EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB PKI

Certification Practice Statement (CPS) (OID:1.3.6.1.4.1.41697.509.10.100.0.1)

Table of Contents

Table of Contents 2

Document control 11

Basic Description 11

Version History 11

Document Review and Signoff 11

Related Documents 11

1 Introduction 14

1.1 Overview 15

1.1.1 Implementation of the ECB PKI certificate authority hierarchy 15

1.2 Document Name and Identification 18

1.3 PKI Participants 21

1.3.1 Certification Authorities 21

1.3.2 Registration Authorities 22

1.3.3 Subscribers 23

1.3.4 Relying parties 23

1.3.5 Other participants 23

1.4 Certificate Usage 23

1.4.1 Appropriate certificate uses 25

1.4.2 Prohibited certificate uses 25

1.5 Policy Administration 26

1.5.1 Organization administering the document 26

1.5.2 Contact person 26

1.5.3 Person determining CPS suitability for the policy 26

1.5.4 CPS approval procedures 26

1.6 Definitions and Acronyms 26

2 Publication and Repository Responsibilities 31

2.1 Repositories 31

2.2 Publication of Certification Information 32

2.3 Time or Frequency of Publication 33

2.4 Access Controls on Repositories 33

3 Identification and Authentication 34

3.1 Naming 34
3.1.1 Types of names 34
3.1.2 Need for names to be meaningful 34
3.1.3 Anonymity or pseudonymity of subscribers 34
3.1.4 Rules for interpreting various name forms 34
3.1.5 Uniqueness of names 34
3.1.6 Recognition, authentication, and role of trademarks 34
3.2 Initial Identity Validation 35
3.2.1 Method to prove possession of private key 35
3.2.2 Authentication of organization identity 35
3.2.3 Authentication of individual identity 35
3.2.4 Non-verified subscriber information 35
3.2.5 Validation of authority 35
3.2.6 Criteria for interoperation 35
3.3 Identification and Authentication for Re-key Requests 36
3.3.1 Identification and authentication for routine re-key 36
3.3.2 Identification and authentication for re-key after revocation 36
3.4 Identification and Authentication for Revocation Requests 36
4 Certificate Life-Cycle Operational Requirements 37
4.1 Certificate Application 37
4.1.1 Who can submit a certificate application 37
4.1.2 Enrolment process and responsibilities 37
4.2 Certificate application processing 38
4.2.1 Performing identification and authentication functions 38
4.2.2 Approval or rejection of certificate applications 39
4.2.3 Time to process certificate applications 39
4.3 Certificate Issuance 39
4.3.1 CA actions during certificate issuance 39
4.3.2 Notification to subscriber by the CA of issuance of certificate 40
4.4 Certificate Acceptance 40
4.4.1 Conduct constituting certificate acceptance 40

4.4.2 Publication of the certificate by the CA 41
4.4.3 Notification of certificate issuance by the CA to other entities 41
4.5 Key Pair and Certificate Usage 41
4.5.1 Subscriber private key and certificate usage 41
4.5.2 Relying party public key and certificate usage 41
4.6 Certificate Renewal 42
4.6.1 Circumstance for certificate renewal 42
4.6.2 Who may request renewal 42
4.6.3 Processing certificate renewal requests 42
4.6.4 Notification of new certificate issuance to subscriber 42
4.6.5 Conduct constituting acceptance of a renewal certificate 42
4.6.6 Publication of the renewal certificate by the CA 43
4.6.7 Notification of certificate issuance by the CA to other entities 43
4.7 Certificate Re-key 43
4.7.1 Circumstance for certificate re-key 43
4.7.2 Who may request certification of a new public key 43
4.7.3 Processing certificate re-keying requests 43
4.7.4 Notification of new certificate issuance to subscriber 43
4.7.5 Conduct constituting acceptance of a re-keyed certificate 43
4.7.6 Publication of the re-keyed certificate by the CA 43
4.7.7 Notification of certificate issuance by the CA to other entities 43
4.8 Certificate Modification 43
4.8.1 Circumstance for Certificate Modification 44
4.8.2 Who may request certificate modification 44
4.8.3 Processing certificate modification requests 44
4.8.4 Notification of new certificate issuance to subscriber 44
4.8.5 Conduct constituting acceptance of modified certificate 44
4.8.6 Publication of the modified certificate by the CA 44
4.8.7 Notification of certificate issuance by the CA to other entities 44
4.9 Certificate Revocation and Suspension 44
4.9.1 Circumstances for revocation 44

4.9.2 Who can request revocation 45
4.9.3 Procedure for revocation request 45
4.9.4 Revocation request grace period 45
4.9.5 Time within which CA must process the revocation request 46
4.9.6 Revocation checking requirement for relying parties 46
4.9.7 CRL issuance frequency 46
4.9.8 Maximum latency for CRLs 46
4.9.9 On-line revocation/status checking availability 46
4.9.10 On-line revocation checking requirements 47
4.9.11 Other forms of revocation advertisements available 47
4.9.12 Special requirements re key compromise 47
4.9.13 Circumstances for suspension 47
4.9.14 Who can request suspension 47
4.9.15 Procedure for suspension request 47
4.9.16 Limits on suspension period 47
4.10 Certificate Status Services 47
4.10.1 Operational characteristics 47
4.10.2 Service availability 47
4.10.3 Optional features 48
4.11 End of Subscription 48
4.12 Key Escrow and Recovery 48
4.12.1 Key escrow and recovery policy and practices 48
4.12.2 Session key encapsulation and recovery policy and practices 48
5 Facility, Management, and Operational Controls 49
5.1 Physical Controls 49
5.1.1 Site location and construction 49
5.1.2 Physical access 49
5.1.3 Power and air conditioning 50
5.1.4 Water exposures 50
5.1.5 Fire prevention and protection 50
5.1.6 Media storage 50

5.1.7 Waste disposal 50
5.1.8 Off-site backup 50
5.2 Procedural Controls 50
5.2.1 Trusted roles 50
5.2.2 Number of persons required per task 51
5.2.3 Identification and authentication for each role 52
5.2.4 Roles requiring separation of duties 52
5.3 Personnel Controls 52
5.3.1 Qualifications, experience, and clearance requirements 52
5.3.2 Background check procedures 53
5.3.3 Training requirements 53
5.3.4 Retraining frequency and requirements 53
5.3.5 Job rotation frequency and sequence 53
5.3.6 Sanctions for unauthorized actions 53
5.3.7 Independent contractor requirements 53
5.3.8 Documentation supplied to personnel 53
5.4 Audit Logging Procedures 53
5.4.1 Types of events recorded 53
5.4.2 Frequency of processing log 54
5.4.3 Retention period for audit log 54
5.4.4 Protection of audit log 54
5.4.5 Audit log backup procedures 54
5.4.6 Audit collection system (internal vs. external) 54
5.4.7 Notification to event-causing subject 55
5.4.8 Vulnerability assessments 55
5.5 Records Archival 55
5.5.1 Types of records archived 55
5.5.2 Retention period for archive 55
5.5.3 Protection of archive 55
5.5.4 Archive backup procedures 55
5.5.5 Requirements for time-stamping of records 55

5.5.6 Archive collection system (internal or external) 55
5.5.7 Procedures to obtain and verify archive information 56
5.6 Key Changeover 56
5.7 Compromise and Disaster Recovery 56
5.7.1 Incident and compromise handling procedures 56
5.7.2 Computing resources, software, and/or data are corrupted 56
5.7.3 Entity private key compromise procedures 57
5.7.4 Business continuity capabilities after a disaster 57
5.8 CA or RA Termination 58
6 Technical Security Controls 59
6.1 Key Pair Generation and Installation 59
6.1.1 Key pair generation 59
6.1.2 Private Key delivery to subscriber 59
6.1.3 Public key delivery to certificate issuer 60
6.1.4 CA public key delivery to relying parties 60
6.1.5 Key Sizes 60
6.1.6 Public key parameters generation and quality checking 61
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 61
6.2 Private Key Protection and Cryptographic Module Engineering Controls 62
6.2.1 Cryptographic module standards and controls 62
6.2.2 Private Key (n out of m) Multi-Person Control 63
6.2.3 Private Key escrow 63
6.2.4 Private Key backup 63
6.2.5 Private Key archival 63
6.2.6 Private Key transfer into or from a cryptographic module 63
6.2.7 Private Key storage using cryptographic module 63
6.2.8 Method of activating private key 64
6.2.9 Method of deactivating private keys 64
6.2.10 Method of destroying private keys 65
6.2.11 Cryptographic Module Rating 65
6.3 Other Aspects of Key Pair Management 65

6.3.1 Public key archival 65
6.3.2 Certificate operational periods and key pair usage periods 65
6.4 Activation Data 66
6.4.1 Activation data generation and installation 66
6.4.2 Activation data protection 66
6.4.3 Other aspects of activation data 66
6.5 Computer Security Controls 67
6.5.1 Specific computer security technical requirements 67
6.5.2 Computer security rating 67
6.6 Life Cycle Technical Controls 67
6.6.1 System development controls 67
6.6.2 Security management controls 67
6.6.3 Life cycle security controls 67
6.7 Network Security Controls 68
6.8 Time-stamping 68
7 Certificate, CRL, and OCSP Profiles 69
7.1 Certificate Profile 72
7.1.1 Version number(s) 79
7.1.2 Certificate extensions 79
7.1.3 Algorithm object identifiers 80
7.1.4 Name forms 81
7.1.5 Name constraints 81
7.1.6 Certificate policy object identifier 81
7.1.7 Usage of Policy Constraints extension 81
7.1.8 Policy qualifiers syntax and semantics 81
7.1.9 Processing semantics for the critical Certificate Policies extension 81
7.2 CRL Profile 81
7.2.1 Version Number(s) 82
7.2.2 CRL and CRL Entry Extensions 82
7.3 OCSP Profile 83
7.3.1 Version number(s) 85

7.3.2 OCSP extensions 85

8 Compliance Audit and Other Assessments 87

8.1 Frequency or circumstances of assessment 87

8.2 Identity/qualifications of assessor 87

8.3 Assessor's relationship to assessed entity 87

8.4 Topics covered by assessment 87

8.5 Actions taken as a result of deficiency 87

8.6 Communication of results 87

9 Other Business and Legal Matters 88

9.1 Fees 88

9.1.1 Certificate issuance or renewal fees 88

9.1.2 Certificate access fees 88

9.1.3 Revocation or status information access fees 88

9.1.4 Fees for other services 88

9.1.5 Refund policy 88

9.2 Financial Responsibility 88

9.2.1 Insurance coverage 88

9.2.2 Other assets 88

9.2.3 Insurance or warranty coverage for end-entities 88

9.3 Confidentiality of Business Information 88

9.3.1 Scope of confidential information 89

9.3.2 Information not within the scope of confidential information 89

9.3.3 Responsibility to protect confidential information 89

9.4 Privacy of Personal Information 89

9.4.1 Privacy plan 89

9.4.2 Information treated as private 89

9.4.3 Information not deemed private 89

9.4.4 Responsibility to protect private information 89

9.4.5 Notice and consent to use private information 90

9.4.6 Disclosure pursuant to judicial or administrative process 90

9.4.7 Other information disclosure circumstances 90
9.5 Intellectual Property Rights 90
9.6 Representations and Warranties 90
9.6.1 CA representations and warranties 90
9.6.2 RA representations and warranties 90
9.6.3 Subscriber representations and warranties 90
9.6.4 Relying party representations and warranties 90
9.6.5 Representations and warranties of other participants 90
9.7 Disclaimers of Warranties 90
9.8 Limitations of Liability 90
9.9 Indemnities 91
9.10 Term and Termination 91
9.10.1 Term 91
9.10.2 Termination 91
9.10.3 Effect of termination and survival 91
9.11 Individual notices and communications with participants 91
9.12 Amendments 91
9.12.1 Procedure for amendment 91
9.12.2 Notification mechanism and period 91
9.12.3 Circumstances under which OID must be changed 92
9.13 Dispute Resolution Provisions 92
9.14 Governing Law 92
9.15 Compliance with Applicable Law 92
9.16 Miscellaneous Provisions 92
9.16.1 Entire agreement 92
9.16.2 Assignment 93
9.16.3 Severability 93
9.16.4 Enforcement (attorneys' fees and waiver of rights) 93
9.16.5 Force Majeure 93
9.17 Other Provisions 93
Annex 1: Types of events logged by the CA 94

Document control

Basic Description

Document title	Certification Practice Statement (CPS) (OID:1.3.6.1.4.1.41697.509.10.100.0.1)
Topic	Certification Practice Statement for the ECB PKI Service based on RFC 3647
Version	1.2
Status	Published release related to introduction of the new ECB PKI and for certification for CAF compliancy for Sub CA 03
Document OID	1.3.6.1.4.1.41697.509.10.100.0.1
Supersedes Document	-
Authors	Daniela Puiu
ECB responsible contact	Daniela Puiu

Version History

Version	Version Date	Comment
1.0	27.02.2024	Initial Draft
1.0	05.09.2024	First version submitted for approval
1.1	28.10.2024	Corrections on CP CPS documents, to address PKI AB inquiries
1.2	05.02.2025	Update due to CAF application for Sub CA 03

Document Review and Signoff

Version	Version Date	Reviewer Name	Signoff Date
1.0	05.09.2024	Alvise Grammatica [ECB CISO]	05.09.2024
1.0	05.09.2024	Alain Busac [ECB CIO]	06.09.2024
1.2			
1.2			

Related Documents

Document title	ECB PKI Certificate Policy (CP) Standard Authentication

Document Name	2025-02-05 ECB PKI - ECB RSA Standard Authentication Certificate Policy (CP) (OID 1.3.6.1.4.1.41697.509.10.100.1.3.1) v1.0.pdf
Description	Certificate Policy for ECB RSA Standard Authentication Services
Document OID	1.3.6.1.4.1.41697.509.10.100.1.3.1
Latest available version	V1.0
Last changed	28.02.2025

Document title	ECB PKI Certificate Policy (CP) Application Authentication
Document Name	2025-02-05 ECB PKI - ECB RSA Service Account Certificate Policy (CP) (OID: 1.3.6.1.4.1.41697.509.10.100.1.3.3) v1.0.pdf
Description	Certificate Policy for ECB RSA Service Account Services
Document OID	1.3.6.1.4.1.41697.509.10.100.1.3.3
Latest available version	V1.0
Last changed	28.02.2025

Document title	ECB PKI Certificate Policy (CP) Shared Mailbox
Document Name	2024-03-01 ECB PKI - ECB RSA Shared Mailbox Certificate Policy (CP) (OID: 1.3.6.1.4.1.41697.509.10.100.1.3.2) v1.0.pdf
Description	Certificate Policy for ECB RSA Advanced Signature Services
Document OID	1.3.6.1.4.1.41697.509.10.100.1.3.2
Latest available version	V1.0
Last changed	28.02.2025

Document title	ECB RSA Certificate Profiles RFC5280
Document Name	ECB RSA Certificate Profiles RFC 5280 v1.0.xlsx
Description	RFC5280 Certificate Profiles for ECB PKI
Latest available version	V1.1
Last changed	28.02.2025

Document title	ECB PKI IANA PEN Namespace
Document Name	ECB PKI IANA PEN Namespace v2.0
Description	Overview of the ECB PKI related IANA PEN Namespace
Latest available version	v2.0
Last changed	10.02.2025

Document title	ECB PKI Operational Concept v1.0
Document Name	ECB PKI Operational Concept v1.0

Description	Overview of the ECB PKI operational processes and procedures
Latest available version	V1.0
Last changed	18.02.2025

1 Introduction

This document is the Certification Practice Statement (CPS) for the European Central Bank Certificate Services Public Key Infrastructure (hereinafter referred to as “ECB PKI”).

The concept of a Certification Practices Statement (CPS) was developed by the American Bar Association (ABA) in its Digital Signature Guidelines (ABA Guidelines) and is defined as a "statement of the practices, which a certification authority employs in issuing certificates." Most organizations that operate certification authorities will document their own practices in a CPS or similar statements. The CPS is one of the organization's means of protecting its PKI and positioning its business relationships with subscribers and other entities.

This Certification Practice Statement document describes the practices of the Certification Authorities (CA) operated by the ECB PKI. It is applicable to all entities that have relationships with the ECB PKI CAs and PKI components, including end users-, cross-certified CAs, and Registration Authorities (RAs). This CPS provides those entities with a clear statement of the practices of the ECB PKI CAs.

The Certification Practice Statement (CPS) helps the user of certification services to determine the level of trust that he can put in the certificates that are issued by the ECB PKI CAs and connected infrastructure services.

The ECB PKI certification service is only as trustworthy as the procedures contained in it. The ECB PKI CPS therefore covers all relevant preconditions, regulations, processes and measures within the ECB PKI certification service as a compact information source for current and potential participants.

This document will rely on other parts of the ECB PKI certification service documentation and will sum up those parts that are of importance for the participating PKI users. Other related documentation is referenced in this Certification Practice Statement documentation where relevant while an overview of other documents is listed in the document control section. The ordering of topics in this document follows IETF rfc3647, thereby facilitating comparisons and mappings among the corresponding documents of other PKIs.

It should be provided for free and publicly accessible to any ECB PKI user.

1.1 Overview

The European Central Bank PKI (ECB PKI) consists of a set of root level policy CAs, each providing the anchor for the associated trust chains. Subscriber certificates are issued by subordinate issuing CAs in a strict two-tier flat hierarchy.

All ECB PKI trust chains inherit the set of up-to-date cryptographic algorithms and key lengths requirements provided by the corresponding policy CA thus offering consistent cryptographic reliability and avoiding vulnerabilities of hybrid algorithmic setups.

Cryptoagility is maintained by the ability to duplicate the entire CA hierarchy using future algorithms and key lengths for the entire trust chain under the otherwise identical policies instead of introducing risk of hybrid chains during re-key transition periods.

All certificates, regardless of CA or subscriber / end-entity, within either underlying cryptographic technology trust chain are required to reflect both the trust cryptographic class definition and governing issuance policy by unambiguous reference to the associated certificate policy.

The implementation of the ECB PKI trust chain model is reflected in OID namespaces of the issuance policy and document identifiers according to the IANA based PEN namespace model of ECB reference to in the related documents section of this document.

1.1.1 Implementation of the ECB PKI certificate authority hierarchy

The following section is a brief overview of the implemented ECB PKI trust chain model and the CA hierarchy for the ECB trust chain including the ECB PKI certification services provided by this architecture.

