

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

**BANCO DE ESPAÑA**  
Eurosistema

## **INFORMATION TECHNOLOGY COMMITTEE**

### **ESCB-PKI SERVICES**



**OIDS: 0.4.0.127.0.10.1.2.3.0**

**CERTIFICATE POLICIES FOR THE EXTERNAL USERS' CERTIFICATES**

**VERSION 1.7**

22 August 2023

## Table of Contents

<b>1</b>	<b><i>Introduction</i></b> .....	<b>9</b>
1.1	<b>Overview</b> .....	<b>9</b>
1.2	<b>Document Name and Identification</b> .....	<b>11</b>
1.3	<b>ESCB-PKI Participants</b> .....	<b>12</b>
1.3.1	The Policy Approval Authority.....	12
1.3.2	Certification Authority .....	12
1.3.3	Registration Authorities .....	12
1.3.4	Validation Authority .....	12
1.3.5	Key Archive.....	12
1.3.6	Users .....	12
1.4	<b>Certificate Usage</b> .....	<b>13</b>
1.4.1	Appropriate certificate use .....	13
1.4.2	Certificate Usage Constraints and Restrictions .....	13
1.5	<b>Policy Approval</b> .....	<b>13</b>
1.6	<b>Definitions and Acronyms</b> .....	<b>13</b>
1.6.1	Definitions .....	13
1.6.2	Acronyms.....	15
<b>2</b>	<b><i>Publication and Repository Responsibilities</i></b> .....	<b>16</b>
2.1	<b>Repositories</b> .....	<b>16</b>
2.2	<b>Publication of Certification Data, CPS and CP</b> .....	<b>16</b>
2.3	<b>Publication Timescale or Frequency</b> .....	<b>16</b>
2.4	<b>Repository Access Controls</b> .....	<b>16</b>
<b>3</b>	<b><i>Identification and Authentication (I&amp;A)</i></b> .....	<b>17</b>
3.1	<b>Naming</b> .....	<b>17</b>
3.1.1	Types of names .....	17
3.1.2	The need for names to be meaningful .....	17
3.1.3	Rules for interpreting various name formats .....	17
3.1.4	Uniqueness of names .....	17
3.1.5	Name dispute resolution procedures .....	17
3.1.6	Recognition, authentication, and the role of trademarks .....	17
3.2	<b>Initial Identity Validation</b> .....	<b>17</b>
3.2.1	Means of proof of possession of the private key .....	17
3.2.2	Identity authentication for an entity .....	18
3.2.3	Identity authentication for an individual .....	18
3.2.4	Non-verified applicant information.....	19
3.2.5	Validation of authority .....	19
3.2.6	Criteria for operating with external CAs.....	19
3.3	<b>Identification and Authentication for Re-key Requests</b> .....	<b>19</b>

3.3.1	Identification and authentication requirements for routine re-key .....	19
3.3.2	Identification and authentication requirements for re-key after certificate revocation .....	19
<b>4</b>	<b><i>Certificate Life-Cycle Operational Requirements</i></b> .....	<b>20</b>
<b>4.1</b>	<b>Certificate Application</b> .....	<b>20</b>
4.1.1	Who can submit a certificate application? .....	20
4.1.2	Enrolment process and applicants' responsibilities .....	20
<b>4.2</b>	<b>Certificate Application Processing</b> .....	<b>22</b>
4.2.1	Performance of identification and authentication procedures .....	22
4.2.2	Approval or rejection of certificate applications .....	22
4.2.3	Time limit for processing the certificate applications .....	22
<b>4.3</b>	<b>Certificate Issuance</b> .....	<b>22</b>
4.3.1	Actions performed by the CA during the issuance of the certificate.....	22
4.3.2	CA notification to the applicants of certificate issuance .....	22
<b>4.4</b>	<b>Certificate Acceptance</b> .....	<b>22</b>
4.4.1	Form of certificate acceptance .....	22
4.4.2	Publication of the certificate by the CA .....	22
4.4.3	Notification of certificate issuance by the CA to other Authorities .....	22
<b>4.5</b>	<b>Key Pair and Certificate Usage</b> .....	<b>22</b>
4.5.1	Certificate subscribers' use of the private key and certificate .....	22
4.5.2	Relying parties' use of the public key and the certificate .....	22
<b>4.6</b>	<b>Certificate Renewal</b> .....	<b>22</b>
<b>4.7</b>	<b>Certificate Re-key</b> .....	<b>23</b>
4.7.1	Circumstances for certificate renewal with key changeover .....	23
4.7.2	Who may request certificate renewal? .....	23
4.7.3	Procedures for processing certificate renewal requests with key changeover.....	23
4.7.4	Notification of the new certificate issuance to the subscriber .....	23
4.7.5	Manner of acceptance of certificates with changed keys .....	23
4.7.6	Publication of certificates with the new keys by the CA .....	23
4.7.7	Notification of certificate issuance by the CA to other Authorities .....	23
<b>4.8</b>	<b>Certificate Modification</b> .....	<b>23</b>
4.8.1	Circumstances for certificate modification .....	23
<b>4.9</b>	<b>Certificate Revocation and Suspension</b> .....	<b>23</b>
4.9.1	Circumstances for revocation.....	23
4.9.2	Who can request revocation? .....	23
4.9.3	Procedures for requesting certificate revocation .....	24
4.9.4	Revocation request grace period .....	24
4.9.5	Time limit for the CA to process the revocation request .....	24
4.9.6	Requirements for revocation verification by relying parties .....	24
4.9.7	CRL issuance frequency .....	24
4.9.8	Maximum latency between the generation of CRLs and their publication .....	24
4.9.9	Online certificate revocation status checking availability .....	24
4.9.10	Online revocation checking requirements.....	24
4.9.11	Other forms of revocation alerts available .....	24

