# DECISIONS

## DECISION 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**

***(ECB/2013/1)***

(2013/132/EU)

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 (hereinafter the 'Statute of the ESCB'), and in particular Article 12.1 in conjunction with Article 3.1, Article 5, Article 12.3 and Articles 16 to 24 thereof,

Whereas:

(1) Pursuant to Article 12.1 of the Statute of the ESCB, the Governing Council adopts the guidelines and takes the decisions necessary to ensure the performance of the tasks entrusted to the European System of Central Banks (ESCB) and to the Eurosystem under the Treaty and the Statute of the ESCB. This includes the power to decide on the organisation of ancillary activities that are necessary for the performance of such tasks, such as the issuance and management of electronic certificates for securing information stored and processed in ESCB and Eurosystem electronic applications, systems, platforms and services, and for data communication to and from them.

(2) Pursuant to Article 12.3 of the Statute of the ESCB, the Governing Council also has the power to determine the internal organisation of the European Central Bank (ECB) and its decision-making bodies. Accordingly, the Governing Council has the power to decide that the ECB will use electronic certificates issued by the Eurosystem's own public key infrastructure.

(3) The number of users accessing a growing number of constantly evolving ESCB and Eurosystem electronic applications, systems, platforms and services is increasing. The Governing Council has identified a need for advanced information security services, such as strong authentication, electronic signatures and encryption, through the use of electronic certificates.

(4) Few ESCB central banks have their own public key infrastructure and many users from third parties that work jointly with ESCB central banks do not have easy access to a certification authority accepted by the ESCB in accordance with its certificate acceptance framework.

(5) There is a need for the Eurosystem to create its own public key infrastructure which can issue all types of electronic certificates such as personal and technical certificates for ESCB and non-ESCB users, and which is flexible enough to adapt to developments in ESCB and Eurosystem electronic applications, systems, platforms and services. This public key infrastructure (hereinafter the 'ESCB-PKI') should complement the services provided by other certification authorities accepted by the ESCB in accordance with the ESCB certificate acceptance framework or by certification authorities accepted by the ESCB for TARGET2 and TARGET2 Securities for those two applications.

(6) On 29 September 2010 the Governing Council decided to launch the ESCB-PKI project to build and implement the ESCB-PKI and to provide the resources required for its completion. It decided that the ESCB-PKI will be developed, hosted and operated by the Banco de España.

(7) The ESCB-PKI indirectly supports the performance of ESCB and Eurosystem tasks. It is based on three levels of governance: Level 1 consists of the Governing Council and the Executive Board, Level 2 of the Eurosystem central banks and Level 3 of the providing central bank.

(8) At Level 1, the Governing Council is responsible for the direction, management and control of the activities and deliverables needed to develop and operate the ESCB-PKI. It is also responsible for decision-making in relation to the ESCB-PKI and decides on the allocation of tasks not specifically attributed to Levels 2 and 3.

(9) The Eurosystem central banks are responsible for the tasks assigned to Level 2, within the general framework defined by the Governing Council. They have competences regarding the technical means of implementing the ESCB-PKI.

(10) The ESCB Information Technology Committee (ITC) has a steering role in the development of the ESCB-PKI. It guides, assesses, controls and approves the project deliverables against the acceptance criteria in accordance with the ESCB certificate acceptance framework, the scope and the schedule approved by the Governing Council.

(11) At Level 3, the Banco de España has been appointed as the providing central bank to carry out the tasks assigned to it within the general framework defined by the Governing Council. The providing central bank has put in place the technical infrastructure and secure devices and services required to create and use a public key infrastructure in accordance with: (a) the national law transposing Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures ([1]), as applicable to it; (b) the national law transposing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ([2]), as applicable to it; and (c) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ([3]).

(12) Since electronic certificates are essential elements used in electronic applications both as an authentication mechanism to implement electronic signatures, and for public key-based encryption, the ESCB-PKI will take into account existing ESCB and Eurosystem electronic applications, systems, platforms and services and current ESCB projects in order to ensure that their needs are covered.