The ECB PKI CA hierarchy is built on a 2-tier model, rooted in the trusted ECB Root CAs, and Issuing subordinate CAs certified by it.

The ECB PKI environment is comprised of ECB RSA Root CA 01 and ECB RSA AV Root CA 01 as the trust anchors and, on the subordinate level, the ECB RSA Sub CA 01, ECB RSA Sub CA 02, ECB RSA Sub CA 03, ECB RSA AV Sub CA 01 and the ECB RSA AV Sub CA 02 providing certificate issuance for different purposes. ECB RSA Sub CA 01 is used for issuance of domain-joined machine or user certificates following directory based assertions, ECB RSA Sub CA 02 is used for issuance of user or machine certificates for authentication, signature or encryption following subject claim based assertions, and ECB RSA Sub CA 03 is used to issue standard authentication, encryption or signature certificates for users. The ECB RSA AV Sub CA 01 is used for issuance of advanced authentication, signature and encryption user-based certificates, while the ECB RSA AV Sub CA 02 is purposed to issue advanced authentication application certificates. All relevant PKI components and application keys are protected by an integrated HSM infrastructure. All cryptographic operations of ECB PKI CAs and backend services are controlled and protected by this HSM implementation.

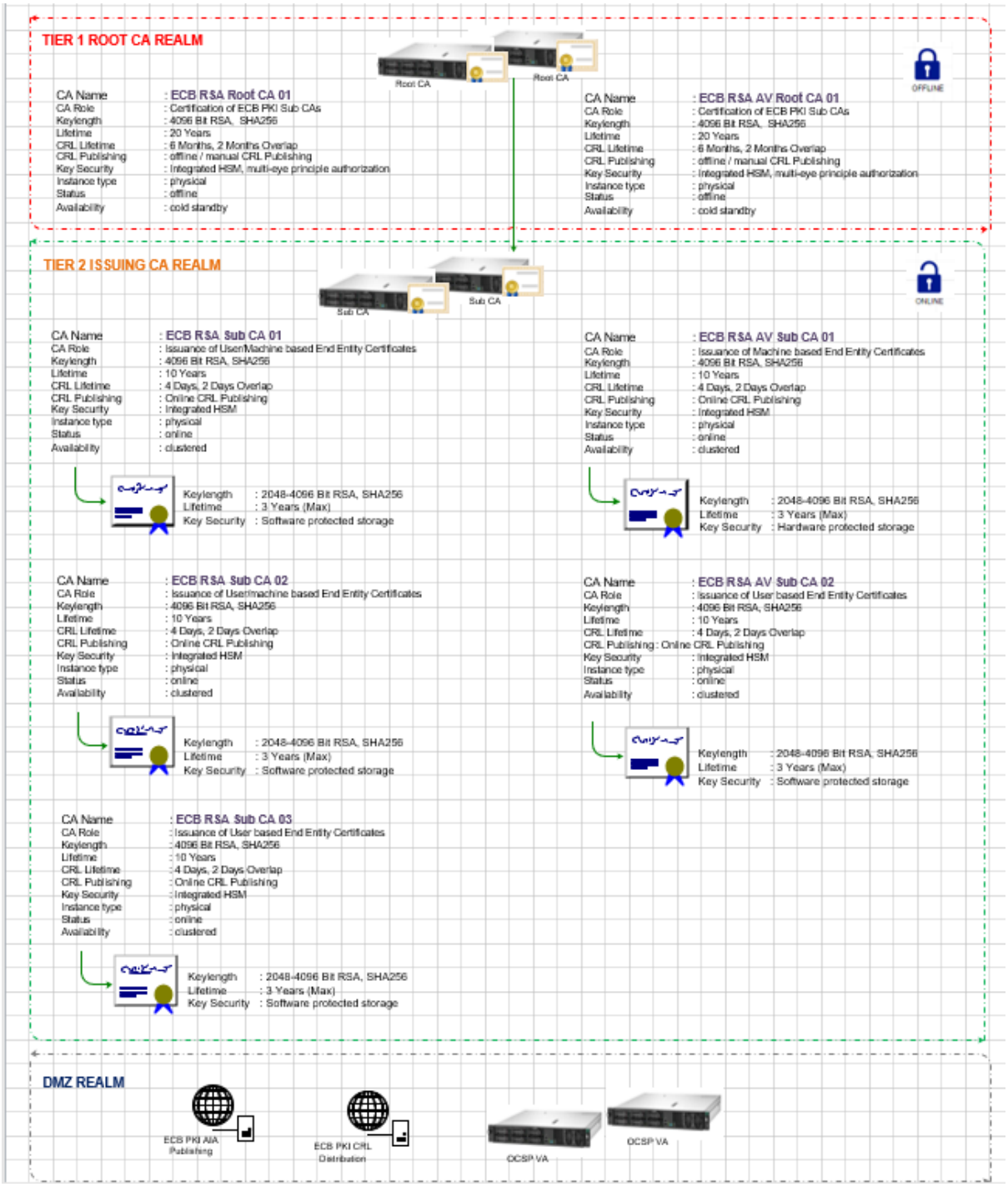
Administrative access to the HSMs (root CA and sub CA) is based on tokens enforcing segregation of duties. Control over the signing key of the root CA is likewise based on separate tokens with segregation of duties, while the operation of the signing keys of the Sub CAs is controlled by mutual

authentication between the respective HSM and the server implementing the relevant PKI component.

The other components in the PKI are built from multi-tenant capable centralized components like certificate validation services and the certificate management solution. The same principle applies to the centralized LDAP directory infrastructure.

As the primary information source for ECB PKI is hosted on a load balancer enabled web server infrastructure, CRLs, CA certificates and the current versions of the CP and CPS documents are also located on these web servers while the main references for revocation and authority information are implemented using HTTP based location information and URLs. In addition to the CRL based revocation information, ECB PKI is also supporting the OCSP protocol (RFC 5019, a profile of the Online Certificate Status Protocol (OCSP) outlined in RFC 2560) based on the current CRL information for OCSP aware PKI clients.

Overview of the ECB PKI trust chain**:**



1.2 Document Name and Identification

This document is the "ECB PKI Certification Practice Statement" for the ECB PKI services. The Object Identifier (OID) representing this document is 1.3.6.1.4.1.41697.509.10.100.0.1. Object Identifier(s) (OID) for specific certificate policies are specified in their respective CPs and used within the ECB PKI hierarchy when issuing certificates for those requirement profiles. For details on OID namespaces please refer to the ECB PKI IANA PEN namespace document referenced in the related documents section.

X.509 OID – ECB PKI

1.3.6.1.4.1.41697.**509** Base of the ECB PKI Namespace

X.509 OID – ECB PKI trust chain identifier

1.3.6.1.4.1.41697.509.**10** Base of the ECB New generation PKI trust chain namespace

X.509 OID –Environment

1.3.6.1.4.1.41697.509.10.**100** Base of the ECB RSA PKI production environment

X.509 OID – Issuance Policies Namespace

1.3.6.1.4.1.41697.509.10.100.**0** Base of the PKI Issuance Policies Namespace

X.509 OID – ECB NG Issuance Policy Reference

1.3.6.1.4.1.41697.509.10.100.0.**0** ECB PKI NG Issuance Policy Reference

X.509 OID – ECB PKI CPS Reference

1.3.6.1.4.1.41697.509.10.100.0.**1** ECB PKI Certification Practice Statement (CPS)

X.509 OID – ECB PKI Internal trust realm

1.3.6.1.4.1.41697.509.10.100.**1** ECB PKI Internal trust realm

X.509 OID – ECB PKI Root Level Sub CA CP

1.3.6.1.4.1.41697.509.10.100.1.**0** ECB PKI Root Level Sub CA CP

X.509 OID – ECB PKI Issuing Authorities CP

1.3.6.1.4.1.41697.509.10.100.1.0.**1** ECB PKI ECB Issuing Authorities CP

X.509 OID – ECB PKI Directory signing realm

1.3.6.1.4.1.41697.509.10.100.1.**1** ECB PKI Directory signing realm

X.509 OID – ECB PKI Directory Certificate Policy (CP)

1.3.6.1.4.1.41697.509.10.100.1.1.**0** ECB PKI Directory Certificate Policy (CP)

X.509 OID – ECB PKI Object signing realm

1.3.6.1.4.1.41697.509.10.100.1.**2** ECB PKI Object signing realm

X.509 OID – ECB PKI ECB Subscriber CP

1.3.6.1.4.1.41697.509.10.100.1.2.**0** ECB PKI ECB Subscriber CP

X.509 OID – ECB PKI CAF Compliant Standard realm

1.3.6.1.4.1.41697.509.10.100.1.**3** ECB PKI CAF Compliant Standard realm

X.509 OID –CP documentation

1.3.6.1.4.1.41697.509.10.100.1.3.**1** ECB Standard Authentication (CP)

1.3.6.1.4.1.41697.509.10.100.1.3.**2** ECB Standard Encryption CP

1.3.6.1.4.1.41697.509.10.100.1.3.**3** ECB Application Authentication CP

X.509 OID – ECB PKI CAF Compliant Advanced realm

1.3.6.1.4.1.41697.509.10.100.**2** ECB PKI CAF Compliant Advanced realm

X.509 OID – ECB PKI Root Level Sub CA CP

1.3.6.1.4.1.41697.509.10.100.2.**0** ECB PKI Root Level Sub CA CP

X.509 OID – ECB PKI AV Issuing Authorities (CP)

1.3.6.1.4.1.41697.509.10.100.2.0.**1** ECB PKI Advanced (AV) Issuing Authorities Certificate policy (CP)

X.509 OID – ECB PKI Advanced profile realm

1.3.6.1.4.1.41697.509.10.100.2.**1** ECB PKI Advanced profile realm

X.509 OID –AV CP documentation

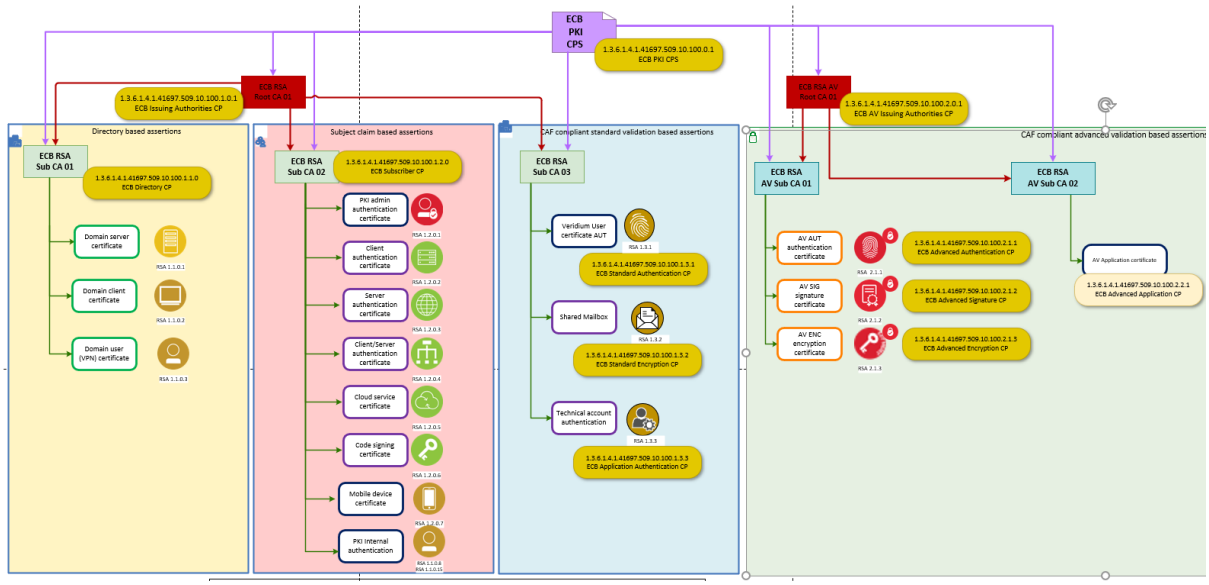
1.3.6.1.4.1.41697.509.10.100.2.**1.1** ECB Advanced Authentication Certificate Policy

1.3.6.1.4.1.41697.509.10.100.2.**1.2** ECB Advanced Signature Certificate Policy

1.3.6.1.4.1.41697.509.10.100.2.**1.3** ECB Advanced Encryption Certificate Policy

X.509 OID – ECB PKI Advanced application profile realm

1.3.6.1.4.1.41697.509.10.100.2.**2** ECB PKI Advanced application profile realm



Along with other documentation, the CP and CPS document locations are accessible to ECB PKI certification service participants at http://cpki.ecb.europa.eu

1.3 PKI Participants

1.3.1 Certification Authorities

European Central Bank operates a two-tier CA hierarchy which issues machine and user certificates to ECB employees and ECB partners. The two-tier CA hierarchy is built upon:

- Policy root CAs (Trust Anchors)
  - ECB RSA Root CA 01
  - ECB RSA AV Root CA 01
- Issuing sub CAs
  - ECB RSA Sub CA 01
  - ECB RSA Sub CA 02
  - ECB RSA Sub CA 03
  - ECB RSA AV Sub CA 01
  - ECB RSA AV Sub CA 02

The certificate services hierarchy does not reflect any ECB organizational hierarchy.

Most significant details of the CAs are listed below:

Distinguished Name	CN = ECB RSA Root CA 01, O = European Central Bank, C = EU
Serial Number	12a6bf064b67b514e71d95fb695ecc3f0d21caf0
Issuer Distinguished Name	CN = ECB RSA Root CA 01, O = European Central Bank, C = EU
Validity Period	From 20 December 2023 14:02:33 to 15 December 2043 14:02:32
Cryptographic algorithms	SHA-256 / RSA 4096

Distinguished Name	CN = ECB RSA Sub CA 01, O = European Central Bank, C = EU
Serial Number	7030b6b6c062162f2e3d1087992b5f90cb671737
Issuer Distinguished Name	CN = ECB RSA Root CA 01, O = European Central Bank, C = EU
Validity Period	From 20 December 2023 15:40:07 to 17 December 2033 15:40:06
Cryptographic algorithms	SHA-256 / RSA 4096

Distinguished Name	CN = ECB RSA Sub CA 02, O = European Central Bank, C = EU
Serial Number	0d4f5cd8e5946df5d9d8b4beef5c0d22246cfbe5
Issuer Distinguished Name	CN = ECB RSA Root CA 01, O = European Central Bank, C = EU
Validity Period	From 20 December 2023 15:47:55 to 17 December 2033 15:47:54
Cryptographic algorithms	SHA-256 / RSA 4096

Distinguished Name	CN = ECB RSA Sub CA 03, O = European Central Bank, C = EU
Serial Number	5e0099ccdfa8542abf31332a16c1704507ff371d
Issuer Distinguished Name	CN = ECB RSA Root CA 01, O = European Central Bank, C = EU
Validity Period	From 30 January 2025 09:25:32 to 28 January 2035 09:25:31
Cryptographic algorithms	SHA-256 / RSA 4096

Distinguished Name	CN = ECB RSA AV Root CA 01, O = European Central Bank, C = EU
Serial Number	3be5fbf7e71f057cbc798c490b3c87825a4509d2
Issuer Distinguished Name	CN = ECB RSA AV Root CA 01, O = European Central Bank, C = EU
Validity Period	From 20 December 2023 14:05:05 to 15 December 2043 14:05:04
Cryptographic algorithms	SHA-256 / RSA 4096

Distinguished Name	CN = ECB RSA AV Sub CA 01, O = European Central Bank, C = EU
Serial Number	7267f61c60b2c03202f4f3b46ba3aa3300d97042
Issuer Distinguished Name	CN = ECB RSA AV Root CA 01, O = European Central Bank, C = EU
Validity Period	From 20 December 2023 15:48:14 to 17 December 2033 15:48:13
Cryptographic algorithms	SHA-256 / RSA 4096

Distinguished Name	CN = ECB RSA AV Sub CA 02, O = European Central Bank, C = EU
Serial Number	7267f61c60b2c03202f4f3b46ba3aa3300d97042
Issuer Distinguished Name	CN = ECB RSA AV Root CA 01, O = European Central Bank, C = EU
Validity Period	From 20 December 2023 15:48:30 to 17 December 2033 15:48:29
Cryptographic algorithms	SHA-256 / RSA 4096

1.3.2 Registration Authorities

ECB PKI recognizes several specialized Registration Authorities interfacing with the ECB PKI CAs to evaluate submitted certificate signing requests or create them on behalf of the PKI subscribers. ECB PKI RAs may either be partially or fully automated systems, evaluating CSRs based on deterministic

business rule sets or inherited trust from upstream systems, or may be infrastructures that include human Registration Officers evaluating CSRs as part of different certification workflows according to the certificate policies of the desired certificate's assertions and trust levels. See the Certificate Policy document corresponding to the desired certificate type for more information on the responsible RAs.

1.3.3 Subscribers

End-entities in this PKI are ECB employees and contractors, computers, network devices, and identities as well as machines of approved ECB partners. All end-entities are certified by the ECB PKI certification authorities and as such are certificate subscribers. The subscriber holds a private key that corresponds to the public key listed in that certificate. Subscribers of the ECB PKI are internal users, machines as well as approved partners with their machines and users according to ECB identity management and security policy.

See also section 1.3.3 on corresponding ECB PKI CP.

1.3.4 Relying parties

A relying party is any entity that acts in reliance of a certificate and /or a digital signature that is issued by an Issuing CA or Root CA and that is used in a manner consistent with the corresponding CP. A relying party could be within or outside the organization of European Central Bank and may or may not also be a Subscriber within the PKI. For instance, a Web Client that checks the validity of a Web Server certificate within the ECB organization or in terms of secure email, using the recipient certificate for encrypting emails to the recipient. Relying parties implicitly agree to the terms of this CPS documentation, the associated CPs documentation and referenced general ECB security policies in their respective latest version.

1.3.5 Other participants

There are no other participants in the ECB PKI.

1.4 Certificate Usage

Certificates issued by the ECB PKI are suitable for internal applications to the extent set forth in the Certificate Policy corresponding to a specific type of certificate or a group of certificates issued under the same CP. Suitable applications and level of assurance are governed by the specific policy the issued certificate refers to by its associated CP Object ID included in the certificate. Partners and other external entities should not assume any higher level of trust than assigned internally within European Central Bank.

