**Financial Markets Department**
Payments & Securities
Current account – Casper helpdesk

boulevard de Berlaimont 14
BE-1000 Brussels

Phone : + 32 (0)2 221 20 48
Email : casper.helpdesk@nbb.be

# Current account opening

**IBAN:** B E _ _ 1 0 0 0 0 _ _ _ _ _ _ _ (to be filled in by the NBB)

**Account name[1]:**

## 1. GENERAL INFORMATION

BIC11 (if applicable):

Company name:

Legal Entity identifier (LEI):

Charter of foundation:
Place
Date (DDMMYYYY)
Publication in the Law Gazette[2]:
Number
Date (DDMMYYYY)
Company number

Address[3]:

Email address (group mailbox):

Phone:

[1] Name of the entity as mentioned in the Articles of Association.

[2] Schedules to the Belgian Official Gazette for companies established in Belgium.
A copy of the publication of the following documents, or official proof of submission for publication, from the Schedules to the Belgian Official Gazette (or, for foreign companies: a copy from the official Gazette of the country where this company is established) must be added to this document:
- the most recent version of the coordinated Articles of Association of the company;
- the resolutions appointing the members of the organs entitled to represent and to bind the company, a.o. the person charged with the day-to-day management or the managing director;
- the possible resolutions of the competent organ designating, pursuant to the Articles of Association, the officers who are authorized to sign on behalf of the company.

[3] Address of the headquarter

Contact person:

First name
Name
Personal email address
Phone/Mobile

## 2. BILLING INFORMATION

Company number:

VAT number:

Billing address[4] [5]:

Billing email address[6]:

Contact person billing:

First name
Name
Personal email address
Phone/Mobile

## 3. STATEMENTS:

*There are three options to receive account statements. Clients using the SWIFT network receive their statements via an MT950 message. Other clients can choose to receive their statements via email either in PDF or CODA[7] format (or both). Clients using SWIFT can opt for additional PDF or CODA formatted statements.*

Format preference (*please select at least one option*):

☐ PDF

Please specify email address[6]

☐ CODA

Please specify email address[6]

☐ MT950 (only if SWIFT BIC)

## 4. INFORMATION MESSAGES:

*The NBB can send its clients information messages via email (e.g. exceptional service announcements).*

Email address (group mailbox)[6]:

[4] Please specify the relevant department

[5] If different from company address

[6] If different from general email address

[7] Coded statement of account: banking standard specifying the layout and structure of coded electronic statements.

## 5. DECLARATION:

*The members of the Board mentioned below declare that they have taken note of the Terms and Conditions governing Current accounts opened in Casper and accept them without any reservation.*

| | |
|---|---|
| First name | First name |
| | |
| Name | Name |
| | |
| Title (function) | Title (function) |
| | |
| Signature | Signature |
| | |
| Date (DDMMYYYY) | Date (DDMMYYYY) |
| | |

**Financial Markets Department**
Payments & Securities
Current account – Casper helpdesk
boulevard de Berlaimont 14
BE-1000 Brussels

Phone : + 32 (0)2 221 20 48
Email : casper.helpdesk@nbb.be

BanqueNationaleBank
DE BELGIQUE VAN BELGIË
Eurosystem

# Power of attorney

**IBAN:**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | E | | | 1 | 0 | 0 | 0 | 0 | | | | | | | |

**opened at the National Bank of Belgium**

**Company** (Current account holder)

**registered at**

The company declares that the persons mentioned hereafter may operate its above-mentioned Current account and hereby assumes responsibility for (all) payments effected by these persons in accordance with this power of attorney.

It annexes hereto, for each person listed, a double-sided copy of the valid identity card (or any other official document of identification which replaces it). It will send of its own accord a copy of each new card replacing an expired card to the National Bank of Belgium.

**Any modification to this list must be notified to the National Bank of Belgium by means of a new form of power of attorney, with the copies of the required identity cards. On its receipt, the new power of attorney list will replace any previous list.**

**Persons who are authorized to sign for the company:**

| | Name and surname | Title | Specimen signature |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |

**According to the following rules:** (separately, jointly by two, etc.)
**If not specified, the signatures are considered to be valid separately.**

| |
|---|
| |

| | | |
|---|---|---|
| | , | |
| (place) | | (date) |

(signature and title of the persons
who bind the company with this statement)

Annex 2: Tariffs

**Financial Markets Department**
Payments & Securities
Current account – Casper helpdesk
boulevard de Berlaimont 14
BE-1000 Brussels

Phone : + 32 (0)2 221 20 48
Email : casper.helpdesk@nbb.be

# Casper Tariffs (19 October 2020)

## 1. All-in fees

Account holders in Casper will be charged with a fixed all-in fee per Current account on a yearly basis. The all-in fee depends on the profile of the Current account. Different account profiles have been identified, based on the number of payment Transactions per year per Current account.

### 1.1. General principles

1) Account holders will be charged at account level based on the profile of their Current account.
2) The account profile depends on the yearly payment Transaction volumes of the Current account.
3) Transactions are all debit and credit transactions related to a Current account, as defined in the Terms and Conditions governing the Current accounts opened in Casper.
4) Unless otherwise mentioned, the fees are automatically debited yearly into the Current account.

### 1.2. All-in-fee rates

The following all-in fees shall be charged by the NBB for the use of the Casper services.

| Account profile | Transaction volumes (yearly) | Tariff (yearly, VAT not included) |
|---|---|---|
| Profile 1 | 0 - 99 | € 250 |
| Profile 2 | 100 - 499 | € 500 |
| Profile 3 | 500 - 4.999 | € 1.500 |
| Profile 4 | 5.000 - 9.999 | € 5.000 |
| Profile 5 | > 10.000 | € 25.000 |

## 2. Casper GUI fees

For the Account holders with GUI access, the use of the Casper GUI is included in the all-in fee as referred to in this Annex.

