Annex IX

BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI SERVICES

OIDS: 0.4.0.127.0.10.1.2.2.0

CERTIFICATE POLICIES FOR TECHNICAL CERTIFICATES

VERSION 1.0

ITC/19/010, 11 February 2019

Table of Contents

Control Sheet

	Title	Certification Policy for the Technical certificates
	Author	ESCB-PKI Service Provider
	Version	1.0
	Date	13.11.2018

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**
1.0	First version	13.11.2018	BdE revision

1 Introduction

1.1 Overview

This document sets out the Certificate Policy (CP) governing certificates issued to technical components (i.e. devices or applications that belong to ESCB Central Banks or SSM National Competent Authorities) by 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**[1].

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.

From the perspective of the X.509 v3 standard, a CP is a set of rules that define the applicability or use of a certificate within a community of users, systems or specific class of applications that have a series of security requirements in common.

This CP details and completes the "Certification Practice Statement" (CPS) of the ESCB-PKI, containing the rules to which the use of the certificates defined in this policy are subject, as well as the scope of application and the technical characteristics of this type of certificate.

This CP 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 any 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:

[1] 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).

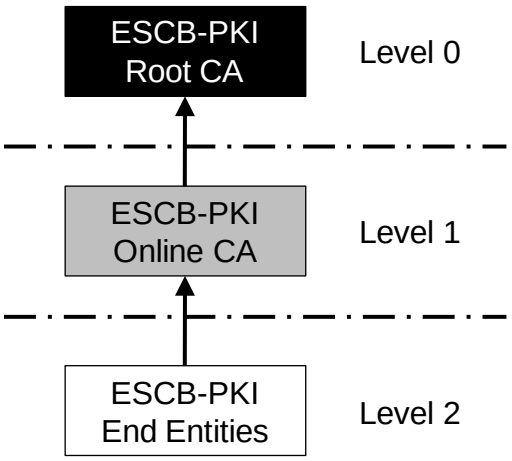
- Decision ECB/2015/47[2];
- General Data Protection Regulation[3]; Directive 1999/93/EC of the European Parliament and of the Council[4]; Regulation (EU) No 910/2014 of the European Parliament and of the Council[5]; Spanish Law 59/2003, of 19 December, the Electronic Signature Act (Spanish Official Journal, 20 December).[6]
- Regulation (EU) 2016/679 of the European Parliament and of the Council[7]; Spanish Organic Law 15/1999, of 13 December 1999, on the protection of personal data.
- Spanish Royal Decree 1720/2007, of 21 December2007, approving the Regulations for the development of Spanish Organic Law 15/1999.
- National legislation transposing the General Data Protection Regulation and the Directive 99/93/EC applicable to the ESCB central banks and SSM national competent authorities acting as Registration Authorities.

This CP 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 CP includes all the activities for managing ESCB/SSM technical 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 CP and adapt their activities to the stipulations therein.

This CP assumes that the reader is conversant with the 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, in hierarchic terms, of ESCB-PKI is as follows:



1.2 Document Name and Identification

[2] 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).

[3] 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.

[4] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

[5] 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).

[6] Spanish legislation is also considered owed to the fact that Banco de España, the Service Provide, is established at Spain.

[7] 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.

Document name	Certificate Policy (CP) for the Technical certificates
Document version	1.0
Document status	Final
Date of issue	13.11.2018
OID (Object Identifiers)	0.4.0.127.0.10.1.2.4.0: Certificate policies for Technical certificates (this document) 0.4.0.127.0.10.1.2.4.1: Certificate Policy for Application certificates 0.4.0.127.0.10.1.2.4.2: Certificate Policy for SSL Server certificates 0.4.0.127.0.10.1.2.4.3: Certificate Policy for Code Signing certificates 0.4.0.127.0.10.1.2.4.4: Certificate Policy for Domain Controller certificates 0.4.0.127.0.10.1.2.4.5: Certificate Policy for IPsec certificates 0.4.0.127.0.10.1.2.5.1: Certificate Policy for external Application certificates
CPS location	http://pki.escb.eu/policies
Related CPS	Certification Practice Statement of ESCB-PKI OID 0.4.0.127.0.10.1.2.1

1.3 ESCB-PKI Participants

As specified in the ESCB-PKI CPS.

1.3.1 The Policy Approval Authority

As specified in the ESCB-PKI CPS.

1.3.2 Certification Authority

As specified in the ESCB-PKI CPS.