The certificates issued by ECB PKI are as follows:

ECB PKI Trust Chain

Certificates issued by ECB RSA AV Root CA 01

Certificate Name Type	Purpose of issued certificate
Subordinate Certification Authority	Issue certificates for ECB RSA PKI subordinate certification authorities

Certificates issued by ECB RSA AV Sub CA 01

Certificate Name Type	Purpose of issued certificate
ECB RSA AV User authentication certificate	ECB Advanced User Authentication
ECB RSA AV User encryption certificate	ECB Advanced User Encryption
ECB RSA AV User signature certificate	ECB Advanced User signature
ECB OCSP Signing	OCSP response signing

Certificates issued by ECB RSA AV Sub CA 02

Certificate Name Type	Purpose of issued certificate
No certificates issued at this point	

Certificates issued by ECB RSA Root CA 01

Certificate Name Type	Purpose of issued certificate
Subordinate Certification Authority	Issue certificates for ECB RSA PKI subordinate certification authorities

Certificates issued by ECB RSA Sub CA 01

Certificate Name Type	Purpose of issued certificate
ECB RSA Domain Server certificate	ECB Domain Server Authentication
ECB RSA Domain Client certificate	ECB Domain Client Authentication
ECB RSA Domain User certificate	ECB Domain User Authentication
ECB OCSP Signing	OCSP response signing

Certificates issued by ECB RSA Sub CA 02

Certificate Name Type	Purpose of issued certificate
ECB RSA PKI Admin Authentication certificate	ECB PKI Admin Authentication
ECB RSA Client Authentication certificate	ECB Client Authentication
ECB RSA Server Authentication certificate	ECB Server Authentication
ECB RSA Client/Server Authentication certificate	ECB Client/Server Authentication
ECB RSA Cloud Service certificate	ECB Cloud Service

ECB RSA Code Signing certificate	ECB Code Signing
ECB RSA Mobile Device Authentication certificate	ECB Mobile Device Authentication
ECB RSA PKI Internal Authentication certificate	ECB PKI Internal Application Authentication
ECB OCSP Signing	OCSP response signing

Certificates issued by ECB RSA Sub CA 03

Certificate Name Type	Purpose of issued certificate
ECB RSA Veridium User Authentication certificate	ECB PKI Standard User Authentication
ECB RSA Shared Mailbox certificate	Standard Encryption of Shared Mailboxes
ECB RSA Service Account Authentication certificate	Standard Authentication for Service Accounts
ECB OCSP Signing	OCSP response signing

See section 1.4 on ECB PKI CP.

1.4.1 Appropriate certificate uses

All certificates issued by the ECB PKI are used for ECB internal business purposes by ECB and approved ECB partners only. ECB PKI certificates for users are issued to ECB employees either for authentication, digital signature or encryption with only one purpose per certificate. ECB PKI machine certificates may only be used for authentication purposes and to ensure the confidentiality of communication channels. Further provisions on permissible uses are regulated individually for each type of certificate by the respective CP.

1.4.2 Prohibited certificate uses

Any usage not covered in sections 1.4 Certificate Usage, 1.4.1 Appropriate certificate uses of this CP is explicitly prohibited.

In general, certificates signed by the subordinate tier 2 Issuing CAs must not:

- be able to sign lower tier CA certificates,
- be used for different purposes other than outlined in the certification request,
- be used outside of their given validity period or after revocation (exception for archived encryption certificates may apply),
- be used for usage of subscriber end entity certificates after revocation by the ECB PKI,
- be issued for non-ECB and on non-certified partner subjects, and
- be used for certificates for non-ECB internal and partner purposes.

1.5 Policy Administration

1.5.1 Organization administering the document

This Certificate Policy is administered by the ECB Digital Security Services Division.

European Central Bank
DG-IS Digital Security Services
Security Governance
Sonnemannstrasse 20
60314 Frankfurt am Main
Germany

1.5.2 Contact person

European Central Bank
DG-IS Digital Security Services Division
Security Governance
Ulrich Kühn
Sonnemannstrasse 20
60314 Frankfurt am Main
Germany
Voice: +49 69-1344-4857
Email: Ulrich.Kuhn@ecb.europa.eu
Web: http://www.pki.ecb.europa.eu

1.5.3 Person determining CPS suitability for the policy

The ECB Policy Management Authority determines the suitability and applicability of this document. It consists of the ECB Director General Information Systems and the ECB Head of Digital Security Services Division.

1.5.4 CPS approval procedures

The European Central Bank Chief Information Officer (CIO) and the European Central Bank Corporate Information Security Officer (CISO) approved this document prior to publication. This document is regularly re-evaluated.

1.6 Definitions and Acronyms

Term	Alias	Definition
Administrative Card Set	ACS	Set of administrator authentication smart card protected private keys to perform actions on HSMs. Usually requires a quorum n out of m cards.

Term	Alias	Definition
Authority Information Access	AIA	Certificate extension containing information about how to get the issuer of this certificate and the address of the OCSP responder from where revocation of this certificate can be checked.
Certificate	public key certificate	A data structure containing the public key of an electronic identity and additional information. A certificate is digitally signed using the private key of the issuing CA binding the subject's identity to the respective public key
Certificate Management over CMS	CMC	Transport mechanism that can be used for obtaining X.509 digital certificates in a PKI
Certificate Policy	CP	A document containing the rules that indicate the applicability and use of certificates issued to ECB PKI subscribers
Certificate Revocation List	CRL	A list of certificates which are no longer valid
Certificate Signing Request	CSR	A request from a Subscriber to an RA to create and sign a certificate for a subject with certain attributes specified in the request
Certification Authority	CA	The unit within ECB PKI to create, assign and revoke public key certificates
Certification Practices Statement	CPS	A document containing the practices that ECB PKI certification authority employs in issuing certificates and maintaining PKI related operational status
Common Name	CN	An identifier for an end entity (subject)
Decryption		Cryptographic transformation that restores encrypted data to its original state.
Directory		A database containing information and data related to identities, certificates and CAs

Term	Alias	Definition
Encryption		Cryptographic transformation of data (called plaintext) into a form (called cipher text) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called decryption, which is a transformation that restores encrypted data to its original state.
End Of Life	EOL	An end-of-life product is at the end of the product lifecycle which prevents users from receiving updates, indicating that the product is at the end of its useful life.
End-Entity		An entity that is a subscriber, a relying party, or both
ESCB Certificate Acceptance Framework	CAF	The criteria established by the ESCB ITC to identify the certification authorities, both internal and external to the ESCB, which can be trusted in relation to ESCB and Eurosystem electronic applications, systems, platforms and service.
FIPS 140		FIPS 140 is the (US) Federal Information Processing Standard that outlines security requirements for cryptographic modules. FIPS 140 is one of several cryptographic standards maintained by the Computer Security Division of NIST (National Institute for Standards and Technology)
Hardware Security Module	HSM	A hardware encryption device that is connected to a server at the device level via direct physical interfaces.
Heating, Ventilation and Air Conditioning		HVAC is the use of various technologies to control the temperature, humidity, and purity of the air in an enclosed space.
Identity Governance and Administration Management	IGAM	Service that enables security administrators to efficiently manage user identities and access across the enterprise.
Intellectual Property Rights	IPR	Rights on a category of property that includes intangible creations of the human intellect like patents, copyrights, trademarks, and trade secrets.

Term	Alias	Definition
Internal Auditors Committee	IAC	Committee in charge of ESBC annual internal audit program.
Internet Assigned Numbers Authority	IANA	A standards organization that oversees global Internet Protocol–related symbols and Internet numbers
Internet Engineering Task Force	IETF	It is a standards organization for the Internet and is responsible for the technical standards that make up the Internet protocol suite.
Key Escrow		The purpose of escrow is to allow a third party (such as an organization or government) to obtain the private key without the cooperation of the subscriber.
Machine Readable Zone	MRZ	The visual part of an official identity or travel document designed to be interpreted using optical character recognition
Master Backup Key	MBK	Cryptographic encryption key required to decipher HSM key material backups into new or recovered PKI systems. Cryptographically divided into key shards to enforce a n out of m multi person control scheme.
Object Identifier	OID	An identification mechanism jointly developed by ITU-T and ISO/IEC for naming any type of object, concept or "thing" with a globally unambiguous name
Personal Identification Number	PIN	In practice a (chiefly numeric) password to authenticate a user upon smart card access
Policy Management Authority	PMA	This management authority sets the overall policies of the ECB PKI and approves the policies and procedures of trust domains within the PKI
Private Enterprise Number	PEN	IANA assigned Private Enterprise Numbers are identifiers that can be used in SNMP configurations, in LDAP configurations, and wherever the use of an ASN.1 object identifier (OID) is appropriate

Term	Alias	Definition
Public Key Cryptography Standards	PKCS	Are a group of public key cryptography standards published by RSA Security LLC
Public Key Infrastructure	PKI	Framework of technical components and related organizational processes for the distribution and management of private keys, public keys and corresponding certificates
Re-Key		Certificate re-key means duplicating unaltered identifying information from a valid certificate into a new certificate except a new public key and updated validity period.
Registration Authority	RA	An entity that is responsible for the identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is the delegate of certain tasks on behalf of a CA) A Registration Authority (RA) could provide the following functions: • proving identity of certificate applicants • approve or reject certificate applications • process subscriber requests to revoke their certificates
Relying Party		A recipient of a certificate issued by an ECB PKI CA who relies on the certificate, the respective ECB PKI trust chain and its corresponding policies
Renewal		Certificate renewal means duplicating all identifying information and the public key from the old certificate into a new certificate except for an updated validity period.
Security Information and Event Management	SIEM	It is a security solution that helps recognize and address potential security threats and vulnerabilities before they may disrupt operations.
Subject		Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate
Subject Alternative Name	SAN	The SAN is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field.

Term	Alias	Definition
Subscriber		Entity subscribing with a Certification Authority on behalf of one or more subjects. It is the subject named or identified in a certificate and holds the private key that corresponds to the associated certificate.
Uninterruptible Power Supply	UPS	A type of continual power system that provides automated backup electric power to a load when the input power source or mains power fails.
Veridium		Integrated Passwordless Platform (https://www.veridiumid.com/)
VeridiumID Authenticator		Mobile application integrated with Veridium server to provide user identification and authorization

2 Publication and Repository Responsibilities

In accordance with the corresponding Certificate Policy (CP) of the ECB PKI system.

2.1 Repositories

ECB PKI is responsible for the repository functions for its own CAs. The PKI publishes certificates it issues to subscribers in the corresponding issuing CA repository. Upon revocation of a subscriber's certificate, ECB PKI publishes notice of such revocation in the corresponding CA repository. ECB PKI issues CRLs for its own CAs pursuant to the provisions of this CPS.

ECB PKI repositories are listed below:

Root CA CRLs distribution point:

- ECB PKI website:
  - https://cpki.ecb.europa.eu/cdp/ECB-RSA-Root-CA-01-2043.crl
  - https://cpki.ecb.europa.eu/cdp/ECB-RSA-AV-Root-CA-01-2043.crl

Issuing CAs CRLs distribution point:

- ECB PKI website:
  - https://cpki.ecb.europa.eu/cdp/ECB-RSA-Sub-CA-01-2033.crl
  - https://cpki.ecb.europa.eu/cdp/ECB-RSA-Sub-CA-02-2033.crl

- https://cpki.ecb.europa.eu/cdp/ECB-RSA-Sub-CA-03-2035.crl
- https://cpki.ecb.europa.eu/cdp/ECB-RSA-AV-Sub-CA-01-2033.crl
- https://cpki.ecb.europa.eu/cdp/ECB-RSA-AV-Sub-CA-02-2033.crl

Online validation service that implements the OCSP protocol:

- http://ocsp.ecb.europa.eu

Root CAs certificate distribution point:

- ECB PKI website:
  - https://cpki.ecb.europa.eu/aia/ECB-RSA-Root-CA-01-2043.cer
  - https://cpki.ecb.europa.eu/aia/ECB-RSA-AV-Root-CA-01-2043.cer

Issuing CAs certificate distribution point:

- ECB PKI website:
  - https://cpki.ecb.europa.eu/aia/ECB-RSA-Sub-CA-01-2033.cer
  - https://cpki.ecb.europa.eu/aia/ECB-RSA-Sub-CA-02-2033.cer
  - https://cpki.ecb.europa.eu/aia/ECB-RSA-Sub-CA-03-2035.cer
  - https://cpki.ecb.europa.eu/aia/ECB-RSA-AV-Sub-CA-01-2033.cer
  - https://cpki.ecb.europa.eu/aia/ECB-RSA-AV-Sub-CA-02-2033.cer

For CPS and CPs:

- ECB PKI website: https://cpki.ecb.europa.eu/

ECB PKI repository does not contain any information of a confidential nature.

2.2 Publication of Certification Information

The ECB PKI is responsible for publishing information regarding its practices, certificates and the current status of such certificates. ECB PKI maintains a web-based repository that permits relying parties to make online inquiries regarding revocation and other certificate status information. It provides relying parties with information on how to find the associated repository to check a given certificate's status and how to query the related OCSP responder. CA certificates, Certificate Policy documents and the Certification Practice Statement must be publicly accessible using an unencrypted HTTP webservice. Certificate status information must be available by publishing Certificate Revocation Lists over unencrypted HTTP. It must additionally be available via publicly accessible OCSP service. Certificate issuer certificate information and the address of the OCSP service shall be incorporated in

each issued certificate's Authority Information Access extension. In addition, such information may be published to one or more appropriate ECB repositories.

2.3 Time or Frequency of Publication

Minor updates of the ECB PKI CP and CPS documents may be published once a year. Critical changes of ECB PKI CP and CPS documents are published immediately.

CRLs and CA certificates are published using a defined schedule. For details, please refer to chapter “CRL issuance frequency” regarding CRLs and chapter “Circumstance for certificate modification” for CA certificates.

2.4 Access Controls on Repositories

The ECB PKI makes the relevant information for its subscribers and relying parties (CRTs, CRLs, CP and CPS) available on its web site internally inside the ECB and anonymously and unencrypted via HTTP over the Internet. Additionally, an OCSP service must be accessible ECB internally and publicly over the internet. The ECB has implemented logical and physical security controls to restrict modifying (including adding and deleting) repository entries to authorized staff only. Any of the above-mentioned information may as well be published to internal repositories, internal access only web servers and directories or trusted third party directory services at the PKI maintainer’s sole discretion.

3 Identification and Authentication

In accordance with the corresponding Certificate Policy (CP) of the ECB PKI system.

3.1 Naming

3.1.1 Types of names

Names assigned to certificate subjects are required to be X.500 distinguished names.

See also section 3.1.1 on corresponding ECB PKI CP.

3.1.2 Need for names to be meaningful

Names are required to be meaningful in the term that the name form has commonly understood semantics to determine the identity of a person or organizational unit (e.g. in group mailboxes). Directory names should be meaningful in the term that the name form has commonly understood semantics to determine the identity of a system or functional item.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymous users as well as pseudonyms for users are not supported by the ECB PKI. Machine/device and functional (e.g., group mailbox) subjects of certificates must not be anonymous, but may use pseudonymous unique names and aliases as long as these names are unique throughout the whole ECB internal namespace / network while pseudonym and alternative names need to be matched to a responsible administrative contact / person during the registration process.

3.1.4 Rules for interpreting various name forms

- Distinguished Names must follow the X.500 naming context as well as RFC 2247
- Distinguished Names must represent the LDAP naming context referring to RFC 2247
- Name forms not encoded in Latin character sets shall be translated into Latin characters. In case of names derived from identity cards or passports, the Latin representation of the name on the MRZ of the document must be used.

3.1.5 Uniqueness of names

For user certificates the entity distinguished name must be unique over the lifetime of the issuing CA, and the subject alternative names must be unique at any given point in time. For machine certificates the subject distinguished name and subject alternative names of the certificates should be unique at any given point in time. Exceptions may be allowed for environments with technical requirements to have multiple certificates issued with identical SAN due to high availability implementations.

3.1.6 Recognition, authentication, and role of trademarks

Certificate applicants are prohibited from using names in their certificate applications that infringe upon the intellectual property rights of others. ECB, however, will not conduct explicit checks whether a certificate applicant has IPR in the name appearing in an application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark,

or service mark. ECB PKI is entitled, without liability to any subscriber, to reject or suspend any certificate signing request because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

The certificate subscriber must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. This is achieved by digitally signing the PKCS #10 or CMC certificate request with the corresponding private key. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber.

3.2.2 Authentication of organization identity

See section 3.2.2 on corresponding ECB PKI CP.

3.2.3 Authentication of individual identity

For each type of certificate, the corresponding CP will define the identification procedure for an individual.

See section 3.2.3 on corresponding ECB PKI CP.

3.2.4 Non-verified subscriber information

Any enrolment request that holds non verifiable information and / or information that cannot be validated as a valid ECB contact responsible for enrolment of the corresponding end-entity certificate is discarded without any further notice.

3.2.5 Validation of authority

Users are eligible for enrolling with the ECB PKI for user certificates if they are ECB employees or ECB contractors. This is validated by establishing a unique mapping between the user's identity, his/her smart card and his/her Active Directory user account. Enrolment requests are invalid if the user account is disabled, which indicates that the user is, at that point in time, no longer eligible to enrol. In case the end-entity is a machine or a device, enrolment requests containing alias names or pseudonyms must be validated by a responsible administrative contact in charge for the end-entity machine or device that requests certification during the enrolment process. Change of responsibility or role of the administrative contact while the ECB PKI end-entity certificate is still in use must be communicated to the responsible ECB PKI certificate and enrolment authority without being requested to do so. Unless the machine or device is considered EOL and is to be decommissioned a new administrative contact taking up the responsibilities of the former administrative contact is mandatory. This explicitly applies to virtual machines as well and is not limited to physical hardware.

3.2.6 Criteria for interoperation

See section 3.2.6 on ECB Class 2 PKI CP.

3.3 Identification and Authentication for Re-key Requests

See section 3.3 on corresponding ECB PKI CP.

3.3.1 Identification and authentication for routine re-key

Automated re-key procedures ensure that the person requesting to rekey a subscriber certificate is in fact the subscriber of the certificate. The only acceptable procedure is by proof of possession of the private key through signing the re-key request with the existing private key corresponding to the to be replaced public key of the still valid certificate about to expire. Upon re-key of a certificate, if a subscriber correctly submits the signed request with the subscriber's reenrollment information, and the enrollment information has not changed, a re-keyed Certificate is automatically issued.

See also section 3.3.1 on corresponding ECB PKI CP.

3.3.2 Identification and authentication for re-key after revocation

After revocation the initial identity validation process (see 3.2) must be followed to obtain a replacement certificate.

