EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB CLASS 2 PKI

Issuance Policy
(1.3.6.1.4.1.41697.509.2.100.10.1)

Table of Contents

EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB CLASS 2 PKI

Certificate Policy (CP)

Table of Contents

Document control

Basic Description

Document title	ECB CLASS 2 PKI Certificate Policy (CP)
Topic	Certificate Policy for the ECB CLASS 2 PKI Service based on RFC 3647
Version	3.1
Status	Published release related to recertification for CAF compliancy
Document OID	1.3.6.1.4.1.41697.509.2.100.20.1
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	CP format adjusted to RFC.3467, further amendments
2.0	08.07.2015	Published version according to Release 2.0 of ECB PKI
3.0	04.08.2020	Revised version for Certificate Services Release 4.0
3.1	10.01.2024	Revised version for regular CAF compliancy review

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 Divison)	22.04.2020
3.0	04.08.2020	Magi Clave (Deputy Director General Information Systems)	27.08.2020

Related Documents

Document title	ECB CLASS 2 PKI Certification Practice Statement (CPS)
Document Name	ECB CLASS 2 PKI CPS v3.1.pdf
Description	Certification Practice Statement for the ECB CLASS 2 PKI Service
Document OID	1.3.6.1.4.1.41697.509.2.100.20.2
Latest available version	V3.1
Last changed	10.01.2024

Document title	ECB PKI Certificate Profiles
Document Name	ECB PKI Certificate Profiles RFC 5280 v4.0.xlsx
Description	RFC5280 Certificate Profiles for ECB CLASS 2 PKI
Latest available version	V3.1
Last changed	13.06.2023

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

1 Introduction

The X.509 standard defines a Certificate Policy (CP) as "a named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements". An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.

The Certificate Policy (CP) 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 acting according to the certificate policy. Thus, the existence of policies is critical when dealing with a reliable PKI or certification services.

This certificate policy document describes the policies of the Certification Authorities (CAs) operated by European Central Bank. It is applicable to all entities that have relationships with the ECB PKI CAs, including end users-, cross-certified CAs, and Registration Authorities (RAs). This Certificate Policy document provides those entities with a clear statement of the policies and responsibilities of the ECB PKI and its CAs, as well as the responsibilities of each entity in dealing with ECB PKI CAs.

The ECB PKI certification service is only as trustworthy as the procedures contained and operated in it. The ECB Class 2 PKI Certificate Policy therefore covers all relevant preconditions, regulations, processes and measures within the ECB Class 2 PKI certification service as a compact information source for current and potential participants.

This document will rely on other parts of the general ECB PKI certification service documentation and will sum up information that is of importance for the participating PKI users. Other related documentation is referenced in this Certificate Policy document where relevant while an overview of other documents is listed in the document control section.

It should be provided for free and be 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"[1] which supports up to date cryptographic algorithms. All certificates, regardless of CA or subscriber / end-entity, within the 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, and issuing subordinate CAs certified by it. The Root CA and Issuing subordinate CAs in the Class 2 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 issuance of machine-based certificates, while the ECB Class 2 Sub CA 02 is used to issue user-based certificates. The Root CA and Issuing subordinate CAs in the Class 2 define the whole CA certificate chain.

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

[1] When ECB PKI infrastructure was designed, a Class 1 and a Class 2 trust chains were built, ECB Class 1 for providing legacy cryptographic algorithms and ECB Class 2 for providing up to date implementations. In the meantime, the ECB Class 1 trust chain has been decommissioned so only the ECB Class 2 trust chain is in place at the moment.

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 directory infrastructure.

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 CP is called "**ECB Class 2 PKI Certificate Policy**" 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 N.B.: The ECB Class 2 PKI issuance policy is a unified document, comprised of both the ECB Class 2 PKI Certificate Policy (OID 1.3.6.1.4.1.41697.509.2.100.20.1) and the ECB Class 2 PKI Certificate Practice Statement (OID 1.3.6.1.4.1.41697.509.2.100.20.2), identified by an OID within this namespace.

X.509 OID – Issuance Policy identifiers

1.3.6.1.4.1.41697.509.2.100.10.**1**	ECB Class 2 PKI issuance policy (the actual issuance policy document, comprised of both the ECB Class 2 PKI Certificate Policy (OID 1.3.6.1.4.1.41697.509.2.100.20.1) and the ECB Class 2 PKI Certificate Practice Statement (OID 1.3.6.1.4.1.41697.509.2.100.20.2).

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 v3.1

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 v3.1

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

1.3.1 Certification Authorities

European Central Bank operates a two-tier CA hierarchy ECB Class 2 trust chain, which issues machine and user certificates to ECB employees and ECB partners.

The two-tier CA hierarchy is built upon:

- the offline ECB Class 2 Root CA
- two issuing subordinate CAs:
  - ECB Class 2 Sub CA 01 for machine-based certificates (listed here for completeness),
  - ECB Class 2 Sub CA 02 (for user-based certificates)

The certificate services hierarchy does not depend on the existing ECB LDAP directory hierarchy, it can be structured independently.

Physically, the offline Root CA and the respective two issuing CAs as well as all other PKI related infrastructure services are located in the ECB data centres at Frankfurt, Germany.

1.3.2 Registration Authorities

ECB PKI Registration Authority (RA) is an integral function of ECB PKI with online access to the Certificate Authority. The ECB PKI RA allows initiating a certificate request to the CA. For online requests only ECB Active Directory authorized objects are allowed to request for issuance of certificates. Offline requests for manually enrolled certificates following different subject naming schemes or enrolment requests for Active Directory integrated systems are issued with manual validation by authorized personnel before issuance.

User authorization is granted through the ECB identity and access management process. The Registration Authority console is the interface which is provided by the ECB PKI certificate management solution based on the existing ECB identity management processes.

The ECB PKI user authentication certificates are based on dedicated USB-based smartcards. The provisioning of these tokens is performed by the ECB Service Desk team according to the rules and procedures defined for the ECB employees and contractors.

In addition, ECB PKI issues software certificates for Code Signing and specifically for user client authentication based on automated certificate enrolment controlled by Active Directory service and permissions.

Machine authorization is granted by the ECB hardware / software deployment process while automated machine-based certificate enrolment is controlled by Active Directory service and permissions.

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.

1.3.4 Relying parties

A relying party is any entity who relies upon a certificate that is issued by an Issuing CA or Root CA and that is used in a manner consistent with this CP. A relying party could be within or outside the organization of European Central Bank. For instance, a web application that checks the validity of a user authentication certificate during log on. Relying parties implicitly agree to the terms of this CP documentation, the CPS documentation and referenced general ECB security policies in their respective latest version.

1.3.5 Other participants

Not applicable

1.4 Certificate Usage

The use and protection of keys and certificates will be on the sole responsibility of each subscriber and relying party.

The ECB PKI is primarily for internal use, and therefore no certification by any external mutual trusted third party is sought for trust validation. Partners and other external entities should not assume any higher level of trust than assigned internally within European Central Bank.

The certificates issued by the ECB PKI are as follows:

ECB Class 2 Trust Chain

Certificates issued by ECB Class 2 Root CA

Certificate Name Type	Purpose of issued certificate
Subordinate Certification Authority	Issue certificates for ECB Class 2 PKI subordinate certification authorities

Certificates issued by ECB Class 2 Sub CA 01

Certificate Name Type	Purpose of issued certificate
ECB Class 2 Domain Controller Authentication	Domain Controller Authentication

ECB Class 2 Domain Controller Authentication CSR	Domain Controller Authentication
ECB Class 2 Server Authentication	Server Authentication
ECB Class 2 Server Authentication CSR	Server Authentication
ECB Class 2 Client Authentication	Client Authentication
ECB Class 2 Server Client Authentication	Server Authentication, Client Authentication
ECB Class 2 Server Client Authentication CSR	Server Authentication, Client Authentication
ECB Class 2 OCSP Response Signing	OCSP response signing
ECB Exchange Enrolment Agent (Offline request)	Certificate Request Agent
ECB CEP Encryption	Certificate Request Agent
ECB NDES Encryption	
ECN NDES Signature	
ECB NDES Signature Encryption	Client Authentication
ECB Class 2 Mobile Client Authentication	Client Authentication
ECB Class 2 Hybrid Client Authentication	Client Authentication

Certificates issued by ECB Class 2 Sub CA 02

Certificate Name Type	Purpose of issued certificate
ECB Class 2 User Authentication	ECB user authentication
ECB Class 2 User Encryption	ECB user encryption
ECB Class 2 User Signature	ECB user signature
ECB Class 2 OCSP Response Signing	OCSP response signing
ECB Class 2 FIM CM Agent	Certificate management Enrolment agent authentication
ECB Class 2 FIM CM Agent Admin - Key Diversify	Certificate management admin key diversification
ECB Class 2 FIM CM Enrolment Agent	Certificate management certificate request agent
ECB Class 2 FIM CM KR Agent	Certificate management Key recovery agent
ECB Class 2 Code Signing	Code Signing
ECB Class 2 User Client Authentication	Client Authentication

For further details please refer to the RFC5280 certificate profile document referenced in the related documents section which is available upon request.

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 to ECB employees are issued in two forms:

- USB-Based smartcards for authentication, digital signature or encryption with only one purpose per certificate
- Software-based for Code Signing and VPN client authentication, with only one purpose per certificate (distinguishable from the USB-based smartcard certificates)

ECB PKI machine certificates may only be used for authentication purposes and to ensure the confidentiality of communication channels.