1.3.3 Registration Authorities

As specified in the ESCB-PKI CPS.

1.3.3.1 Registration Authorities' roles

From the list of Registration Authorities' roles described in the CPS the ones required to manage technical certificates are the following:

- **Registration Officers For Technical Components (RO4TC)**
- **Trusted Agents (TA)**
- **Technical Certificate Subscribers (TCS)**

1.3.4 Validation Authority

As specified in the ESCB-PKI CPS.

1.3.5 Key Archive

Not applicable.

1.3.6 Users

As specified in the ESCB-PKI CPS.

1.3.6.1 Certificate Subscribers

Certificate subscribers are defined in accordance with the ESCB-PKI CPS.

The categories of technical components that may be subscribers of technical certificates issued by the ESCB-PKI Online CA are limited to those included in the following chart:

Certification Authority	Certificate subscribers
Online CA	Internal organisation components, devices or applications External organisation applications

Even though these are technical component certificates, there shall always be a person responsible for it. The responsible person for each different category of certificates usually is:

Certificate type	Responsible
Application	Application manager
SSL Server	Web server manager
Code Signing	Development project leader
Domain Controller	Active Directory manager
IPsec	Networking manager

1.3.6.2 Relying Parties

As specified in the ESCB-PKI CPS.

1.4 Certificate Usage

1.4.1 Appropriate certificate use

Technical certificates issued by ESCB-PKI may only be used to identify components or secure communications within the ESCB/SSM. See below the detailed appropriate usage for each certificate type:

Certificate type	Appropriate usage
Application	Identify applications within the ESCB/SSM Identify applications from external organisations accessing ESCB/SSM services Secure email
SSL Server	ESCB/SSM Web server identification
Code Signing	Signing code to guarantee code integrity and authentication within the ESCB/SSM
Domain Controller	Domain Controller authentication to smart card logon clients within the ESCB/SSM
IPsec	IPSec tunnelling within the ESCB/SSM

Within the scope above, certificates issued by ESCB-PKI may be used for financial activities.

1.4.2 Certificate Usage Constraints and Restrictions

Any other use not included in the previous point shall be excluded.

1.5 Policy Approval

As specified in the ESCB-PKI CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

Within the scope of this CP the following terms are used:

Authentication: the process of confirming the identity of a certificate subscriber.

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

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

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

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

Central Bank: In this CP 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.

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.

ESCB/SSM user: user that belongs to an ESCB Central Bank or to a SSM National Competent Authority.

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.

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).

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.

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

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

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

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.

ESCB-PKI Certification Authority: means the entity, trusted by users, to issue, manage, revoke and renew certificates in accordance with the ESCB certificate acceptance framework.

Trust 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.

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

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.

Certificate applicants: the individuals who request the issuance of certificates.

Certificate subscribers: the individuals for which an electronic certificate is issued and by whom it is accepted.

Relying parties: individuals or entities, other than certificate subscribers, that decide to accept and rely on a certificate issued by ESCB-PKI.

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.

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 CP 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.

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)

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

As specified in the ESCB-PKI CPS.

2.2 Publication of Certification Data, CPS and CP

As specified in the ESCB-PKI CPS.

2.3 Publication Timescale or Frequency

As specified in the ESCB-PKI CPS.

2.4 Repository Access Controls

As specified in the ESCB-PKI CPS.

3 Identification and Authentication (I&A)

3.1 Naming

3.1.1 Types of names

The certificates issued by ESCB-PKI contain the Distinguished Name (or DN) X.500 of the issuer and that of the certificate subject in the fields *issuer name* and *subject name*, respectively.

Attribute Common Name (CN) references the specific component, which makes use of the certificate.

Certificate type	Common Name
Application	CN = [AUT] <ESCB_Application_Code> <ESCB_Application_DisplayName>
SSL Server	CN = <hostname>
Code Signing	CN = < DisplayName>
Domain Controller	CN = <Domain Controller DNS name>
IPsec	CN = <hostname>

Additionally, Application certificates also include the following field (optionally):

- PS (OID: 2.5.4.65) = <Unique identifier at ESCB/SSM level>

The rest of the DN attributes shall have the following fixed values:

- C [Country where the Registration Authority is located]
- O EUROPEAN SYSTEM OF CENTRAL BANKS
- OU Central Bank or National Competent Authority to which the certificate subscriber belongs to

3.1.2 The need for names to be meaningful

In all cases the distinguished names of the certificates are meaningful because they are subject to the rules established in the previous point in this respect.

