EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB CLASS 2 PKI

Certification Practice Statement (CPS)

Table of Contents

Document control

Basic Description

Document title	ECB CLASS 2 PKI Certification Practice Statement (CPS)
Topic	Certification Practice Statement for the ECB CLASS 2 PKI Service based on RFC 3647
Version	3.0
Status	Published release related to Certificate Services Release 2.0
Document OID	1.3.6.1.4.1.41697.509.2.100.20.2
Supersedes Document	-
Authors	Daniela Puiu, Carlos Mendez, Ulrich Kühn
ECB responsible contact	Daniela Puiu

Version History

Version	Version Date	Comment
0.1	22.09.2014	Initial Draft
1.0	13.02.2015	First version submitted for approval
1.1	25.02.2015	Corrections on ECB device certificates incorporated
1.2	18.04.2015	Extensions for ECB User smartcards incorporated
1.3	08.06.2015	Corrections on ECB User smartcards incorporated
1.4	29.06.2015	CPS format adjusted to RFC.3467, further amendments
2.0	08.07.2015	Published version according to Release 2.0 of ECB PKI
3.0	01.07.2020	Revised version according to Certificate Services Release 4.0

Document Review and Signoff

Version	Version Date	Reviewer Name	Signoff Date
1.1	25.02.2015	Koenraad De Geest [ECB CIO]	26.02.2015
1.1	25.02.2015	Alvise Grammatica [ECB CISO]	26.02.2015
2.0	08.07.2015	Magi Clave on behalf of Koenraad De Geest [ECB CIO]	30.06.2015
2.0	08.07.2015	Alvise Grammatica [ECB CISO]	30.06.2015
3.0	22.04.2020	Alvise Grammatica (Head of Digital Security Services Division)	22.04.2020
3.0	01.07.2020	Magi Clave (Deputy Director General Information Systems)	27.08.2020

Related Documents

Document title	ECB CLASS 2 PKI Certificate Policy (CP)
Document Name	ECB CLASS 2 PKI CP v3.0.pdf
Description	Certificate Policy for ECB CLASS 2 PKI Service
Document OID	1.3.6.1.4.1.41697.509.2.100.20.1
Latest available version	V3.0
Last changed	04.08.2020

Document title	ECB PKI Certificate Profiles
Document Name	ECB PKI Certificate Profiles RFC 5280 v3.0.xlsx
Description	RFC5280 Certificate Profiles for ECB CLASS 2 PKI
Latest available version	V3.0
Last changed	17.06.2020

Document title	ECB PKI IANA PEN Namespace
Document Name	ECB PKI IANA PEN Namespace v1.2
Description	Overview of the ECB PKI related IANA PEN Namespace
Latest available version	v1.2
Last changed	23.09.2014

1 Introduction

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.

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 one trust chain named “ECB Class 2” which supports up to date cryptographic algorithms All certificates, regardless of CA or subscriber / end-entity, within the respective trust chain are required to reflect the trust chain class definition and the appropriate algorithms either by name or by the trust chain based issuance policy.

The ECB Class 2 trust chain is the platform built to provide certification services for the long term at the ECB. It is designed with support for up to date cryptographic algorithms, i.e. RSA for signing/verification operations and SHA-256 as hashing algorithm.

The implementation of the ECB PKI “Class 2” 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.

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 Class 2 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 Class 2 Root CA, and Issuing subordinate CAs certified by it. The Root CA and Issuing subordinate CAs in the Class 2 trust chain define the whole CA certificate chain.

The ECB Class 2 PKI environment is comprised of ECB Class 2 Root CA as the trust anchor and, on the subordinate level, the ECB Class 2 Sub CA 01 and the ECB Class 2 Sub CA 02 providing certificate issuance for different purposes. The ECB Class 2 Sub CA 01 is used for issuing machine based certificates, while the ECB Class 2 Sub CA 02 is used to issue certificates for users.

All relevant PKI components and application keys are protected by an HSM infrastructure. All cryptographic operations of ECB PKI CAs and backend services are controlled and protected by this HSM implementation.

The root certification authority of the ECB Class 2 trust chain is implemented using a dedicated hardware security module (offline). The ECB Class 2 Sub CAs are implemented on network-connected HSMs (shared between the Sub CAs). 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.