Although the prior subscription to the NBB-Net VPN infrastructure is mandatory in order to access the Casper GUI, this connection via internet is not part of the Terms and Conditions governing the Current accounts opened in Casper and shall be charged separately by the NBB.

In order to access the Casper GUI, Account holders must use a token with electronic certificate provided by the NBB that remains valid for a period of maximum three years. A fee of 200 EUR per token is charged for the issuance of such token, which covers the costs of issuance, maintenance and support of the said token and certificate during the validity period. The same fee of 200 EUR per token is charged for each consecutive renewal of the validity period. In case of revocation of the certificate, in case of loss or theft of the token or in case of damage brought to the token making it unfit for use, a new token/certificate must be issued, which shall be charged at the same fee of 200 EUR and shall be valid for a new period of three years, without any refunding or deduction “pro rata temporis” of the fee paid for the issuance or renewal of the revoked certificate or of the lost, stolen or damaged token.

## 3. Information

**National Bank of Belgium**
Payments and securities
Casper helpdesk

Email: casper.helpdesk@nbb.be
Phone: +32 (0)2 221 20 48

**Financial Markets Department**
Payments & Securities
Current account – Casper helpdesk
boulevard de Berlaimont 14
BE-1000 Brussels

Phone : + 32 (0)2 221 20 48
Email : casper.helpdesk@nbb.be

BanqueNationaleBank
DE BELGIQUE VAN BELGIË
Eurosystem

# Conditions of use of the Casper Graphical User Interface

## Table of Contents

## 1. Scope

As referred into Article 7.3. of the Terms and Conditions governing Current accounts opened in Casper (hereinafter the "Casper Terms and Conditions'), an Account holder may issue Payment orders via the Casper Graphical User Interface (GUI). The connection to the Casper GUI is optional.

This Annex aims at defining the conditions of access, connection and use of the Casper 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 3 of the Casper Terms and Conditions. Furthermore, for the purpose of this Annex:

- **"Account holder's member"** means a natural person who is either a member of the staff of an Account holder or a member of its decision-making bodies;
- **"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 Casper 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;
  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 Account holder 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 (Account holders and Certificate users) to create, issue, manage, revoke and renew valid Certificates in the framework of the Casper 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, from its request to its end of subscription or revocation, as well as the relations that are established between the Account holder, 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 Account holders 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;
- **"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 Casper GUI by Account holders;

- **"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 (Account holders 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 Account holder 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 Casper GUI

The Account holder can access the Casper GUI if:

- it has installed and maintains a domestic IT infrastructure allowing a proper connection with the NBB;
- 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 Current account opening forms (Annex 1) and any additional information required or deemed useful by the NBB for the Account holder's registration;
- at least one Trusted agent appointed among the Account holder's members has undersigned and sent to the NBB the sub-Annex 3.3 of the Casper 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 Casper GUI; and
- it has successfully passed the Account holder certification tests.

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

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

### 4.1. Applicable rules: CPS, CP

As a rule, each Account holder 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 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 Account holder acknowledges and agrees that in its relations with the NBB, with the BdE in its capacity of Certification authority, 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. However, it is understood – and accepted by the Account holder – that for the analogical application to the NBB 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 Casper;
- 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 Casper;
- the Account holders 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 Casper account holders (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" for the application of Article 1.4 of the CPS;
- except when explicitly otherwise provided for in this Document, contacts between the Account holder, 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 Casper Terms and Conditions and its Annexes 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 Account holder 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 Account holder.

The version 1.3 of the ESCB-PKI CPS (dated June 1, 2015) is joined as sub-Annex 3.1 of the Casper Terms and Conditions, the version 1.3 of the ESCB-PKI CP for ESCB/SSM users' Certificates (dated May 11, 2015) is joined as sub-Annex 3.2a of the Casper Terms and Conditions and the version 1.2 of the ESCB-PKI CP for the non-ESCB/non-SSM users' Certificates (dated May 11, 2015) is joined as sub-Annex 3.2a of the Casper Terms and conditions. The Account holder 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 Casper website.

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

### 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 Account holder 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 Account holder 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 Casper 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.

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 Casper 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 Casper GUI and provide them with the adequate technical equipment;
- verifying the Account holder’s identity and its ongoing eligibility status with regard to the adherence to the NBB;
- 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 Account holder 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 Casper 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 Casper 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 an Account holder's access to Casper, which is not imputable to either SWIFT, the NBB-Net or the Account holder's network service provider.

4.2.3. The Account holder

The NBB shall validly rely on any information or message authenticated by a Certificate delivered to a Certificate holder who is an Account holder's member and shall lawfully carry out instructions and settle Payment orders signed with such a Certificate in the name of the said Account holder on its own behalf. The Account holder hereby acknowledges and agrees that it shall irrevocably, fully and definitely be bound by information, messages, instructions carried out and Payment orders settled by the NBB that are authenticated or signed with a Certificate delivered on behalf of one of the Account holder's members and, therefore, that it bears full and exclusive responsibility and liability toward other Account holders 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 Account holders 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 Account holder's members or not. No Certificate may be used as a group or entity bound Certificate. The Account holder 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 Account holder shall appoint at least one (preferably two or more) Trusted agent among the Account holder'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 Account holder shall verify that the Trusted agent has signed the "Terms and conditions relating to Trusted agents", joined as sub-Annex 3.3 of the Terms and conditions, and shall send the duly signed form to the NBB. Together with the Trusted agent, the Account holder 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 Account holder'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.