(13) Non-euro area national central banks (NCBs) may decide to use the certificates and services provided by the ESCB-PKI,

HAS ADOPTED THIS DECISION:

*Article 1*

**Definitions**

For the purposes of this Decision:

1. 'certificate' or 'electronic certificate' means an electronic file, issued by a certification authority, which binds a public key with a certificate subscriber's identity and is used for all or some of the following: (a) to verify that a public key belongs to a certificate subscriber; (b) to authenticate a certificate subscriber; (c) to check a certificate's subscriber signature; (d) to encrypt a message addressed to a certificate subscriber; (e) to verify a certificate subscriber's access rights to ESCB and Eurosystem electronic applications, systems, platforms and services. Any reference in this Decision to a certificate or electronic certificate includes a reference to the data carrier devices on which the certificate or electronic certificate is held;

2. 'ESCB and Eurosystem electronic applications, systems, platforms and services' means the electronic applications, systems, platforms and services that the ESCB and/or the Eurosystem use when carrying out the tasks entrusted to them under the Treaty and the Statute of the ESCB;

3. 'public key infrastructure' means 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;

4. 'user' means either a certificate subscriber or a relying party, or both;

5. 'authentication' means the process of verifying the identity of a certificate applicant or certificate subscriber;

6. 'ESCB central bank' means either a Eurosystem central bank or a non-euro area NCB;

7. 'Eurosystem central bank' means either an NCB of a Member State whose currency is the euro, including the providing central bank, or the ECB;

8. 'providing central bank' means the NCB appointed by the Governing Council to develop the ESCB-PKI and to provide ESCB-PKI services on behalf of and for the benefit of the Eurosystem central banks;

9. 'non-euro area NCB' means an NCB of a Member State whose currency is not the euro;

10. 'ESCB-PKI certification authority' means the entity, trusted by users, to issue, manage, revoke and renew certificates on behalf of the ESCB central banks or the Eurosystem central banks in accordance with the ESCB certificate acceptance framework;

11. 'ESCB-PKI validation authority' means the entity, trusted by users, which provides information on the validity of certificates issued by the ESCB-PKI certification authority;

12. 'certificate subscriber' means either an individual who is the subject of an electronic certificate and has been issued an electronic certificate, or a technical component manager who has accepted an electronic certificate issued by the ESCB-PKI certification authority for a technical component, or both;

13. 'ESCB certificate acceptance framework' means the criteria established by the ESCB ITC to identify the certification

([1]) OJ L 13, 19.1.2000, p. 12.
([2]) OJ L 281, 23.11.1995, p. 31.
([3]) OJ L 8, 12.1.2001, p. 1.

authorities, both internal and external to the ESCB, which can be trusted in relation to ESCB and Eurosystem electronic applications, systems, platforms and services;

14. 'registration authority' means an entity, trusted by users, which verifies the identity of a certificate applicant before the ESCB-PKI certification authority issues a certificate;

15. 'relying party' means an individual or an entity other than a certificate subscriber which accepts and relies on a certificate;

16. 'audit policy' means the ESCB audit policy defined by the Governing Council on 7 October 1998, as published on the ECB's website ([1]);

17. 'certificate applicant' means an individual who requests the issuance of a certificate for themself or for a technical component;

18. 'technical component' means any software or any hardware equipment that can be identified by using electronic certificates.

*Article 2*

**Scope**

1. This Decision establishes the framework for the ESCB-PKI. The ESCB-PKI is the Eurosystem's own 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's certificate acceptance framework.

2. As ESCB-PKI services may affect relying parties, this Decision also sets out the conditions under which such parties may rely on ESCB-PKI certificates.

*Article 3*

**Scope and objectives of the ESCB-PKI**

1. ESCB and Eurosystem electronic applications, systems, platforms and services with medium or above medium criticality shall only be accessed and used if a user has been authenticated by means of an electronic certificate issued and managed by a certification authority accepted by the ESCB in accordance with the ESCB certificate acceptance framework, including by the ESCB-PKI certification authority, or by certification authorities accepted by the ESCB for TARGET2 and TARGET2 Securities for those two applications.

2. The ESCB-PKI certification authority shall issue electronic certificates and provide other electronic certification services for certificate subscribers of the ESCB central banks and of third parties working with them to enable them to securely access and use ESCB and Eurosystem electronic applications, systems, platforms and services.

