Annex II

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

BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI SERVICES

OIDS: 0.4.0.127.0.10.1.2.2.0

CERTIFICATE POLICIES FOR THE INTERNAL USERS' CERTIFICATES

VERSION 1.8

22 August 2023

Table of Contents

1 Introduction 9

1.1 Overview 9

1.2 Document Name and Identification 10

1.3 ESCB-PKI Participants 11

1.3.1 The Policy Approval Authority 11
1.3.2 Certification Authority 11
1.3.3 Registration Authorities 11
1.3.4 Validation Authority 12
1.3.5 Key Archive 12
1.3.6 Users 12

1.4 Certificate Usage 13

1.4.1 Appropriate certificate use 13
1.4.2 Certificate Usage Constraints and Restrictions 14

1.5 Policy Approval 14

1.6 Definitions and Acronyms 14

1.6.1 Definitions 14
1.6.2 Acronyms 15

2 Publication and Repository Responsibilities 16

2.1 Repositories 16

2.2 Publication of Certification Data, CPS and CP 16

2.3 Publication Timescale or Frequency 17

2.4 Repository Access Controls 17

3 Identification and Authentication (I&A) 18

3.1 Naming 18

3.1.1 Types of names 18
3.1.2 The need for names to be meaningful 18
3.1.3 Rules for interpreting various name formats 18
3.1.4 Uniqueness of names 18
3.1.5 Name dispute resolution procedures 18
3.1.6 Recognition, authentication, and the role of trademarks 19

3.2 Initial Identity Validation 19

3.2.1 Means of proof of possession of the private key 19
3.2.2 Identity authentication for an entity 19
3.2.3 Identity authentication for an individual 19
3.2.4 Non-verified applicant information 20
3.2.5 Validation of authority 20
3.2.6 Criteria for operating with external CAs 20

3.3 Identification and Authentication for Re-key Requests 20

3.3.1 Identification and authentication requirements for routine re-key 20

3.3.2 Identification and authentication requirements for re-key after certificate revocation 20

4 Certificate Life-Cycle Operational Requirements 21

4.1 Certificate Application 21

4.1.1 Who can submit a certificate application? 21

4.1.2 Enrolment process and applicants' responsibilities 21

4.2 Certificate Application Processing 25

4.2.1 Performance of identification and authentication procedures 25

4.2.2 Approval or rejection of certificate applications 25

4.2.3 Time limit for processing the certificate applications 25

4.3 Certificate Issuance 25

4.3.1 Actions performed by the CA during the issuance of the certificate 25

4.3.2 CA notification to the applicants of certificate issuance 25

4.4 Certificate Acceptance 25

4.4.1 Form of certificate acceptance 25

4.4.2 Publication of the certificate by the CA 25

4.4.3 Notification of certificate issuance by the CA to other Authorities 25

4.5 Key Pair and Certificate Usage 26

4.5.1 Certificate subscribers' use of the private key and certificate 26

4.5.2 Relying parties' use of the public key and the certificate 26

4.6 Certificate Renewal 26

4.7 Certificate Re-key 26

4.7.1 Circumstances for certificate renewal with key changeover 26

4.7.2 Who may request certificate renewal? 26

4.7.3 Procedures for processing certificate renewal requests with key changeover 26

4.7.4 Notification of the new certificate issuance to the certificate subscriber 26

4.7.5 Manner of acceptance of certificates with changed keys 26

4.7.6 Publication of certificates with the new keys by the CA 26

4.7.7 Notification of certificate issuance by the CA to other Authorities 26

4.8 Certificate Modification 27

4.8.1 Circumstances for certificate modification 27

4.9 Certificate Revocation and Suspension 27

4.9.1 Circumstances for revocation 27

4.9.2 Who can request revocation? 27

4.9.3 Procedures for requesting certificate revocation 27

4.9.4 Revocation request grace period 27

4.9.5 Time limit for the CA to process the revocation request 27

4.9.6 Requirements for revocation verification by relying parties 27

4.9.7 CRL issuance frequency 27

4.9.8 Maximum latency between the generation of CRLs and their publication 27

4.9.9 Online certificate revocation status checking availability 28

4.9.10 Online revocation checking requirements 28

4.9.11 Other forms of revocation alerts available 28

4.9.12 Special requirements for the revocation of compromised keys 28

4.9.13 Causes for suspension 28

4.9.14 Who can request the suspension? 28
4.9.15 Procedure for requesting certificate suspension 28
4.9.16 Suspension period limits 28
4.10 Certificate Status Services 28
4.11 End of Subscription 28
4.12 Key Escrow and Recovery 28
4.12.1 Key Archive and recovery practices and policies 28
4.12.2 Session key protection and recovery policies and practices 29
5 Facility, Management, and Operational Controls 30
5.1 Physical Security Controls 30
5.2 Procedural Controls 30
5.3 Personnel Controls 30
5.4 Audit Logging Procedures 30
5.5 Records Archival 30
5.5.1 Types of records archived 30
5.5.2 Archive retention period 30
5.5.3 Archive protection 30
5.5.4 Archive backup procedures 30
5.5.5 Requirements for time-stamping records 30
5.5.6 Audit data archive system (internal vs. external) 30
5.5.7 Procedures to obtain and verify archived information 30
5.6 Key Changeover 30
5.7 Compromise and Disaster Recovery 30
5.8 CA or RA Termination 30
6 Technical Security Controls 31
6.1 Key Pair Generation and Installation 31
6.1.1 Key pair generation 31
6.1.2 Delivery of private keys to certificate subscribers 32
6.1.3 Delivery of the public key to the certificate issuer 33
6.1.4 Delivery of the CA's public key to relying parties 33
6.1.5 Key sizes 33
6.1.6 Public key generation parameters and quality checks 33
6.1.7 Key usage purposes (KeyUsage field in X.509 v3) 33
6.2 Private Key Protection and Cryptographic Module Engineering Controls 34
6.2.1 Cryptographic module standards 34
6.2.2 Private key multi-person (k out of n) control 34
6.2.3 Escrow of private keys 34
6.2.4 Private key backup copy 34
6.2.5 Private key archive 34
6.2.6 Private key transfer into or from a cryptographic module 34
6.2.7 Private key storage in a cryptographic module 35
6.2.8 Private key activation method 35