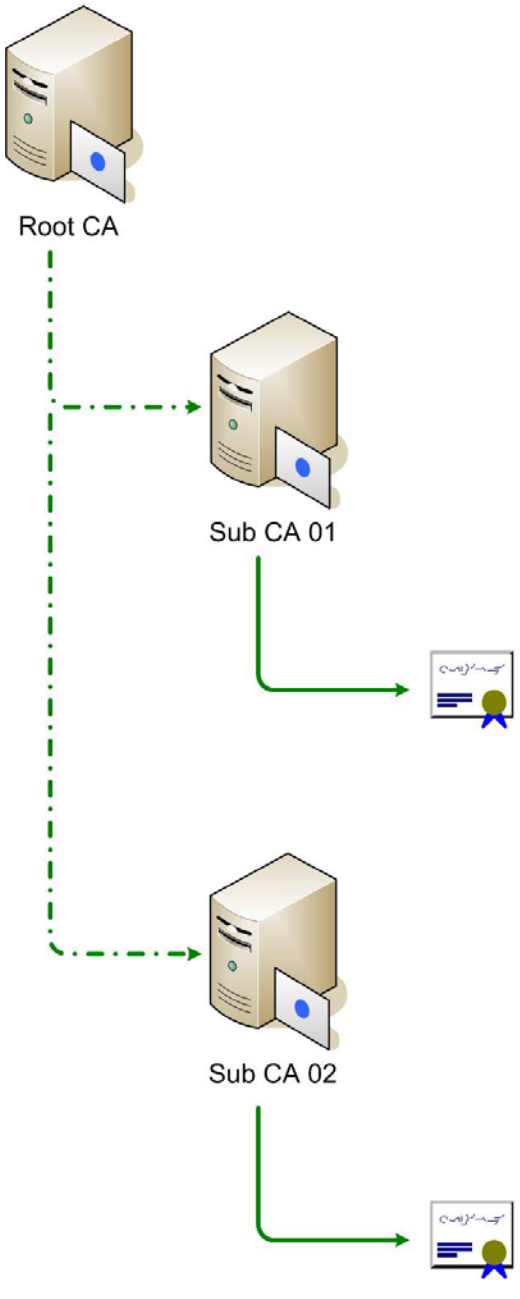
The other components in the PKI are built from multi-tenant capable centralized components like certificate validation services including OCSP responders and the certificate management solution. The same principle applies to the centralized LDAP directory infrastructure.

All installed components, especially the CAs, are reduced to a minimal level to provide additional security while different components and roles are installed on separate servers in the infrastructure as required from a functional perspective.

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.

Besides several additional infrastructure components four high-available web site clusters using load balancer infrastructure exist as part of the ECB PKI for all related HTTP based locations and references. Two high-available web clusters (one for CRL, one for OCSP) are implemented to support internal network ECB clients and servers, while two web clusters are dedicated to external traffic providing identical services as the two internal facing web clusters. The external facing web clusters are protected by an application layer gateway infrastructure to provide additional security measures and to enforce protocol compliance of incoming requests.

Overview of the ECB Class 2 trust chain:



CA Name : ECB CLASS 2 Root CA
CA Role : Certification of ECB PKI Sub CAs
Keylength : 4096 Bit RSA, SHA256
Lifetime : 20 Years
CRL Lifetime : 6 Months, 2 Months Overlap
CRL Publishing : offline / manual CRL Publishing
Key Security : Dedicated HSM, multi-eye principle authorization
Instance type : physical
Status : offline
Availability : cold standby

CA Name : ECB CLASS 2 Sub CA 01
CA Role : Issuance of Machine based End Entity Certificates
Keylength : 4096 Bit RSA, SHA256
Lifetime : 10 Years
CRL Lifetime : 5 Days, 3 Days Overlap
CRL Publishing : Online CRL Publishing
Key Security : Network HSM
Instance type : physical
Status : online
Availability : clustered

Keylength : 2048 Bit RSA, SHA256
Lifetime : 3 Years (Max)

Key Security : Software protected storage for machine based certificates

CA Name : ECB CLASS 2 Sub CA 02
CA Role : Issuance of User based End Entity Certificates
Keylength : 4096 Bit RSA, SHA256
Lifetime : 10 Years
CRL Lifetime : 5 Days, 3 Days Overlap
CRL Publishing : Online CRL Publishing
Key Security : Network HSM
Instance type : physical
Status : online
Availability : clustered

Keylength : 2048 Bit RSA, SHA256
Lifetime : 3 Years (Max)

Key Security : Hardware protected storage for user based certificates

1.2 Document Name and Identification

This CPS is called "**ECB Class 2 PKI Certification Practice Statement**" and has its own Object Identifier. For details please refer to the ECB PKI IANA PEN namespace document outlined 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 Class identifier

1.3.6.1.4.1.41697.509.**2** Base of the ECB Class 2 PKI trust chain namespace

X.509 OID –Environment

1.3.6.1.4.1.41697.509.2.**100** Base of the ECB Class 2 PKI production environment

X.509 OID – Issuance Policy namespace

1.3.6.1.4.1.41697.509.2.100.**10** Base of the ECB Class 2 PKI issuance policy reference

X.509 OID – Issuance Policy identifiers

1.3.6.1.4.1.41697.509.2.100.10.**1** ECB Class 2 PKI issuance policy reference

X.509 OID – PKI Policy

1.3.6.1.4.1.41697.509.2.100.**20** Base of the ECB Class 2 PKI documents namespace

X.509 OID – Current CP documentation

1.3.6.1.4.1.41697.509.2.100.20.**1** ECB Class 2 PKI Certificate Policy v3.0

X.509 OID – Current CPS documentation

1.3.6.1.4.1.41697.509.2.100.20.**2** ECB Class 2 PKI Certification Practice Statement v3.0

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

1.3 PKI Participants

See section 1.3 on ECB Class 2 PKI CP

1.3.1 Certification Authorities

See section 1.3.1 on ECB Class 2 PKI CP.

1.3.2 Registration Authorities

See section 1.3.2 on ECB Class 2 PKI CP.

1.3.3 Subscribers

See section 1.3.3 on ECB Class 2 PKI CP.

1.3.4 Relying parties

See section 1.3.4 on ECB Class 2 PKI CP.

1.3.5 Other participants

See section 1.3.5 on ECB Class 2 PKI CP.

1.4 Certificate Usage

See section 1.4 on ECB Class 2 PKI CP.

1.4.1 Appropriate certificate uses

See section 1.4.1 on ECB Class 2 PKI CP.

