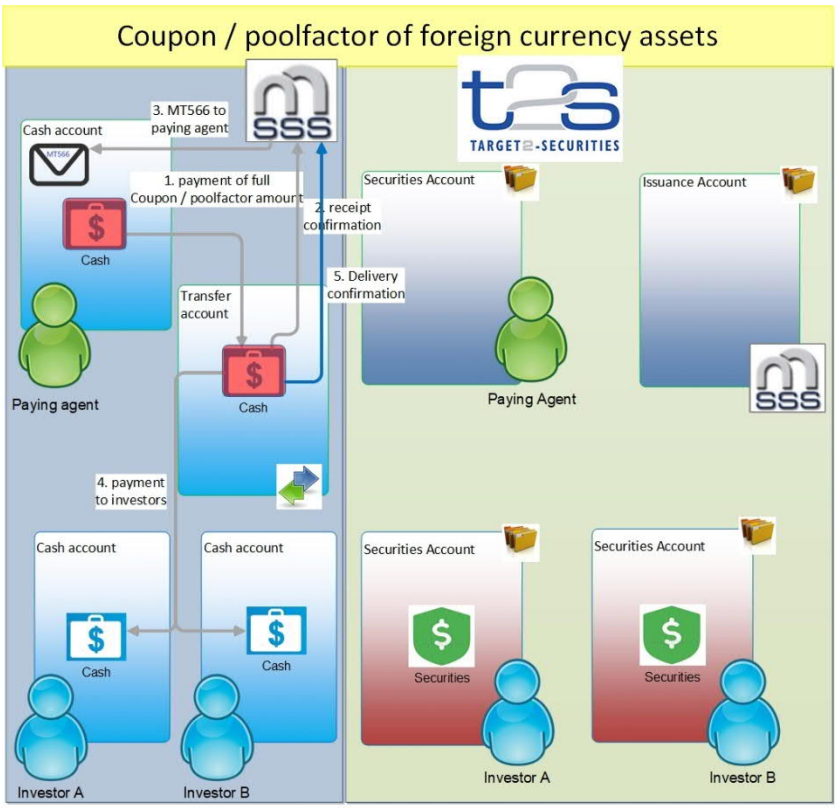
3. The NBB-SSS sends the corporate action confirmation (MT566) to the Paying Agent.



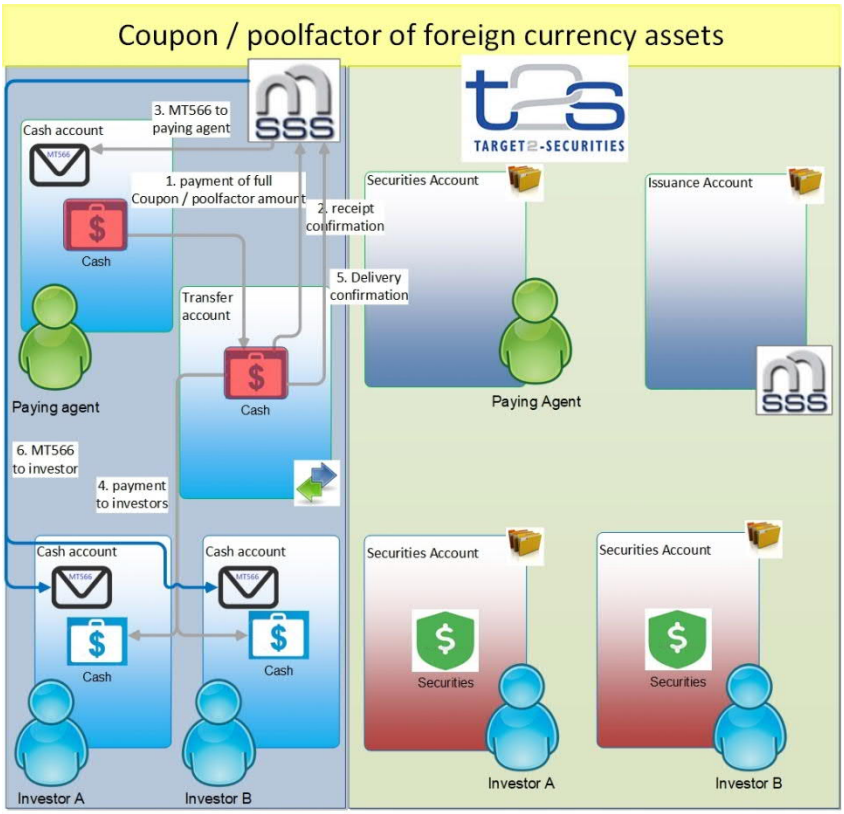
4. The NBB-SSS sends the cash transfer debiting the Paying Agent's DTA and crediting FCA of Participants having a position in the securities (MT202).



5. The NBB-SSS receives the debit confirmation for Paying Agent's DTA (MT900).



6. The NBB-SSS sends the Corporate action confirmation (MT566) to the Participants having a position in the securities.

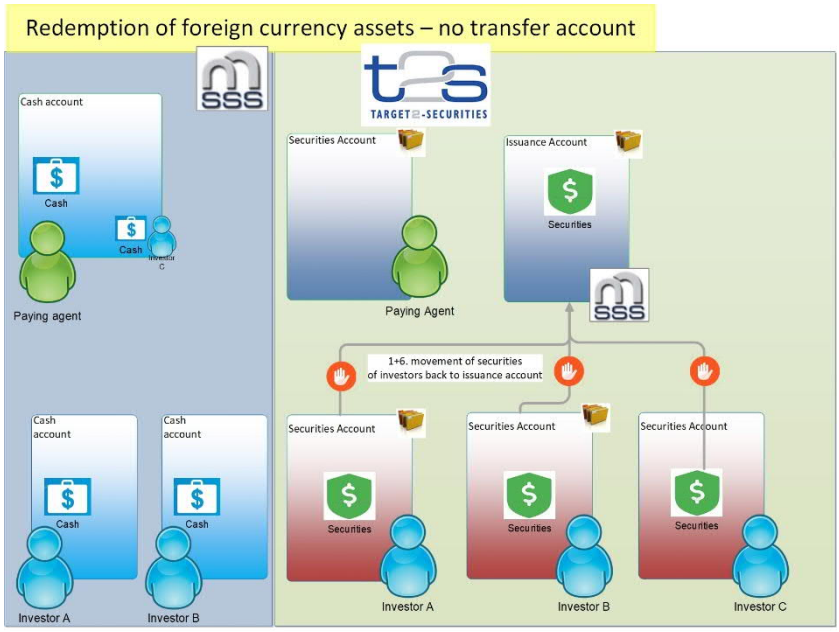


2.2.2 Corporate action payments without the use of a Dedicated Transfer Account (DTA) – Exceptional procedure upon Paying Agent's request.

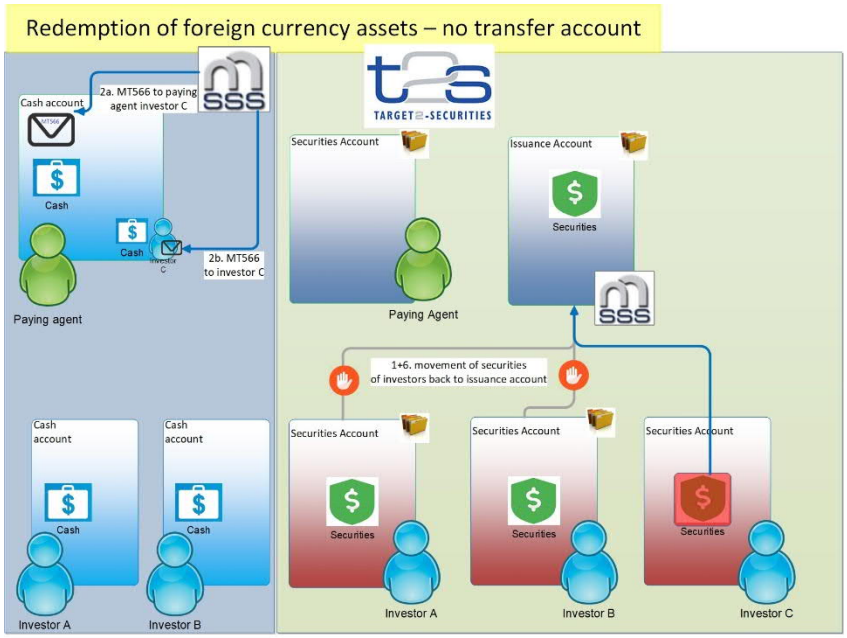
In exceptional circumstances the NBB-SSS may allow the payment of Corporate actions directly via the Paying Agent's FCA (without DTA).
Pro's and Con's of this scenario are listed in chapter 2.2.3.

2.2.2.1 Redemptions

1. When the Paying Agent has opted in the NBB-SSS' Foreign currency financial service the system detects a Corporate action in Foreign currencies. The transactions delivering the position from investor's securities account to issuance account[2] are put on hold.

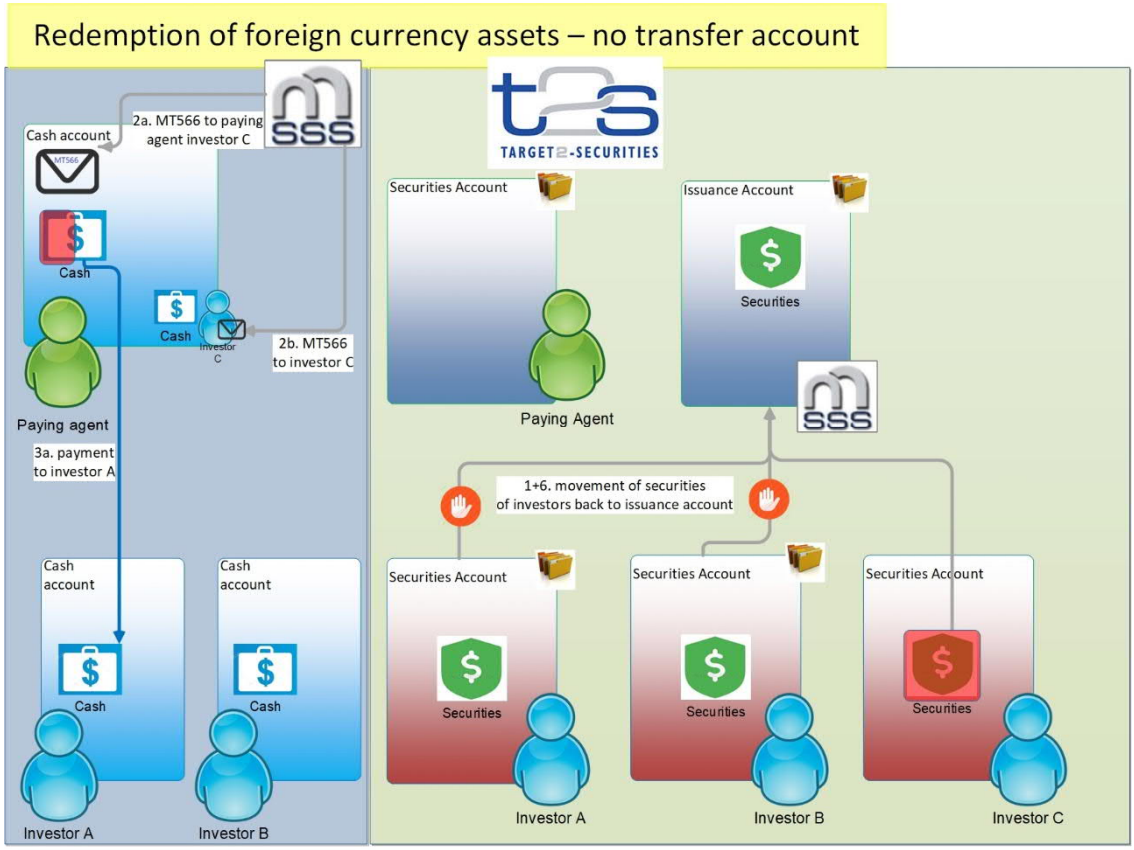


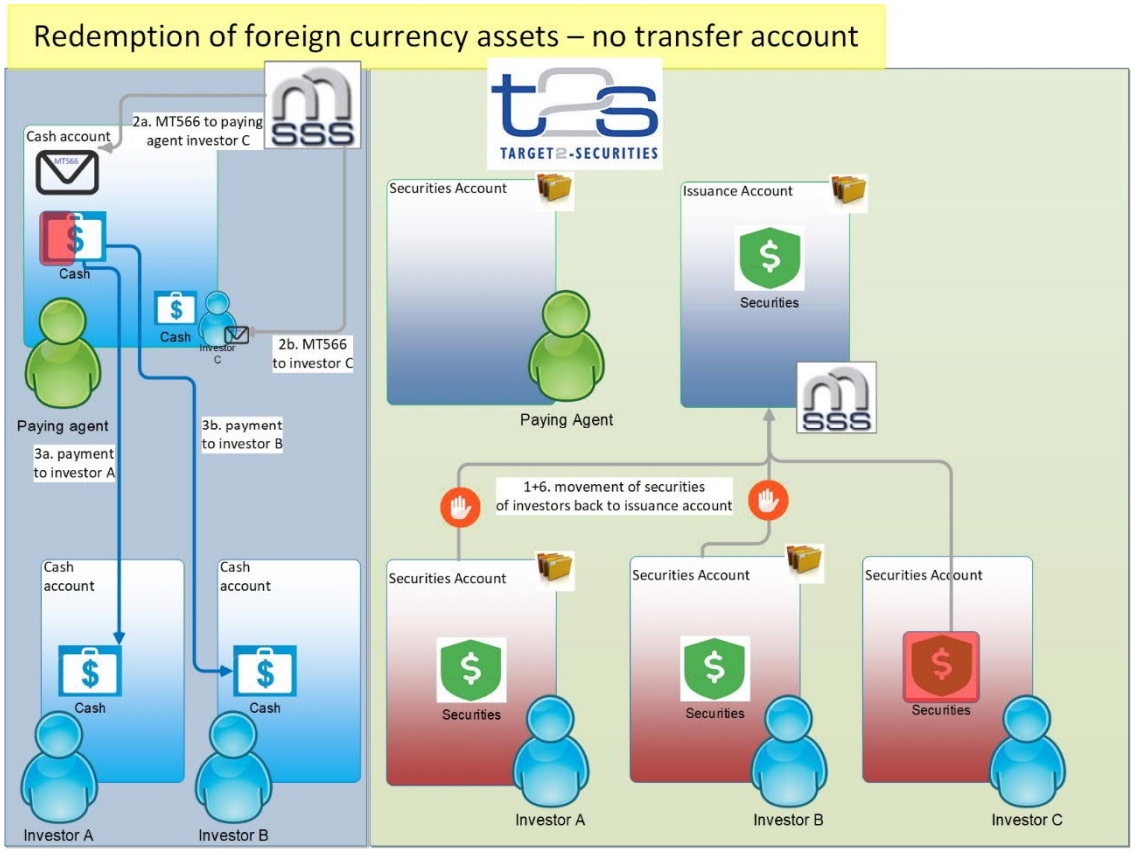
2. NBB-SSS detects that the Paying Agent's FCA to debit is equal to Investor C's FCA to credit, and immediately releases the securities transfer and sends the MT566 to both Paying agent and Investor C without creating a cash transfer.



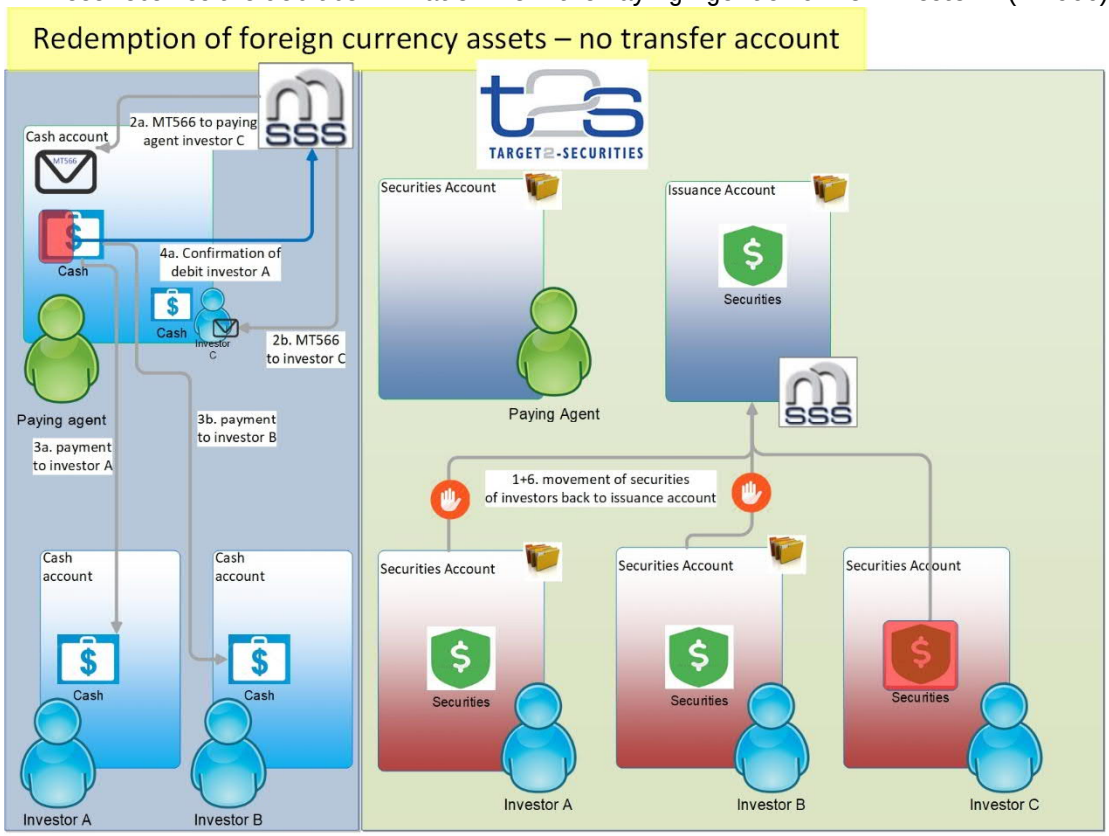
[2] In the first phase the cash amount will not be filled, this functionality will be added later.

3. Cash transfers debiting the Paying Agent's FCA and crediting FCA of Participants having a position in the securities are sent (MT202/pacs.009).

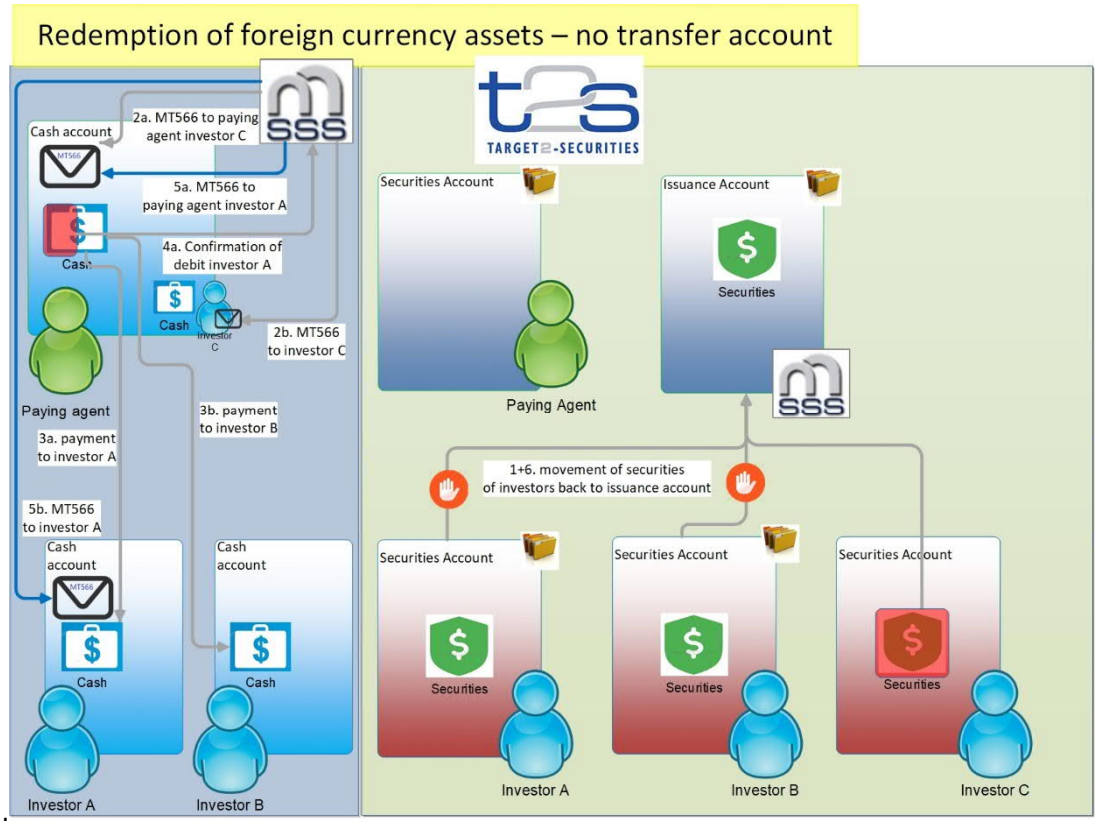




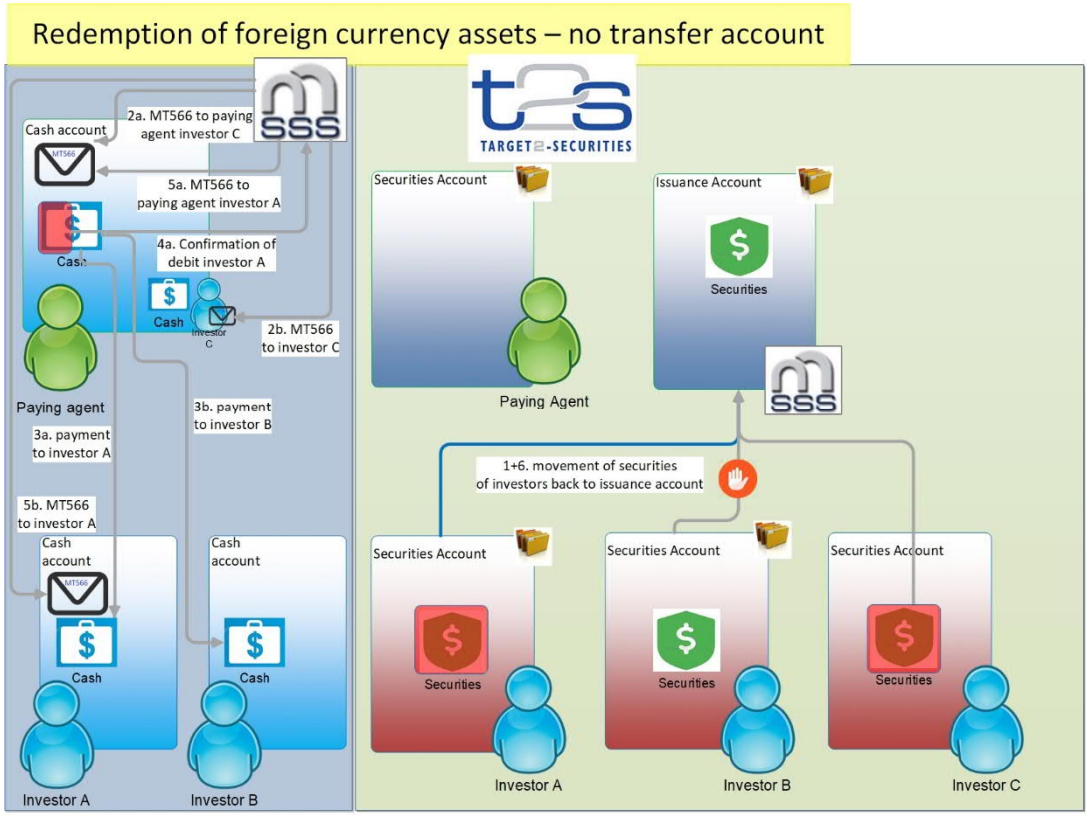
4. On the Paying Agent's FCA there is enough money to pay Investor A but not for investor B. NBB-SSS receives the debit confirmation from the Paying Agent's FCA for Investor A (MT900).



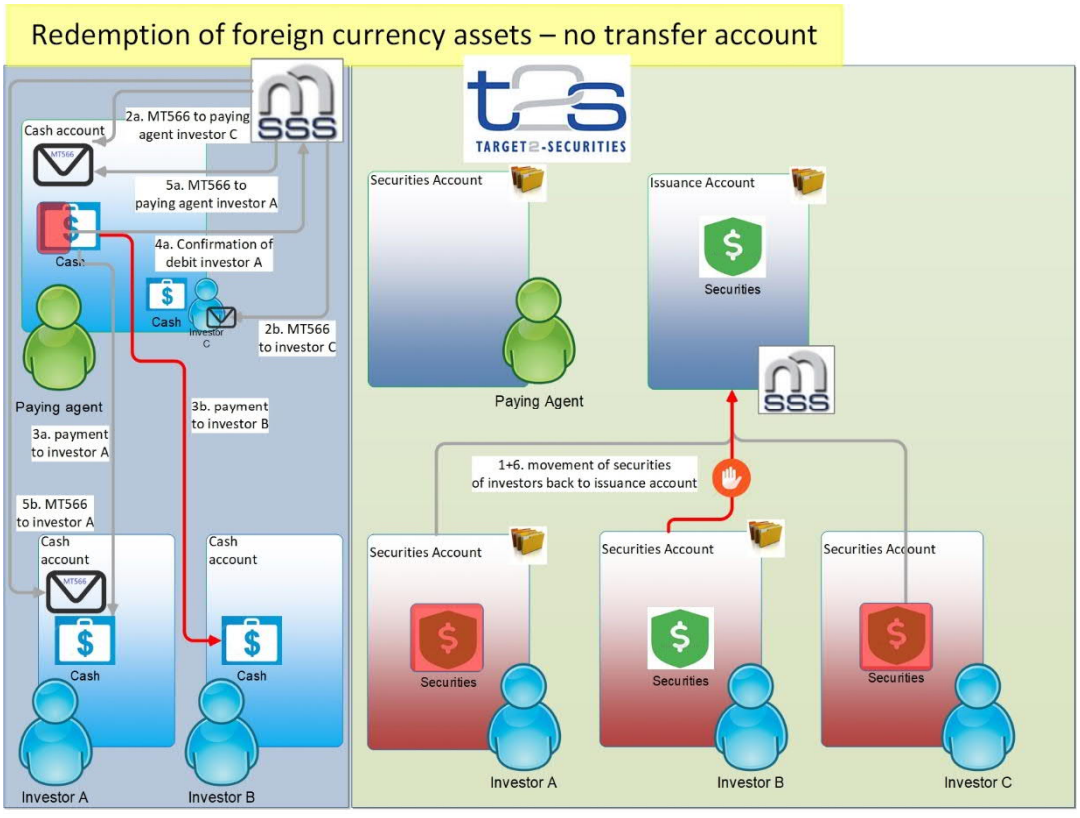
5. NBB-SSS sends the corporate action confirmation (MT566/seev.036) to the Paying agent and the investor A.



6. The Release of the transaction (type “CORP”) that moves the position of Participant A to the issuance account.



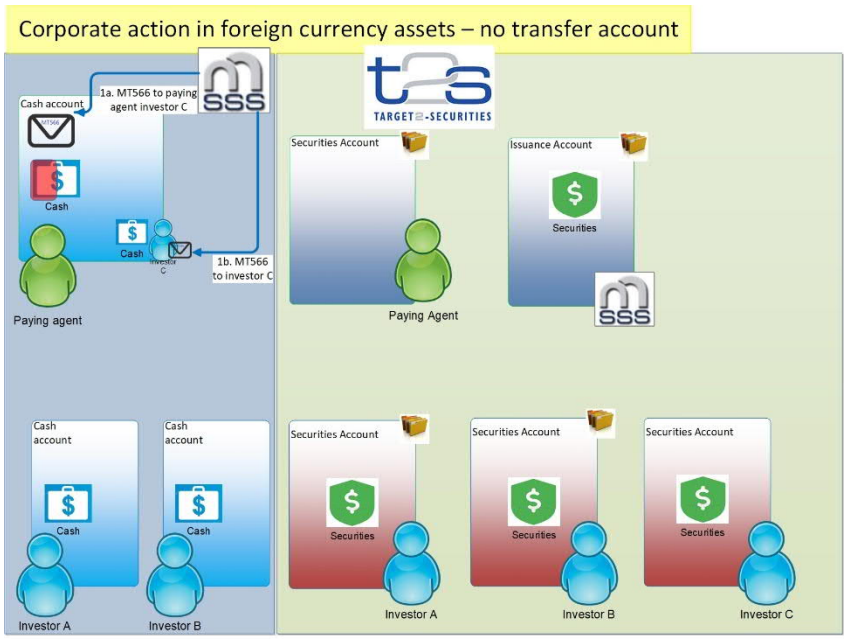
7. The payment of investor B and release of investor B’s position will remain blocked until sufficient cash is available.