6.2.9 Private key deactivation method 35
6.2.10 Private key destruction method 35
6.2.11 Cryptographic module classification 35
6.3 Other Aspects of Key Pair Management 35
6.3.1 Public key archive 35
6.3.2 Operational period of certificates and usage periods for key pairs 35
6.4 Activation Data 35
6.5 Computer Security Controls 35
6.6 Life Cycle Security Controls 35
6.7 Network Security Controls 36
6.8 Timestamping 36
7 Certificate, CRL, and OCSP Profiles 37
7.1 Certificate Profile 37
7.1.1 Version number 37
7.1.2 Certificate extensions 37
7.1.3 Algorithm Object Identifiers (OID) 58
7.1.4 Name formats 58
7.1.5 Name constraints 58
7.1.6 Certificate Policy Object Identifiers (OID) 58
7.1.7 Use of the "PolicyConstraints" extension 58
7.1.8 Syntax and semantics of the “PolicyQualifier” extension 58
7.1.9 Processing semantics for the critical “CertificatePolicy” extension 58
7.2 CRL Profile 58
7.3 OCSP Profile 58
8 Compliance Audit and Other Assessment 59
9 Other Business and Legal Matters 60
9.1 Fees 60
9.1.1 Certificate issuance or renewal fees 60
9.1.2 Certificate access fees 60
9.1.3 Revocation or status information fees 60
9.1.4 Fees for other services, such as policy information 60
9.1.5 Refund policy 60
9.2 Financial Responsibility 60
9.3 Confidentiality of Business Information 60
9.3.1 Scope of confidential information 60
9.3.2 Non-confidential information 60
9.3.3 Duty to maintain professional secrecy 60
9.4 Privacy of Personal Information 60
9.4.1 Personal data protection policy 60
9.4.2 Information considered private 60
9.4.3 Information not classified as private 60
9.4.4 Responsibility to protect personal data 60

9.4.5 Notification of and consent to the use of personal data 60
9.4.6 Disclosure within legal proceedings 61
9.4.7 Other circumstances in which data may be made public 61
9.5 Intellectual Property Rights 61
9.6 Representations and Warranties 61
9.7 Disclaimers of Warranties 61
9.8 Limitations of Liability 61
9.9 Indemnities 61
9.10 Term and Termination 61
9.10.1 Term 61
9.10.2 CP substitution and termination 61
9.10.3 Consequences of termination 61
9.11 Individual notices and communications with participants 61
9.12 Amendments 61
9.13 Dispute Resolution Procedures 61
9.14 Governing Law 61
9.15 Compliance with Applicable Law 61
9.16 Miscellaneous Provisions 62
9.16.1 Entire agreement clause 62
9.16.2 Independence 62
9.16.3 Resolution through the courts 62
9.17 Other Provisions 62

Control Sheet

	Title	Certification Policy for the internal users' certificates
	Author	ESCB-PKI Service Provider
	Version	1.8
	Date	22.08.2023

RELEASE NOTES

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column "Release number" refer to the current version of the document.

Release number	Status	Date	Change Reason
0.1	Draft	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	10.12.2013	New certificate types for mobile devices, shared mailbox, administrator and provisional
1.3	Final	11.05.2015	Hashing algorithm update
1.4	Final	29.11.2018	• Key usage KeyEncipherment added to authentication certificate profile. • anyExtendedKeyUsage extended key usage removed in all certificate profiles. • Modifications to comply with Regulation Nº 910/2014: o New extensions escbIssuerName and escbIssuerVAT are included to comply with Regulation (EU) No 910/2014. • Modifications to comply with ETSI EN 319 401: o Added a reference to the ESCB/SSM Information Systems Risk Management methodology o Added a reference to the ESCB/SSM Information Systems Security Policy

			○ Added a statement to clarify that ESCB-PKI services shall be provided in accordance with the principle of non-discrimination ○ Added a statement to clarify that ESCB-PKI services shall be provided in accordance with the principle of non-discrimination ○ Added various statements to clarify relations with potential contractors ○ Updated chapters 1.3 and 5.2.1 to better clarify the ESCB-PKI role allocation procedures. ○ Updated the CA termination plan ○ Updated the Life-Cycle Security Controls ○ Other minor updates
1.5	Final	26.08.2019	Update after PKI-AB revision
1.6	Final	09.10.2020	• A new type of participant organisation, namely *Cooperating Authorities* has been included. One of the consequences of this has been that this document has been renamed, from *Certification Policy for the ESCB/ SSM users' certificates* to *Certification Policy for the internal users' certificates*. • References to SHA1 certificates has been removed, as these certificates are no longer valid. • CA certificates hierarchy description has been updated to include potential new CA in the future. • Acceptance of Term & Conditions by subscribers is no longer required to be made by handwritten signature in paper, but with a combination of the two following factors: ○ The subscriber will express their acceptance in the Registration Authority web application, using a designated checkbox. ○ 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. • Subscriber identification may be made by remote means. • Updated references to the 2018 Spanish Data Protection Law.
1.7	Final	10.02.2021	• Update to Law 6/2020, of November 11, Regulating Certain Aspects of Trusted Electronic Services. This new Law repeals Law 59/2003 on Electronic Signatures.