1.4.2 Prohibited certificate uses

See section 1.4.2 on ECB Class 2 PKI CP.

1.5 Policy Administration

1.5.1 Organization administering the document

This Certificate Policy is administered by the ECB Security and Architecture Division. To contact refer to the contact person given in section 1.5.2.

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

See 1.5.2 Contact person.

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

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 Policy (CP): A document containing the rules that indicate the applicability and use of certificates issued to ECB PKI subscribers

Certification Practices Statement (CPS): A document containing the practices that ECB PKI certification authority employs in issuing certificates and maintaining PKI related operational status.

Certification Authority (CA): The unit within ECB PKI to create, assign and revoke public key certificates.

Directory: A database containing information and data related to identities, certificates and CAs.

End-Entity: An entity that is a subscriber, a relying party, or both.

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.

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.

Subscriber: A person or a machine that is the subject named or identified in a certificate and holds the private key that corresponds to the associated certificate. In particular and besides several other use cases, LDAP directory member machines are the most common ECB PKI subscribers.

2 Publication and Repository Responsibilities

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

2.1 Repositories

See section 2.1 on ECB Class 2 PKI CP

2.2 Publication of Certification Information

See section 2.2 on ECB Class 2 PKI CP.

2.3 Time or Frequency of Publication

See section 2.3 on ECB Class 2 PKI CP.

2.4 Access Controls on Repositories

See section 2.4 on ECB Class 2 PKI CP.

3 Identification and Authentication

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

3.1 Naming

See section 3.1 on ECB Class 2 PKI CP.

3.1.1 Types of names

See section 3.1.1 on ECB Class 2 PKI CP.

3.1.2 Need for names to be meaningful

See section 3.1.2 on ECB Class 2 PKI CP.

3.1.3 Anonymity or pseudonymity of subscribers

See section 3.1.3 on ECB Class 2 PKI CP.

3.1.4 Rules for interpreting various name forms

See section 3.1.4 on ECB Class 2 PKI CP.

3.1.5 Uniqueness of names

See section 3.1.5 on ECB Class 2 PKI CP.

The required uniqueness of names, i.e. the subject attribute, of certificates relating to users is ensured by the ECB's identity management system which ensures that the attribute values, which the ECB PKI system obtains from the ECB's Active Directory, are unique over the lifetime of the CA.

3.1.6 Recognition, authentication, and role of trademarks

See section 3.1.6 on ECB Class 2 PKI CP.

3.2 Initial Identity Validation

See section 3.2 on ECB Class 2 PKI CP

3.2.1 Method to prove possession of private key

See section 3.2.1 on ECB Class 2 PKI CP.

3.2.2 Authentication of organization identity

See section 3.2.2 on ECB Class 2 PKI CP.

3.2.3 Authentication of individual identity

See section 3.2.3 on ECB Class 2 PKI CP.

3.2.4 Non-verified subscriber information

See section 3.2.4 on ECB Class 2 PKI CP.

3.2.5 Validation of authority

See section 3.2.5 on ECB Class 2 PKI CP.

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 ECB Class 2 PKI CP.

3.3.1 Identification and authentication for routine re-key

See section 3.3.1 on ECB Class 2 PKI CP.

3.3.2 Identification and authentication for re-key after revocation

See section 3.3.2 on ECB Class 2 PKI CP.

3.4 Identification and Authentication for Revocation Requests

See section 3.4 on ECB Class 2 PKI CP.

4 Certificate Life-Cycle Operational Requirements

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

4.1 Certificate Application

See section 4.1 on ECB Class 2 PKI CP.

4.1.1 Who can submit a certificate application

See section 4.1.1 on ECB Class 2 PKI CP.

4.1.2 Enrolment process and responsibilities

See section 4.1.2 on ECB Class 2 PKI CP.

4.2 Certificate application processing

See section 4.2 on ECB Class 2 PKI CP.

4.2.1 Performing identification and authentication functions

See section 4.2.1 on ECB Class 2 PKI CP.

4.2.2 Approval or rejection of certificate applications

See section 4.2.2 on ECB Class 2 PKI CP.

4.2.3 Time to process certificate applications

See section 4.2.3 on ECB Class 2 PKI CP.

4.3 Certificate Issuance

See section 4.3 on ECB Class 2 PKI CP.

4.3.1 CA actions during certificate issuance

See section 4.3.1 on ECB Class 2 PKI CP.

4.3.2 Notification to subscriber by the CA of issuance of certificate

See section 4.3.2 on ECB Class 2 PKI CP.

4.4 Certificate Acceptance

See section 4.4 on ECB Class 2 PKI CP.

4.4.1 Conduct constituting certificate acceptance

See section 4.4.1 on ECB Class 2 PKI CP.

4.4.2 Publication of the certificate by the CA

See section 4.4.2 on ECB Class 2 PKI CP.

4.4.3 Notification of certificate issuance by the CA to other entities

See section 4.4.3 on ECB Class 2 PKI CP.

4.5 Key Pair and Certificate Usage

See section 4.5 on ECB Class 2 PKI CP

4.5.1 Subscriber private key and certificate usage

See section 4.5.1 on ECB Class 2 PKI CP.

4.5.2 Relying party public key and certificate usage

See section 4.5.2 on ECB Class 2 PKI CP.

4.6 Certificate Renewal

See section 4.6 on ECB Class 2 PKI CP.