1.4.2 Prohibited certificate uses

Generally, any usage not covered in sections 1.4. Certificate Usage, 1.4.1 Appropriate certificate uses, in particular, the following use is explicitly prohibited:

- use of subscriber end entity certificates as CA certificates,
- use of subscriber end entity certificate for different purposes other than outlined in the certification request,
- use of subscriber end entity certificates outside of their given validity period,
- use of subscriber end entity certificates after revocation by the ECB PKI,
- use of machine certificates on non-ECB and on non-certified partner machines and devices, and
- use of 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. 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
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 CP approval procedures

The European Central Bank Deputy Director General Information Systems and the European Central Bank Head of Digital Security Services Division 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 to delegate 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

2.1 Repositories

The central repository for the ECB PKI CAs is provided by an LDAP directory. The protocol used to access the directory is the Lightweight Directory Access Protocol (LDAP) version 3, as specified in Internet RFC 4510.

For availability reasons and to ease access to specific information, such as CP / CPS documentation and certificate-based references, an alternate repository is provided (ECB PKI Web site located at http://www.pki.ecb.europa.eu). The protocol used to access the ECB PKI site and certificate-based references is HTTP, with the latest version of the CP/CPS at:

https://cps.pki.ecb.europa.eu/CPS/ECB-CLASS-2-PKI-CPS-v3.0-FINAL.pdf Both documents, CP and CPS, are subject of the regulations in place at the ECB defined in the internal rules.

2.2 Publication of Certification Information

The ECB PKI publishes information regarding its PKI services (CRLs and CA certificates) except CP and CPS to both locations listed in 2.1. CP and CPS documentation is published to the ECB PKI web site only.

ECB PKI end-entity certificates may be published in the central repositories depending on appropriate end-entity certificate purposes according to certificate profiles in their most current version.

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 via the Internet. Additionally an OCSP service is accessible ECB internally and externally. The ECB has implemented logical and physical security controls to restrict modifying (including adding and deleting) repository entries to authorized staff only. The ECB Active Directory repository is limited to ECB internal certificate subscribers and trusted relying parties who have a valid ECB Active Directory account. Access to this repository is controlled by appropriate Active Directory permissions and is based on the ECB identity and access management policies.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

ECB Class 2 Trust Chain

CA certificate naming of the **ECB Class 2 Root CA**

Attribute	Value
Subject Name	CN = ECB Class 2 Root CA O = European Central Bank C = EU
Subject Alternative Name	None

CA certificate naming of the **ECB Class 2 Sub CA 01** (listed here for completeness)

Attribute	Value
Subject Name	CN = ECB Class 2 Sub CA 01 O = European Central Bank C = EU
Subject Alternative Name	None

CA certificate naming of the **ECB Class 2 Sub CA 02**

Attribute	Value
Subject Name	CN = ECB Class 2 Sub CA 02 O = European Central Bank C = EU
Subject Alternative Name	None

Subscriber certificate naming of **ECB Class 2 Domain Controller Authentication**

Attribute	Value
Subject Name	CN = <Domain Controller FQDN>
Subject Alternative Name (DNS)	<Domain Controller FQDN> <Domain DNS Name> <Domain NetBios Shortname>

Subscriber certificate naming of **ECB Class 2 Domain Controller Authentication CSR**

Attribute	Value
Subject Name	CN = <Domain Controller FQDN>

Subject Alternative Name (DNS)	<Domain Controller FQDN> <Domain DNS Name> <Domain NetBios Shortname> <LDAP FQDN>

Subscriber certificate naming of **ECB Class 2 Server Authentication**

Attribute	Value
Subject Name	CN = <Server FQDN / HTTP Host Header>
Subject Alternative Name (DNS)	<Multiple Server FQDN / HTTP Host Header / Domain Names>

Subscriber certificate naming of **ECB Class 2 Server Authentication CSR**

Attribute	Value
Subject Name	CN = <Server FQDN / HTTP Host Header>
Subject Alternative Name (DNS)	<Multiple Server FQDN / HTTP Host Header / Domain Names>

Subscriber certificate naming of **ECB Class 2 Client Authentication**

Attribute	Value
Subject Name	CN = <Client FQDN>
Subject Alternative Name (DNS)	<Client FQDN>

Subscriber certificate naming of **ECB Class 2 Server Client Authentication**

Attribute	Value
Subject Name	CN = <Server / Client FQDN / HTTP Host Header>
Subject Alternative Name (DNS)	<Multiple Server FQDN / HTTP Host Header / Domain Names>

Subscriber certificate naming of **ECB Class 2 Server Client Authentication CSR**

Attribute	Value
Subject Name	CN = <Server / Client FQDN / HTTP Host Header>
Subject Alternative Name (DNS)	<Multiple Server FQDN / HTTP Host Header / Domain Names>

Subscriber certificate naming of **ECB Exchange Enrolment Agent (Offline Request)**

Attribute	Value
Subject Name	CN = <[SCEP Server]-MSCEP-RA-SIGN >

Subscriber certificate naming of **ECB CEP Encryption**

Attribute	Value
Subject Name	CN = <[SCEP Server]-MSCEP-RA-ENC >

Subscriber certificate naming of **ECB NDES Signature Encryption**

Attribute	Value
Subject Name	CN = <Client FQDN>
Subject Alternative Name (DNS)	<Client FQDN>

Subscriber certificate naming of **ECB NDES Encryption**

Attribute	Value
Subject Name	CN =
Subject Alternative Name (DNS)	

Subscriber certificate naming of **ECB NDES Signature**

Attribute	Value
Subject Name	CN =
Subject Alternative Name (DNS)	

Subscriber certificate naming of **ECB Class 2 OCSP Response Signing**

Attribute	Value
Subject Name	CN = <OCSP Responder FQDN>
Subject Alternative Name (DNS)	<OCSP Responder FQDN>

Subscriber certificate naming of **ECB Class 2 Mobile Client Authentication**

Attribute	Value
Subject Name	E = <First Name>.<Last Name>@ecb.europa.eu CN = <First Name>.<Last Name>
Subject Alternative Name (DNS)	<Mobile Client FQDN>

Subscriber certificate naming of **ECB Class 2 Hybrid Client Authentication**

Attribute	Value

Subject Name	CN = <FQDN Client>
Subject Alternative Name (DNS)	<MachineNetBIOS>

Currently issued subscriber certificate naming of **ECB Class 2 User Authentication**

Attribute	Value
Subject Name	CN = <[AUT]> <Last Name>, <First Name>
Subject Alternative Name (UPN)	<UPN of Standard User Account>

Currently issued subscriber certificate naming of **ECB Class 2 User Encryption**

Attribute	Value
Subject Name	CN = <[ENC]> <Last Name>, <First Name>
Subject Alternative Name (Email)	<Email of Standard User Account>

Currently issued subscriber certificate naming of **ECB Class 2 User Signature**

Attribute	Value
Subject Name	CN = <[SIG]> <Last Name>, <First Name>
Subject Alternative Name (Email)	<Email of Standard User Account>

*Future Subscriber certificate naming of **ECB Class 2 User Authentication***

Attribute	*Value*
Subject Name	*CN = <[AUT]> <Last Name>, <First Name> (<User Login>)*
Subject Alternative Name (UPN)	*<UPN of Standard User Account>*

*Future Subscriber certificate naming of **ECB Class 2 User Encryption***

Attribute	*Value*
Subject Name	*CN = <[ENC]> <Last Name>, <First Name> (<User Login>)*
Subject Alternative Name (UPN)	*<Email of Standard User Account>*

*Future Subscriber certificate naming of **ECB Class 2 User Signature***

Attribute	*Value*
Subject Name	*CN = <[SIG]> <Last Name>, <First Name> (<User Login>)*
Subject Alternative Name (UPN)	*<Email of Standard User Account>*

Subscriber certificate naming of **ECB Class 2 FIM CM Agent**

Attribute	Value	
Subject Name	CN =	<FIM CM Agent Name>
Subject Alternative Name (UPN)		<UPN of FIM CM Agent Account>

Subscriber certificate naming of **ECB Class 2 FIM CM Agent Admin Key Diversification**

Attribute	Value	
Subject Name	CN =	<FIM CM Agent Name>
Subject Alternative Name (UPN)		<UPN of FIM CM Admin Key Diversification User Account>

Subscriber certificate naming of **ECB Class 2 FIM CM Enrolment Agent**

Attribute	Value	
Subject Name	CN =	<FIM CM Enrolment Agent Name>
Subject Alternative Name (UPN)		<UPN of FIM CM Enrolment Agent User Account>

Subscriber certificate naming of **ECB Class 2 FIM CM KR Agent**

Attribute	Value	
Subject Name	CN =	<FIM CM Key Recovery Agent Name>
Subject Alternative Name (UPN)		<UPN of FIM CM KR Agent Account>

Subscriber certificate naming of **ECB Class 2 Code Signing**

Attribute	Value	
Subject Name	CN =	<Service / Application Name>

Subscriber certificate naming of **ECB Class 2 User Client Authentication**

Attribute	Value
Subject Name	CN = <[AUT]> <Last Name>, <First Name>
Subject Alternative Name (UPN)	<UPN of Standard User Account>

3.1.2 Need for names to be meaningful

The semantics of the names used is commonly understood; therefore the identity of the subjects can be determined. User names and all machine names must exactly match the entries in the forms supplied at the time of the subscriber's registration and certificate enrolment.

3.1.3 Anonymity or pseudonymity of subscribers

ECB PKI supports neither anonymous users nor pseudonyms for users.