3.1.3 Rules for interpreting various name formats

As specified in the ESCB-PKI CPS.

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.

Certificate DNs must not be repeated. Technical controls are established that do not allow a new technical component to be registered in the system if it would allow to issue certificates with the same DN than an existing one of the same type.

3.1.5 Name dispute resolution procedures

As specified in the ESCB-PKI CPS.

3.1.6 Recognition, authentication, and the role of trademarks

As specified in the ESCB-PKI CPS.

3.2 Initial Identity Validation

3.2.1 Means of proof of possession of the private key

If the ESCB-PKI Online CA creates the key pair, this section does not apply.

If the key pair are created by other means, the responsible for the component will be required to provide a certificate request containing the public key signed by its associated private key.

3.2.2 Identity authentication for an entity

This CP does not consider the issuance of certificates for entities.

3.2.3 Identity authentication for an individual

Evidence of the subject's identity is checked against an accepted authentication certificate.

3.2.4 Non-verified applicant information

All the information provided by the certificate requestor must be verified.

3.2.5 Validation of authority

As specified in the ESCB-PKI CPS.

3.2.6 Criteria for operating with external CAs

As specified in the ESCB-PKI CPS.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication requirements for routine re-key

The same process as for initial identity validation is used.

3.3.2 Identification and authentication requirements for re-key after certificate revocation

The same process as for initial identity validation is used.

4 Certificate Life-Cycle Operational Requirements

This chapter contains the operational requirements for the life cycle of ESCB/SSM technical certificates issued by the ESCB-PKI CA. Despite the fact that these certificates might be stored on technical components or HSM, it is not the purpose of the CP to regulate the management of these elements.

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Technical component certificate requests will be created by Technical Certificate Subscribers, providing all the required data, including if applicable, the signed public key.

4.1.2 Enrolment process and applicants' responsibilities

In the case the certificates purpose is within the ESCB/SSM, the following procedure applies:

The enrolment process is the same for all types of technical component certificates and is wholly managed by the ESCB-PKI web interface, which requires advanced means of authentication[8] to any of the mentioned participants:

1. The Technical Certificate Subscriber provides the technical component required information and creates a certificate request of the appropriate type, including if applicable the signed public key.
2. The Registration Officer for Technical Components review the certificate requests and approve or reject it.
3. If the request has been approved, the Technical Certificate Subscriber issues the certificate, fulfilling the issuance process.

In the case the certificate is requested by an external organisation, the following procedure applies:

The external organisation Trusted Agent sends a signed email containing the technical component information to his contact in the ESCB/SSM organisation. The process continues then equally to the previously described for certificates within the ESCB/SSM.

4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

The identification and authentication process will be done as specified in section 3.2.3 of this CP.

4.2.2 Approval or rejection of certificate applications

As specified in the ESCB-PKI CPS.

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 and its delivery. As far as possible, the Certification Authority will process requests within 24 hours.

4.3 Certificate Issuance

4.3.1 Actions performed by the CA during the issuance of the certificate

As specified in the ESCB-PKI CPS.

[8] As per the ESCB/SSM Identity and Management Policy states, advanced authentication means token based authentication certificates provided by any CAF compliant Certification Authority.

4.3.2 CA notification to the applicants of certificate issuance

Applicants will be advised of the availability of the certificates via e-mail.

4.4 Certificate Acceptance

4.4.1 Form of certificate acceptance

The act of filling a certificate request by a Technical Certificate Subscribers is considered itself as acceptance of the certificate usage conditions.

4.4.2 Publication of the certificate by the CA

The ESCB-PKI CA publishes a copy of ESCB/SSM technical certificates in an internal LDAP directory located at the service provider's premises, only available to ESCB/SSM systems on a need-to-know basis.

4.4.3 Notification of certificate issuance by the CA to other Authorities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Certificate subscribers' use of the private key and certificate

The certificates regulated by this CP may be used according to their key usage and extended key usage extensions to provide the following security services:

Certificate type	Appropriate usage
Application	Technical component authentication and secure exchange of information
SSL Server	Web server TLS/SSL authentication
Code Signing	Code signature providing integrity and code authentication
Domain Controller	Domain Controller authentication against Smart Card Logon users
IPsec	Web server tunnelling

4.5.2 Relying parties' use of the public key and the certificate

As specified in ESCB-PKI CPS.

4.6 Certificate Renewal

As specified in ESCB-PKI CPS.