1.8	Final	22.08.2023	• Update for the release of the new Certification Authority: Online CA V1.2 • Update 7.1.2 Certificate extensions with new OID and update of keyUsages.

1 Introduction

1.1 Overview

This document sets out the Certificate Policy (CP) governing the personal certificates issued to internal users (i.e. users that belong to ESCB Central Banks, SSM National Competent Authorities or Cooperating 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.

[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).

Likewise, the following relevant legal framework has been considered:

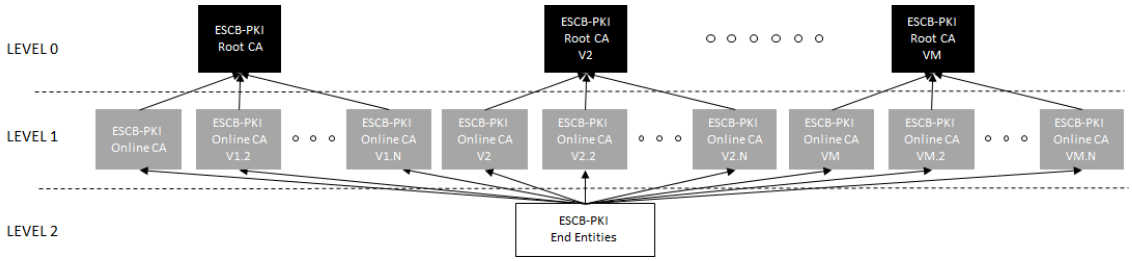
- Decision ECB/2015/47[2];
- Regulation (EU) No 910/2014 of the European Parliament and of the Council[3]; Spanish Law 6/2020 of November 11, Regulating Certain Aspects of Trusted Electronic Services (Spanish Official Journal, 11 November).[4]
- Regulation (EU) 2016/679 of the European Parliament and of the Council[5]; 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 internal users' 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

Document name	Certificate Policy (CP) for the internal users' certificates
Document version	1.8
Document status	Final
Date of issue	22.08.2023
OID (Object Identifiers)	0.4.0.127.0.10.1.2.2.0: Certificate policies for the internal users' certificates (this document)

[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) 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).

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

[5] 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.

	0.4.0.127.0.10.1.2.2.1: Certificate Policy of Advanced Authentication certificate for internal users 0.4.0.127.0.10.1.2.2.2: Certificate Policy of Archived Encryption certificate for internal users 0.4.0.127.0.10.1.2.2.3: Certificate Policy of Non-Archived Encryption certificate for internal users 0.4.0.127.0.10.1.2.2.4: Certificate Policy of Advanced Signature certificate based on a SSCD for internal users 0.4.0.127.0.10.1.2.2.5: Certificate Policy of Advanced Signature certificate for internal users 0.4.0.127.0.10.1.2.2.6: Certificate Policy of Standard Authentication certificate for internal users 0.4.0.127.0.10.1.2.2.7: Certificate Policy of Mobile Device certificate for internal users 0.4.0.127.0.10.1.2.2.8: Certificate Policy of Secure E-mail Gateway certificate for internal users 0.4.0.127.0.10.1.2.2.9: Certificate Policy of Provisional certificate for internal users 0.4.0.127.0.10.1.2.2.10: Certificate Policy of Administrator certificate for internal users 0.4.0.127.0.10.1.2.2.11: Certificate Policy of Shared Mailbox certificate for internal users 0.4.0.127.0.10.1.2.2.12: Certificate Policy of Archived Encryption certificate recoverable in software for internal users
CPS location	https://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 roles available to manage internal users' certificates are the following:

- **Registration Officers**
- **Trusted Agents**
- **Shared Mailbox Administrator**

The following list of roles are also available, but as is mentioned in the CPS, only to the Eurosystem Central Banks and the ECB, as well as by the Central Banks outside the Euro area and the SSM National Competent Authorities:

- **Registration Officers for External Organisations**
- **Key Recovery Officers**

1.3.4 Validation Authority

As specified in the ESCB-PKI CPS.

1.3.5 Key Archive

The Key Archive service, defined in the ESCB-PKI CPS, is only applicable for the archived encryption certificate, as well as the related encryption private key. Thus, no other private keys will be archived.

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 internal users's 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 ESCB Central Banks, SSM National Competent Authorities (internal users) and Cooperating Authorities It will be up to each CB or NCA to decide the legal binding with the group of people that will be certificate subscribers of internal users's certificates (i.e. just internal employees, subcontractors, etc.)
Online CA V1.2	Users from ESCB Central Banks, SSM National Competent Authorities (internal users) and Cooperating Authorities It will be up to each CB or NCA to decide the legal binding with the group of people that will be certificate subscribers of internal users's certificates (i.e. just internal employees, subcontractors, etc.)