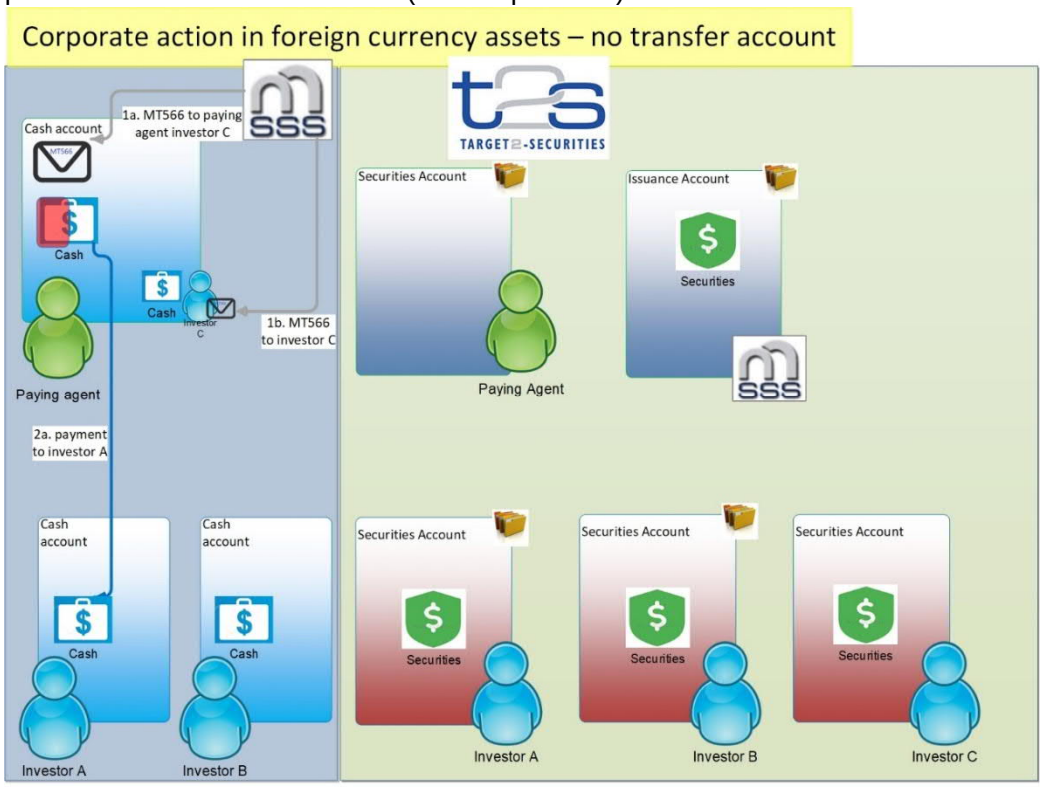
2.2.2.2 Coupons and poolfactors

0. The system detects a corporate action in Foreign currencies the Paying Agent has opted in without usage of a transfer account. There are three investors with a position. Coupons nor poolfactors in foreign currencies are visible as a T2S transaction.

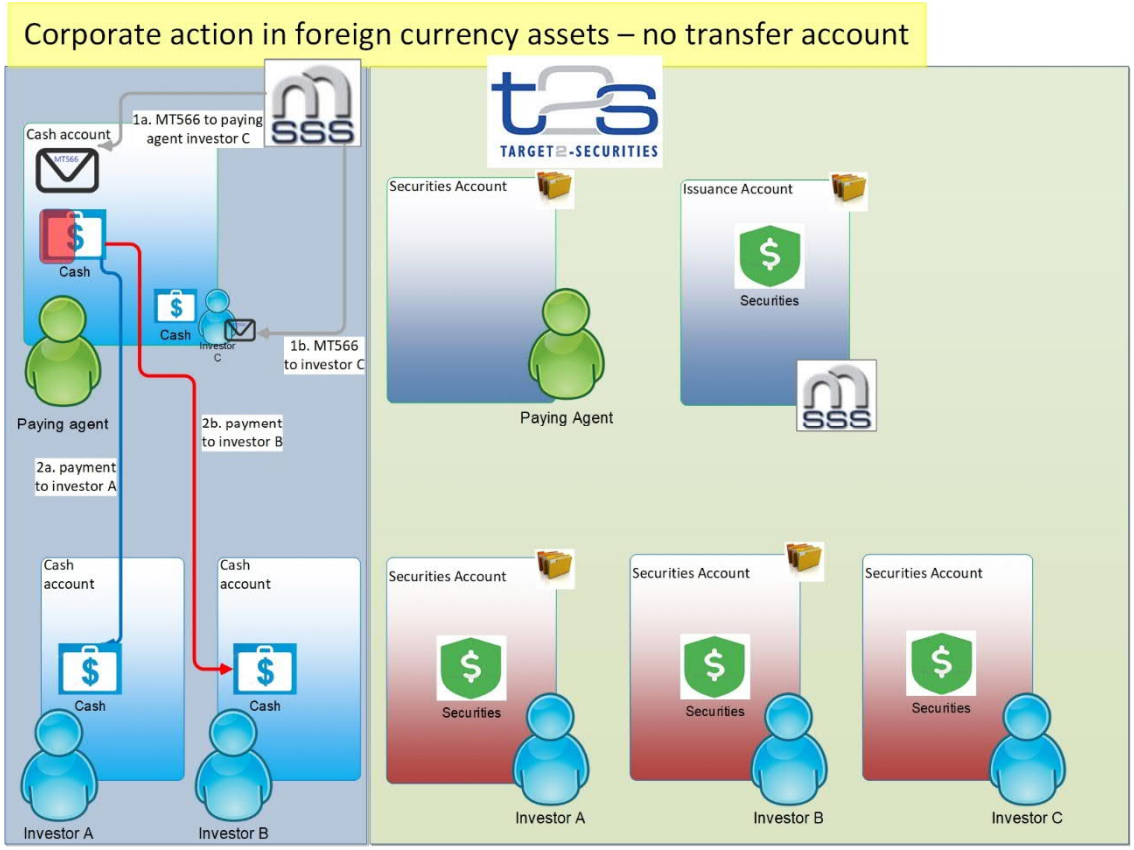
1. NBB-SSS detects that the Paying Agent's FCA to debit is equal to Investor C's FCA to credit, and immediately sends the MT566 to both Paying agent and Investor C without creating a cash transfer.



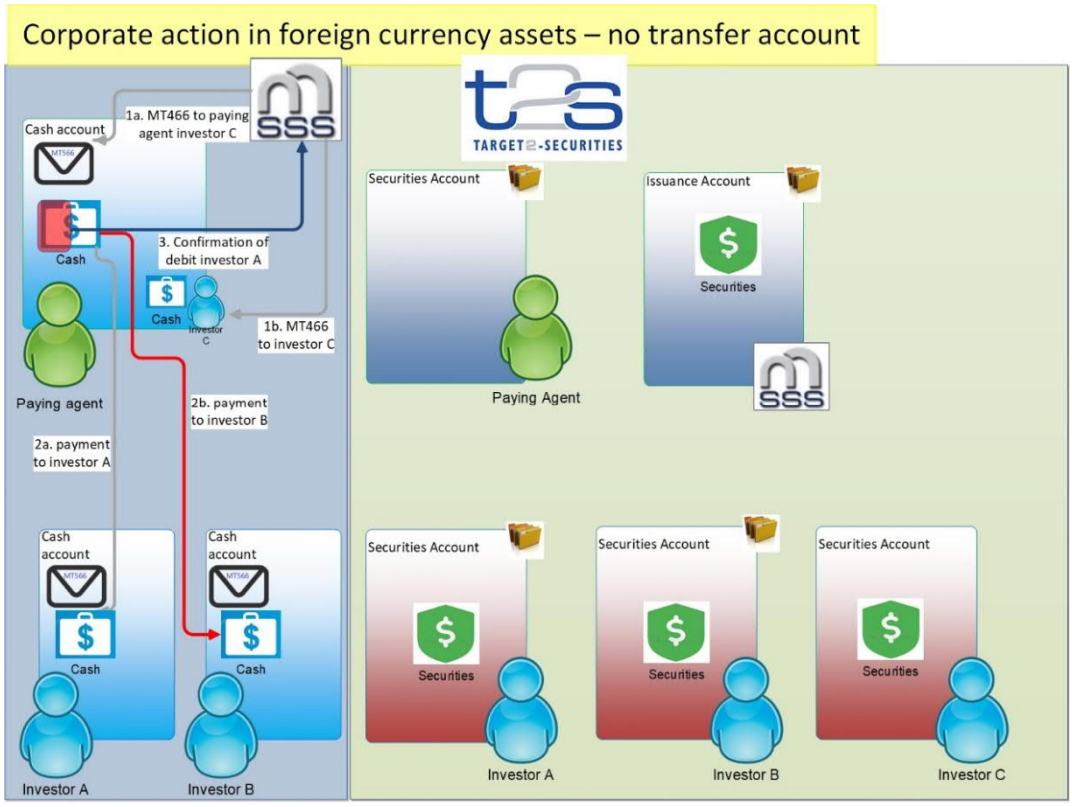
2. Cash transfers debiting the Paying Agent's FCA and crediting FCA of Participants having a position in the securities are sent (MT202/pacs.009).



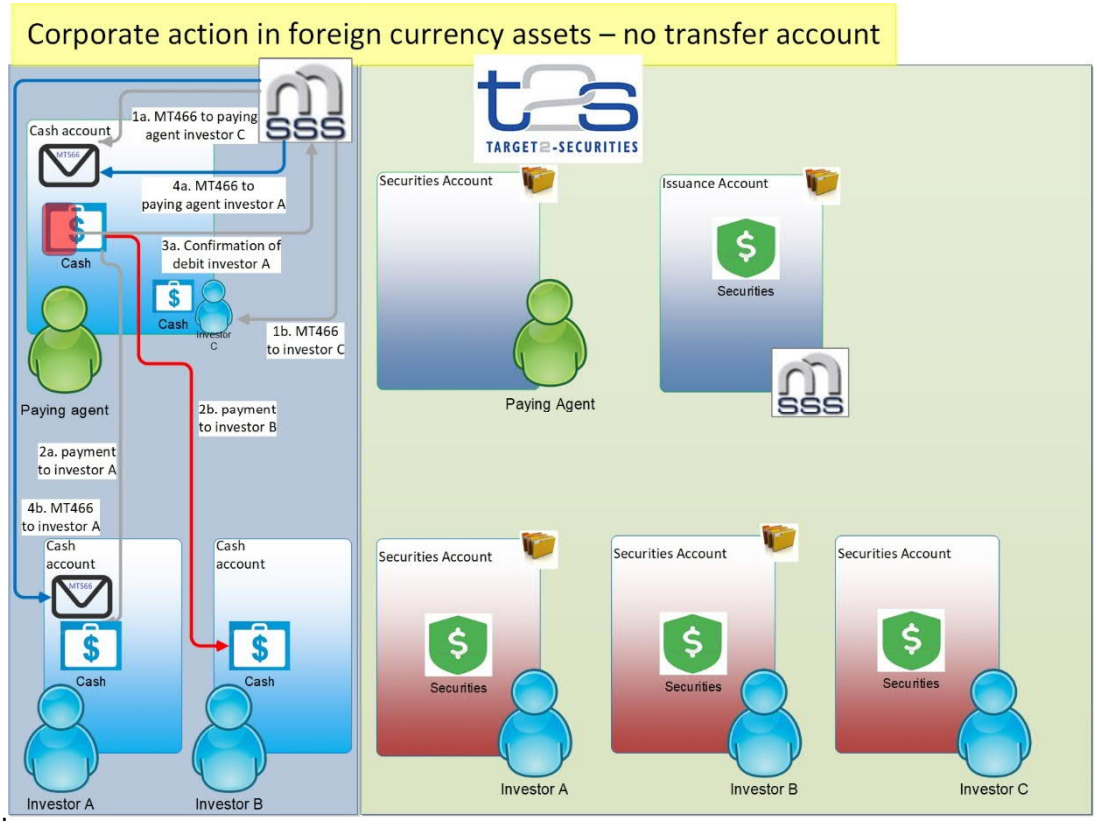
As there is only a position on the paying agent's account that can cover 1 of the coupon payments, the second coupon payment stays in 'to be executed' status.



3. On the Paying Agent's FCA there is enough money to pay Investor A but not for investor B. NBB-SSS receives the debit confirmation from the Paying Agent's FCA for Investor A (MT900).



4. NBB-SSS sends the Corporate action confirmation (MT566/seev.036) of the investor A CA to the Paying agent and the investor A.



2.2.3 Pros and Cons of usage of DTA versus no DTA

With DTA:

This is the standard procedure.

All investors shall be treated equally, as there is a guarantee that the cash leg for executing the total Corporate action is available.

Without DTA:

This procedure could be accepted by NBB-SSS in exceptional circumstances at the Paying Agent's express request and under the sole responsibility of the Paying Agent: for example in case of Foreign currencies in a timezone preceding CET (e.g. AUD, JPY, ...) where no DTA in the Foreign currency timezone could be provided for.

- No payment instructions will be sent in case the account from and account to are equal: in this case the MT566s are released immediately. This will be the case for the positions for which the Paying Agent is also the Foreign Currency Paying Agent.
- All payment debit instructions are sent, but only the executed ones will trigger the sending of an MT566.
- Paying agent will receive an MT566 per position that has been paid (not 1 global one as in the scenario with DTA) and will have to reconcile accordingly.

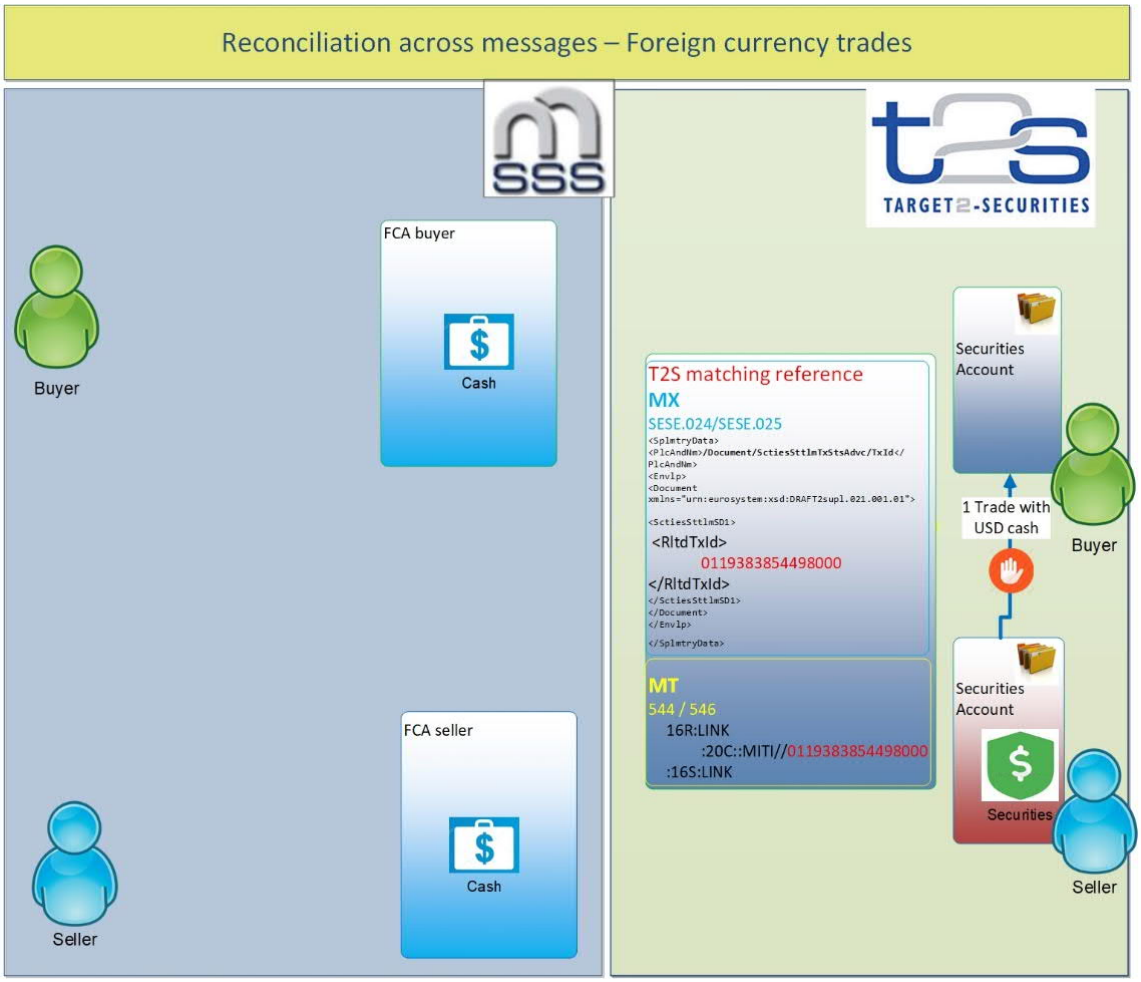
This may be a preferable option in case the currency is in a timezone preceding CET: if Paying Agent and investor both have accounts in the foreign currency timezone preceding CET, a DTA in CET zone can obstruct that the payment reaches the investors before the Foreign currency timezone closes.

3 Reconciliation across messages

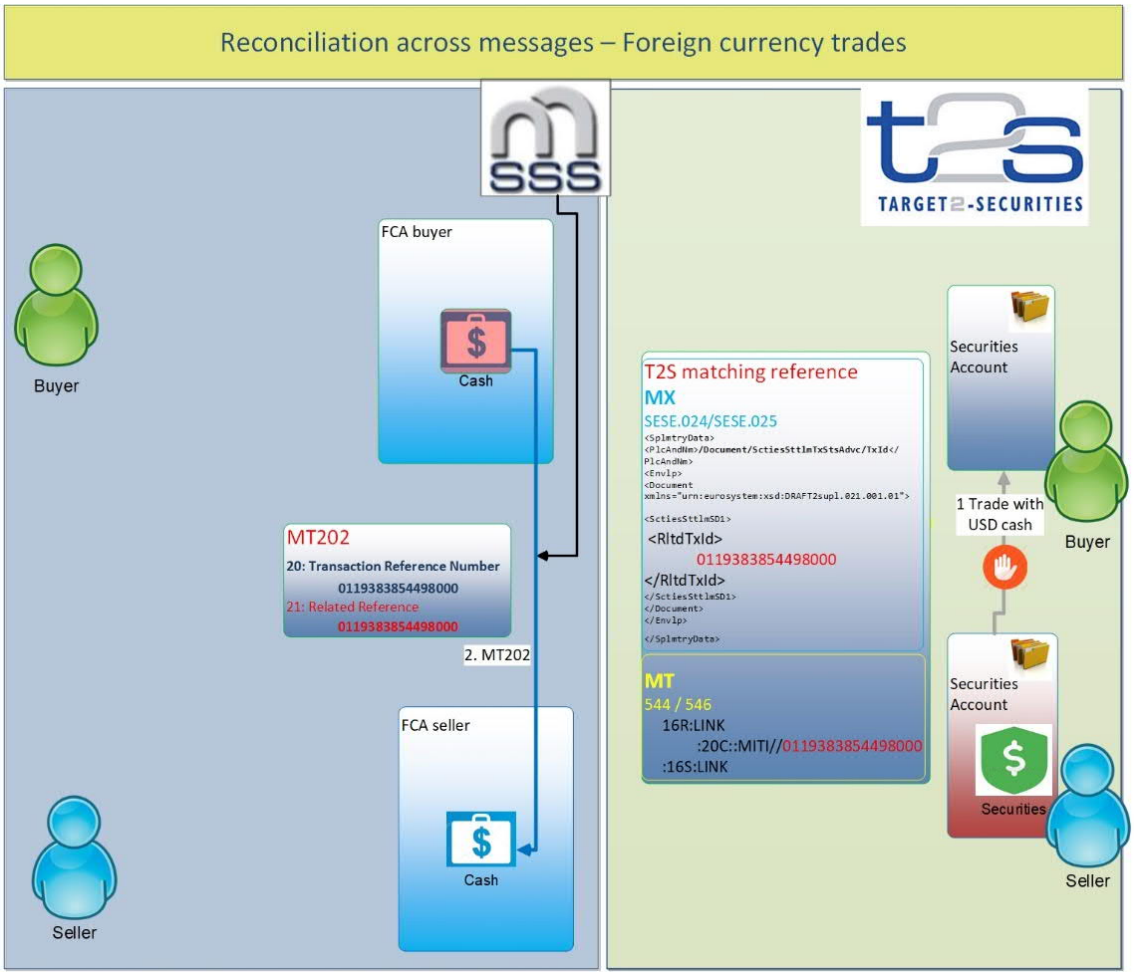
This chapter details the above process to the level of the messages.

3.1 DVP Transaction in Foreign currency

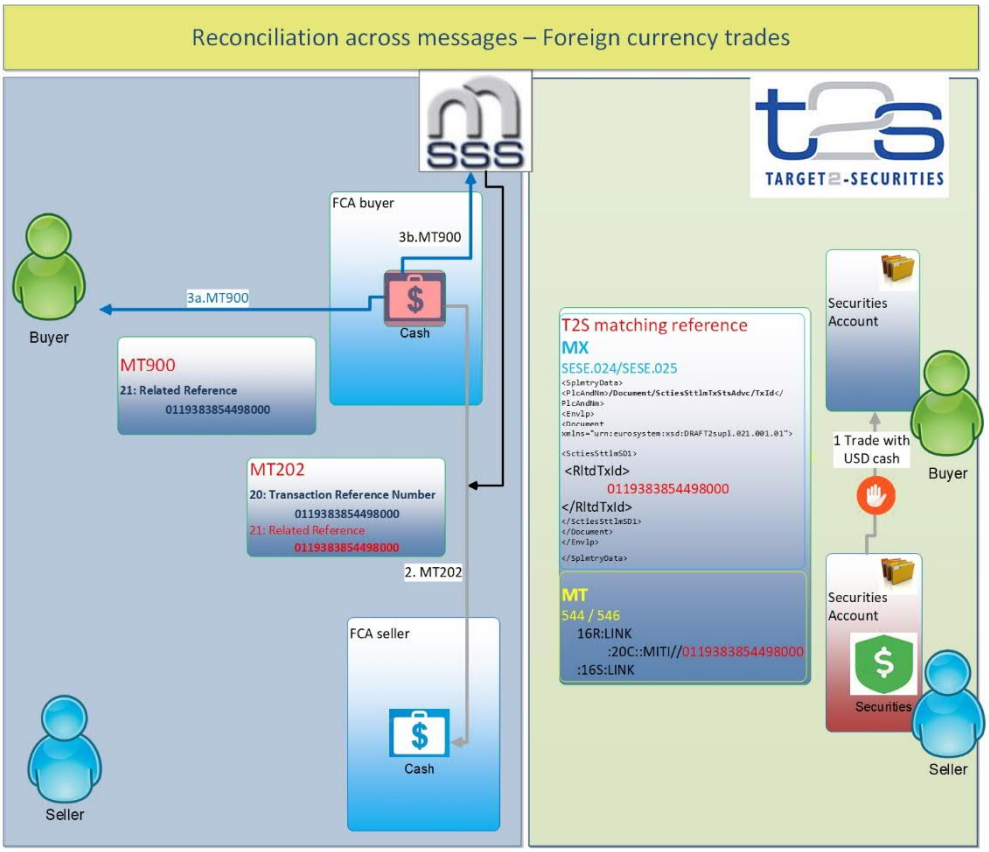
1. T2S matches the instructions and assigns a MITI-reference. As this is a transaction FOP with a cash part, T2S puts it on hold and informs (SEMT.014/.015) NBB-SSS of the (ongoing) reservation of securities at ISD. The T2S matching reference (known by both parties – in this example 0119383854498000) is extracted.
   The T2S matching reference is used in ISO20022 sese.024 (matching confirmation) and later in sese.025 (settlement confirmation). This reference is also present in the ISO15022 MT544/MT546 equivalents.



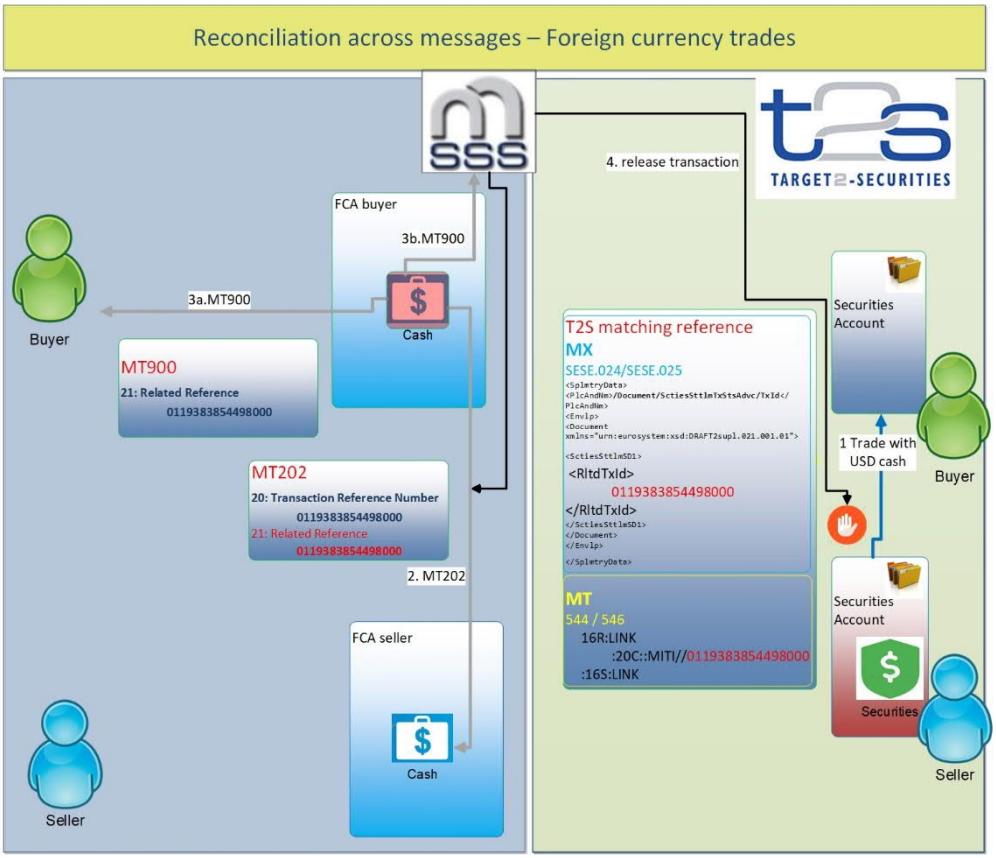
2. On receipt of the SEMT.015, confirming the reservation of the securities, the NBB-SSS instructs the debit of the buyer and the credit of the seller. The transfer instruction holds the T2S matching reference.



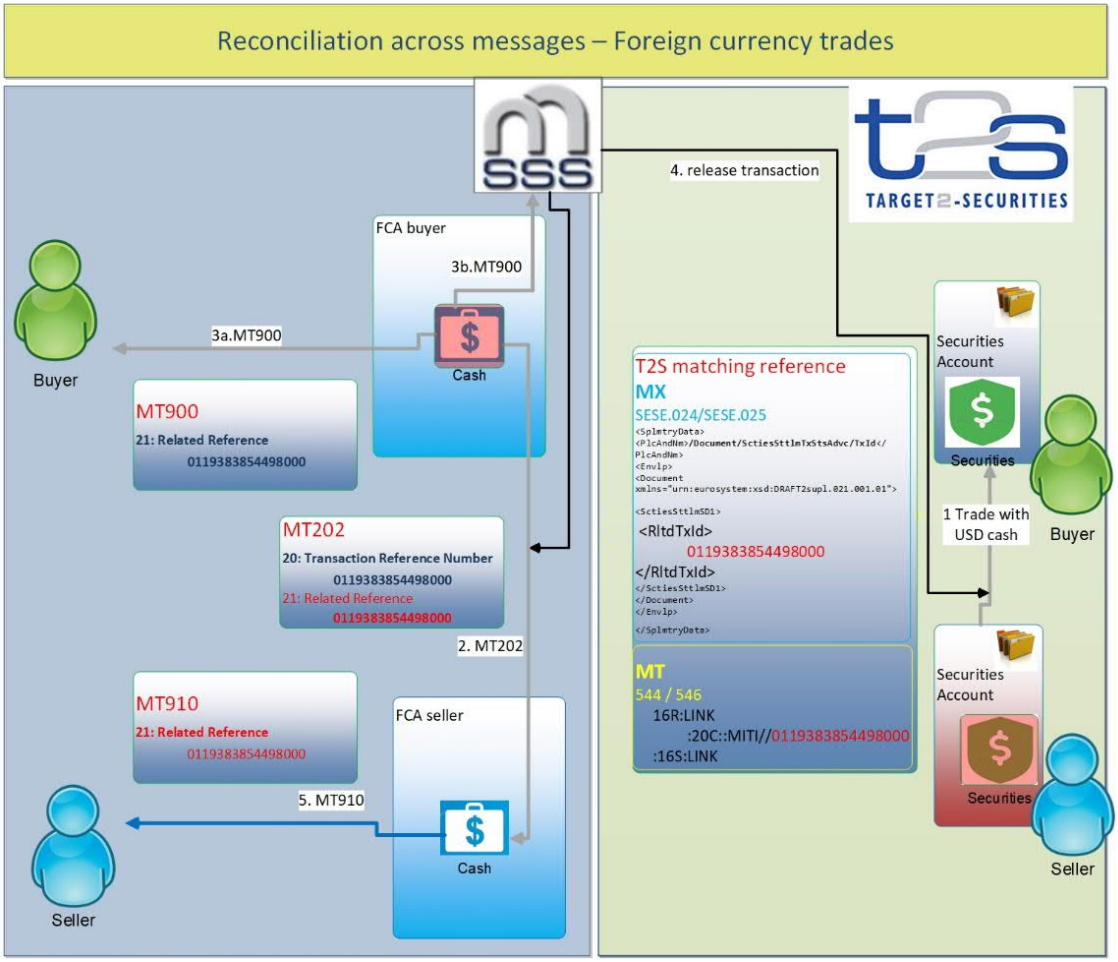
3. Both buyer and NBB-SSS receive the MT900 confirmation of debit with the reference in field 21, allowing NBB-SSS and the buyer to link this debit to the transaction in T2S.