4.7 Certificate Re-key

4.7.1 Circumstances for certificate renewal with key changeover

As specified in ESCB-PKI CPS.

4.7.2 Who may request certificate renewal?

Renewals must be requested by certificate subscribers.

4.7.3 Procedures for processing certificate renewal requests with key changeover

During the renewal process, the RO4TC will check that the information used to verify the identity and attributes of the certificate 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.

If any of the conditions established in this CP have changed, the certificate subscriber must be made aware of this and agree to it.

In any case, certificate renewal is subject to:

- Renewal must be requested as established for initial issuance, as is described in 4.1.2.
- Renewal of certificates may only be requested within the last 100 days of its lifetime.
- The CA not having 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

They are notified by e-mail.

4.7.5 Manner of acceptance of certificates with changed keys

As in the initial certificate issuance.

4.7.6 Publication of certificates with the new keys by the CA

The ESCB-PKI CA publishes a copy of the ESCB/SSM user's certificates in an internal LDAP directory located at the service provider's premises, only available to ESCB/SSM systems on a need-to-know basis.

4.7.7 Notification of certificate issuance by the CA to other Authorities

As specified in the ESCB-PKI CPS.

4.8 Certificate Modification

4.8.1 Circumstances for certificate modification

As specified in ESCB-PKI CPS.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

As specified in ESCB-PKI CPS.

Additionally, revoked ESCB/SSM technical certificates will be eliminated from the directory where they are published.

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 factor that recommends taking such action.

Likewise, certificate subscribers may also request revocation of their certificates, which they must do in accordance with the conditions established under point 4.9.3.

The identification policy for revocation requests will be the same as that of the initial registration.

4.9.3 Procedures for requesting certificate revocation

The certificate subscribers or individuals requesting the revocation must appear before the RO, identifying themselves and indicating the reason for the request.

The RO shall always process the revocation requests submitted by its assigned certificate subscribers. The request is made via an authenticated web Interface.

Apart from this ordinary procedure, PKI System registration officers may immediately revoke any certificate upon becoming aware of the existence of any of the causes for revocation.

4.9.4 Revocation request grace period

As specified in ESCB-PKI CPS.

4.9.5 Time limit for the CA to process the revocation request

Requests for revocation of certificates must be processed as quickly as possible, and in no case may said processing take more 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. CRLs stored in cache[9] memory, even when not expired, do not guarantee availability of updated revocation data.

For ESCB/SSM technical certificates, the ordinary validity verification procedure for a certificate shall be carried out with the ESCB-PKI Validation Authority, which shall indicate, through the OCSP protocol, the status of the certificate.

4.9.7 CRL issuance frequency

As specified in ESCB-PKI CPS.

4.9.8 Maximum latency between the generation of CRLs and their publication

The maximum time allowed between generation of the CRLs and their publication in the repository is 1 hour.

4.9.9 Online certificate revocation status checking availability

As specified in ESCB-PKI CPS.

4.9.10 Online revocation checking requirements

As specified in ESCB-PKI CPS.

4.9.11 Other forms of revocation alerts available

No stipulation.

4.9.12 Special requirements for the revocation of compromised keys

As specified in ESCB-PKI CPS.

4.9.13 Causes for suspension

Certificate suspension is the action that renders a certificate invalid for a period of time prior to its expiry date. Certificate suspension produces the discontinuance of the certificate's validity for a limited period of time, rendering it inoperative as regards its inherent uses and, therefore, discontinuance of the provision of certification services. Suspension of a certificate prevents its legitimate use by the certificate subscriber.

Suspension of a certificate entails its publication on the public-access Certificate Revocation Lists (CRL).

The main effect of suspension as regards the certificate is that certificates become invalid until they are again reactivated. Suspension shall not affect the underlying obligations created or notified by this CP, nor shall its effects be retroactive.

ESCB/SSM technical certificates may be suspended due to:

- Certificate subscriber’s request, under suspicion of key compromise.

4.9.14 Who can request the suspension?

The subscribers of ESCB/SSM technical certificates and Registration Officers.

[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. Its use could entail the risk of operating with outdated data.

4.9.15 Procedure for requesting certificate suspension

Technical certificate subscribers may immediately suspend his certificates via an authenticated Web Interface. Access will be granted by means of one of the following mechanisms:

- an authentication certificate;

4.9.16 Suspension period limits

The CA shall ensure that a certificate is not kept suspended for longer than is necessary to confirm its status.