3. The ESCB-PKI shall provide the following certification services:

(a) certificate issuance, renewal and revocation, and confirmation of a certificate's validity with regard to different certificate types;

(b) issuance of certificates for authentication, electronic signature and encryption in relation to ESCB and non-ESCB users, and technical certificates;

(c) private key recovery to ensure the recovery of public key-based encrypted information in the case of certificate loss;

(d) delivery and management of cryptographic tokens to certificate subscribers when needed;

(e) provision of information on ESCB-PKI certificate management procedures, and technical support to ESCB project managers to help them to integrate ESCB-PKI certificates into their applications.

Other services may be added in the future as required by ESCB and Eurosystem electronic applications, systems, platforms and services.

*Article 4*

**ESCB-PKI framework**

1. Subject to this Decision, the responsibilities and functions of the providing central bank and of the other Eurosystem central banks with regard to ESCB-PKI implementation, operation and use shall be set out in a Level 2 – Level 3 Agreement and further specified in ESCB-PKI certificate policies and the ESCB-PKI certification practice statement.

2. The Level 2 – Level 3 Agreement, which includes the Service Level Agreement, contains the agreement negotiated between the providing central bank and the Eurosystem central banks in relation to the responsibilities and functions of the providing central bank and the Eurosystem central banks. It shall be submitted for endorsement by the Governing Council and then signed by the providing central bank and the Eurosystem central banks.

3. The Service Level Agreement is both an agreement defining the level of services to be provided by the providing central bank to the Eurosystem, and an agreement defining the level of services to be provided by the Eurosystem to the non-euro area NCBs and third parties in relation to the ESCB-PKI.

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 electronic certificates falling under the scope of Directive 1999/93/EC, and electronic certificates falling outside its 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.

([1]) www.ecb.europa.eu

5. An ESCB-PKI certificate policy is a set of rules which is applicable to each type of certificate issued. Each set provides implementation details relating to the ESCB-PKI certification practice statement for each type of certificate issued. ESCB-PKI certificate policies are annexed to the Level 2 – Level 3 Agreement.

6. The ESCB-PKI certificate policies and the ESCB-PKI certification practice statement shall be published on the ESCB-PKI website ([1]).

7. Information concerning the ESCB-PKI certification authority, including its identity, and its technical components is set out in the Annex to this Decision.

*Article 5*

**Responsibilities and roles of the providing central bank**

1. The providing central bank shall be responsible for operating and maintaining the ESCB-PKI for the benefit of the Eurosystem central banks, including hosting, operation and management carried out in accordance with the Level 2 – Level 3 Agreement. In particular, it shall deliver certificates and ESCB-PKI services in accordance with business requirements and technical specifications, such as the ESCB certificate acceptance framework and the requirements and specifications set out in the Level 2 – Level 3 Agreement.

2. The providing central bank shall put the necessary organisational infrastructure in place for creating, issuing and managing certificates and shall ensure that the infrastructure is maintained. For that purpose, in consultation with the ITC, the providing central bank may adopt rules concerning its internal organisation and administration.

3. The providing central bank shall act as the ESCB-PKI certification authority and the ESCB-PKI validation authority.

4. The Level 2 – Level 3 Agreement shall establish the liability regime applying to the providing central bank.

*Article 6*

**Responsibilities and roles of the Eurosystem central banks**

1. Each Eurosystem central bank shall be responsible for identifying its certificate subscribers. It shall create the role of registration officer to perform this task who shall have the authority to register third party users.

2. Each Eurosystem central bank shall act as a relying party in relation to certificates for encryption and electronic signature issued by the ESCB-PKI for other Eurosystem central banks or third party users' certificate subscribers.

3. Each Eurosystem central bank using ESCB-PKI services shall act as a registration authority for its certificate applicants and ensure that its certificate applicants accept and apply the user terms and conditions set out in the ESCB-PKI certification authority's application form for its services.

([1]) http://pki.escb.eu

*Article 7*

**Relationships between the Eurosystem central banks, third parties and certificate subscribers**

Each Eurosystem central bank shall make arrangements with regard to third party secure access and use of the ESCB and Eurosystem electronic applications, systems, platforms and services through the use of ESCB-PKI certificates. These arrangements shall exclusively govern the relationship between the relevant Eurosystem central bank and the third parties that use ESCB-PKI certificates. All third parties shall comply with the ESCB-PKI certificate policies, the ESCB-PKI certification practice statement and the user terms and conditions set out in the ESCB-PKI certification authority's application form for its services.

