EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB PKI

Certificate Policy (CP) Advanced Encryption
OID: 1.3.6.1.4.1.41697.509.10.100.2.1.3

Table of Contents

Table of Contents 2

Document control 11

Basic Description 11

Version History 11

Document Review and Signoff 11

Related Documents 11

1 Introduction 13

1.1 Overview 14

1.1.1 Implementation of the ECB PKI certificate authority hierarchy 14

1.2 Document Name and Identification 16

1.3 PKI Participants 18

1.3.1 Certification Authorities 18

1.3.2 Registration Authorities 19

1.3.3 Subscribers 19

1.3.4 Relying parties 19

1.3.5 Other participants 19

1.4 Certificate Usage 20

1.4.1 Appropriate certificate uses 20

1.4.2 Prohibited certificate uses 20

1.5 Policy Administration 21

1.5.1 Organization administering the document 21

1.5.2 Contact person 21

1.5.3 Person determining CPS suitability for the policy 21

1.5.4 CP approval procedures 21

1.6 Definitions and Acronyms 21

2 Publication and Repository Responsibilities 25

2.1 Repositories 25

2.2 Publication of Certification Information 25

2.3 Time or Frequency of Publication 25

2.4 Access Controls on Repositories 25

3 Identification and Authentication 25

3.1 Naming 25
3.1.1 Types of names 25
3.1.2 Need for names to be meaningful 26
3.1.3 Anonymity or pseudonymity of subscribers 27
3.1.4 Rules for interpreting various name forms 27
3.1.5 Uniqueness of names 27
3.1.6 Recognition, authentication, and role of trademarks 27
3.2 Initial Identity Validation 27
3.2.1 Method to prove possession of private key 27
3.2.2 Authentication of organization identity 27
3.2.3 Authentication of individual identity 27
3.2.4 Non-verified subscriber information 28
3.2.5 Validation of authority 28
3.2.6 Criteria for interoperation 29
3.3 Identification and Authentication for Re-key Requests 29
3.3.1 Identification and authentication for routine re-key 29
3.3.2 Identification and authentication for re-key after revocation 29
3.4 Identification and Authentication for Revocation Requests 29
4 Certificate Life-Cycle Operational Requirements 30
4.1 Certificate Application 30
4.1.1 Who can submit a certificate application 30
4.1.2 Enrolment process and responsibilities 30
4.2 Certificate application processing 31
4.2.1 Performing identification and authentication functions 31
4.2.2 Approval or rejection of certificate applications 31
4.2.3 Time to process certificate applications 31
4.3 Certificate Issuance 31
4.3.1 CA actions during certificate issuance 32
4.3.2 Notification to subscriber by the CA of issuance of certificate 32
4.4 Certificate Acceptance 32
4.4.1 Conduct constituting certificate acceptance 32

4.4.2 Publication of the certificate by the CA 33
4.4.3 Notification of certificate issuance by the CA to other entities 33
4.5 Key Pair and Certificate Usage 33
4.5.1 Subscriber private key and certificate usage 33
4.5.2 Relying party public key and certificate usage 33
4.6 Certificate Renewal 33
4.6.1 Circumstance for certificate renewal 33
4.6.2 Who may request renewal 33
4.6.3 Processing certificate renewal requests 33
4.6.4 Notification of new certificate issuance to subscriber 33
4.6.5 Conduct constituting acceptance of a renewal certificate 34
4.6.6 Publication of the renewal certificate by the CA 34
4.6.7 Notification of certificate issuance by the CA to other entities 34
4.7 Certificate Re-key 34
4.7.1 Circumstance for certificate re-key 34
4.7.2 Who may request certification of a new public key 34
4.7.3 Processing certificate re-keying requests 34
4.7.4 Notification of new certificate issuance to subscriber 34
4.7.5 Conduct constituting acceptance of a re-keyed certificate 34
4.7.6 Publication of the re-keyed certificate by the CA 34
4.7.7 Notification of certificate issuance by the CA to other entities 34
4.8 Certificate Modification 35
4.8.1 Circumstance for Certificate Modification 35
4.8.2 Who may request certificate modification 35
4.8.3 Processing certificate modification requests 36
4.8.4 Notification of new certificate issuance to subscriber 36
4.8.5 Conduct constituting acceptance of modified certificate 36
4.8.6 Publication of the modified certificate by the CA 36
4.8.7 Notification of certificate issuance by the CA to other entities 36
4.9 Certificate Revocation and Suspension 36
4.9.1 Circumstances for revocation 36