4.9.12	Special requirements for the revocation of compromised keys.....	24
4.9.13	Causes for suspension.....	24
4.9.14	Who can request the suspension?.....	25
4.9.15	Procedure for requesting certificate suspension.....	25
4.9.16	Suspension period limits.....	25
<b>4.10</b>	<b>Certificate Status Services.....</b>	<b>25</b>
<b>4.11</b>	<b>End of Subscription.....</b>	<b>25</b>
<b>4.12</b>	<b>Key Escrow and Recovery.....</b>	<b>25</b>
<b>5</b>	<b><i>Facility, Management, and Operational Controls.....</i></b>	<b>26</b>
<b>5.1</b>	<b>Physical Security Controls.....</b>	<b>26</b>
<b>5.2</b>	<b>Procedural Controls.....</b>	<b>26</b>
<b>5.3</b>	<b>Personnel Controls.....</b>	<b>26</b>
<b>5.4</b>	<b>Audit Logging Procedures.....</b>	<b>26</b>
<b>5.5</b>	<b>Records Archival.....</b>	<b>26</b>
5.5.1	Types of records archived.....	26
5.5.2	Archive retention period.....	26
5.5.3	Archive protection.....	26
5.5.4	Archive backup procedures.....	26
5.5.5	Requirements for time-stamping records.....	26
5.5.6	Audit data archive system (internal vs. external).....	26
5.5.7	Procedures to obtain and verify archived information.....	26
<b>5.6</b>	<b>Key Changeover.....</b>	<b>26</b>
<b>5.7</b>	<b>Compromise and Disaster Recovery.....</b>	<b>26</b>
<b>5.8</b>	<b>CA or RA Termination.....</b>	<b>26</b>
<b>6</b>	<b><i>Technical Security Controls.....</i></b>	<b>27</b>
<b>6.1</b>	<b>Key Pair Generation and Installation.....</b>	<b>27</b>
6.1.1	Key pair generation.....	27
6.1.2	Delivery of private keys to subscribers.....	27
6.1.3	Delivery of the public key to the certificate issuer.....	27
6.1.4	Delivery of the CA's public key to relying parties.....	27
6.1.5	Key sizes.....	27
6.1.6	Public key generation parameters and quality checks.....	28
6.1.7	Key usage purposes (KeyUsage field in X.509 v3).....	28
<b>6.2</b>	<b>Private Key Protection and Cryptographic Module Engineering Controls.....</b>	<b>28</b>
6.2.1	Cryptographic module standards.....	28
6.2.2	Private key multi-person (k out of n) control.....	28
6.2.3	Escrow of private keys.....	28
6.2.4	Private key backup copy.....	28
6.2.5	Private key archive.....	28
6.2.6	Private key transfer into or from a cryptographic module.....	28
6.2.7	Private key storage in a cryptographic module.....	29

6.2.8	Private key activation method.....	29
6.2.9	Private key deactivation method.....	29
6.2.10	Private key destruction method.....	29
6.2.11	Cryptographic module classification.....	29
<b>6.3</b>	<b>Other Aspects of Key Pair Management.....</b>	<b>29</b>
6.3.1	Public key archive.....	29
6.3.2	Operational period of certificates and usage periods for key pairs.....	29
<b>6.4</b>	<b>Activation Data.....</b>	<b>29</b>
<b>6.5</b>	<b>Computer Security Controls.....</b>	<b>29</b>
<b>6.6</b>	<b>Life Cycle Security Controls.....</b>	<b>29</b>
<b>6.7</b>	<b>Network Security Controls.....</b>	<b>29</b>
<b>6.8</b>	<b>Timestamping.....</b>	<b>30</b>
<b>7</b>	<b><i>Certificate, CRL, and OCSP Profiles.....</i></b>	<b><i>31</i></b>
<b>7.1</b>	<b>Certificate Profile.....</b>	<b>31</b>
7.1.1	Version number.....	31
7.1.2	Certificate extensions.....	31
7.1.3	Algorithm Object Identifiers (OID).....	41
7.1.4	Name formats.....	41
7.1.5	Name constraints.....	41
7.1.6	Certificate Policy Object Identifiers (OID).....	41
7.1.7	Use of the "PolicyConstraints" extension.....	41
7.1.8	Syntax and semantics of the "PolicyQualifier" extension.....	41
7.1.9	Processing semantics for the critical "CertificatePolicy" extension.....	41
<b>7.2</b>	<b>CRL Profile.....</b>	<b>41</b>
<b>7.3</b>	<b>OCSP Profile.....</b>	<b>41</b>
<b>8</b>	<b><i>Compliance Audit and Other Assessment.....</i></b>	<b><i>42</i></b>
<b>9</b>	<b><i>Other Business and Legal Matters.....</i></b>	<b><i>43</i></b>
<b>9.1</b>	<b>Fees.....</b>	<b>43</b>
9.1.1	Certificate issuance or renewal fees.....	43
9.1.2	Certificate access fees.....	43
9.1.3	Revocation or status information fees.....	43
9.1.4	Fees for other services, such as policy information.....	43
9.1.5	Refund policy.....	43
<b>9.2</b>	<b>Financial Responsibility.....</b>	<b>43</b>
<b>9.3</b>	<b>Confidentiality of Business Information.....</b>	<b>43</b>
9.3.1	Scope of confidential information.....	43
9.3.2	Non-confidential information.....	43
9.3.3	Duty to maintain professional secrecy.....	43
<b>9.4</b>	<b>Privacy of Personal Information.....</b>	<b>43</b>
9.4.1	Personal data protection policy.....	43
9.4.2	Information considered private.....	43