Machine/device subscribers of certificate services cannot be anonymous, but are allowed to 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 / teams (technical groups) 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

3.1.5 Uniqueness of names

For user certificates the subject attribute must be unique over the lifetime of the CA, and the subject alternative names must be unique at any given point in time.

For machine certificates the uniqueness of the subject name and subject alternative names of the certificates must be unique at any given point in time, except for environments with technical requirements to have multiple certificates issued with the same name due to high availability implementations.

3.1.6 Recognition, authentication, and role of trademarks

No trademarks will be knowingly used. No explicit check of any name will be conducted, as all names will only be used by ECB internally and approved business partners and not published on any open sources.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

The certificate applicant's possession of a private key is proved through the use of a digitally signed PKCS#10 or CMC[2] certificate request. This request is signed with the corresponding private key of the certificate subscriber.

3.2.2 Authentication of organization identity

Not applicable.

[2] See RFC 5272, "Certificate Management over CMS (CMC)", https://tools.ietf.org/html/rfc5272

3.2.3 Authentication of individual identity

The group of users who can be the subject of a user certificate under this Certificate Policy (to be issued by ECB PKI Class 2 Sub CA 02 either through own request or enrolled on behalf) entity requesting a certificate depends on the type of entity, and as such on the sub CA which will issue the certificate. In any case certificate requests to the ECB PKI are restricted to subscribers with a valid user account in the ECB central Identity Governance & Access Management (IGAM) system. Authentication of the individual user identity is established as follows:

1. Certificates on smartcards for individual subscribers (users) rely on the HR, physical security, and identity management processes which provide a relation between identity, corporate badge and user account in Active Directory. When users are on-boarded a badge is issued to them based on pre-entered HR and contract information which was obtained and recorded during the hiring process. During the ECB's badge issuing process the user's identity is verified by ECB's physical security officers against a national ID document, i.e. the physical security officer verifies the national ID document for authenticity, checks the person against the document and then issues the badge which includes a photograph of the user taken on that occasion. Thereby the badge is a representation of the positive outcome of this identity verification process. For remote onboarding where no badge is supplied, the successful identity verification is recorded in ISIS and the user account gets created only when the outcome of this action is positive – via IGAM. The following scenarios apply, following the ECB's general decision to employ 2-factor authentication, in particular on end-user systems (laptops, desktops) using USB-based smartcards:
    a. Users are subscribed[3] as part of the on-boarding process when they join the organization. The USB-based smartcard with certificates is produced by the registration officer on behalf of the user and protected by a randomly generated PIN. The USB-based smart card and the PIN letter – for remote onboarding SMS (personal phone and shipping address being confirmed during identity verification) are separately delivered to the new user on the first day, at least one of them after verifying the subscriber's identity using the badge (or a photo ID if the badge is not yet ready)[4]. The users are instructed to change the initial PIN at first use, and are handed over the terms & conditions. Certificate acceptance is corroborated by use of the USB-based smart card (see section 4.4).
    b. A guided enrolment procedure is possible as backup procedure. The registration officer verifies the existence of the user account (and thus the user's eligibility) and the user identity, and subsequently triggers the enrolment. The PKI system sends an email with a one-time-password to the user. The user then finalizes the enrolment of

[3] Authorisation is implicitly given by the ECB's decision to introduce 2-factor authentication on all its end-user systems, thereby requiring issuance of the USB-based smartcard to all its member of staff and eligible contractors.

[4] Thus, user identity is verified either directly or indirectly via the corporate badge which is only issued after the physical security officer has successfully verified the user's identity using a photo ID.

the USB-based smartcard in the PKI system using the one-time password. Finally, the user reviews the certificates (and accepts them by this action, see section 4.4) and sets the activation data (PIN) for the USB-based smart card.

c. When a user has lost or forgotten the USB-based smart card, or it is defective, the user needs to appear at the service desk, or in case of remote onboarding the user must have personal phone and shipping address confirmed, where the user's badge or photo ID is checked, and a new smartcard is issued with new certificates, with a random PIN, which the user is instructed to change on next use. The old certificates are revoked as per section 4.8. Certificate acceptance is corroborated by use of the USB-based smart card and the containing certificates (see section 4.4).

d. (For historic reference) For the initial rollout, i.e. first-time issuance of certificates, of the USB-based smartcards and their respective PINs to the existing users the users are subscribed[5] centrally by an registration agent who prepares the smartcard, prints the PIN letter (with a randomly generated PIN), and places both in separate envelopes, with a tamper-evident seal applied to the PIN letter. The USB-based smartcards and PIN letters are handed out via an organizational entity's management assistant who verifies the user's identity using the badge. Users are handed over the terms & conditions, and are educated about the properties of the tamper-evident seal, and are instructed to look for an unbroken seal, report if tampered with, and otherwise change the PIN on first use. Certificate acceptance is corroborated by use of the USB-based smart card (see section 4.4).

2. Software Certificates for individual subscribers (users) for Code Signing and VPN Client authentication can only be requested by users with a valid Active Directory account. The authentication is performed by a successful logon to the ECB Identity Management system.
3. Certificates for machine or device subscribers requested online or offline via the ECB PKI certificate enrolment process can only be requested by users with a valid Active Directory user account. The authentication is performed by
   a) A successful logon to the ECB LDAP directory,
   b) A valid corporate ECB email address and addition information to verify the requestor during the enrolment and approval process, or
   c) On behalf of an approved partner user or devices by authorized ECB internal staff.

In the cases of item 1.a., 1.b., and 1.d. the terms & conditions handed over to the subscriber serve as a reminder of already existing and contractually agreed-to obligations as stated in the ECB internal rules. Explicit certificate acceptance does not apply as per section 4.4.

[5] Authorisation is implicitly given by the ECB's decision to introduce 2-factor authentication on all its end-user systems, thereby requiring issuance of the USB-based smartcard to all its member of staff and eligible contractors.

3.2.4 Non-verified subscriber information

All information in user certificates is obtained from the ECB Identity systems, thus, there is no non-verified subscriber information to handle. Machine certificate requests require a valid ECB contact responsible for enrolment of the corresponding end-entity certificate. Code Signing certificate requests are validated against ECB internal IT Service Catalogue.

All other non-verifiable information and / or information that cannot be validated 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 USB-based smartcard 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 need to be validated to 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 needs to be communicated without prior notice to the responsible ECB PKI certificate and enrolment authority. Unless the machine or device is considered "End of Life" and is to be decommissioned a new administrative contact taking up the responsibilities of the former administrative contact is mandatory. This especially applies to virtual machines and is not limited to physical hardware.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and Authentication for Re-key Requests

The ECB PKI offers that a subscriber obtains a new certificate before the existing certificate expiresvia a re-key request. A requirement of the ECB PKI is that the existing certificate is still valid and not revoked at the time of the request, and that a new key pair is replacing the existing key pair. This is verified on the public keys.

If a valid certificate does not exist anymore, e.g. due to expiration or revocation, a new enrolment procedure as per section 3.2 is required.

3.3.1 Identification and authentication for routine re-key

A re-key request must contain the new key and is signed using the current valid key. Failure to conduct a routine re-keying process before expiration of the existing certificate requires a new initial enrolment request as per section 3.2. In case of Encryption certificates, the re-key request will contain the new key signed with the current valid key which continues to exist on the respective USB based smartcard.

Routine re-key for user certificates

The HR and identity management processes of the ECB ensure that user accounts and physical access badges of users who are no longer ECB employees are disabled. This ensures that physical and logical access to the ECB's systems including facilities to request re-keying is only possible for users who, at that particular day, are ECB employees or ECB contractors. This constitutes an implicit authorization of eligibility for re-keying. As these are integrated automated processes, the particular user has no influence, and thus cannot self-renew his/her certificate.

The mapping established for the initial enrolment between the user's identity, his/her USB-based smartcard and his/her user account, a valid and non-disabled user account in the Active Directory and an existing valid certificate authorize a user to issue a re-key request.

Given the certificate package ECB users have (authentication/signature/encryption certificates) on the USB-based smartcard, the re-key request must contain, besides the signature with an existing key, all the new keys of the new package (1 or 3 keys) at the same time. No individual re-key of a single certificate in a 3-key package is supported.

Routine re-key for machine certificates requested manually online or offline via ECB PKI certificate management process

Routine re-keying for auto-enrolled machine and device certificates is performed automatically, prior to certificate expiration within the certificate renewal period. Subscribers are identified and authenticated for the automatic re-keying process by the Active Directory and corresponding permissions. A re-key request contains the new key and is signed using the current valid key.

Routine re-keying for device certificates requested online or offline via ECB PKI certificate management process is performed manually prior to certificate expiration within the certificate renewal period.

(Technical) users are identified and authenticated for the controlled re-keying process by

(1) a successful logon to the ECB Active Directory, or
(2) a valid corporate ECB email address and additional information identifying the requestor.

3.3.2 Identification and authentication for re-key after revocation

No re-key is supported after revocation of a certificate. The process for initial enrolment needs to be followed in this case, see section 3.2

3.4 Identification and Authentication for Revocation Requests

In order to avoid delay in disabling compromised credentials, temporary revocation requests can be raised by any ECB employee with minimal validation requirements (e.g. known telephone number, known email address or personal knowledge). Any temporary revocation request will trigger a process to either permanently invoke or cancel the revocation which includes appropriate identification and authentication mechanisms.