Each Account holder 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 Casper GUI.

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

The Account holder 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 Casper GUI. The NBB may request further information about the incident and, if necessary, request that the Account holder takes appropriate measures to prevent a recurrence of such an event. The NBB may also impose additional security requirements on the Account holder.

The Account holder 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 Account holders 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.

**Financial Markets Department**
Payments & Securities
Current account – Casper helpdesk
boulevard de Berlaimont 14
BE-1000 Brussels

Phone : + 32 (0)2 221 20 48
Email : casper.helpdesk@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

**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<br>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/2015/46**[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 ECB/2015/47[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 (EU) 2016/187 of the European Central Bank of 11 December 2015 amending Decision ECB/2013/1 laying down the framework for a public key infrastructure for the European System of Central Banks (ECB/2015/46).

[2] Decision (EU) 2016/188 of the European Central Bank of 11 December 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/2015/47).

[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]

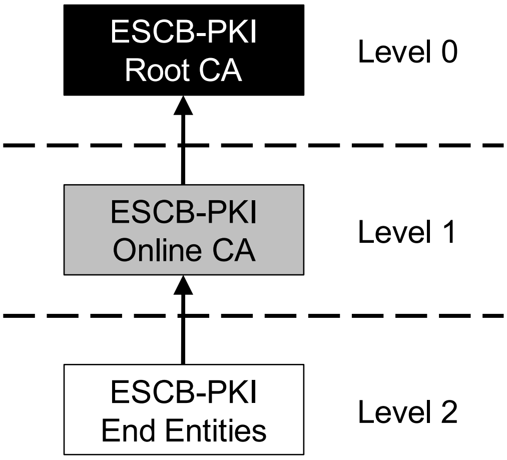
- Spanish Organic Law 15/1999, of 13 December 1999, on the protection of personal data
- Spanish Royal Decree 1720/2007, of 21 December2007, approving the Regulations for the development of Spanish Organic Law 15/1999.
- National legislation transposing Directive 95/46/EC and the Directive 99/93/EC applicable 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 Authorit**y (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)<br>Users from external organisations non-ESCB/non-SSM users)<br>Individuals in charge of the ESCB/SSM applications and technical components that use the certificate<br>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<br>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:<br>• SIGNATURE<br>• AUTHENTICATION<br>• ENCRYPTION<br>• MOBILE DEVICE<br>• SECURE EMAIL GATEWAY<br>• PROVISIONAL<br>• ADMINISTRATOR<br>• 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:<br>- Spanish Law 59/2003, of 19 December 2009, on electronic signature.<br>- 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.<br>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 ECB/2015/46 and Decision ECB/2015/47.

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 ECB/2015/47[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 of the European Central Bank 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/2015/47), not yet published in the Official Journal of the European Union.

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

**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/2015/46**[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 (EU) 2016/187 of the European Central Bank of 11 December 2015 amending Decision ECB/2013/1 laying down the framework for a public key infrastructure for the European System of Central Banks (ECB/2015/46).

[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 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.

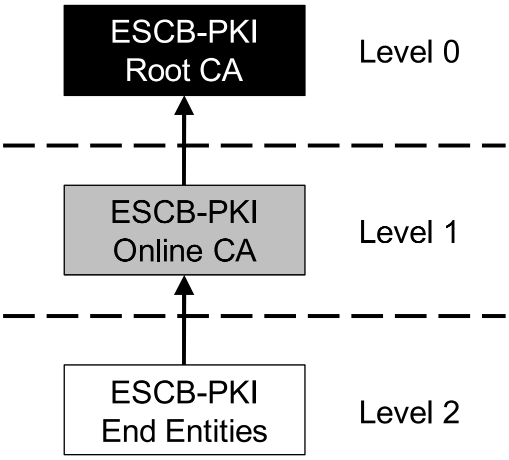
- Decision ECB/2015/47[6].

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)<br>0.4.0.127.0.10.1.2.2.1: Certificate Policy of |

[6] Decision (EU) 2016/188 of the European Central Bank of 11 December 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/2015/47).