4. NBB-SSS releases the transaction in T2S.



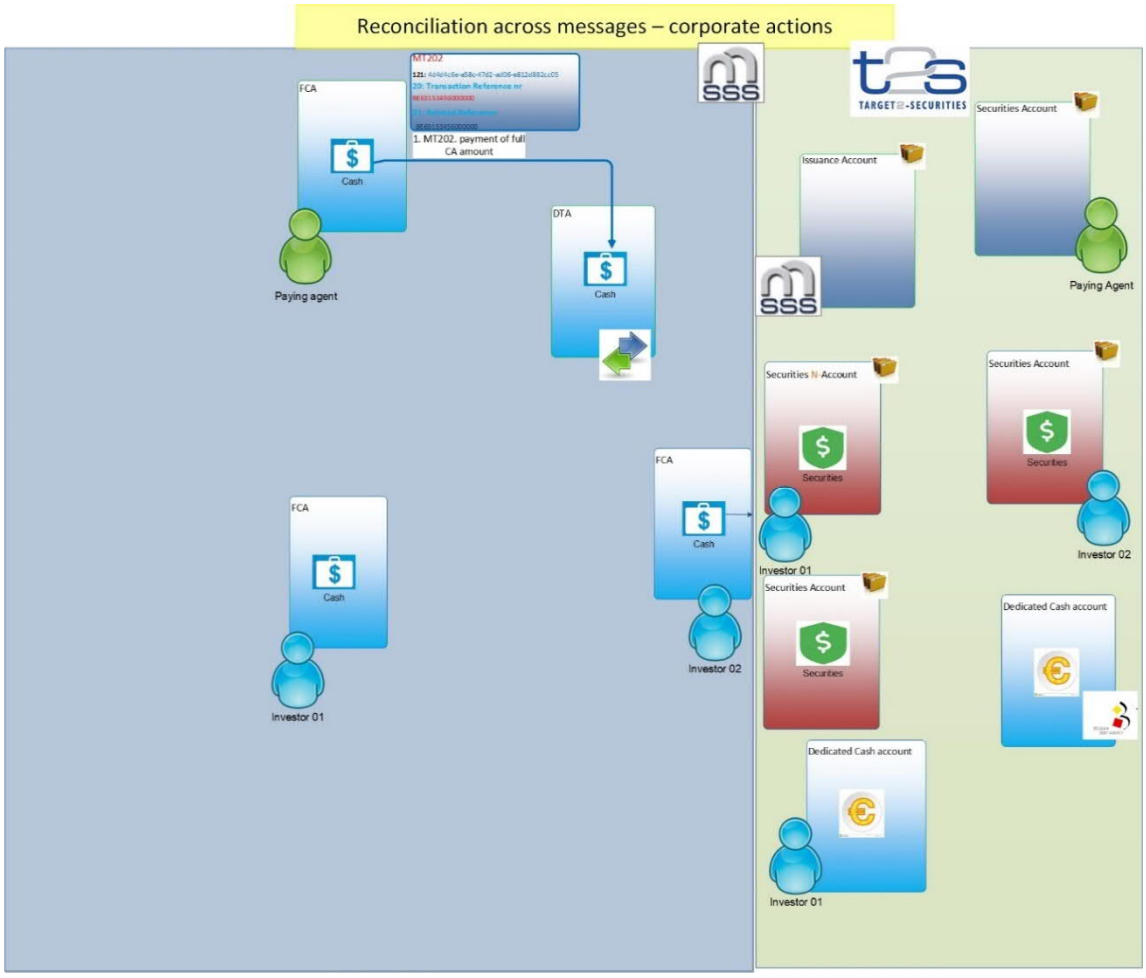
5. If the seller's FCA provider supports this functionality, the seller receives the MT910 confirmation of credit with the reference in field 21, allowing the seller to link this credit to the transaction in T2S.



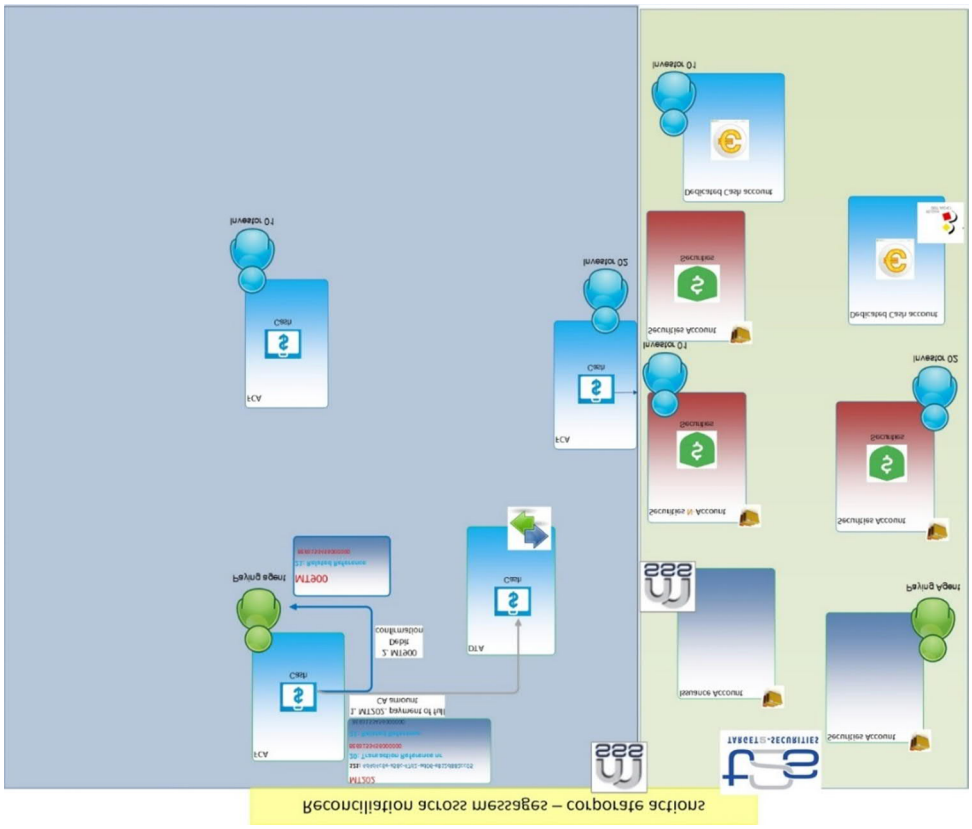
3.2 Corporate action (CA) in Foreign currency

3.2.1 With a Dedicated Transfer Account (DTA)

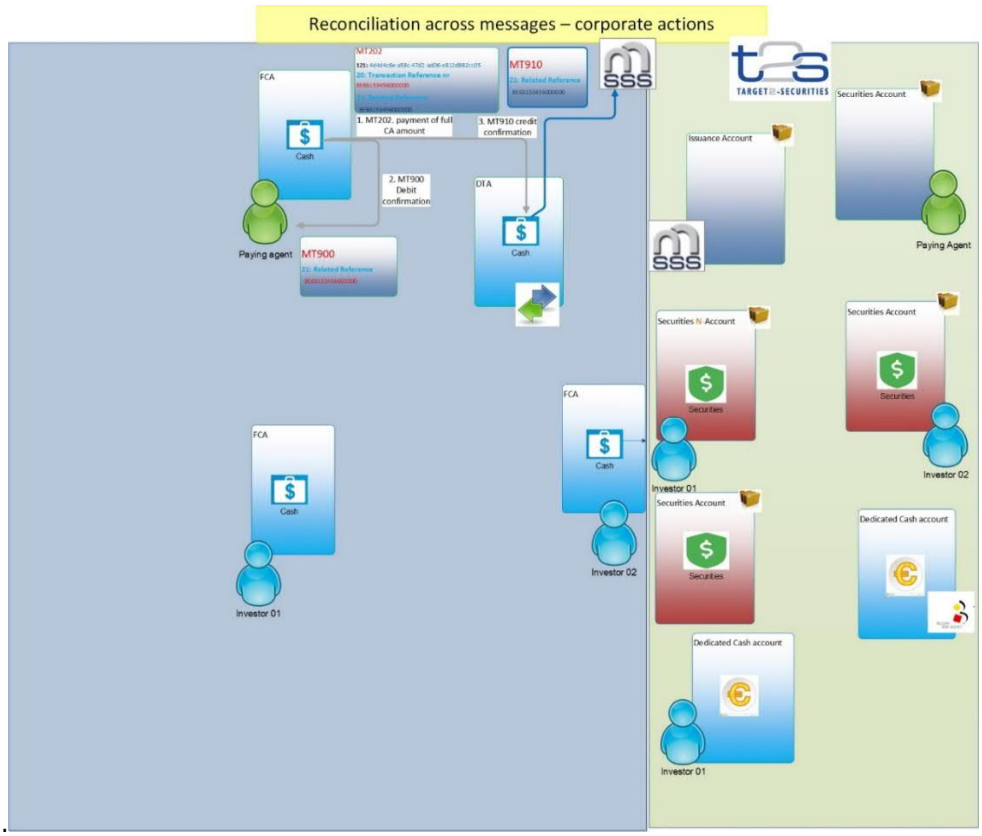
1. At End of Day the system detects a CA in Foreign currencies for which the NBB-SSS provides the Foreign currency financial service and sends out an MT202, to the designated FCA of the Paying Agent for the total amount of the CA to credit the Paying Agent's DTA.
   Fields 20 and 21 of the MT202 hold the ASRF (Account Servicer Reference, see annex 2). The ASRF is unique per CA movement. This reference allows the reconciliation between the cash movements and the messages sent out by the NBB-SSS (MT566 or seev.036) by all parties involved. The MT202 also contains a UETR generated by Ramses, the NBB-SSS application, that may allow to track the cash transfer through SWIFT GPI.



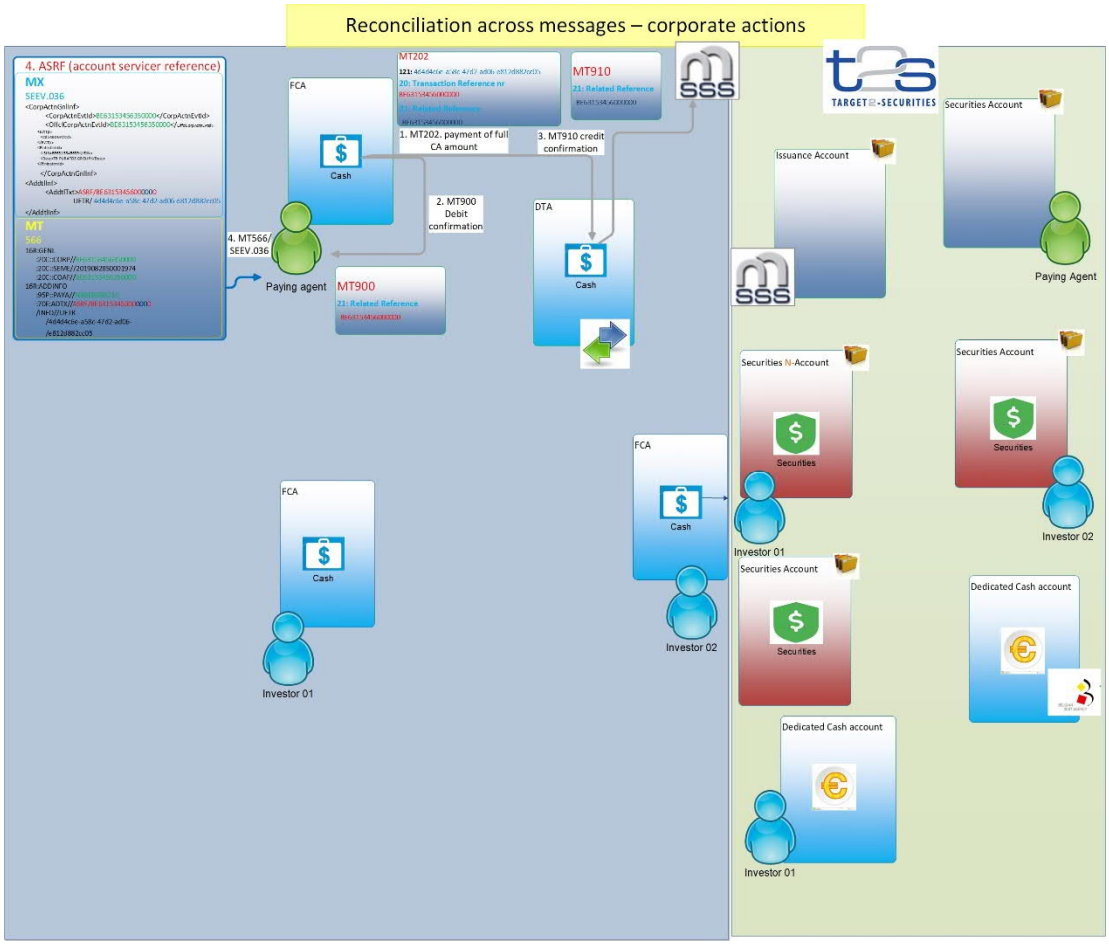
2. The Paying Agent receives the MT900 confirmation of debit with the ASRF reference in field 21. This field is a copy from MT202's field 20.



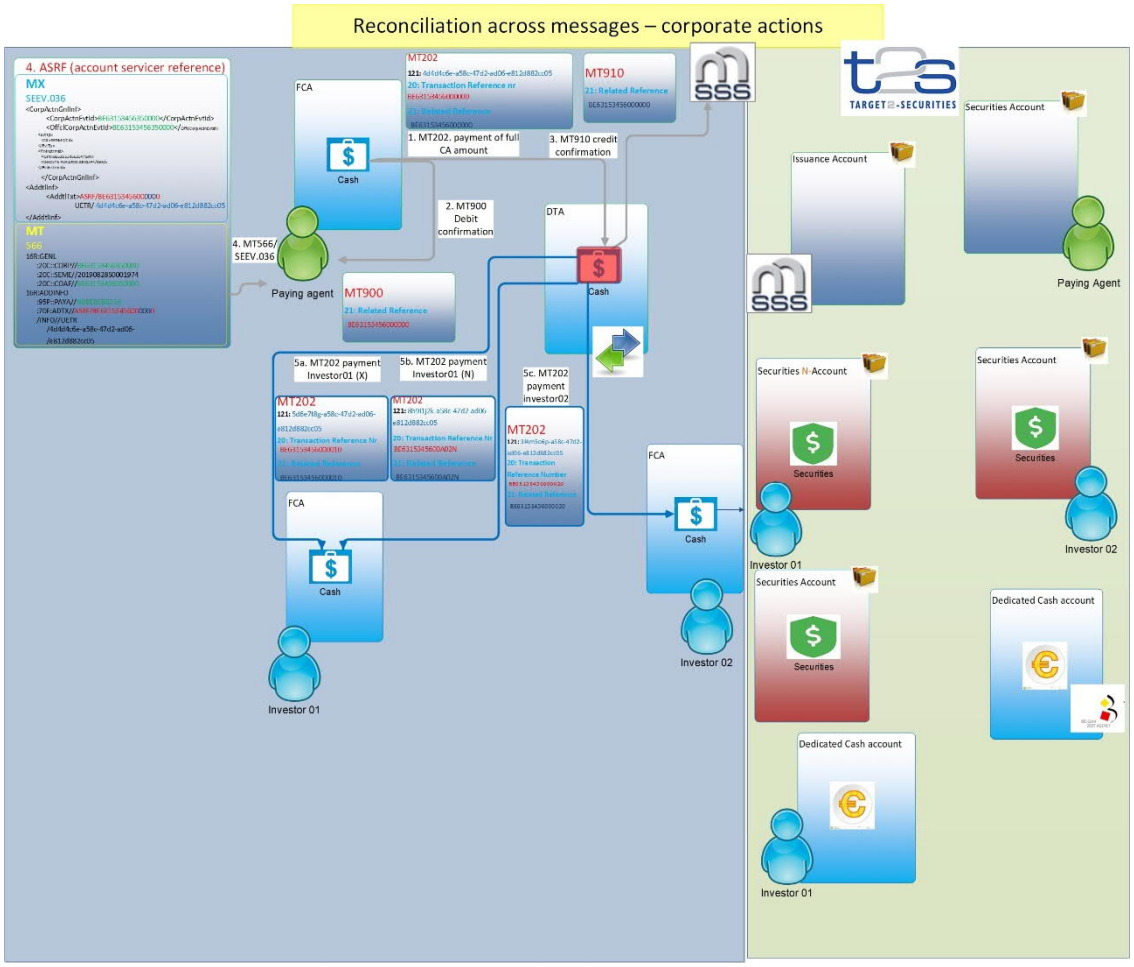
3. When the cash has been credited on the Dedicated Transfer Account, the NBB-SSS receives the MT910 confirmation of credit with the ASRF in field 21. This field is a copy from MT202's field 21



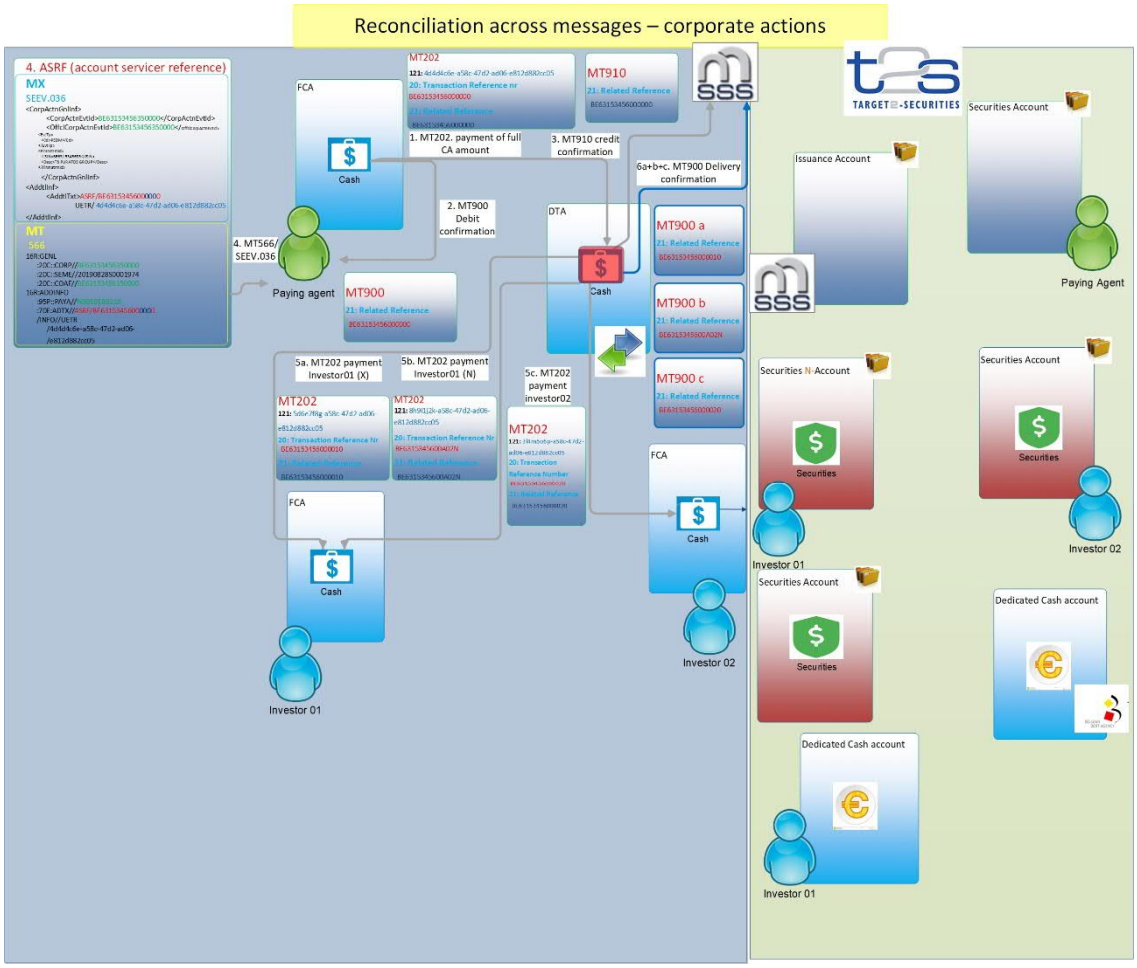
4. The NBB-SSS sends the MT566 (or its MX equivalent seev.036) with the ASRF reference and UETR to the Paying Agent.



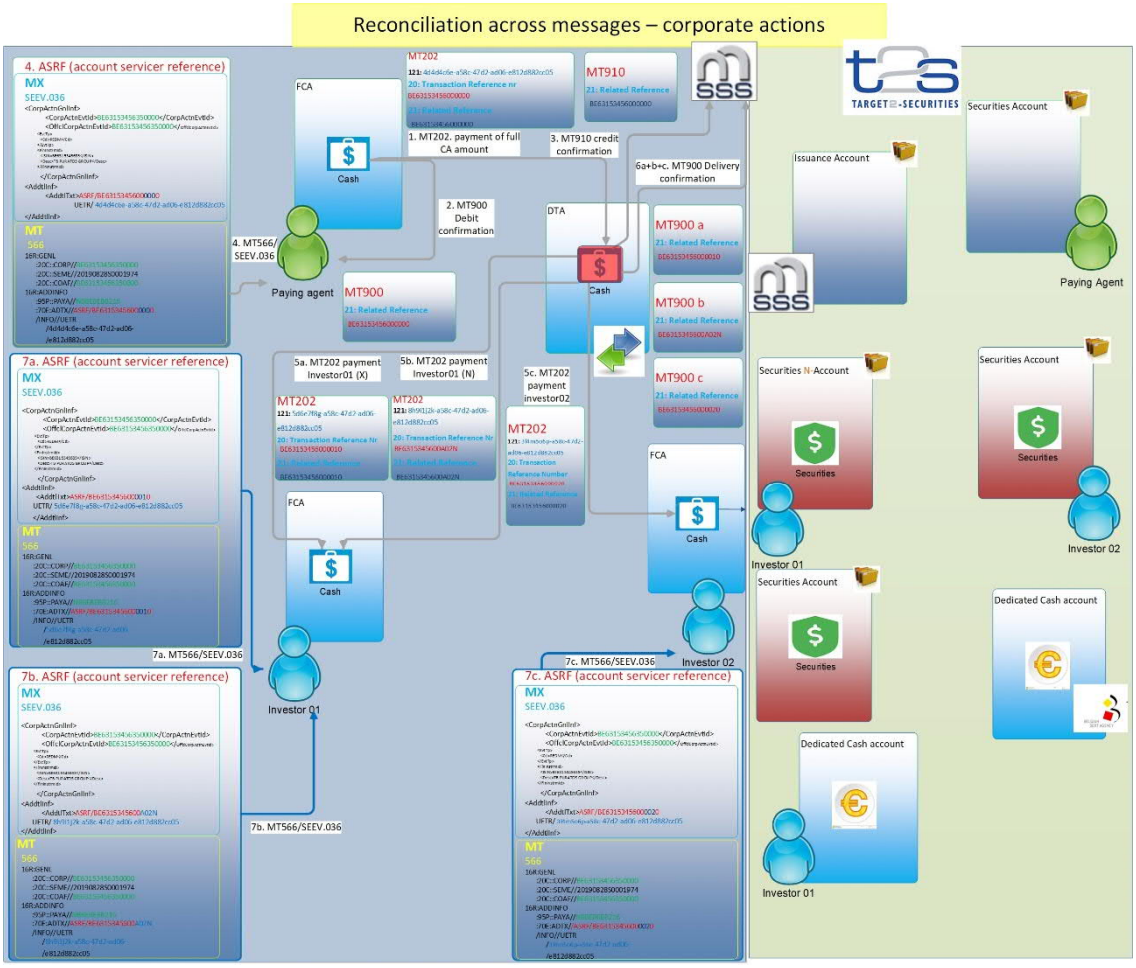
5. The NBB-SSS instructs the MT202's for debiting the Paying Agent's DTA and crediting the designated FCA of the investors. These MT202s are created per position. If a participant has different positions on different accounts, there will be an MT202 per position, with a unique ASRF reference and UETR (header field 121) per position. In this example investor 01 receives 2 MT202's, i.e. a) for the position on the securities X-account and b) for the position on the N-account. An ASRF that is linked with an N-account ends with N.



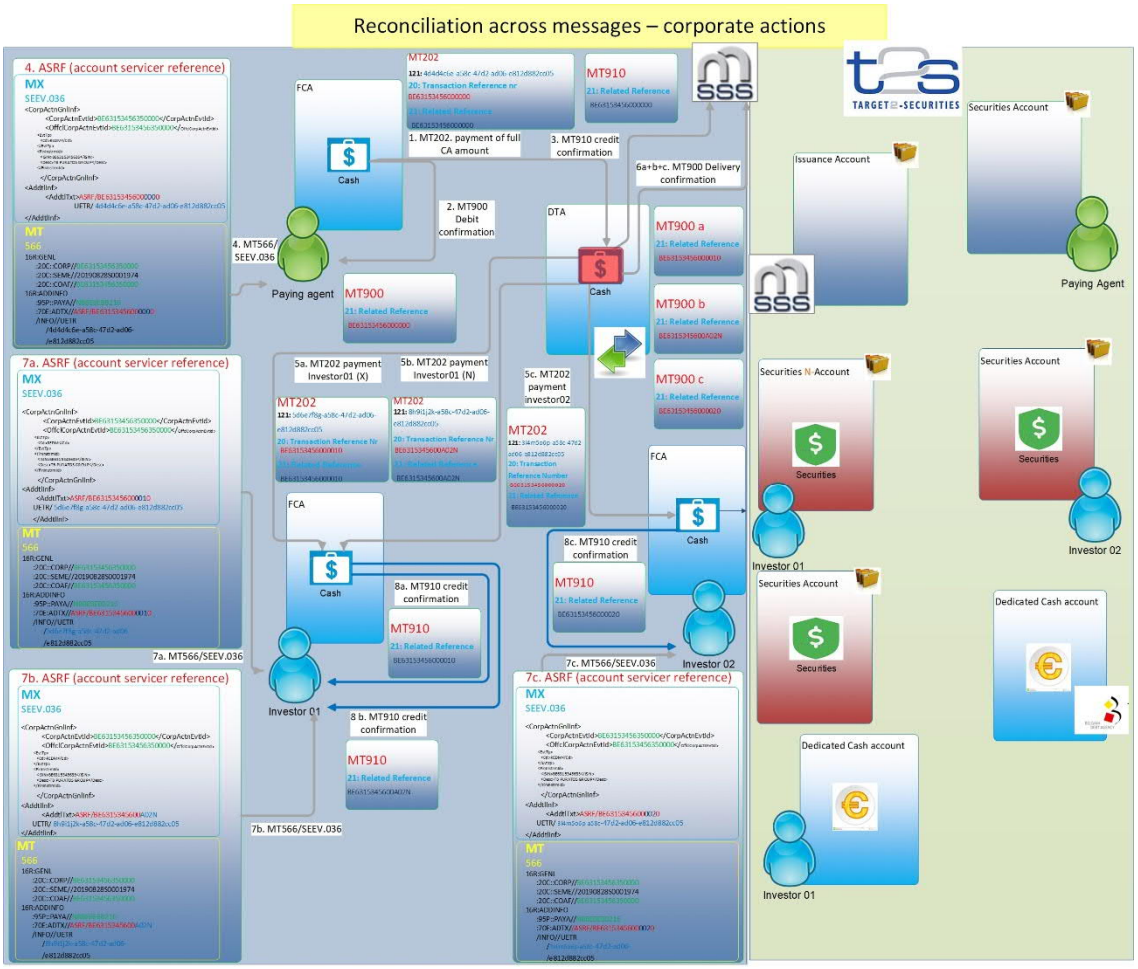
6. The NBB-SSS receives for each instructed MT202 an MT900 confirmation of debit with the unique ASRF in field 21 for the transfer account.



