2024/2683

15.10.2024

DECISION (EU) 2024/2683 OF THE EUROPEAN CENTRAL BANK

of 8 October 2024

amending Decision ECB/2013/1 laying down the framework for a public key infrastructure for the European System of Central Banks (*ECB/2024/26*)

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 and Article 132(1) 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 Articles 3.1 and 12.3, and Article 34 thereof,

Whereas:

(1) Decision ECB/2013/1 of the European Central Bank ([1]) established the framework for the Eurosystem public key infrastructure (hereinafter the 'ESCB-PKI') to regulate the issuance and management of electronic certificates that are required to access and use ESCB and Eurosystem electronic applications, systems, platforms and services with medium or above medium criticality.

(2) The technology used by the ESCB-PKI has reached the end of its life and has been replaced. It is therefore necessary to introduce a new online ESCB-PKI certification authority (hereinafter the 'online ESCB-PKI certification authority V1.2'), which should also take into account that the three-year validity of the certificates issued for ESCB and non-ESCB users and technical components under an online ESCB-PKI certification authority cannot expire later than the expiration of the certificate of that online ESCB-PKI certification authority itself. The certificate of the existing online ESCB-PKI certification authority expires on 22 July 2026, and thereafter the online ESCB-PKI certification authority V1.2 would be the sole online ESCB-PKI certification authority, until the expiry of its certificate.

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

HAS ADOPTED THIS DECISION:

Article 1

Amendment

The Annex to Decision ECB/2013/1 is replaced by the Annex to this Decision.

Article 2

Entry into force

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

Done at Frankfurt am Main, 8 October 2024.

The President of the ECB
Christine LAGARDE

([1]) 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).

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 three technical components:

1. **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:

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

2. **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. It expires on 22 July 2026. Its most significant data are:

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

3. **The Online ESCB-PKI certification authority V1.2**: 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. After 22 July 2026 it is the sole online ESCB-PKI certification authority, until its expiry. Its most significant data are:

Distinguished name	CN = ESCB-PKI ONLINE CA V1.2, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number	1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653
Distinguished name of issuer	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period	From 08-06-2023 17:07:00 to 08-06-2038 17:07:00
Message digest (SHA-1)	DC92 042E 6316 CB60 F8F6 109B 8C43 F3C6 AF2F B2F3
Message Digest (SHA-256)	96B7 8E9C F914 ED4D 072D 93C8 C531 DEEF D102 7571 7218 A202 0924 3216 99D8 1C48
Cryptographic algorithms	SHA-256/RSA 4096’