DECISIONS

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)

THE GOVERNING COUNCIL OF THE EUROPEAN CENTRAL BANK,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 127 thereof,

Having regard to the Statute of the European System of Central Banks and of the European Central Bank, and in particular Article 12.1 in conjunction with Article 3.1, Article 5, Article 12.3 and Articles 16 to 24 and 34 thereof,

Whereas:

(1) Regulation (EU) No 910/2014 of the European Parliament and of the Council ([1]) has repealed Directive 1999/93/EC of the European Parliament and of the Council ([2]) with effect from 1 July 2016. Therefore, it is appropriate to refer to Regulation (EU) No 910/2014 in Decision ECB/2013/1 ([3]).

(2) Information concerning the ESCB-PKI certification authority, including its identity and its technical components, as set out in the Annex to Decision ECB/2013/1, needs to be updated.

(3) Therefore, Decision ECB/2013/1 should be amended accordingly,

HAS ADOPTED THIS DECISION:

Article 1

Amendments

Decision ECB/2013/1 is amended as follows:

(1) in Article 1, point 10 is replaced by the following:

'10. "ESCB-PKI certification authority" means the entity, trusted by users, to issue, manage, revoke and renew ESCB-PKI certificates in accordance with the ESCB/SSM certificate acceptance framework;';

(2) in Article 4, paragraph 4 is replaced by the following:

'4. The ESCB-PKI certification practice statement is a set of rules governing the life cycle of electronic certificates, from the initial request to the subscription end or revocation, as well as the relationships between the certificate applicant or subscriber, the ESCB-PKI certification authority and the relying parties. It covers certificates falling under the scope of Directive 1999/93/EC and Regulation (EU) No 910/2014 of the European Parliament and of the

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

Council (*) and certificates falling outside their scope. It also sets out the roles and responsibilities of all parties and establishes the procedures concerning issuing and managing certificates. It is annexed to the Level 2 — Level 3 Agreement.

(*) 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).';

(3) in Article 10, the introductory statement and point (a) of paragraph 1 are replaced by the following:

'1. Unless they prove that they have not acted negligently, the Eurosystem central banks shall be liable in accordance with their functions and responsibilities in the ESCB-PKI for any damage caused to a user who reasonably relies on a qualified certificate, as defined in Directive 1999/93/EC and Regulation (EU) No 910/2014, as regards:

(a) the accuracy at the time of issuance of all the information contained in a qualified certificate, and the question of whether the certificate contains all the details prescribed for a qualified certificate as defined in Directive 1999/93/EC and Regulation (EU) No 910/2014;';

(4) the Annex is replaced by the Annex to this Decision.

Article 2

Entry into force

This Decision shall enter into force on the third day following that of its publication in the *Official Journal of the European Union*.

Done at Frankfurt am Main, 11 December 2015.

The President of the ECB

Mario DRAGHI

ANNEX

'ANNEX

Information concerning the ESCB-PKI certification authority, including its identity, and its technical components

The ESCB-PKI certification authority is identified in its certificate as the issuer and its private key is used to sign certificates. The ESCB-PKI certification authority is in charge of:

(i) issuing private and public key certificates;

(ii) issuing revocation lists;

(iii) generating key pairs associated with specific certificates, e.g. those that require key recovery;

(iv) maintaining overall responsibility for the ESCB-PKI and ensuring that all the requirements necessary to operate it are met.

The ESCB-PKI certification authority includes all individuals, policies, procedures and computer systems entrusted with issuing electronic certificates and assigning them to the certificate subscribers.

The ESCB-PKI certification authority includes two technical components:

— **The Root ESCB-PKI certification authority**: This certification authority, at the first level, only issues certificates for itself and its subordinate certification authorities. It is only in operation when carrying out its own narrowly-defined responsibilities. Its most significant data are:

a) 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

b) 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

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

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**: This certification authority, at the second level, is subordinate to the Root ESCB-PKI certification authority. It is responsible for issuing ESCB-PKI certificates for users. Its most significant data are:

a) SHA-1 certificate ([1]):

Distinguished name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number	2C13 E18F FDB5 91CE 4E9 550B B5A3 F59C
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)	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

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