| | |
|---|---|
| | Advanced Authentication certificate for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.2: Certificate Policy of Archived Encryption certificate for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.3: Certificate Policy of Non-Archived Encryption certificate for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.4: Certificate Policy of Advanced Signature certificate based on a SSCD for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.5: Certificate Policy of Advanced Signature certificate for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.6: Certificate Policy of Standard Authentication certificate for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.7: Certificate Policy of Mobile Device certificate for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.8: Certificate Policy of Secure E-mail Gateway certificate for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.9: Certificate Policy of Provisional certificate for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.10: Certificate Policy of Administrator certificate for ESCB/SSM users<br>0.4.0.127.0.10.1.2.2.11: Certificate Policy of Shared Mailbox certificate for ESCB/SSM users<br>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<br>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)<br>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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject | | |
| C | *[Registration Organisation Country]* | |
| O | EUROPEAN SYSTEM OF CENTRAL BANKS | |
| OU | *Central Bank or National Competent Authority within which user is member* | |
| PS | *User identifier (UID)* | |
| CN | [AUT:A] *Name Middle name Surnames* | |
| Subject Public Key Info | | |
| Algorithm | RSA Encryption | |
| Minimum Length | 2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier | | |
| KeyIdentifier | *SHA-1 hash over CA Issuer public key* | |
| AuthorityCertIssuer | *Not used* | |
| AuthorityCertSerialNumber | *Not used* | |
| KeyUsage | | Yes |
| Digital Signature[8] | 1 | |
| Non Repudiation | 0 | |
| Key Encipherment | 0 | |
| Data Encipherment | 0 | |
| Key Agreement | 1 | |
| Key Certificate Signature | 0 | |
| CRL Signature | 0 | |
| 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<br>UPN (1.3.6.1.4.1.311.20.2.3) | *User Principal Name (if available)* | |
| rfc822 | *Subject's Email* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.1.1) | *Subject's Name* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.1.2) | *Subject's Middle Name (if any)* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.1.3) | *Subject's Surname* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.1.10) | *Subject's First surname* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.1.4) | *Subject's Secondary surname (if any)* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.1.7) | *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]*<br>*[HTTP URI OCSP]*<br>*[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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject<br>C<br>O<br>OU<br>PS<br>CN | <br>*[Registration Organisation Country]*<br>EUROPEAN SYSTEM OF CENTRAL BANKS<br>*Central Bank or National Competent Authority within which user is member*<br>*User identifier (UID)*<br>[SIG:Q] *Name Middle name Surnames*<br>*OR*<br>[SIG:A] *Name Middle name Surnames*[9] | |
| Subject Public Key Info<br>Algorithm<br>Minimum Length | <br>RSA Encryption<br>2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier<br>KeyIdentifier<br>AuthorityCertIssuer<br>AuthorityCertSerialNumber | <br>*SHA-1 hash over CA Issuer public key*<br>*Not used*<br>*Not used* | |
| KeyUsage<br>Digital Signature<br>Non Repudiation<br>Key Encipherment<br>Data Encipherment<br>Key Agreement<br>Key Certificate Signature<br>CRL Signature | <br>0<br>1<br>0<br>0<br>0<br>0<br>0 | Yes |
| extKeyUsage | <br>emailProtection (1.3.6.1.5.5.7.3.4)<br>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 | *[OID ESCBPKI]*.2.2.4<br>OR<br>*[OID ESCBPKI]*.2.2.5[10] | |
| URL CPS | *[CPS-URL]* | |
| Subject Alternative Names | | |
| rfc822 | *Subject's Email* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.1) | *Subject's Name* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.2) | *Subject's Middle Name (if any)* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.3) | *Subject's Surname* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.10) | *Subject's First surname* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.4) | *Subject's Secondary surname (if any)* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.7) | *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]*<br>*[HTTP URI OCSP]*<br>*[IAM URI OCSP]* | |
| qcStatements | id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)<br>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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject | | |
| C | *[Registration Organisation Country]* | |
| O | EUROPEAN SYSTEM OF CENTRAL BANKS | |
| OU | *Central Bank or National Competent Authority within which user is member* | |
| PS | *User identifier (UID)* | |
| CN | [ENC:K] *Name Middle name Surnames*<br>[ENC:A] *Name Middle name Surnames*<br>[ENC:S] *Name Middle name Surnames* [12] | |
| Subject Public Key Info | | |
| Algorithm | RSA Encryption | |
| Minimum Length | 2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier | | |
| KeyIdentifier | *SHA-1 hash over CA Issuer public key* | |
| AuthorityCertIssuer | *Not used* | |
| AuthorityCertSerialNumber | *Not used* | |
| KeyUsage | | Yes |
| Digital Signature | 0 | |
| Non Repudiation | 0 | |
| Key Encipherment | 1 | |
| Data Encipherment | 1 | |
| Key Agreement | 0 | |
| Key Certificate Signature | 0 | |
| CRL Signature | 0 | |
| 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 | *[OID ESCBPKI]*.2.2.2<br>*[OID ESCBPKI]*.2.2.3<br>*[OID ESCBPKI]*.2.2.12 [13] | |
| URL CPS | *[CPS-URL]* | |
| Subject Alternative Names | | |
| rfc822 | *Subject's Email* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.1) | *Subject's Name* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.2) | *Subject's Middle Name (if any)* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.3) | *Subject's Surname* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.10) | *Subject's First surname* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.4) | *Subject's Secondary surname (if any)* | |
| RegisteredID (*[OID ESCBPKI]*.1.1.7) | *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]*<br>*[HTTP URI OCSP]*<br>*[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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject | | |
| C | *[Registration Organisation Country]* | |
| O | EUROPEAN SYSTEM OF CENTRAL BANKS | |
| OU | *Central Bank or National Competent Authority within which user is member* | |
| PS | *User identifier (UID)* | |
| CN | [AUT:S] *Name Middle name Surnames* | |
| Subject Public Key Info | | |
| Algorithm | RSA Encryption | |
| Minimum Length | 2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier | | |
| KeyIdentifier | *SHA-1 hash over CA Issuer public key* | |
| AuthorityCertIssuer | *Not used* | |
| AuthorityCertSerialNumber | *Not used* | |
| KeyUsage | | Yes |
| Digital Signature[14] | 1 | |
| Non Repudiation | 0 | |
| Key Encipherment[15] | 1 | |
| Data Encipherment[12] | 1 | |
| Key Agreement | 1 | |
| Key Certificate Signature | 0 | |
| CRL Signature | 0 | |
| extKeyUsage | | |
| | clientAuth (1.3.6.1.5.5.7.3.2)<br>emailProtection (1.3.6.1.5.5.7.3.4)<br>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<br>URL CPS | *[OID ESCBPKI]*.2.2.6<br>*[CPS-URL]* | |
| Subject Alternative Names<br>rfc822<br>RegisteredID (*[OID ESCBPKI]*.1.1)<br>RegisteredID (*[OID ESCBPKI]*.1.2)<br>RegisteredID (*[OID ESCBPKI]*.1.3)<br>RegisteredID (*[OID ESCBPKI]*.1.10)<br>RegisteredID (*[OID ESCBPKI]*.1.4)<br>RegisteredID (*[OID ESCBPKI]*.1.7) | <br>*Subject's Email*<br>*Subject's Name*<br>*Subject's Middle Name (if any)*<br>*Subject's Surname*<br>*Subject's First surname*<br>*Subject's Secondary surname (if any)*<br>*ESCB user identifier (UID)* | |
| Basic Constraints<br>CA<br>Path Length Constraint | <br>FALSE<br>*Not used* | Yes |
| CRL Distribution Points | | |
| Private Extensions | | |
| Authority Information Access<br>caIssuers<br>caIssuers<br>ocsp | <br>*[HTTP URI Root CA]*<br>*[HTTP URI Sub CA]*<br>*[HTTP URI OCSP ALIAS]*<br>*[HTTP URI OCSP]*<br>*[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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject | | |
| C | *[Registration Organisation Country]* | |
| O | EUROPEAN SYSTEM OF CENTRAL BANKS | |
| OU | *Central Bank or National Competent Authority within which user is member* | |
| PS | *User identifier (UID)* | |
| CN | [MOB:S] *Name Middle name Surnames* | |
| Subject Public Key Info | | |
| Algorithm | RSA Encryption | |
| Minimum Length | 2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier | | |
| KeyIdentifier | *SHA-1 hash over CA Issuer public key* | |
| AuthorityCertIssuer | *Not used* | |
| AuthorityCertSerialNumber | *Not used* | |
| KeyUsage | | Yes |
| Digital Signature | 1 | |
| Non Repudiation | 0 | |
| Key Encipherment | 0 | |
| Data Encipherment | 0 | |
| Key Agreement | 1 | |
| Key Certificate Signature | 0 | |
| CRL Signature | 0 | |
| extKeyUsage | | |
| | clientAuth (1.3.6.1.5.5.7.3.2)<br>emailProtection (1.3.6.1.5.5.7.3.4)<br>anyExtendedKeyUsage (2.5.29.37.0) | |
| Certificate Policies | | |
| Policy Identifier | *[OID ESCBPKI]*.2.2.7 | |
| URL CPS | *[CPS-URL]* | |
| Subject Alternative Names | | |