3.4 Identification and Authentication for Revocation Requests

Revocation requests can be raised by any ECB employee with a valid account in the ECB central Identity Governance & Access Management (IGAM) system and owner of an active ECB PKI user certificate. Authentication of the individual user identity is validated by the Service Desk support team and the minimal validation requirements the user needs to provide are UserID and ECB Badge number.

Further details are given in section 4.9.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

See section 4.1.1 on corresponding ECB PKI CP.

4.1.2 Enrolment process and responsibilities

Enrolment process

- Advanced certificate package (cryptographic token-based): Advanced User Authentication, Signature and Encryption certificates to subscribers are enrolled on a USB-based smart card according to ECB PKI certificate enrolment processes and procedures in combination with the ECB Registration Authority Officer using the certificate management portal.

  If the user does not have a smart card a new one is issued.

- Standard certificates (software-based): Standard User Authentication certificates are generated on the subscriber's laptop upon logon and after successful identification and authorization by Veridium Server through Veridium mobile app. Any user holding an active account in Active Directory and registered with Veridium system is eligible and authorized to receive such a certificate.
- Client Authentication certificates to machine subscribers are enrolled automatically via Directory Group Policies based on computer object group membership.
- OCSP Responder certificates to machine subscribers are enrolled automatically via OCSP responder machine and OCSP responder configuration.
- Code Signing, Shared Mailboxes, Service/Application Account, Server Authentication, Server Client Authentication and Domain Controller Authentication certificates to user or machine subscribers are enrolled manually according to ECB PKI certificate enrolment processes and procedures in combination with the administrative contact that

  - generates a certificate signing request for ECB internal machine and device or

  - requests a certificate for an ECB internal user, machine or device including private key generation following the ECB PKI certificate request policies enforced by the certificate management portal.

Responsibilities

For user certificates the RA operator is responsible (see also section 3.2.3 for an overview of the overall process)

- (for in-person interaction, user present) to verify the user's identity against the user's badge and establish the mapping between the user's identity, the smart card and the user's account in the Active Directory.

- (for remote activities) to establish the mapping between the user's account in Active Directory and the smart card, and later on ensure that the smart card is delivered via the predetermined processes through which the user's identity is verified during hand-over.
- (for auto-enrolled scenario: Veridium User Authentication) to validate the certificate requests received from the Veridium Credential Provider and to start issuance of certificate
- (for manual enrollment scenarios) to review the certificate requests and approve or reject them

ECB PKI engineering together with operations staff are responsible for successful enrolment of all auto-enrolled certificates. The administrative contact of each system is responsible for correct and appropriate use of the enrolled certificate based on the ECB PKI certificate policies. For manually enrolled certificate types the administrative contact as the certificate requestor on behalf is responsible for successful enrolment and use after successful issuance of the certificate according to the existing ECB PKI certificate policies.

4.2 Certificate application processing

Applications for user advanced certificates are processed via the standard ECB identity management processes. For new users the certificates are requested as part of user account creation, for existing users the process is conducted by the service desk with user presence, and the initial certificate creation of existing users is processed as part of the introduction of the smart cards for 2-factor authentication. In any case the core ECB PKI user certificate process is being followed.

Applications for standard user authentication certificates are processed via standard ECB identity governance and management processes.

Applications for machine/device certificates are part of the standard ECB IT change management process where the ECB change management policies and regulations apply.

See section 4.2 on corresponding ECB PKI CP.

4.2.1 Performing identification and authentication functions

Identification and authentication of users eligible for advanced certificates is done by an RA operator verifying the requester's identity in person by

- checking the user's badge with photograph, relying on the fact that the physical security officer issued the badge only after verification of an official picture ID document, and
- ensuring the unique mapping between the user's identity, the smart card and the Directory-based user account.

In case of remote authentication, the validation will be done using other alternate means which provide equivalent assurance to physical presence.

Identification and authentication of users eligible for Veridium user certificates is done by the Veridium Server that verifies the user's identity in the ECB Active Directory and ensures a unique mapping between the user's identity and their mobile device.

Identification and authentication of requesters for Shared Mailboxes and Service Account certificates is done by ECB Identity Governance and Access Management system.

On a technical level identification and authentication is performed by the ECB Directory. All requesting entities require a valid Active Directory account for authentication or an appropriate administrative contact. Active Directory account is required for enrolment on behalf of non-Directory-integrated devices.

4.2.2 Approval or rejection of certificate applications

Certificate applications shall be accepted upon meeting certificate criteria set forth in the respective CP.
The issuing authority may accept a certificate application not meeting the criteria by replacing, adding or deleting information in the request according to the respective CP.
Certificate applications must be rejected if the request must not or cannot be amended to meet the criteria set forth within the corresponding CP.

See also section 4.2.2 on corresponding ECB PKI CP.

4.2.3 Time to process certificate applications

Certificate requests for existing certificate profiles including a defined enrolment process will be processed according to the

- ECB IT Certificate Services Operational Level Agreement, or
- ECB IT Change Management Operational Level Agreement

Requests for new certificate types will be processed under the Change or Release Management processes in place for Certificate Services.

4.3 Certificate Issuance

See section 4.3 on corresponding ECB PKI CP.

4.3.1 CA actions during certificate issuance

During the issuance of the certificate, the ECB PKI Issuing CAs perform the following actions:

- validate the RA signature
- validate RA authority on the desired certificate profile
- validate the request subject DN and extensions against the target certificate profile
- if the certificate type permits, the CA may add, remove or alter certificate information to match the profile
- evaluate the public key to enforce a unique public key constraint throughout ECB PKI
- evaluate the subject DN to enforce a unique name constraint throughout ECB PKI
- for certificate profiles stipulating key backup, the CA will generate the key pair and escrow the private key
- store or update the subscriber end entity object in the CA database
- sign (optionally amended) the certificate signing request and issue the subscriber certificate

- store issued certificates in the CA database

4.3.2 Notification to subscriber by the CA of issuance of certificate

Notifications of certificate issuance to the subscriber may be provided by e-mail in case the process itself does not include an implicit confirmation like being offered to download the certificate.

Automated issuance processes should not cause notifications to the subscriber.

Deviations from this default behaviour may be defined on the corresponding CP for the certificate issued.

See also section 4.3.2 on corresponding ECB PKI CP.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

User certificates on smart cards

Receiving the certificate is integrated into a workflow which

- Generates new key pairs,
- Generates a random PIN for the protection of the private key against unauthorized use,
- Informs the user about the terms and conditions set out in the ECB internal rules, and about the requirement to change the initial generated PIN,
- Requests the actual issuance of the certificate, and
- Generates the certificate package on the smart card.

Completion of this process and handover of smart card and the PIN plus terms and conditions (via different channels) to the user constitutes acceptance of the certificate(s).

Manual enrollment of machine certificates

After receiving the certificate, the administrative contact responsible for the service or application the certificate was requested on behalf of, has to verify the certificates. If the certificate contains invalid information or if the key or the certificate is faulty, the administrative contact has to notify the ECB PKI operations staff immediately. In case of proper keys and certificates, a certificate acceptance is constituted.

All auto-enrolled user or machine certificates

After successful automatic certificate enrolment on the target machine a certificate acceptance is constituted.

Code Signing, Shared Mailbox, Service/Application Account certificates

Same principles as for Manual enrollment of machine certificates apply.

4.4.2 Publication of the certificate by the CA

The certificates of ECB PKI certification authorities are published in the ECB Active Directory and on the ECB PKI website. ECB PKI end-entity certificates may be published in the central repositories depending on appropriate end-entity purposes according to certificate profiles in their most current version and / or technical requirements depending on the desired use case.

4.4.3 Notification of certificate issuance by the CA to other entities

See section 4.4.3 on corresponding ECB PKI CP.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

The ECB-internal rules for user conduct contain the general security obligations which apply to all users. These guidelines can be found on the ECB intranet. They state in particular that the user is responsible for:

- securing the use of his/her personal user ID and of his/her workstation and the information therein;
- protecting and regularly changing passwords assigned to him/her, as well as protecting other security devices and tools at his/her disposal (e.g. encryption keys and smart cards);
- using individually granted access to systems and data stores solely for the purpose of the tasks he/she is instructed to perform;
- complying with legal requirements regarding, inter alia, privacy and copyright restrictions; and
- notifying local management and the IT Service Desk of any detected or suspected information security incidents, problems or shortcomings.

In case of a discovered or believed private key compromise or violation of any other requirements mentioned above and connected ECB security policies, the subscriber must immediately notify ECB Service Desk, request certificate revocation, discontinue any further use and take appropriate measures in connection with ECB PKI processes to mitigate any security risk arising from key compromise.

See also section 4.5.1 on corresponding ECB PKI CP.

4.5.2 Relying party public key and certificate usage

Relying parties must assess if a given certificate is appropriate for the specific purpose.

In particular they must verify that a certificate is used in accordance to the private key and certificate usage set forth by the associated CP. Certificates may only be relied upon if the following verification steps are successful:

- Identifying a certificate chain up to the explicitly trusted ECB PKI Root CA (trust anchor) including its subordinate CAs
- Verifying the certificate chain and end-entity certificates, including

- Verifying that the claimed identity is identical to the identity corroborated by the presented certificate
- Validation of each digital signature
- All certificate extensions including key usage and extended key usage extension matching to the appropriate and approved purposes
- Validation of validity period at the time of checking
- Conduct certificate revocation checking either by CRL or OCSP while systems supporting OCSP should prefer OCSP as the primary method for revocation checking and may fall back to CRL if the OCSP responder service is unavailable. This fall back method does not apply to an OCSP response stating the certificate as invalid.

Relying parties may not compromise the ECB PKI security measures, policies and verification steps and neither disrupt nor interfere with ECB PKI certification services. In case of any security violation the relying parties must discontinue any further usage, notify ECB Service Desk immediately and apply countermeasures as advised by ECB PKI operations team without question or delay.

4.6 Certificate Renewal

Certificate renewal as defined in RFC 3647 is the process whereby a new certificate with an updated validity period is created for the same identity and the same existing key pair without any change to other certificate data.

As a general matter, the ECB PKI does not support certificate renewal.

Instead, the only similar operation supported by the ECB PKI is most closely described as “certificate modification with re-key” (requiring a new key pair and updating identity information from the data source for subscriber information, e.g., the identity management system via Active Directory for user certificates) as further detailed in section 4.8. This operation is possible during the validity period of a certificate, whereas after expiration the certificate issuance process needs to be executed.

4.6.1 Circumstance for certificate renewal

See section 4.6.1 on corresponding ECB PKI CP.

4.6.2 Who may request renewal

See section 4.6.2 on corresponding ECB PKI CP.

4.6.3 Processing certificate renewal requests

See section 4.6.3 on corresponding ECB PKI CP.

4.6.4 Notification of new certificate issuance to subscriber

See section 4.6.4 on corresponding ECB PKI CP.

4.6.5 Conduct constituting acceptance of a renewal certificate

See section 4.6.5 on corresponding ECB PKI CP.

4.6.6 Publication of the renewal certificate by the CA

See section 4.6.6 on corresponding ECB PKI CP.

4.6.7 Notification of certificate issuance by the CA to other entities

See section 4.6.7 on corresponding ECB PKI CP.

4.7 Certificate Re-key

Certificate re-key as defined in RFC 3647 means to extend the certificate lifetime including generation of a new key pair without changing any other data in the certificate.

As a general matter, the ECB PKI does not support Certificate re-key.

Instead, the only similar operation supported by the ECB PKI is most closely described as “certificate modification with re-key” (requiring a new key pair and updating identity information from the data source for subscriber information, e.g. the identity management system via Active Directory for user certificates) as further detailed in section 4.8. This operation is possible during the validity period of a certificate, whereas after expiration the certificate issuance process needs to be executed.

4.7.1 Circumstance for certificate re-key

See section 4.7.1 on corresponding ECB PKI CP.

4.7.2 Who may request certification of a new public key

See section 4.7.2 on corresponding ECB PKI CP.

4.7.3 Processing certificate re-keying requests

See section 4.7.3 on corresponding ECB PKI CP.

4.7.4 Notification of new certificate issuance to subscriber

See section 4.7.4 on corresponding ECB PKI CP.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See section 4.7.5 on corresponding ECB PKI CP.

4.7.6 Publication of the re-keyed certificate by the CA

See section 4.7.6 on corresponding ECB PKI CP.

4.7.7 Notification of certificate issuance by the CA to other entities

See section 4.7.7 on corresponding ECB PKI CP.

4.8 Certificate Modification

While the definition in RFC 3647 for certificate modification speaks about changing any entry in the certificate except the public key, the operation the ECB PKI supports is most closely described as certification modification with re-key.

If modification of subscriber information is required a new certificate needs to be requested following revocation of the old certificates upon issuance of the new certificate. However, during the validity period of the existing certificate this can be used to prove the identity of the subscriber (this distinguishes this from the "new certificate" process). Technically a new certificate is issued containing the current information on the subscriber that is on record, together with a new key.

The revocation of the old certificate is triggered immediately, thus the revoked certificate will show up in the CRL and the OCSP status response after the next publishing cycle.

4.8.1 Circumstance for Certificate Modification

See section 4.8.1 on corresponding ECB PKI CP.

4.8.2 Who may request certificate modification

See section 4.8.2 on corresponding ECB PKI CP.

4.8.3 Processing certificate modification requests

See section 4.8.3 on corresponding ECB PKI CP.

4.8.4 Notification of new certificate issuance to subscriber

See section 4.8.4 on corresponding ECB PKI CP.

4.8.5 Conduct constituting acceptance of modified certificate

See section 4.8.5 on corresponding ECB PKI CP.

4.8.6 Publication of the modified certificate by the CA

See section 4.8.6 on corresponding ECB PKI CP.

4.8.7 Notification of certificate issuance by the CA to other entities

See section 4.8.7 on corresponding ECB PKI CP.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

Certificate revocation is the action that makes a certificate invalid prior to its expiry date.

A certificate revocation must be performed when:

- the ECB PKI Certification Authority which issued the certificate ceases operations for any reason
- the private key associated with the public key listed in the certificate or the media holding such private key is suspected or known to have been stolen, disclosed in an unauthorized manner or otherwise compromised
- the key, the USB token / smartcard and/ or device is stolen / lost / retired and the certificate is still in its validity period

- there is a violation by the subscriber of any of its material and essential obligations under the ECB PKI CP and CPS or the subscriber agreement
- there is a given determination, in the ECB PKI Authority's sole discretion, that the certificate was not issued in accordance with the terms and conditions of the ECB CP and CPS
- there is a determination by the ECB PKI authority that continued use of the certificate is inappropriate or injurious to the proper functioning or intent of the ECB PKI
- the subscriber is no longer authorized to have an ECB PKI Certificate
- The certificate has undergone modification with re-key, and thus the old one shall no longer be valid.

The main effect of the revocation regarding the certificate is the immediate termination of its term of validity, with which the certificate becomes invalid.

4.9.2 Who can request revocation

The following persons or roles can request a revocation for certificates

- ECB PKI certificate subscribers
- ECB PKI associated RAs
- ECB PKI CAs
- Administrative contact or security officer for the certificate
- Line Manager for certificates in the sphere of his or her responsibility
- Any authorized member of European Central Bank's Information Security Team

4.9.3 Procedure for revocation request

A revocation request for user certificates can be raised by

- visiting ECB IT Service Desk office
- calling ECB IT Service Desk
- sending an email to the ECB IT Service Desk
- using another written or electronic form, for instance via ECB IT Service Desk Portal

In all cases a ticket linked to the subscriber (for user certificates identical with the subject) is created in the IT service management tool. The subscriber is informed about status changes of the ticket via email, which includes the processing of the revocation request.

4.9.4 Revocation request grace period

The revocation request grace period is the maximum period between when a subscriber suspects compromise or loss of control of the Private Key has occurred and when the incident is reported to ECB IT Service Desk. As a general rule, there is no revocation request grace period. All revocation requests are considered effective with the request reaching the ECB Service Desk or ECB PKI operations staff and appropriate measures are started to be applied immediately according to the ECB PKI service level agreement

4.9.5 Time within which CA must process the revocation request

ECB has a 24/7 Service Desk and second level support teams and upon request they can trigger the certificate revocation which takes effect immediately, together with the publishing of a new CRL.

4.9.6 Revocation checking requirement for relying parties

ECB PKI relying parties must check the certificate revocation status prior to making decisions based on the information derived from the certificate. This revocation status check must be performed during initial authentication and should be repeated for session time extension according to the underlying business and security requirements.

See also section 4.9.6 on corresponding ECB PKI CP.

4.9.7 CRL issuance frequency

ECB PKI base CRL issuance frequency

Certificate Authority	Publication	Overlap	Lifetime
ECB RSA AV Root CA 01	6 Months	2 Months	8 Months
ECB RSA AV Sub CA 01	4 Days	2 Days	6 Days
ECB RSA AV Sub CA 02	4 Days	2 Days	6 Days
ECB RSA Root CA 01	6 Months	2 Months	8 Months
ECB RSA Sub CA 01	4 Days	2 Days	6 Days
ECB RSA Sub CA 02	4 Days	2 Days	6 Days
ECB RSA Sub CA 03	4 Days	2 Days	6 Days

4.9.8 Maximum latency for CRLs

The maximum latency for publishing ECB PKI CRLs is 60 minutes following certificate revocation. Certificate status information available via OCSP is updated immediately.

4.9.9 On-line revocation/status checking availability

OCSP (Online Certificate Status Protocol) is available to ECB PKI participants in the ECB's internal network as well as externally and implemented to support revocation checking of end-entity certificates. The OCSP service, as an alternative to CRL download, is provided by the OCSP responders within the ECB PKI environment supporting internal clients using different installations / machines to mitigate security risks.

The OCSP responders are authorized by ECB RSA issuing CAs using OCSP response signing certificates issued by each Sub CA.

The ECB PKI OCSP responders rely on up-to-date CRL information that is retrieved automatically on a regular basis.

ECB PKI OCSP responder accuracy in immediate revocation scenarios when CRLs are published manually by the ECB PKI operations staff after revocation of important certificates is due to caching

mechanisms in combination with regular CRL retrieval interval expected not to exceed 60 minutes under normal operational conditions.

On-line revocation/status checking shall be available at http://ocsp.ecb.europa.eu using OCSP via HTTP. Where Security considerations demand it, this service may optionally be available via HTTPS in addition.

4.9.10 On-line revocation checking requirements

OCSP revocation checking is mandatory for any user authentication requirement. It is recommended for all certificate validity checking due to its near real time accuracy and lower traffic requirements compared to CRL publishing latencies and repetitive full CRL downloads.