Revocation will be processed immediately after receiving the certificate subscriber confirmation for revocation (see 4.9).

4.10 Certificate Status Services

As specified in ESCB-PKI CPS.

4.11 End of Subscription

As specified in ESCB-PKI CPS.

4.12 Key Escrow and Recovery

4.12.1 Key Archive and recovery practices and policies

ESCB-PKI does not archive technical certificates private keys.

4.12.2 Session key protection and recovery policies and practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

As specified in the ESCB-PKI CPS.

5.2 Procedural Controls

As specified in the ESCB-PKI CPS.

5.3 Personnel Controls

As specified in the ESCB-PKI CPS.

5.4 Audit Logging Procedures

As specified in the ESCB-PKI CPS.

5.5 Records Archival

5.5.1 Types of records archived

As specified in the ESCB-PKI CPS.

5.5.2 Archive retention period

The retention period for records related to ESCB/SSM technical certificates is 15 years, which is the legally mandated period according to the Spanish legislation.

5.5.3 Archive protection

As specified in the ESCB-PKI CPS.

5.5.4 Archive backup procedures

As specified in the ESCB-PKI CPS.

5.5.5 Requirements for time-stamping records

As specified in the ESCB-PKI CPS.

5.5.6 Audit data archive system (internal vs. external)

As specified in the ESCB-PKI CPS.

5.5.7 Procedures to obtain and verify archived information

As specified in the ESCB-PKI CPS.

5.6 Key Changeover

As specified in the ESCB-PKI CPS.

5.7 Compromise and Disaster Recovery

As specified in the ESCB-PKI CPS.

5.8 CA or RA Termination

As specified in the ESCB-PKI CPS.

6 Technical Security Controls

Technical security controls for internal ESCB-PKI components, and specifically those controls for Root CA and Online CA, during certificate issue and certificate signature processes, are described in the ESCB-PKI CPS.
In this paragraph, technical security controls for the issuance of certificates under this CP are covered.

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Keys for ESCB/SSM technical certificates issued by the Online CA may be created by the subscriber or the Online CA, depending on the choice preferred by the subscriber. If the subscriber prefers to create the keys himself, a PKCS#10 will have to be provided to the ESCB-PKI in order to obtain his certificate.

6.1.2 Delivery of private keys to certificate subscribers

If the subscriber selects not to provide a PKCS#10 to the ESCB-PKI, the ESCB-PKI will create the key pair and the associated certificate and request the subscriber to provide a password. Finally, by means of an authenticated web interface, a PKCS#12 file containing the key pair and certificate, protected with the subscriber password will be provided to the subscriber.

6.1.3 Delivery of the public key to the certificate issuer

If the subscriber selects to provide a PKCS#10 to the ESCB-PKI, the public keys are generated by certificate subscribers and then delivered to the ESCB-PKI Online CA within the process required to obtain the certificate.

6.1.4 Delivery of the CA's public key to relying parties

The ESCB-PKI Online CA public key is included in the certificate of that CA. The ESCB-PKI Online CA certificate is not included in the certificate package generated for the certificate subscriber. The ESCB-PKI Online CA certificate must be obtained from the repository specified in this document where it is available by certificate subscribers and relying parties to carry out any type of verification.

6.1.5 Key sizes

The key size of any ESCB/SSM technical certificates is 2048 bits.

6.1.6 Public key generation parameters and quality checks

Public keys are encoded pursuant to RFC 5280 and PKCS#1. The key generation algorithm is the RSA.

6.1.7 Key usage purposes (KeyUsage field in X.509 v3)

The ‘Key Usage’ and ‘Extended Key Usage’ fields of the certificates included in this CP are described in the 7.1.2.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

The Hardware Security Module (HSM) used for the creation of keys used by ESCB-PKI Online CA is pursuant to FIPS 140-2 Level 3.
Start-up of each of the Certification Authorities, taking into account that a HSM is used, involves the following tasks:

a HSM module status boot up.
b Creation of administration and operator cards.
c Generation of the CA keys.

As regards the cryptographic token, they will be pursuant to the FIPS 140-2 level 3 or CC EAL4+ specification or equivalent. In the case of advanced signature certificates based on a SSCD, they will be also pursuant to the SSCD specification (CWA 14169).

6.2.2 Private key multi-person (k out of n) control

The private key, both for Root CA as for Subordinate CA, is under multi-person control; its activation is done through CA software initialisation by means of a combination of CA and HSM operators. This is the only activation method for said private key.