| | | |
|---|---|---|
| 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]*<br>*[HTTP URI OCSP]*<br>*[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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject | | |
| C | *[Registration Organisation Country]* | |
| O | EUROPEAN SYSTEM OF CENTRAL BANKS | |
| OU | *Central Bank or National Competent Authority within which user is member* | |
| PS | *User identifier (UID)* | |
| CN | [EGW:S] *Name Middle name Surnames* | |
| Subject Public Key Info | | |
| Algorithm | RSA Encryption | |
| Minimum Length | 2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier | | |
| KeyIdentifier | *SHA-1 hash over CA Issuer public key* | |
| AuthorityCertIssuer | *Not used* | |
| AuthorityCertSerialNumber | *Not used* | |
| KeyUsage | | Yes |
| Digital Signature | 1 | |
| Non Repudiation | 0 | |
| Key Encipherment | 1 | |
| Data Encipherment | 1 | |
| Key Agreement | 0 | |
| Key Certificate Signature | 0 | |
| CRL Signature | 0 | |
| extKeyUsage | | |
| | emailProtection (1.3.6.1.5.5.7.3.4) | |
| | anyExtendedKeyUsage (2.5.29.37.0) | |
| Certificate Policies | | |
| Policy Identifier | *[OID ESCBPKI]*.2.2.8 | |
| URL CPS | *[CPS-URL]* | |
| Subject Alternative Names | | |
| rfc822 | *Subject's Email* | |

| | | |
|---|---|---|
| RegisteredID<br>(*[OID ESCBPKI]*.1.1) | *Subject's Name* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.2) | *Subject's Middle Name (if any)* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.3) | *Subject's Surname* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.10) | *Subject's First surname* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.4) | *Subject's Secondary surname (if any)* | |
| RegisteredID<br>(*[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]*<br>*[HTTP URI OCSP]*<br>*[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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *Maximum 1 month* | |
| Subject | | |
| C | *[Registration Organisation Country]* | |
| O | EUROPEAN SYSTEM OF CENTRAL BANKS | |
| OU | *Central Bank or National Competent Authority within which user is member* | |
| PS | *User identifier (UID)* | |
| CN | [TMP:A] *Name Middle name Surnames* | |
| Subject Public Key Info | | |
| Algorithm | RSA Encryption | |
| Minimum Length | 2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier | | |
| KeyIdentifier | *SHA-1 hash over CA Issuer public key* | |
| AuthorityCertIssuer | *Not used* | |
| AuthorityCertSerialNumber | *Not used* | |
| KeyUsage | | Yes |
| Digital Signature | 1 | |
| Non Repudiation | 0 | |
| Key Encipherment | 0 | |
| Data Encipherment | 0 | |
| Key Agreement | 1 | |
| Key Certificate Signature | 0 | |
| CRL Signature | 0 | |
| 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 | *[OID ESCBPKI]*.2.2.9 | |
| URL CPS | *[CPS-URL]* | |