4.6.1 Circumstance for certificate renewal

See section 4.6.1 on ECB Class 2 PKI CP.

4.6.2 Who may request renewal

See section 4.6.2 on ECB Class 2 PKI CP.

4.6.3 Processing certificate renewal requests

See section 4.6.3 on ECB Class 2 PKI CP.

4.6.4 Notification of new certificate issuance to subscriber

See section 4.6.4 on ECB Class 2 PKI CP.

4.6.5 Conduct constituting acceptance of a renewal certificate

See section 4.6.5 on ECB Class 2 PKI CP.

4.6.6 Publication of the renewal certificate by the CA

See section 4.6.6 on ECB Class 2 PKI CP.

4.6.7 Notification of certificate issuance by the CA to other entities

See section 4.6.7 on ECB Class 2 PKI CP.

4.7 Certificate Re-key

See section 4.7 on ECB Class 2 PKI CP.

4.7.1 Circumstance for certificate re-key

See section 4.7.1 on ECB Class 2 PKI CP.

4.7.2 Who may request certification of a new public key

See section 4.7.2 on ECB Class 2 PKI CP.

4.7.3 Processing certificate re-keying requests

See section 4.7.3 on ECB Class 2 PKI CP.

4.7.4 Notification of new certificate issuance to subscriber

See section 4.7.4 on ECB Class 2 PKI CP.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See section 4.7.5 on ECB Class 2 PKI CP.

4.7.6 Publication of the re-keyed certificate by the CA

See section 4.7.6 on ECB Class 2 PKI CP.

4.7.7 Notification of certificate issuance by the CA to other entities

See section 4.7.7 on ECB Class 2 PKI CP.

4.8 Certificate Modification

See section 4.8 on ECB Class 2 PKI CP

4.8.1 Circumstance for Certificate Modification

See section 4.8.1 on ECB Class 2 PKI CP.

4.8.2 Who may request certificate modification

See section 4.8.2 on ECB Class 2 PKI CP

4.8.3 Processing certificate modification requests

See section 4.8.3 on ECB Class 2 PKI CP.

4.8.4 Notification of new certificate issuance to subscriber

See section 4.8.4 on ECB Class 2 PKI CP.

4.8.5 Conduct constituting acceptance of modified certificate

See section 4.8.5 on ECB Class 2 PKI CP.

4.8.6 Publication of the modified certificate by the CA

See section 4.8.6 on ECB Class 2 PKI CP

4.8.7 Notification of certificate issuance by the CA to other entities

See section 4.8.7 on ECB Class 2 PKI CP.

4.9 Certificate Revocation and Suspension

See section 4.9 on ECB Class 2 PKI CP

4.9.1 Circumstances for revocation

See section 4.9.1 on ECB Class 2 PKI CP.

4.9.2 Who can request revocation

See section 4.9.2 on ECB Class 2 PKI CP.

4.9.3 Procedure for revocation request

See section 4.9.3 on ECB Class 2 PKI CP.

4.9.4 Revocation request grace period

See section 4.9.4 on ECB Class 2 PKI CP.

4.9.5 Time within which CA must process the revocation request

See section 4.9.5 on ECB Class 2 PKI CP.

4.9.6 Revocation checking requirement for relying parties

See section 4.9.6 on ECB Class 2 PKI CP.

4.9.7 CRL issuance frequency

See section 4.9.7 on ECB Class 2 PKI CP.

4.9.8 Maximum latency for CRLs

See section 4.9.8 on ECB Class 2 PKI CP.

4.9.9 On-line revocation/status checking availability

See section 4.9.9 on ECB Class 2 PKI CP.

4.9.10 On-line revocation checking requirements

See section 4.9.10 on ECB Class 2 PKI CP.

4.9.11 Other forms of revocation advertisements available

See section 4.9.11 on ECB Class 2 PKI CP.

4.9.12 Special requirements re key compromise

See section 4.9.12 on ECB Class 2 PKI CP.

4.9.13 Circumstances for suspension

See section 4.9.13 on ECB Class 2 PKI CP.

4.9.14 Who can request suspension

See section 4.9.14 on ECB Class 2 PKI CP.

4.9.15 Procedure for suspension request

See section 4.9.15 on ECB Class 2 PKI CP.

4.9.16 Limits on suspension period

See section 4.9.16 on ECB Class 2 PKI CP.

4.10 Certificate Status Services

See section 4.10 on ECB Class 2 PKI CP

4.10.1 Operational characteristics

See section 4.10.1 on ECB Class 2 PKI CP

4.10.2 Service availability

See section 4.10.2 on ECB Class 2 PKI CP

4.10.3 Optional features

See section 4.10.3 on ECB Class 2 PKI CP

4.11 End of Subscription

See section 4.11 on ECB Class 2 PKI CP

4.12 Key Escrow and Recovery

See section 4.12 on ECB Class 2 PKI CP

4.12.1 Key escrow and recovery policy and practices

See section 4.12.1 on ECB Class 2 PKI CP.

4.12.2 Session key encapsulation and recovery policy and practices

See section 4.12.2 on ECB Class 2 PKI CP.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

The central CA components are operated by the ECB PKI operations staff in the organization of the ECB DG-IS IT Department under the terms of its general regulations and policies. The CAs have implemented appropriate physical security controls to restrict access to CA hardware and software, including the servers, workstations, and any cryptographic hardware modules, used in connection with providing CA services.

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.

