Annex I

Annex B to the Level 2 – Level 3 Agreement is replaced by the following:

BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI SERVICES

OID: 0.4.0.127.0.10.1.2.1

CERTIFICATION PRACTICE STATEMENT

VERSION 1.8

22 August 2023

Table of Contents

Control Sheet

	Title	Certification Practice Statement
	Author	ESCB-PKI Service Provider
	Version	1.8
	Date	22.08.2023

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 Scope extension to ESCB/SSM.
1.4	Final	15.11.2018	• Key usage KeyEncipherment added to authentication certificate profile. • anyExtendedKeyUsage extended key usage removed in all certificate profiles. • Modifications to comply with Regulation Nº 910/2014: o New extensions escbIssuerName and escbIssuerVAT are included to comply with Regulation (EU) No 910/2014. • Modifications to comply with ETSI EN 319 401:

			○ Added a reference to the ESCB/SSM Information Systems Risk Management methodology ○ Added a reference to the ESCB/SSM Information Systems Security Policy ○ Added a statement to clarify that ESCB-PKI services shall be provided in accordance with the principle of non-discrimination ○ Added a statement to clarify that ESCB-PKI services shall be provided in accordance with the principle of non-discrimination ○ Added various statements to clarify relations with potential contractors ○ Updated chapters 1.3 and 5.2.1 to better clarify the ESCB-PKI role allocation procedures. ○ Updated the CA termination plan ○ Updated the Life-Cycle Security Controls ○ Other minor updates
1.5	Final	26.08.2019	• Update after PKI-AB revision
1.6	Final	09.10.2020	• A new type of participant organisation, namely *Cooperating Authorities* has been included. • References to SHA1 certificates has been removed, as these certificates are no longer valid. • CA certificates hierarchy description has been updated to include potential new CA in the future. • Acceptance of certificates by the subscribers do no longer require the signature of the Term & Conditions document, but the wilful acceptance of the related Term & Conditions. • Updated references to the 2018 Spanish Data Protection Law.
1.7	Final	10.02.2021	• Update to Law 6/2020, of November 11, Regulating Certain Aspects of Trusted Electronic Services. This new Law repeals Law 59/2003 on Electronic Signatures.
1.8	Final	22.08.2023	• Update for the release of the new Certification Authority: Online CA V1.2

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 Regulation (EU) No 910/2014 of the European Parliament and of the Council[1].
- 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:
  - The Certificate Policies for the internal users' certificates, governing the personal certificates issued by the ESCB-PKI Certification Authority for internal users (i.e. users that belong to ESCB Central Banks or SSM National Competent Authorities).
  - The Certificate Policies for the external users' certificates, governing the personal certificates issued by the ESCB-PKI Certification Authority for external users (i.e. users that belong to external organisations outside the ESCB and the SSM).
  - The Certificate Policies for technical certificates, governing the technical certificates issued by the ESCB-PKI Certification Authority (i.e. servers or applications).
- 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 https://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.
- 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.

[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 (OJ L 257, 28.8.2014, p. 73).

For more information, consult the website established for this purpose at https://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**[2].

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 EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. This standard replaces ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust Service Providers issuing EU qualified certificates. This standard replaces ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements. This standard replaces ETSI TS 101 862: Qualified Certificate Profile.

Likewise, the following relevant legal framework has been considered:

- Decision ECB/2015/47[3];
- Regulation (EU) No 910/2014 of the European Parliament and of the Council[4]; Spanish Law 6/2020 of November 11, Regulating Certain Aspects of Trusted Electronic Services (Spanish Official Journal, 11 November).[5]

[2] 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).

[3] 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).

[4] 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).

[5] Spanish legislation is also considered owed to the fact the Service Provider is established at Spain.

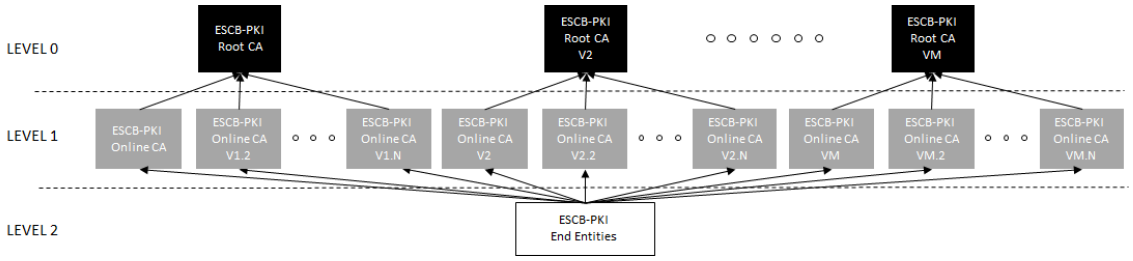
- Regulation (EU) 2016/679 of the European Parliament and of the Council[6]; Spanish Organic Law 3/2018, of 5 December 2018, for the Protection of Personal Data and guarantee of digital rights.
- National legislation transposing the General Data Protection Regulation, the Directive 99/93/EC, and Regulation (EU) No 910/2014, 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:



As is shown in the image above, the ESCB-PKI will consist on a two-level hierarchy Certification Authority infrastructure. Due to renewal needs of CA certificates, there may be more than one valid Root and/or Online CA certificates at the same time, but just one of the CA will be the active issuer of new certificates.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

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	1.8
Document status	Final
Date of issue	22.08.2023
OID (Object Identifier)	0.4.0.127.0.10.1.2.1
CPS location	https://pki.escb.eu/policies

1.3 ESCB-PKI Participants

The participating entities and persons are:

- The Eurosystem Central Banks, as the owners of the ESCB-PKI. The Information Technologies Committee (ITC), composed of at least one representative of each organisation, is the System Owner of the ESCB-PKI service. Each one of these ITC members is considered the Local System Owner (LSO) of 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.
- The Service Provider has also the responsibilities assigned in this document to the Certification Authority, Validation Authority and Key Archive.
- The Service Provider will provide ESCB-PKI services in accordance with the principle of non-discrimination.
- The ESCB Central Banks including the Service Provider, the SSM National Competent Authorities, and Cooperating 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 the Service Provider.
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-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[7] certificates. Its most significant data are:

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

[7] In this CPS the term end entity is used to represent users in general including their roles as subscribers and relying parties.

- **The Online ESCB-PKI Certification Authority V1.2**: Certification Authority subordinated to the ESCB-PKI Root CA. It is responsible for issuing the ESCB-PKI end entities[8] certificates. Its most significant data are:

SHA-256 certificate:

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

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 certificates 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 shall be performed in accordance with this CPS and the relevant CPs. The Registration Authority *Application Approver Controlle*r, who shall be nominated by each organisation LSO, shall approve these roles assignment.

The following roles shall be performed by all the Eurosystem Central Banks, as well as by the Central Banks outside the Euro area, the SSM National Competent Authorities and the Cooperating Authorities that join the ESCB-PKI:

- **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

[8] In this CPS the term end entity is used to represent users in general including their roles as subscribers and relying parties.

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 subscribers** (TCS).

- **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.

The following roles shall be performed by all the Eurosystem Central Banks, 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.

- **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.

1.3.4 Validation Authority

The Validation Authority (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 the Service Provider.
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, SSM National Competent Authorities or Cooperating Authorities (internal users) Users from external organisations (external users) Individuals in charge of the internal applications and technical components that use the certificate ESCB-PKI entities
Online CA V1.2	Users from ESCB Central Banks, SSM National Competent Authorities or Cooperating Authorities (internal users) Users from external organisations (external users) Individuals in charge of the internal applications and technical components that use the certificate 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 the Service Provider 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 internal to the ESCB/SSM
- **b** External users who 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 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 will elaborate the new versions of this CPS and the CPs. The Governing Council, with the assistance of the Eurosystem/ESCB Committees, 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.
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.
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.

Certification Service Provider (CSP): entity or a legal person who issues certificates or provides other services related to electronic signatures.

Directory: a data repository that is accessed through the LDAP protocol.

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.

ESCB Central Bank: means either a Eurosystem Central Bank or a non-euro area NCB**.**

Eurosystem Central Bank: means either an NCB of a Member State whose currency is the euro or the ECB.

External Organisation: public or private organisation that do not belong to the European System of Central Banks (ESCB) or the Single Supervisory Mechanism (SSM), and neither is a Cooperating Authority.

Identification: the process of verifying the identity of those applying for a certificate.

Internal user: user that belongs to an ESCB Central Bank, SSM National Competent Authority or Cooperating Authority.

Key agreement: a process used by two or more technical components to agree on a session key in order to protect a communication.

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 user: user that belongs to an external organisation.

Non-euro area NCB: means an NCB of a Member State whose currency is not the euro.

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.

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).

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.

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.

Relying parties: an individual or entity other than a certificate subscriber that decide to accept and rely on a certificate issued by ESCB-PKI.

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.

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.

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).

System Owner: the Information Technologies Committee (ITC), composed of at least one representative of each organisation. Each one of these ITC members is considered the **Local System Owner** (LSO) of ESCB-PKI.