See also section 4.9.10 on corresponding ECB PKI CP.

4.9.11 Other forms of revocation advertisements available

See section 4.9.11 on corresponding ECB PKI CP.

4.9.12 Special requirements re key compromise

See section 4.9.12 on corresponding ECB PKI CP.

4.9.13 Circumstances for suspension

As a general rule, ECB PKI does not support certificate suspension.

4.9.14 Who can request suspension

See section 4.9.14 on corresponding ECB PKI CP.

4.9.15 Procedure for suspension request

See section 4.9.15 on corresponding ECB KI CP.

4.9.16 Limits on suspension period

See section 4.9.16 on corresponding ECB PKI CP.

4.10 Certificate Status Services

ECB provides CRLs for the public CAs it operates. They can be downloaded from https://cpki.ecb.europa.eu/ along with the corresponding CA certificates.

In addition, ECB operates a public OCSP responder that is available at http://ocsp.ecb.europa.eu.

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

Certificate Status services are available 24/7 free of charge.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

CRL and OCSP subscription ends when the ECB PKI CA certificate is expired, or the ECB PKI CA and connected PKI service is terminated.

- All CRL and OCSP subscription ends, when the ECB PKI AV Root CA 01, respectively ECB RSA Root CA 01 certificate in question is expired or the respective root CA service is terminated.
- CRL and OCSP of ECB PKI sub CAs subscriptions end, when the respective ECB PKI Sub CA certificate is expired or the ECB PKI Sub CA service is terminated.

See section 4.11 on corresponding ECB PKI CP.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

See section 4.12.1 on corresponding ECB PKI CP.

4.12.2 Session key encapsulation and recovery policy and practices

See section 4.12.2 on corresponding ECB PKI CP.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

The central components of the ECB PKI are hosted in the ECB secure data centres conforming to the general ECB standards for physical and environmental security and are operated by authorised personnel of the ECB's IT department under the terms of its general regulations and (security) policies. The buildings hosting ECB PKI infrastructure are equipped with access control systems that permit only authorized personnel to enter; all critical ECB PKI operations are being carried out inside physically secure facilities.

In particular the following physical security measures are implemented:

- Surveillance cameras,
- Guards,
- Absence of windows,
- Physical access control based on badge and biometrics,
- Fire detection and prevention systems: detectors and extinguishing systems,
- UPS,
- Cooling.

All central infrastructure components of the ECB PKI, such as CA servers and OCSPs, are located in those data centres.

The CA limits access to hardware and software to those personnel performing a trusted role. The CA controls access to its components by sufficient access control mechanisms.

The CA components are operated in a secure environment, where only trusted and authorized staff can access these components.

Furthermore, the components of the RA are operated by the ECB DG-IS IT department under the terms of its general regulations and policies as well as dedicated procedures.

5.1.1 Site location and construction

The ECB's data centre locations are designed to provide sufficient protection for the hosted components of the ECB PKI from physical and environmental impact. This includes a physical perimeter designed to integrate with physical access control measures to ensure that only authorised personnel can physically access to the central infrastructure components of the ECB PKI as well as supporting systems. For redundancy two physically separate sites are used with sufficient distance between them.

5.1.2 Physical access

ECB PKI critical components are located inside a protected security perimeter with alarms and physical protection against intrusion. Physical access of individuals to the building is controlled at the entry and exit, with authorisation provided only in case of a need to access. Access authorisations are reviewed

periodically and corrected where necessary. The deployed access control measures require a badge and biometrics for authentication before physical access is granted (if authorised).

5.1.3 Power and air conditioning

ECB PKI infrastructure systems are located in data centre rooms fed by redundant power supplies, connected to an UPS. An HVAC system provides cooling and atmospheric control within the data centre rooms.

5.1.4 Water exposures

Water detectors are in place, and constructive measures have been taken to limit the impact of water leakage.

5.1.5 Fire prevention and protection

ECB PKI components are located in data centre rooms with fire detectors and fire extinguishing systems.

5.1.6 Media storage

ECB PKI systems are redundant and distributed over separate protected ECB datacenter location which protect against unauthorised access, theft and physical deterioration or destruction of storage media from environmental impact.

5.1.7 Waste disposal

Waste management measures have been put in place to guarantee destruction of critical material and removable media.

5.1.8 Off-site backup

ECB PKI infrastructure systems are located in two ECB datacentres which are physically separated, thus providing sufficient redundancy in case of a data centre loss.

Backups of online systems are saved onto network storage in separate redundant ECB datacenter locations. Encrypted offline system backups are saved onto encrypted portable media and stored in a fireproof safe outside the datacenter on secure ECB premises.

5.2 Procedural Controls

Personnel within the CA and RA serve in trusted roles, particularly those who have access to or control over cryptographic keys and operations. A trusted role refers to one who’s incumbent functions can introduce security problems if not carried out appropriately (whether unwillingly, accidentally or deliberately).

Strong mechanisms for identification, authentication and authorization are used as far as possible.

5.2.1 Trusted roles

The ECB PKI recognizes the following trusted roles associated to its operations:

- PKI Architect: responsible for the architecture and development of the PKI, including the related processes, makes decisions and performs tasks related to the lifecycle of the CAs and the respective PKI architecture; appoints the staff for other trusted roles except auditors
- Security Officer: responsible for evaluating the claims in certificate requests against the respective set of rules, deciding to either deny or approve them; also responsible for administering the implementation of security policies and practices
- System (PKI) Administrator: responsible for the technical lifecycle of the PKI, i.e., installation, configuration, and technical operation of the PKI
- System (PKI) Operator: responsible for operating the PKI system on a day-to-day basis, performing tasks such as fixing technical issues or backup and restoration
- Registration Officer: responsible for approval of certificate issuance and revocation/suspension
- System (PKI) Auditor: responsible for auditing the entire PKI, including issuance of certificates, PKI configuration data, log files and documentation. They ensure that the operation of the PKI is in compliance with the applicable regulations.
- Smart Card Custodian: responsible for safekeeping one or more smart cards and their associated PINs

Descriptions of the operational duties of these roles are provided in the internal operational documentation of ECB.

5.2.2 Number of persons required per task

CA cryptographic operations in the ECB PKI are protected by HSMs. For sensitive key operations at least multi person control / multi-eye principle is performed and required on the HSM.

Task	Role(s)	Quorum
Restoring PKI master backup secret	PKI Administrators	3 of 5
Root CA key generation/re-key	CA Officer	3 of 3
Root CA key activation	CA Officer	3 of 3
Root CA CRL creation	CA Officer	3 of 3
Root CA OCSP responder certificate signing	CA Officer	3 of 3
Sub CA certificate signing	CA Officer	3 of 3
Sub CA revocation	CA Officer	3 of 3

5.2.3 Identification and authentication for each role

In-person-proof and smartcard authentication for HSM transactions is performed for each role.

Role	Identification	Authentication
PKI Administrator	holding a personally assigned smart card of the MBK card set	smart card PIN entry
CA Officer	holding a personally assigned smart card of the ACS	smart card PIN entry
	in possession of the private key to an authorized administrator certificate	TLS client certificate presentation within enhanced security administration environment
RA Officer	member of the IGAM group for RA officers	presentation of TLS client certificate or PAM authentication within enhanced security administration environment
PKI Auditors	member of the IGAM group for PKI Auditors	presentation of TLS client certificate or PAM authentication within enhanced security administration environment

5.2.4 Roles requiring separation of duties

CA cryptographic operations in the ECB PKI are protected by HSMs. For sensitive key operations the quorum required to perform such actions is divided between various teams performing Security Advisory, Operations Support and Engineering of the ECB PKI systems.

The RA Operators role prevents them from any HSMs access or System Administrator privileges.

The role of System Administrator (both Engineering and Operations Support) and Security Advisor (both for Governance Policies and Operations Support) are mutually exclusive.

The ECB PKI Auditor and security testing roles are assigned outside of the ECB PKI responsible teams.

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

Persons bestowed with trusted tasks within ECB PKI operations must have proven competence and experience that is appropriate for the respective tasks. Persons holding a trusted ECB PKI role must follow the in place clearance and confidentiality agreements.

5.3.2 Background check procedures

Based on the ECB standard identity and access management regulations background checks for every person operating the ECB IT environment are performed.

These checks include:

- Government issued criminal record certificate
- signed ECB Privacy Statement and Self-Declaration for the Security Clearance

5.3.3 Training requirements

The ECB ensures that employees receive the required training to perform their job responsibilities competently and satisfactorily. The ECB periodically reviews its training program.

5.3.4 Retraining frequency and requirements

The ECB periodically re-trains employees. Frequency and training contents are individually tailored to each employee depending on his job profile and responsibilities. Re-training ensures that employees maintain the required level of proficiency to perform their job.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

In case of unauthorized actions or violation of ECB corporate policies and procedures human resources and line management will initiate appropriate disciplinary actions.

5.3.7 Independent contractor requirements

Definitions in section 5.2 also apply to ECB certified independent contractors and IT Service Partners.

5.3.8 Documentation supplied to personnel

ECB PKI operations staff personnel are required to read ECB PKI CP and CPS documents including accompanying documents. Additionally, ECB PKI operations personnel receive further documents according to their respective job responsibilities.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

All major events of ECB PKI certification services are recorded according to ECB DG-IS IT Department Standard Server logging mechanisms.

For all ECB PKI CA or ECB PKI related components additional application-level logging is conducted, in particular for all events related to the management of the CA and the handling of certificates.

The server logging standard procedures and requirements for the ECB DG-IS IT department shall apply to the ECB PKI central components, capturing all major events.

Furthermore, all major events such as:

- Change CA configuration.
- Change CA security settings.
- Certificate lifecycle: Issuance, revocation and other certificate related requests.
- Publishing of CRLs.
- Storage and retrieval of archived keys.

are audited on the ECB PKI CAs. Annex 1:Types of events logged by the CA has an exhaustive list of the event types logged.

The events include the “TimeStamp” field, which is the time, in milliseconds since epoch, when the event occurred.

The logging of all events relating to the preparation of secure user devices is handled by the Credential Management System (CMS).

5.4.2 Frequency of processing log

Audit log events mirrored to the external syslog device provide a continuous monitoring opportunity. The audit log is archived during daily online system backup procedures. Offline CAs are backed up manually at least every 6 months during CRL signing. Manual log processing occurs following alarms or anomalous events.

5.4.3 Retention period for audit log

Recorded events shall be retained in the audit log for at least 3 months. The components of the ECB offline Root CAs shall keep recorded events for at least 6 months.

5.4.4 Protection of audit log

To preserve the confidentiality, audit logs are accessible by authenticated administrators and auditors only. They are recorded in an integrity protected log device in the CA database. Database integrity protection consists of an additional rowProtection column in all protected tables. Each log event records an identification of the CA appliance node and a monotone sequence number that is part of the integrity protected data. Audit logs are enclosed in the periodic PKI backup procedures.

5.4.5 Audit log backup procedures

Audit logs are backed up and included in the CA integrity protected database backup. An automated backup is scheduled daily for online CAs and manual backups are done at least semi-annually for offline CAs during CRL renewal activity or other Root CA related tasks.

5.4.6 Audit collection system (internal vs. external)

The ECB PKI audit logs shall store audit log events internally to the hardware appliances CA database. In addition, ECB PKI is on-boarded to the ECB SIEM solution, which is an independent internal audit collection system in place to collect and aggregate all relevant log information from the several ECB PKI systems. PKI audit log events are mirrored to the appliances syslog which are then forwarded to SIEM syslog server for continuous evaluation and archival.

5.4.7 Notification to event-causing subject

Not applicable.

5.4.8 Vulnerability assessments

A part of the general ECB security management and maintenance activities regular vulnerability assessments and security checks are performed on every system within the ECB PKI. In addition, audit events exported to external syslog are continuously monitored by SIEM for potential attempts to breach ECB PKI system security.

All ECB PKI components must be handled according to the ECB vulnerability and patch management procedures.

In addition, a penetration test will be performed every 3 years on the ECB PKI systems.

5.5 Records Archival

Certification application information for certificates is archived as part of the standard ECB and ECB PKI change management process.

5.5.1 Types of records archived

ECB PKI archives all audit data and certificate application information.

5.5.2 Retention period for archive

Retention period for archive is according to the standard ECB PKI and ECB change management archival process.

5.5.3 Protection of archive

Archive access must be limited to trusted auditors only. The archive shall be protected against modification by securely storing it to write once media that should be kept in a fireproof safe to protect it from deletion and destruction. To prevent media deterioration during the retention period of the archive, archive data may periodically be migrated to fresh media. Log entries are stored in hardware and software independent formats like XML to protect audit logs against obsolescence of hardware, operating systems, and other software.

5.5.4 Archive backup procedures

Not applicable.

5.5.5 Requirements for time-stamping of records

Audit logs, archived records, certificates, CRLs, and other entries contain time and date information. The ECB synchronizes all system date and times. There is no special RFC3161 compliant cryptographic time stamping service in place.

5.5.6 Archive collection system (internal or external)

Not applicable.

5.5.7 Procedures to obtain and verify archive information

Not applicable.

5.6 Key Changeover

The key changeover for the ECB PKI CA key pairs is timed according to the maximum key lifetimes and renewal periods set out in the corresponding ECB PKI CP.

The CA key changeover process is designed so that

- It is guaranteed at all times that a CA's certificate lifetime encompasses all lifetimes of certificates, which are subordinate to it in the hierarchy.
- A new key pair of a CA is generated before the point in time where its remaining lifetime equals the subordinate certificate's validity period to avoid lifetime cuts in the respective certificate chain.
- At the latest from the point in time where a CA's key pair remaining lifetime equals the subordinate certificate's validity period will all certificates be signed by the new CA key pair.
- However, a CA continues to issue CRLs signed with the original CA private key until the expiration date of the last issued certificate using the original key pair has been reached

Following an ECB PKI CA re-key, the new public key shall be provided to its users by the same procedure for providing the current key.

5.7 Compromise and Disaster Recovery

ECB has implemented a high security environment according to commonly accepted best practices to minimize the risk and potential impact of a key compromise or disaster. The main goal is to restore ECB PKI operations within a reasonable period of time in the event of a CA key compromise or disaster or any failure to related PKI components.

5.7.1 Incident and compromise handling procedures

To manage all operational processes, the ECB PKI operations teams and the ECB internal IT department has adopted the ITIL best practice model. In particular the ECB operates a Service Desk which receives and processes all service calls including ECB PKI related processes and procedures. Further ITIL processes like incident and problem management are implemented.

The ECB PKI is part of Technical Service "Certificate Services" which is on-boarded in the ECB Service Portfolio and is compliant with ECB ITSCM process performing regular test exercises on RTO/RTC for the service. ECB PKI system is configured to use redundancy for most critical components, procedures for backup and restore scenarios have been prepared to describe steps to be taken in case of a disaster, regular restore tests are taking place periodically to ensure completion and accuracy of the procedures and backups.

5.7.2 Computing resources, software, and/or data are corrupted

The ECB PKI Root CAs and its subordinate online issuing certification authorities and related PKI online service components are implemented as a 24x7 high availability cluster solution. The ECB PKI Root

certification authorities are implemented using a cold standby solution, providing fast replacement of required Hardware and Software components in case of failure or data corruption.

The issuing certification authority servers and online PKI service components underlie a daily backup process. The backup for the ECB PKI Root certification authorities is conducted on occasion in a reasonable timeframe, at least before any changes to these systems within 6 months.

In the event of suspected or evident corruption of computing resources, software and/or data, downstream ECB PKI operations shall cease until a secure environment has been re-established by wiping/replacing affected hardware and setting up from known good backups or from scratch following the ECB PKI installation and configuration documentation. Any certificate that cannot transparently tracked back to its authorized issuance (e.g. due to audit log or subscriber/application data corruption) must be revoked. The new public key (if applicable) shall be provided to its users by the same procedure for providing the current key.

Subjects affected by this event shall be re-certified according to the initial certification process.

5.7.3 Entity private key compromise procedures

If an ECB PKI entity private key compromise is suspected or discovered it should directly be reported to the ECB IT Service Desk and the affected entity certificate must be revoked and re-keyed immediately.

Notification to subscribers and other entities with which CA has agreements or other form of established relations such as relying parties and CAs will be conducted using the standard ECB channels like Intranet announcements and emails. The notification will include information that certificates and revocation status information issued using the CA key may no longer be valid.

In case any of the algorithms, or associated parameters, used by the CA or its subscribers become insufficient for its remaining intended usage, notification to all subscribers and other entities with which CA has agreements or other form of established relations such as relying parties and CAs will be conducted and revocation of the affected certificate will be performed.

In case of a re-key, the re-keyed entity may choose to re-issue otherwise unaltered downstream entities certificates signed by the new replacement key. Such replacement certificates and the new public key distribution and provisioning of the new public key should be provided to the subscribers by the same procedures for providing the compromised key and existing certificates.

5.7.4 Business continuity capabilities after a disaster

The general disaster recovery procedures are defined as part of the general ECB Business Continuity Plans including the ECB PKI Operations Guide. ECB PKI systems are redundantly distributed over failover clusters spanning to a remote hot-site to seamlessly recover operations. Additional cold spare systems are available to replace failing/lost hardware appliances and master backup keys can be restored using the redundant sharded MBK smart card set held by the ECB PKI administrators and site redundant backups.

In order to restore ECB PKI systems, including its private keys, in case of a disaster requires:

- New systems with hardware and software as the original ones
- Installation and restore procedures
- Backup of the systems prior to the disaster
- Administrator cards for the HSMs

5.8 CA or RA Termination

If ever necessary for ECB to terminate its ECB PKI operations, ECB makes a reasonable effort to notify all involved parties e.g., subscribers, relying parties, and other affected entities within a reasonable timeframe in advance.

Further, ECB guarantees the preservation of the ECB PKI CA's archives and records for the period of time as determined in section 5.4.3 Retention period for audit log for audit logs and in section 5.5.2 Retention period for archive for the archive. ECB will develop a detailed termination plan whenever necessary at a future point in time.

The terminal plan will address the following notification of the termination to affected entities, such as subscribers and relying parties, taking into account the aim to minimize the disruption to subscribers and relying parties:

- What type of support services will be continued, migrated, and/or discontinued and adjust authorizations and related process and systems accordingly
- How and if revocation and the issuance of CRLs will be continued; in any case the ECB preserves the ECB PKI CA's archives and records for the period of time as determined in section 5.4.3 "Retention period for audit log" for audit logs and in section 5.5.2 "Retention period for archive" for the archive
- Decisions if valid certificates of subscribers and subordinate CAs will be revoked
- Possible issuance of replacement certificates by a successor CA
- Destruction or withdrawal of the CA's private key and the respective cryptographic devices
- Provisions needed for the transition of the CA's services to a successor CA

6 Technical Security Controls

6.1 Key Pair Generation and Installation

Key pair generation and installation is considered for the ECB PKI Certificate Authorities, Registration Authorities and all ECB PKI certificate subscribers.