9.4.3	Information not classified as private .....	43
9.4.4	Responsibility to protect personal data .....	43
9.4.5	Notification of and consent to the use of personal data .....	43
9.4.6	Disclosure within legal proceedings .....	44
9.4.7	Other circumstances in which data may be made public .....	44
<b>9.5</b>	<b>Intellectual Property Rights .....</b>	<b>44</b>
<b>9.6</b>	<b>Representations and Warranties.....</b>	<b>44</b>
<b>9.7</b>	<b>Disclaimers of Warranties .....</b>	<b>44</b>
<b>9.8</b>	<b>Limitations of Liability .....</b>	<b>44</b>
<b>9.9</b>	<b>Indemnities .....</b>	<b>44</b>
<b>9.10</b>	<b>Term and Termination.....</b>	<b>44</b>
9.10.1	Term.....	44
9.10.2	CP substitution and termination .....	44
9.10.3	Consequences of termination .....	44
<b>9.11</b>	<b>Individual notices and communications with participants .....</b>	<b>44</b>
<b>9.12</b>	<b>Amendments.....</b>	<b>44</b>
<b>9.13</b>	<b>Dispute Resolution Procedures.....</b>	<b>44</b>
<b>9.14</b>	<b>Governing Law .....</b>	<b>44</b>
<b>9.15</b>	<b>Compliance with Applicable Law .....</b>	<b>44</b>
<b>9.16</b>	<b>Miscellaneous Provisions .....</b>	<b>45</b>
9.16.1	Entire agreement clause .....	45
9.16.2	Independence .....	45
9.16.3	Resolution through the courts .....	45
<b>9.17</b>	<b>Other Provisions .....</b>	<b>45</b>

## Control Sheet

	<b>Title</b>	Certification Policy for the external users' certificates
	<b>Author</b>	ESCB-PKI Service Provider
	<b>Version</b>	1.7
	<b>Date</b>	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	27.05.2011	BdE revision
0.2	Draft	15.06.2011	BdE revision
0.3	Draft	14.07.2011	BdE revision
0.4	Draft	22.07.2011	BdE revision
0.5	Draft	26.07.2011	Add CA Fingerprint
0.6	Draft	15.09.2011	Revision of certificate profiles
1.0	Final	19.10.2011	Update after ITC approval.
1.1	Final	11.01.2013	GovC approval
1.2	Final	11.05.2015	Hashing algorithm update
1.3	Final	29.11.2018	<ul style="list-style-type: none"> <li>• Key usage KeyEncipherment added to authentication certificate profile.</li> <li>• anyExtendedKeyUsage extended key usage removed in all certificate profiles.</li> <li>• Modifications to comply with Regulation № 910/2014: <ul style="list-style-type: none"> <li>○ New extensions escbIssuerName and escbIssuerVAT are included to comply with Regulation (EU) No 910/2014.</li> </ul> </li> <li>• Modifications to comply with ETSI EN 319 401: <ul style="list-style-type: none"> <li>○ Added a reference to the ESCB/SSM Information Systems Risk Management methodology</li> <li>○ Added a reference to the ESCB/SSM Information Systems Security Policy</li> </ul> </li> </ul>

			<ul style="list-style-type: none"> <li>○ Added a statement to clarify that ESCB-PKI services shall be provided in accordance with the principle of non-discrimination</li> <li>○ Added a statement to clarify that ESCB-PKI services shall be provided in accordance with the principle of non-discrimination</li> <li>○ Added various statements to clarify relations with potential contractors</li> <li>○ Updated chapters 1.3 and 5.2.1 to better clarify the ESCB-PKI role allocation procedures.</li> <li>○ Updated the CA termination plan</li> <li>○ Updated the Life-Cycle Security Controls</li> <li>○ Other minor updates</li> </ul>
1.4	Final	26.08.2019	Update after PKI-AB revision
1.5	Final	09.10.2020	<ul style="list-style-type: none"> <li>• A new type of participant organisation, namely <i>Cooperating Authorities</i> has been included. One of the consequences of this has been that this document has been renamed, from <i>Certification Policy for the non-ESCB/non-SSM users' certificates</i> to <i>Certification Policy for the external users' certificates</i>.</li> <li>• References to SHA1 certificates has been removed, as these certificates are no longer valid.</li> <li>• CA certificates hierarchy description has been updated to include potential new CA in the future.</li> <li>• Acceptance of Term &amp; Conditions by subscribers is no longer required to be made by handwritten signature in paper, but with a combination of the two following factors: <ul style="list-style-type: none"> <li>○ The subscriber will express their acceptance in the Registration Authority web application, using a designated checkbox.</li> <li>○ After the issuance of certificates, the subscriber will have one week to manifest their repudiation of their certificate acceptance. In this case, the certificates will be revoked.</li> </ul> </li> <li>• Subscriber identification may be made by remote means.</li> <li>• Updated references to the 2018 Spanish Data Protection Law.</li> </ul>
1.6	Final	10.02.2021	<ul style="list-style-type: none"> <li>• 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.</li> </ul>



1.7	Final	22.08.2023	<ul style="list-style-type: none"> <li>• Update for the release of the new Certification Authority: Online CA V1.2</li> <li>• Update 7.1.2 Certificate extensions with new OID and update of keyUsages.</li> </ul>
-----	-------	------------	--

## 1 Introduction

### 1.1 Overview

This document sets out the Certificate Policy (CP) governing the personal certificates issued to external users (i.e. users that belong to organisations external to ESCB Central Banks and SSM National Competent Authorities)<sup>1</sup> 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**<sup>2</sup>.

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

---

<sup>1</sup> Other organisations who are not ESCB Central Banks and SSM National Competent Authorities, such as the Cooperating Authorities, are not allowed to issue certificates for external organisations.

<sup>2</sup> 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).