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.

Trusted 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.

User identifier: a set of characters that are used to uniquely identify the user of a system.

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

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%20V**M**,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint, where the M value depends on the ESCB-PKI Root CA version.
- ESCB-PKI website (HTTP): http://pki.escb.eu/crls/rootCAvM.crl, where the M value depends on the ESCB-PKI Root CA version.

Online CA CRLs distribution point:

- ESCB-PKI Directory Service (LDAP): ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20CA%20V**MN**,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint, where the M and N values depends on the issuer CA and ESCB-PKI Online CA versions.
- ESCB-PKI website (HTTP): http://pki.escb.eu/crls/subCAvMN.crl, where the M and N values depends on the issuer CA and ESCB-PKI Online CA versions.

Online validation service that implements the OCSP protocol:

- **¡Error! Referencia de hipervínculo no válida.**

RootCA certificate distribution point:

- ESCB-PKI website (HTTP): http://pki.escb.eu/certs/rootCAvM.crt, where the M value depends on the ESCB-PKI Root CA version.

Online CA certificate distribution point:

- ESCB-PKI website (HTTP): http://pki.escb.eu/certs/subCAvMN.crt, where the M and N values depends on the issuer CA and ESCB-PKI Online CA versions.

For CPSs and CPs:

- ESCB-PKI website (HTTP): https://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 the Service Provider of the ESCB-PKI is authorised to modify, substitute or eliminate information from its repository or website. For this purpose, the Service Provider 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 wilfully accept the ESCB-PKI terms and conditions before the certificate is created.

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. Requirements for the identification and authentication of Natural Person 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 of a natural 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 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 wilfully accept the terms and conditions application.

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 the 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.

4.5 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 notification 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 trusted 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[9] 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.

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*.

[9] 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.

4.9.10 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 Security Controls

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. 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 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 eye biometrics identification (iris recognition).

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

Components that are critical for the secure operation of the trust service are located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

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.

Storage systems containing sensitive information shall be managed according to the relevant ESCB/SSM security policy.

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

The Service Provider, as a member of the European System of Central Banks, is obliged to operate according to the ESCB/SSM Information Systems Security Policy.

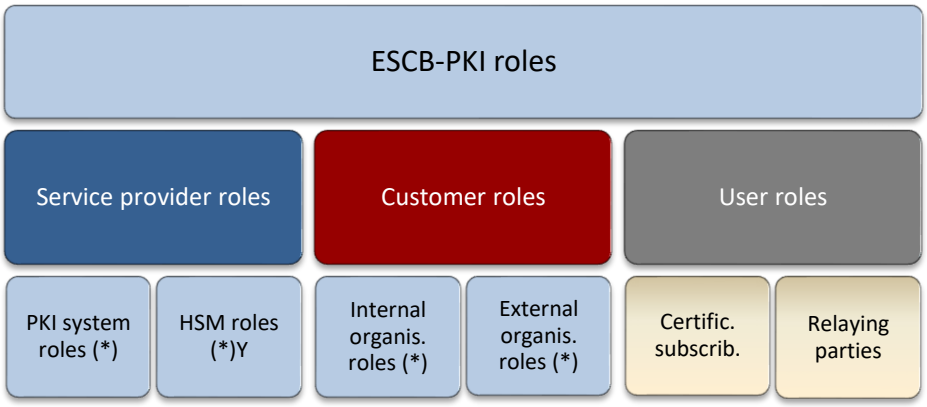
The Service Provider endeavours to ensure that all management, related to both operational and administrative procedures, is carried out in a secure manner, pursuant to the guidelines in this document, carrying out periodic audits. (See Chapter 8 *Performing audits and other conformity controls*).

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 required roles to implement the ESCB Public Key Infrastructure are:

- Service provider roles;
- Customer roles;
- User roles.



Only the Service Provider roles will be described here. Refer to chapter *1.3.3 Registration Authorities* and *1.3.6 Users* for the description of the Customer roles and User roles.