6.1.1 Key pair generation

Cryptographic keys of ECB PKI components including Root CA and all subordinate CA's are generated in hardware security modules with the FIPS 140-2 Level 3 certification. It is assured that trustworthy systems are used for the key generation. The process to assure this trustworthiness and required procedures, as well as the detailed definitions of the key generation procedures is not part of this document and outlined in the Key ceremony documentation that can be provided upon request. Generation of CA keys follows the requirements of FIPS 140-2 Level 3.

Generation of subscriber key pairs is performed at the time of registration, and it must meet the following criteria:

- Strong user authentication (e.g. smartcard logon) key pairs are generated in smart cards with CC EAL 4+ or FIPS 140-2 level 3 certification or higher
- User signature (e.g. document/mail signing) key pairs are generated in smart cards with CC EAL 4+ or FIPS 140-2 level 3 certification or higher.
- Data encryption (e.g. to encrypt data sent between systems or users) key pairs are generated in secure environments at least meeting the requirement of FIPS 140-2 Level 3 and installed into smart cards with CC EAL 4+ or FIPS 140-2 level 3 certification or higher. A copy of the exported keys may be stored for approved private key archival/backup/escrow scenarios and requires encryption where the decryption key material is under the issuing CA's control and has been generated in an HSM.
- Remote access authentication (e.g. VPN client authentication), machine, Code Signing, Application/Service Account, Shared Mailbox, Mobile Device, User Standard authentication key pairs are generated at least in a software cryptographic module with FIPS 140-2 level 1 certification.

6.1.2 Private Key delivery to subscriber

ECB PKI CA private keys

CA private keys, which are being used for signing operations, are stored locally using the Security Environment of the HSM protected key store. Therefore, no additional private key delivery process to the CAs is required.

ECB PKI subscriber private keys (user/machine)

See section 6.1.2 on corresponding ECB PKI CP.

Standard User Authentication certificates

The delivery of private keys to the certificate subscribers in case of standard certificates, is conducted by Veridium RA server in a secure way, encrypted both in transit and at rest..

Shared Mailbox certificates

The delivery of private keys to the certificate subscribers in case of standard certificates, is conducted in a secure way by means of an authenticated web portal. The certificate subscriber receives the key pair (e.g. PKCS#12 file secured by a passphrase) to provide end to end confidentiality and mutual authentication of all related parties and PKI components.

Application/Service Account certificates

Same applies as for Shared Mailbox certificates

Technical certificates

Same applies as for Shared Mailbox certificates.

6.1.3 Public key delivery to certificate issuer

All public keys are delivered electronically to the ECB PKI certificate issuer (Certificate Authority) by CMC (Certificate Management Messages over CMS – Cryptographic Message Syntax) or PKCS #10 (Public Key Cryptographic Standard No. 10).

The current ECB PKI implementation of CMC follows RFC 5272 while the certificate service request (CSR) or PKCS #10 implementation is conducted according to RFC 2986.

https://www.ietf.org/rfc/rfc5272.txthttp://www.ietf.org/rfc/rfc2986.txt

Corresponding protocols for public key delivery rely on HTTP, RPC, SMB or SMTP transport Protocols.

6.1.4 CA public key delivery to relying parties

The CA public keys are encapsulated in the CA certificates. ECB LDAP directory and ECB PKI web site infrastructure provide the main location for CA certificates. Delivery of public keys to relying parties is initiated when downloading the CA certificates by LDAP or HTTP. It is also reasonable to send the ECB PKI CA certificates via email or file transport to subscriber or relying party while sending HTTP based URLs / links to the official ECB PKI web site and the respective HTTP locations is recommended.

6.1.5 Key Sizes

ECB PKI CA Key Size and Algorithms

Certification Authority	Key Size and Key Algorithm
ECB RSA AV Root CA 01	4096 Bit RSA
ECB RSA AV Sub CA 01	4096 Bit RSA
ECB RSA AV Sub CA 02	4096 Bit RSA
ECB RSA Root CA 01	4096 Bit RSA
ECB RSA Sub CA 01	4096 Bit RSA
ECB RSA Sub CA 02	4096 Bit RSA
ECB RSA Sub CA 03	4096 Bit RSA

ECB PKI Subscriber Key Size

Entity	Key Size and Key Algorithm
Subscriber	2048 Bit RSA 3072 Bit RSA 4096 Bit RSA

See section 6.1.5 on corresponding ECB PKI CP.

6.1.6 Public key parameters generation and quality checking

ECB PKI trust chain

Public Key Algorithm 1.2.840.113549.1.1.1 (RSA)

Signature Algorithm 1.2.840.113549.1.1.11 (SHA-256 with RSA Encryption)

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

ECB RSA AV Root CA 01 key usage

Certificate Signing

CRL Signing / Off-line CRL Signing

Digital Signature

ECB RSA AV Sub CA 01 key usage

Certificate Signing

CRL Signing / Off-line CRL Signing

ECB RSA AV Sub CA 02 key usage

Certificate Signing

CRL Signing / Off-line CRL Signing

ECB RSA Root CA 01 key usage

Certificate Signing

CRL Signing / Off-line CRL Signing

Digital Signature

ECB RSA Sub CA 01 key usage

Certificate Signing

CRL Signing / Off-line CRL Signing

ECB RSA Sub CA 02 key usage

Certificate Signing

CRL Signing / Off-line CRL Signing

ECB RSA Sub CA 03 key usage

Certificate Signing

CRL Signing / Off-line CRL Signing**ECB PKI Subscriber Certificate Key Usage**

ECB RSA Server Authentication certificate	Key Encipherment, Key Agreement
ECB RSA Client/Server Authentication certificate	Key Encipherment, Key Agreement Digital
ECB OCSP Response Signing	Digital Signature
ECB RSA AV User Authentication	Digital Signature
ECB RSA AV User Encryption	Key Encipherment
ECB RSA AV User Signature	Digital Signature (non-repudiation)
ECB RSA User Client Authentication	Digital Signature, Key Encipherment
AdminEndEntity	Digital Signature, Non-Repudiation, Key Encipherment
ECB RSA Code Signing	Digital Signature (non-repudiation), Key Encipherment
ECB RSA Application/Service Account	Digital Signature, Key Encipherment
ECB RSA Veridium User Authentication	Digital Signature
ECB RSA Shared Mailbox	Key Encipherment

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

- All ECB PKI RSA Root CA, Issuing CA and OCSP key pairs are generated by a hardware security module (HSM) that complies at least with FIPS 140-2 Level 3.
- ECB RSA AV Sub CA 01 subscriber user key pairs (authentication, signature, and encryption) are generated on USB tokens / smartcards with CC EAL 4+ or FIPS 140-2 level 3 certificates. User key pairs used for encryption allow a one-time export of the private key with the certificate service request (CSR) for key archival.
- Other ECB PKI subscriber user key pairs (e.g. remote access, shared mailbox, standard user/account authentication) must be generated in at least FIPS 140-2 level 1 compliant software cryptographic providers.
- ECB PKI machine subject key pairs should be generated in at least FIPS 140-2 level 1 compliant software cryptographic providers.

See also section 6.2.1 on respective ECB PKI CP.

6.2.2 Private Key (n out of m) Multi-Person Control

Not applicable for ECB PKI subscriber private keys.

On ECB PKI root CA components cryptographic operations and private key access requires multi person based authorization. This is cryptographically enforced on HSM access by requiring a quorum of 3 out of 5 keys on an ACS spread over multiple secure authorization smart cards issued to multiple trusted persons.

6.2.3 Private Key escrow

Private Key escrow is supported only for advanced encryption certificates and the escrow is performed by the subscriber themselves.

6.2.4 Private Key backup

Online CA keys are backed up within the scheduled backup procedures. The CA keys are protected by the HSM and therefore only encrypted CA keys are backed up. The CA key backup can only be used in conjunction with the assigned HSM and authentication mechanisms in combination with appropriate multi-person control wherever applicable.

The ECB PKI Root CA key backup must be copied manually to data storage devices which are to be kept in a secure place. The Root CA backups are performed each time before any changes are made to the respective systems, at least every 6 months.

6.2.5 Private Key archival

ECB PKI subscriber private keys that are used to encrypt data sent between systems or users are stored in an encrypted form in EJBCA database and are backed up and archived as part of the configured backups.

6.2.6 Private Key transfer into or from a cryptographic module

Private Key transfer from a cryptographic module protected storage is prohibited. Private keys stored in software cryptographic storages (e.g. certstore/keyring) must not be exportable. For key archival/backup/escrow purposes on user encryption certificates, private keys may be generated in a trusted secure environment and transferred into approved smart cards via encrypted transfer channels.

6.2.7 Private Key storage using cryptographic module

- ECB PKI Root CA private keys are protected by a Hardware Security Module (HSM) in conjunction with a multi-person control key access authorization implementation.
- ECB PKI Sub CA and OCSP private keys are protected by a Hardware Security Module (HSM).
- All ECB PKI advanced subscriber (user) key pairs (authentication, encryption and signature) are protected on smartcards with CC EAL 4+ or FIPS 140-2 level 3 certification.
- The ECB PKI subscriber (user) key pairs for Veridium User Authentication or VPN client authentication are protected by software cryptographic module certified according to FIPS 140-2 level 1.

- The ECB PKI subscriber (user) key pairs for Code Signing, Application/Service Account, Shared Mailbox are protected by software cryptographic module certified according to FIPS 140-2 level 1.

6.2.8 Method of activating private key

- ECB PKI Root CA private keys must be activated by presenting a full multi person control ACS including individual PIN entry to unlock the HSM slot containing the desired private key. Activation lasts until the HSM slot is locked by administrator command or upon returning the CA appliance into offline mode or power it down. Initial key generation was conducted during the key ceremony process outlined in the key ceremony documentation referenced in the document control section.
- ECB PKI Sub CA private keys are activated automatically on boot to enable PKI automation and redundant fail over cluster operations for high availability. Initially, ECB PKI Sub CA private keys have been activated before first use via the procedure to create and install the corresponding certificate (issued by the ECB PKI Root CA under multi-person control), thus implicitly exercising multi-person control for key activation. Initial key generation was conducted during the key ceremony and installation process outlined in the key ceremony documentation referenced in the document control section of this document.
- OCSP response signing keys are activated automatically by a Hardware Security Module (HSM) at first use.
- ECB PKI uses only hardware-based keys for user advanced authentication, signature and encryption certificates for users on USB-based smartcards. Activation of private keys is performed by successful PIN provision after presenting the corresponding USB-based smartcard.
- ECB PKI uses software-based keys for end-entity VPN client authentication certificates for users on physical computers. Activation of private keys is performed by successful domain logon of the user using the USB based smartcard.
- ECB PKI uses software-based keys for end-entity Veridium User authentication certificates for users on physical computers. Activation of private keys is performed by successful offline logon of the user using VeridiumID Authenticator authentication method.
- ECB PKI uses software-based keys for end-entity certificates on machines besides special PKI components. Activation of private keys is either performed by successful domain logon of the machine or user or by successful start of the respective network device.
- ECB PKI delivers standard encryption and application account certificate private keys in a PKCS#12 file protected by a password. The password is required to activate the private key.

6.2.9 Method of deactivating private keys

- ECB PKI Root CA private keys are deactivated by returning the CA appliance to its offline mode after maintenance.
- ECB PKI Sub CA and OCSP responder private keys are deactivated by locking the HSM slot on or powering down the hardware appliance.

- Shutdown of the subscriber machine will deactivate the private keys on the local machine.
- Withdrawal of the USB-based smartcard from the USB port will deactivate the contained private keys.

6.2.10 Method of destroying private keys

Destroying CA keys

CA key destruction is performed by a PKI Administrator by deleting the key from its HSM slot on the CA appliance.

Destroying user keys on smartcards

User private keys stored on a USB-based smartcard are destructed when the USB-based smartcard is retired. This process requires the physical return of the USB-based smartcard. In case the USB-based smartcard is not available the certificate will be revoked. In case the USB-based smartcard is returned in a damaged state to ECB Service Desk, the USB-based smartcard is permanently decommissioned by physical destruction using a shredder. In any case the archived private keys for a user's encryption certificates are still kept in the archive.

Destroying user software keys

User private keys (for user client authentication) stored on the ECB computers in user personal store are destructed when the certificate is revoked or deleted from the store.

The private keys for shared mailboxes or service accounts are destroyed by overwriting the key either through renewal or through deletion.

6.2.11 Cryptographic Module Rating

Cryptographic Module Rating is listed in Section 6.2.1 Cryptographic module standards and controls.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The CA public key and subscriber public key certificates are archived in the CA database.

The CA database is backed up according to the procedures described in section 5.5.4 "Archive backup procedures".

6.3.2 Certificate operational periods and key pair usage periods

For ECB PKI the key pair usage period relies directly on the certificate operational period. Certificate renewal is performed only by modification with re-keying. Therefore, the certificate operational period matches the key pair usage period.

The following certificate operational periods are defined within ECB PKI certification services.

Certificate Type	Validity Period	Renewal Period
ECB PKI Root CAs	20 years	14 years

ECB Sub CAs	10 years	7 years

ECB PKI subscriber key usage periods

For end entity certificates, operational periods and key usage periods are specified in the corresponding CP document.

6.4 Activation Data

6.4.1 Activation data generation and installation

- Activation data generation for machine subscriber keys is performed automatically during machine setup by the local security subsystem. Only local system access is granted to the key store.
- Activation data generation for user subscriber keys for VPN client authentication on ECB computers is performed automatically after user logon and activation of relevant Group Policy Object settings.
- Activation data generation for user subscriber keys for Veridium user authentication on ECB computers is performed automatically at user offline logon.
- Activation data generation for user subscriber keys for Code Signing/Service Account/Shared Mailbox is done upon certificate installation (password is provided during this process).
- Activation data generation for Subscriber's private key (PIN) on USB-based smartcards is performed via the smartcard enrolment process during which a random PIN is set at the time of generating a cryptographic key on user's USB-based smartcard. Activation Data is either handed over immediately or delivered later on to the user, either in person in a sealed envelope or, in case of remote users, via post also in a sealed envelope.
- Shared secrets used for the protection of the CA private keys are generated using HSM devices and are protected by an HSM operator card set that requires quorum for data activation. ACS and OCS Smartcards are PIN protected.
- Activation data for network devices or user subscriber keys must at least follow the ECB internal IT Department's password policy and regulations.

6.4.2 Activation data protection

ECB PKI subscribers are required to assert that any activation data is kept secret and is never disclosed to a third party.

CA private key activation requires the use presence of all ACS cards assigned to HSM Operators. Smart cards with components of a shared secret are distributed to HSM Operators. Non personalised smartcards are stored in facilities protected by an access control system. PIN codes protecting the cards are not stored at the same place as the cards.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer Security Controls

Hardening procedures of the ECB PKI CA servers and relevant PKI components have been performed, which includes the implementation of up-to-date security patches. Server and component hardening is conducted on general ECB guidelines and common best-practices.

6.5.1 Specific computer security technical requirements

Specific computer security technical requirements at ECB include:

- Access to these systems is limited to trusted persons who need access to perform their trusted roles.
- Every system has anti-virus software installed. Further, ECB monitors the systems to detect malicious software on a continuous basis.
- Regulations are in place regarding email. In particular, all incoming and outgoing emails are checked by a central anti-virus system.
- Use of passwords to authenticate users. Guidelines are put in place concerning password handling. Passwords are required to have a minimum character length and a combination of alphanumeric and special characters. Periodic password change is required.
- All computer systems are locked or shut down if not used or in idle mode depending on the period of time.

6.5.2 Computer security rating

ECB PKI certification services are built on hardware appliances bundling hardened operating system servers and integrated FIPS 140-2 Level 3-certified HSMs.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

Not applicable.

6.6.2 Security management controls

Monitoring and auditing mechanisms are used to ensure that systems and networks are operated in compliance with the ECB internal IT Department and ECB PKI specific security policies.

6.6.3 Life cycle security controls

Quality assurance processes were employed during the system deployment. A set of three complete separated test and staging environments was configured to provide testing and quality assurance according to ECB standards.

Regarding the cryptographic hardware, the HSM is FIPS 140-2 Level 3 Certified, it includes tamper-evident physical security mechanisms. Data centre access to ECB PKI hardware is controlled by two factors; valid badge and iris recognition. To activate the CA signing keys the simultaneous presence of 3 trusted employees is needed.

The ECB PKI processes include checking the HSM is working correctly as well as the deletion of the keys upon device retirement.

6.7 Network Security Controls

Network protection is applied according to best practices and ECB security policies based on a defined network communication matrix outlining the required protocols and communicating systems within the ECB PKI implementation.

ECB PKI systems run in dedicated separated network segments protected from any foreign traffic by VLANs and firewalls. Network traffic is subject to continuous monitoring for vulnerability scanning and threat assessment.

6.8 Time-stamping

ECB PKI certificates and CRLs bear an issuance timestamp.
The time source is the CA hardware appliance NTP synchronized local clock. The local computer clock of the standalone ECB PKI Root CAs is not regularly but occasionally synchronized manually when started for maintenance purposes.

A trusted and evaluated RFC 3161 time stamping component is not part of ECB PKI environment.

7 Certificate, CRL, and OCSP Profiles

Certificates and Certificate Revocation Lists issued by the ECB PKI Certification Services are compliant to ITU-T recommendations and Internet RFCs. Further certificate profile details are provided on request.

Besides the ECB PKI trust chain oriented class definition ECB PKI facilitates certificate security levels in combination with technical and security related aspects based on use cases of the respective certificates. These security levels are implemented on an organizational basis without any Issuance Policy based enforcement. Six certificate levels are planned based on the current ECB PKI implementation phase with subject to future extension where applicable. Certificate level 1 has the highest security standards and certificate level 6 is the lowest acceptable security implementation.

Every certificate published by ECB PKI CAs must only be assigned to one security level at the same time.