- 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:

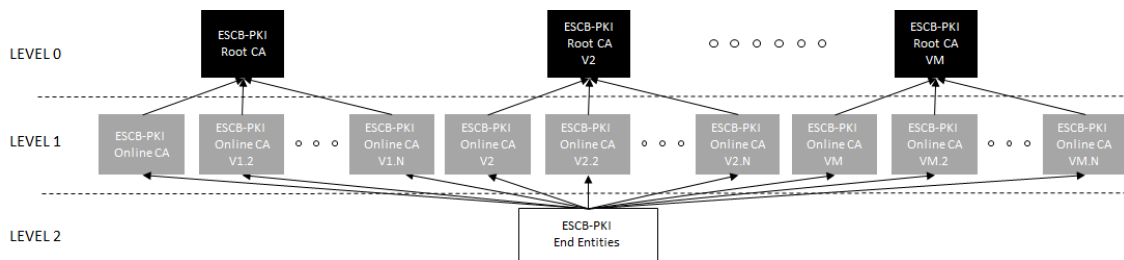
- Decision ECB/2015/47<sup>3</sup>;
- Regulation (EU) No 910/2014 of the European Parliament and of the Council<sup>4</sup>; Spanish Law 6/2020 of November 11, Regulating Certain Aspects of Trusted Electronic Services (Spanish Official Journal, 11 November).<sup>5</sup>
- Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>6</sup>; 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 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 the external users' certificates throughout their life cycle, and serves as a guide for the relations between the Online CA and its users. Consequently, all the PKI participants (see section 1.3) involved 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

<b>Document name</b>	Certificate Policy (CP) for the external users' certificates
<b>Document version</b>	1.7
<b>Document status</b>	Final
<b>Date of issue</b>	22.08.2023

<sup>3</sup> 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).

<sup>4</sup> 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).

<sup>5</sup> Spanish legislation is also considered owed to the fact the Service Provider is established at Spain.

<sup>6</sup> 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.

---

<b>OID (Object Identifiers)</b>	<p>0.4.0.127.0.10.1.2.3.0: Certificate policies for the external users' certificates (this document)</p> <p>0.4.0.127.0.10.1.2.3.1: Certificate Policy of Advanced Authentication certificate for external users</p> <p>0.4.0.127.0.10.1.2.3.2: Certificate Policy of Advanced Encryption certificate for external users</p> <p>0.4.0.127.0.10.1.2.3.4: Certificate Policy of Advanced Signature certificate based on a SSCD for external users</p> <p>0.4.0.127.0.10.1.2.3.5: Certificate Policy of Advanced Signature certificate for external users</p> <p>0.4.0.127.0.10.1.2.3.6: Certificate Policy of Standard Authentication certificate for external users</p>
<b>CPS location</b>	<a href="https://pki.escb.eu/policies">https://pki.escb.eu/policies</a>
<b>Related CPS</b>	<p>Certification Practice Statement of ESCB-PKI</p> <p>OID 0.4.0.127.0.10.1.2.1</p>

---

### 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 external users' certificates are the following:

- **Registration Officers for External Organisations**
- **Trusted Agents**

#### 1.3.4 *Validation Authority*

As specified in the ESCB-PKI CPS.

#### 1.3.5 *Key Archive*

No 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 persons who may be certificate subscribers of external users' certificates issued by the ESCB-PKI Online CA are limited to those included in the following chart:

Certification Authority	Certificate subscribers
Online CA	Users from external organisations that need to communicate with ESCB/SSM applications (as external users)
Online CA V1.2	Users from external organisations that need to communicate with ESCB/SSM applications (as external users)

Certificate subscribers will be able to receive any of the following certificate packages:

- **Advanced certificates**, where all the following certificates will be stored in a smartcard or other cryptographic token (e.g. USB device):
  - Advanced authentication certificate. The corresponding key pair will be generated inside the cryptographic token.
  - Advanced signature certificate or advanced signature certificate based on a SSCD depending upon if the cryptographic token has got a SSCD certification or not. In both cases, the corresponding private key will be generated inside the cryptographic token.
  - Advanced encryption certificate without key archive. The key pair will be generated inside the cryptographic token and no other copy will be archived.
- **Standard certificates**, where the private key will be generated by the CA and stored in a software device. The only type of standard certificate described in this CP is the authentication certificate.

#### 1.3.6.2 Relying Parties

As specified in the ESCB-PKI CPS.

### 1.4 Certificate Usage

#### 1.4.1 Appropriate certificate use

1 Certificates issued by ESCB-PKI in the scope of this CP may only be used within the scope of the ESCB/SSM by users from external organisations.

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

The certificates regulated by this CP shall be used for personal authentication, signing and/or encryption purposes, depending on the corresponding *keyUsage* extension and OID attribute in the *certificatePolicies* extension.

#### 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 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

**RO4EO:** Registration Officer for External Organisations

**RFC:** Request For Comments (Standard issued by the IETF)

**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.

Moreover, a copy of the external users' certificates is published in the directory of the ESCB Identity and Access Management (IAM) service.

### **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.

The CN (Common Name) attribute of the DN contains a prefix that identifies the certificate usage, and the following are accepted:

- [AUT:S] → Standard Authentication certificate
- [AUT:A] → Advanced Authentication certificate
- [SIG:A] → Advanced Signature certificate based on a token without SSCD certification
- [SIG:Q] → Advanced Signature certificate based on a token with SSCD certification
- [ENC:A] → Advanced Encryption certificate without private key archive

This prefix will be followed by the name, middle name and surnames of the certificate subscribers.

Additionally, the following field is used:

- PS (OID: 2.5.4.65) = <User 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 External organisation to which the 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. The use of the user identifier at ESCB/SSM level guarantees the uniqueness of the DN.

##### 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

Depending on the specific certificate type, the means of proof of private key possession will be different:

- [AUT:S] → standard authentication certificate: the key pair will be created by the ESCB-PKI Online Certification Authority, so this section does not apply.
- [AUT:A] → advanced authentication certificate: the key pair will be created by the subject in the private zone into his cryptographic token and the public key will be provided to the ESCB-PKI Online CA for its certification.