4.9.2 Who can request revocation 36
4.9.3 Procedure for revocation request 36
4.9.4 Revocation request grace period 37
4.9.5 Time within which CA must process the revocation request 37
4.9.6 Revocation checking requirement for relying parties 37
4.9.7 CRL issuance frequency 37
4.9.8 Maximum latency for CRLs 37
4.9.9 On-line revocation/status checking availability 37
4.9.10 On-line revocation checking requirements 37
4.9.11 Other forms of revocation advertisements available 37
4.9.12 Special requirements re key compromise 37
4.9.13 Circumstances for suspension 37
4.9.14 Who can request suspension 38
4.9.15 Procedure for suspension request 38
4.9.16 Limits on suspension period 38
4.10 Certificate Status Services 38
4.10.1 Operational characteristics 38
4.10.2 Service availability 38
4.10.3 Optional features 38
4.11 End of Subscription 38
4.12 Key Escrow and Recovery 38
4.12.1 Key escrow and recovery policy and practices 38
4.12.2 Session key encapsulation and recovery policy and practices 39
5 Facility, Management, and Operational Controls 40
5.1 Physical Controls 40
5.1.1 Site location and construction 40
5.1.2 Physical access 40
5.1.3 Power and air conditioning 40
5.1.4 Water exposures 40
5.1.5 Fire prevention and protection 40
5.1.6 Media storage 40

5.1.7 Waste disposal 40
5.1.8 Off-site backup 41
5.2 Procedural Controls 41
5.2.1 Trusted roles 41
5.2.2 Number of persons required per task 41
5.2.3 Identification and authentication for each role 41
5.2.4 Roles requiring separation of duties 41
5.3 Personnel Controls 41
5.3.1 Qualifications, experience, and clearance requirements 41
5.3.2 Background check procedures 42
5.3.3 Training requirements 42
5.3.4 Retraining frequency and requirements 42
5.3.5 Job rotation frequency and sequence 42
5.3.6 Sanctions for unauthorized actions 42
5.3.7 Independent contractor requirements 42
5.3.8 Documentation supplied to personnel 42
5.4 Audit Logging Procedures 42
5.4.1 Types of events recorded 42
5.4.2 Frequency of processing log 43
5.4.3 Retention period for audit log 43
5.4.4 Protection of audit log 43
5.4.5 Audit log backup procedures 43
5.4.6 Audit collection system (internal vs. external) 43
5.4.7 Notification to event-causing subject 43
5.4.8 Vulnerability assessments 43
5.5 Records Archival 43
5.5.1 Types of records archived 43
5.5.2 Retention period for archive 43
5.5.3 Protection of archive 43
5.5.4 Archive backup procedures 43
5.5.5 Requirements for time-stamping of records 43