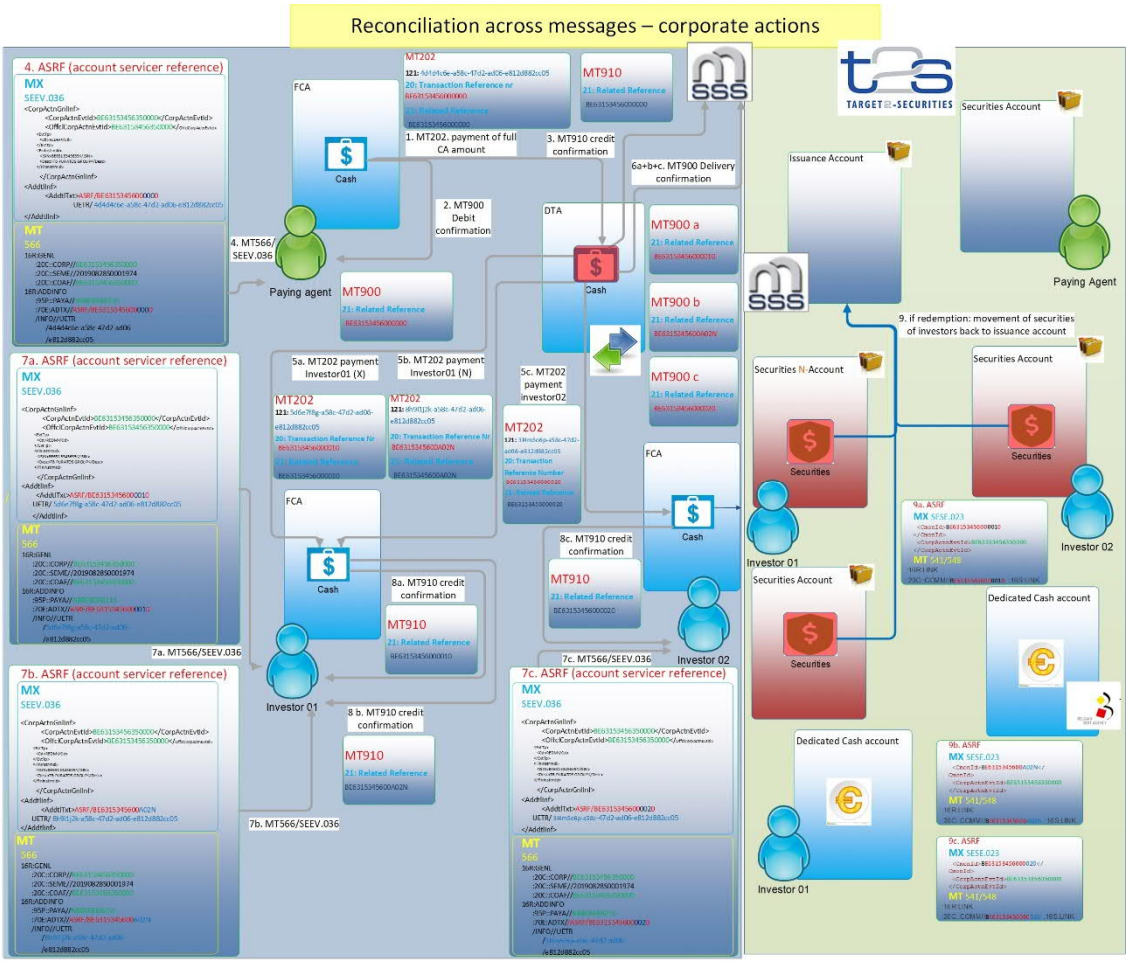
7. The NBB-SSS generates an MT566 (or its MX equivalent seev.036) for each received MT900. These MT566s contain the unique ASRF references and the UETR.



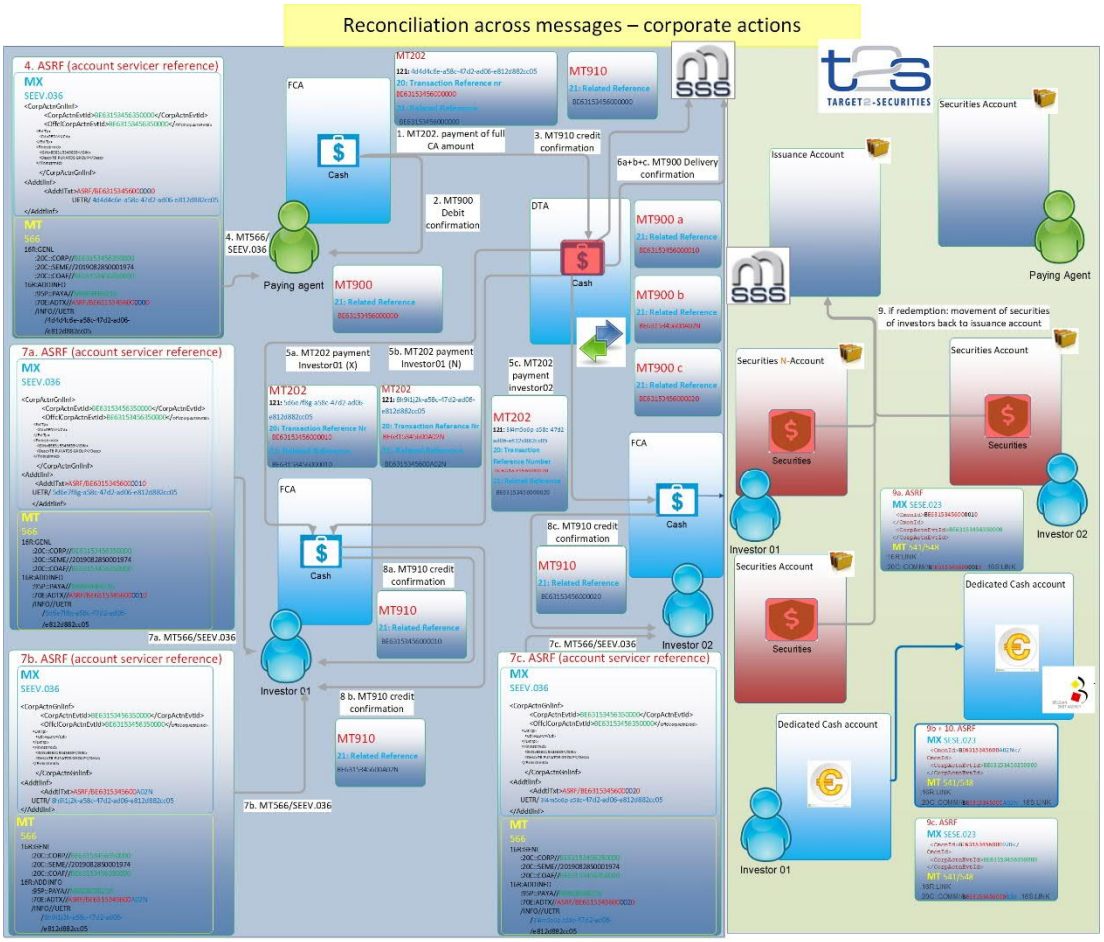
8. The Participants having a position in the securities receive the MT910 confirmation of credit with the unique ASFR reference in field 21, if their Foreign currency cash Provider supports this feature.



9. In case of a redemption the positions are moved from the accounts of Participants having a position in the securities to the issuance accounts with the unique ASFR.



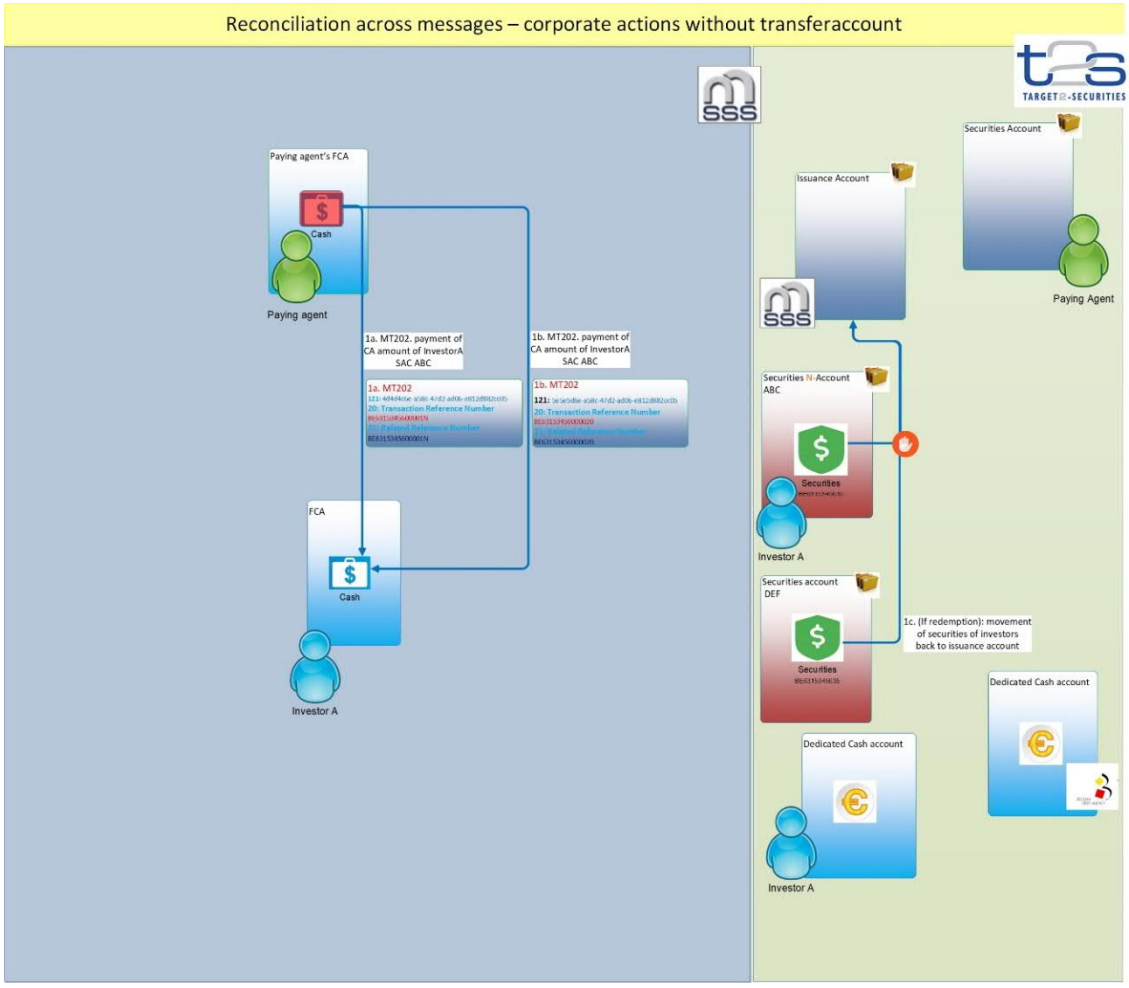
10. If an N-account is involved, the Withholding Tax Transaction also holds the unique ASRF reference in the CMONId field[3].



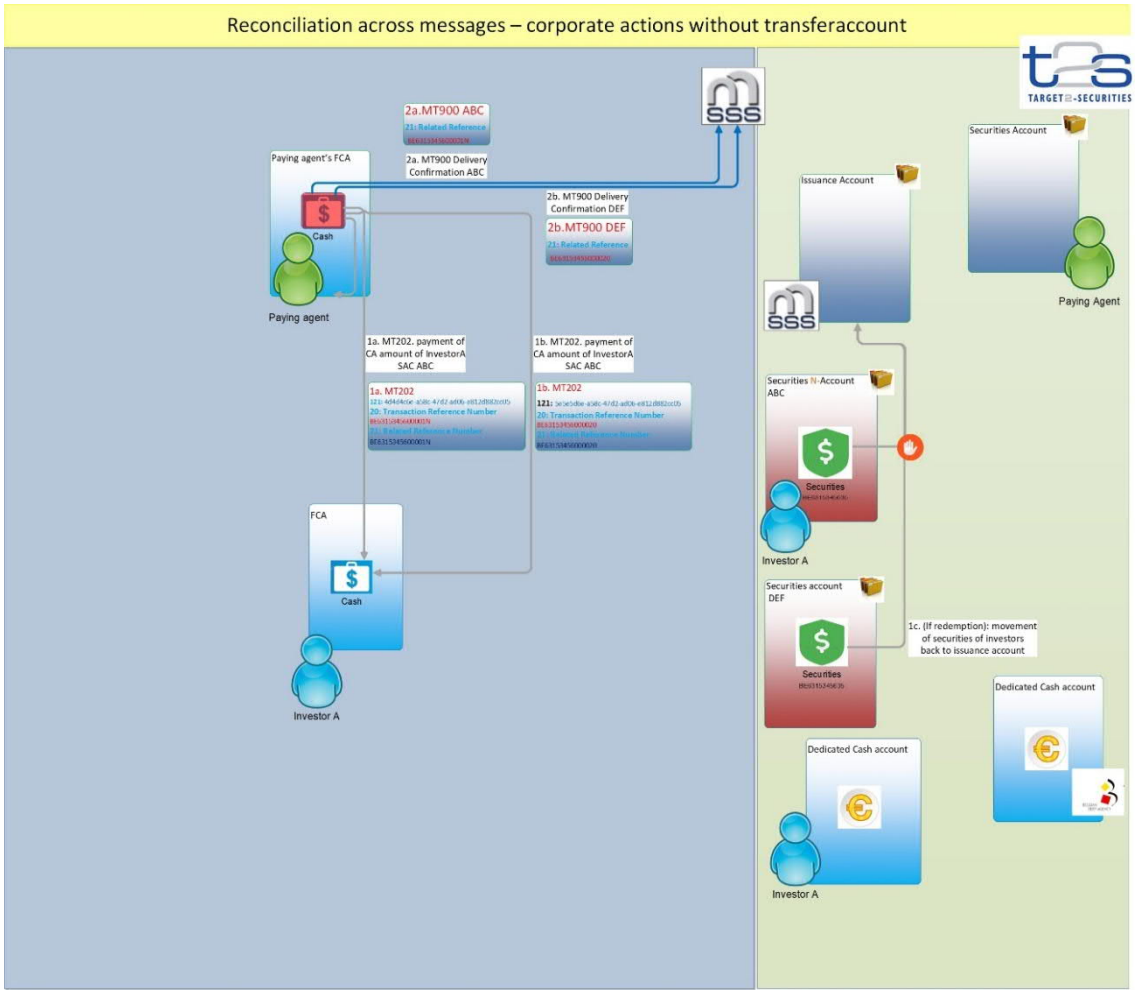
[3] Analogue with Withholding Tax Transaction in T2S settlement currencies where CMonID holds the T2S reference of the transactions between the investor and the issuance account (PFOD (coupon) or DVP (redemption)).

3.2.2 Without Dedicated Transfer account

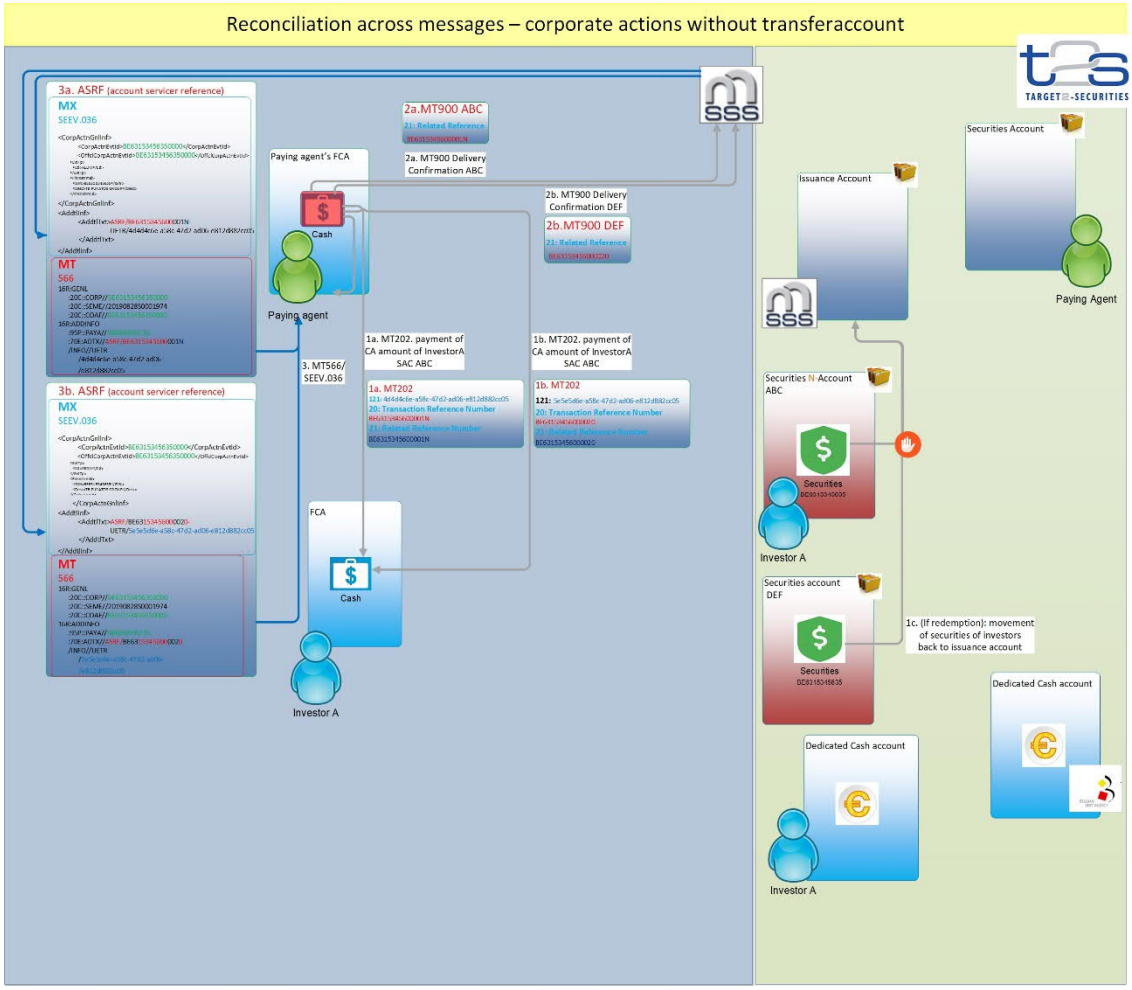
1. At End of Day the system detects a CA in Foreign currencies for which the NBB-SSS provides the Foreign currency financial service and the Paying Agent has chosen not to use a Dedicated Transfer Account for. Per position NBB-SSS sends out an MT202 to the designated FCA of the Paying Agent for the CA amount of each position to credit each investor FCA.
   Fields 20 and 21 of the MT202 hold the ASRF (Account Servicer Reference, see annex 2). The ASRF is unique per CA movement. This reference allows the reconciliation between the cash movements and the messages sent out by the NBB-SSS (MT566 or seev.036) by all parties involved. In the example below, there was also a position on an N account. An N-account linked ASRF will always end on N in the last position.
   Field 121 of the MT202 will reflect the UETR that also will be found in the MT566/seev.036. This UETR allows reconciliation as well, but also the possible tracking of the payment though SWIFT GPI.
   In case of redemption, the movement of the securities from investors account toward the issuance account is instructed and put on hold. This sese.023 movement also contains the ASRF code (no UETR).



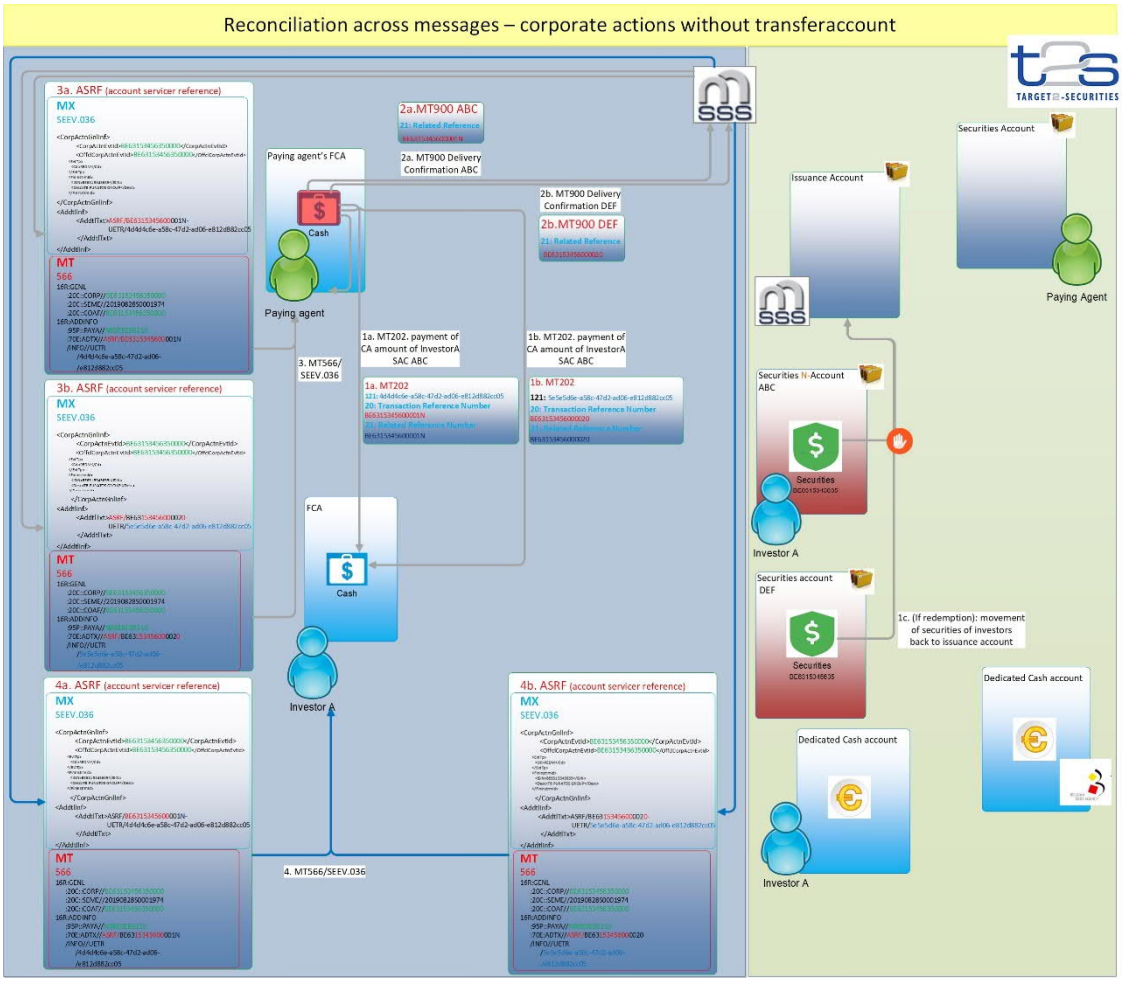
2. NBB-SSS receives, together with the Paying Agent, the MT900 confirmation of debit with the ASRF reference in field 21. This field is a copy from MT202's field 20.



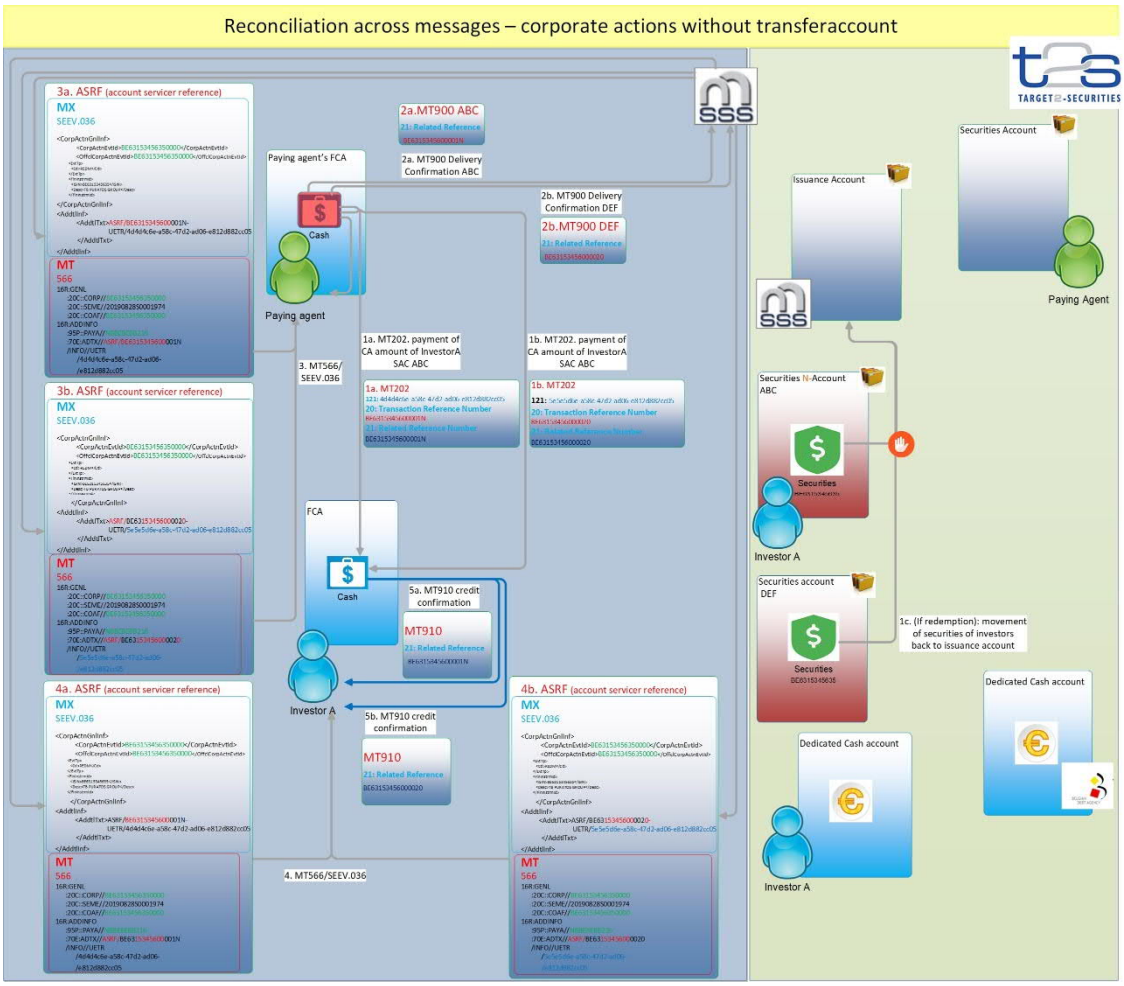
3. NBB-SSS will create an MT566/SEEV.036 per MT900 received and send it to the Paying Agent. The the MT566/SEEV.036 will contain the ASRF and UETR references of the MT202 sent out in step 1.



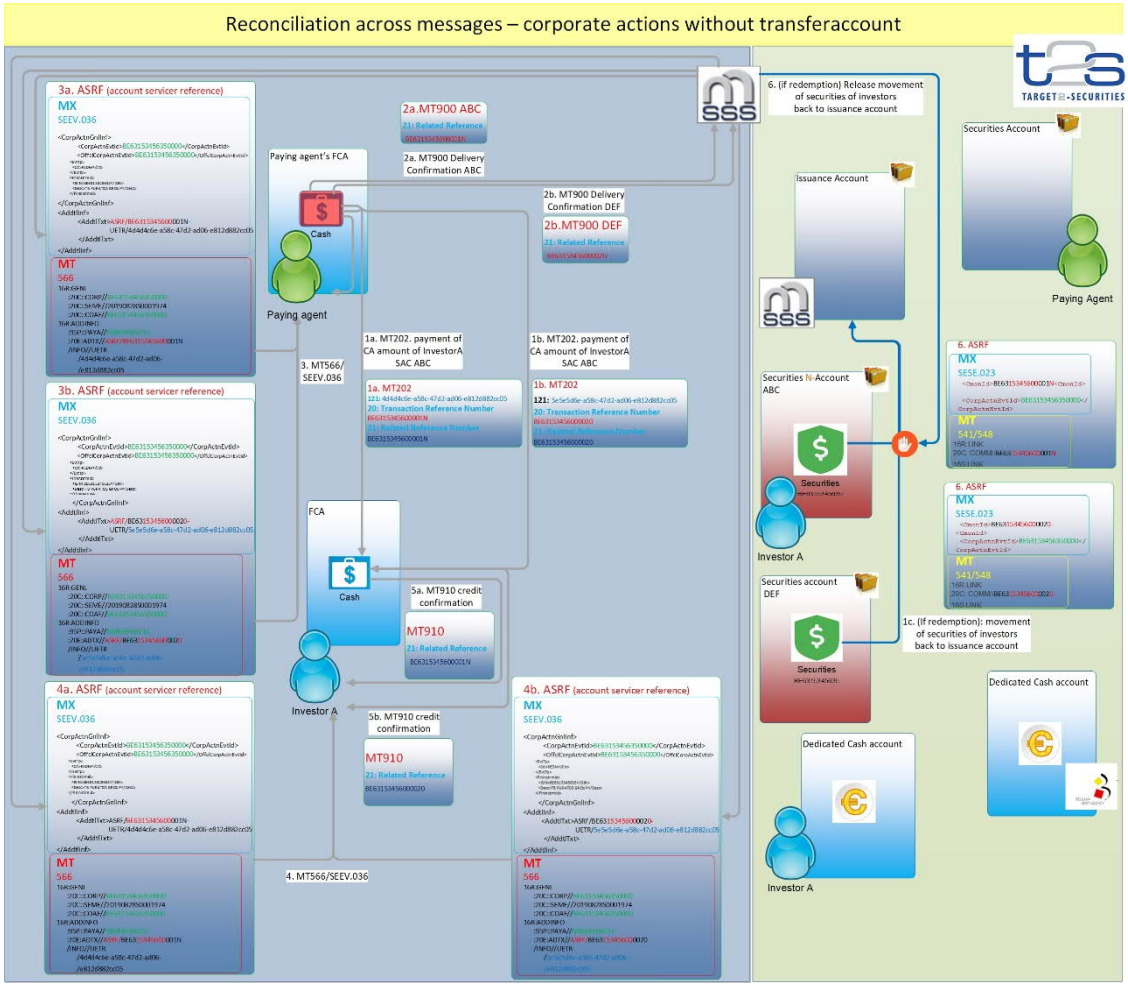
4. Simultaneous with step 3, NBB-SSS generates an MT566 (or its MX equivalent seev.036) for each investor position that is sent to the investors. The MT566s contain the unique ASRF and UETR references as well.