- [SIG:A] → advanced signature certificate (no SSCD token): the key pair will be created by the subject in the private zone into his cryptographic token and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [SIG:Q] → advanced Signature certificate based on a SSCD token: the key pair will be created by the subject in the SSCD zone of a secure signature creation device and the public key will be provided to the ESCB-PKI Online CA for its certification.
- [ENC:A] → advanced encryption without key archive: the key pair will be created by the subject in the private zone into his secure signature creation device and the public key will be provided to the ESCB-PKI Online CA for its certification.

### **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 a natural person, either in person or using remote means of identification.

#### **Validation of the individual**

Unless the certificate applicant has already been identified previously by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process with the same requirements, the certificate applicant shall provide evidences of, at least, the following information:

- Full name, and
- Date and place of birth, or reference to a nationally recognized identity document, or other attributes which may be used to distinguish the person from others with the same name.

To validate the previous information, the certificate applicant must present a document as proof of identity. The acceptable documents are:

- Passport, or
- National Identity Card, or
- Any other legal document accepted by the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority to dully identify an individual.

The validation of the identity will be performed by a Registration Officer for External Organisations or by a Trusted Agent delegated at the external organisation.

**Validation of the external organisation**

Unless the external organisation to which the certificate applicant belongs has already been validated previously by the Central Bank or National Competent Authority through a process with the same requirements, the following information must be provided:

1. To validate the external organisation:
  - Recent constitutive act of the external organisation, or
  - Recent extract of the national commercial register, or
  - Any equivalent document accepted by the applicable national legislation to fully identify an Organisation
  
2. To prove the applicant's relations with the external organisation:
  - An authorisation of one of the physical persons who are a legal representative of the external organisation, to request external users' certificates to be used in the communication between the ESCB/SSM and the Organisation
  - A copy of the identity evidence (National Identity card, Passport or any other legal document accepted by the applicable national legislation) of the physical person who is the legal representative of the Organisation; in case this person cannot be physically present, the copy must be certified by a competent authority according to the national legislation.

**3.2.4 Non-verified applicant information**

All the information stated in the previous section 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 external users' certificates issued by the ESCB-PKI CA. Despite the fact that these certificates might be stored on cryptographic tokens, it is not the purpose of the Certificate Policy to regulate the management of said tokens and, therefore, it is also assumed that the certificate applicants have previously obtained their cryptographic tokens.

### 4.1 Certificate Application

#### 4.1.1 *Who can submit a certificate application?*

Certificates for external users will be managed by a Registration Officer for External Organisations (RO4EO). RO4EOs will be able to request certificate types mentioned in section 1.3.6.

Application for a certificate does not mean it will be obtained if the applicant does not fulfil the requirements established in the CPS or in this CP for external users' certificates (e.g. if the certificate applicant does not provide the RO4EO with the documents necessary for his/her identification).

#### 4.1.2 *Enrolment process and applicants' responsibilities*

##### **Advanced certificates (cryptographic token-based)**

This process is carried out to obtain a certificate package consisting on three certificates: authentication, encryption and signature certificates. The certificate package will be stored in a cryptographic token. The procedure is the same independently on the type of token (with or without SSCD certification) to be used. The procedure is as follows:

1. Cryptographic token-based certificate requests for an external user can be initiated:
  - a. either using ESCB Identity Access Management (IAM) interfaces,
  - b. or using ESCB-PKI web interface;
2. The certificate applicant must explicitly accept the terms and conditions of the application form (T&C) by his/her selection of the term and conditions acceptance using a checkbox. The T&C will incorporate the following data:
  - a. the attributes to be included in the certificate: first name, middle name (if any), surname, name of the organisation that the user belongs to, user identifier and e-mail address;
  - b. the serial number of the certificate applicant's cryptographic token;
  - c. under the conditions and limitations of the applicable data protection law, central banks may require that the certificate applicant provides on the T&C the attributes required to distinguish the person from others with the same name (see Section 3.2.3), namely, the number of a national recognized identity document according to the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority, or the date and place of birth.
3. The RO4EO must validate the information included in the certificate request against the documentation provided by the certificate applicant, including the T&C. In case the certificate applicant identification has been made by a Trusted Agent, the RO will also validate that a valid Trusted Agent confirms having identified the applicant in accordance to section 3.2 of this CP;
4. The RO4EO, using the ESCB-PKI web interface, will either:
  - a. Start the issuance of certificates
  - b. Approve a remote download

In both cases the certificate applicant must hold his/her token and, when requested, must insert it and type his/her personal PIN to generate the keys and store the certificates,

5. The RO4EO must securely archive all the documentation during the retention period described in section 5.5.2 of this CP:
  - a. under the conditions and limitations of the applicable data protection law, the central bank may choose to ask their RO4EO to retain a copy of the official identification document used to validate the certificate applicant's identity or, if this were not legally feasible, a copy of other identification document, preferable with the certificate applicant's photography;

#### **Standard certificates (software-based)**

This process is carried out to obtain a single certificate valid for authentication that will be stored in a software keystore (i.e. a password protected file).