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 hosting location is in secure data centres conforming to the general ECB standards for physical and environmental security. Further details may be available on request.

5.1.2 Physical access

See section 5.1.1 on this document.

5.1.3 Power and air conditioning

See section 5.1.1 on this document.

5.1.4 Water exposures

See section 5.1.1 on this document.

5.1.5 Fire prevention and protection

See section 5.1.1 on this document.

5.1.6 Media storage

See section 5.1.1 on this document.

5.1.7 Waste disposal

See section 5.1.1 on this document.

5.1.8 Off-site backup

See section 5.1.1 on this document.

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

Within the ECB and the ECB PKI the following roles are defined as trusted: Registration Officer, PKI Operations Team (CA administrators), Information Security Officer, IT Operations Managers and Auditor.

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.

5.2.3 Identification and authentication for each role

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

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

ECB has in its employment sufficient staff with the necessary qualifications, know-how and experience to offer its ECB PKI services.

5.3.1 Qualifications, experience, and clearance requirements

Persons who are going to perform trusted tasks conforming to "Procedural Controls" must have and prove competence and experience that is appropriate for the respective tasks.

Every person has signed an agreement of confidentiality with regard to processed data.

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.

5.4.2 Frequency of processing log

In case of irregularities, unusual activities or incidents event logs are reviewed thoroughly.

5.4.3 Retention period for audit log

Recorded events are retained in the audit log for at least 12 months, thereby exceeding the minimum requirements of the CP.

5.4.4 Protection of audit log

Audit logs are protected in such a way that confidentiality and integrity is guaranteed and unauthorized access is prevented. An appropriate combination of physical and logical access controls is in place.

5.4.5 Audit log backup procedures

Backup of online CA systems is performed per working day including all containing log information. For offline PKI Systems and components regular backup procedures including audit log files are conducted on a defined schedule prior to changes applied to the systems.

5.4.6 Audit collection system (internal vs. external)

An independent internal audit collection system is in place to collect and aggregate all relevant log information from the several ECB PKI systems and components. This system includes storage of historical data for later review and archival of information to a defined timeframe in compliance to ECB and governmental policies.

The ECB PKI is on-boarded to the ECB SIEM solution to facilitate the security teams alerting and store all events related to the ECB PKI in a central store.

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.

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

Certificate application information is archived.

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

The archive is protected in such a way that confidentiality and integrity is ensured and unauthorized access is prevented. An appropriate combination of physical and logical access controls is set in place.

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 are timed according to the maximum key lifetimes and renewal periods set out in the ECB Class 2 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

5.7 Compromise and Disaster Recovery

See section 5.7 of the ECB Class 2 PKI CP.

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 RTC for the service.

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

The ECB Class 2 Root CA 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.

5.7.3 Entity private key compromise procedures

If a compromise is suspected or discovered it should directly be reported to the ECB IT Service Desk and the revocation procedure of affected certificates and keys must be started immediately. Notification to subscribers and relying parties will be conducted using the standard ECB channels like Intranet announcements.

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.

5.8 CA or RA Termination

The terminal plan from section 5.8 of the ECB Class 2 PKI CP will address the following Notification of the termination to affected entities, such as subscribers and relying parties

- What type of support services will be continued
- How and if revocation and the issuance of CRLs will be continued
- Decisions if valid certificates of subscribers and subordinate CAs will be revoked
- Issuance of replacement certificates by a successor CA
- Destruction or storage 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

In accordance with the Certification Policy (CP) of the ECB Class 2 PKI

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 in Class 2 Trust Chain, are generated in hardware security modules with the FIPS 140-2 Level 3 certification.

All CA key pair generation is performed by a support of a HSM (Hardware Security Module). 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 at least follows the requirements of FIPS 140-2 Level 2.

Generation of subscriber key pairs is performed at the time of registration using at least a software cryptographic module meeting the requirement of FIPS 140-2 Level 2.

The Subscribers' cryptographic keys that serve to authenticate in systems are generated on USB-based smartcards with FIPS 140-2 level 3 certificates.

The Subscribers' cryptographic keys that are used to create an electronic signature are generated on USB-based smartcards with FIPS 140-2 level 3 certificates.

The Subscribers' cryptographic keys that serve to encrypt data sent between systems or users are generated in secure environment and installed on USB-based smartcards with FIPS 140-2 level 3 certificates with a copy on the security base of the issuing CA.

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

Private keys for ECB PKI subscribers are generated and protected locally (in particular keys for user certificates for authentication and signatures) or are generated remote to the subscriber within a secured environment using the ECB PKI certificate management application (in particular keys for user certificates for encryption).

For user certificates the delivery and transport of private keys is thus avoided where possible (for authentication and signature keys), and conducted in secured form where necessary (encryption key

pairs) to provide end to end confidentiality and mutual authentication of all related parties and PKI components.

For other subscribers (in case of machine certificates) the delivery and transport of private keys to subscribers is discouraged, and in case it is needed conducted in secured form (e.g. PKCS12 secured by a passphrase) to provide end to end confidentiality and mutual authentication of all related parties and PKI components.

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 Class 2 Root CA	4096 Bit RSA
ECB Class 2 Sub CA 01	4096 Bit RSA
ECB Class 2 Sub CA 02	4096 Bit RSA

ECB PKI Subscriber Key Size

All subscriber certificates will follow a standard of at least 2048 bit RSA while the use of keys below ECB PKI standard is prohibited in general and only applicable in connection with special business justification and approval of the ECB Security Board on a timely limited basis with clear indication of migration of the consuming application within the next 6 months.