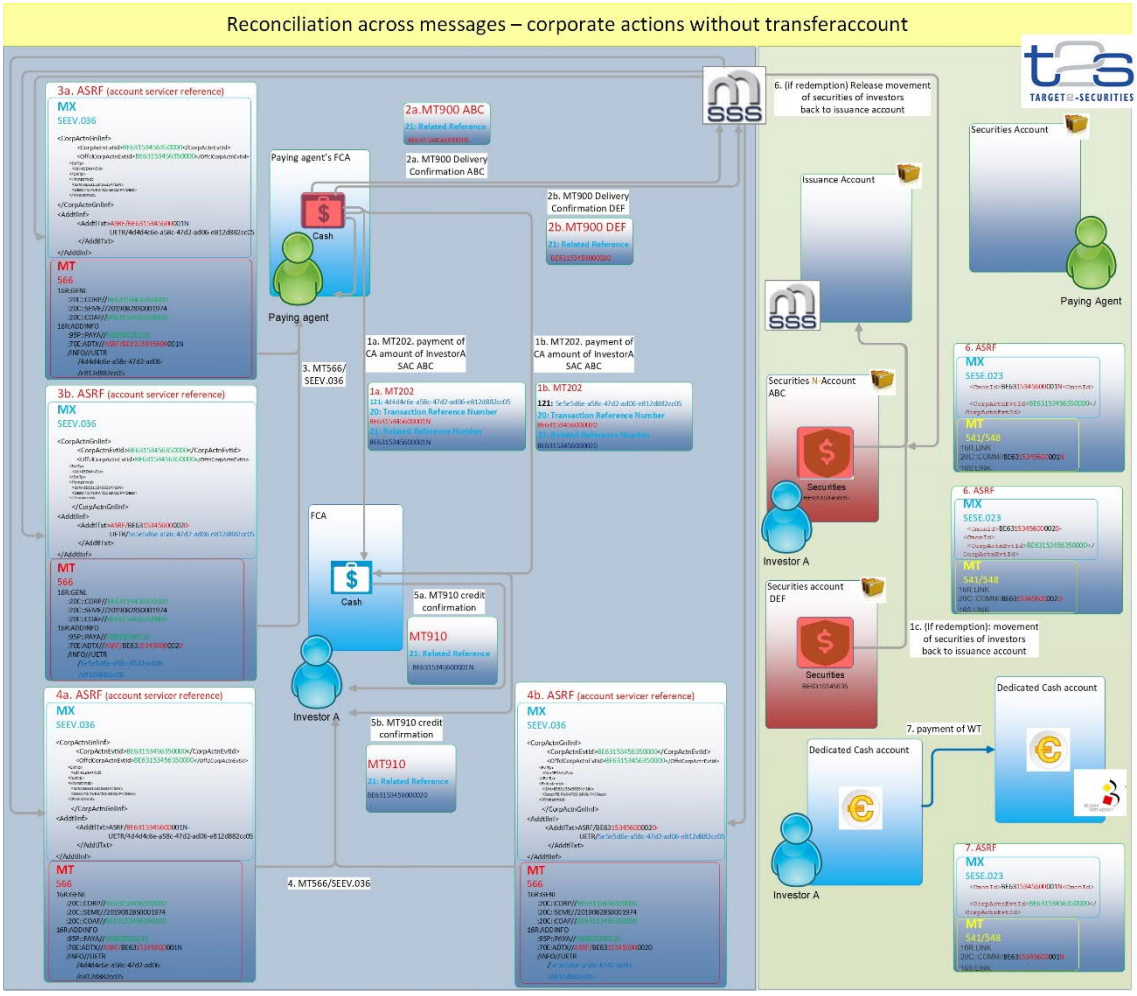
5. When the cash is credited on its FCA, and if it's Foreign currency cash Provider is supporting this functionality, the investor will receive an MT910 for each credit, containing the ASRF in field 21 of the CA movement, allowing the investor to reconcile with the MT566/SEEV.036 received from NBB-SSS. This ASRF is deducted from the (step 1) MT202's field 21.



6. In case of a redemption, NBB-SSS will release the delivery of the positions from the accounts of Participants having a position in the securities to the issuance accounts. The sese.023 will contain the ASRF as well.



7. If an N-account is involved, the Withholding Tax Transaction also holds the unique ASRF reference in the CMONId field[4].



[4] Analogue with Withholding Tax Transaction in T2S settlement currencies where CMonID holds the T2S reference of the transactions between the investor and the issuance account (PFOD (coupon) or DVP (redemption)).

4 Actions required from the Participant

4.1 Declaring Foreign Currency Cash account (FCA) and Dedicated Transfer Account (DTA)

Each Participant acting as buyer

- needs to designate an FCA (see Terms and Conditions governing the participation in the NBB-SSS, Article 4.3) and shall give NBB-SSS a mandate (PoA-Annex 18.8) to instruct debit movements on this account. The FCA can be held with the Foreign currency cash Provider of its choice. NBB-SSS must be able to instruct MT202's upon it and receive MT900 messages filled out according to market practices (MT202's field 20 must be reproduced in MT900's field 21 as explained above).
- must be able to instruct a message FOP with cash fields filled out (see also Article 5.3.1).

Each Participant acting as seller

- shall designate an FCA (see Terms and Conditions governing the participation in the NBB-SSS Article 4.3)to allow NBB-SSS to instruct credit movements to this account. The FCA can be held with the Foreign currency cash Provider of its choice. In the absence of a designated FCA, the transaction will be kept pending and the Participant will be fined for keeping this transaction unsettled (hold) (see Terms and conditions governing the participation in the NBB-SSS - Article 8.2.1.4.).
- must be able to instruct a message FOP with cash fields filled out. (see also Article 5.3.2).

Each Participant acting as investor (= Participant having a position in the securities)

- shall designate an FCA (see Terms and Conditions governing the participation in the NBB-SSS Article 4.3) to allow NBB-SSS to instruct Corporate actions (CA) credit movements. The FCA can be held with the Foreign currency cash Provider of its choice. In the absence of designated FCA, the Corporate action will remain unsettled. The investor will inform NBB-SSS of its account through the proper channels (T&C annex 27.b) after which Ramses will automatically transfer the CA amount.

Each Participant acting as Paying Agent

- shall designate an FCA (see Article 4.3 Terms and Conditions governing the participation in the NBB-SSS) and shall give NBB-SSS a mandate (PoA-annex 18.8) to instruct Corporate actions (CA) debit movements from this account. The FCA can be held with the Foreign currency cash Provider of its choice. NBB-SSS must be able to instruct MT202's upon it and receive MT900 messages filled out according to market practices (MT202's field 20 must be reproduced in MT900's field 21 as explained above).
- Shall designate a Dedicated Transfer Account (DTA) (see Article 4.3.1 Terms and Conditions governing the participation in the NBB-SSS) and shall give NBB-SSS a mandate (PoA-annex 18.8) to instruct Coporate Actions (CA) debit movements from this account. The DTA can be held with the Foreign currency cash Provider of its choice and must have NBB-SSS Corporate actions as sole purpose. NBB-SSS must be able to instruct MT202's upon it and receive both MT910 and MT900 messages filled out according to market practices (MT202's field 20 must be reproduced in MT900's field 21 as explained above).
    - When participants acting as Paying Agent opt for the Foreign currency financial service, the opening and the designation of an FCA and a DTA is a prerequisite.

4.2 Foreign currency cash Provider and Foreign currency cash account at different levels

The Participant can define the Foreign cash account static data through annex 27b at following levels:

- currency
- debit[5]/credit of cash
- transactions/Corporate actions
- Participant level (default)/securities account level (when different from the account submitted at Participant level).

4.3 Corporate actions

4.3.1 Unique reference ASRF

4.3.1.1 Compiling a unique reference

In order to link all the messages, a Corporate action needs a unique ASRF-reference for the issuer and per investor's position. This reference will be a 16 characters string, see annex 2 (5.2).

4.3.1.2 Usage of unique ASRF-reference

sese.023 (redemption – withholding tax)	MT566	MT202	MT900	MT910
ASRF-field (account servicer reference) CMONID	ASRF field (field 70)	Field 20 Field 21	Field 21	Field 21
	Cashmove Cashparties 20C reference			

4.3.2 Generation of Corporate actions on Record Date

At End of Day (18:00 CET – 18:45 CET) on Record Date, NBB-SSS generates the next day coupons, poolfactors or redemptions in the Foreign currency assets for which the Paying Agent has opted in. This timing is parameter driven and can be postponed to a later time, e.g. in case of USD, where the currency's timezone is following the CET timezone.

[5] The debit of corporate actions is reserved for Paying Agents and is possible at participant level only.

4.3.2.1 NBB-SSS creates WT transactions for coupons and redemptions and puts them on hold

4.3.2.2 NBB-SSS instructs cash transfer MT202

NBB-SSS debits the Foreign currency cash account of the Paying Agent. The instruction contains the ASRF-reference.

In case of usage of a DTA:
- one MT202 for the whole redemption,
- one MT202 for the whole poolfactor,
- one MT202 for the whole coupon,
- Field 20 contains unique Paying Agent ASRF-reference.

In case of no usage of a DTA: per investor-account position
- one MT202 for the redemption,
- one MT202 for the poolfactor,
- one MT202 for the coupon,
- Field 20 contains unique Paying Agent ASRF-reference.

4.3.2.3 In case of redemption NBB-SSS creates sese.023

The movement from Investor account towards Issuance account is created.

The sese.023 holds the unique ASRF reference and is put on hold.

4.3.2.4 Credit on transfer account triggers MT900 – MT910 – MT566 to the Paying Agent

In case of usage of a DTA:

The MT900 from the Paying Agent's Foreign currency cash account is ignored.

The MT910 from the DTA triggers:

- Creation of the MT566 to the Paying Agent with the unique reference in both ASRF field and CASHMOVE.
- Creation of the MT202 towards the investors. The MT202's will debit the DTA and credit the investor accounts with the unique ASRF reference per payment in field 20 per investor position, e.g. if the Participant holds positions on five accounts, then five MT202's will be created. Even if all five SAC are linked to the same Foreign currency cash account.

Each MT900 for the DTA holds the unique ASRF reference in field 21 and triggers:

- The creation of the MT566 to the investor with the unique reference in both ASRF field and CASHMOVE.

In case of no usage of a DTA:

The MT900 from the Paying Agent's Foreign currency cash Account (FCA) triggers.

- Creation of the MT566 to the Paying Agent and the investors with the unique reference in both ASRF field and CASHMOVE.

In case of redemption: release of the sese.023 from the investor account to the issuance account

4.4 End of Day functions

4.4.1 Cash Forecast

4.4.1.1 Cash Forecast through Swift: camt.052

Each FCA is linked to one accountholder. At the Start Of Day, the accountholder receives the cash forecast of his account.

An accountholder of an FCA has the possibility to act as a Foreign currency Paying Agent. Consequently, Securities Accounts of other Participants may be linked to the FCA of the Foreign currency Paying Agent.

In this case the cash forecast for the Foreign currency Paying Agent will be aggregated for all securities accounts that are linked to this FCA.

The other Participants who are using the FCA of another Participant, are considered sub-owner; They can opt for receiving the camt.052 related to transactions on their accounts only.

At the moment of editing the first version of the Manual, the camt.052 is under construction. In a future version an example will be added in the annexes.

4.4.1.2 Cash Forecast in GUI

The cash forecast will also be made available through the RAMSES GUI.

At the moment of editing the first version of the Manual, this RAMSES GUI screen is under construction. In a future version an example will be added in the annexes.

4.4.1.3 Scope

The cash forecast will cover the cash needs of the five upcoming business days, where per business day and per currency the total debit and credit amounts will be given for:

- Transactions that should settle on that business day. For the first upcoming business day this includes pending unsettled transactions with ISD preceding that day.
- Unmatched instructions that should settle on that business day
- Corporate actions for that business day.

Paying Agents of Foreign currency assets shall not net a to be debited corporate action amount with incoming cash flows but provide the total CA amount to be debited.

When the NBB-SSS receives the End of Day statement for the Foreign currency cash account of the Participant (MT950 or camt.053) this position shall also be reflected in the cash forecast, making it more accurate.

4.5 Administrative fines

4.5.1 Timing

A FOP transaction is considered to be timely settled if settled by FOP cut-off at ISD (Intended Settlement Date) of the transaction, i.e. 18:00 CET.

However, the Foreign currency cash leg needs to settle as well and before the FOP transaction. The Foreign currency cash cut-off at ISD is 15:00 CET. Consequently, the securities must be provided before the Foreign currency cash cut-off has been reached.

4.5.2 MONY

If the Foreign currency cash transfer cannot be made on ISD and the securities position is confirmed (semt.015) before the Foreign currency cash cut-off, the reason for non-settlement is 'MONY' (T&C Art. 8.2.1.2).

4.5.3 LACK

If at ISD the transaction remains unsettled and the securities position was only confirmed (semt.015) after the cash cut-off, the reason for non-settlement is LACK (T&C Art. 8.2.2.1).

5 Annexes

5.1 Annex 1 – currencies of which exchange rates are published by the ECB

Eligible Foreign currencies for NBB-SSS Foreign trades	
GBP - Pound Sterling	INR - Indian Rupee
NOK - Norwegian Krona	ISK - Icelandic Krona
USD - US Dollar	JPY - Japanese Yen
	KRW - Korean Won
AUD - Australian Dollar	MXN - Mexican Peso
BGN - Bulgarian Lev	MYR - Malaysian Ringgit
BRL - Brazilian Real	NZD - New Zealand Dollar
CAD - Canadian Dollar	PHP - Philippine Peso
CHF - Swiss Franc	PLN - Polish Zloty
CHY - Chinese Yuan Renminbi	RON - Romanian Leu
CZK - Czech Koruna	RUB - Russian Ruble
HKD - Hong Kong Dollar	SEK - Swedish Krona
HRK - Croatian Kuna	SGD - Singapore Dollar
HUF - Hungarian Forint	THB - Thai Baht
IDR - Indonesian Rupiah	TRY - Turkish Lira
ILS - Israeli Shekel	ZAR - South African Rand

5.2 Annex 2 – ASRF compilation

Compilation of the ASRF (account servicer reference)

Position	Description	example
1-10	First ten chars of the isin	BE63155093
11-12	Corporate action Redemption 00 Coupon 1 01 Coupon 2 02 Coupon 100 A1 …	00
13-15	Sequence of creation of payment in Ramses for this CA (paying agent: 000 Investor position 1: 001 Investor position 1000:A00)	002
16	Standard: 0 / N (in case of N-account)	0

5.3 Annex 3 - Overview of used swift messages: equivalent MT vs MX

Action	Actor	MT message	**MX message**
Buy instruction	Buying participant	MT540	sese.023
Sell instruction	Selling participant	MT542	sese.023
Matching of transaction	T2S	MT548	sese.024
Transaction on CoSD hold	T2S		semt.014
Reservation of asset	T2S		semt.015
Cash transfer from “to debit” account to “to credit” account	NBB-SSS	MT202	pacs.009
Confirmation of debit	Foreign currency Provider	MT900	camt.054
Confirmation of credit	Foreign currency Provider	MT910	camt.054
Release of transaction	T2S		sese.030 + sese.031
Settlement of transaction	T2S	MT544 – MT546	sese.025
Statement of Account (EOD)	Foreign currency Provider	MT950	camt.053
Cash forecast	NBB-SSS		camt.052
Corporate action notification	NBB-SSS	MT564	seev.031
Corporate action confirmation	NBB-SSS	MT566	seev.036

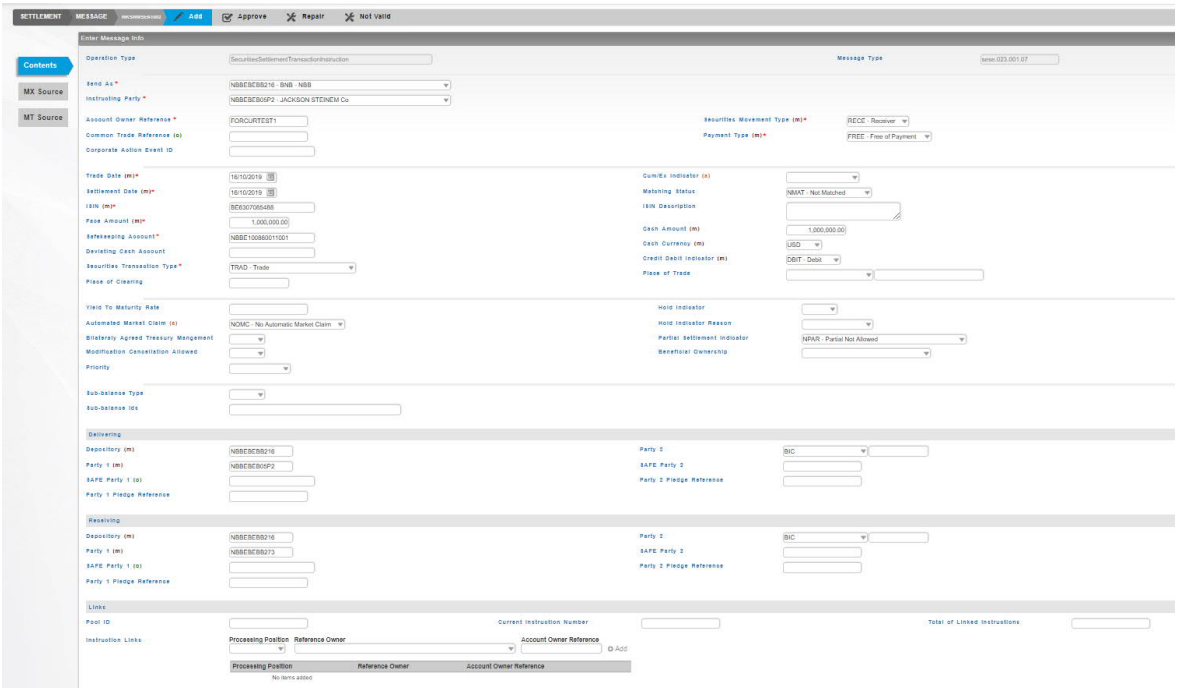
5.4 Annex 4 - Examples

5.4.1 DVP in foreign Currencies

5.4.1.1 Buy instruction FOP with cash

5.4.1.1.1 INPUT

5.4.1.1.1.1 IN RAMSES



5.4.1.1.1.2 BY MT540 – RECEIVE FREE OF PAYMENT WITH CASH

:16R:GENL
:20C::SEME//FORCURTEST1
:23G:NEWM
:16S:GENL
:16R:TRADDET
:98A::SETT//20191016
:98A::TRAD//20191016
:35B:ISIN BE6307085488
:16S:TRADDET
:16R:FIAC
:36B::SETT//FAMT/1000000,0
:97A::SAFE//NBBE100860011001
:16S:FIAC
:16R:SETDET
:22F::STCO//NPAR
:22F::STCO//NOMC
:22F::SETR//TRAD
:16R:SETPRTY
:95P::PSET//NBBEBEBB216
:16S:SETPRTY
:16R:SETPRTY
:95P::DEAG//NBBEBEBB273
:97A::SAFE//NBBE100860021001
:16S:SETPRTY
:16R:SETPRTY
:95P::REAG//NBBEBEB05P2
:97A::SAFE//NBBE100860011001
:16S:SETPRTY
:16R:AMT
:19A::SETT//USD1000000,0
:16S:AMT
:16S:SETDET

5.4.1.1.1.3 BY SESE.023 – RECEIVE FREE OF PAYMENT WITH CASH

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEB05P2</BICFI>
               <ClrSysMmbId>
                  <ClrSysId>
                     <Prtry>T2S</Prtry>
                  </ClrSysId>
                  <MmbId>NBBSSS</MmbId>
               </ClrSysMmbId>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>FORCURTEST1</BizMsgIdr>
      <MsgDefIdr>sese.023.001.07</MsgDefIdr>
      <CreDt>2019-10-16T15:28:34Z</CreDt>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.023.001.07">
      <SctiesSttlmTxInstr>
         <TxId>FORCURTEST1</TxId>
         <SttlmTpAndAddtlParams>
            <SctiesMvmntTp>RECE</SctiesMvmntTp>
            <Pmt>FREE</Pmt>
         </SttlmTpAndAddtlParams>
         <TradDtls>
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </TradDt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
         </TradDtls>
         <FinInstrmId>
            <ISIN>BE6307085488</ISIN>
         </FinInstrmId>
         <QtyAndAcctDtls>
            <SttlmQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttlmQty>
            <SfkpgAcct>
               <Id>NBBE100860011001</Id>
            </SfkpgAcct>
         </QtyAndAcctDtls>
         <SttlmParams>
            <SctiesTxTp>
               <Cd>TRAD</Cd>
            </SctiesTxTp>
```

```
            <SttlmTxCond>
               <Cd>NOMC</Cd>
            </SttlmTxCond>
            <PrtlSttlmInd>NPAR</PrtlSttlmInd>
         </SttlmParams>
         <DlvrgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEBB273</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860021001</Id>
               </SfkpgAcct>
            </Pty1>
         </DlvrgSttlmPties>
         <RcvgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEB05P2</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860011001</Id>
               </SfkpgAcct>
            </Pty1>
         </RcvgSttlmPties>
         <SttlmAmt>
            <Amt Ccy="USD">1000000</Amt>
            <CdtDbtInd>DBIT</CdtDbtInd>
         </SttlmAmt>
      </SctiesSttlmTxInstr>
   </Document>
</Saa:Body>
```

5.4.1.1.2 OUTPUT

5.4.1.1.2.1 SESE.024 – TO BUYER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEB05P2</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
```

```
    </To>
    <BizMsgIdr>1077594624000</BizMsgIdr>
    <MsgDefIdr>sese.024.001.08</MsgDefIdr>
    <CreDt>2019-10-17T12:49:21Z</CreDt>
    <Prty>2019101700000250</Prty>
  </AppHdr>
  <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.024.001.08">
    <SctiesSttlmTxStsAdvc>
      <TxId>
        <AcctOwnrTxId>FORCURTEST1</AcctOwnrTxId>
        <MktInfrstrctrTxId>1910160298256173</MktInfrstrctrTxId>
      </TxId>
      <SttlmSts>
        <Flng>
          <Rsn>
            <Cd>
              <Cd>CYCL</Cd>
            </Cd>
            <AddtlRsnInf>AwaitingNextSettlementCycle</AddtlRsnInf>
              </Rsn>
        </Flng>
      </SttlmSts>
      <TxDtls>
        <SfkpgAcct>
          <Id>NBBE100860011001</Id>
        </SfkpgAcct>
        <FinInstrmId>
          <ISIN>BE6307085488</ISIN>
        </FinInstrmId>
        <SttlmQty>
          <Qty>
            <FaceAmt>1000000</FaceAmt>
          </Qty>
        </SttlmQty>
        <SttlmAmt>
          <Amt Ccy="USD">1000000</Amt>
          <CdtDbtInd>DBIT</CdtDbtInd>
        </SttlmAmt>
        <SttlmDt>
          <Dt>
            <Dt>2019-10-16</Dt>
          </Dt>
        </SttlmDt>
        <TradDt>
          <Dt>
            <Dt>2019-10-16</Dt>
          </Dt>
        </TradDt>
        <SctiesMvmntTp>RECE</SctiesMvmntTp>
        <Pmt>FREE</Pmt>
        <SttlmParams>
          <SttlmTxCond>
            <Cd>NOMC</Cd>
          </SttlmTxCond>
          <SctiesTxTp>
            <Cd>TRAD</Cd>
          </SctiesTxTp>
          <PrtlSttlmInd>NPAR</PrtlSttlmInd>
        </SttlmParams>
        <RcvgSttlmPties>
          <Dpstry>
            <Id>
              <AnyBIC>NBBEBEBB216</AnyBIC>
            </Id>
          </Dpstry>
          <Pty1>
            <Id>
              <AnyBIC>NBBEBEB05P2</AnyBIC>
            </Id>
```

```
                  <SfkpgAcct>
                     <Id>NBBE100860011001</Id>
                  </SfkpgAcct>
               </Pty1>
            </RcvgSttlmPties>
            <DlvrgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEBB273</AnyBIC>
                  </Id>
                  <SfkpgAcct>
                     <Id>NBBE100860021001</Id>
                  </SfkpgAcct>
               </Pty1>
            </DlvrgSttlmPties>
         </TxDtls>
         <SplmtryData>
            <PlcAndNm>/Document/SctiesSttlmTxStsAdvc/TxId</PlcAndNm>
            <Envlp>
               <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">
                     <SctiesSttlmSD1>
                     <RltdTxId>0119052141062000</RltdTxId>
                  </SctiesSttlmSD1>
               </Document>
            </Envlp>
         </SplmtryData>
      </SctiesSttlmTxStsAdvc>
   </Document>
</Saa:Body>
```

5.4.1.1.2.2 MT548 – TO BUYER

```
:16R:GENL
:20C::SEME//1077552206000
:23G:INST
:98C::PREP//20191016173057
:16R:LINK
:20C::RELA//FORCURTEST1
:16S:LINK
:16R:LINK
:20C::MITI//0119052141062000
:16S:LINK
:16R:LINK
:20C::PCTI//1910160298256173
:16S:LINK
:16R:STAT
:25D::SETT//PEND
:16R:REAS
:24B::PEND//FUTU
:70D::REAS//AwaitingSettlementDate
:16S:REAS
:16S:STAT
:16R:STAT
:25D::IPRC//PACK
:16R:REAS
:24B::PACK//NARR
:70D::REAS//NORE
:16S:REAS
:16S:STAT
:16S:GENL
:16R:SETTRAN
:35B:ISIN BE6307085488
:36B::SETT//FAMT/1000000,0
:19A::SETT//USD1000000,0
:97A::SAFE//NBBE100860011001
```

```
:22F::SETR//TRAD
:22H::REDE//RECE
:22H::PAYM//FREE
:22F::STCO//NPAR
:22F::STCO//NOMC
:98A::TRAD//20191016
:98A::SETT//20191016
:16R:SETPRTY
:95P::PSET//NBBEBEBB216
:16S:SETPRTY
:16R:SETPRTY
:95P::DEAG//NBBEBEBB273
:97A::SAFE//NBBE100860021001
:16S:SETPRTY
:16R:SETPRTY
:95P::REAG//NBBEBEB05P2
:97A::SAFE//NBBE100860011001
:16S:SETPRTY
:16S:SETTRAN
```