Level	Description of conditions and requirements
1	Private Key Material of the certificates is required to be not exportable Key pair is generated on the corresponding system in a secured hardware environment / HSM, import of non-system key material is not allowed. Use of HSMs with FIPS 140-2 L3 or higher is required Authorization for key access is based on a 3 of n multi-eye principle with additional protection for exposed systems Separation of the system from the active network (offline mode) is required Purpose of use are machine-based Root CA certificates or machine-based certificates with similar protection requirements Key generation and certificate enrolment only by authorized staff and after consultation with ECB Security Board Minimum key length of 4096 bit RSA with SHA-256 or higher grade algorithms for duration of 20 years in connection with the separation of the system from active network (offline mode) Implementation of a revocation checking of certificates in use according to established standards (CRL, OCSP, etc.) is mandatory Reuse of existing key material for renewal or re-key of the certificate is not allowed after certificate expiration.

Level	Description of conditions and requirements
2	Private Key Material of the certificates is required to be not exportable Key pair is generated on the corresponding system in a secured hardware environment / HSM, import of non-system key material is not allowed. Use of HSMs with FIPS 140-2 L3 or higher is required Authorization for key access is based on additional protection implemented by HSMs or similar protection mechanisms. Strict network access control to the system is recommended Purpose of use are Sub CA and PKI online service certificates or certificates with similar protection requirements Key generation and certificate enrolment only by authorized staff and after approval from ECB Security Board Minimum key length of 4096 bit RSA with SHA-256 or higher grade algorithms for a maximum validity period of 10 years. Implementation of a revocation checking of certificates in use according to established standards (CRL, OCSP, etc.) is mandatory except for OCSP response signing certificates. Reuse of existing key material for renewal or re-key of the certificate is not allowed after certificate expiration.
3	Private Key Material of the Certificates is required to be "not exportable" as a general requirement. The only exception is a one-time secured private key handling (key archival) Key pair is generated on the corresponding system in a secured environment, import of non-system key material is not allowed. Storage of certificate key pair in hardware with additional PIN protection is required. Initial external key generation with appropriate security measures during key transport to the hardware device is acceptable. Purpose of use are personalized certificates Enrolment on behalf for the user only acceptable as part of the initial user on-boarding process by RA operators. Delivery of hardware holding the keys and activation data via separate channels required. Otherwise user interaction is required. Check of identity are mandatory. Use of non-personalized certificates in terms of group based certificates is not allowed. Min. key length 2048 bit RSA with SHA-256 or higher grade algorithms with a maximum validity period of 3 years. Implementation of a cyclic revocation checking of certificates according to established standards (CRL, OCSP, etc.) is recommended Reuse of existing key material for renewal or re-key of the certificate is not allowed after certificate expiration.
4	Private Key Material of the Certificates is required to be "not exportable" as an overall and recommended requirement. Exceptions may be acceptable for special technical requirements of legacy devices / applications based on special approval or general key archival requirements.

Level	Description of conditions and requirements
	The key pair is to be generated in a secured environment while one-time import to the target key storage container is acceptable, import of not use-case related key material is not allowed. Generation and storage of the key pair and certificate in a software based environment is acceptable Purpose of use are machine or technical service user certificates or certificates with similar protection requirements Enrolment on behalf for the machine or the technical service account by authorized personal (Service or authorized System Administrator) is acceptable Minimum RSA key length is 2048 bit with SHA-256 or higher grade algorithms with a maximum validity period of 3 years. Reuse of existing key material for renewal or re-key of the certificate is not allowed after expiration
5	Private Key Material of the Certificates is required to be "not exportable" as an overall and recommended requirement. Exceptions may be acceptable for special technical requirements of legacy devices / applications and load balanced environments based on special approval or general key archival requirements. The key pair is to be generated on the requesting machine or in a secured environment while one-time import to the target key storage container is acceptable, import of not use-case related key material is not allowed. Generation and storage of the key pair and certificate in a software-based environment is acceptable Purpose of use are user, machine or technical service account certificates or certificates with similar protection requirements Enrolment on behalf by authorized personal (Service - or authorized System Administrator) is acceptable Minimum RSA key length is 2048 bit RSA with SHA-256 or higher grade algorithms with a maximum validity period of 2 years. Reuse of existing key material for renewal or re-ley of the certificate is not allowed after expiration
6	Private Key Material of the Certificates is required to be "not exportable" as an overall and recommended requirement. Exceptions may be acceptable for special technical requirements of legacy devices / applications and load balanced environments based on special approval or general key archival requirements. The key pair is to be generated on the requesting machine or in a secured environment while one-time import to the target key storage container is acceptable, import of not use-case related key material is not allowed. Generation and storage of the key pair and certificate in a software-based environment is acceptable

Level	Description of conditions and requirements
	Purpose of use are admin account certificates or certificates with similar protection requirements Enrolment on behalf for the machine or the technical service account by authorized personal (Service - or authorized System Administrator) is acceptable Minimum RSA key length is 4096-bit RSA with SHA-256 or higher grade algorithms with a maximum validity period of 5 years. Reuse of existing key material for renewal or re-ley of the certificate is not allowed after expiration

Certificates issued by ECB PKI are assigned to the following certificate security levels based on the current implementation and deployment of ECB PKI.

Certificate Type	Level
ECB PKI Root CAs	1
ECB PKI Sub CAs	2
ECB PKI OCSP Response Signing	2
ECB RSA AV User Authentication	3
ECB RSA AV User Encryption	4
ECB RSA AV User Signature	3
ECB RSA Server Authentication certificate	5
ECB RSA Client/Server Authentication certificate	5
ECB RSA User Client Authentication	5
ECB RSA PKI Administrator certificate	6
ECB RSA Service Account Authentication certificate	5
ECB RSA Shared Mailbox certificate	5
ECB RSA Veridium User Authentication	5

7.1 Certificate Profile

ECB PKI certificates conform to the

- ITU-T recommendation X.509 (1997):
  Information Technology - Open Systems Interconnection
  The Directory: Authentication Framework, June 1997.

The certificates and CRL are profiled in accordance with

- RFC 5280 (obsoletes RFC 3280):
  Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

The basic certificate fields are as follows

Attribute	Value
Version	See 7.1.1 Version number(s)
Serial Number	Unique value in the namespace of each CA
Signature Algorithm	Designation of algorithm used to sign the certificate. See 7.1.3 Algorithm object identifiers for details
Issuer	See 7.1.4 Name forms
Validity	Validity (from and to) time and date information.
Subject	See 7.1.4 Name forms
Subject Public Key	Public Key
Signature	CA Signature

ECB PKI CA certificate profiles

Following tables provide overview information of certificate profiles defined for the ECB PKI certification services. This list represents the current certificate profile set and maybe extended at some point. Further detailed information outlined in the ECB PKI Certificate Profile documentation is available upon request as referenced in the document control section.

ECB RSA Root CA 01	
X.509 Version	V3
Serial Number	12a6bf064b67b514e71d95fb695ecc3f0d21caf0
Signature Algorithm	sha256RSA
Issuer	CN = ECB RSA Root CA 01 O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	20 December 2023 14:02:33
Valid to	15 December 2043 14:02:32
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB RSA Root CA 01 O = European Central Bank C = EU
Key Usage (critical)	Digital Signature, Certificate Signing, CRL Signing, CRL Signing (offline).
Basic Constraints (critical)	Subject Type=CA, Path Length Constraint=1
Subject Key Identifier	4a7fe198361630c01d138b71bc4a08aef2d4b98c
Authority Key Identifier	4a7fe198361630c01d138b71bc4a08aef2d4b98c
CRL Distribution Points	none
Authority Information Access	none
Subject Alternative Name	none

ECB RSA Root CA 01	
Extended Key Usage	none

ECB RSA AV Root CA 01	
X.509 Version	V3
Serial Number	3be5fbf7e71f057cbc798c490b3c87825a4509d2
Signature Algorithm	sha256RSA
Issuer	CN = ECB RSA AV Root CA 01 O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	20 December 2023 13:05:05
Valid to	15 December 2043 13:05:04
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB RSA AV Root CA 01 O = European Central Bank C = EU
Key Usage (critical)	Digital Signature, Certificate Signing, CRL Signing, CRL Signing (offline).
Basic Constraints (critical)	Subject Type=CA, Path Length Constraint=1
Subject Key Identifier	ab3fa77b167329b799790e1b8ae4ea9010a7358b
Authority Key Identifier	ab3fa77b167329b799790e1b8ae4ea9010a7358b
CRL Distribution Points	none
Authority Information Access	none
Subject Alternative Name	none
Extended Key Usage	none

ECB RSA Sub CA 01	
X.509 Version	V3
Serial Number	7030b6b6c062162f2e3d1087992b5f90cb671737
Signature Algorithm	sha256RSA
Issuer	CN = ECB RSA Root CA 01 O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	20 December 2023 14:40:07
Valid to	17 December 2033 14:40:06

ECB RSA Sub CA 01	
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB RSA Sub CA 01 O = European Central Bank C = EU
Key Usage (critical)	Certificate Signing, CRL Signing, CRL Signing (offline).
Basic Constraints (critical)	Subject Type=CA, Path Length Constraint=0
Subject Key Identifier	6f0ff70e86576161f2e6b3043fd36cc92e259e5d
Authority Key Identifier	4a7fe198361630c01d138b71bc4a08aef2d4b98c
CRL Distribution Points	http://cpki.ecb.europa.eu/cdp/ECB-RSA-Root-CA-01-2043.crl
Authority Information Access	http://cpki.ecb.europa.eu/aia/ECB-RSA-Root-CA-01-2043.cer
Subject Alternative Name	none
Extended Key Usage	none

ECB RSA Sub CA 02	
X.509 Version	V3
Serial Number	0d4f5cd8e5946df5d9d8b4beef5c0d22246cfbe5
Signature Algorithm	sha256RSA
Issuer	CN = ECB RSA Root CA 01 O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	20 December 2023 14:47:55
Valid to	17 December 2033 14:47:54
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB RSA Sub CA 02 O = European Central Bank C = EU
Key Usage (critical)	Certificate Signing, CRL Signing, CRL Signing (offline).
Basic Constraints (critical)	Subject Type=CA, Path Length Constraint=0
Subject Key Identifier	ee13c46d21ecf31318d50f9bd5548c35440456f2
Authority Key Identifier	4a7fe198361630c01d138b71bc4a08aef2d4b98c
CRL Distribution Points	http://cpki.ecb.europa.eu/cdp/ECB-RSA-Root-CA-01-2043.crl

ECB RSA Sub CA 02	
Authority Information Access	http://cpki.ecb.europa.eu/aia/ECB-RSA-Root-CA-01-2043.cer
Subject Alternative Name	none
Extended Key Usage	none

ECB RSA Sub CA 03	
X.509 Version	V3
Serial Number	5e0099ccdfa8542abf31332a16c1704507ff371d
Signature Algorithm	sha256RSA
Issuer	CN = ECB RSA Root CA 01 O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	30 January 2025 09:25:32
Valid to	28 January 2035 09:25:31
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB RSA Sub CA 03 O = European Central Bank C = EU
Key Usage (critical)	Certificate Signing, CRL Signing, CRL Signing (offline).
Basic Constraints (critical)	Subject Type=CA, Path Length Constraint=0
Subject Key Identifier	fba080552eac4db33250e60095527e427d2684ae
Authority Key Identifier	4a7fe198361630c01d138b71bc4a08aef2d4b98c
CRL Distribution Points	http://cpki.ecb.europa.eu/cdp/ECB-RSA-Root-CA-01-2043.crl
Authority Information Access	http://cpki.ecb.europa.eu/aia/ECB-RSA-Root-CA-01-2043.cer
Subject Alternative Name	none
Extended Key Usage	none

ECB RSA AV Sub CA 01	
X.509 Version	V3
Serial Number	7267f61c60b2c03202f4f3b46ba3aa3300d97042
Signature Algorithm	sha256RSA

ECB RSA AV Sub CA 01	
Issuer	CN = ECB RSA AV Root CA 01 O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	20 December 2023 14:48:14
Valid to	17 December 2033 14:48:13
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB RSA AV Sub CA 01 O = European Central Bank C = EU
Key Usage (critical)	Certificate Signing, CRL Signing, CRL Signing (offline).
Basic Constraints (critical)	Subject Type=CA, Path Length Constraint=0
Subject Key Identifier	e5be69fb25843cc04ba2e70553a6c31a8e28a567
Authority Key Identifier	ab3fa77b167329b799790e1b8ae4ea9010a7358b
CRL Distribution Points	http://cpki.ecb.europa.eu/cdp/ECB-RSA-AV-Root-CA-01-2043.crl
Authority Information Access	http://cpki.ecb.europa.eu/aia/ECB-RSA-AV-Root-CA-01-2043.cer
Subject Alternative Name	none
Extended Key Usage	none

ECB RSA AV Sub CA 02	
X.509 Version	V3
Serial Number	7942c1f7597b2ea40f60931012bbd5bd59e5aebe
Signature Algorithm	sha256RSA
Issuer	CN = ECB RSA AV Root CA 01 O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	20 December 2023 14:48:30
Valid to	17 December 2033 14:48:29
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB RSA AV Sub CA 02 O = European Central Bank C = EU
Key Usage (critical)	Certificate Signing, CRL Signing, CRL Signing (offline).

ECB RSA AV Sub CA 02	
Basic Constraints (critical)	Subject Type=CA, Path Length Constraint=0
Subject Key Identifier	f1fcd40dd5266968f48c4a4043f5b789433945a4
Authority Key Identifier	ab3fa77b167329b799790e1b8ae4ea9010a7358b
CRL Distribution Points	http://cpki.ecb.europa.eu/cdp/ECB-RSA-AV-Root-CA-01-2043.crl
Authority Information Access	http://cpki.ecb.europa.eu/aia/ECB-RSA-AV-Root-CA-01-2043.cer
Subject Alternative Name	none
Extended Key Usage	none

ECB PKI end-entity certificate profiles

The following tables provide sample information for the structure and certificate attribute information implemented in the ECB PKI end-entity certificates. Further detailed information outlined in the ECB PKI Certificate Profile documentation is available upon request as referenced in the document control section.

ECB PKI End-Entity Certificate	
X.509 Version	V3
Serial Number	present
Signature Algorithm	sha256RSA
Issuer	CN = ECB RSA AV Sub CA 01 O = European Central Bank C = EU - or - CN = ECB RSA AV Sub CA 02 O = European Central Bank C = EU - or – CN = ECB RSA Sub CA 01 O = European Central Bank C = EU - or – CN = ECB RSA Sub CA 02 O = European Central Bank C = EU - or – CN = ECB RSA Sub CA 03 O = European Central Bank C = EU

ECB PKI End-Entity Certificate	
Key Length	2048 Bit
Valid from	present
Valid to	present
Public Key	RSA (2048-Bit) Key Blob
Subject	present, depending on detailed certificate profile
Key Usage (critical)	present
Basic Constraints (critical)	Subject Type=End-Entity, Path Length Constraint=none
Subject Key Identifier	present
Authority Key Identifier	present
CRL Distribution Points	HTTP URL reference to CDP Location
Authority Information Access	HTTP URL reference to AIA Location HTTP URL reference to OCSP Location
Subject Alternative Name	present, depending on detailed certificate profile
Extended Key Usage	present, depending on detailed certificate profile

7.1.1 Version number(s)

ECB PKI issues X.509 version 3 certificates only.

7.1.2 Certificate extensions

ECB PKI uses the following extensions in the issued certificates in accordance with RFC 5280.

Extension	Possible Values	Critical Flag
Key Usage	Digital Signature, Key Encipherment, Certificate Signing, CRL Signing, CRL Signing (offline)	YES
Basic Constraints	Subject Type=CA, Path Length Constraint=1 - or - Subject Type=CA, Path Length Constraint=0 - or - Subject Type=End-Entity, Path Length Constraint=none	YES
Extended Key Usage	Client Authentication, Server Authentication, Smartcard Logon, KDC Authentication,	No

Extension	Possible Values	Critical Flag
	IP security IKE intermediate, OCSP Signing Certificate Request Agent Key Recovery Agent Document Encryption Secure Email BitLocker Encrypting File System	
Subject Key Identifier	Unique number corresponding to the subject's public key. The key identifier method is used.	No
Authority Key Identifier	Unique number corresponding to the authority's public key. The key identifier method is used.	No
CRL Distribution Point	Contains a HTTP URL to obtain the current CRL	No
Authority Information Access	Contains a HTTP URL to obtain the current CA certificate (CA Issuers method) and HTTP URL for OCSP responder where applicable	No
Subject Alternative Name	Contains the subscriber's additional names when needed	No
Certificate Policies	See section 7.1.6	No

Additionally ECB PKI uses the following private extensions

Extension	OID	Critical Flag
Microsoft Certificate Template Information	1.3.6.1.4.1.311.21.7	No
MS Security Identifier	1.3.6.1.4.1.311.25.2	No

7.1.3 Algorithm object identifiers

ECB PKI certification authorities are signing issued certificates with Sha256WithRSAEncryption signature algorithm.

Algorithm OID 1.2.840.113549.1.1.11 (Sha256WithRSAEncryption)

ECB PKI certificate subscriber generate RSA keys according to

Algorithm OID 1.2.840.113549.1.1.1 (RSA)

7.1.4 Name forms

ECB PKI Issuer and Subject Distinguished Names are set in accordance with section 3.1.1. in the following order if applicable

CN = [common name],

O = [organization],

C = [country]

Certificate subject is built from Active Directory information having Common Name as Subject Name format.

The Common Name of ECB user accounts is created having a firstname.lastname (userid) structure, and in case of users with identical firstname and lastname, a number i.e. 1 is added to the respective user logon name and Common Name. In this way Active Directory system has ensured that no duplicates accounts are created and correspondingly the information in the user certificates is ensured as being unique.

7.1.5 Name constraints

See section 7.1.5 of the corresponding CP document.

7.1.6 Certificate policy object identifier

ECB PKI CPS OID is 1.3.6.1.4.1.41697.509.10.100.0.1

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

ECB PKI certificate policy qualifier ID is CPS

The Policy location is referenced by an URL https://cpki.ecb.europa.eu/

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL Profile

ECB PKI CRLs conform to the

- ITU-T recommendation X.509 (1997):
  Information Technology - Open Systems Interconnection
  The Directory: Authentication Framework, June 1997.

The certificates and CRL are profiled in accordance with

- RFC 5280 (obsoletes RFC 3280):
  Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

For details please refer to the ECB PKI Certificate Profile documentation referenced in the document control section of this document.

The basic CRL fields are as follows

Field	Value
Version	See 7.2.1 Version Number(s)
Issuer	Contains the Distinguished Name of the issuing CA
This update	Time and date of CRL issuance.
Next update	Time and date of next CRL update.
Signature Algorithm	Designation of algorithm used to sign the CRL. See 7.1.3 Algorithm object identifiers
Signature	CAs signature

7.2.1 Version Number(s)

ECB PKI issues X.509 Version 2 CRL.