Depending on the type of organisations they belong to, certificate subscribers will be able to receive any of the following certificate packages:

- **Advanced certificate package**, 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.
- One of the following encryption certificates: i) advanced encryption certificate without key archive, ii) advanced encryption certificate with archived private key only recoverable in a token, or iii) standard encryption certificate with archived private key recoverable in software format or in a token. In the first case, the key pair will be generated inside the cryptographic token and no other copy will be archived. In the second and third cases, the key pair will be generated by the ESCB-PKI Subordinate CA and afterwards stored in the cryptographic device and another copy in the Key Archive service. The archived copies of the private key will be recoverable only in a token (second case) or in software format or in a token (third case)

- **Standard certificates**, where the private key will be generated by the CA and stored in a software device. The standard certificate will be mainly valid for authentication, although signature and encryption is also allowed.
- **Mobile device certificates**, where the private key will be generated by the CA and stored in a software keystore with the aim of being imported into a mobile device. This certificate is mainly valid for authentication, although signature is also allowed.
- **Secure e-mail gateway certificates**, where the private key will be generated by the CA and stored in a software keystore with the aim of being imported into a secure e-mail gateway. This certificate is valid for e-mail signing and encryption.
- **Administrator certificates**, where the private key will be generated and stored in a smartcard or other cryptographic token (e.g. USB device). This certificate is oriented for those subscribers that have got an administrator account to access IT or business services with special privileges. The certificate is mainly valid for authentication, although signature is also allowed.
- **Provisional certificates**, where the private key will be generated and stored in a smartcard or other cryptographic token (e.g. USB device). This certificate is oriented for those subscribers of advanced or administrator certificates that have forgotten their smartcard and need to access IT or business services that require two-factor authentication. The certificate has a limited lifetime (less or equal to 31 days) and is mainly valid for authentication, although signature is also allowed.
- **Shared mailbox certificates**, where the private key will be generated by the CA and stored in a software keystore so that each person that needs to access the shared mailbox has a copy of the keys. This certificate is oriented to protecting information exchanged by a shared mailbox. The certificate is mainly valid for e-mail signing and encryption, although authentication is also allowed.

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 any of the ESCB Central Banks, National Competent Authorities and Cooperating Authorities.

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
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.

Moreover, a copy of the internal 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
- [ENC:K] → Advanced Encryption certificate with private key archive only recoverable in a token
- [ENC:S] → Encryption certificate with private key archive recoverable in software
- [MOB:S] → Mobile Device certificate
- [EGW:S] → Secure E-mail Gateway certificate
- [TMP:A] → Provisional certificate
- [ADM:A] → Administrator certificate
- [SHM:S] → Shared mailbox certificate

This prefix will be followed by the name, middle name and surnames of the certificate subscribers but in the case of shared mailbox certificates where it will be followed by the shared mailbox's display name.

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 Central Bank, National Competent Authority or Cooperating 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. 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 CA, 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.
- [ENC:K] → advanced encryption with key archive: Advanced Encryption certificate key pair will be created by the ESCB-PKI Online CA so this section does not apply.
- [ENC:S] → encryption with key archive recoverable in software: the key pair will be created by the ESCB-PKI Online CA so this section does not apply.
- [MOB:S] → mobile device certificate: the key pair will be created by the ESCB-PKI Online CA so this section does not apply.
- [EGW:S] → secure e-mail gateway: the key pair will be created by the ESCB-PKI Online CA so this section does not apply.
- [TMP:A] → provisional certificate: 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.
- [ADM:A] → administrator certificate: 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.
- [SHM:S] → shared mailbox certificate: the key pair will be created by the ESCB-PKI Online CA so this section does not apply.

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

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.

If the case of shared mailbox certificates the certificate applicant will be the person responsible for the shared mailbox.

If the certificate applicant has already been identified by the Central Bank, National Competent Authority or Cooperating Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the employee identification card is accepted as sufficient to identify the certificate applicant.

The validation of the identity will be performed by a Registration Officer or by a Trusted Agent.

Validation of the organisation

To prove his relation with the organisation acting as Registration Authority the certificate applicant must present his employee identification card.

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 internal users's 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 CP 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 internal users will be managed by a Registration Officer (RO). ROs will be able to request certificate types mentioned in section 1.3.6.

In case of shared mailbox certificates the attributes required to identify the shared mailbox will be entered by a Shared Mailbox Administrator (SMA).

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 internal users' certificates (e.g. if the certificate applicant does not provide the RO with the documents necessary for his/her identification).

4.1.2 Enrolment process and applicants' responsibilities

Depending on the type of organisation the subscriber belongs to, some of the following certificate profiles could not be available.

Advanced certificate package (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 internal user can be initiated:
    a. either using ESCB Identity Access Management (IAM) interfaces,
    b. or using ESCB-PKI web interface (this option may not be available depending on the organisation acting as Registration Authority);
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 Registration Authority, user identifier and e-mail address;
    b. 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, National Competent Authority or Cooperating Authority acting as Registration Authority, or the date and place of birth, or, if the certificate applicant has already been identified by the Central Bank, National Competent Authority or Cooperating Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the number of the employee identification card or the employee number if this is printed on the employee identification card;
    c. the serial number of the certificate applicant's cryptographic token.
3. The RO must validate the information included in the certificate request against the documentation provided by the certificate applicant (see Section 3.2.3) 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 RO, using the ESCB-PKI web interface, will either:
    a. Start the issuance of the certificates
    b. Approve a remote download

   In both cases the certificate applicant must hold his/her cryptographic token and, when requested, must insert it and type his/her personal PIN to generate the keys and store the certificates
5. The RO must securely archive the following documentation during the retention period described in Section 5.5.2 of this CP:
    a. if the certificate applicant has not already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, a copy of the 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, under the conditions and limitations of the applicable law

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 a internal user can be initiated:
    a. either using ESCB Identity Access Management (IAM) interfaces,
    b. or using ESCB-PKI web interface (this option may not be available depending on the organisation acting as Registration Authority);
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 Registration Authority, user identifier and e-mail address;
    b. 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, National Competent Authority or Cooperating Authority acting as Registration Authority, or the date and place of birth, or, if the certificate applicant has already been identified by the Central Bank, National Competent Authority or Cooperating Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the number of the employee identification card or the employee number if this is printed on the employee identification card.
3. The RO must validate the information included in the certificate request against the documentation provided by the certificate applicant (see Section 3.2.3) 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 RO, 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 RO must securely archive all the following documentation during the retention period described in Section 5.5.2 of this CP:

a. if the certificate applicant has not already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, a copy of the 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, under the conditions and limitations of the applicable law

Mobile device certificates (software-based)

The same applies as in case of standard certificates.