| | | |
|---|---|---|
| Subject Alternative Names | | |
| 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]*<br>*[HTTP URI OCSP]*<br>*[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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject<br>C<br>O<br>OU<br>PS<br>CN | <br>*[Registration Organisation Country]*<br>EUROPEAN SYSTEM OF CENTRAL BANKS<br>*Central Bank or National Competent Authority within which user is member*<br>*User identifier (UID)*<br>[ADM:A] *Name Middle name Surnames* | |
| Subject Public Key Info<br>Algorithm<br>Minimum Length | <br>RSA Encryption<br>2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier<br>KeyIdentifier<br>AuthorityCertIssuer<br>AuthorityCertSerialNumber | <br>*SHA-1 hash over CA Issuer public key*<br>*Not used*<br>*Not used* | |
| KeyUsage<br>Digital Signature<br>Non Repudiation<br>Key Encipherment<br>Data Encipherment<br>Key Agreement<br>Key Certificate Signature<br>CRL Signature | <br>1<br>0<br>0<br>0<br>1<br>0<br>0 | Yes |
| extKeyUsage | <br>emailProtection (1.3.6.1.5.5.7.3.4)<br>clientAuth (1.3.6.1.5.5.7.3.2)<br>smartCardLogon (1.3.6.1.4.1.311.20.2.2)<br>anyExtendedKeyUsage (2.5.29.37.0) | |
| Certificate Policies<br>Policy Identifier<br>URL CPS | <br>*[OID ESCBPKI]*.2.2.10<br>*[CPS-URL]* | |

| | | |
|---|---|---|
| Subject Alternative Names | | |
| RegisteredID<br>UPN (1.3.6.1.4.1.311.20.2.3) | *User Principal Name (if available)* | |
| rfc822 | *Subject's Email* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.1) | *Subject's Name* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.2) | *Subject's Middle Name (if any)* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.3) | *Subject's Surname* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.10) | *Subject's First surname* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.4) | *Subject's Secondary surname (if any)* | |
| RegisteredID<br>(*[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]*<br>*[HTTP URI OCSP]*<br>*[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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject<br>C<br>O<br>OU<br>PS<br>CN | <br>*[Registration Organisation Country]*<br>EUROPEAN SYSTEM OF CENTRAL BANKS<br>*Central Bank or National Competent Authority of the shared mailbox*<br>*ESCB user identifier (UID)*<br>[SHM:S] *Display Name* | |
| Subject Public Key Info<br>Algorithm<br>Minimum Length | <br>RSA Encryption<br>2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier<br>KeyIdentifier<br>AuthorityCertIssuer<br>AuthorityCertSerialNumber | <br>*SHA-1 hash over CA Issuer public key*<br>*Not used*<br>*Not used* | |
| KeyUsage<br>Digital Signature<br>Non Repudiation<br>Key Encipherment<br>Data Encipherment<br>Key Agreement<br>Key Certificate Signature<br>CRL Signature | <br>1<br>0<br>1<br>1<br>1<br>0<br>0 | Yes |
| extKeyUsage | <br>emailProtection (1.3.6.1.5.5.7.3.4)<br>clientAuth (1.3.6.1.5.5.7.3.2)<br>anyExtendedKeyUsage (2.5.29.37.0) | |
| Certificate Policies<br>Policy Identifier<br>URL CPS | <br>*[OID ESCBPKI]*.2.2.11<br>*[CPS-URL]* | |
| Subject Alternative Names | | |

| | | |
|---|---|---|
| rfc822<br>RegisteredID<br>(*[OID ESCBPKI]*.1.11)<br>RegisteredID<br>(*[OID ESCBPKI]*.1.7) | *Subject’s Email*<br>*Shared mailbox display name*<br><br>*ESCB user identifier (UID)* | |
| Basic Constraints<br>CA<br>Path Length Constraint | <br>FALSE<br>*Not used* | Yes |
| CRL Distribution Points | | |
| Private Extensions | | |
| Authority Information Access<br>caIssuers<br>caIssuers<br>ocsp | <br>*[HTTP URI Root CA]*<br>*[HTTP URI Sub CA]*<br>*[HTTP URI OCSP ALIAS]*<br>*[HTTP URI OCSP]*<br>*[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.

**Financial Markets Department**
Payments & Securities
Current account – Casper helpdesk
boulevard de Berlaimont 14
BE-1000 Brussels

Phone : + 32 (0)2 221 20 48
Email : casper.helpdesk@nbb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

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

**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/2015/46**[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 (EU) 2016/187 of the European Central Bank of 11 December 2015 amending Decision ECB/2013/1 laying down the framework for a public key infrastructure for the European System of Central Banks (ECB/2015/46).

[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

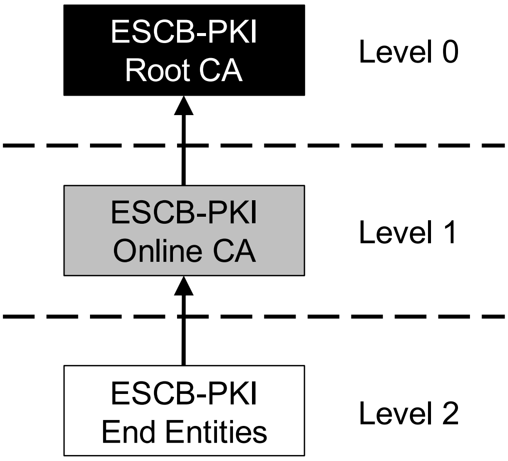
- Spanish Organic Law 15/1999, of 13 December 1999, on the protection of personal data
- Spanish Royal Decree 1720/2007, of 21 December2007, approving the Regulations for the development of Spanish Organic Law 15/1999.
- National legislation transposing Directive 95/46/EC and the Directive 99/93/EC applicable to the ESCB central banks and SSM national competent authorities acting as Registration Authorities.
- Decision ECB/2015/47[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 |
| **OID (Object Identifiers)** | 0.4.0.127.0.10.1.2.3.0: Certificate policies for the |

[6] Decision (EU) 2016/188 of the European Central Bank of 11 December 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/2015/47).