6.1.6 Public key parameters generation and quality checking

ECB Class 2 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 Class 2 Root CA key usage

Certificate Signing

CRL Signing / Off-line CRL Signing

ECB Class 2 Sub CA 01 key usage

Certificate Signing

CRL Signing / Off-line CRL Signing

ECB Class 2 Sub CA 02 key usage

Certificate Signing

CRL Signing / Off-line CRL Signing

ECB PKI Subscriber Certificate Key Usage

ECB Class 2 Server Authentication	Digital Signature, Key Encipherment
ECB Class 2 Server Authentication CSR	Digital Signature, Key Encipherment
ECB Class 2 Server Client Authentication	Digital Signature, Key Encipherment
ECB Class 2 Server Client Authentication CSR	Digital Signature, Key Encipherment
ECB Class 2 Domain Controller Authentication	Digital Signature, Key Encipherment
ECB Class 2 Domain Controller Authentication CSR	Digital Signature, Key Encipherment
ECB Class 2 Client Authentication	Digital Signature
ECB Class 2 Client Authentication Manual	Digital Signature
ECB Class 2 OCSP Response Signing	Digital Signature
ECB Class 2 Admin Authentication	Digital Signature
ECB Class 2 User Authentication	Digital Signature
ECB Class 2 User Encryption	Key Encipherment
ECB Class 2 User Signature	Digital Signature (non-repudiation)
ECB Class 2 FIM CM Agent	Digital Signature, Key Encipherment
ECB Class 2 FIM CM Agent Admin Key Div.	Digital Signature, Key Encipherment
ECB Class 2 FIM CM Enrolment Agent	Digital Signature
ECB Class 2 FIM CM KR Agent	Key Encipherment

ECB Exchange Enrolment Agent (Offline request)	Digital Signature
ECB NDES Encryption	Key Encipherment
ECB NDES Signature	Digital Signature, Non-repudiation
ECB NDES Signature Encryption	Digital Signature, Key Encipherment
ECB CEP Encryption	Key Encipherment
ECB Class 2 Mobile Client Authentication	Digital Signature, Key Encipherment

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

- ECB Class 2 PKI Root CA key pairs are generated by a hardware security module (HSM) that complies at least with FIPS 140-2 Level 2.
- ECB Class 2 PKI Sub CA 01 key pair is generated by a hardware security module (HSM) that complies with FIPS 140-2 Level 2.
- ECB Class 2 PKI Sub CA 02 key pair is generated by a hardware security module (HSM) that complies with FIPS 140-2 Level 2.
- ECB Class 2 Sub CA 01 and Sub CA 02 based OCSP Response Signing certificate key pairs are generated by a hardware security module (HSM) that complies at least with FIPS 140-2 Level 2.
- ECB PKI ECB Class 2 Sub CA 02 subscriber user key pairs (authentication, signature, and encryption) are generated on USB tokens / smartcards with 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.

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

Not applicable for ECB PKI subscriber private keys.

On ECB Class 2 Root CA components cryptographic operations and private key access is implemented using a multi-eye principle based authorization, e.g. multiple trusted persons are needed to provide a quorum of required authorization tokens. This is achieved by using HSM token based authentication mechanisms that enforce multi-person control for key access authorization.

Indirectly the same is applicable for ECB Class 2 PKI Sub CA and OCSP responder private keys being protected by a shared Security Boundary for all related Hardware Security Modules and the respective administrative authorization tokens required within the HSM implementation: Due to high-availability and 24x7 automatic cluster failover requirements key access for these subordinate CAs and OCSP responder servers is granted based on existing configuration settings, HSM security boundary membership and in conjunction with the defined HSM modules which were configured based on the administrative authorization granted and enforced using a multi-eye principle based authentication.

6.2.3 Private Key escrow

Private Key escrow is not supported in the current ECB PKI implementation.

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 Class 2 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 archived. The keys are protected and stored encrypted using the implemented Key Recovery Agent certificate.

6.2.6 Private Key transfer into or from a cryptographic module

Private Key transfer into or from a cryptographic module protected storage is prohibited. Only HSM protected and initial created and HSM based private keys are allowed.

6.2.7 Private Key storage using cryptographic module

- ECB Class 2 Root CA private keys are protected by a Hardware Security Module (HSM) in conjunction with a multi-person control key access authorization implementation.
- ECB Class 2 PKI Sub CA 01 private keys are protected by a Hardware Security Module (HSM).
- ECB Class 2 PKI Sub CA 02 private keys are protected by a Hardware Security Module (HSM).
- ECB Class 2 OCSP response signing end-entity certificates and private keys are protected by a Hardware Security Module (HSM).
- All ECB PKI ECB Class 2 Sub CA 02 subscriber (user) key pairs (authentication, encryption, signature) are protected on smartcards with FIPS 140-2 level 3 certificates.

6.2.8 Method of activating private key

- ECB PKI uses only hardware-based keys for end-entity 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 only 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 Class 2 Root CA private keys are activated by a Hardware Security Module (HSM) in conjunction with a multi-person control implementation. Initial key generation was conducted during the key ceremony process outlined in the key ceremony documentation referenced in the document control section.

- ECB Class 2 Sub CA 01/ 02 and OCSP response signing private keys are activated by a Hardware Security Module (HSM). 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.