5.5.6 Archive collection system (internal or external) 43
5.5.7 Procedures to obtain and verify archive information 44
5.6 Key Changeover 44
5.7 Compromise and Disaster Recovery 44
5.7.1 Incident and compromise handling procedures 44
5.7.2 Computing resources, software, and/or data are corrupted 44
5.7.3 Entity private key compromise procedures 44
5.7.4 Business continuity capabilities after a disaster 44
5.8 CA or RA Termination 44
6 Technical Security Controls 45
6.1 Key Pair Generation and Installation 45
6.1.1 Key pair generation 45
6.1.2 Private Key delivery to subscriber 45
6.1.3 Public key delivery to certificate issuer 45
6.1.4 CA public key delivery to relying parties 45
6.1.5 Key Sizes 45
6.1.6 Public key parameters generation and quality checking 46
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 46
6.2 Private Key Protection and Cryptographic Module Engineering Controls 46
6.2.1 Cryptographic module standards and controls 46
6.2.2 Private Key (n out of m) Multi-Person Control 46
6.2.3 Private Key escrow 46
6.2.4 Private Key backup 47
6.2.5 Private Key archival 47
6.2.6 Private Key transfer into or from a cryptographic module 47
6.2.7 Private Key storage using cryptographic module 47
6.2.8 Method of activating private key 47
6.2.9 Method of deactivating private keys 47
6.2.10 Method of destroying private keys 48
6.2.11 Cryptographic Module Rating 48
6.3 Other Aspects of Key Pair Management 48

6.3.1 Public key archival 48
6.3.2 Certificate operational periods and key pair usage periods 48
6.4 Activation Data 48
6.4.1 Activation data generation and installation 48
6.4.2 Activation data protection 48
6.4.3 Other aspects of activation data 48
6.5 Computer Security Controls 48
6.5.1 Specific computer security technical requirements 48
6.5.2 Computer security rating 49
6.6 Life Cycle Technical Controls 49
6.6.1 System development controls 49
6.6.2 Security management controls 49
6.6.3 Life cycle security controls 49
6.7 Network Security Controls 49
6.8 Time-stamping 49
7 Certificate, CRL, and OCSP Profiles 50
7.1 Certificate Profile 50
7.1.1 Version number(s) 50
7.1.2 Certificate extensions 50
7.1.3 Algorithm object identifiers 51
7.1.4 Name forms 51
7.1.5 Name constraints 51
7.1.6 Usage of Policy Constraints extension 51
7.1.7 Policy qualifiers syntax and semantics 51
7.1.8 Processing semantics for the critical Certificate Policies extension 51
7.2 CRL Profile 51
7.2.1 Version Number(s) 51
7.2.2 CRL and CRL Entry Extensions 51
7.3 OCSP Profile 52
7.3.1 Version number(s) 52
7.3.2 OCSP extensions 52

8 Compliance Audit and Other Assessments 53
8.1 Frequency or circumstances of assessment 53
8.2 Identity/qualifications of assessor 53
8.3 Assessor's relationship to assessed entity 53
8.4 Topics covered by assessment 53
8.5 Actions taken as a result of deficiency 53
8.6 Communication of results 53
9 Other Business and Legal Matters 54
9.1 Fees 54
9.1.1 Certificate issuance or renewal fees 54
9.1.2 Certificate access fees 54
9.1.3 Revocation or status information access fees 54
9.1.4 Fees for other services 54
9.1.5 Refund policy 54
9.2 Financial Responsibility 54
9.2.1 Insurance coverage 54
9.2.2 Other assets 54
9.2.3 Insurance or warranty coverage for end-entities 54
9.3 Confidentiality of Business Information 54
9.3.1 Scope of confidential information 55
9.3.2 Information not within the scope of confidential information 55
9.3.3 Responsibility to protect confidential information 55
9.4 Privacy of Personal Information 55
9.4.1 Privacy plan 55
9.4.2 Information treated as private 55
9.4.3 Information not deemed private 55
9.4.4 Responsibility to protect private information 55
9.4.5 Notice and consent to use private information 55
9.4.6 Disclosure pursuant to judicial or administrative process 55
9.4.7 Other information disclosure circumstances 55
9.5 Intellectual Property Rights 56