There is no multi-person control established for accessing the private keys of the certificates issued under this CP. When key archive service is requested by the CB, the recovery process will be as described in section 4.12.1

6.2.3 Escrow of private keys

No technical certificates are escrowed

6.2.4 Private key backup copy

The certificate subscribers will have to keep the PKCS#12 file and corresponding protection password as a backup copy.

6.2.5 Private key archive

ESCB-PKI will not keep any archive of the private key associated to technical certificates.

6.2.6 Private key transfer into or from a cryptographic module

No stipulated

6.2.7 Private key storage in a cryptographic module

Private keys for technical certificates created by the ESCB-PKI Online CA are created using the ESCB-PKI Online CA cryptographic module, but they are not subsequently saved.

6.2.8 Private key activation method

Private keys delivered in a PKCS#12 file are protected by a password. The password is required to activate the private key.

6.2.9 Private key deactivation method

No stipulation.

6.2.10 Private key destruction method

No stipulation.

6.2.11 Cryptographic module classification

The cryptographic modules used by ESCB-PKI technical components comply with the FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archive

As specified in the ESCB-PKI CPS.

6.3.2 Operational period of certificates and usage periods for key pairs

All certificates and their linked key pair have a lifetime of 3 years, although the ESCB-PKI Online CA may establish a shorter period at the time of their issue.

6.4 Activation Data

As specified in the ESCB-PKI CPS.

6.5 Computer Security Controls

As specified in the ESCB-PKI CPS.

6.6 Life Cycle Security Controls

As specified in the ESCB-PKI CPS.

6.7 Network Security Controls

As specified in the ESCB-PKI CPS.

6.8 Timestamping

As specified in the ESCB-PKI CPS.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version number

Certificates for the ESCB/SSM users are compliant with the X.509 version 3 (X.509 v3) standard.

7.1.2 Certificate extensions

The certificate extensions used generically are:

- *Subject Key Identifier*. Classified as non-critical.
- *Authority Key Identifier*. Classified as non-critical.
- *KeyUsage*. Classified as critical.
- *extKeyUsage.* Classified as non-critical.
- *CertificatePolicies*. Classified as non-critical.
- *SubjectAlternativeName*. Classified as non-critical.
- *BasicConstraints*. Classified as critical.
- *CRLDistributionPoint*. Classified as non-critical.
- *Auth. Information Access*. Classified as non-critical.
- escbUseCertType *(0.4.0.127.0.10.1.3.1)*. Classified as non-critical.
- escbIssuerName *(0.4.0.127.0.10.1.3.2)*. Classified as non-critical.
- escbIssuerVAT *(0.4.0.127.0.10.1.3.3)*. Classified as non-critical.

For understanding purposes, all ESCB-PKI OID attributes references are made under the [OID ESCBPKI] mark, which corresponds to 0.4.0.127.0.10.1.

7.1.2.1 Application

Application certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (accepted for legacy systems only) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which responsible is member* *ESCB_Unique_Identifier (UID)*[10] [AUT] *ESCB_Application_Code ESCB_Application_DisplayName*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature[11] Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 1 1 1 0 0	Yes
extKeyUsage	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.4.1 ó *[OID ESCBPKI]*.2.5.1[12] *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1.7)	 *Subject's Email* *ESCB user identifier (UID)*	

[10] Optional

[11] This usage is allowed in the scenarios where a digital signature is generated to authenticate the certificate subscriber

[12] [OID ESCBPKI].2.4.1 if the organisation is a participant organisation in ESCB-PKI. [OID ESCBPKI].2.5.1 if it is an external organisation.

RegisteredID (*[OID ESCBPKI]*.1.1.9) RegisteredID (*[OID ESCBPKI]*.1.1.11)	*ESCB Application Code* *ESCB Application Display Name*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access caIssuers caIssuers Ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbUseCertType	AUTHENTICATION AND ENCRYPTION	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.2 SSL Server

SSL Server certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (accepted for legacy systems only) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which responsible is member* *Host name*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 1 0 1 0 0	Yes
extKeyUsage	serverAuth (1.3.6.1.5.5.7.3.1) clientAuth (1.3.6.1.5.5.7.3.2)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.4.2 *[CPS-URL]*	
Subject Alternative Names DNSName IPAddress rfc822	 *Full Qualified Distinguished Name (one or several)* *IP Server Address (if applicable)* *Contact Email Address (if applicable)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access		

caIssuers caIssuers Ocsp	*[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.3 Domain Controller