Further details are given in section 4.9.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Requests for

-
- ECB Class 2 Hybrid Mobile Authentication
- ECB Class 2 User Authentication
- ECB Class 2 User Encryption
- ECB Class 2 User Signature
- ECB Class 2 FIM CM Agent
- ECB Class 2 FIM CM Agent Admin Key Diversification
- ECB Class 2 FIM CM Enrolment Agent
- ECB Class 2 FIM CM KR Agent
- ECB Exchange Enrolment Agent (Offline Request)
- ECB CEP Encryption
- ECB NDES Encryption
- ECB NDES Signature
- ECB NDES Signature Encryption
- ECB Class 2 Code Signing

certificates are requested manually.

User (authentication, signature, and encryption) certificates on smartcards are requested via the IT request portal and issued via the ECB PKI certificate management portal after initial managerial approval. For new users the generation of a new USB-based smart card and corresponding certificates is part of the on-boarding and account creation process and relies on its overarching managerial approval.

Requests for ECB Class 2 User Client Authentication certificates serving VPN client authentication purpose are requested via an automated enrolment deployment. The process is controlled by the ECB identity management system processes and requires appropriate permissions in ECB Active Directory and on the respective certificate template.

Requests for

- ECB Class 2 Server Authentication
- ECB Class 2 Server Client Authentication
- ECB Class 2 Server Authentication CSR
- ECB Class 2 Server Client Authentication CSR
- ECB Class 2 Domain Controller Authentication CSR

certificates are requested manually via ITSP however using an automated workflow based on ECB IT Service Portal, ECB Automation system and ECB PKI infrastructure. The request contains details such as Application/Service Name as per ECB Service Catalogue, contact information, certificate Common Name and/or Subject Alternative Name(s).

The other end-entity certificates, as well as requests performed in case the automated workflow has failed, are requested via built-in operating system mechanisms or via the ECB PKI certificate management portal and the respective ECB PKI processes.

Machine/device requests for

- ECB Class 2 Client Authentication
- ECB Class 2 OCSP Response Signing
- ECB Class 2 Mobile Device Authentication

certificates are handled in an automatic enrolment scenario. The process is controlled by the existing ECB identity and access management processes and requires prior machine or device registration and appropriate permissions in the ECB Active Directory.

4.1.1 Who can submit a certificate application

ECB employees and approved partners of ECB can submit a certificate application. A valid ECB Active Directory user account and appropriate authorization according to the applicants' role is required.

For every system or device within ECB a named administrative contact is appointed and authorized to initiate the request for an appropriate certificate to be executed through the ECB IT Service Portal & Automation system or by the operations team responsible of the system or device..

For ECB standard devices and machines an automatic enrolment scenario is supported by the ECB PKI. For this process only an initial administrative contact to initiate the enrolment request is required. Certificates of this type are controlled by the ECB PKI operations staff in combination with automatic enrolment mechanisms; therefore no dedicated request is required for single certificates.

4.1.2 Enrolment process and responsibilities

Enrolment process

- User Authentication, Signature and Encryption certificates to subscribers are enrolled on a USB-based smartcard of the user according ECB PKI certificate enrolment processes and procedures in combination with the ECB Registration Authority Operator using the certificate management portal. If the user does not have a USB-based smartcard a new one is issued.
- User Client Authentication certificates are enrolled automatically via Active Directory Group Policies based on user object group membership
- Client Authentication certificates to machine subscribers are enrolled automatically via Active Directory Group Policies based on computer object group membership.
- Client Authentication certificates to mobile device subscribers are enrolled automatically via Microsoft Intune policies upon registration of respective user device.
- OCSP Responder certificates to machine subscribers are enrolled automatically via OCSP responder machine and OCSP responder array configuration.

Server Authentication, Server Client Authentication and Domain Controller Authentication certificates to machine subscribers are enrolled manually via ECB IT Service Portal according to ECB PKI certificate

enrolment processes and procedures in combination with the administrative contact that (1) generates a certificate signing request for ECB internal machine and device or (2) requests a certificate for an ECB internal machine or device including private key generation following the ECB PKI certificate request policies enforced by the ECB IT Service Portal and ECB certificate management portal.

Responsibilities

For user certificates on smartcards 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 USB-based smartcard and the user's account in the Active Directory.
- (for offline activities, such as initial on-boarding) to establish the mapping between the user's account in Active Directory and the USB-based smartcard, and later on ensure that the USB-based smartcard is delivered via the predetermined processes through which the user's identity is verified during hand-over.

ECB PKI operations staff is 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

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 USB-based smartcards for 2-factor authentication. In any case the core ECB PKI user certificate process is being followed, with the relevant user identity information stemming from the standard ECB identity 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.

4.2.1 Performing identification and authentication functions

Identification and authentication of users 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
- establishing the unique mapping between the user's identity, the USB-based smartcard and the Active Directory-based user account.

On a technical level identification and authentication is performed by the ECB Active Directory. All requesting entities require a valid Active Directory account for authentication and an appropriate

administrative contact Active Directory account is required for enrolment on behalf of non-Active-Directory-integrated devices.

4.2.2 Approval or rejection of certificate applications

With the management decision to introduce 2-factor authentication in general every user of ECB internal systems, i.e. ECB staff and contractors having an account in the ECB's Active Directory, is eligible for obtaining user certificates on USB-based smartcards as the second authentication factor, and therefore authorised.[6] The HR and physical security processes ensure that at the time a user is no longer eligible to have a certificate, the enrolment or re-keying will no longer be possible. Furthermore, existing certificates are revoked if a user is no longer eligible to have a certificate. Effectively this means that in case of a user not or no longer being eligible any potential certificate request is automatically rejected.

For every system within ECB a named administrative contact is appointed and authorized to perform the certification application requests.

For auto-enrolled machine/device certificates only initial administrative contact approval of the corresponding device or machine is required. Certificates of this type are controlled and approved by the ECB PKI operations staff, therefore no dedicated approval or rejection is required for single certificates.

For manually enrolled machine/device certificate types the administrative contact as the certificate requestor is responsible for successful enrolment and use after successful issuance of the respective certificate according to the existing ECB PKI certificate policies. The ECB PKI operations team is responsible for enrolment requests to match to existing certificate policies and that certificate enrolment for machines is conducted by authorized administrative contact only.

4.2.3 Time to process certificate applications

Certificate requests for existing certificate templates 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 (machine/device certificates).

Requests for new certificate types will be processed under the release management in place for Certificate Services.

4.3 Certificate Issuance

Certificates for individual users (on USB-based smartcards) are issued either as part of the user on-boarding process after hiring, or to replace a lost/forgotten/broken smartcard. Since the ECB decided to generally adopt 2-factor authentication based on USB-based smartcards any user holding an active

[6] This applies also the initial production and roll-out of USB-based smartcard to every existing eligible user.

account in Active Directory is eligible and authorized to obtain the device with corresponding certificates. The request is either

- executed by the registration authority operator on behalf of the user, before the user arrives at the first time at the ECB, where the operator initializes the USB-based smartcard, has the certificates issued and the random PIN generated, with the USB-based smartcard and the PIN letter handed over to the user separately on arrival; or
- triggered by a registration authority operator for users foreseen for guided enrolment after verification of the user's identity; the user is then sent all mean to get the certificates issued him/herself; or
- executed by the registration authority operator to replace a lost/stolen/forgotten/broken USB-based smartcard, with the user personally present, with the new certificates issued on the spot; or
- executed by the registration authority officer for initial rollout to existing users by initializing the USB-base smartcard, having the certificates issued and the random PIN generated, and preparing the separate envelopes for delivery to the user.

Certificates for individual users in a software-based form are issued automatically to users upon logon and after having applied the respective Active Directory Group Policies. Any user holding an active account in Active Directory is eligible and authorized to be added to the AD group granting the permission to receive such a certificate.

Machine and device certificates requested manually (online or offline) in an administrative contact based "enrol on behalf" scenario are issued by the certificate management portal web interface (see 4.1.2 Enrolment process and responsibilities for details). In all other cases, certificate issuance is performed automatically based on the configuration settings in the ECB LDAP directory.

A machine / device certificate which is requested manually (online or offline) is created and issued following the approval of a certificate application. ECB PKI creates and issues a certificate based on the information given in the approved certificate application in connection with ECB internal repositories to validate authorization and administrative responsibility for the desired system.

4.3.1 CA actions during certificate issuance

Before issuing certificates to ECB PKI subscribers, the following procedures are performed by the ECB PKI Issuing CAs, ECB PKI Certificate Management platform, ECB IT Service Portal (ITSP) or ECB PKI operations staff:

Check the certificate request for alignment to ECB PKI CP and CPS

- Check the requestor's permissions and role to request a certificate for the desired end-entity certificate template
- For user certificate requests:
    - Verify that there is a valid account assigned to the user's identity;
    - A USB-based smartcard is present and not assigned to another user;

    - If an encryption certificate is among the requested certificates generate a new key pair, and transmit the certificate and the private key securely after issuance to the user's smartcard.
- For manual requests via ITSP, automatically submit a change in ECB ticketing system (ITSM) and set respective Service Coordinator approval
- For manual machine/device certificate requests check the requestor to match to the administrative contact role for the desired system
- Store subscriber's certificate request in the CA database
- Issue the subscriber certificate(s)
- Store subscriber's certificate(s) in the CA database
- If the requested certificate is a user's encryption certificate store the corresponding key for private key backup purposes in a secure way.