Secure e-mail gateway certificates (software-based)

The same applies as in the case of standard certificates.

Administrator certificates (token-based)

The process will be similar to the process for advanced certificates. The only difference is that only one certificate, valid for authentication and signature, will be generated instead of three certificates.

Provisional certificates (token-based)

This process is carried out to obtain a certificate stored in a cryptographic token. This certificate will be only used in case that the subscriber of an advanced certificate package or an administrator certificate has forgotten his token. The provisional certificate lifetime will be less or equal to 31 days.

The procedure is as follows:

1. Only requests for provisional certificates coming from users that have already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity and that are subscribers of advanced (token-based) or administrator certificates will be accepted;
2. Provisional certificate requests for an internal user can be initiated:
    a. either using ESCB Identity Access Management (IAM) interfaces,
    b. or using ESCB-PKI web interface (this option may not be available depending on the organisation acting as Registration Authority);
3. 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 central bank or national competent authority, user identifier and e-mail address;
    b. 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, or, if the certificate applicant has already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the number of the employee identification card or the employee number if this is printed on the employee identification card;
    c. the serial number of the provisional cryptographic token where the subscriber will download the provisional certificate;
4. The RO must validate the information included in the certificate request against the documentation provided by the certificate applicant (see Section 3.2.3) including the T&C.

Alternatively, in order to deal with the situation in which the user has not got any identification document (e.g. he has forgotten his wallet) the RO will be allowed to identify the user by means of a local directory with photograph;

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;

5. The RO, using the ESCB-PKI web interface, will decide how long the certificate will be valid (less or equal than 31 days). Afterwards he will either:
    a. Start the issuance of the certificate
    b. Approve a remote download

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

Shared mailbox certificates (software-based)

This process is carried out to obtain a certificate for a mailbox shared by several users. In this case there must be a natural person responsible for the certificate and carrying out the role of the applicant.

The procedure is as follows:

1. Shared mailbox certificate requests for an internal user can be initiated:
    a. either using ESCB Identity Access Management (IAM) interfaces,
    b. or using ESCB-PKI web interface (this option may not be available depending on the organisation acting as Registration Authority);
2. A Shared Mailbox Administrator (SMA) will participate in the process to enter or complement the attributes of the shared mailbox or the person that is acting as the certificate subscriber;
3. The certificate applicant must explicitly accept the terms and conditions of the application form (T&C) his/her selection of the term and conditions acceptance using a checkbox. The T&C will incorporate the following data:
    a. the shared mailbox attributes to be included in the certificate: display name, name of the Registration Authority, user identifier and e-mail address;
    b. the attributes to identify the certificate subscriber, that will not be included in the certificate: first name, middle name (if any), surname, e-mail address and 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, National Competent Authority or Cooperating Authority acting as Registration Authority, or the date and place of birth, or, if the certificate applicant has already been identified by the Central Bank, National Competent Authority or Cooperating Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, the number of the employee identification card or the employee number if this is printed on the employee identification card.
4. The RO must validate the information included in the certificate request against the documentation provided by the certificate applicant (see Section 3.2.3) 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;
5. The RO, using the ESCB-PKI web interface, will approve the certificate download;
6. The SMA, using the ESCB-PKI web interface, will download the certificate. For this, it will be required to type a password to protect the keystore (file) that will be generated with the certificate and its corresponding private key;

7. The SMA will deliver the certificate file to the certificate subscriber by means of local procedures (e.g. by means of a USB stick);
8. The RO must securely archive all the following documentation during the retention period described in Section 5.5.2 of this CP:
    a. if the certificate applicant has not already been identified by the Central Bank or National Competent Authority acting as Registration Authority through a face-to-face identification process and a proof of identity, a copy of the 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, under the conditions and limitations of the applicable law.

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 internal 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 internal 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 of the subscriber.
- 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.

Provisional certificates cannot be renewed. Every time that a user requires a provisional certificate a new one will be generated.

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 RO 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 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 internal 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 internal 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, 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 contact a RO, identify themselves in person or using remote means of identification, and indicate 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[6] memory, even when not expired, do not guarantee availability of updated revocation data.

For internal 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.

[6] 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.

4.9.9 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.

Internal 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 internal users' certificates and Registration Officers

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 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

4.12.1 Key Archive and recovery practices and policies

The Key Recovery service for ESCB-PKI encryption certificates (and the associated private key) will be available only to those CBs or NCAs that demand this service. For these organisations, the CA will send a copy of any user encryption key pair to the Key Archive, as to allow key recovery in case of cryptographic token loss or replacement.

4.12.1.1 Key recovery with the participation of the certificate subscriber

Certificate subscribers will be able to download a copy of the key encryption pair contained in previous cryptographic tokens.

The procedure will be the following:

- The certificate subscriber accesses a Web interface using his authentication certificate;
- The certificate subscriber downloads and installs the encryption his pair in the cryptographic token. In case that the encryption certificate is enabled for recovery in software format (name starting with [ENC:S]), the certificate subscriber will able to choose between installing the recovered keys in a cryptographic token, or downloading a software keystore protected with a password previously entered by the subscriber.