5.4.1.1.2.3 SESE.028 – ALLEGEMENT (TO THE COUNTERPARTY)

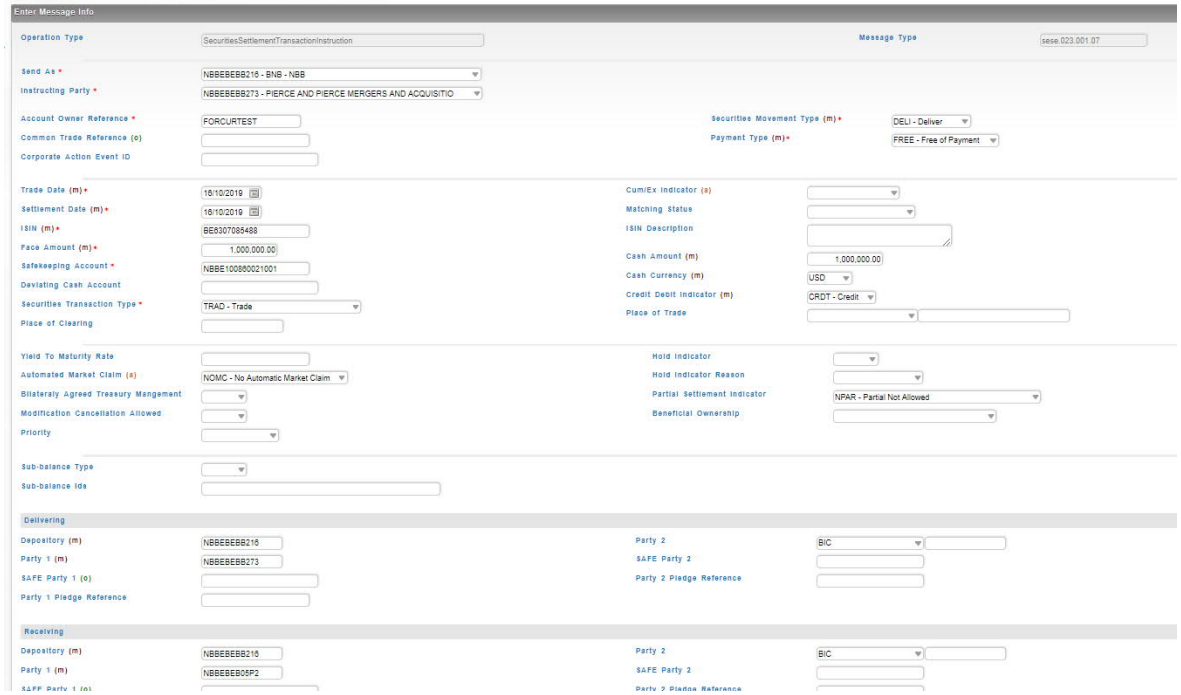
```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077594624000</BizMsgIdr>
      <MsgDefIdr>sese.028.001.06</MsgDefIdr>
      <CreDt>2019-10-16T10:20:09Z</CreDt>
      <Prty>2019091700000010</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.028.001.06">
      <SctiesSttlmTxAllgmtNtfctn>
         <TxId>1909170296843546</TxId>
         <SttlmTpAndAddtlParams>
            <SctiesMvmntTp>RECE</SctiesMvmntTp>
            <Pmt>FREE</Pmt>
         </SttlmTpAndAddtlParams>
         <MktInfrstrctrTxId>
            <Id>1909170296841799</Id>
         </MktInfrstrctrTxId>
         <TradDtls>
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </TradDt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
         </TradDtls>
```

```
            <FinInstrmId>
               <ISIN> BE6307085488</ISIN>
            </FinInstrmId>
            <QtyAndAcctDtls>
               <SttlmQty>
                  <FaceAmt>1000000</FaceAmt>
               </SttlmQty>
               <AcctOwnr>
                  <Id>
                     <AnyBIC>NBBEBEB05P2</AnyBIC>
                  </Id>
               </AcctOwnr>
               <SfkpgAcct>
                  <Id>NONREF</Id>
               </SfkpgAcct>
            </QtyAndAcctDtls>
            <SttlmParams>
               <SctiesTxTp>
                  <Cd>TRAD</Cd>
               </SctiesTxTp>
               <PrtlSttlmInd>NPAR</PrtlSttlmInd>
            </SttlmParams>
            <DlvrgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEB05P2</AnyBIC>
                  </Id>
               </Pty1>
            </DlvrgSttlmPties>
            <RcvgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEBB273</AnyBIC>
                  </Id>
                  <SfkpgAcct>
                     <Id>NBBE100860021001</Id>
                  </SfkpgAcct>
               </Pty1>
            </RcvgSttlmPties>
            <SttlmAmt>
               <Amt Ccy="USD">1000000</Amt>
               <CdtDbtInd>DBIT</CdtDbtInd>
            </SttlmAmt>
         </SctiesSttlmTxAllgmtNtfctn>
      </Document>
   </Saa:Body>
```

5.4.1.2 Sell instruction FOP with cash

5.4.1.2.1 INPUT

5.4.1.2.1.1 IN RAMSES



5.4.1.2.1.2 MT542 – DELIVER FREE OF PAYMENT WITH CASH

```
:16R:GENL
:20C::SEME//FORCURTEST
:23G:NEWM
:16S:GENL
:16R:TRADDET
:98A::SETT//20191016
:98A::TRAD//20191016
:35B:ISIN BE6307085488
:16S:TRADDET
:16R:FIAC
:36B::SETT//FAMT/1000000,0
:97A::SAFE//NBBE100860021001
:16S:FIAC
:16R:SETDET
:22F::STCO//NPAR
:22F::STCO//NOMC
:22F::SETR//TRAD
:16R:SETPRTY
:95P::PSET//NBBEBEBB216
:16S:SETPRTY
:16R:SETPRTY
:95P::DEAG//NBBEBEBB273
:97A::SAFE//NBBE100860021001
:16S:SETPRTY
:16R:SETPRTY
:95P::REAG//NBBEBEB05P2
:97A::SAFE//NBBE100860011001
:16S:SETPRTY
:16R:AMT
:19A::SETT//USD1000000,0
:16S:AMT
:16S:SETDET
```

5.4.1.2.1.3 SESE.023

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB273</BICFI>
               <ClrSysMmbId>
                  <ClrSysId>
                     <Prtry>T2S</Prtry>
                  </ClrSysId>
                  <MmbId>NBBSSS</MmbId>
               </ClrSysMmbId>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>FORCURTEST</BizMsgIdr>
      <MsgDefIdr>sese.023.001.07</MsgDefIdr>
      <CreDt>2019-10-15T13:26:00Z</CreDt>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.023.001.07">
      <SctiesSttlmTxInstr>
         <TxId>FORCURTEST</TxId>
         <SttlmTpAndAddtlParams>
            <SctiesMvmntTp>DELI</SctiesMvmntTp>
            <Pmt>FREE</Pmt>
         </SttlmTpAndAddtlParams>
         <TradDtls>
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </TradDt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
         </TradDtls>
         <FinInstrmId>
            <ISIN>BE6307085488</ISIN>
         </FinInstrmId>
         <QtyAndAcctDtls>
            <SttlmQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttlmQty>
            <SfkpgAcct>
               <Id>NBBE100860021001</Id>
            </SfkpgAcct>
         </QtyAndAcctDtls>
         <SttlmParams>
            <SctiesTxTp>
               <Cd>TRAD</Cd>
            </SctiesTxTp>
```

```
            <SttlmTxCond>
               <Cd>NOMC</Cd>
            </SttlmTxCond>
            <PrtlSttlmInd>NPAR</PrtlSttlmInd>
         </SttlmParams>
         <DlvrgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEBB273</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860021001</Id>
               </SfkpgAcct>
            </Pty1>
         </DlvrgSttlmPties>
         <RcvgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEB05P2</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860011001</Id>
               </SfkpgAcct>
            </Pty1>
         </RcvgSttlmPties>
         <SttlmAmt>
            <Amt Ccy="USD">1000000</Amt>
            <CdtDbtInd>CRDT</CdtDbtInd>
         </SttlmAmt>
      </SctiesSttlmTxInstr>
   </Document>
</Saa:Body>
```

5.4.1.2.2 OUTPUT

5.4.1.2.2.1 SESE.024 TO SELLER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB273</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
```

```
      </To>
      <BizMsgIdr>1077551387000</BizMsgIdr>
      <MsgDefIdr>sese.024.001.08</MsgDefIdr>
      <CreDt>2019-10-16T15:30:56Z</CreDt>
      <Prty>2019101600000283</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.024.001.08">
      <SctiesSttlmTxStsAdvc>
         <TxId>
            <AcctOwnrTxId>FORCURTEST</AcctOwnrTxId>
            <MktInfrstrctrTxId>1910150298151773</MktInfrstrctrTxId>
         </TxId>
         <MtchgSts>
            <Mtchd />
         </MtchgSts>
         <SttlmSts>
            <Pdg>
               <Rsn>
                  <Cd>
                     <Cd>FUTU</Cd>
                  </Cd>
                  <AddtlRsnInf>AwaitingSettlementDate</AddtlRsnInf>
               </Rsn>
            </Pdg>
         </SttlmSts>
         <TxDtls>
            <SfkpgAcct>
               <Id>NBBE100860021001</Id>
            </SfkpgAcct>
            <FinInstrmId>
               <ISIN>BE6307085488</ISIN>
            </FinInstrmId>
            <SttlmQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttlmQty>
            <SttlmAmt>
               <Amt Ccy="USD">1000000</Amt>
               <CdtDbtInd>CRDT</CdtDbtInd>
            </SttlmAmt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </TradDt>
            <MtchdStsTmStmp>2019-10-16T15:28:52Z</MtchdStsTmStmp>
            <SctiesMvmntTp>DELI</SctiesMvmntTp>
            <Pmt>FREE</Pmt>
            <SttlmParams>
               <SttlmTxCond>
                  <Cd>NOMC</Cd>
               </SttlmTxCond>
               <SctiesTxTp>
                  <Cd>TRAD</Cd>
               </SctiesTxTp>
               <PrtlSttlmInd>NPAR</PrtlSttlmInd>
            </SttlmParams>
            <RcvgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
```

```
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEB05P2</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860011001</Id>
               </SfkpgAcct>
            </Pty1>
         </RcvgSttlmPties>
         <DlvrgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEBB273</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860021001</Id>
               </SfkpgAcct>
            </Pty1>
         </DlvrgSttlmPties>
      </TxDtls>
      <SplmtryData>
         <PlcAndNm>/Document/SctiesSttlmTxStsAdvc/TxId</PlcAndNm>
         <Envlp>
            <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">
               <SctiesSttlmSD1>
                  <RltdTxId>01190521410620000</RltdTxId>
               </SctiesSttlmSD1>
            </Document>
         </Envlp>
      </SplmtryData>
   </SctiesSttlmTxStsAdvc>
</Document>
</Saa:Body>
```

5.4.1.3 Matching related instructions

5.4.1.3.1 SESE.024 TO BUYER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEB05P2</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077552207000</BizMsgIdr>
      <MsgDefIdr>sese.024.001.08</MsgDefIdr>
```

```
   <CreDt>2019-10-16T15:30:58Z</CreDt>
   <Prty>2019101600000285</Prty>
</AppHdr>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.024.001.08">
   <SctiesSttlmTxStsAdvc>
      <TxId>
         <AcctOwnrTxId>FORCURTEST1</AcctOwnrTxId>
         <MktInfrstrctrTxId>1910160298256173</MktInfrstrctrTxId>
      </TxId>
      <MtchgSts>
         <Mtchd />
      </MtchgSts>
      <SttlmSts>
         <Pdg>
            <Rsn>
               <Cd>
                  <Cd>FUTU</Cd>
               </Cd>
               <AddtlRsnInf>AwaitingSettlementDate</AddtlRsnInf>

            </Rsn>
         </Pdg>
      </SttlmSts>
      <TxDtls>
         <SfkpgAcct>
            <Id>NBBE100860011001</Id>
         </SfkpgAcct>
         <FinInstrmId>
            <ISIN>BE6307085488</ISIN>
         </FinInstrmId>
         <SttlmQty>
            <Qty>
               <FaceAmt>1000000</FaceAmt>
            </Qty>
         </SttlmQty>
         <SttlmAmt>
            <Amt Ccy="USD">1000000</Amt>
            <CdtDbtInd>DBIT</CdtDbtInd>
         </SttlmAmt>
         <SttlmDt>
            <Dt>
               <Dt>2019-10-16</Dt>
            </Dt>
         </SttlmDt>
         <TradDt>
            <Dt>
               <Dt>2019-10-16</Dt>
            </Dt>
         </TradDt>
         <MtchdStsTmStmp>2019-10-16T15:28:52Z</MtchdStsTmStmp>
         <SctiesMvmntTp>RECE</SctiesMvmntTp>
         <Pmt>FREE</Pmt>
         <SttlmParams>
            <SttlmTxCond>
               <Cd>NOMC</Cd>
            </SttlmTxCond>
            <SctiesTxTp>
               <Cd>TRAD</Cd>
            </SctiesTxTp>
            <PrtlSttlmInd>NPAR</PrtlSttlmInd>
         </SttlmParams>
         <RcvgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
```

```
                  <AnyBIC>NBBEBEB05P2</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860011001</Id>
               </SfkpgAcct>
            </Pty1>
         </RcvgSttlmPties>
         <DlvrgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEBB273</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860021001</Id>
               </SfkpgAcct>
            </Pty1>
         </DlvrgSttlmPties>
      </TxDtls>
      <SplmtryData>
         <PlcAndNm>/Document/SctiesSttlmTxStsAdvc/TxId</PlcAndNm>
         <Envlp>
            <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

               <SctiesSttlmSD1>
                  <RltdTxId>0119052141062000</RltdTxId>
               </SctiesSttlmSD1>
            </Document>
         </Envlp>
      </SplmtryData>
   </SctiesSttlmTxStsAdvc>
</Document>
</Saa:Body>
```

5.4.1.3.2 SESE.024 TO SELLER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB273</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077551387000</BizMsgIdr>
      <MsgDefIdr>sese.024.001.08</MsgDefIdr>
      <CreDt>2019-10-16T15:30:56Z</CreDt>
      <Prty>2019101600000283</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.024.001.08">
```

```
<SctiesSttlmTxStsAdvc>
   <TxId>
      <AcctOwnrTxId>FORCURTEST</AcctOwnrTxId>
      <MktInfrstrctrTxId>1910150298151773</MktInfrstrctrTxId>
   </TxId>
   <MtchgSts>
      <Mtchd />
   </MtchgSts>
   <SttlmSts>
      <Pdg>
         <Rsn>
            <Cd>
               <Cd>FUTU</Cd>
            </Cd>
            <AddtlRsnInf>AwaitingSettlementDate</AddtlRsnInf>

         </Rsn>
      </Pdg>
   </SttlmSts>
   <TxDtls>
      <SfkpgAcct>
         <Id>NBBE100860021001</Id>
      </SfkpgAcct>
      <FinInstrmId>
         <ISIN>BE6307085488</ISIN>
      </FinInstrmId>
      <SttlmQty>
         <Qty>
            <FaceAmt>1000000</FaceAmt>
         </Qty>
      </SttlmQty>
      <SttlmAmt>
         <Amt Ccy="USD">1000000</Amt>
         <CdtDbtInd>CRDT</CdtDbtInd>
      </SttlmAmt>
      <SttlmDt>
         <Dt>
            <Dt>2019-10-16</Dt>
         </Dt>
      </SttlmDt>
      <TradDt>
         <Dt>
            <Dt>2019-10-16</Dt>
         </Dt>
      </TradDt>
      <MtchdStsTmStmp>2019-10-16T15:28:52Z</MtchdStsTmStmp>
      <SctiesMvmntTp>DELI</SctiesMvmntTp>
      <Pmt>FREE</Pmt>
      <SttlmParams>
         <SttlmTxCond>
            <Cd>NOMC</Cd>
         </SttlmTxCond>
         <SctiesTxTp>
            <Cd>TRAD</Cd>
         </SctiesTxTp>
         <PrtlSttlmInd>NPAR</PrtlSttlmInd>
      </SttlmParams>
      <RcvgSttlmPties>
         <Dpstry>
            <Id>
               <AnyBIC>NBBEBEBB216</AnyBIC>
            </Id>
         </Dpstry>
         <Pty1>
            <Id>
               <AnyBIC>NBBEBEB05P2</AnyBIC>
            </Id>
            <SfkpgAcct>
               <Id>NBBE100860011001</Id>
```

```
                  </SfkpgAcct>
               </Pty1>
            </RcvgSttlmPties>
            <DlvrgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEBB273</AnyBIC>
                  </Id>
                  <SfkpgAcct>
                     <Id>NBBE100860021001</Id>
                  </SfkpgAcct>
               </Pty1>
            </DlvrgSttlmPties>
         </TxDtls>
         <SplmtryData>
            <PlcAndNm>/Document/SctiesSttlmTxStsAdvc/TxId</PlcAndNm>
            <Envlp>
               <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

                  <SctiesSttlmSD1>
                     <RltdTxId>0119052141062000</RltdTxId>
                  </SctiesSttlmSD1>
               </Document>
            </Envlp>
         </SplmtryData>
      </SctiesSttlmTxStsAdvc>
   </Document>
</Saa:Body>
```

5.4.1.3.3 SESE.029: ALLEGEMENT REMOVAL ADVICE

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB273</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077552208000</BizMsgIdr>
      <MsgDefIdr>sese.029.001.04</MsgDefIdr>
      <CreDt>2019-10-16T15:30:12Z</CreDt>
      <Prty>2019101600000286</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.029.001.04">
      <SctiesSttlmAllgmtRmvlAdvc>
         <AcctSvcrTxId>
            <TxId>NONREF</TxId>
            <SctiesMvmntTp>DELI</SctiesMvmntTp>
            <Pmt>FREE</Pmt>
         </AcctSvcrTxId>
         <MktInfrstrctrTxId>
```

```
            <Id>1910150298152245</Id>
         </MktInfrstrctrTxId>
         <AcctOwnr>
            <Id>
               <AnyBIC>NBBEBEB05P2</AnyBIC>
            </Id>
         </AcctOwnr>
         <SfkpgAcct>
            <Id>NBBE100860011001</Id>
         </SfkpgAcct>
         <TxDtls>
            <FinInstrmId>
               <ISIN>BE6307085488</ISIN>
            </FinInstrmId>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
            <SttlmQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttlmQty>
            <DlvrgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEBB273</AnyBIC>
                  </Id>
               </Pty1>
            </DlvrgSttlmPties>
            <RcvgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEB05P2</AnyBIC>
                  </Id>
               </Pty1>
            </RcvgSttlmPties>
         </TxDtls>
      </SctiesSttlmAllgmtRmvlAdvc>
   </Document>
</Saa:Body>
```

5.4.1.4 Instructions on ISD

5.4.1.4.1 SESE.031 PUT THE TRANSACTION ON HOLD

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
 <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
  <Fr>
   <FIId>
    <FinInstnId>
     <BICFI>TRGTXE2SXXX</BICFI>
     <Othr>
      <Id>NBBEBEBB216</Id>
     </Othr>
    </FinInstnId>
   </FIId>
```

```
    </Fr>
    <To>
      <FIId>
        <FinInstnId>
          <BICFI>NBBEBEBB273</BICFI>
          <Othr>
            <Id>NBBEBEBB216</Id>
          </Othr>
        </FinInstnId>
      </FIId>
    </To>
    <BizMsgIdr>1077552209000</BizMsgIdr>
    <MsgDefIdr>sese.031.001.07</MsgDefIdr>
    <CreDt>2019-10-16T15:30:12Z</CreDt>
    <Prty>2019101600000288</Prty>
  </AppHdr>
  <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.031.001.07">
    <SctiesSttlmCondModStsAdvc>
      <ReqRef>
        <Id>NONREF</Id>
      </ReqRef>
      <SfkpgAcct>
        <Id>NBBE100860021001</Id>
      </SfkpgAcct>
      <ReqDtls>
        <Ref>
          <AcctOwnrTxId>FORCURTEST</AcctOwnrTxId>
          <MktInfrstrctrTxId>1910150298151773</MktInfrstrctrTxId>
        </Ref>
        <HldInd>
          <Ind>true</Ind>
          <Rsn>
            <Cd>
              <Cd>CDEL</Cd>
            </Cd>
            <AddtlInf>300032260</AddtlInf>
          </Rsn>
        </HldInd>
      </ReqDtls>
      <PrcgSts>
        <Cmpltd />
      </PrcgSts>
    </SctiesSttlmCondModStsAdvc>
  </Document>
</Saa:Body>
```

5.4.1.4.2 RESERVATION COMPLETED – SEMT.015

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
```

```
   <Fr>
      <FIId>
         <FinInstnId>
            <BICFI>TRGTXE2SXXX</BICFI>
            <Othr>
               <Id>NBBEBEBB216</Id>
            </Othr>
         </FinInstnId>
      </FIId>
   </Fr>
   <To>
      <FIId>
         <FinInstnId>
            <BICFI>NBBEBEBB273</BICFI>
            <Othr>
               <Id>NBBEBEBB216</Id>
            </Othr>
         </FinInstnId>
      </FIId>
   </To>
   <BizMsgIdr>1077551390000</BizMsgIdr>
   <MsgDefIdr>semt.015.001.06</MsgDefIdr>
   <CreDt>2019-10-16T15:30:12Z</CreDt>
   <Prty>2019101600000289</Prty>
</AppHdr>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:semt.015.001.06">
   <IntraPosMvmntConf>
      <AddtlParams>
         <MktInfrstrctrTxId>0219052141063000</MktInfrstrctrTxId>
      </AddtlParams>
      <AcctOwnr>
         <AnyBIC>NBBEBEBB273</AnyBIC>
      </AcctOwnr>
      <SfkpgAcct>
         <Id>NBBE100860021001</Id>
      </SfkpgAcct>
      <FinInstrmId>
         <ISIN>BE6307085488</ISIN>
      </FinInstrmId>
      <IntraPosDtls>
         <SttldQty>
            <FaceAmt>1000000</FaceAmt>
         </SttldQty>
         <SctiesSubBalId>
            <Id>1905214106202001</Id>
         </SctiesSubBalId>
         <SttlmDt>
            <DtTm>2019-10-16T17:28:54.872186</DtTm>
         </SttlmDt>
         <BalFr>
            <Tp>
               <Cd>AWAS</Cd>
            </Tp>
         </BalFr>
         <BalTo>
            <Tp>
               <Prtry>
                  <Id>COSP</Id>
                  <Issr>T2S</Issr>
                  <SchmeNm>RT</SchmeNm>
               </Prtry>
            </Tp>
         </BalTo>
      </IntraPosDtls>
      <SplmtryData>
         <PlcAndNm>/Document/IntraPosMvmntConf/AddtlParams</PlcAndNm>
            <Envlp>
         <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">
            <SctiesSttlmSD1>
```

```
                  <RltdTxId>1910150298151773</RltdTxId>
               </SctiesSttlmSD1>
            </Document>
         </Envlp>
      </SplmtryData>
   </IntraPosMvmntConf>
</Document>
</Saa:Body>
```

5.4.1.4.3 SESE.024 – INFO ON RESERVATION TOWARDS SELLER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1076573172000</BizMsgIdr>
      <MsgDefIdr>sese.024.001.08</MsgDefIdr>
      <CreDt>2019-10-16T13:20:19Z</CreDt>
      <Prty>2019091700000044</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.024.001.08">
      <SctiesSttlmTxStsAdvc>
         <TxId>
            <AcctOwnrTxId>NONREF</AcctOwnrTxId>
            <AcctSvcrTxId> FORCURTEST </AcctSvcrTxId>
            <MktInfrstrctrTxId>1910150298151773</MktInfrstrctrTxId>
         </TxId>
         <SttlmSts>
            <Pdg>
               <Rsn>
                  <Cd>
                     <Cd>PRSY</Cd>
                  </Cd>
                  <AddtlRsnInf>300032260</AddtlRsnInf>
               </Rsn>
            </Pdg>
         </SttlmSts>
         <TxDtls>
            <SfkpgAcct>
               <Id> NBBE100860021001</Id>
            </SfkpgAcct>
            <FinInstrmId>
               <ISIN> BE6307085488</ISIN>
            </FinInstrmId>
            <SttlmQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttlmQty>
            <SttlmAmt>
               <Amt Ccy="USD">1000000</Amt>
               <CdtDbtInd>CRDT</CdtDbtInd>
```

```
            </SttlmAmt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </TradDt>
            <SctiesMvmntTp>DELI</SctiesMvmntTp>
            <Pmt>FREE</Pmt>
            <SttlmParams>
               <HldInd>
                  <Ind>true</Ind>
                  <Rsn>
                     <Cd>
                        <Cd>CDEL</Cd>
                     </Cd>
                     <AddtlInf>300032260</AddtlInf>
                  </Rsn>
               </HldInd>
               <SctiesTxTp>
                  <Cd>TRAD</Cd>
               </SctiesTxTp>
               <PrtlSttlmInd>NPAR</PrtlSttlmInd>
            </SttlmParams>
            <RcvgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC> NBBEBEB05P2</AnyBIC>
                  </Id>
               </Pty1>
            </RcvgSttlmPties>
            <DlvrgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC> NBBEBEBB273</AnyBIC>
                  </Id>
               </Pty1>
            </DlvrgSttlmPties>
         </TxDtls>
         <SplmtryData>
            <PlcAndNm>/Document/SctiesSttlmTxStsAdvc/TxId</PlcAndNm>

            <Envlp>
               <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

                  <SctiesSttlmSD1>
                     <RltdTxId>0119052141062000</RltdTxId>

                  </SctiesSttlmSD1>
               </Document>
            </Envlp>
         </SplmtryData>
      </SctiesSttlmTxStsAdvc>
   </Document>
</Saa:Body>
```

5.4.1.4.4 SESE.024 – INFO RESERVATION TOWARDS BUYER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEB05P2</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077551389000</BizMsgIdr>
      <MsgDefIdr>sese.024.001.08</MsgDefIdr>
      <CreDt>2019-10-16T15:31:00Z</CreDt>
      <Prty>2019101600000291</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.024.001.08">
      <SctiesSttlmTxStsAdvc>
         <TxId>
            <AcctOwnrTxId>FORCURTEST1</AcctOwnrTxId>
            <MktInfrstrctrTxId>1910160298256173</MktInfrstrctrTxId>
         </TxId>
         <SttlmSts>
            <Pdg>
               <Rsn>
                  <Cd>
                     <Cd>PRCY</Cd>
                  </Cd>
                  <AddtlRsnInf>SPST002 - Settlement Instruction is unsettled because i
ts counterpart settlement
 instruction is 'On Hold'</AddtlRsnInf>
               </Rsn>
            </Pdg>
         </SttlmSts>
         <TxDtls>
            <SfkpgAcct>
               <Id>NBBE100860011001</Id>
            </SfkpgAcct>
            <FinInstrmId>
               <ISIN>BE6307085488</ISIN>
            </FinInstrmId>
            <SttlmQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttlmQty>
            <SttlmAmt>
               <Amt Ccy="USD">1000000</Amt>
               <CdtDbtInd>DBIT</CdtDbtInd>
            </SttlmAmt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
```

```
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </TradDt>
            <SctiesMvmntTp>RECE</SctiesMvmntTp>
            <Pmt>FREE</Pmt>
            <SttlmParams>
               <SttlmTxCond>
                  <Cd>NOMC</Cd>
               </SttlmTxCond>
               <SctiesTxTp>
                  <Cd>TRAD</Cd>
               </SctiesTxTp>
               <PrtlSttlmInd>NPAR</PrtlSttlmInd>
            </SttlmParams>
            <RcvgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEB05P2</AnyBIC>
                  </Id>
                  <SfkpgAcct>
                     <Id>NBBE100860011001</Id>
                  </SfkpgAcct>
               </Pty1>
            </RcvgSttlmPties>
            <DlvrgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEBB273</AnyBIC>
                  </Id>
                  <SfkpgAcct>
                     <Id>NBBE100860021001</Id>
                  </SfkpgAcct>
               </Pty1>
            </DlvrgSttlmPties>
         </TxDtls>
         <SplmtryData>
            <PlcAndNm>/Document/SctiesSttlmTxStsAdvc/TxId</PlcAndNm>
            <Envlp>
               <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