4.3.2 Notification to subscriber by the CA of issuance of certificate

For the initial enrolment the Enrolment Agent is notified at the end of the enrolment process of the successful issuance. The certificate subscriber is notified of the successful issuance at the moment of token handover. For the renewal of existing user certificates, the certificate subscriber is notified at the end of the enrolment process of the successful issuance. In case of machine-based certificate subscribers, the related administrative contact responsible for the service or application is notified with the receipt of requested certificates. Notification does not apply to automatically enrolled certificate subscribers.

4.4 Certificate Acceptance

In the standard case of user enrolment on behalf the certificate subscriber is handed out the USB-based smartcard containing the certificates (in case of production of a new token) or handed back his/her existing token (in case of certificate modification with re-key). When receiving a new USB-based smartcard the user is also handed out the terms & conditions. The use of the certificates establishes the corroboration of the acceptance of the certificates as well as the terms and conditions. In any case the user has accepted the general rules for user conduct in place at the ECB as part of the work contract.

For guided user enrolment the user directly reviews the created certificates and sets the activation data for the USB-based token for future use, thereby accepting the certificates. (see also section 4.5.1)

Explicit acceptance does not apply to subscribers with automatically enrolled certificates.

4.4.1 Conduct constituting certificate acceptance

User certificates on USB-based smartcards

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 USB-based smartcard.

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

Manual enrolled machine certificates via ITSP

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 requesting machine a certificate acceptance is constituted.

4.4.2 Publication of the certificate by the CA

The certificates of ECB PKI certification authorities are published in the ECB LDAP directory and on the ECB PKI website:

- ECB Class 2 Root CA certificates (current and renewed CA certificate)
- ECB Class 2 Sub CA 01 certificates (current and renewed CA certificate)
- ECB Class 2 Sub CA 02 certificates (current and renewed CA certificate)

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

Notification of other entities is not supported.

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 website. They state in particular that the user is responsible for

- the secure 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 […] Service Desk of any detected or suspected information security incidents, problems or shortcomings.

In case of a discovered or suspected private key compromise or violation of any other requirements mentioned above and relevant 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.

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 with "1.4. Certificate Usage".

Certificates may only be relied upon if the following verification steps are successful

- Identifying a certificate chain up to the trusted ECB Class 2 Root CA 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 in each certificate in the certificate chain
    - 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 responder 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 and 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

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

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

Not applicable.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

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.

For user certificates 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.

In case of machine / device certificates the change management process established in the ECB needs to be completed, i.e. the new certificate must be installed in the (production) system before the revocation can actually be done. This process is required to take at most one month.

4.8.1 Circumstance for Certificate Modification

CA and end-entity certificate modification with re-key takes place when the certificate lifetime is in the defined renewal period or operational and / or security measures require certificate modification with re-key due to possible security countermeasures.

CA certificate modification with re-key scheme

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

Furthermore, certificate modification with re-key can or must take place under the following circumstances:

- When a subscriber's certificate is about to expire

- After a subscriber's certificate is lost by accident and any recovery procedure if applicable is not successful, or
- After a subscriber's certificate is deleted

4.8.2 Who may request certificate modification

- For user certificates on individual USB-based smartcards, the ECB subscriber must request a certificate modification with re-key still within the validity period of the existing certificate[7]. This essentially is very similar to a new enrolment process initiated by the RA Operator based on confirmation of the validity of the user account. The identity management systems at the ECB are aligned with the HR systems and guarantee the accuracy and up-to-dateness of the subscriber's data and working status at the ECB. In any case it is this data that is supplied to the PKI systems by the identity management system which is being placed in certificates.
- Auto-enrolment certificates are automatically requested by the subscriber user or machine for certificate modification with re-key.
- For manually enrolled machine certificates, the responsible ECB administrative contact must request a new certificate in the validity period of the existing certificate followed by the revocation of the existing certificate.

4.8.3 Processing certificate modification requests

For the processing of requests for certificate modification with re-keying see section 4.1 Certificate Application.

The process for certificate modification with re-keying for auto-enrolled user or computer certificates will take place automatically, therefore there is no specific process needed.

The process for initial manually enrolled end-entity certificates is the same as the initial enrolment process.

4.8.4 Notification of new certificate issuance to subscriber

See section 4.3 Certificate Issuance.

4.8.5 Conduct constituting acceptance of modified certificate

See section 4.4.1 Conduct constituting certificate acceptance.

4.8.6 Publication of the modified certificate by the CA

See section 4.4.2 Publication of the certificate by the CA

4.8.7 Notification of certificate issuance by the CA to other entities

Notification of other entities is not supported.

[7] Since this is the only operation of changing a certificate supported by the ECB-PKI, the slightly incorrect term "certificate renewal" is applied when outside the strict PKI context, as opposed to the strictly used terms in this document and the accompanying CPS.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

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
- violation by the subscriber of any of its material and essential obligations under the ECB PKI CP and CPS or the subscriber agreement
- 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
- 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
- Devices and/ or Machines are reinstalled and the respective end-entity certificate is still in its validity period
- The certificate has undergone modification with re-key, and thus the old one shall no longer be valid.

4.9.2 Who can request revocation

The following persons or roles can request a revocation for certificates

- ECB PKI certificate subscribers, especially users
- Administrative contact or security officer for the certificate
- Line Manager for certificates in the sphere of his or her responsibility
- Authorized service administrators
- Any authorized member of European Central Bank's Information Security Team

4.9.3 Procedure for revocation request

A revocation request 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
- ECB IT change request tools
- ECB IT Service Portal
- ECB PKI system

If the identity of the requestor cannot be fully established[8], a certificate shall only be suspended, so that erroneous requests can be corrected. With subsequent proper subscriber authentication a suspended certificate can be revoked permanently. The (possible) authorisation of the requestor shall be checked against the list provided in section 4.9.2.

In all such 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

There is no revocation request grace period. All revocation requests are considered effective with the request reaching the 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 Service Desk 24/7 support and upon request they can trigger the certificate suspension/revocation which triggers immediately the publishing of a new CRL.

4.9.6 Revocation checking requirement for relying parties

ECB PKI relying parties must have revocation checking and full chain validation capabilities wherever possible and technically applicable.

4.9.7 CRL issuance frequency

ECB PKI base CRL issuance frequency

Certificate Authority	Publication	Overlap	Lifetime
ECB Class 2 Root CA	6 Months	2 Months	8 Months
ECB Class 2 Sub CA 01	5 Days	3 Days	8 Days
ECB Class 2 Sub CA 02	5 Days	3 Days	8 Days

Delta CRLs are not directly exposed / referenced to the certificate subscriber but are used as a technical vehicle to enhance OCSP responder accuracy relying on CRL / delta CRL revocation information. There the following information is considered for documentation purposes only.

ECB PKI delta CRL issuance frequency

Certificate Authority	Publication	Overlap	Lifetime
ECB Class 2 Sub CA 01	24 Hours	12 Hours	36 Hours
ECB Class 2 Sub CA 02	24 Hours	12 Hours	36 Hours

[8] Some request channels allow for requestor authentication, such as using the ECB IT service management tool, or when visiting the ECB IT service desk office in person while presenting a badge. In other cases, such as calling the service desk, the requestor identity cannot be easily established.

Subscribers' smartcards are managed using ECB PKI management interface. When a smartcard is disabled the certificate package is revoked and new CRL and delta CRL published. The same concept is implemented for device certificates.

4.9.8 Maximum latency for CRLs

The latency depends on the location where a CRL is published:

- ECB PKI CRLs published on ECB PKI validation services web location
- CRLs are immediately available after CRL update and publication to the internal and external web site locations.
- ECB PKI CRLs published in ECB LDAP directory
- CRL availability depends on the maximum LDAP directory replication latency and site topology with a maximum delay of 60 minutes under normal operational conditions

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 Class 2 issuing CAs using OCSP response signing certificates issued by each Sub CA.

The ECB PKI OCSP responders rely on up-to-date CRL and / or delta 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 and / or delta CRL retrieval interval expected not to exceed 60 minutes under normal operational conditions.

4.9.10 On-line revocation checking requirements

For a user certificate it is the responsibility of the relying party to check the current status of validity of a certificate prior to relying on it, see section 4.5.2 Relying party public key and certificate usage.

Machines running Windows 10, Windows 11, Windows Server 2008 or higher as well as other devices with OCSP client capabilities are able to check certificate revocation status via OCSP. Devices or software without OCSP capability check certificate status by CRLs and ignore any available OCSP extension.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements re key compromise

Not applicable.

4.9.13 Circumstances for suspension

Certificate suspension is supported in Class 2 PKI trust chains for individual smartcards on the user USB token / smartcard certificate package.

Circumstances for suspension requests are all applicable reasons that require temporarily revoking certificates.

4.9.14 Who can request suspension

See 4.9.2

4.9.15 Procedure for suspension request

The certificate will be flagged as “revoked”. The revocation reason code for this certificate will be set to “Certificate Hold”. This will disable all associated functions related to the certificate while enabling future final revocation or un-revocation during the certificate’s validity period if required.

See 4.9.3

4.9.16 Limits on suspension period

PKI responsible team looks periodically – at least every 30 days to the list of suspended certificates and follows up with Service Desk to ensure suspended certificates are either permanently disabled or reinstated..

4.10 Certificate Status Services

Not applicable.

4.10.1 Operational characteristics

Not applicable

4.10.2 Service availability

Not applicable

4.10.3 Optional features

Not applicable

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 Class 2 Root CA certificate is expired or the respective Root CA service is terminated.
- CRL and OCSP of ECB Class 2 Sub CA 01 subscription ends, when the ECB Class 2 Sub CA 01 certificate is expired or the ECB Class 2 Sub CA 01 service is terminated.
- CRL and OCSP of the ECB Class 2 Sub CA 02 subscription ends, when the ECB Class 2 Sub CA 02 certificate is expired or the ECB Class 2 Sub CA 02 service is terminated.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

Key recovery for the encryption certificate is supported in Class 2 PKI trust chains for individual smartcards on the user smartcards certificate package. No key recovery or escrow is supported for USB-based smartcards user authentication or user signature certificates.