5.2.1.1 Service provider roles

The ESCB-PKI Service Provider is responsible for:

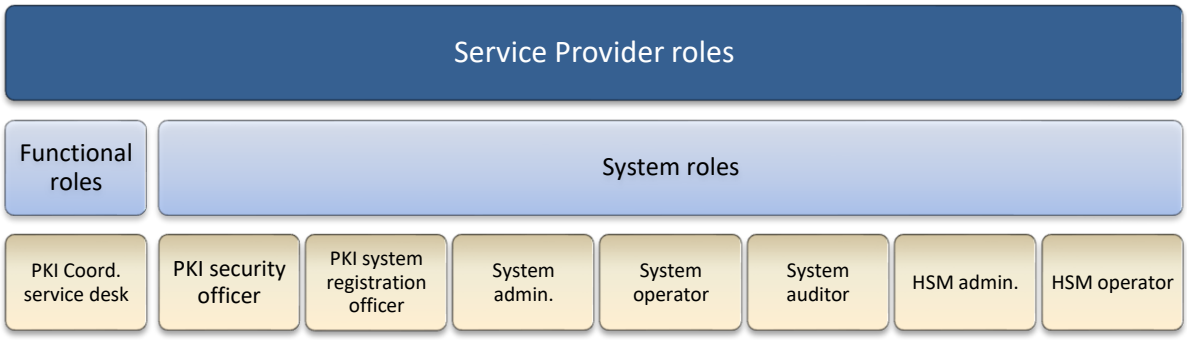
- Guaranteeing that the data for the creation and verification of the digital signature is complementary;
- Providing information to the certificate subscriber, free of charge, either in written form or by email about her responsibilities;
- Keeping an up-to-date directory containing the certificates and information about their current expiration and revocation status;
- Employing qualified personnel experienced in the certification services offered;
- Revoking certificates and publishing this fact through CRLs in an elapsed time no longer than that is stated by the SLA, once the revocation request has been received;
- Facilitating access by electronic means to the latest version of the CPS and the CPs;
- Abiding by applicable personal data protection law, including refraining from keeping or copying subscriber information other than that necessary for the provision of the service;

- Issuing all requested certificates according to the norms and procedures established in the CPS and subsequent CPs;
- In general, abiding by all the obligations imposed by the CPS, CPs and applicable legislation.

The Service provider LSO shall approve the assignment to a Service provider role, which shall be assigned by the principle of least privilege.

This section describes the roles required to operate the ESCB-PKI services by the Service Provider. The roles are grouped in two categories:

- Roles for operating the PKI system;
- Roles for operating the Hardware Security Modules.



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 the Service Provider premises:

- *HSM Administrators*: Four eyes principle has been established on HSM administration. The HSM Administrators are responsible for carrying out the following operations:
- Recovery of cryptographic hardware functionality in the event of HSM failure.
- Key recovery in the event of accidental deleting.
- Replacement of a set of administrator cards. This operation only needs to be carried out when increasing or reducing the number of administrator cards.
- 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
- Increase in the number of HSM integrated in the infrastructure.
- 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:
- Key activation for their use. This means that each initiation of a CA requires the insertion of the operator cards linked to the keys.
- 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.
- 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 the Service Provider, 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 the Service Provider, 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 the Service Provider, 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 the Service Provider and are in charge of managing certificates for the PKI subsystems (CA, RA, VA and KA);
- **Registration Officers** nominated by the Registration Authorities, who are in charge of managing end user certificates. See chapter *1.3.3 Registration Authorities.*
- **Trusted Agents**: delegated at the Central Banks, National Competent Authorities, Cooperating Authorities or external organisations. They act as a representative of a Registration Authority only for user identification.
- **System Operators:** System Operators, belonging to the Service Provider, 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

Service Provider personnel assignment shall be done according to the following incompatibility matrix:

	PKI security Officers	PKI system Registration Officers	System Admin.	System Operators	System Auditors
PKI security Officers			✘		✘
PKI system Registration Officers					✘
System Admin.	✘				✘
System Operators					✘
System Auditors	✘	✘	✘	✘	

✘ = 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. These requirements also apply whenever contracting third parties are involved in the performance of any of the services related to the ESCB-PKI. Therefore, 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 background checks and clearance procedures are performed.

5.3.3 Training requirements

In accordance with the procedures established by the Service Provider 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

The Service Provider 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 the Service Provider Labour Regulations and in applicable law, without prejudice to the liabilities of any other kind that may be incurred.

5.3.7 Requirements for third party contracting

The Service Provider general regulations shall be applied to contracting. The Service Provider will have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

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:

Outcome: Success or failure of the event
Date: Date and time of the event.
Actors: Distinguished Name of the Authority that generated the event.
Partition: Partition where the even was generated.
Remote Client: Client IP address that generated the event.
Error Message: If the event is in failure, this is the error message that can help finding the root cause.
Error Code: If the event is in failure, this number will uniquely identifies the type of error.
Module: Identifies the module that generated the event.