The procedure is as follows:

1. Software-based certificate requests for an external user can be initiated:
  - a. either using ESCB Identity Access Management (IAM) interfaces,
  - b. or using ESCB-PKI web interface;
2. The certificate applicant must explicitly accept the terms and conditions of the application form (T&C) by his/her selection of the term and conditions acceptance using a checkbox. The T&C will incorporate the following data:
  - a. the attributes to be included in the certificate: first name, middle name (if any), surname, name of the organisation that the user belongs to, user identifier and e-mail address;
  - b. under the conditions and limitations of the applicable data protection law, central banks may require that certificate applicant provides on the T&C the attributes required to distinguish the person from others with the same name (see Section 3.2.3), namely, the number of a national recognized identity document, according to the legislation applicable to the Central Bank or National Competent Authority acting as Registration Authority, or the date and place of birth.
3. The RO4EO must validate the information included in the certificate request against the documentation provided by the certificate applicant, including the T&C. In case the certificate applicant identification has been made by a Trusted Agent, the RO will also validate that a valid Trusted Agent confirms having identified the applicant in accordance to section 3.2 of this CP;
4. The RO4EO, using the ESCB-PKI web interface, will either:
  - a. Start the issuance of the certificate.
  - b. Approve a remote download

In both cases the certificate applicant will be requested to type a password to protect the keystore (file) to be generated with the certificate and its corresponding private key;
5. The RO4EO must securely archive all the documentation during the retention period described in section 5.5.2 of this CP:
  - a. under the conditions and limitations of the applicable data protection law, the Central Bank or National Competent Authority may choose to ask their RO4EO to retain a copy of the official identification document used to validate the certificate applicant's identity or, if this were not legally feasible, a copy of other identification document, preferable with the certificate applicant's photography;

## 4.2 Certificate Application Processing

### 4.2.1 *Performance of identification and authentication procedures*

The validation of certificate requests will require face-to-face authentication of the certificate applicant, in person or using remote means of authentication, or using other alternate means which provide equivalent assurance to physical presence.

A Registration Officer or a Trusted Agent will perform the certificate applicant's identification and authentication and will ensure that all the information provided is correct at the time of registration. 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.

### 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*

Certificate applicants must confirm acceptance of the external users' certificates and of its conditions by his/her selection of the term and conditions acceptance using a checkbox. After the certificate issuance, the subscriber has one week to repudiate his/her new certificates, which will deem the certificates invalid.

### 4.4.2 *Publication of the certificate by the CA*

The ESCB-PKI CA publishes a copy of the external user's certificates: i) in an internal LDAP directory located at the service provider's premises, only available to ESCB/SSM systems on a need-to-know basis, and ii) in the directory of the ESCB Identity and Access Management (IAM) service.

### 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 only to provide the following security services:

- Authentication certificates: authentication against ESCB/SSM applications.
- Encryption certificates: encryption of email messages and files.
- Signature certificates: digital signature of transactions, email messages and files.

### 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 RO4EO 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.

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 established 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 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 external user's certificates: i) in an internal LDAP directory located at the service provider's premises, only available to ESCB/SSM systems on a need-to-know basis, and ii) in the directory of the ESCB Identity and Access Management (IAM) service.

### 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 external users' certificates will be eliminated from the directories in which they are published.

### 4.9.2 *Who can request revocation?*

The CA or any of the RAs may, of 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 contact a RO4EO, identify themselves in person or using remote means of identification, and indicate the reason for the request. The RO4EO shall always process the revocation requests submitted by its assigned 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<sup>7</sup> memory, even when not expired, do not guarantee availability of updated revocation data.

For external users' 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 subscriber.

---

<sup>7</sup>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.



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.

External users' 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 external users' certificates and Registration Officers for External Organisations.

#### **4.9.15 Procedure for requesting certificate suspension**

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

- an authentication certificate;
- an user ID and password for the ESCB Identity and Access Management (IAM) system;
- a suspension code (secret shared with the ESCB-PKI system)

#### **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**

Not applicable.

## **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 external users' 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 external users' certificates issued by the Online CA are generated under the following circumstances, depending on the certificate type:

- **Advanced certificates**, where all the following certificates will be stored in a smartcard or other cryptographic token:
  - Advanced authentication certificate. The corresponding key pair will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent.
  - Advanced signature certificate. The corresponding private key will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent.
  - Advanced signature certificate based on a SSCD. The corresponding private key will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent and to the SSCD (CWA 14169) specification.
  - Advanced encryption certificate without key archive. The key pair will be generated inside the cryptographic token pursuant to the FIPS 140-2 Level 3 or CC EAL4+ specification or equivalent, and no other copy will be archived.
- **Standard certificates**, where the private key will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification.

#### 6.1.2 Delivery of private keys to subscribers

##### 6.1.2.1 Advanced certificates

The private keys will be generated directly by the subscribers in their secure token and, therefore, no delivery is required.

##### 6.1.2.2 Standard certificates

For standard certificates, the delivery of the private key to the certificate subscriber will be performed by means of an authenticated web interface. The certificate subscriber will receive the key pair in a file pursuant to the PKCS#12 specification protected with a password selected by him/her.

#### 6.1.3 Delivery of the public key to the certificate issuer

In case of standard authentication certificates, public keys are generated by the ESCB-PKI Online CA, and therefore delivery to the certificate issuer is not applicable.

In the other cases, the public keys are generated by certificate subscribers on their cryptographic tokens 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 generated by 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 external users' certificate is 2048 bits.

### **6.1.6 Public key generation parameters and quality checks**

Public keys are encoded pursuant to RFC 3280 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 one 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.

### **6.2.3 Escrow of private keys**

Not applicable

### **6.2.4 Private key backup copy**

#### **Advanced certificates**

The certificate subscribers cannot backup their certificates because the keys cannot be exported outside of the cards and these cannot be cloned.

#### **Standard certificates**

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**

#### **Advanced certificates**

The private keys are generated on cryptographic cards, they are not exported under any circumstances, and access to operations with said cards is protected by a PIN code.

#### **Standard certificates**

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

### **6.2.6 Private key transfer into or from a cryptographic module**

#### **Advanced certificates**

Provided that the private key is generated inside the cryptographic token there is no transmission of this key to or from any cryptographic module.

#### **Standard certificates**

No stipulated

### **6.2.7 Private key storage in a cryptographic module**

#### **Advanced certificates**

Private keys are created on the cryptographic token and are stored there

#### **Standard certificates**

Private keys are created in the ESCB-PKI Online CA's cryptographic module, but they are not subsequently saved.