Circumstances for key recovery requests are subject to evaluation on a case-by-case basis.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable and not implemented in the current level of implementation.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

The central CA components must be protected against unauthorized physical access and other physical and environmental impact. Physical access is to be restricted to those personnel of the ECB PKI operations staff.

5.1.1 Site location and construction

The central components of the ECB PKI shall be located in the ECB secure data centres conforming to the general ECB standards for physical and environmental security, in particular protecting the components from unauthorised physical access and other physical or environmental impact.

5.1.2 Physical access

ECB PKI critical components shall be hosted in a location providing a security perimeter, protecting against intrusions and allowing physical access only to authorised personnel.

5.1.3 Power and air conditioning

The hosting location for the ECB PKI infrastructure systems shall provide sufficient electrical power and cooling, and protect against power outages.

5.1.4 Water exposures

Appropriate measures shall be in place to prevent exposure of ECB PKI infrastructure equipment to water.

5.1.5 Fire prevention and protection

ECB PKI components shall be hosted in locations with fire detection and extinguishing systems.

5.1.6 Media storage

Any media used to store data related to ECB PKI systems, in particular backup media, shall be protected against unauthorised physical access, theft and removal as well as against deterioration and other physical damage.

5.1.7 Waste disposal

Critical material and removable media shall be securely disposed of, protecting the information contained in them against unauthorised access.

5.1.8 Off-site backup

ECB PKI infrastructure systems and the respective backups shall offer sufficient redundancy to protect against loss of systems or backups.

5.2 Procedural Controls

Operations on the CA and RA must be handled by authorized personnel assigned with the trusted roles only. Strong mechanisms for identification, authentication and authorization must be used where in particular sensitive operations are conducted.

5.2.1 Trusted roles

Trusted roles must be identified and defined with respect to the ECB PKI operations. Among them are registration officer, the PKI operations team (CA administrators), Information Security Officer, IT Operations Managers as well as Auditors. Trusted roles at the ECB can be found in the CPS section 5.2.1.

5.2.2 Number of persons required per task

CA cryptographic operations must be protected by HSMs. Furthermore, operations involving the private key of the ECB Class 2 Root CA must involve multi-person control.

5.2.3 Identification and authentication for each role

HSM transactions must involve two-factor authentication. Furthermore, any role assignment must involve managerial approval and in-person proof according to the ECB personnel processes.

5.2.4 Roles requiring separation of duties

For any HSM operation requiring multi-person control the necessary quorum to perform the operation must be divided between teams performing security advisory, operations support and engineering for the ECB PKI system.

The role of an RA Operator must be assigned to separate personnel than PKI operations. The roles of system administrators and security advisor are mutually exclusive.

The auditor and security testing roles must be assigned outside the ECB PKI operations team.

5.3 Personnel Controls

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. Furthermore, confidentiality agreements must be signed by the personnel entrusted with the operation of the ECB PKI. In addition they are also given detailed instructions on the processes.

5.3.2 Background check procedures

Background checks on ECB PKI personnel must be conducted in accordance with ECB personnel screening procedures prior to role assignment.

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

Re-training must be scheduled as deemed necessary for the personnel to maintain the skills required for the job profile and responsibilities.

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 appropriate disciplinary actions shall be sought in line with ECB human resources procedures.

5.3.7 Independent contractor requirements

The same requirements as set out in section 5.2 shall apply to ECB certified independent contractors and IT service partners as well.

5.3.8 Documentation supplied to personnel

The ECB PKI CP and CPS documents and accompanying documents, e.g. with details on specific procedures, shall be provided to ECB PKI operations staff employees for study and consultation. If necessary, further documents according to the respective job responsibilities shall be supplied.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

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
- Issue and manage certificate requests
- Revoke certificates and publish CRLs
- Store and retrieve archived keys

are audited on the ECB CAs.

5.4.2 Frequency of processing log

Event logs shall be reviewed regularly, and additionally in case of irregularities or unusual activities.

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 Class 2 Root CA (offline components) shall keep recorded events for at least 6 months.

5.4.4 Protection of audit log

Audit logs must be kept in such a way that their confidentiality and integrity are maintained at all times. Preferably a combination of physical and logical access controls should be used.

5.4.5 Audit log backup procedures

Standard server backup procedures for audit logs shall apply. For offline components regular manual audit log backup procedures shall be in place.

5.4.6 Audit collection system (internal vs. external)

The ECB PKI shall store audit logs at least internally to each component. Furthermore, the audit logs should be transferred to a central audit log collection system for archival and central evaluation.

5.4.7 Notification to event-causing subject

Not applicable.

5.4.8 Vulnerability assessments

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

5.5 Records Archival

5.5.1 Types of records archived

At least all certificate application information must be archived.

5.5.2 Retention period for archive

The retention period of the archive must be at least according to the standard ECB PKI and ECB change management archival retention period.

5.5.3 Protection of archive

The archive must be kept in such a way that their confidentiality and integrity are maintained at all times. Preferably a combination of physical and logical access controls should be used.

5.5.4 Archive backup procedures

Not applicable.

5.5.5 Requirements for time-stamping of records

All archived information shall contain information about time and date based on synchronized clocks. No RFC 3161 compliant cryptographic time stamping service is 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

ECB PKI CA key pairs have to be modified and re-keyed before their expiration to guarantee the continuity of offered services. New CA key pairs have to be generated either to replace an expiring key pair or to offer new services.

According to ECB PKI CA re-Keying schedule, the following maximum CA certificate validity periods have been determined:

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

See section 5.6 on ECB Class 2 PKI CPS for further details.

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

See section 5.7.1 on ECB Class 2 PKI CPS for details.

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

See section 5.7.2 on ECB Class 2 PKI CPS for details.

5.7.3 Entity private key compromise procedures

See section 5.7.3 on ECB Class 2 PKI CPS for details.

5.7.4 Business continuity capabilities after a disaster

See section 5.7.4 on ECB Class 2 PKI CPS for details.

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.

See section 5.8 on ECB Class 2 PKI CPS for details.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

Key pair generation and installation is to be 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 Class 2 trust chain must be generated in hardware security modules with the FIPS 140-2 Level 3 certification.

User key pairs for authentication and signature must be generated on smartcards certified according to FIPS 140-2 level 3. User certificates for encryption of data may be generated in secure environments and installed on USB tokens / smartcards certified according to ITSEC E3 high or FIPS 140-2 level 3. A copy of the key pair may be retained in the security base of the issuing CA (private key backup).

Machine, Code Signing and user VPN client authentication key pairs must be generated at least in a software cryptographic module certified according to FIPS 140-2 level 1 and may be generated at time of registration.

See section 6.1.1 on ECB Class 2 PKI CPS.

6.1.2 Private Key delivery to subscriber

CA private keys must be generated locally and never leave the secure HSM environment in unprotected form.

User private keys for authentication and signature must not leave the secure environment they are generated in.

User private keys for data encryption must be delivered, if generated outside the smartcard, in securely encrypted form “end-to-end” after mutual authentication of the related parties and the PKI components.

In any case, local generation should be preferred, and delivery of private keys avoided.

See section 6.1.2 on ECB Class 2 PKI CPS.

6.1.3 Public key delivery to certificate issuer

Established message standards should be followed.

See section 6.1.3 on ECB Class 2 PKI CPS.

6.1.4 CA public key delivery to relying parties

See section 6.1.4 on ECB Class 2 PKI CPS.

6.1.5 Key Sizes

CA keys must be at least 4096 bits in length, subscriber keys must be at least 2048 bits in length.

See section 6.1.5 on ECB Class 2 PKI CPS.

6.1.6 Public key parameters generation and quality checking

The ECB PKI supports only RSA as public key algorithm and SHA-256 for Class 2 trust chain as cryptographic hash algorithms.

See section 6.1.6 on ECB Class 2 PKI CPS.

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

The key usage fields must be set according to the intended use of the keys.

See section 6.1.7 on ECB Class 2 PKI CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

See section 6.2 on ECB Class 2 PKI CPS.

6.2.1 Cryptographic module standards and controls

The key pairs, in particular the private key, of the following PKI components must be protected by a hardware security module (HSM) complying at least to FIPS 140-2 level 3:

- ECB Class 2 Root CA
- All direct Sub CAs of the ECB Class 2 Root CA
- All OCSP response signing keys of direct Sub CAs of the ECB Class 2 Root CA

User key pairs for authentication or signature must be protected by a USB token / smartcard complying with FIPS 140-2 level 3. User key pairs for encryption are stored in encrypted form in ECB PKI database, encrypted under an HSM-protected Key Recovery Agent certificate/key. Other subscriber key pairs of the ECB Class 2 Sub CA must be protected at least by a software cryptographic module.

See section 6.2.1 on ECB Class 2 PKI CPS.

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

Cryptographic operations involving the private key of the ECB Class 2 Root CA must be implemented using multi-person controls for authorization.

Multi-person control is not applicable to ECB Class 2 PKI subscriber private keys.

See section 6.2.2 on ECB Class 2 PKI CPS.

6.2.3 Private Key escrow

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

6.2.4 Private Key backup

The private keys of the ECB Class 2 Root CA and its Sub CAs must be backed up such that the private key is protected by cryptographic controls and multi-person authorization.