Domain Controller certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before 12/01/2016) or SHA256-WithRSAEncryption (for certificates issued after 12/01/2016)	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which responsible is member* *DNS Name*	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 1 0 0 0 0	Yes
extKeyUsage	serverAuth (1.3.6.1.5.5.7.3.1) clientAuth (1.3.6.1.5.5.7.3.2)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.4.4 *[CPS-URL]*	
Subject Alternative Names RegisteredID GUID (1.3.6.1.4.1.311.25.1) DNSName	 *Globally Unique Identifier* *DNS name*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access		

caIssuers caIssuers ocsp	*[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	
Other Extensions		
Certificate Template Name (1.3.6.1.4.1.311.20.2)	*DomainController (BMP Data)*	

7.1.2.4 Code Signing

Code Signing certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (for certificates issued before 12/01/2016) or SHA256-WithRSAEncryption (for certificates issued after 12/01/2016)	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject C O OU CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Central Bank or National Competent Authority within which responsible is member* DisplayName	
Subject Public Key Info Algorithm Minimum Length	 RSA Encryption 2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier KeyIdentifier AuthorityCertIssuer AuthorityCertSerialNumber	 *SHA-1 hash over CA Issuer public key* *Not used* *Not used*	
KeyUsage Digital Signature[13] Non Repudiation Key Encipherment[14] Data Encipherment[12] Key Agreement Key Certificate Signature CRL Signature	 1 0 0 0 0 0 0	Yes
extKeyUsage	codeSigning (1.3.6.1.5.5.7.3.3)	
Certificate Policies Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.4.3 *[CPS-URL]*	
Subject Alternative Names rfc822	 *Contact Email Address (if applicable)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		

[13] This usage is allowed in the scenarios where a digital signature is generated to authenticate the certificate subscriber

[14] keyEncipherment and dataEncipherment are allowed for emailProtection only. The private key is never stored in the Key Archive.

Private Extensions		
Authority Information Access		
calssuers	*[HTTP URI Root CA]*	
calssuers	*[HTTP URI Sub CA]*	
ocsp	*[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.5 IPsec

IPsec certificate		
Field	**Value**	**Critical**
Base Certificate		
Version	3	
Serial Number	*Random*	
Signature Algorithm	SHA1-WithRSAEncryption (accepted for legacy systems only) or SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	*3 years*	
Subject		
C	*[Registration Organisation Country]*	
O	EUROPEAN SYSTEM OF CENTRAL BANKS	
OU	*Central Bank or National Competent Authority within which responsible is member*	
CN	*Host name*	
Subject Public Key Info		
Algorithm	RSA Encryption	
Minimum Length	2048 bits	
Standard Extensions		
Subject Key Identifier	*SHA-1 hash over subject public key*	
Authority Key Identifier		
KeyIdentifier	*SHA-1 hash over CA Issuer public key*	
AuthorityCertIssuer	*Not used*	
AuthorityCertSerialNumber	*Not used*	
KeyUsage		Yes
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
extKeyUsage	serverAuth (1.3.6.1.5.5.7.3.1) clientAuth (1.3.6.1.5.5.7.3.2) id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17)	
Certificate Policies		
Policy Identifier	*[OID ESCBPKI]*.2.4.5	
URL CPS	*[CPS-URL]*	

Subject Alternative Names DNSName IPAddress rfc822	 *Full Qualified Distinguished Name (one or several)* *IP Server Address (if applicable)* *Contact Email Address (if applicable)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
CRL Distribution Points		
Private Extensions		
Authority Information Access calssuers calssuers Ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.3 Algorithm Object Identifiers (OID)

Cryptographic algorithm object identifiers (OID):

SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)

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

See section 3.1.1.

7.1.6 Certificate Policy Object Identifiers (OID)

The OIDs for this CP are the following:

[OID ESCBPKI].2.4.0.X.Y: Certificate policies for Technical certificates (this document)

[OID ESCBPKI].2.4.1.X.Y: Certificate Policy of Application certificates within the ESCB/SSM

[OID ESCBPKI].2.5.1.X.Y: Certificate Policy of Application certificates for external organisations

[OID ESCBPKI].2.4.2.X.Y: Certificate Policy of SSL Server certificates within the ESCB/SSM

[OID ESCBPKI].2.4.3.X.Y: Certificate Policy of Domain Controller certificates within the ESCB/SSM

[OID ESCBPKI].2.4.4.X.Y: Certificate Policy of Digital Signature certificates within the ESCB/SSM

[OID ESCBPKI].2.4.5.X.Y: Certificate Policy of IPsec certificates within the ESCB/SSM

Where:

- [OID ESCBPKI]: represents the OID 0.4.0.127.0.10.1
- X.Y indicate the version.