| | |
|---|---|
| | non-ESCB/non-SSM users' certificates (this document)<br>0.4.0.127.0.10.1.2.3.1: Certificate Policy of Advanced Authentication certificate for non-ESCB/non-SSM users<br>0.4.0.127.0.10.1.2.3.2: Certificate Policy of Advanced Encryption certificate for non-ESCB/non-SSM users<br>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<br>0.4.0.127.0.10.1.2.3.5: Certificate Policy of Advanced Signature certificate for non-ESCB/non-SSM users<br>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<br>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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject | | |
| C | [Registration Organisation Country] | |
| O | EUROPEAN SYSTEM OF CENTRAL BANKS | |
| OU | Organisation within which user is member | |
| PS | User identifier (UID) | |
| CN | [AUT:A] Name Middle name Surnames | |
| Subject Public Key Info | | |
| Algorithm | RSA Encryption | |
| Minimum Length | 2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier | | |
| KeyIdentifier | *SHA-1 hash over CA Issuer public key* | |
| AuthorityCertIssuer | *Not used* | |
| AuthorityCertSerialNumber | *Not used* | |
| KeyUsage | | Yes |
| Digital Signature[8] | 1 | |
| Non Repudiation | 0 | |
| Key Encipherment | 0 | |
| Data Encipherment | 0 | |
| Key Agreement | 1 | |
| Key Certificate Signature | 0 | |
| CRL Signature | 0 | |
| 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<br>rfc822<br>RegisteredID (*[OID ESCBPKI]*.1.1)<br>RegisteredID (*[OID ESCBPKI]*.1.2)<br>RegisteredID (*[OID ESCBPKI]*.1.3)<br>RegisteredID (*[OID ESCBPKI]*.1.10)<br>RegisteredID (*[OID ESCBPKI]*.1.4)<br>RegisteredID (*[OID ESCBPKI]*.1.7) | <br>*Subject's Email*<br>*Subject's Name*<br>*Subject's Middle Name (if any)*<br>*Subject's Surname*<br>*Subject's First surname*<br>*Subject's Secondary surname (if any)*<br>*ESCB user identifier (UID)* | |
| Basic Constraints<br>CA<br>Path Length Constraint | <br>FALSE<br>*Not used* | Yes |
| CRL Distribution Points | | |
| Private Extensions | | |
| Authority Information Access<br>caIssuers<br>caIssuers<br>Ocsp | <br>*[HTTP URI Root CA]*<br>*[HTTP URI Sub CA]*<br>*[HTTP URI OCSP ALIAS]*<br>*[HTTP URI OCSP]*<br>*[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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject<br>C<br>O<br>OU<br>PS<br>CN | <br>*[Registration Organisation Country]*<br>EUROPEAN SYSTEM OF CENTRAL BANKS<br>*Organisation within which user is member*<br>*User identifier (UID)*<br>[SIG:Q] *Name Middle name Surnames*<br>*OR*<br>[SIG:A] *Name Middle name Surnames* [9] | |
| Subject Public Key Info<br>Algorithm<br>Minimum Length | <br>RSA Encryption<br>2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier<br>KeyIdentifier<br>AuthorityCertIssuer<br>AuthorityCertSerialNumber | <br>*SHA-1 hash over CA Issuer public key*<br>*Not used*<br>*Not used* | |
| KeyUsage<br>Digital Signature<br>Non Repudiation<br>Key Encipherment<br>Data Encipherment<br>Key Agreement<br>Key Certificate Signature<br>CRL Signature | <br>0<br>1<br>0<br>0<br>0<br>0<br>0 | Yes |
| extKeyUsage | <br>emailProtection (1.3.6.1.5.5.7.3.4)<br>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 | *[OID ESCBPKI]*.2.3.4<br>OR<br>*[OID ESCBPKI]*.2.3.5[10] | |
| URL CPS | *[CPS-URL]* | |
| Subject Alternative Names | | |
| 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]*<br>*[HTTP URI OCSP]*<br>*[IAM URI OCSP]* | |
| qcStatements | | |
| | id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)<br>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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject<br>C<br>O<br>OU<br>PS<br>CN | <br>*[Registration Organisation Country]*<br>EUROPEAN SYSTEM OF CENTRAL BANKS<br>*Organisation within which user is member*<br>*User identifier (UID)*<br>[ENC:A] *Name Middle name Surnames* | |
| Subject Public Key Info<br>Algorithm<br>Minimum Length | <br>RSA Encryption<br>2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier<br>KeyIdentifier<br>AuthorityCertIssuer<br>AuthorityCertSerialNumber | <br>*SHA-1 hash over CA Issuer public key*<br>*Not used*<br>*Not used* | |
| KeyUsage<br>Digital Signature<br>Non Repudiation<br>Key Encipherment<br>Data Encipherment<br>Key Agreement<br>Key Certificate Signature<br>CRL Signature | <br>0<br>0<br>1<br>1<br>0<br>0<br>0 | Yes |
| extKeyUsage | <br>emailProtection (1.3.6.1.5.5.7.3.4)<br>anyExtendedKeyUsage (2.5.29.37.0) | |
| Certificate Policies<br>Policy Identifier<br>URL CPS | <br>*[OID ESCBPKI]*.2.3.2<br>*[CPS-URL]* | |
| Subject Alternative Names<br>rfc822 | <br>*Subject's Email* | |