Private key backup for subscriber certificates must be supported for user certificates used for data encryption. Private key backup for user certificates for authentication or signature is prohibited.

See section 6.2.4 on ECB Class 2 PKI CPS.

6.2.5 Private Key archival

Private key archival for subscriber certificates must be supported for user certificates used for data encryption. Private key archival for user certificates for authentication or signature is prohibited.

See section 6.2.5 on ECB Class 2 PKI CPS.

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

See section 6.2.1 of this CP.

See section 6.2.7 on ECB Class 2 PKI CPS.

6.2.8 Method of activating private key

ECB Class 2 Root CA private keys must only be activated after multi-person authentication and authorization against the HSM holding the key.

ECB Class 2 Sub CA signing keys must be activated via multi-person authentication before first use in the ECB PKI. This may be conducted implicitly and in conjunction with the certificate creation for the ECB Class 2 Sub CA signing key by the ECB Class 2 Root CA. The OCSP response signing keys may be implicit activated by the HSM at first use after certificate generation.

Private keys of user certificates protected by a smartcard must be protected against unauthorized activation by a PIN.

See section 6.2.1 on ECB Class 2 PKI CPS.

6.2.9 Method of deactivating private keys

The private keys of the ECB Class 2 Root CA must be deactivated immediately upon removal of the last HSM multi-person control token or upon session termination.

Subscriber private keys protected by a USB token / smartcard must be deactivated when withdrawn from the USB port / smartcard reader or removal of the power supply.

See section 6.2.9 on ECB Class 2 PKI CPS.

6.2.10 Method of destroying private keys

CA keys must be destroyed securely by the relevant HSM after successful multi-person authorization.

Subscriber private keys must be destroyed according to the ECB data destruction policies.

See section 6.2.10 on ECB Class 2 PKI CPS.

6.2.11 Cryptographic Module Rating

See section 6.2.1 of this CP.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

All public keys of CAs and subscribers must be backed up.

6.3.2 Certificate operational periods and key pair usage periods

For the ECB PKI certificate validation requires that all certificates in the chain up to the root CA are valid at time of verification. As certificate renewal is performed only by modification with re-keying, the certificate operational period matches the key pair usage period.

Exceptions may be made for certificates used for data encryption, where the private key may be used for decryption after the period of validity expired.

6.4 Activation Data

6.4.1 Activation data generation and installation

Explicit activation data for CA private keys must be generated using the HSM devices such that a quorum is required for activation. Furthermore, the activation tokens for enforcing multi-person authorization must be PIN-protected.

Activation data for private keys held in user smartcards is set originally during the enrolment process during which a random PIN is set at the time of generating a cryptographic key on user's USB token / smartcard. When receiving the USB-based smartcard the user is instructed to change the PIN before first use. The USB based smartcard and the PIN are handed over to the user via separate channels if the user is not present during the procedure conducted by the operator. In case of guided enrolment the subscriber does set the PIN him/herself.

Activation data for machine subscribers should be generated automatically during machine setup. It must be protected against unauthorized disclosure and misuse on the local system.

6.4.2 Activation data protection

ECB PKI subscribers are required to assert that the activation data they originally received is updated and is then kept secret and is never disclosed to a third party.

Activation data for CA private keys must be protected such that the multi-person authorization requirement cannot be circumvented.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer Security Controls

Hardening procedures and security patching procedures according to the ECB internal IT security policies must be applied for all ECB PKI CA machines and relevant components.

6.5.1 Specific computer security technical requirements

Hardening procedures and security patching procedures according to the ECB internal IT security policies must be applied for all ECB PKI CA machines and relevant components.

In particular, access control must be present with authorization based on need-to-access, and anti-malware must be installed as well as its operation monitored.

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

Quality assurance processes must be employed during the system deployment.

6.6.2 Security management controls

Monitoring and auditing must be employed to ensure compliance of all ECB PKI components with the relevant policies.

6.6.3 Life cycle security controls

Quality assurance processes must be employed during the system deployment.

6.7 Network Security Controls

Network security controls must be employed in accordance with the relevant ECB network security policies.

6.8 Time-stamping

All ECB PKI CAs must make use of synchronized clocks. However, a trusted and evaluated RFC 3161 compliant time stamping component is not supported by the ECB PKI.

7 Certificate, CRL, and OCSP Profiles

Details are given in the Certification Practice Statement (CPS) of the ECB Class 2 PKI.

7.1 Certificate Profile

See section 7.1 on ECB Class 2 PKI CPS.

7.1.1 Version number(s)

See section 7.1.1 on ECB Class 2 PKI CPS.

7.1.2 Certificate extensions

See section 7.1.2 on ECB Class 2 PKI CPS.

7.1.3 Algorithm object identifiers

See section 7.1.3 on ECB Class 2 PKI CPS.

7.1.4 Name forms

See section 7.1.4 on ECB Class 2 PKI CPS.

7.1.5 Name constraints

See section 7.1.5 on ECB Class 2 PKI CPS.

7.1.6 Certificate policy object identifier

See section 7.1.6 on ECB Class 2 PKI CPS.

7.1.7 Usage of Policy Constraints extension

See section 7.1.7 on ECB Class 2 PKI CPS.

7.1.8 Policy qualifiers syntax and semantics

See section 7.1.8 on ECB Class 2 PKI CPS.

7.1.9 Processing semantics for the critical Certificate Policies extension

See section 7.1.9 on ECB Class 2 PKI CPS.

7.2 CRL Profile

See section 7.2 on ECB Class 2 PKI CPS

7.2.1 Version Number(s)

See section 7.1.1 on ECB Class 2 PKI CPS.

7.2.2 CRL and CRL Entry Extensions

See section 7.2.2 on ECB Class 2 PKI CPS.

7.3 OCSP Profile

See section 7.3 of the ECB Class 2 PKI CPS.

7.3.1 Version number(s)

See section 7.3.1 on ECB Class 2 PKI CPS.

7.3.2 OCSP extensions

See section 7.3.2 on ECB Class 2 PKI CPS

8 Compliance Audit and Other Assessments

Details are described in the Certification Practice Statement (CPS) of the ECB PKI system

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.

See section 8.1 on ECB Class 2 PKI CPS.

8.2 Identity/qualifications of assessor

The auditors need to have the necessary qualifications to conduct an audit regarding compliance and / or security.

See section 8.2 on ECB Class 2 PKI CPS.

8.3 Assessor's relationship to assessed entity

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

See section 8.3 on ECB Class 2 PKI CPS.

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.

See section 8.4 on ECB Class 2 PKI CPS.

8.5 Actions taken as a result of deficiency

If an audit detects deficiencies, an action plan for remediation is initiated to address the deficiencies.

See section 8.5 on ECB Class 2 PKI CPS.

8.6 Communication of results

Audit results are generally kept confidential.

9 Other Business and Legal Matters

The following section applies to business, legal and data privacy matters of ECB PKI certification services. The current PKI and related infrastructure are designed for internal and approved ECB business partner use only. Therefore, the 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.

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

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

9.3.3 Responsibility to protect confidential information

See section 9.3.3 on ECB Class 2 PKI CPS.

9.4 Privacy of Personal Information

Subscribers and all relying parties should treat any ECB PKI related personal information as to being covered by applicable ECB general Information Security and Confidentiality Policies unless otherwise stated. This does not apply to publicly 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

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.

9.6 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 CP shall come into force from the moment it is published in the ECB PKI repository.

This CP 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 CP is substituted, it shall be substituted by 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 CP 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 CP, 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 CP 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 CP and the referenced CPS 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 CP or the referenced CPS 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 respective certificates.

9.12.3 Circumstances under which OID must be changed

In case of amendment, when numbering the new version of this 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 Union apply to the ECB PKI.

The ECB processes personal data in accordance 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

All users and relying parties of ECB PKI accept the content of the latest version of this CP 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.

Annex A. Terms and conditions for user certificate package (authentication, encryption and signature)

The binding obligations for handling of ECB IT equipment, user IDs, PINs, as well as on acceptable system use and notification in case of security incidents are laid out in the business rulebook.

Furthermore, together with the USB-based smartcard and the separate PIN letter the user is handed over the following reminder of the contractual obligations:

You, the user shall:

- Use the certificates only for the purpose they have been issued to you by the ECB;
- Take the necessary security measures within your control in order to avoid any loss, modification or unauthorized use of the cryptographic card, as well as keep any third party from obtaining knowledge of the PIN and PUK secret number for activation and unlocking of the cryptographic card;
- Request the revocation of the certificate in case the data specified in the certificate changes, or when you have knowledge or reasonable suspicion that the private key might be under risk due to, among other causes, loss, theft or third parties having acquired knowledge of the PIN and/or PUK;
- Inform the ECB via the Service Desk without undue delay of any kind of technical or procedural vulnerability of the cryptographic card, the technical or organizational implementation of the ECB-PKI;
- Not transfer or delegate to third parties the obligations pertaining to the certificate assigned to you (e.g. not transfer the cryptographic card or its corresponding PIN and/or PUK).
- Ensure that your certificates contain accurate and complete information about you as a person, and notify the ECB of changes of such information.

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	3.1
Status	Published release related to recertification for CAF compliancy
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
3.1	10.01.2024	Revised version for regular CAF compliancy review

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 v3.1.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	V3.1
Last changed	10.01.2024

Document title	ECB PKI Certificate Profiles
Document Name	ECB PKI Certificate Profiles RFC 5280 v4.0.xlsx
Description	RFC5280 Certificate Profiles for ECB CLASS 2 PKI
Latest available version	V3.0
Last changed	14.06.2023

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.