7.2.2 CRL and CRL Entry Extensions

ECB PKI uses the following CRL extensions in accordance with RFC 5280.

Extension	Value	Critical Flag
Authority Key Identifier (2.5.29.35)	Unique number corresponding to the authority's public key. The key identifier method is used.	No
CRL Number (2.5.29.20)	Unique increasing number per CRL	No

ECB PKI uses the following CRL Entry extension in accordance with RFC 5280.

Entry Extension	Possible Value	Critical Flag
Reason Code	unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL	No

7.3 OCSP Profile

ECB PKI online Sub CAs issue OCSP Response Signing Certificates to internal and external facing OCSP responders using the following certificate profile information.

For details please refer to the ECB PKI Certificate Profile documentation referenced in the document control section.

ECB OCSP Signing (Internal)	
X.509 Version	V3
Serial Number	present
Signature Algorithm	Sha256RSA
Issuer	CN= ECB RSA Sub CA 01 O= European Central Bank C= EU - or - CN= ECB RSA Sub CA 02 O= European Central Bank C= EU - or - CN= ECB RSA Sub CA 03 O= European Central Bank C= EU - or - CN= ECB RSA AV Sub CA 01 O= European Central Bank C= EU - or - CN= ECB RSA AV Sub CA 02 O= European Central Bank C= EU
Key Length	2048
Valid from	Present
Valid to	Present
Public Key	RSA (2048-Bit) Key Blob
Subject	CN = ECB RSA 01 OCSP Validation Authority Internal - or – CN = ECB RSA 02 OCSP Validation Authority Internal - or – CN = ECB RSA 03 OCSP Validation Authority Internal - or – CN = ECB RSA AV 01 OCSP Validation Authority Internal

ECB OCSP Signing (Internal)	
	- or - CN = ECB RSA AV 02 OCSP Validation Authority Internal
Key Usage	Digital Signature
Subject Key Identifier	present
Authority Key Identifier	<ECB RSA Sub CA 01 Key ID Hash> - or - <ECB RSA Sub CA 02 Key ID Hash> Or <ECB RSA Sub CA 03 Key ID Hash> or <ECB RSA AV Sub CA 01 Key ID Hash> - or – <ECB RSA AV Sub CA 02 Key ID Hash>
Subject Alternative Name	None
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)
Thumbprint Algorithm	sha1
Thumbprint	present

ECB OCSP Signing (External)	
X.509 Version	V3
Serial Number	present
Signature Algorithm	Sha256RSA
Issuer	CN= ECB RSA Sub CA 01 O= European Central Bank C= EU - or - CN= ECB RSA Sub CA 02 O= European Central Bank C= EU - or – CN= ECB RSA Sub CA 03 O= European Central Bank C= EU - or – CN= ECB RSA AV Sub CA 01 O= European Central Bank C= EU

ECB OCSP Signing (External)	
	- or - CN= ECB RSA AV Sub CA 02 O= European Central Bank C= EU
Key Length	2048
Valid from	Present
Valid to	Present
Public Key	RSA (2048-Bit) Key Blob
Subject	CN = ECB RSA 01 OCSP Validation Authority - or – CN = ECB RSA 02 OCSP Validation Authority - or – CN = ECB RSA 03 OCSP Validation Authority - or – CN = ECB RSA AV 01 OCSP Validation Authority - or - CN = ECB RSA AV 02 OCSP Validation Authority
Key Usage	Digital Signature
Subject Key Identifier	present
Authority Key Identifier	<ECB RSA Sub CA 01 Key ID Hash> - or - <ECB RSA Sub CA 02 Key ID Hash> Or <ECB RSA Sub CA 03 Key ID Hash> or <ECB RSA AV Sub CA 01 Key ID Hash> - or - <ECB RSA AV Sub CA 02 Key ID Hash>
Subject Alternative Name	None
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)
Thumbprint Algorithm	sha1
Thumbprint	present

7.3.1 Version number(s)

ECB PKI issues X.509 Version 3 OCSP signing certificates.

7.3.2 OCSP extensions

ECB PKI uses the following extensions in OCSP response signing certificates in accordance with RFC 5280.

ECB PKI populates the following OCSP extensions:

- 1.3.6.1.5.5.7.48.1.2 OCSP NONCE (non critical)
- 1.3.6.1.5.5.7.48.1.6 Archive Cutoff (non critical)

Extension	Value	Critical Flag
Key Usage	Digital Signature	YES
Basic Constraints	Subject Type=End-Entity, Path Length Constraint=none	YES
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	No
Subject Key Identifier	Unique number corresponding to the subject's public key. The key identifier method is used.	No
Authority Key Identifier	Unique number corresponding to the authority's public key. The key identifier method is used.	No
Subject Alternative Name	Contains the subscriber's additional names where applicable	No
OCSP No Revocation Checking	05 00	No

Additionally ECB PKI uses the following private extensions for OCSP certificates

Extension	OID	Critical Flag
Certificate Template Information	1.3.6.1.4.1.311.21.8	No
Application Policies	1.3.6.1.5.5.7.3.9	No

8 Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

Audits of the ECB PKI and related infrastructure components will be performed along with regular ECB internal IT Department and Security Audits.

Additionally ECB PKI will be audited by an auditor with proven track record in PKI audits at least once every 3 years, in accordance with the ESCB/SSM Certificate Acceptance Framework, to check for compliance with the CP.

Security Penetration Tests on ECB PKI infrastructure will also be conducted regularly, at least every 3 years.

8.2 Identity/qualifications of assessor

Compliance audits are performed by ECB internal Audit or the ESCB Internal Auditors Committee (IAC) according to the annual audit program.

Security audit on ECB PKI must have knowledge, appropriate training and experience in PKI, security, cryptographic technology and audit procedures.

8.3 Assessor's relationship to assessed entity

The ECB auditors are organizationally independent to ECB PKI certification service responsible parties.

8.4 Topics covered by assessment

The audit verifies ECB PKI compliance with its CP and CPS documents including verification of existing processes, procedures, and disaster recovery plans.

8.5 Actions taken as a result of deficiency

If an audit detects deficiencies, an action plan for remediation is initiated. ECB PKI operations staff and / or ECB internal DG-IS IT department management is responsible for developing and implementing of such action plan. Actions are prioritized depending on the severity of the deficiencies which have been discovered.

After implementation of the action plan, it is verified that the deficiencies have been successfully corrected. ECB internal DG-IS IT department management and ECB PKI operations team including responsible Security Officers are informed of the results.

8.6 Communication of results

Audit results are generally kept confidential.

9 Other Business and Legal Matters

Following section applies to business, legal and data privacy matters of ECB PKI certification services. The current PKI and related infrastructure is designed for internal and approved ECB business partner use only. Therefore following topics are regarded as Not applicable. while no guarantees or warranties are accepted in any case besides the standard ECB internal and approved ECB Business Partner Service Level Agreements.

In accordance with the Certification Policy (CP) of the ECB PKI system.

9.1 Fees

Not applicable.

9.1.1 Certificate issuance or renewal fees

Not applicable.

9.1.2 Certificate access fees

Not applicable.

9.1.3 Revocation or status information access fees

Not applicable.

9.1.4 Fees for other services

Not applicable.

9.1.5 Refund policy

Not applicable.

9.2 Financial Responsibility

In accordance with Article 35.3 of the Statute of the ECB and ESCB, the ECB shall be subject to the liability regime provided for in Article 340 of the Treaty on the Functioning of the European Union.

9.2.1 Insurance coverage

Not applicable.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

See section 9.2.

9.3 Confidentiality of Business Information

ECB general Information Security Policies and Privacy Statements in their latest versions apply.

9.3.1 Scope of confidential information

ECB general Information Security Policies and Privacy Statements in their latest versions apply.

9.3.2 Information not within the scope of confidential information

Any information in published documents like this document and accompanying regulations are not within the scope of confidentiality. Information contained within certificate signing requests sent to the ECB PKI are supposed to be publicly available on the resulting certificates within their respective application environment and thus considered public information. So certificate applicants must not provide confidential information as part of CSRs, as the resulting certificate may become publicly available.

9.3.3 Responsibility to protect confidential information

Subscribers and all relying parties should treat any ECB PKI related information to be covered by applicable ECB general Information Security Policies unless otherwise stated. This does not apply to public available information or general means in terms of industry standards.

9.4 Privacy of Personal Information

Subscribers and all relying parties should treat any ECB PKI related personal information to be covered by applicable ECB general Information Security and Confidentiality Policies unless otherwise stated. This does not apply to public available information or general means in terms of industry standards.

9.4.1 Privacy plan

ECB general Information Security Policies and Privacy Statement in their latest version apply.

9.4.2 Information treated as private

ECB general Information Security Policies and Privacy Statement in their latest version apply.

Any personal information on subscribers stored or processed in ECB PKI systems including its log records and meta information is treated as private information.

9.4.3 Information not deemed private

ECB general Information Security Policies and Privacy Statement in their latest version apply.

All information related to ECB PKI and the ECB PKI infrastructure design, subscriber information, relying parties and business partnerships is considered private and confidential information unless otherwise stated.

9.4.4 Responsibility to protect private information

ECB general Information Security Policies and Privacy Statement in their latest version apply.

All ECB PKI participants that receive private information are responsible to secure it, refrain from using it for any other purpose than its intended usage or disclose it to third parties.

9.4.5 Notice and consent to use private information

ECB general Information Security Policies and Privacy Statement in their latest version apply.

9.4.6 Disclosure pursuant to judicial or administrative process

ECB general Information Security Policies and Privacy Statement in their latest version apply.

9.4.7 Other information disclosure circumstances

ECB general Information Security Policies and Privacy Statement in their latest version apply.

9.5 Intellectual Property Rights

ECB general Information Security Policies and Privacy Statement in their latest version apply. This does not apply to public available information or general means in terms of industry standards.

9.6 Representations and Warranties

Not applicable.

9.6.1 CA representations and warranties

Not applicable.

9.6.2 RA representations and warranties

Not applicable.

9.6.3 Subscriber representations and warranties

Not applicable.

9.6.4 Relying party representations and warranties

Not applicable.

9.6.5 Representations and warranties of other participants

Not applicable.

9.7 Disclaimers of Warranties

Not applicable.

9.8 Limitations of Liability

ECB PKI is operated under ECB general DG-IS IT Department operations policies including Service Level Agreements with / to business partners consuming ECB PKI services.

In accordance with Article 35.3 of the Statute of the ECB and ESCB, the ECB shall be subject to the liability regime provided for in Article 340 of the Treaty on the Functioning of the European Union.

9.9 Indemnities

In accordance with Article 35.3 of the Statute of the ECB and ESCB, the ECB shall be subject to the liability regime provided for in Article 340 of the Treaty on the Functioning of the European Union.

9.10 Term and Termination

9.10.1 Term

This CPS shall come into force from the moment it is published in the ECB PKI repository. Amendments to this CPS become effective upon publication in the ECB PKI repository.

This CPS shall remain valid until such time as it is expressly terminated by issuance of a new version or upon re-key of the Root CA keys, at which time a new version may be created.

9.10.2 Termination

If this CPS is substituted, it shall be substituted for a new and updated version, regardless of the importance of the changes carried out therein. Accordingly, it shall always be applicable in its entirety.

If the CPS is terminated, it shall be withdrawn from the ECB PKI repository, though a copy hereof shall be held available for 10 years.

9.10.3 Effect of termination and survival

The obligations established under this CPS, referring to audits, confidential information, possible ESB PKI obligations and liabilities that came into being whilst it was in force shall continue to prevail following its termination or substitution, in the latter case only with respect to those terms which are not contrary to the new version.

9.11 Individual notices and communications with participants

All notifications, demands, applications or any other type of communication required in the practices described in this CPS shall be carried out by electronic message or in writing, by registered post addressed to any of the addresses contained in section 1.5 “Policy Administration”. Electronic notifications shall be effective upon receipt by the recipients to which they are addressed.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments or special agreements need to be laid out in written form with compliance to existing ECB PKI and / or applicable general ECB legal policies. The authority empowered to carry out and approve amendments to this CPS and the referenced CP is the Policy Approval Authority (PAA). The PAA's contact details can be found in section 1.5 “Policy Administration”.

9.12.2 Notification mechanism and period

Should ECB PKI PAA deem that the amendments to this CPS or the referenced CP could affect the acceptability of the certificates for specific purposes, it shall request the ECB PKI and related

infrastructure services to notify the users of the certificates corresponding to the amended CP or CPS that an amendment has been carried out and that possibly affected these parties should consult the new CPS in the relevant ECB PKI repository. When, in the opinion of the PAA, the changes do not affect the acceptance of certificates, the changes shall not be disclosed to the users of the certificates.

9.12.3 Circumstances under which OID must be changed

In case of amendment, when numbering the new version of the CPS or the relevant CP:

- If the PAA deems that the amendments could affect the acceptability of the certificates for specific purposes, the major version number indicated under the respective ECB PKI IANA PEN document OID namespace of the document shall be changed and its lowest number if applicable reset to zero.
- If the PAA deems that the amendments do not affect the acceptability of the certificates for specific purposes, the lowest version number or an added version index of the document based on the existing ECB PKI IANA PEN document OID namespace will be increased maintaining the major version number of the document, as well as the rest of the associated OID.

9.13 Dispute Resolution Provisions

Resolution of any dispute between users and the ECB PKI that may arise shall be submitted to the ECB Security Board or ECB PKI DG-IS Security Governance Team for resolution. As outlined before ECB PKI in general accepts no liability for ECB PKI certificates or any related PKI service beyond regulations and circumstances laid out in the existing ECB DG-IS IT Service Level Agreements.

9.14 Governing Law

The Laws of the European Economic Community apply to the ECB PKI.

The ECB processes personal data in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC of the European Parliament.

9.15 Compliance with Applicable Law

ECB PKI participants are responsible for existing compliance with applicable jurisdiction.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

This CPS extended by the relevant associated CP and the documents referred to herein constitute the entire agreement among the ECB PKI participants and no party shall be liable or bound to any other party in any manner by any warranties, representations or covenants except as specifically set forth herein or therein..

9.16.2 Assignment

Not applicable.

9.16.3 Severability

Not applicable.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

Not applicable.

9.17 Other Provisions

Not applicable.

Annex 1: Types of events logged by the CA

Type of event	Description
ACCESS_CONTROL	Authorization check to resource of authenticated entity.
AUTHENTICATION	Authentication check of an entity.
CA_CREATION	Creation of a Certificate Authority.
CA_DELETION	Removal of a Certificate Authority.
CA_EDITING	Modification of a Certificate Authority.
CA_KEYACTIVATE	Certificate Authority starts using a different key pair.
CA_KEYGEN	Generation of a new key pair that can be used by the Certificate Authority during renewal or update.
CA_RENAMING	Internal application name change of a Certificate Authority.
CA_SERVICEACTIVATE	Certificate Authority state change to start serving requests.
CA_SERVICEDEACTIVATE	Certificate Authority state change to stop serving requests.
CERT_CHANGEDSTATUS	Change of a certificate's status to unassigned, inactive, active, notified about expiration, revoked or archived.
CERT_CREATION	Issuance of a certificate by a Certificate Authority.
CERT_CTPRECERT_SUBMISSION	Certificate Transparency log servers responds to a pre-certificate submission from a Certificate Authority.
CERT_REQUEST	A request for certificate issuance from a Certificate Authority is submitted.
CERT_REVOKED	Change of a certificate's status to revoked or active.
CERT_STORED	Persistence of a certificate to the database.
CERTPROFILE_CREATION	Creation of a certificate profile.
CERTPROFILE_DELETION	Removal of a certificate profile.
CERTPROFILE_EDITING	Modification of a certificate profile.
CERTPROFILE_RENAMING	Name change of a certificate profile.
CRL_CREATION	Issuance of a Certificate Revocation List by a Certificate Authority.

Type of event	Description
CRL_STORED	Persistence of a Certificate Revocation List to the database.
CRYPTOTOKEN_ACTIVATION	Activation of a Crypto Token, making the key material available for use by the application.
CRYPTOTOKEN_CREATE	Creation of a Crypto Token.
CRYPTOTOKEN_DEACTIVATION	Deactivation of a Crypto Token, making the key material unavailable for use by the application.
CRYPTOTOKEN_DELETE_ENTRY	Removal of a key pair from the Crypto Token key material or key pair place-holder from the Crypto Token object.
CRYPTOTOKEN_DELETION	Removal of a Crypto Token.
CRYPTOTOKEN_EDIT	Modification of a Crypto Token.
CRYPTOTOKEN_GEN_KEYPAIR	Generation of a new key pair in the Crypto Token.
CRYPTOTOKEN_REACTIVATION	Attempted reactivation of a Crypto Token.
CRYPTOTOKEN_UPDATEPIN	Modification of the Crypto Token's auto-activation PIN.
INTERNALKEYBINDING_CREATE	Creations of a new Internal Key Binding.
INTERNALKEYBINDING_DELETE	Removal of an existing Internal Key Binding.
INTERNALKEYBINDING_EDIT	Modification of an existing Internal Key Binding.
LOG_DELETE	Removal of persisted audit log records.
LOG_EXPORT	Export of audit log records.
LOG_MANAGEMENT_CHANGE	Change of protection settings for audit log records.
LOG_VERIFY	Verification of existing audit log records.
ROLE_ACCESS_RULE_CHANGE	Modifications of existing access rules in an administrative role.
ROLE_ACCESS_USER_ADDITION	New administrator added to administrative role.
ROLE_ACCESS_USER_CHANGE	Change of existing administrator in an administrative role.
ROLE_ACCESS_USER_DELETION	Removal of existing administrator from administrative role.
ROLE_CREATION	Creation of an administrative role.

Type of event	Description
ROLE_DELETION	Removal of an administrative role.
ROLE_RENAMING	Name change of an administrative role.
SYSTEMCONF_CREATE	Creation of new system settings stored in the database.
SYSTEMCONF_EDIT	Modification of existing system settings stored in the database.
VALIDATOR_CHANGE	Modification of an existing validator.
VALIDATOR_CREATION	Creation of a new validator.
VALIDATOR_REMOVAL	Removal of an existing validator.
VALIDATOR_RENAME	Name change of an existing validator.
VALIDATOR_VALIDATION_FAILED	Validation failed.
VALIDATOR_VALIDATION_SUCCESS	Validation succeeded.