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 profile that issued the certificate.
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 encryption 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

According to the ESCB Information Systems Risk Management methodology, the Service Provider performs a periodic assessment of ESCB-PKI services, and implements mitigation plans for those threats that remain unmitigated after the 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 CA stores, 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 encryption 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 encryption 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 an Incident Response Plan that sets out the actions to be taken in case a security incident is detected.

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.
- Steps to be taken in the event of a disaster:
- Start-up of an alternative backup centre.
- Following the disaster, potential improvements to the service to avoid repetition of a disaster.
- Complete and periodic checks of the backup copy service.

In the event of any compromise of the CA private key, 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 the ESCB-PKI System Owner decides the termination of activities of the CA, 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.
- will notify all subscribers and other entities with which it has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies. In addition, this information shall be made available to other relying parties.
- will terminate any subcontractor acting on his behalf in carrying out any functions relating to the process of issuing trust service tokens.
- will transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information will destroy, or withdrawn from use, the affected private keys, in a manner such that the private keys cannot be retrieved.

In the event the System Owner of the ESCB-PKI service decides to transfer the activity to another Services Provider:

- The System Owner shall notify their certificate subscribers regarding the transfer agreements. For this purpose, the System Owner 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 Service Provider shall
- notify the National Supervisory Body 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.
- send the National Supervisory Body, prior to final termination of its activity, the data related to the certificates for which validity has been terminated
- Likewise, it shall report any other relevant circumstance that could prevent activity continuity.
- 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 the Service Provider 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:

- HSM module status boot up.
- Creation of administration and operator cards.
- 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 encryption 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.

6.2.5 Private key archive

Private keys for signature certificates of individuals are never archived in order to guarantee non-repudiation.

Encryption 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

[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.

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 Service Provider shall apply life-cycle safety measures related to:

- Change management, to manage new projects, evolutionary and software corrections.
- Malicious software control, to protect the system integrity against viruses or malicious software.
- Management of media, against storage media obsolescence and deterioration.
- Control of updates and security patches, against vulnerabilities in the system.

The Service Provider shall use trustworthy systems and products that are protected against modification and ensure technical security an reliability of the life-cycle, in particular:

- Change control procedures are applied for releases, modifications and emergency software corrections which applies the ESCB/SSM security policy.
- The integrity of the TSP's system is protected against viruses and malicious and unauthorised software.
- Media management procedures that protect against obsolescence and deterioration are required.
- Procedures are established for all trusted and administrative roles that impact on the provision of the service.
- Procedures for ensuring the application of security patches within a reasonable time after they come available, unless they introduce additional vulnerabilities.

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 non-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: • SIGNATURE • AUTHENTICATION • ENCRYPTION • MOBILE DEVICE • SECURE EMAIL GATEWAY • PROVISIONAL • ADMINISTRATOR • SHARED MAILBOX
0.4.0.127.0.10.1.3.2	escbIssuerName	Name of the Service Provider. This extension value will always be "BANCO DE ESPAÑA".
0.4.0.127.0.10.1.3.3	escbIssuerVAT	National value added tax identification number of the Service Provider. This extension value will always be "VATES-Q2802472G"

7.1.3 Algorithm Object Identifiers (OID)

Cryptographic algorithm objects identifiers (OID):

SHA-1 with RSA Encryption (1.2.840.113549.1.1.5) – no longer used after 12th January 2016

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" extension

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), 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

Risks that may incur the liability of the CA are covered by the Service Provider.

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, National Competent Authorities and Cooperating Authorities implementing the General Data Protection Regulation.

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), the Service Provider and the non-Eurosystem Central Banks and the National Competent Authorities and the Cooperating 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 General Data Protection Regulation.

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 *4.9 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: • Regulation (EU) No 910/2014 of the European Parliament and of the Council. • Spanish Organic Law 3/2018, of 5 December 2018, for the Protection of Personal Data and guarantee of digital rights.
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
CAO.21	A suitable time before expiration of its CA signing key, the CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key.

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. 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 Service Provider 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, the Service Provider 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 the Service Provider can prove that it has not acted negligently.

9.7.2 Scope of liability coverage

The provision of the ESCB-PKI service, in accordance to the Spanish Law aw 6/2020, of November 11, Regulating Certain Aspects of Trusted Electronic Services, as a service provided by the public sector, is covered by the Service Provider with its own funds.

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 6/2020, of November 11, Regulating Certain Aspects of Trusted Electronic Services, and are fully recognised within the European Union in accordance with the national laws and regulations implementing 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:

- General Data Protection Regulation of the European Parliament and of the Council[2];
- 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] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88.
[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.