### **6.2.8 Private key activation method**

#### **Advanced certificates**

Private keys are stored in a cryptographic token protected with a PIN code that is required to activate the keys.

#### **Standard certificates**

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

### **6.2.9 Private key deactivation method**

#### **Advanced certificates**

Private keys can be deactivated by removing the card from the reader.

#### **Standard certificates**

No stipulation.

### **6.2.10 Private key destruction method**

#### **Advanced certificates**

Private keys can be destroyed by destroying the cryptographic token.

#### **Standard certificates**

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 external 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 Advanced authentication certificate

Advanced authentication certificate		
Field	Value	Critical
Base Certificate		
Version	3	
Serial Number	Random	
Signature Algorithm	SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA V1.2, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	3 years	
Subject		
C	[Registration Organisation Country]	
O	EUROPEAN SYSTEM OF CENTRAL BANKS	
OU	Organisation within which user is member	
PS	User identifier (UID)	
CN	[AUT:A] Name Middle name Surnames	
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 <sup>8</sup>	1	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
extKeyUsage	clientAuth (1.3.6.1.5.5.7.3.2) smartCardLogon (1.3.6.1.4.1.311.20.2.2)	
Certificate Policies		
Policy Identifier	[OID ESCBPKI].2.3.1	
URL CPS	[CPS-URL]	
Policy Identifier	[OID ESCBPKI].2.1	
URL CPS	[CPS-URL]	
Subject Alternative Names		
rfc822	Subject's Email	
RegisteredID ([OID ESCBPKI].1.1)	Subject's Name	
RegisteredID ([OID ESCBPKI].1.2)	Subject's Middle Name (if any)	
RegisteredID ([OID ESCBPKI].1.3)	Subject's Surname	

<sup>8</sup> This usage is allowed in the scenarios where a digital signature is generated to authenticate the certificate subscriber



RegisteredID ([OID ESCBPKI].1.10)	<i>Subject's First surname</i>	
RegisteredID ([OID ESCBPKI].1.4)	<i>Subject's Secondary surname (if any)</i>	
RegisteredID ([OID ESCBPKI].1.7)	<i>ESCB user identifier (UID)</i>	
Basic Constraints		Yes
CA	FALSE	
Path Length Constraint	<i>Not used</i>	
CRL Distribution Points	URL=http://escbpci/crls/subCAv12.crl URL=http://pki.escb.eu/crls/subCAv12.crl URL=ldap://ldap-pki.escb.eu/CN=ESCB-PKI ONLINE CA V1.2,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint (ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20ONLINE%20CA%20V1.2,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint) URL=http://iam-crl.escb.eu/escb/subCAv12.crl	
Private Extensions		
Authority Information Access		
calssuers	<i>[HTTP URI Root CA]</i>	
calssuers	<i>[HTTP URI Sub CA]</i>	
Ocsp	<i>[HTTP URI OCSP ALIAS]</i> <i>[HTTP URI OCSP]</i> <i>[IAM URI OCSP]</i>	
[ESCB] Extensions		
escbUseCertType	AUTHENTICATION	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.2 *Advanced signature certificate and advanced signature certificate based on a SSCD*

Advanced signature certificate and SSCD signature certificate		
Field	Value	Critical
Base Certificate		
Version	3	
Serial Number	Random	
Signature Algorithm	SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA V1.2, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	3 years	
Subject		
C	[Registration Organisation Country]	
O	EUROPEAN SYSTEM OF CENTRAL BANKS	
OU	Organisation within which user is member	
PS	User identifier (UID)	
CN	[SIG:Q] Name Middle name Surnames OR [SIG:A] Name Middle name Surnames <sup>9</sup>	
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	0	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4)	
Certificate Policies		
Policy Identifier	[OID ESCBPKI].2.3.4 OR [OID ESCBPKI].2.3.5 <sup>10</sup>	
URL CPS	[CPS-URL]	
Policy Identifier	[OID ESCBPKI].2.1	
URL CPS	[CPS-URL]	
Subject Alternative Names		
rfc822	Subject's Email	
RegisteredID ([OID ESCBPKI].1.1)	Subject's Name	
RegisteredID ([OID ESCBPKI].1.2)	Subject's Middle Name (if any)	
RegisteredID ([OID ESCBPKI].1.3)	Subject's Surname	

RegisteredID ([OID ESCBPKI].1.10)	Subject's First surname	
RegisteredID ([OID ESCBPKI].1.4)	Subject's Secondary surname (if any)	
RegisteredID ([OID ESCBPKI].1.7)	ESCB user identifier (UID)	
Basic Constraints		Yes
CA	FALSE	
Path Length Constraint	Not used	
CRL Distribution Points	URL=http://escbpci/crls/subCAv12.crl URL=http://pki.escb.eu/crls/subCAv12.crl URL=ldap://ldap-pki.escb.eu/CN=ESCB-PKI ONLINE CA V1.2,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint (ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20ONLINE%20CA%20V1.2,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint) URL=http://iam-crl.escb.eu/escb/subCAv12.crl	
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		
escbUseCertType	SIGNATURE	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.3 Advanced encryption certificate

Advanced encryption certificate		
Field	Value	Critical
Base Certificate		
Version	3	
Serial Number	Random	
Signature Algorithm	SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA V1.2, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	3 years	
Subject		
C	[Registration Organisation Country]	
O	EUROPEAN SYSTEM OF CENTRAL BANKS	
OU	Organisation within which user is member	
PS	User identifier (UID)	
CN	[ENC:A] Name Middle name Surnames	
Subject Public Key Info		
Algorithm	RSA Encryption	
Minimum Length	2048 bits	

<sup>9</sup> [SIG:Q] in case of advanced signature certificates based on a SSCD

[SIG:A] in case of advanced signature certificates

<sup>10</sup> [OID ESCBPKI].2.3.4 in case of advanced signature certificates based on a SSCD.

