Van Dycke Patrick

From:	Van Den Broek Wim on behalf of Sss
Sent:	maandag 6 augustus 2018 14:55
To:	Sss
Subject:	NBB-SSS: e-signed e-mails deadline approaching
Attachments:	Trusted Certificate Authority Application Form.pdf
Signed By:	sss@nbb.be

Dear Participants,

As you were informed in our below e-mail *dd.* 25 April 2018, Participants shall e-sign their e-mails to the NBB-SSS from 1 January 2019 onwards using a certification authority trusted by the NBB, in line with the NBB-SSS Terms & conditions.

You have four options to use e-signed e-mails:

1) The NBB recommends to use certificates from certification authorities which have already been accepted by the NBB:
   Option 1a:
   You can sign with your RAMSES-token which holds the certificates of ESCB-PKI (Eurosystem) with Banco de España as technical provider.
   Option 1b:
   You can use another EU trusted certification authority to sign your e-mails as these have already been accepted by the NBB: https://ec.europa.eu/digital-single-market/en/news/eu-trusted-lists-certification-service-providers.
   A more user-friendly list is available on this website : https://webgate.ec.europa.eu/tl-browser/#/.

2) If you wish to use a certification authority which is not on the EU trusted list, you have two rather cumbersome options:
   Option 2a:
   You request NBB to recognize your certification authority as trusted:
   We need the following information: a completed "Trusted certification authority application form" (see attached), the chain of certification (i.e. the certificate of the CA which is included in every client certificate and can be extracted from the certificate) and an e-mail with a "test" certificate with the password delivered in a separate e-mail, upon which the NBB can verify and install the certificate as trusted. You will then receive validation of your certificate.
   Option 2b:
   You request your certification authority to take the necessary steps to get registered as trusted by the European Commission:
   Aspiring certification authorities should apply to get trusted by their own country. To find out which authorized authority to contact, visit https://webgate.ec.europa.eu/tl-browser/#/, select the applicable country, go to detailed information and trusted list information. For example, for Belgium, for more information https://tsl.belgium.be/ with FOD/SPF Economie as authorized authority. Once the authorized authority classifies a certification authority as trusted, it can contact the European Commission to notify them of its decision, at which point the European Commission can add the certification authority to the EU trusted list, which completes this heavy process.

3) In addition, some Participants are using "own certificates", i.e. Bank X signs e-mail with certificate by Bank X itself. When the own certification authority (Bank X) is not on the EU trusted list, we consider the e-signature as non-compliant and you will still need to apply one of the four options 1a, 1b, 2a, 2b described above, e.g. by having your own certification authority added to the EU list in option 2b.

4) Finally, a “disclaimer” that states that your e-signed e-mail does not commit your institution should be omitted.

Should you need additional information, please first contact your IT-support. If questions still remain, feel free to contact us.

Kind regards,

NBB SSS Customer Relations
+32 (0)2 221 36 00
sss@nbb.be

From: Van Der Wolf Renan [mailto:Renan.VanDerWolf@nbb.be] On Behalf Of Sss
Sent: Wednesday, April 25, 2018 11:38 AM
To: Sss <sss@nbb.be>
Subject: Use of signed e-mails to communicate with the NBB-SSS

Dear Participants,

IT security is becoming lastly increasingly important and in this context, we have taken several measures to improve it on our side and offer you reliable and robust services. Using signed e-mails is one of them : using it ensures that the message originates from the e-mail address used as sender and that its content has not been modified.

However, it also depends on you to have a secure communication channel : if both parties do not use secure e-mails, it is pointless. Therefore, we ask you to also start using only signed e-mails. It was already required in the chapter 10 “Communications” of our Terms & Conditions (details in the annex 16 “Guidelines for the use of secure e-mail”) and until now we have not been strict, but considering the current context and the potential consequences we can no longer afford this luxury.

As agreed during the last NBB-SSS User Committee (https://www.nbb.be/doc/ti/minutes_12th_user_committee_20180308.pdf), we request you to use only signed e-mails starting from the 31/12/2018 and will grant a grace period until the 30/06/2019.
The certificates used to sign the e-mails must be issued by a Certification Authority on the EU trusted lists. These ones are available on these websites :

- https://ec.europa.eu/digital-single-market/en/news/eu-trusted-lists-certification-service-providers
- http://tlbrowser.tsl.website/tools/

After the 31/12/2018, e-mails that are not signed with the right certificate will still exceptionally be processed. After the end of the grace period, so the 30/06/2019, e-mails not signed with the right certificate will not be processed at all anymore as they could be tampered with.

Have a nice day and best regards,

The NBB-SSS team

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

TRUSTED CERTIFICATION AUTHORITY APPLICATION FORM

NBB-SSS Participant BIC11: _____

Certificate Authority: _____

Certificate Authority Contact: Name + Title _____

E-mail address _____

Phone Number _____

Root CA Common Name: _____

CA Owner Country Code: _____

Motivation to accept the new CA in the trusted list:

_____

_____

_____

Technical information about the CA:

CAF classes you apply for:

Signature: ☐ Standard ☐ Advanced

*The NBB-SSS requires standard signature certificate at a minimum

Certificate expiry: _____

Certificate cert hash value: _____

CRL distribution point: _____

OCSP points in "Authority Information Acces": _____

The NBB-SSS participant commits to:

- providing the NBB with any information required for the evaluation procedure in due time
- informing the NBB of any change related to the CA, in particular change to the Certificate Policy or Certification Practise Statement.
- offering free certificate validation service or free access to a public list of revoked certificates

☐ The NBB-SSS participant shall provide the chain of CA certification and a test end user certificate.

☐ The NBB-SSS participant acknowledges and agrees that the NBB shall not be liable for damages that may be caused by the CA or RA failing to meet the obligations and procedures described in the Certificate Policy and Certification Practice Statement.

Name, signature, date and place