9.6 Representations and Warranties 56
9.6.1 CA representations and warranties 56
9.6.2 RA representations and warranties 56
9.6.3 Subscriber representations and warranties 56
9.6.4 Relying party representations and warranties 56
9.6.5 Representations and warranties of other participants 56
9.7 Disclaimers of Warranties 56
9.8 Limitations of Liability 56
9.9 Indemnities 56
9.10 Term and Termination 56
9.10.1 Term 56
9.10.2 Termination 57
9.10.3 Effect of termination and survival 57
9.11 Individual notices and communications with participants 57
9.12 Amendments 57
9.12.1 Procedure for amendment 57
9.12.2 Notification mechanism and period 57
9.12.3 Circumstances under which OID must be changed 57
9.13 Dispute Resolution Provisions 58
9.14 Governing Law 58
9.15 Compliance with Applicable Law 58
9.16 Miscellaneous Provisions 58
9.16.1 Entire agreement 58
9.16.2 Assignment 58
9.16.3 Severability 58
9.16.4 Enforcement (attorneys' fees and waiver of rights) 58
9.16.5 Force Majeure 58
9.17 Other Provisions 58

Annex A. Terms and conditions for user certificate package (authentication, encryption and signature) 59

Document control

Basic Description

Document title	ECB PKI Certificate Policy (CP) Advanced Encryption OID: 1.3.6.1.4.1.41697.509.10.100.2.1.3
Topic	Certificate Policy for the ECB PKI Service based on RFC 3647
Version	1.1
Status	Published release related to introduction of the new ECB PKI and for certification for CAF compliancy
Document OID	1.3.6.1.4.1.41697.509.10.100.2.1.3
Supersedes Document	-
Authors	Daniela Puiu, Ulrich Kühn
ECB responsible contact	Daniela Puiu

Version History

Version	Version Date	Comment
1.0	27.02.2024	Initial Draft
1.0	05.09.2024	First version submitted for approval
1.1	28.10.2024	Corrections on CP CPS documents, to address PKI AB inquiries

Document Review and Signoff

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

Related Documents

Document title	ECB PKI Certification Practice Statement (CPS)
Document Name	2024-03-01 ECB PKI Certification Practice Statement (CPS) (OID:1.3.6.1.4.1.41697.509.10.100.0.1) v1.0.pdf
Description	Certification Practice Statement for the ECB PKI Service
Document OID	1.3.6.1.4.1.41697.509.10.100.0.1
Latest available version	V1.1
Last changed	28.10.2024

Document title	ECB RSA Certificate Profiles RFC5280
Document Name	ECB RSA Certificate Profiles RFC 5280 v1.0.xlsx
Description	RFC5280 Certificate Profiles for ECB PKI
Latest available version	V1.0
Last changed	05.03.2024

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	v2.0
Last changed	27.06.2024

Document title	ECB PKI Operational Concept v1.0
Document Name	ECB PKI Operational Concept v1.0
Description	Overview of the ECB PKI operational processes and procedures
Latest available version	V1.0
Last changed	28.10.2024

1 Introduction

This document is a Certificate Policy (CP) for the European Central Bank Certificate Services Public Key Infrastructure (hereinafter referred to as “ECB PKI”).

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 Authority ECB RSA AV Sub CA 01 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 PKI Certificate Policy 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 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) offers a variety of certificates applicable to distinct user groups and/or certificate applications. While the ECB PKI CPS sets forth the responsibilities of the PKI participants, technical and organisational measures taken to ensure operational continuity and security for meeting specific requirements on certificate issuance, this CP document sets forth the requirements certificate applicants and subjects must satisfy to qualify for such type of certificate.

Doing so, the CP states what level of assertion can be expected from a specific certificate issued by the ECB PKI, thus enabling relying parties assessing the level of trust they may associate to presented ECB PKI certificates of this type.

1.1.1 Implementation of the ECB PKI certificate authority hierarchy

The following section is a brief overview of the implemented ECB PKI trust chain model and the CA hierarchy for the ECB RSA 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 RSA, and issuing subordinate CAs certified by it. The Root CA and Issuing subordinate CAs define the whole CA certificate chain.