[OID ESCBPKI].2.3.5 in case of advanced signature certificates.

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	0	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4)	
Certificate Policies		
Policy Identifier	[OID ESCBPKI].2.3.2	
URL CPS	[CPS-URL]	
Policy Identifier	[OID ESCBPKI].2.1	
URL CPS	[CPS-URL]	
Subject Alternative Names		
rfc822	Subject's Email	
RegisteredID ([OID ESCBPKI].1.1)	Subject's Name	
RegisteredID ([OID ESCBPKI].1.2)	Subject's Middle Name (if any)	
RegisteredID ([OID ESCBPKI].1.3)	Subject's Surname	
RegisteredID ([OID ESCBPKI].1.10)	Subject's First surname	
RegisteredID ([OID ESCBPKI].1.4)	Subject's Secondary surname (if any)	
RegisteredID ([OID ESCBPKI].1.7)	ESCB user identifier (UID)	
Basic Constraints		Yes
CA	FALSE	
Path Length Constraint	Not used	
CRL Distribution Points	URL=http://escbpki/crls/subCAv12.crl URL=http://pki.escb.eu/crls/subCAv12.crl URL=ldap://ldap-pki.escb.eu/CN=ESCB-PKI ONLINE CA V1.2,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint (ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20ONLINE%20CA%20V1.2,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint) URL=http://iam-crl.escb.eu/escb/subCAv12.crl	
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		
escbUseCertType	ENCRYPTION	

escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

## 7.1.2.4 Standard authentication certificate

Standard authentication certificate		
Field	Value	Critical
Base Certificate		
Version	3	
Serial Number	<i>Random</i>	
Signature Algorithm	SHA256-WithRSAEncryption	
Issuer Distinguished Name	CN= ESCB-PKI ONLINE CA V1.2, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU	
Validity	<i>3 years</i>	
Subject		
C	<i>[Registration Organisation Country]</i>	
O	EUROPEAN SYSTEM OF CENTRAL BANKS	
OU	<i>Organisation within which user is member</i>	
PS	<i>User identifier (UID)</i>	
CN	<i>[AUT:S] Name Middle name Surnames</i>	
Subject Public Key Info		
Algorithm	RSA Encryption	
Minimum Length	2048 bits	
Standard Extensions		
Subject Key Identifier	<i>SHA-1 hash over subject public key</i>	
Authority Key Identifier		
KeyIdentifier	<i>SHA-1 hash over CA Issuer public key</i>	
AuthorityCertIssuer	<i>Not used</i>	
AuthorityCertSerialNumber	<i>Not used</i>	
KeyUsage		Yes
Digital Signature <sup>11</sup>	1	
Non Repudiation	0	
Key Encipherment <sup>12</sup>	1	
Data Encipherment <sup>10</sup>	1	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
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	<i>[OID ESCBPKI].2.3.6</i>	
URL CPS	<i>[CPS-URL]</i>	
Policy Identifier	<i>[OID ESCBPKI].2.1</i>	
URL CPS	<i>[CPS-URL]</i>	
Subject Alternative Names		
rfc822	<i>Subject's Email</i>	
RegisteredID ( <i>[OID ESCBPKI].1.1</i> )	<i>Subject's Name</i>	
RegisteredID ( <i>[OID ESCBPKI].1.2</i> )	<i>Subject's Middle Name (if any)</i>	
RegisteredID	<i>Subject's Surname</i>	

<sup>11</sup> This usage is allowed in the scenarios where a digital signature is generated to authenticate the certificate subscriber

<sup>12</sup> keyEncipherment and dataEncipherment are allowed for emailProtection only. The private key is never stored in the Key Archive.

([OID ESCBPKI].1.3) RegisteredID ([OID ESCBPKI].1.10) RegisteredID ([OID ESCBPKI].1.4) RegisteredID ([OID ESCBPKI].1.7)	Subject's First surname  Subject's Secondary surname (if any)  ESCB user identifier (UID)	
Basic Constraints CA Path Length Constraint	FALSE  Not used	Yes
CRL Distribution Points	URL=http://escbpci/crls/subCAv12.crl URL=http://pki.escb.eu/crls/subCAv12.crl URL=ldap://ldap-pki.escb.eu/CN=ESCB-PKI ONLINE CA V1.2,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint (ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20ONLINE%20CA%20V1.2,OU=PKI,OU=ESCB-PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint) URL=http://iam-crl.escb.eu/escb/subCAv12.crl	
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		
escbUseCertType	AUTHENTICATION AND ENCRYPTION	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	



### **7.1.3 Algorithm Object Identifiers (OID)**

Cryptographic algorithm object identifiers (OID):  
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<sup>13</sup>:

- [OID ESCBPKI].2.3.0.X.Y: Certificate policies for the external users' certificates (this document)
- [OID ESCBPKI].2.3.1.X.Y: Certificate Policy of Advanced Authentication certificate for external users
- [OID ESCBPKI].2.3.2.X.Y: Certificate Policy of Advanced Encryption certificate for external users
- [OID ESCBPKI].2.3.4.X.Y: Certificate Policy of Advanced Signature certificate based on a SSCD for external users
- [OID ESCBPKI].2.3.5.X.Y: Certificate Policy of Advanced Signature certificate for external users
- [OID ESCBPKI].2.3.6.X.Y: Certificate Policy of Standard Authentication certificate for external users

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.

---

<sup>13</sup> The OID [OID ESCBPKI].2.3.3 is not used

## 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 external users' 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. Moreover, a copy of the external users' certificates is published in the directory of the ESCB Identity and Access Management (IAM) service.

#### **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.