4.12.1.2 Key recovery without the participation of the certificate subscriber

Key Recovery Officers (KROs) participate during the recovery of encryption key pairs from the Key Archive when the owner of the key pair is not available. There shall be at least two KROs at each organisation as to carry away the process of "Key recovery without the participation of the certificate subscriber". The KROs shall assume one or more of the following interim roles (see incompatibility matrix) for every key recovery operation:

- The Requestor KRO will request the key recovery of an encryption key pair that belongs to a particular certificate subscriber from that organisation (i.e. he will trigger "Key recovery without the participation of the certificate subscriber" process).
- The Approver KROs are in charge of endorsing the recovery Request placed by the Requestor KRO.
- The Operator KRO recovers the key pair and stores it in a blank cryptographic token.

Key recovery process

Recovery of encryption certificates requested by someone else than the certificate subscriber will involve the participation of, at least, K different Key Recovery Officers of the total N KROs available at the certificate subscriber's organisation.

The precise values for K and N will be determined individually at each organisation. Four-eye principle will always be complied with, i.e. K will always be equal or greater than 2.

The procedure will be the following:

- One of the N KROs available at the organisation, acting as a Requestor KRO, requests the key recovery of an encryption key pair that belongs to a particular certificate subscriber from that CB;
- The ESCB-PKI randomly generates a password and uses it to encrypt the key pair;
- A secret-sharing scheme is applied for the password: it is split into N pieces in such a way that any K pieces are required to reconstruct the password;
- The certificate subscriber receives an informative e-mail;
- All the N KROs from the organisation receive an e-mail with one of the N pieces of the shared secret. It is required the participation of at least K KROs to get access to the encryption certificate. These K KROs will act as Approver KROs;
- One of the N KROs, acting as the Operator KRO (cannot be the same that the Requestor KRO) accesses a Web interface available through Corenet;
- The Operator KRO introduces his/her piece of the shared secret and other K-1 Approver KROs introduce theirs;
- The Operator KRO recovers the key pair and stores it in a blank cryptographic token.

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

- **Advanced certificate package**, 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.
    - Advanced encryption certificate with key archive recoverable only in a token. The key pair will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification. Once generated, the key pair will be stored in the Key Archive service that will use a cryptographic module with the same requirements, and another copy will be stored in the cryptographic token pursuant to the CC EAL 4+ specification or equivalent.
    - Standard encryption certificate with key archive recoverable in software format or in a token. The key pair will be generated by the ESCB-PKI Online CA, using a cryptographic module pursuant to the FIPS 140-2 level 3 specification. Once generated, the key pair will be stored in the Key Archive service that will use a cryptographic module with the same requirements, and another copy will be stored in the cryptographic token pursuant to the CC EAL 4+ specification or equivalent.
- **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, and stored in a file pursuant to the PKCS#12 specification.
- **Mobile devices 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, and stored in a file pursuant to the PKCS#12 specification.
- **Secure e-mail gateway 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, and stored in a file pursuant to the PKCS#12 specification.
- **Administrator certificates**, where 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.

- **Provisional certificates**, where 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.
- **Shared mailbox 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, and stored in a file pursuant to the PKCS#12 specification.

6.1.2 Delivery of private keys to certificate subscribers

6.1.2.1 Advanced certificate package

With the exception of the advanced encryption certificates with key archive and the encryption certificates with archived keys recoverable in software format, the private keys will be generated directly by the certificate subscribers in their secure token and, therefore, no delivery is required.

Delivery of the private key for advanced encryption certificates with key archive:

- As mentioned in section 6.1.1, the private keys are generated by the Online CA in a file pursuant to the PKCS#12 specification.
- The PKCS#12 file will be delivered to:
    - The certificate subscriber, in the case of:
        - The habitual certificate package delivery process, next to the authentication and signature certificates. The RA application will force to download the PKCS#12 file in a cryptographic token.
        - In case that the certificate subscriber requires to retrieve a copy of the encryption key pair from the KA (e.g. in case of substitution of the cryptographic token). The certificate subscriber will use a specific authenticated web interface that will force to download the PKCS#12 file in a cryptographic token.
    - The required number of Key Recovery Officers nominated by the CB. This will be case when the certificate subscriber is not available. Four-eye principle will be required to recover a key pair in this case. KROs will use a specific authenticated web interface that will force to download the PKCS#12 file in a cryptographic token.
- To guarantee delivery security, the availability of the generation and subsequent downloading of the certificate shall be notified by e-mail to the certificate subscriber.

Delivery of the private key for encryption certificates with archived keys recoverable in software format:

- As mentioned in section 6.1.1, the private keys are generated by the Online CA in a file pursuant to the PKCS#12 specification.
- The PKCS#12 file will be delivered to:
    - The certificate subscriber, in the case of:
        - The habitual certificate package delivery process, next to the authentication and signature certificates. The RA application will force to download the PKCS#12 file in a cryptographic token.
        - In case that the certificate subscriber requires to retrieve a copy of the encryption key pair from the KA (e.g. in case of substitution of the cryptographic token). The certificate subscriber will use a specific authenticated web interface that will allow downloading the PKCS#12 file in a software keystore protected with a password selected by the subscriber, or in a cryptographic token.
    - The required number of Key Recovery Officers nominated by the CB. This will be case when the certificate subscriber is not available. Four-eye principle will be required to

recover a key pair in this case. KROs will use a specific authenticated web interface that will force to download the PKCS#12 file in a cryptographic token.

- To guarantee delivery security, the availability of the generation and subsequent downloading of the certificate shall be notified by e-mail to the certificate subscriber.

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.

6.1.2.3 Mobile device certificates

For mobile device 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.

6.1.2.4 Secure e-mail gateway certificates

For secure e-mail gateway 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.