                  <SctiesSttlmSD1>
                     <RltdTxId>0119052141062000</RltdTxId>
                  </SctiesSttlmSD1>
               </Document>
            </Envlp>
         </SplmtryData>
      </SctiesSttlmTxStsAdvc>
   </Document>
</Saa:Body>
```

5.4.1.4.5 SESE.024 AWAITING RELEASE BY CSD TO SELLER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
```

```
            <Othr>
               <Id>TRGTXE2SXXX</Id>
            </Othr>
         </FinInstnId>
      </FIId>
   </Fr>
   <To>
      <FIId>
         <FinInstnId>
            <BICFI>NBBEBEBB273</BICFI>
            <Othr>
               <Id>NBBEBEBB216</Id>
            </Othr>
         </FinInstnId>
      </FIId>
   </To>
   <BizMsgIdr>1077552210000</BizMsgIdr>
   <MsgDefIdr>sese.024.001.08</MsgDefIdr>
   <CreDt>2019-10-16T15:30:59Z</CreDt>
   <Prty>2019101600000290</Prty>
</AppHdr>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.024.001.08">
   <SctiesSttlmTxStsAdvc>
      <TxId>
         <AcctOwnrTxId>FORCURTEST</AcctOwnrTxId>
         <MktInfrstrctrTxId>1910150298151773</MktInfrstrctrTxId>
      </TxId>
      <SttlmSts>
         <Pdg>
            <Rsn>
               <Cd>
                  <Cd>CDLR</Cd>
               </Cd>
               <AddtlRsnInf>CoSD awaiting from Administering Party</AddtlRsnInf>

            </Rsn>
         </Pdg>
      </SttlmSts>
      <TxDtls>
         <SfkpgAcct>
            <Id>NBBE100860021001</Id>
         </SfkpgAcct>
         <FinInstrmId>
            <ISIN>BE6307085488</ISIN>
         </FinInstrmId>
         <SttlmQty>
            <Qty>
               <FaceAmt>1000000</FaceAmt>
            </Qty>
         </SttlmQty>
         <SttlmAmt>
            <Amt Ccy="USD">1000000</Amt>
            <CdtDbtInd>CRDT</CdtDbtInd>
         </SttlmAmt>
         <SttlmDt>
            <Dt>
               <Dt>2019-10-16</Dt>
            </Dt>
         </SttlmDt>
         <TradDt>
            <Dt>
               <Dt>2019-10-16</Dt>
            </Dt>
         </TradDt>
         <SctiesMvmntTp>DELI</SctiesMvmntTp>
         <Pmt>FREE</Pmt>
         <SttlmParams>
            <HldInd>
               <Ind>true</Ind>
```

```
                  <Rsn>
                     <Cd>
                        <Cd>CDEL</Cd>
                     </Cd>
                     <AddtlInf>300032260</AddtlInf>
                  </Rsn>
               </HldInd>
               <SttlmTxCond>
                  <Cd>NOMC</Cd>
               </SttlmTxCond>
               <SctiesTxTp>
                  <Cd>TRAD</Cd>
               </SctiesTxTp>
               <PrtlSttlmInd>NPAR</PrtlSttlmInd>
            </SttlmParams>
            <RcvgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEB05P2</AnyBIC>
                  </Id>
                  <SfkpgAcct>
                     <Id>NBBE100860011001</Id>
                  </SfkpgAcct>
               </Pty1>
            </RcvgSttlmPties>
            <DlvrgSttlmPties>
               <Dpstry>
                  <Id>
                     <AnyBIC>NBBEBEBB216</AnyBIC>
                  </Id>
               </Dpstry>
               <Pty1>
                  <Id>
                     <AnyBIC>NBBEBEBB273</AnyBIC>
                  </Id>
                  <SfkpgAcct>
                     <Id>NBBE100860021001</Id>
                  </SfkpgAcct>
               </Pty1>
            </DlvrgSttlmPties>
         </TxDtls>
         <SplmtryData>
            <PlcAndNm>/Document/SctiesSttlmTxStsAdvc/TxId</PlcAndNm>
            <Envlp>
               <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

                  <SctiesSttlmSD1>
                     <RltdTxId>0119052141062000</RltdTxId>
                  </SctiesSttlmSD1>
               </Document>
            </Envlp>
         </SplmtryData>
      </SctiesSttlmTxStsAdvc>
   </Document>
</Saa:Body>
```

5.4.1.4.6 RELEASE OF TRANSACTION BY ADMINISTRATIVE PARTY (CSD) – SESE.030 SENT BY CSD

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <ClrSysMmbId>
                  <ClrSysId>
                     <Prtry>T2S</Prtry>
                  </ClrSysId>
                  <MmbId>NBBSSS</MmbId>
               </ClrSysMmbId>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>20191017S0000060</BizMsgIdr>
      <MsgDefIdr>sese.030.001.07</MsgDefIdr>
      <CreDt>2019-10-17T12:48:20Z</CreDt>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.030.001.07">
      <SctiesSttlmCondsModReq>
         <SfkpgAcct>
            <Id>NBBE100860021001</Id>
         </SfkpgAcct>
         <ReqDtls>
            <Ref>
               <MktInfrstrctrTxId>1910150298151773</MktInfrstrctrTxId>

            </Ref>
            <HldInd>
               <Ind>false</Ind>
               <Rsn>
                  <Cd>
                     <Cd>CDEL</Cd>
                  </Cd>
                  <AddtlInf>300032260</AddtlInf>
               </Rsn>
            </HldInd>
         </ReqDtls>
      </SctiesSttlmCondsModReq>
   </Document>
</Saa:Body>
```

5.4.1.4.7 SESE.031 (CONFIRMATION OF RELEASE) RECEIVED BY CSD

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077594623000</BizMsgIdr>
      <MsgDefIdr>sese.031.001.07</MsgDefIdr>
      <CreDt>2019-10-17T12:48:42Z</CreDt>
      <Prty>2019101700000252</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.031.001.07">
      <SctiesSttlmCondModStsAdvc>
         <ReqRef>
            <Id>20191017S0000060</Id>
         </ReqRef>
         <SfkpgAcct>
            <Id>NBBE100860021001</Id>
         </SfkpgAcct>
         <ReqDtls>
            <Ref>
               <AcctOwnrTxId>FORCURTEST</AcctOwnrTxId>
               <MktInfrstrctrTxId>1910150298151773</MktInfrstrctrTxId>

            </Ref>
            <HldInd>
               <Ind>false</Ind>
               <Rsn>
                  <Cd>
                     <Cd>CDEL</Cd>
                  </Cd>
                  <AddtlInf>300032260</AddtlInf>
               </Rsn>
            </HldInd>
         </ReqDtls>
         <PrcgSts>
            <Cmpltd />
         </PrcgSts>
      </SctiesSttlmCondModStsAdvc>
   </Document>
</Saa:Body>
```

5.4.1.4.8 SESE.024 TO BUYER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEB05P2</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077594624000</BizMsgIdr>
      <MsgDefIdr>sese.024.001.08</MsgDefIdr>
      <CreDt>2019-10-17T12:48:42Z</CreDt>
      <Prty>2019101700000250</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.024.001.08">
      <SctiesSttlmTxStsAdvc>
         <TxId>
            <AcctOwnrTxId>FORCURTEST1</AcctOwnrTxId>
            <MktInfrstrctrTxId>1910160298256173</MktInfrstrctrTxId>
         </TxId>
         <SttlmSts>
            <Flng>
               <Rsn>
                  <Cd>
                     <Cd>CYCL</Cd>
                  </Cd>
                  <AddtlRsnInf>AwaitingNextSettlementCycle</AddtlRsnInf>

               </Rsn>
            </Flng>
         </SttlmSts>
         <TxDtls>
            <SfkpgAcct>
               <Id>NBBE100860011001</Id>
            </SfkpgAcct>
            <FinInstrmId>
               <ISIN>BE6307085488</ISIN>
            </FinInstrmId>
            <SttlmQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttlmQty>
            <SttlmAmt>
               <Amt Ccy="USD">1000000</Amt>
               <CdtDbtInd>DBIT</CdtDbtInd>
            </SttlmAmt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
```

```
                </Dt>
             </TradDt>
             <SctiesMvmntTp>RECE</SctiesMvmntTp>
             <Pmt>FREE</Pmt>
             <SttlmParams>
                <SttlmTxCond>
                   <Cd>NOMC</Cd>
                </SttlmTxCond>
                <SctiesTxTp>
                   <Cd>TRAD</Cd>
                </SctiesTxTp>
                <PrtlSttlmInd>NPAR</PrtlSttlmInd>
             </SttlmParams>
             <RcvgSttlmPties>
                <Dpstry>
                   <Id>
                      <AnyBIC>NBBEBEBB216</AnyBIC>
                   </Id>
                </Dpstry>
                <Pty1>
                   <Id>
                      <AnyBIC>NBBEBEB05P2</AnyBIC>
                   </Id>
                   <SfkpgAcct>
                      <Id>NBBE100860011001</Id>
                   </SfkpgAcct>
                </Pty1>
             </RcvgSttlmPties>
             <DlvrgSttlmPties>
                <Dpstry>
                   <Id>
                      <AnyBIC>NBBEBEBB216</AnyBIC>
                   </Id>
                </Dpstry>
                <Pty1>
                   <Id>
                      <AnyBIC>NBBEBEBB273</AnyBIC>
                   </Id>
                   <SfkpgAcct>
                      <Id>NBBE100860021001</Id>
                   </SfkpgAcct>
                </Pty1>
             </DlvrgSttlmPties>
          </TxDtls>
          <SplmtryData>
             <PlcAndNm>/Document/SctiesSttlmTxStsAdvc/TxId</PlcAndNm>

             <Envlp>
                <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

                   <SctiesSttlmSD1>
                      <RltdTxId>0119052141062000</RltdTxId>

                   </SctiesSttlmSD1>
                </Document>
             </Envlp>
          </SplmtryData>
       </SctiesSttlmTxStsAdvc>
    </Document>
</Saa:Body>
```

5.4.1.4.9 SESE.024 TO SELLER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB273</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077595376000</BizMsgIdr>
      <MsgDefIdr>sese.024.001.08</MsgDefIdr>
      <CreDt>2019-10-17T12:48:42Z</CreDt>
      <Prty>2019101700000249</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.024.001.08">
      <SctiesSttlmTxStsAdvc>
         <TxId>
            <AcctOwnrTxId>FORCURTEST</AcctOwnrTxId>
            <MktInfrstrctrTxId>1910150298151773</MktInfrstrctrTxId>
         </TxId>
         <SttlmSts>
            <Flng>
               <Rsn>
                  <Cd>
                     <Cd>CYCL</Cd>
                  </Cd>
                  <AddtlRsnInf>AwaitingNextSettlementCycle</AddtlRsnInf>

               </Rsn>
            </Flng>
         </SttlmSts>
         <TxDtls>
            <SfkpgAcct>
               <Id>NBBE100860021001</Id>
            </SfkpgAcct>
            <FinInstrmId>
               <ISIN>BE6307085488</ISIN>
            </FinInstrmId>
            <SttlmQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttlmQty>
            <SttlmAmt>
               <Amt Ccy="USD">1000000</Amt>
               <CdtDbtInd>CRDT</CdtDbtInd>
            </SttlmAmt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
```

```
            </Dt>
         </TradDt>
         <SctiesMvmntTp>DELI</SctiesMvmntTp>
         <Pmt>FREE</Pmt>
         <SttlmParams>
            <SttlmTxCond>
               <Cd>NOMC</Cd>
            </SttlmTxCond>
            <SctiesTxTp>
               <Cd>TRAD</Cd>
            </SctiesTxTp>
            <PrtlSttlmInd>NPAR</PrtlSttlmInd>
         </SttlmParams>
         <RcvgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEB05P2</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860011001</Id>
               </SfkpgAcct>
            </Pty1>
         </RcvgSttlmPties>
         <DlvrgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEBB273</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860021001</Id>
               </SfkpgAcct>
            </Pty1>
         </DlvrgSttlmPties>
      </TxDtls>
      <SplmtryData>
         <PlcAndNm>/Document/SctiesSttlmTxStsAdvc/TxId</PlcAndNm>

         <Envlp>
            <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

               <SctiesSttlmSD1>
                  <RltdTxId>0119052141062000</RltdTxId>

               </SctiesSttlmSD1>
            </Document>
         </Envlp>
      </SplmtryData>
   </SctiesSttlmTxStsAdvc>
</Document>
</Saa:Body>
```

5.4.1.4.10 SECURITIES SETTLEMENT CONFIRMATIONS INSTRUCTIONS

5.4.1.4.10.1 SESE.025 TO BUYER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEB05P2</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077595379000</BizMsgIdr>
      <MsgDefIdr>sese.025.001.07</MsgDefIdr>
      <CreDt>2019-10-17T12:49:31Z</CreDt>
      <Prty>2019101700000255</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.025.001.07">
      <SctiesSttlmTxConf>
         <TxIdDtls>
            <AcctOwnrTxId>FORCURTEST1</AcctOwnrTxId>
            <MktInfrstrctrTxId>1910160298256173</MktInfrstrctrTxId>
            <SctiesMvmntTp>RECE</SctiesMvmntTp>
            <Pmt>FREE</Pmt>
         </TxIdDtls>
         <TradDtls>
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </TradDt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
            <FctvSttlmDt>
               <Dt>
                  <DtTm>2019-10-17T14:48:31.610987</DtTm>
               </Dt>
            </FctvSttlmDt>
         </TradDtls>
         <FinInstrmId>
            <ISIN>BE6307085488</ISIN>
         </FinInstrmId>
         <QtyAndAcctDtls>
            <SttldQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttldQty>
            <SfkpgAcct>
               <Id>NBBE100860011001</Id>
            </SfkpgAcct>
         </QtyAndAcctDtls>
         <SttlmParams>
```

```
            <SctiesTxTp>
               <Cd>TRAD</Cd>
            </SctiesTxTp>
            <SttlmTxCond>
               <Cd>NOMC</Cd>
            </SttlmTxCond>
            <PrtlSttlmInd>NPAR</PrtlSttlmInd>
            <SctiesSubBalTp>
               <Id>AWAS</Id>
               <Issr>T2S</Issr>
               <SchmeNm>RT</SchmeNm>
            </SctiesSubBalTp>
         </SttlmParams>
         <DlvrgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEBB273</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860021001</Id>
               </SfkpgAcct>
            </Pty1>
         </DlvrgSttlmPties>
         <RcvgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEB05P2</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860011001</Id>
               </SfkpgAcct>
            </Pty1>
         </RcvgSttlmPties>
         <SplmtryData>
            <PlcAndNm>/Document/SctiesSttlmTxConf/TxIdDtls</PlcAndNm>
            <Envlp>
               <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

                  <SctiesSttlmSD1>
                     <RltdTxId>0119052141062000</RltdTxId>
                  </SctiesSttlmSD1>
               </Document>
            </Envlp>
         </SplmtryData>
      </SctiesSttlmTxConf>
   </Document>
</Saa:Body>
```

5.4.1.4.10.2 SESE.025 TO SELLER

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB273</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>1077595378000</BizMsgIdr>
      <MsgDefIdr>sese.025.001.07</MsgDefIdr>
      <CreDt>2019-10-17T12:49:30Z</CreDt>
      <Prty>2019101700000254</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.025.001.07">
      <SctiesSttlmTxConf>
         <TxIdDtls>
            <AcctOwnrTxId>FORCURTEST</AcctOwnrTxId>
            <MktInfrstrctrTxId>1910150298151773</MktInfrstrctrTxId>
            <SctiesMvmntTp>DELI</SctiesMvmntTp>
            <Pmt>FREE</Pmt>
         </TxIdDtls>
         <TradDtls>
            <TradDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </TradDt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-10-16</Dt>
               </Dt>
            </SttlmDt>
            <FctvSttlmDt>
               <Dt>
                  <DtTm>2019-10-17T14:48:31.610987</DtTm>
               </Dt>
            </FctvSttlmDt>
         </TradDtls>
         <FinInstrmId>
            <ISIN>BE6307085488</ISIN>
         </FinInstrmId>
         <QtyAndAcctDtls>
            <SttldQty>
               <Qty>
                  <FaceAmt>1000000</FaceAmt>
               </Qty>
            </SttldQty>
            <SfkpgAcct>
               <Id>NBBE100860021001</Id>
            </SfkpgAcct>
         </QtyAndAcctDtls>
         <SttlmParams>
            <SctiesTxTp>
               <Cd>TRAD</Cd>
            </SctiesTxTp>
            <SttlmTxCond>
               <Cd>NOMC</Cd>
            </SttlmTxCond>
```

```
            <PrtlSttlmInd>NPAR</PrtlSttlmInd>
            <SctiesSubBalTp>
               <Id>AWAS</Id>
               <Issr>T2S</Issr>
               <SchmeNm>RT</SchmeNm>
            </SctiesSubBalTp>
         </SttlmParams>
         <DlvrgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEBB273</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860021001</Id>
               </SfkpgAcct>
            </Pty1>
         </DlvrgSttlmPties>
         <RcvgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEB05P2</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100860011001</Id>
               </SfkpgAcct>
            </Pty1>
         </RcvgSttlmPties>
         <SplmtryData>
            <PlcAndNm>/Document/SctiesSttlmTxConf/TxIdDtls</PlcAndNm>
            <Envlp>
               <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

                  <SctiesSttlmSD1>
                     <RltdTxId>0119052141062000</RltdTxId>
                  </SctiesSttlmSD1>
               </Document>
            </Envlp>
         </SplmtryData>
      </SctiesSttlmTxConf>
   </Document>
</Saa:Body>
```

5.4.1.4.10.3 EXAMPLE OF MT544 FOR A TRADE IN FOREIGN CURRENCY (BUYER) – DELIVER FREE CONFIRMATION

```
:16R:GENL
:20C::SEME//1077595379000
:23G:NEWM
:98C::PREP//20191017144931
:16R:LINK
:20C::RELA//FORCURTEST1
:16S:LINK
:16R:LINK
:20C::MITI//0119052141062000
:16S:LINK
:16R:LINK
:20C::PCTI//1910160298256173
:16S:LINK
:16S:GENL
:16R:TRADDET
:98A::SETT//20191016
:98A::TRAD//20191016
:98C::ESET//20191017144831
```

```
:35B:ISIN BE6307085488
:16S:TRADDET
:16R:FIAC
:36B::ESTT//FAMT/1000000,0
:97A::SAFE//NBBE100860011001
:16S:FIAC
:16R:SETDET
:22F::STCO//NPAR
:22F::STCO//NOMC
:22F::SETR//TRAD
:22F::SSBT/T2S/AWAS
:16R:SETPRTY
:95P::PSET//NBBEBEBB216
:16S:SETPRTY
:16R:SETPRTY
:95P::DEAG//NBBEBEBB273
:97A::SAFE//NBBE100860021001
:16S:SETPRTY
:16R:SETPRTY
:95P::REAG//NBBEBEB05P2
:97A::SAFE//NBBE100860011001
:16S:SETPRTY
:16S:SETDET
```

5.4.1.4.10.4 EXAMPLE OF MT546 FOR A TRADE IN FOREIGN CURRENCY (SELLER) – RECEIVE FREE CONFIRMATION

```
:16R:GENL
:20C::SEME//1077595378000
:23G:NEWM
:98C::PREP//20191017144930
:16R:LINK
:20C::RELA//FORCURTEST
:16S:LINK
:16R:LINK
:20C::MITI//0119052141062000
:16S:LINK
:16R:LINK
:20C::PCTI//1910150298151773
:16S:LINK
:16S:GENL
:16R:TRADDET
:98A::SETT//20191016
:98A::TRAD//20191016
:98C::ESET//20191017144831
:35B:ISIN BE6307085488
:16S:TRADDET
:16R:FIAC
:36B::ESTT//FAMT/1000000,0
:97A::SAFE//NBBE100860021001
:16S:FIAC
:16R:SETDET
:22F::STCO//NPAR
:22F::STCO//NOMC
:22F::SETR//TRAD
:22F::SSBT/T2S/AWAS
:16R:SETPRTY
:95P::PSET//NBBEBEBB216
:16S:SETPRTY
:16R:SETPRTY
:95P::DEAG//NBBEBEBB273
:97A::SAFE//NBBE100860021001
:16S:SETPRTY
:16R:SETPRTY
:95P::REAG//NBBEBEB05P2
:97A::SAFE//NBBE100860011001
:16S:SETPRTY
:16S:SETDET
```

5.4.1.4.11 THE CASH SETTLEMENT INSTRUCTIONS

5.4.1.4.11.1 EXAMPLE OF A MT202 FOR A TRADE

:20:0119052141062000
:21:0119052141062000
:32A:191016USD1000000,0
:52A:NBBEBEBB216
:53B:/BE88058910810441
:57A:GKCCBEBBXXX
:58A:/BE13058910810239
NBBEBEBB216
:72:/BNF/ORDER null BE6307085488

5.4.1.4.11.2 MT900 FOR THE SAME TRADE

:20:CMI1008113124254
:21:0119052141062000
:25:/BE13058910810239
:32A:191008USD10000000,
:52A:NBBEBEBB216
:72:/BNF/ORDER NULL BE6270360868

5.4.1.4.11.3 MT910 FOR THE SAME TRADE

:20:CMI1008113124149
:21:0119052141062000
:25:/BE88058910810441
:32A:191008USD10000000,
:52A:NBBEBEBB216
:72: BNF ORDER NULL BE6307085488

5.4.2 Corporate actions in Foreign currency (with transferaccount DTA)

5.4.2.1 Instruct MT202 to debit of FCA of Paying agent towards DTA.

```
UETR in header field 121 4d4d4c6e-a58c-47d2-ad06-e812d882cc05

:20:BE63070854005000
:21:BE63070854005000
:32A:191119USD2606250,0
:52A:NBBEBEBB216
:53B:/BE02058910810340
:58A:/BE55058910810744
NBBEBEBB216
:72:/BNF/ORDER GEBABEBB36A BE6307085488
```

5.4.2.2 Reception of MT910 (credit of DTA)

```
:20:CMI1119130032446
:21:BE63070854005000
:25:/BE55058910810744
:32A:191119USD2606250,
:52A:NBBEBEBB216
:72: BNF ORDER GEBABEBB36A BE6307085488
```

5.4.2.3 MT566 to paying agent

```
:16R:GENL
:20C::CORP//BE63070854880005
:20C::SEME//20191119S0000003
:20C::COAF//BE63070854880005
:23G:NEWM
:22F::CAEV//INTR
:98C::PREP//20191119130716
:16S:GENL
:16R:USECU
:95P::ACOW//NBBEBEBB216
:97A::SAFE//NBBE100899999982
:35B:ISIN BE6307085488
EMTN BNP PARIBAS FORTIS
:16R:FIA
:11A::DENO//USD
:98A::COUP//20191119
:98A::MATU//20250805
:98A::ISSU//20180805
:92A::INTR//25,0
:16S:FIA
:93B::CONB//FAMT/0,0
:16S:USECU
:16R:CADETL
:98A::XDTE//20191119
:98A::RDTE//20191118
:69A::INPE//20191113/20191119
:99A::DAAC//006
:92A::INTR//25,0
:16S:CADETL
:16R:CACONF
:13A::CAON//001
:22H::CAOP//CASH
:16R:CASHMOVE
:22H::CRDB//DEBT
:97A::CASH//BE55058910810744
:19B::PSTA//USD2606250,0
:19B::RESU//EUR0,0
:98A::POST//20191119
:98A::VALU//20191119
:98A::FXDT//20191118
:98A::PAYD//20191119
```

```
:92B::EXCH//USD/EUR/0,90628965
:92A::INTP//0,416666667
:92A::RATE//100,0
:92A::TAXR//0,0
:16S:CASHMOVE
:16S:CACONF
:16R:ADDINFO
/ASRF//BE63070854005000
/INFO//UETR
      /4d4d4c6e-a58c-47d2-ad06-
       /e812d882cc05
:95P::PAYA//NBBEBEBB216
:16S:ADDINFO
```

5.4.2.4 Instruct MT202 to debit DTA towards FCA investor

Here we show payback of third position found in Ramses, which is also an N-account

```
UETR in header field 121 4d4d4c6e-a58c-47d2-ad06-e812d882cc06
```

```
:20:BE63070854005033N
:21:BE6307085400503N
:32A:191119USD343725,0
:52A:NBBEBEBB216
:53B:/BE55058910810744
:58A:/BE66058910810643
NBBEBEBB216
:72:/BNF/ORDER GEBABEBB36A BE6307085488
```

5.4.2.5 Reception of MT900 (debit of transferaccount)

```
:20:CMI1119130826067
:21:BE6307085400503N
:25:/BE55058910810744
:32A:191119USD343725,
:52A:NBBEBEBB216
:72: BNF ORDER GEBABEBB36A BE6307085488
```

5.4.2.6 MT566 to investor

```
:16R:GENL
:20C::CORP//BE63070854880005
:20C::SEME//20191119S0000018
:20C::COAF//BE63070854880005
:23G:NEWM
:22F::CAEV//INTR
:98C::PREP//20191119130938
:16S:GENL
:16R:USECU
:95P::ACOW//NBBEBEBB216
:97A::SAFE//NBBE100899999982
:35B:ISIN BE6307085488
EMTN BNP PARIBAS FORTIS
:16R:FIA
:11A::DENO//USD
:98A::COUP//20191119
:98A::MATU//20250805
:98A::ISSU//20180805
:92A::INTR//25,0
:16S:FIA
:93B::CONB//FAMT/0,0
:16S:USECU
:16R:CADETL
:98A::XDTE//20191119
:98A::RDTE//20191118
:69A::INPE//20191113/20191119
:99A::DAAC//006
:92A::INTR//25,0
:16S:CADETL
:16R:CACONF
:13A::CAON//001
:22H::CAOP//CASH
:16R:CASHMOVE
```

```
:22H::CRDB//CRED
:97A::CASH//BE66058910810643
:19B::PSTA//USD343725,0
:19B::RESU//EUR0,0
:98A::POST//20191119
:98A::VALU//20191119
:98A::FXDT//20191118
:98A::PAYD//20191119
:92B::EXCH//USD/EUR/0,90628965
:92A::INTP//0,416666667
:92A::RATE//100,0
:92A::TAXR//0,0
:16S:CASHMOVE
:16S:CACONF
:16R:ADDINFO
/ASRF//BE6307085400503N
/INFO//UETR
      /4d4d4c6e-a58c-47d2-ad06-
      /e812d882cc06
:95P::PAYA//NBBEBEBB216
:16S:ADDINFO
```

5.4.2.7 In case of redemption: Release of Debit of Investor Securities Account

5.4.2.7.1 SESE.023 – MOVING THE POSITION BACK TO THE ISSUANCE ACCOUNT

Here the example shows the return of the position to be redeemed (so ASRF **BE6307085400003N**)
find third in the system on an N account.