*Article 8*

**Relationships with relying parties**

An electronic certificate issued under this Decision may be relied upon provided that a relying party:

(a) verifies the validity, suspension or revocation of the certificate using current revocation status information;

(b) takes account of any limitations on use specified in the certificate; and

(c) accepts the ESCB-PKI certification practice statement and the applicable ESCB-PKI certificate policies.

*Article 9*

**Rights to the ESCB-PKI**

1. The ESCB-PKI shall be fully owned by the Eurosystem central banks.

2. In view thereof, the providing central bank shall grant to the Eurosystem central banks, to the extent feasible under applicable legislation, all licenses regarding the intellectual property rights required to enable the Eurosystem central banks to use the ESCB-PKI and its components and the full range of ESCB-PKI services and also provide ESCB-PKI services to third parties under the ESCB-PKI certification practice statement and the ESCB-PKI certificate policies. The providing central bank shall indemnify the Eurosystem central banks against any infringement claims raised by third parties in relation to such intellectual property rights.

3. The details regarding the Eurosystem central banks' rights to the ESCB-PKI shall be agreed between Level 2 and Level 3 in the Level 2 – Level 3 Agreement.

*Article 10*

**Liability of Eurosystem central banks towards users**

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, 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;

(b) any assurance that at the time of issuance of a qualified certificate, the certificate subscriber identified therein held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

(c) any assurance that the signature-creation device and the signature-verification device function together in a complementary manner, in cases where the ESCB-PKI generates both;

(d) any failure to register revocation of a qualified certificate.

2. The Eurosystem central banks assume no commitments, give no guarantees and accept no liability towards users unless expressly stated in this Decision and in the ESCB-PKI certification practice statement.

*Article 11*

**Participation of non-euro area NCBs in the ESCB-PKI**

1. A non-euro area NCB may act as a registration authority for its internal users as well as for third party users, and may create the role of a registration officer to perform this task.

2. Subject to the approval of the Governing Council, a non-euro area NCB may also decide to use ESCB-PKI services under the same conditions as those applying to Eurosystem central banks. For that purpose, the non-euro area NCB shall submit a declaration to the Governing Council in which it confirms that it will comply with the obligations laid down in this Decision and in the Level 2 – Level 3 Agreement. A non-euro area NCB shall not become co-owner of the ESCB-PKI and shall not be obliged to contribute to the ESCB-PKI financial envelope.

*Article 12*

**Data protection**

Eurosystem central banks shall comply with the data protection legislation applicable to their processing of personal data in the performance of their functions related to the ESCB-PKI.

*Article 13*

**Audit**

Audits of the ESCB-PKI shall be performed in accordance with the principles and arrangements set out in the audit policy. They shall be without prejudice to the internal controls and audit rules that apply to or are adopted by the Eurosystem central banks.

*Article 14*

**Financial arrangements**

The Eurosystem central banks shall bear the costs of developing and operating the ESCB-PKI as further specified in the ESCB-PKI financial envelope.

*Article 15*

**Role of the Executive Board**

1. In accordance with Article 17.3 of Decision ECB/2004/2 of 19 February 2004 adopting the Rules of Procedure of the European Central Bank [1], the Governing Council delegates its normative powers to the Executive Board to take any measures to implement this Decision that are necessary for the efficiency and security of the ESCB-PKI, and to adopt amendments **relating** to the technical aspects of the ESCB-PKI and ESCB-PKI services provided for in the annexes to the Level 2 – Level 3 Agreement after taking into consideration the advice of the ITC and, if applicable, of the Eurosystem IT Steering Committee.

2. The Executive Board shall notify the Governing Council of any measure that it takes pursuant to paragraph 1 without undue delay and shall abide by any decision adopted by the Governing Council on the matter.

Done at Frankfurt am Main, 11 January 2013.

*The President of the ECB*

Mario DRAGHI

[1] OJ L 80, 18.3.2004, p. 33.

*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:

| | |
|---|---|
| **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 |

— **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:

| | |
|---|---|
| **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 |
| **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 |