6.1.2.5 Administrator certificates

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

6.1.2.6 Provisional certificates

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

6.1.2.7 Shared mailbox certificates

For shared mailbox certificates, the delivery of the private key to the shared mailbox administrator will be performed by means of an authenticated web interface. The shared mailbox administrator 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 advanced encryption certificates with key archive and 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 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 internal 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 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

Only advanced encryption certificates with key archive are escrowed. See sections 4.12.1 and 6.1.1.

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. When key archive service is requested by the CB the certificate subscriber belongs to, the encryption private keys are subject to key archive as described in section *4.12.1.*

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 of the authentication and signature certificates 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.

The private keys of the encryption certificate are stored on cryptographic cards held by their certificate subscribers, they are not exported under any circumstances, and access to operations with said cards is protected by a PIN. When key archive service is requested by the CB the certificate subscriber belongs to, the encryption private keys are subject to key archive as described in section *4.12.1 Key Archive and recovery practices and policies.*

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 of authentication, signature and encryption certificates without key archive are created on the cryptographic token and are stored there. Private keys of encryption certificates with key archive are generated by the CA's cryptographic module and afterwards stored in the KA's cryptographic module and in cryptographic token.

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 internal 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 O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Internal organisation within which user is member* *User identifier (UID)* [AUT:A] *Name Middle name Surnames*	
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[7] Non Repudiation Key Encipherment Data Encipherment Key Agreement Key Certificate Signature CRL Signature	 1 0 0 0 1 0 0	Yes
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 URL CPS Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.1 *[CPS-URL]* *[OID ESCBPKI].2.1* *[CPS-URL]*	
Subject Alternative Names RegisteredID UPN (1.3.6.1.4.1.311.20.2.3) rfc822 RegisteredID (*[OID ESCBPKI]*.1.1.1) RegisteredID (*[OID ESCBPKI]*.1.1.2) RegisteredID (*[OID ESCBPKI]*.1.1.3)	 *User Principal Name (if available)* *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname*	

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

RegisteredID (*[OID ESCBPKI]*.1.1.10) RegisteredID (*[OID ESCBPKI]*.1.1.4) RegisteredID (*[OID ESCBPKI]*.1.1.7)	*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://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 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	
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 advanced signature certificate based on a SSCD		
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 O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Internal organisation within which user is member* *User identifier (UID)* [SIG:Q] *Name Middle name Surnames* *OR* [SIG:A] *Name Middle name Surnames*[8]	
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	 0 1 0 0 0 0 0	Yes
extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4)	
Certificate Policies Policy Identifier URL CPS Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.4 OR *[OID ESCBPKI]*.2.2.5[9] *[CPS-URL]* *[OID ESCBPKI].2.1* *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1.1) RegisteredID (*[OID ESCBPKI]*.1.1.2) RegisteredID (*[OID ESCBPKI]*.1.1.3) RegisteredID (*[OID ESCBPKI]*.1.1.10)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname*	

RegisteredID (*[OID ESCBPKI]*.1.1.4) RegisteredID (*[OID ESCBPKI]*.1.1.7)	*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://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 caIssuers caIssuers Ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbUseCertType	SIGNATURE	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

[8] *[SIG:Q]* in case of qualified signature certificates based on a SSCD. *[SIG:A]* in case of advanced signature certificates.

[9] *[OID ESCBPKI]*.2.2.4 in case of advanced signature certificates based on a SSCD. *[OID ESCBPKI]*.2.2.5 in case of advanced signature certificates.

7.1.2.3 Standard or Advanced encryption certificate with and without key archive

Standard encryption certificate with and without key archive		
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 O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Internal organisation within which user is member* *User identifier (UID)* [ENC:K] *Name Middle name Surnames* [ENC:A] *Name Middle name Surnames* [ENC:S] *Name Middle name Surnames* [10]	
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	 0 0 1 1 0 0 0	Yes
extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4)	
Certificate Policies Policy Identifier URL CPS Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.2 *[OID ESCBPKI]*.2.2.3 *[OID ESCBPKI]*.2.2.12 [11] *[CPS-URL]* *[OID ESCBPKI].2.1* *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1.1) RegisteredID (*[OID ESCBPKI]*.1.1.2) RegisteredID (*[OID ESCBPKI]*.1.1.3) RegisteredID (*[OID ESCBPKI]*.1.1.10)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname*	

RegisteredID (*[OID ESCBPKI]*.1.1.4) RegisteredID (*[OID ESCBPKI]*.1.1.7)	*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://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 caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]*	
[ESCB] Extensions		
escbUseCertType	ENCRYPTION	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

[10] *[ENC:K]* in case of advanced encryption certificates with key archive recoverable only in a token
[ENC:A] in case of advanced encryption certificates without key archive
[ENC:S] in case of encryption certificates with key archive recoverable in software
[11] *[OID ESCBPKI]*.2.2.2 in case of advanced encryption certificates with key archive recoverable only in a token
[OID ESCBPKI].2.2.3 in case of advanced encryption certificates without key archive
[OID ESCBPKI].2.2.12 in case of encryption certificates with key archive recoverable in software

7.1.2.4 Standard authentication certificate

Standard 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 O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Internal organisation within which user is member* *User identifier (UID)* [AUT:S] *Name Middle name Surnames*	
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[12] Non Repudiation Key Encipherment[13] Data Encipherment[12] 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 Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.6 *[CPS-URL]* *[OID ESCBPKI].2.1* *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname*	

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

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

([*OID ESCBPKI*].1.10)		
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		
caIssuers	*[HTTP URI Root CA]*	
caIssuers	*[HTTP URI Sub CA]*	
ocsp	*[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	AUTHENTICATION	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.5 Mobile device certificate