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <ClrSysMmbId>
                  <ClrSysId>
                     <Prtry>T2S</Prtry>
                  </ClrSysId>
                  <MmbId>NBBSSS</MmbId>
               </ClrSysMmbId>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>20191105S0000363</BizMsgIdr>
      <MsgDefIdr>sese.023.001.07</MsgDefIdr>
      <CreDt>2019-11-05T17:26:49Z</CreDt>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.023.001.07">
      <SctiesSttlmTxInstr>
         <TxId>NBBE19309CR00007</TxId>
         <SttlmTpAndAddtlParams>
            <SctiesMvmntTp>DELI</SctiesMvmntTp>
            <Pmt>FREE</Pmt>

             <CmonId>BE6307085400003N </CmonId>
            <CorpActnEvtId>BE63070854880000</CorpActnEvtId>
         </SttlmTpAndAddtlParams>
```

```
<TradDtls>
   <TradDt>
      <Dt>
         <Dt>2019-11-18</Dt>
      </Dt>
   </TradDt>
   <SttlmDt>
      <Dt>
         <Dt>2019-11-19</Dt>
      </Dt>
   </SttlmDt>
   <MtchgSts>
      <Cd>MACH</Cd>
   </MtchgSts>
</TradDtls>
<FinInstrmId>
   <ISIN>BE6307085488</ISIN>
</FinInstrmId>
<QtyAndAcctDtls>
   <SttlmQty>
      <Qty>
         <FaceAmt>500000</FaceAmt>
      </Qty>
   </SttlmQty>
   <AcctOwnr>
      <Id>
         <AnyBIC>GKCCBEBBXXX</AnyBIC>
      </Id>
   </AcctOwnr>
   <SfkpgAcct>
      <Id>NBBE100808302044</Id>
   </SfkpgAcct>
</QtyAndAcctDtls>
<SttlmParams>
   <HldInd>
      <Ind>true</Ind>
      <Rsn>
         <Cd>
            <Cd>CSDH</Cd>
         </Cd>
      </Rsn>
   </HldInd>
   <Prty>
      <Nmrc>0001</Nmrc>
   </Prty>
   <SctiesTxTp>
      <Cd>CORP</Cd>
   </SctiesTxTp>
   <SttlmTxCond>
      <Cd>NOMC</Cd>
   </SttlmTxCond>
   <PrtlSttlmInd>NPAR</PrtlSttlmInd>
   <ModCxlAllwd>
      <Ind>false</Ind>
   </ModCxlAllwd>
</SttlmParams>
<DlvrgSttlmPties>
   <Dpstry>
      <Id>
         <AnyBIC>NBBEBEBB216</AnyBIC>
      </Id>
   </Dpstry>
   <Pty1>
      <Id>
         <AnyBIC>GKCCBEBBXXX</AnyBIC>
      </Id>
      <SfkpgAcct>
         <Id>NBBE100808302044</Id>
      </SfkpgAcct>
```

```
            </Pty1>
         </DlvrgSttlmPties>
         <RcvgSttlmPties>
            <Dpstry>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
            </Dpstry>
            <Pty1>
               <Id>
                  <AnyBIC>NBBEBEBB216</AnyBIC>
               </Id>
               <SfkpgAcct>
                  <Id>NBBE100899999982</Id>
               </SfkpgAcct>
            </Pty1>
         </RcvgSttlmPties>
      </SctiesSttlmTxInstr>
   </Document>
</Saa:Body>
```

5.4.2.8 (in case of N-account) Release of WT-transaction Debit of Investor DCA

This is WT transaction is linked with the coupon payment 5.4.2.7.

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>PARBFRPPXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>4662105751000</BizMsgIdr>
      <MsgDefIdr>sese.025.001.07</MsgDefIdr>
      <CreDt>2019-11-19T07:54:14Z</CreDt>
      <Prty>2019111900010318</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.025.001.07">
      <SctiesSttlmTxConf>
         <TxIdDtls>
            <AcctOwnrTxId>NONREF</AcctOwnrTxId>
            <AcctSvcrTxId>NBBE19274WT00006</AcctSvcrTxId>
            <MktInfrstrctrTxId>1910014517653925</MktInfrstrctrTxId>
            <SctiesMvmntTp>DELI</SctiesMvmntTp>
            <Pmt>APMT</Pmt>
            <CmonId>BE6307085400503N</CmonId>
         </TxIdDtls>
         <TradDtls>
            <TradDt>
               <Dt>
                  <Dt>2019-11-18</Dt>
               </Dt>
```

```
      </TradDt>
      <SttlmDt>
         <Dt>
            <Dt>2019-11-19</Dt>
         </Dt>
      </SttlmDt>
      <FctvSttlmDt>
         <Dt>
            <DtTm>2019-11-19T08:52:55.313477</DtTm>
         </Dt>
      </FctvSttlmDt>
   </TradDtls>
   <FinInstrmId>
      <ISIN>BE6307085488</ISIN>
   </FinInstrmId>
   <QtyAndAcctDtls>
      <SttldQty>
         <Qty>
            <FaceAmt>0</FaceAmt>
         </Qty>
      </SttldQty>
      <AcctOwnr>
         <Id>
            <AnyBIC>PARBFRPPXXX</AnyBIC>
         </Id>
      </AcctOwnr>
      <SfkpgAcct>
         <Id>NBBE100840172002</Id>
      </SfkpgAcct>
      <CshAcct>
         <Prtry>CFREURPARBFRPPXXX-MAIN-ACCOUNT</Prtry>
      </CshAcct>
   </QtyAndAcctDtls>
   <SttlmParams>
      <Prty>
         <Nmrc>0001</Nmrc>
      </Prty>
      <SctiesTxTp>
         <Cd>TRAD</Cd>
      </SctiesTxTp>
   </SttlmParams>
   <DlvrgSttlmPties>
      <Dpstry>
         <Id>
            <AnyBIC>NBBEBEBB216</AnyBIC>
         </Id>
      </Dpstry>
      <Pty1>
         <Id>
            <AnyBIC>PARBFRPPXXX</AnyBIC>
         </Id>
         <SfkpgAcct>
            <Id>NBBE100840172002</Id>
         </SfkpgAcct>
      </Pty1>
   </DlvrgSttlmPties>
   <RcvgSttlmPties>
      <Dpstry>
         <Id>
            <AnyBIC>NBBEBEBB216</AnyBIC>
         </Id>
      </Dpstry>
      <Pty1>
         <Id>
            <AnyBIC>NBBEBEBBWTX</AnyBIC>
         </Id>
         <SfkpgAcct>
            <Id>NBBE100899900101</Id>
         </SfkpgAcct>
```

```
            </Pty1>
         </RcvgSttlmPties>
         <SttldAmt>
            <Amt Ccy="EUR">234.9</Amt>
            <CdtDbtInd>CRDT</CdtDbtInd>
         </SttldAmt>
         <SplmtryData>
            <PlcAndNm>/Document/SctiesSttlmTxConf/TxIdDtls</PlcAndNm>
            <Envlp>
               <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

                  <SctiesSttlmSD1>
                     <RltdTxId>0119398362452000</RltdTxId>
                  </SctiesSttlmSD1>
               </Document>
            </Envlp>
         </SplmtryData>
      </SctiesSttlmTxConf>
   </Document>
</Saa:Body>
```

5.4.3 Corporate actions in Foreign currency (without transferaccount)

5.4.3.1 MT202: Instruct debit of FCA of Paying agent towards FCA of Investor.

```
Payment of 01st investor position of coupon 20.

UETR in header field 121 4d4d4c6e-a58c-47d2-ad06-e812d882cc07

:20:BE6317370502001 0[6]
:21:BE63173705020010
:32A:191115USD270,00
:52A:NBBEBEBB216
:53B:/BE02058910810340
:58A:/BE66058910810643
NBBEBEBB216
:72:/BNF/ORDER NBBEBEBB243 BE6317370516
```

5.4.3.2 Reception of MT900 (debit confirmation of FCA)

```
:20:CMI1115130105099
:21:BE63173705020010
:25:/BE02058910810340
:32A:191115USD270,00
:52A:NBBEBEBB216
:72: BNF ORDER NBBEBEBB243 BE6317370516
```

5.4.3.3 Send MT566 to paying agent

```
:16R:GENL
:20C::CORP//BE63173705160002
:20C::SEME//20191115S0000509
:20C::COAF//BE63173705160002
:23G:NEWM
:22F::CAEV//INTR
:98C::PREP//20191115130139
:16S:GENL
:16R:USECU
:95P::ACOW//NBBEBEBB216
:97A::SAFE//NBBE100899999982
:35B:ISIN BE6317370516
BELFIUS FINANCING CY SA
:16R:FIA
:11A::DENO//USD
```

---

[6] This is different from the ASRF in the MT564 – as the MT564 is a general message for the complete corporate action. MT566s will be dispersed to the paying agent per accountposition.

```
:98A::COUP//20191115
:98A::MATU//20211113
:98A::ISSU//20191113
:92A::INTR//2,0
:16S:FIA
:93B::CONB//FAMT/13500,0
:16S:USECU
:16R:CADETL
:98A::XDTE//20191115
:98A::RDTE//20191114
:69A::INPE//20191114/20191115
:99A::DAAC//001
:92A::INTR//2,0
:16S:CADETL
:16R:CACONF
:13A::CAON//001
:22H::CAOP//CASH
:16R:CASHMOVE
:22H::CRDB//DEBT
:97A::CASH//BE66058910810643
:19B::PSTA//USD270,00
:19B::GRSS//USD270,00
:98A::POST//20191115
:98A::VALU//20191115
:98A::FXDT//20191114
:98A::PAYD//20191115
:92B::EXCH//USD/EUR/0,90859531
:92A::INTP//0,005555556
:92A::RATE//100,0
:92A::TAXR//0,0
:16S:CASHMOVE
:16S:CACONF
:16R:ADDINFO
:70E::ADTX//ASRF// BE63173705020010
/INFO//UETR
      /4d4d4c6e-a58c-47d2-ad06-
      /e812d882cc07
:95P::PAYA//NBBEBEBB216
:16S:ADDINFO
```

5.4.3.4 Send MT566 to investor (if investor position is on X-account)

```
:16R:GENL
:20C::CORP//BE63173705160002
:20C::SEME//20191115S0000512
:20C::COAF//BE63173705160002
:23G:NEWM
:22F::CAEV//INTR
:98C::PREP//20191115130145
:16S:GENL
:16R:USECU
:95P::ACOW//NBBEBEBB273
:97A::SAFE//NBBE100860021001
:35B:ISIN BE6317370516
BELFIUS FINANCING CY SA
:16R:FIA
:11A::DENO//USD
:98A::COUP//20191115
:98A::MATU//20211113
:98A::ISSU//20191113
:92A::INTR//2,0
:16S:FIA
:93B::CONB//FAMT/13500,0
:16S:USECU
:16R:CADETL
:98A::XDTE//20191115
:98A::RDTE//20191114
:69A::INPE//20191114/20191115
:99A::DAAC//001
:92A::INTR//2,0
:16S:CADETL
:16R:CACONF
:13A::CAON//001
:22H::CAOP//CASH
```

```
:16R:CASHMOVE
:22H::CRDB//CRED
:97A::CASH//BE66058910810643
:19B::PSTA//USD270,00
:19B::GRSS//USD270,00
:98A::POST//20191115
:98A::VALU//20191115
:98A::FXDT//20191114
:98A::PAYD//20191115
:92B::EXCH//USD/EUR/0,90859531
:92A::INTP//0,005555556
:92A::RATE//100,0
:92A::TAXR//0,0
:16S:CASHMOVE
:16S:CACONF
:16R:ADDINFO
:70E::ADTX//ASRF// BE63173705020010
/INFO//UETR
      /4d4d4c6e-a58c-47d2-ad06-
      /e812d882cc07
:95P::PAYA//NBBEBEBB216
:16S:ADDINFO
```

5.4.3.5 Send MT566 to investor (if investor position is on N-account)

```
:16R:GENL
:20C::CORP//BE63173705160002
:20C::SEME//20191115S0000512
:20C::COAF//BE63173705160002
:23G:NEWM
:22F::CAEV//INTR
:98C::PREP//20191115130145
:16S:GENL
:16R:USECU
:95P::ACOW//NBBEBEBB273
:97A::SAFE//NBBE100860022001
:35B:ISIN BE6317370516
BELFIUS FINANCING CY SA
:16R:FIA
:11A::DENO//USD
:98A::COUP//20191115
:98A::MATU//20211113
:98A::ISSU//20191113
:92A::INTR//2,0
:16S:FIA
:93B::CONB//FAMT/13500,0
:16S:USECU
:16R:CADETL
:98A::XDTE//20191115
:98A::RDTE//20191114
:69A::INPE//20191114/20191115
:99A::DAAC//001
:92A::INTR//2,0
:16S:CADETL
:16R:CACONF
:13A::CAON//001
:22H::CAOP//CASH
:16R:CASHMOVE
:22H::CRDB//CRED
:97A::CASH//BE66058910810643
:19B::PSTA//USD270,00
:19B::GRSS//USD270,00
:19B::NETT//USD270,00
:19B::WITL//EUR73,60
:98A::POST//20191115
:98A::VALU//20191115
:98A::FXDT//20191114
:98A::PAYD//20191115
:92B::EXCH//USD/EUR/0,90859531
:92A::INTP//0,005555556
:92A::RATE//100,0
:92A::TAXR//30,0
:16S:CASHMOVE
:16S:CACONF
:16R:ADDINFO
```

```
:70E::ADTX//ASRF// BE6317370502002N
/INFO//UETR
      /4d4d4c6e-a58c-47d2-ad06-
      /e812d882cc08
:95P::PAYA//NBBEBEBB216
:16S:ADDINFO
```

5.4.3.6 Debit of Investor Securities Account in case of redemption

5.4.3.6.1 SESE.023 DEBITING INVESTOR SECURITIES (N-)ACCOUNT TOWARDS ISSUANCE ACCOUNT.

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <ClrSysMmbId>
                  <ClrSysId>
                     <Prtry>T2S</Prtry>
                  </ClrSysId>
                  <MmbId>NBBSSS</MmbId>
               </ClrSysMmbId>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>20191105S0000363</BizMsgIdr>
      <MsgDefIdr>sese.023.001.07</MsgDefIdr>
      <CreDt>2019-11-05T17:26:49Z</CreDt>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.023.001.07">
      <SctiesSttlmTxInstr>
         <TxId>NBBE19309CR00007</TxId>
         <SttlmTpAndAddtlParams>
            <SctiesMvmntTp>DELI</SctiesMvmntTp>
            <Pmt>FREE</Pmt>

             <CmonId>BE6317370500002N</CmonId>
            <CorpActnEvtId>BE63173705160000</CorpActnEvtId>
         </SttlmTpAndAddtlParams>
         <TradDtls>
            <TradDt>
               <Dt>
                  <Dt>2019-11-05</Dt>
               </Dt>
            </TradDt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-11-06</Dt>
               </Dt>
            </SttlmDt>
            <MtchgSts>
               <Cd>MACH</Cd>
            </MtchgSts>
         </TradDtls>
         <FinInstrmId>
```

```
      <ISIN>BE6317370516</ISIN>
   </FinInstrmId>
   <QtyAndAcctDtls>
      <SttlmQty>
         <Qty>
            <FaceAmt>13500</FaceAmt>
         </Qty>
      </SttlmQty>
      <AcctOwnr>
         <Id>
            <AnyBIC>NBBEBEBB273</AnyBIC>
         </Id>
      </AcctOwnr>
      <SfkpgAcct>
         <Id>NBBE100860022001</Id>
      </SfkpgAcct>
   </QtyAndAcctDtls>
   <SttlmParams>
      <HldInd>
         <Ind>true</Ind>
         <Rsn>
            <Cd>
               <Cd>CSDH</Cd>
            </Cd>
         </Rsn>
      </HldInd>
      <Prty>
         <Nmrc>0001</Nmrc>
      </Prty>
      <SctiesTxTp>
         <Cd>CORP</Cd>
      </SctiesTxTp>
      <SttlmTxCond>
         <Cd>NOMC</Cd>
      </SttlmTxCond>
      <PrtlSttlmInd>NPAR</PrtlSttlmInd>
      <ModCxlAllwd>
         <Ind>false</Ind>
      </ModCxlAllwd>
   </SttlmParams>
   <DlvrgSttlmPties>
      <Dpstry>
         <Id>
            <AnyBIC>NBBEBEBB216</AnyBIC>
         </Id>
      </Dpstry>
      <Pty1>
         <Id>
            <AnyBIC>NBBEBEBB273</AnyBIC>
         </Id>
         <SfkpgAcct>
            <Id>NBBE100860022001</Id>
         </SfkpgAcct>
      </Pty1>
   </DlvrgSttlmPties>
   <RcvgSttlmPties>
      <Dpstry>
         <Id>
            <AnyBIC>NBBEBEBB216</AnyBIC>
         </Id>
      </Dpstry>
      <Pty1>
         <Id>
            <AnyBIC>NBBEBEBB216</AnyBIC>
         </Id>
         <SfkpgAcct>
            <Id>NBBE100899999982</Id>
         </SfkpgAcct>
      </Pty1>
```

```
         </RcvgSttlmPties>
      </SctiesSttlmTxInstr>
   </Document>
</Saa:Body>
```

5.4.3.7 (in case of N-account) Settlement of WT-transaction Debit of Investor DCA

5.4.3.7.1 THE SESE.023 FOR WTX LINKED TO A SESE.023 OF A REDM

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <ClrSysMmbId>
                  <ClrSysId>
                     <Prtry>T2S</Prtry>
                  </ClrSysId>
                  <MmbId>NBBSSS</MmbId>
               </ClrSysMmbId>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>TRGTXE2SXXX</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>20191126S0002468</BizMsgIdr>
      <MsgDefIdr>sese.023.001.07</MsgDefIdr>
      <CreDt>2019-11-26T19:06:10Z</CreDt>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.023.001.07">
      <SctiesSttlmTxInstr>
         <TxId>NBBE19330WT00098</TxId>
         <SttlmTpAndAddtlParams>
            <SctiesMvmntTp>RECE</SctiesMvmntTp>
            <Pmt>APMT</Pmt>
            <CmonId>BE6317370502002N</CmonId>
         </SttlmTpAndAddtlParams>
         <Lnkgs>
            <PrcgPos>
               <Cd>AFTE</Cd>
            </PrcgPos>
            <Ref>
               <MktInfrstrctrTxId>1910014517653925</MktInfrstrctrTxId>

            </Ref>
         </Lnkgs>
         <TradDtls>
            <TradDt>
               <Dt>
                  <Dt>2019-09-26</Dt>
               </Dt>
            </TradDt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-09-30</Dt>
               </Dt>
            </SttlmDt>
```

```
      <MtchgSts>
         <Cd>MACH</Cd>
      </MtchgSts>
   </TradDtls>
   <FinInstrmId>
      <ISIN>BE6317370516</ISIN>
   </FinInstrmId>
   <QtyAndAcctDtls>
      <SttlmQty>
         <Qty>
            <FaceAmt>0</FaceAmt>
         </Qty>
      </SttlmQty>
      <AcctOwnr>
         <Id>
            <AnyBIC>NBBEBEBB273</AnyBIC>
         </Id>
      </AcctOwnr>
      <SfkpgAcct>
         <Id> NBBE100860022001</Id>
      </SfkpgAcct>
   </QtyAndAcctDtls>
   <SttlmParams>
      <HldInd>
         <Ind>false</Ind>
         <Rsn>
            <Cd>
               <Cd>PTYH</Cd>
            </Cd>
         </Rsn>
      </HldInd>
      <Prty>
         <Nmrc>0001</Nmrc>
      </Prty>
      <SctiesTxTp>
         <Cd>CORP</Cd>
      </SctiesTxTp>
      <BnfclOwnrsh>
         <Ind>true</Ind>
      </BnfclOwnrsh>
      <ModCxlAllwd>
         <Ind>false</Ind>
      </ModCxlAllwd>
   </SttlmParams>
   <DlvrgSttlmPties>
      <Dpstry>
         <Id>
            <AnyBIC>NBBEBEBB216</AnyBIC>
         </Id>
      </Dpstry>
      <Pty1>
         <Id>
            <AnyBIC>NBBEBEBBWTX</AnyBIC>
         </Id>
         <SfkpgAcct>
            <Id>NBBE100899900101</Id>
         </SfkpgAcct>
      </Pty1>
   </DlvrgSttlmPties>
   <RcvgSttlmPties>
      <Dpstry>
         <Id>
            <AnyBIC>NBBEBEBB216</AnyBIC>
         </Id>
      </Dpstry>
      <Pty1>
         <Id>
            <AnyBIC> NBBEBEBB273</AnyBIC>
         </Id>
```

```
            <SfkpgAcct>
               <Id>NBBE100860022001</Id>
            </SfkpgAcct>
         </Pty1>
      </RcvgSttlmPties>
      <SttlmAmt>
         <Amt Ccy="EUR">73.60</Amt>
         <CdtDbtInd>DBIT</CdtDbtInd>
      </SttlmAmt>
   </SctiesSttlmTxInstr>
</Document>
</Saa:Body>
```

5.4.3.7.2 THE SESE.025 FOR WTX LINKED TO A SESE.023 OF A REDM

```
<Saa:Body xmlns:Saa="urn:swift:saa:xsd:saa.2.0">
   <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
      <Fr>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB216</BICFI>
               <Othr>
                  <Id>TRGTXE2SXXX</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </Fr>
      <To>
         <FIId>
            <FinInstnId>
               <BICFI>NBBEBEBB273</BICFI>
               <Othr>
                  <Id>NBBEBEBB216</Id>
               </Othr>
            </FinInstnId>
         </FIId>
      </To>
      <BizMsgIdr>4662105751000</BizMsgIdr>
      <MsgDefIdr>sese.025.001.07</MsgDefIdr>
      <CreDt>2019-11-19T07:54:14Z</CreDt>
      <Prty>2019111900010318</Prty>
   </AppHdr>
   <Document xmlns="urn:iso:std:iso:20022:tech:xsd:sese.025.001.07">
      <SctiesSttlmTxConf>
         <TxIdDtls>
            <AcctOwnrTxId>NONREF</AcctOwnrTxId>
            <AcctSvcrTxId>NBBE19274WT00006</AcctSvcrTxId>
            <MktInfrstrctrTxId>1910014517653925</MktInfrstrctrTxId>
            <SctiesMvmntTp>DELI</SctiesMvmntTp>
            <Pmt>APMT</Pmt>
            <CmonId>BE6317370502002N</CmonId>
         </TxIdDtls>
         <TradDtls>
            <TradDt>
               <Dt>
                  <Dt>2019-09-26</Dt>
               </Dt>
            </TradDt>
            <SttlmDt>
               <Dt>
                  <Dt>2019-09-30</Dt>
               </Dt>
            </SttlmDt>
            <FctvSttlmDt>
               <Dt>
                  <DtTm>2019-11-19T08:52:55.313477</DtTm>
               </Dt>
            </FctvSttlmDt>
         </TradDtls>
         <FinInstrmId>
```

```
      <ISIN>BE6317370516</ISIN>
   </FinInstrmId>
   <QtyAndAcctDtls>
      <SttldQty>
         <Qty>
            <FaceAmt>0</FaceAmt>
         </Qty>
      </SttldQty>
      <AcctOwnr>
         <Id>
            <AnyBIC>NBBEBEBB273</AnyBIC>
         </Id>
      </AcctOwnr>
      <SfkpgAcct>
         <Id>NBBE100860022001</Id>
      </SfkpgAcct>
      <CshAcct>
         <Prtry>CFREUR NBBEBEBB273-MAIN-ACCOUNT</Prtry>
      </CshAcct>
   </QtyAndAcctDtls>
   <SttlmParams>
      <Prty>
         <Nmrc>0001</Nmrc>
      </Prty>
      <SctiesTxTp>
         <Cd>TRAD</Cd>
      </SctiesTxTp>
   </SttlmParams>
   <DlvrgSttlmPties>
      <Dpstry>
         <Id>
            <AnyBIC>NBBEBEBB216</AnyBIC>
         </Id>
      </Dpstry>
      <Pty1>
         <Id>
            <AnyBIC> NBBEBEBB273</AnyBIC>
         </Id>
         <SfkpgAcct>
            <Id> NBBE100860022001</Id>
         </SfkpgAcct>
      </Pty1>
   </DlvrgSttlmPties>
   <RcvgSttlmPties>
      <Dpstry>
         <Id>
            <AnyBIC>NBBEBEBB216</AnyBIC>
         </Id>
      </Dpstry>
      <Pty1>
         <Id>
            <AnyBIC>NBBEBEBBWTX</AnyBIC>
         </Id>
         <SfkpgAcct>
            <Id>NBBE100899900101</Id>
         </SfkpgAcct>
      </Pty1>
   </RcvgSttlmPties>
   <SttldAmt>
      <Amt Ccy="EUR">73.60</Amt>
      <CdtDbtInd>CRDT</CdtDbtInd>
   </SttldAmt>
   <SplmtryData>
      <PlcAndNm>/Document/SctiesSttlmTxConf/TxIdDtls</PlcAndNm>
      <Envlp>
         <Document xmlns="urn:eurosystem:xsd:DRAFT2supl.021.001.01">

            <SctiesSttlmSD1>
               <RltdTxId>0119398362452000</RltdTxId>
```

```
                </SctiesSttlmSD1>
             </Document>
          </Envlp>
       </SplmtryData>
    </SctiesSttlmTxConf>
 </Document>
</Saa:Body>
```

NBB – Payments and Securities Service
Securities Settlement System
Boulevard de Berlaimont 14
BE-1000 Brussels
Phone + 32 (0)2 221 36 00
sss@nbb.be

FOREIGN CURRENCY CASH ACCOUNT SET-UP

Participant Name: .....

Participant BIC11: .....

Currency: - Select -

Usage: - Select -

Securities Account (Optional*): .....

.....

.....

.....

.....

** If no securities account is defined, this set-up will be considered as default for this currency.*

Debit	**MT202**	**Production**
Foreign Cash Account Provider BIC11	receiver	
Foreign Cash Account Provider Name	receiver	
Foreign Cash Account Owner BIC11	52a	
Foreign Cash Account Owner Name	52a	
Debit Account	53b	

Credit	**MT202**	**Production**
Intermediary BIC11 (Optional)	56a	
Intermediary Name (Optional)	56a	
Foreign Cash Account Provider BIC11	57a	
Foreign Cash Account Provider Name	57a	
Credit Account	58a	
Foreign Cash Account Owner BIC11	58a	
Foreign Cash Account Owner Name	58a	

Place and date of signature:

(Signature, name and position of the person(s) entitled to validly commit the institution)

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 28

INSOLVENCY PROCEDURE

In accordance with Article 41 CSDR and the TARGET2-Securities Manual Of Procedures, the NBB has defined rules and procedures applicable in case of default of its Participants. Those rules and procedures are described in the Terms and Conditions governing the participation in the NBB-SSS (NBB-SSS Terms and Conditions).

The main purpose of this Annex is to provide information on actions that the NBB shall take in the event of the opening of Insolvency proceedings[1] against a Participant. The procedure follows the principles laid down in the Settlement Finality Directive and the Settlement Finality Law as well as the NBB-SSS Terms and Conditions.

NBB-SSS Operational Procedure

Upon receipt of information regarding the opening of Insolvency proceedings against a Participant, the NBB-SSS shall i) inform the TARGET2-Securities (T2S) community and the NBB-SSS community (including the NBB's crisis management bodies), and ii) manage the insolvency operationally in its application RAMSES.

The NBB-SSS shall set the parameter "Under Insolvency Situation" for the insolvent Participant and shall monitor any settlement on the involved Securities Accounts in accordance with the Settlement Finality Directive. The NBB-SSS shall also take measures in order to prevent the introduction of new Instructions into the system. The NBB-SSS shall suspend or remove any power of attorney, suspend or remove technical privileges in T2S and restrict Participant's privileges in the RAMSES GUI to "view only" in order to remove the Participant's ability to enter new Instructions and/or to manage Instructions on the T2S platform.

The NBB-SSS operates its securities settlement system within T2S and in accordance with the Settlement Finality Directive. T2S identifies six scenarios in which Instructions can be impacted by the Participant's Insolvency proceedings. The NBB-SSS covers those scenarios in its operational procedures:

[1] As defined in the NBB-SSS Terms and Conditions (Article 2)

1) Transfer orders entered before the opening of insolvency proceedings;
2) Transfer orders entered after the opening of insolvency proceedings, which were matched on the T2S platform before the CSD/NCB becomes aware and for settlement on the same business day;
3) Transfer orders entered after the opening of insolvency proceedings, which were matched on the T2S platform before the CSD/NCB becomes aware but for settlement later than on the day of insolvency;
4) Transfer orders entered after the opening of insolvency proceedings, which were not matched on the T2S platform by the time the CSD/NCB becomes aware;
5) Transfer orders entered after the moment the CSD/NCB becomes aware of insolvency proceedings upon request of the insolvency liquidator;
6) Transfer orders entered after the moment the CSD/NCB becomes aware of insolvency proceedings without involvement of the insolvency liquidator.

According to Article 6.2.2.9 of the NBB-SSS Terms and Conditions (Handling of Instructions upon Insolvency event) any Instruction impacted by Insolvency proceedings entered into the system may be cancelled by the NBB-SSS at the End of Day on the day of the opening of the Insolvency proceeding, or on the subsequent days, provided that the Instruction has not been settled yet, regardless the Intended Settlement Date and regardless whether the Instruction has been "matched" or not. The decision to cancel shall depend on information/instructions received from the appointed administrator/curator and/or of decision taken by the NBB's crisis management bodies. Pending reverse auto-collateralisation Instructions and relocation Instructions shall in principle continue to be settled. The insolvent Participant, the T2S community and the NBB-SSS community will be kept informed without due delay whenever relevant.

Upon completion of the insolvency operational procedures the NBB-SSS shall terminate the participation of the insolvent Participant in accordance with Article 10.2.2 of the NBB-SSS Terms and Conditions.

Testing of the Procedure

The NBB-SSS shall undertake with its Participants periodic testing and review of its insolvency procedure. Such test shall be performed at least annually and, in any case following any substantive changes to the NBB-SSS insolvency procedure.

Prior to each test, the NBB-SSS shall define the parameters according to which such test shall be run and taking into account different types of Participants. The NBB-SSS shall issue an assessment report of the test. This report and any changes to the insolvency rules and procedure, if any, will be shared with the Management Committee, the Risk Committee, the Chief Risk Officer and with the User Committee.

NBB – Payments and Securities
Securities Settlement System
Boulevard de Berlaimont 14
1000 Brussels
+32 (0)2 221 36 00
sss@nbb.be

Annex 29

Static Data for

STATUS ELIGIBLE COUNTERPARTY CSD

BIC 11 of Investor CSD, Participant in NBB-SSS	
Name of Investor CSD, Participant in NBB-SSS	
LEI of Investor CSD, Participant in NBB-SSS	

BIC11 of Instructing CSD	
Name of Instructing CSD	
LEI of Instructing CSD	

Valid from	

To comply with the T2S Requirement T2S.05.126 “Eligible Counterpart CSD Validation” and T2S.16.920 ”Attribute requirements for Eligible Counterpart CSD” as stated in the T2S User Requirements Document (T2S URD), the Investor CSD, acting as Participant in the NBB-SSS, expressly authorises the NBB-SSS to set the Instructing CSD’s static data as “Eligible Counterparty CSD”. The investor CSD acknowledges and agrees that such authorisation allows the Instructing CSD to send, on its behalf, settlement Instructions in NBB-SSS ISINs.

The Investor CSD, Participant in the NBB-SSS, undertakes to inform the NBB-SSS in writing, without delay, of any withdrawal of the above authorisation. The Participant recognises that such withdrawal shall, however, only take effect, and thus entail an obligation on the NBB-SSS to refuse instructions sent by the Instructing CSD, in the case of instructions sent on or after the NBB-SSS working day following the date on which the NBB-SSS receives notification of the said withdrawal.

Place and date of signature Investor CSD

Place and date of signature Instructing CSD

[Signature, name and position of the person(s) entitled to validly commit the institution]

National Bank of Belgium
Limited Liability company
RLP Brussels – Company's number: 0203.201.340
Registered office: boulevard de Berlaimont 14 – BE-1000 Brussels
www.nbb.be

Further information

Anyone requiring further information on the content of this document can contact the Payments and Securities division of the National Bank of Belgium

Tel. +32 2 221 22 18

sss@nbb.be – www.nbbsss.be

Editor

Dirk Ooms
Head of the Financial Markets department

National Bank of Belgium
boulevard de Berlaimont 14 – BE-1000 Brussels

Published in January 2020