7.1.7 Use of the "PolicyConstraints" extension

As specified in the ESCB-PKI CPS.

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 to the CP that govern the certificate.

The content for certificates regulated under this policy can be seen in point *7.1.2 Certificate extensions*.

7.1.9 Processing semantics for the critical "CertificatePolicy" extension

As specified in the ESCB-PKI CPS.

7.2 CRL Profile

As specified in the ESCB-PKI CPS.

7.3 OCSP Profile

As specified in the ESCB-PKI CPS.

8 Compliance Audit and Other Assessment

As specified in the ESCB-PKI CPS.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

ESCB-PKI will not charge any direct fee to the certificate subscribers for the issuance or renewal of ESCB/SSM technical certificates.

9.1.2 Certificate access fees

Access to certificates issued under this Policy is free of charge and, therefore, no fee is applicable to them.

9.1.3 Revocation or status information fees

Access to information on the status or revocation of the certificates is open and free of charge and, therefore, no fees are applicable.

9.1.4 Fees for other services, such as policy information

No fee shall be applied for information services on this policy, nor on any additional service that is known at the time of drawing up this document.

9.1.5 Refund policy

Not applicable.

9.2 Financial Responsibility

As specified in the ESCB-PKI CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

As specified in the ESCB-PKI CPS.

9.3.2 Non-confidential information

As specified in the ESCB-PKI CPS.

9.3.3 Duty to maintain professional secrecy

As specified in the ESCB-PKI CPS.

9.4 Privacy of Personal Information

As specified in the ESCB-PKI CPS.

9.4.1 Personal data protection policy

As specified in the ESCB-PKI CPS.

9.4.2 Information considered private

As specified in the ESCB-PKI CPS.

9.4.3 Information not classified as private

As specified in the ESCB-PKI CPS.

9.4.4 Responsibility to protect personal data

As specified in the ESCB-PKI CPS.

9.4.5 Notification of and consent to the use of personal data

The mechanisms to notify certificate applicants and, when appropriate, obtain their consent for the processing of their personal data is the terms and conditions application form.

9.4.6 Disclosure within legal proceedings

As specified in the ESCB-PKI CPS.

9.4.7 Other circumstances in which data may be made public

As specified in the ESCB-PKI CPS.

9.5 Intellectual Property Rights

As specified in the ESCB-PKI CPS.

9.6 Representations and Warranties

As specified in the ESCB-PKI CPS.

9.7 Disclaimers of Warranties

As specified in the ESCB-PKI CPS.

9.8 Limitations of Liability

As specified in the ESCB-PKI CPS.

9.9 Indemnities

As specified in the ESCB-PKI CPS.

9.10 Term and Termination

9.10.1 Term

This CP shall enter into force from the moment it is approved by the PAA and published in the ESCB-PKI repository.

This CP 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 Corporate CA keys, at which time it is mandatory to issue a new version.

9.10.2 CP substitution and termination

This CP shall always be substituted by a new version, regardless of the importance of the changes carried out therein, meaning that it will always be applicable in its entirety.

When the CP is terminated, it will be withdrawn from the ESCB-PKI public repository. Nevertheless, it will be kept for 15 years.

9.10.3 Consequences of termination

The obligations and constraints established under this CP, 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 substitution or termination with a new version in all terms which are not contrary to said new version.

9.11 Individual notices and communications with participants

As specified in the ESCB-PKI CPS.

9.12 Amendments

As specified in the ESCB-PKI CPS.

9.13 Dispute Resolution Procedures

As specified in the ESCB-PKI CPS.

9.14 Governing Law

As specified in the ESCB-PKI CPS.

9.15 Compliance with Applicable Law

As specified in the ESCB-PKI CPS.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement clause

As specified in the ESCB-PKI CPS.

9.16.2 Independence

Should any of the provisions of this CP 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 CP would render the latter without legal effect.

9.16.3 Resolution through the courts

As specified in the ESCB-PKI CPS.

9.17 Other Provisions

As specified in the ESCB-PKI CPS.