Mobile device 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 O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Internal organisation within which user is member* *User identifier (UID)* [MOB:S] *Name Middle name Surnames*	
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 0 0 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 Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.7 *[CPS-URL]* *[OID ESCBPKI].2.1* *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4)	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)*	

RegisteredID (*[OID ESCBPKI]*.1.7)	*ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
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 caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	MOBILE DEVICE	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.6 Secure e-mail gateway certificate

Secure e-mail gateway 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 O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Internal organisation within which user is member* *User identifier (UID)* [EGW:S] *Name Middle name Surnames*	
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 1 0 0 0	Yes
extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4)	
Certificate Policies Policy Identifier URL CPS Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.8 *[CPS-URL]* *[OID ESCBPKI].2.1* *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID (*[OID ESCBPKI]*.1.4) RegisteredID	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)* *ESCB user identifier (UID)*	

(*[OID ESCBPKI]*.1.7)		
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
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 caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	SECURE EMAIL GATEWAY	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.7 *Provisional certificate*

Provisional 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	*Maximum 1 month*	
Subject C O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Internal organisation within which user is member* *User identifier (UID)* [TMP:A] *Name Middle name Surnames*	
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 0 0 1 0 0	Yes
extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4) 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 URL CPS Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.9 *[CPS-URL]* *[OID ESCBPKI].2.1* *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID (*[OID ESCBPKI]*.1.10) RegisteredID	 *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname* *Subject's Secondary surname (if any)*	

([*OID ESCBPKI*].1.4) RegisteredID ([*OID ESCBPKI*].1.7)	 *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
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 caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	PROVISIONAL	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.8 Administrator certificate

Administrator 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 O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Internal organisation within which user is member* *User identifier (UID)* [ADM:A] *Name Middle name Surnames*	
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 0 0 1 0 0	Yes
extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4) 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 URL CPS Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.10 *[CPS-URL]* *[OID ESCBPKI].2.1* *[CPS-URL]*	
Subject Alternative Names RegisteredID UPN (1.3.6.1.4.1.311.20.2.3) rfc822 RegisteredID (*[OID ESCBPKI]*.1.1) RegisteredID (*[OID ESCBPKI]*.1.2) RegisteredID (*[OID ESCBPKI]*.1.3) RegisteredID	 *User Principal Name (if available)* *Subject's Email* *Subject's Name* *Subject's Middle Name (if any)* *Subject's Surname* *Subject's First surname*	

([*OID ESCBPKI*].1.10)		
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		
caIssuers	*[HTTP URI Root CA]*	
caIssuers	*[HTTP URI Sub CA]*	
ocsp	*[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	ADMINISTRATOR	
escbIssuerName	BANCO DE ESPAÑA	
escbIssuerVAT	VATES-Q2802472G	

7.1.2.9 Shared mailbox certificate

Shared mailbox 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 O OU PS CN	 *[Registration Organisation Country]* EUROPEAN SYSTEM OF CENTRAL BANKS *Internal organisation of the shared mailbox* *ESCB user identifier (UID)* [SHM:S] *Display 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 1 1 0 0	Yes
extKeyUsage	emailProtection (1.3.6.1.5.5.7.3.4) clientAuth (1.3.6.1.5.5.7.3.2)	
Certificate Policies Policy Identifier URL CPS Policy Identifier URL CPS	 *[OID ESCBPKI]*.2.2.11 *[CPS-URL]* *[OID ESCBPKI].2.1* *[CPS-URL]*	
Subject Alternative Names rfc822 RegisteredID (*[OID ESCBPKI]*.1.11) RegisteredID (*[OID ESCBPKI]*.1.7)	 *Subject's Email* *Shared mailbox display name* *ESCB user identifier (UID)*	
Basic Constraints CA Path Length Constraint	 FALSE *Not used*	Yes
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 caIssuers caIssuers ocsp	 *[HTTP URI Root CA]* *[HTTP URI Sub CA]* *[HTTP URI OCSP ALIAS]* *[HTTP URI OCSP]* *[IAM URI OCSP]]*	
[ESCB] Extensions		
escbUseCertType	SHARED MAILBOX	
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:

[OID ESCBPKI].2.2.0.X.Y: Certificate policies for the internal users' certificates (this document)

[OID ESCBPKI].2.2.1.X.Y: Certificate Policy of Advanced Authentication certificate for internal users

[OID ESCBPKI].2.2.2.X.Y: Certificate Policy of Archived Encryption certificate recoverable in token for internal users

[OID ESCBPKI].2.2.3.X.Y: Certificate Policy of Non-Archived Encryption certificate for internal users

[OID ESCBPKI].2.2.4.X.Y: Certificate Policy of Advanced Signature certificate based on a SSCD for internal users

[OID ESCBPKI].2.2.5.X.Y: Certificate Policy of Advanced Signature certificate for internal users

[OID ESCBPKI].2.2.6.X.Y: Certificate Policy of Standard Authentication certificate for internal users
[OID ESCBPKI].2.2.7.X.Y: Certificate Policy of Mobile Device certificate for internal users
[OID ESCBPKI].2.2.8.X.Y: Certificate Policy of Secure E-mail Gateway certificate for internal users
[OID ESCBPKI].2.2.9.X.Y: Certificate Policy of Provisional certificate for internal users
[OID ESCBPKI].2.2.10.X.Y: Certificate Policy of Administrator certificate for internal users
[OID ESCBPKI].2.2.11.X.Y: Certificate Policy of Shared Mailbox certificate for internal users
[OID ESCBPKI].2.2.12.X.Y: Certificate Policy of Archived encryption certificate for internal 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.

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 internal 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 internal 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.