| | | |
|---|---|---|
| RegisteredID<br>(*[OID ESCBPKI]*.1.1) | *Subject's Name* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.2) | *Subject's Middle Name (if any)* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.3) | *Subject's Surname* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.10) | *Subject's First surname* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.4) | *Subject's Secondary surname (if any)* | |
| RegisteredID<br>(*[OID ESCBPKI]*.1.7) | *ESCB user identifier (UID)* | |
| Basic Constraints<br>CA<br>Path Length Constraint | <br>FALSE<br>*Not used* | Yes |
| CRL Distribution Points | | |
| Private Extensions | | |
| Authority Information Access<br>caIssuers<br>caIssuers<br>ocsp | <br>*[HTTP URI Root CA]*<br>*[HTTP URI Sub CA]*<br>*[HTTP URI OCSP ALIAS]*<br>*[HTTP URI OCSP]*<br>*[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)<br>or<br>SHA256-WithRSAEncryption | |
| Issuer Distinguished Name | CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU | |
| Validity | *3 years* | |
| Subject<br>C<br>O<br>OU<br>PS<br>CN | <br>*[Registration Organisation Country]*<br>EUROPEAN SYSTEM OF CENTRAL BANKS<br>*Organisation within which user is member*<br>*User identifier (UID)*<br>[AUT:S] *Name Middle name Surnames* | |
| Subject Public Key Info<br>Algorithm<br>Minimum Length | <br>RSA Encryption<br>2048 bits | |
| Standard Extensions | | |
| Subject Key Identifier | *SHA-1 hash over subject public key* | |
| Authority Key Identifier<br>KeyIdentifier<br>AuthorityCertIssuer<br>AuthorityCertSerialNumber | <br>*SHA-1 hash over CA Issuer public key*<br>*Not used*<br>*Not used* | |
| KeyUsage<br>Digital Signature[12]<br>Non Repudiation<br>Key Encipherment[13]<br>Data Encipherment[10]<br>Key Agreement<br>Key Certificate Signature<br>CRL Signature | <br>1<br>0<br>1<br>1<br>1<br>0<br>0 | Yes |
| extKeyUsage | <br>clientAuth (1.3.6.1.5.5.7.3.2)<br>emailProtection (1.3.6.1.5.5.7.3.4)<br>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<br>URL CPS | *[OID ESCBPKI]*.2.3.6<br>*[CPS-URL]* | |
| Subject Alternative Names<br>rfc822<br>RegisteredID (*[OID ESCBPKI]*.1.1)<br>RegisteredID (*[OID ESCBPKI]*.1.2)<br>RegisteredID (*[OID ESCBPKI]*.1.3)<br>RegisteredID (*[OID ESCBPKI]*.1.10)<br>RegisteredID (*[OID ESCBPKI]*.1.4)<br>RegisteredID (*[OID ESCBPKI]*.1.7) | <br>*Subject's Email*<br>*Subject's Name*<br>*Subject's Middle Name (if any)*<br>*Subject's Surname*<br>*Subject's First surname*<br>*Subject's Secondary surname (if any)*<br>*ESCB user identifier (UID)* | |
| Basic Constraints<br>CA<br>Path Length Constraint | <br>FALSE<br>*Not used* | Yes |
| CRL Distribution Points | | |
| Private Extensions | | |
| Authority Information Access<br>caIssuers<br>caIssuers<br>ocsp | <br>*[HTTP URI Root CA]*<br>*[HTTP URI Sub CA]*<br>*[HTTP URI OCSP ALIAS]*<br>*[HTTP URI OCSP]*<br>*[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.

Annex 3.3: Trusted agent terms and conditions

**Financial Markets Department**
Payments & Securities
Current account – Casper helpdesk
boulevard de Berlaimont 14
BE-1000 Brussels

Phone : + 32 (0)2 221 20 48
Email : casper.helpdesk@nbb.be

# Trusted agent for the NBB Registration Authority: Terms and conditions

## 1. Scope

In accordance with Article 7.3. of the Terms and Conditions governing Current accounts opened in Casper (hereinafter the “Casper Terms and Conditions’), an Account holder can manually send Payment orders and receive information from the NBB through the Casper Graphical User Interface (GUI). The connection to the Casper GUI is optional.

The conditions of use of the Casper GUI, including the related certificates and tokens, are described in Annex 3 of the Casper Terms and conditions. Article 4.2.2 of the said Annex 3 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 an Account holder’s member entrusted, in the framework of the Account holder’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 3 provides that each Account holder needs to appoint at least one (preferably two or more) Trusted agent among the Account holder’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 3.3 defines the terms and conditions of the power of attorney delivered by the NBB to the Trusted agent appointed by the Account holder 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 3 of the Casper Terms and conditions, in Article 2 of Annex 3 and in the sub-Annexes 3.1 and 3.2 of the Casper Terms and conditions.

## 3. Terms and conditions

### 3.1 Principle

In the framework of the operation of the Casper 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 3 of the Casper Terms and conditions, the CPS and the CP, the Trusted agent shall similarly comply with the terms of Annex 3, 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 Account holder and of the Trusted agent

The Account holder 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 Account holder 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 Account holder shall verify that the Trusted agent has signed the present sub-Annex 3.3 of the Casper 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 Account 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 Account holder's name as soon as the Trusted agent has delivered to the NBB a signed receipt of the concerned Tokens.

## 3.3 Liability

The Account holder shall be liable toward other Account holders 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 Account holder 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 Account holder 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 Account holder 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 Account holder'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 Account holder 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 Account holder 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: |
| **Account holder's data** |
| Organisation's name: |
| BIC11: |
| Address: |

| |
|---|
| **Representative(s) entitled to validly commit the Account holder** |
| 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 Account holder and the Trusted Agent irrevocably agree to the Casper Terms and Conditions, the terms of Annex 3 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 Account holder.

Name and signature of the NBB's representative

Name and signature of the Account holder's representative

Name and signature of the Account holder'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).*