6.2.9 Method of deactivating private keys

- ECB Class 2 Root CA private keys are deactivated immediately by removal of the last HSM multi-person control token, upon session termination or service restart.
- ECB Class 2 Sub CA 01, Sub CA 02 and OCSP responder private keys are deactivated by a Hardware Security Module (HSM) or session termination.
- Shutdown of the subscriber machine will deactivate access to private keys on the local machine.
- Withdrawal of the USB-based smartcard from the USB port will deactivate access to private keys.

6.2.10 Method of destroying private keys

Destroying CA keys

CA keys are destroyed, when ECB terminates the ECB PKI certification services or implements a new certification service with new CA keys. CA key destruction is performed by securely deleting relevant HSM protected key containers and / or corresponding multi-person key control tokens.

Destroying user's 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.

6.2.11 Cryptographic Module Rating

Cryptographic Module Rating is listed in Section 3.2.1 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 2.5.4 "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 Class 2 Root CA	20 years	14 years
ECB Class 2 Sub CA 01	10 years	7 years
ECB Class 2 Sub CA 02	10 years	7 years

ECB PKI subscriber key usage periods

Subscriber Certificate Template	Validity Period	Renewal Period
ECB Class 2 Server Authentication	2 years	6 weeks
ECB Class 2 Server Authentication CSR	2 years	6 weeks
ECB Class 2 Server Client Authentication	2 years	6 weeks
ECB Class 2 Server Client Authentication CSR	2 years	6 weeks
ECB Class 2 Domain Controller Authentication	1 year	6 weeks
ECB Class 2 Domain Controller Authentication CSR	2 years	6 weeks
ECB Class 2 Client Authentication	1 year	6 weeks
ECB Class 2 OCSP Response Signing	2 weeks	2 days
ECB Class 2 Admin Authentication	3 years	6 weeks
ECB Class 2 User Authentication	3 years	6 weeks
ECB Class 2 User Encryption	3 years	6 weeks
ECB Class 2 User Signature	3 years	6 weeks
ECB Class 2 FIM CM Agent	3 years	8 weeks
ECB Class 2 FIM CM Agent Admin Key Diversification	3 years	8 weeks
ECB Class 2 FIM CM Enrolment Agent	3 years	8 weeks
ECB Class 2 FIM CM KR Agent	3 years	8 weeks
ECB Exchange Enrolment Agent (Offline request)	2 years	6 weeks
ECB CEP Encryption	2 years	6 weeks
ECB NDES Encryption	2 years	6 weeks
ECN NDES Signature	2 years	6 weeks
ECB NDES Signature Encryption	2 years	6 weeks
ECB Class 2 Mobile Client Authentication	1 year	6 weeks

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 Subscriber's private key (PIN) is performed via MIM CM enrolment process during which a random PIN is set at the time of generating a cryptographic key on user's USB-based smartcard. They are mostly used for individual authentication. Activation Data is either handed over immediately or delivered later on to the user, via a different channel than the USB token. In case of guided enrolment of a subscriber the activation data is chosen and set by the subscriber and does not need transport or transmission.

Shared secrets used for the protection of the CA private keys are generated using HSM devices and are protected by Security World that requires quorum for data activation using smart cards assigned to HSM Operators. 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 OCS quorum 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 hardened operating system servers and HSM components.

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.

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.

6.8 Time-stamping

ECB PKI CAs uses time stamps to provide information of the issuance time of certificates and CRLs. The time source is the local computer clock device of the directory integrated CAs that is synchronized with ECB directory domain controllers themselves using a qualified external time source.

The local computer clock of the standalone ECB Class 2 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 Class 2 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. Five 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 5 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 L2 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 and in the presence of the ECB Security Board representatives 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 L2 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 and in the presence of the ECB Security Board representatives 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. 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.

Level	Description of conditions and requirements
	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 machine or technical service 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 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

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 Class 2 Root CA	1
ECB Class 2 Sub CA 01	2
ECB Class 2 Sub CA 02	2
ECB Class 2 OCSP Response Signing	2
ECB Class 2 Admin Authentication	3
ECB Class 2 User Authentication	3
ECB Class 2 User Encryption	4
ECB Class 2 User Signature	3

ECB Class 2 FIM CM Agent	4
ECB Class 2 FIM CM Agent Admin Key Diversification	4
ECB Class 2 FIM CM Enrolment Agent	4
ECB Class 2 FIM CM KR Agent	4
ECB Class 2 Domain Controller Authentication	5
ECB Class 2 Domain Controller Authentication CSR	5
ECB Class 2 Client Authentication	5
ECB Class 2 Server Authentication	5
ECB Class 2 Server Authentication CSR	5
ECB Class 2 Server Client Authentication	5
ECB Class 2 Server Client Authentication CSR	5
ECB Exchange Enrolment Agent (Offline request)	5
ECB CEP Encryption	5
ECB NDES Encryption	5
ECN NDES Signature	5
ECB NDES Signature Encryption	5
ECB Class 2 Mobile Client 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

Attribute	Value
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 Class 2 Root CA	
X.509 Version	V3
Serial Number	present
Signature Algorithm	sha256RSA
Issuer	CN = ECB Class 2 Root CA O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	present
Valid to	present
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB Class 2 Root CA 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=1
Subject Key Identifier	present
Authority Key Identifier	present
CRL Distribution Points	none
Authority Information Access	none
Subject Alternative Name	none
Extended Key Usage	none
Thumbprint Algorithm	sha1
Thumbprint	present