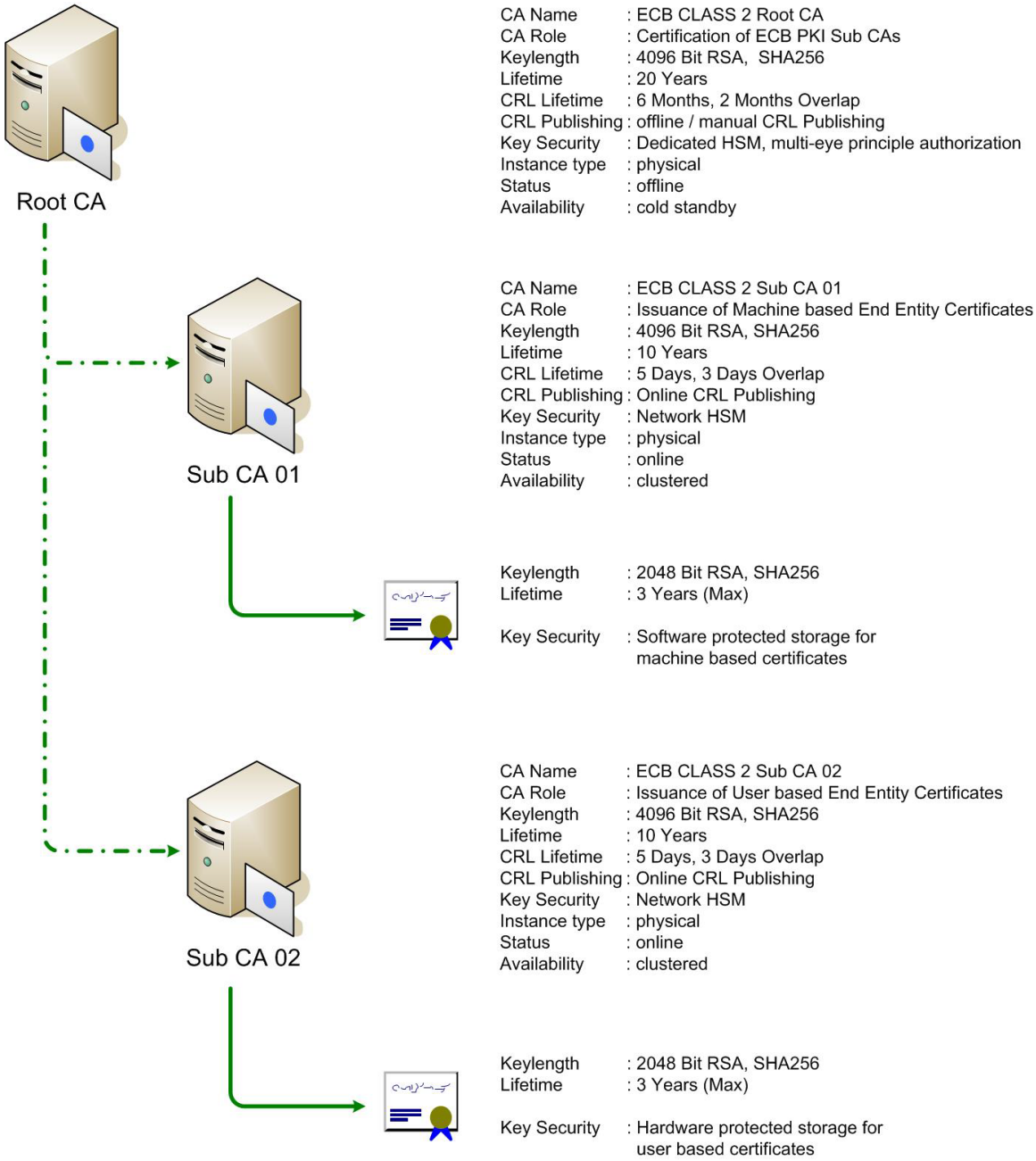
The other components in the PKI are built from multi-tenant capable centralized components like certificate validation services including OCSP responders and the certificate management solution. The same principle applies to the centralized LDAP directory infrastructure.

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:



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 N.B.: The ECB Class 2 PKI issuance policy is a unified document, comprised of both the ECB Class 2 PKI Certificate Policy (OID 1.3.6.1.4.1.41697.509.2.100.20.1) and the ECB Class 2 PKI Certificate Practice Statement (OID 1.3.6.1.4.1.41697.509.2.100.20.2), identified by an OID within this namespace.

X.509 OID – Issuance Policy identifiers

1.3.6.1.4.1.41697.509.2.100.10.**1**	ECB Class 2 PKI issuance policy (the actual issuance policy document, comprised of both the ECB Class 2 PKI Certificate Policy (OID 1.3.6.1.4.1.41697.509.2.100.20.1) and the ECB Class 2 PKI Certificate Practice Statement (OID 1.3.6.1.4.1.41697.509.2.100.20.2).

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 v3.1

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 v3.1

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 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 HSMs, 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.

Further details are be available on request.

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 with UPS-protected power supply and air-conditioning, protecting them from power failures.

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 being backed up using standard the ECB backup system. The backup, storage and recovery of the CA private signing keys are performed by personnel in trusted roles only (ACS card owners among which there are persons from Certificate Services, System Administration, Security Services) and in a physically secured environment (ECB datacentres), 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 and the respective backups are located in two ECB datacentres which are physically separated, thus providing sufficient redundancy in case of a data centre loss.

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. 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 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.

If computing resources, software and/or data are corrupted, ECB PKI operations will be stopped until the security of the environment has been re-established. In case issued certificates are affected, respective users will be notified, their certificates revoked and new ones issued.

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 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..

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.

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

- New systems with hardware and software like the one 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

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, 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

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 follows the requirements of FIPS 140-2 Level 3.

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 3.

For user key pairs/certificates the key generation is as follows:

- The Subscribers' cryptographic keys that are used for strong user authentication (e.g. during logon to ECB computers) are generated on USB-based smartcards with FIPS 140-2 level 3 certification.
- The Subscribers' cryptographic keys that are used to create an electronic signature are generated on USB-based smartcards with FIPS 140-2 level 3 certification.
- 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 certification with a copy on the security base of the issuing CA.
- The subscribers' cryptographic keys that are used for VPN client authentication are generated on user's computer, with private key marked as not exportable. User authentication certificates for VPN are very similar to a user-specific machine certificate and at the same time clearly distinguishable from the user advanced certificates that we submit to the CAF approval process.
- The cryptographic keys for users that are used for Code Signing are generated on user's computer.

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 Mobile Client Authentication	Digital Signature, Key Encipherment
ECB Class 2 Hybrid Client Authentication	Digital Signature, Key Encipherment
ECB Class 2 OCSP Response Signing	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 Code Signing	Digital Signature
ECB Class 2 User 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 3.
- ECB Class 2 PKI Sub CA 01 key pair is generated by a hardware security module (HSM) that complies with FIPS 140-2 Level 3.
- ECB Class 2 PKI Sub CA 02 key pair is generated by a hardware security module (HSM) that complies with FIPS 140-2 Level 3.
- 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 3.
- 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.
- ECB PKI ECB Class 2 Sub CA 02 subscriber user key pairs for VPN authentication are generated on the ECB laptops and installed into the personal user profiles

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).
- The ECB PKI ECB Class 2 Sub CA 02 subscriber (user) key pairs for user authentication, encryption and signature are protected on smartcards with FIPS 140-2 level 3 certification.

- The ECB PKI Class 2 Sub CA 02 subscriber (user) key pairs for VPN client authentication are protected by software cryptographic module certified according to FIPS 140-2 level 1.
- The ECB PKI Class 2 Sub CA 02 subscriber (user) key pairs for Code Signing are protected by software cryptographic module certified according to FIPS 140-2 level 1.

6.2.8 Method of activating private key

- 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 signing keys are activated before first use via the procedure to create and install the corresponding certificate (issued by the ECB Class 2 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 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 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.

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.
- 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 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.

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.

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 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 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 Mobile Client Authentication	1 year	6 weeks
ECB Class 2 Hybrid Client Authentication	1 year	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 Code Signing	2 years	6 weeks
ECB Class 2 User 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 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 Code Signing 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 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.

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 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 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
ECB Class 2 Hybrid Client Authentication	5
ECB Class 2 Code Signing	5
ECB Class 2 User 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

Attribute	Value
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 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

ECB Class 2 Sub CA 01	
X.509 Version	V3

ECB Class 2 Sub CA 01	
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 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

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).
Basic Constraints (critical)	Subject Type=CA,

ECB Class 2 Sub CA 02	
	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

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
Authority Information Access	HTTP URL reference to AIA Location HTTP URL reference to OCSP Location
Subject Alternative Name	present, depending on detailed certificate profile

ECB Class 2 End-Entity Certificate	
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, 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
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

Extension	Possible Values	Critical Flag
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]

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

In the past the Common Name of ECB user accounts was created having a firstname.lastname structure, and in case of users with identical firstname and lastname, a number i.e. 1 would be 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.

Currently, the Common Name of ECB user accounts is created having a firstname.lastname.userlogonname structure, userlogonname being corelated to User ID and stored

in the ECB Identity and Access Management system, thus ensuring creation of unique user logon even after account deletion or renaming

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 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	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

ECB Class 2 OCSP Response Signing	
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
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

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

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

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

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.

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

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.