ECB Class 2 Sub CA 01	
X.509 Version	V3
Serial Number	present

ECB Class 2 Sub CA 01	
Signature Algorithm	sha256RSA
Issuer	CN = ECB Class 2 Root CA O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	present
Valid to	present
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB Class 2 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	present
Authority Key Identifier	present
CRL Distribution Points	HTTP URL reference to CDP Location
Authority Information Access	HTTP URL reference to AIA Location
Subject Alternative Name	none
Extended Key Usage	none
Thumbprint Algorithm	sha1
Thumbprint	present

ECB Class 2 Sub CA 02	
X.509 Version	V3
Serial Number	present
Signature Algorithm	sha256RSA
Issuer	CN = ECB Class 2 Root CA O = European Central Bank C = EU
Key Length	4096 Bit
Valid from	present
Valid to	present
Public Key	RSA (4096-Bit) Key Blob
Subject	CN = ECB Class 2 Sub CA 02 O = European Central Bank C = EU
Key Usage (critical)	Certificate Signing, CRL Signing, CRL Signing (offline).

ECB Class 2 Sub CA 02	
Basic Constraints (critical)	Subject Type=CA, Path Length Constraint=0
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
Subject Alternative Name	none
Extended Key Usage	none
Thumbprint Algorithm	sha1
Thumbprint	present

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 Class 2 End-Entity Certificate	
X.509 Version	V3
Serial Number	present
Signature Algorithm	sha256RSA
Issuer	CN = ECB Class 2 Sub CA 01 O = European Central Bank C = EU - or - CN = ECB Class 2 Sub CA 02 O = European Central Bank C = EU
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

ECB Class 2 End-Entity Certificate	
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
Thumbprint Algorithm	sha1
Thumbprint	present

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, IP security IKE intermediate, OCSP Signing Certificate Request Agent Key Recovery Agent Document Encryption Secure Email BitLocker Encrypting File System	No
Subject Key Identifier	Unique number corresponding to the subject's public key. The key identifier method is used.	No

Extension	Possible Values	Critical Flag
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	[1]Certificate Policy: Policy Identifier=ECB Class 2 Issuance Policy [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.pki.ecb.europa.eu/	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
Application Policies	1.3.6.1.4.1.311.21.10	No

7.1.3 Algorithm object identifiers

ECB Class 2 PKI certification authorities are signing issued certificates with Sha256WithRSAEncryption signature algorithm.

Algorithm OID 1.2.840.113549.1.1.11 (Sha256WithRSAEncryption)

ECB Class 2 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]

7.1.5 Name constraints

Not applicable.

7.1.6 Certificate policy object identifier

- ECB Class 2 PKI Trust Chain is using policy OID of 1.3.6.1.4.1.41697.509.2.100.10.1

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 http://www.pki.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 certificate. 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	Unique number corresponding to the authority's public key. The key identifier method is used.	No
CRL Number	Unique increasing number per CRL	No
Freshest CRL	Only in complete CRLs. Identifies how delta CRL information for this complete CRL is obtained	No

Additionally ECB PKI uses the following Microsoft CRL extensions.

Extension	OID	Critical Flag
CA Version	1.3.6.1.4.1.311.21.1	No
Next CRL Publish	1.3.6.1.4.1.311.21.4	No
Published CRL Locations	1.3.6.1.4.1.311.21.14	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 Class 2 PKI online Sub CAs issue OCSP Response Signing Certificates to internal 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 Class 2 OCSP Response Signing	
X.509 Version	V3
Serial Number	present
Signature Algorithm	Sha256RSA
Issuer	CN= ECB Class 2 Sub CA 01 O= European Central Bank C= EU - or -

ECB Class 2 OCSP Response Signing	
	CN= ECB Class 2 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	DNS=<FQDN OCSP Server>
Key Usage	Digital Signature
Subject Key Identifier	present
Authority Key Identifier	<ECB Class 2 Sub CA 01 Key ID Hash> - or - <ECB Class 2 Sub CA 02 Key ID Hash>
Subject Alternative Name	DNS=<FQDN OCSP Server>
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 ECB Class 2 OCSP response signing certificates in accordance with RFC 5280.

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
Certificate Issuance Policies	[1]Certificate Policy: Policy Identifier=ECB Class 2 Issuance Policy [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS	No

Extension	Value	Critical Flag
	Qualifier: http://www.pki.ecb.europa.eu/	

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. The audit report will be shared with the PKI AB.

8.2 Identity/qualifications of assessor

Compliance audits are performed by ECB internal resources or the ESCB Internal Auditors Committee (IAC) according to the annual audit program. Compliancy Audit for the ECB PKI is conducted by the PKI-AB.

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 ECB-PKI will be audited by the PKI-AB at least once every 3 years, in accordance with the ESCB Certificate Acceptance Framework, compliancy to CAF requirement will be provided to SRM-WG by written procedure within the defined time frame.

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.

Additional communication must be provided to PKI-AB in written within the defined time frame.

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

No liability accepted.

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

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.

9.3.3 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.

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.

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

9.10 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. Term and Termination

9.10.1 Term

This CPS shall come into force from the moment it is published 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 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regards to the processing of personal data by the Community institutions and bodies and of free movement of such a data.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

All users and relying parties of ECB PKI accept the content of the latest version of this CPS and the applicable CPs in their entirety.

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.