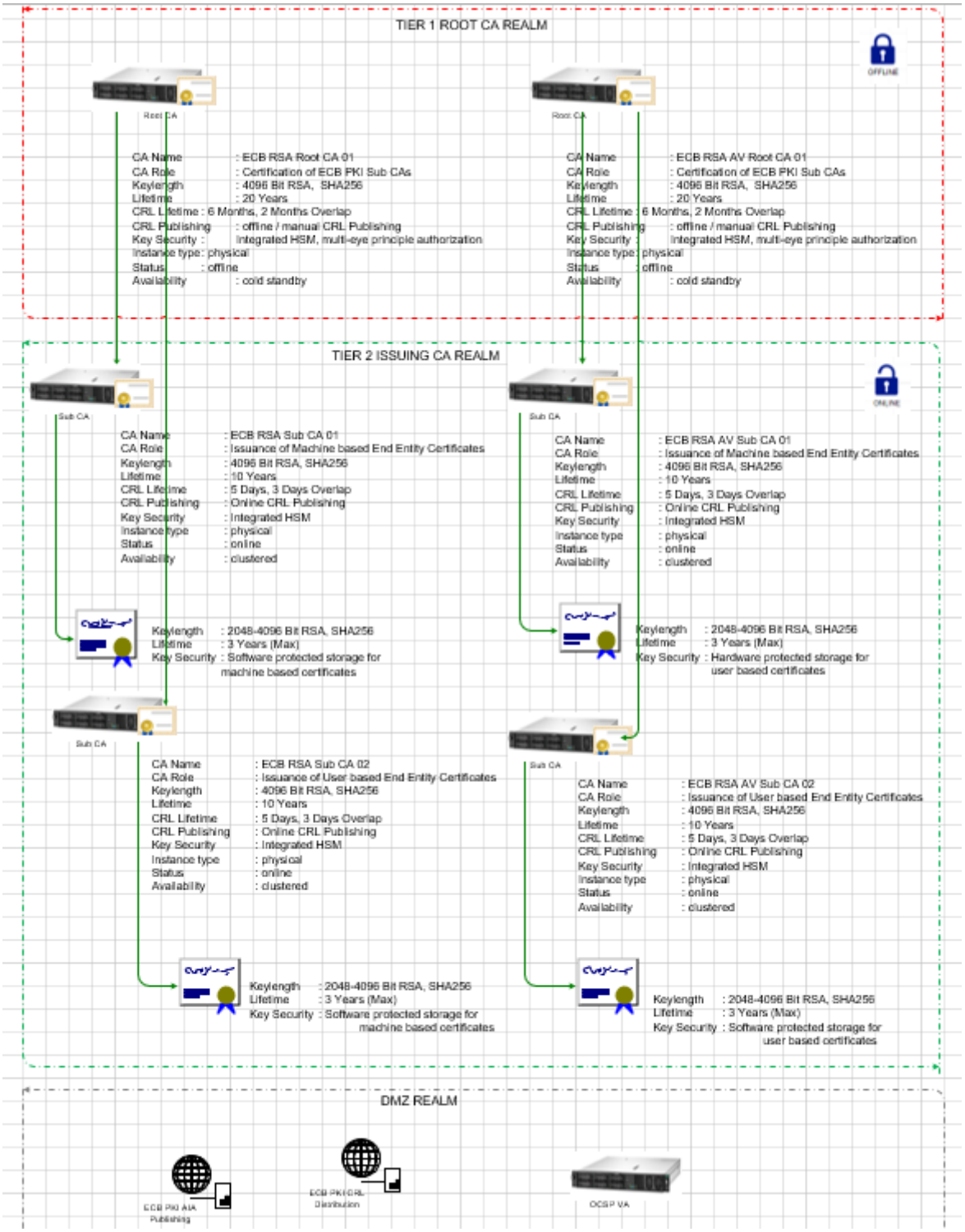
The ECB PKI environment is comprised of ECB RSA AV Root CA 01 as the trust anchor and, on the subordinate level, the ECB RSA AV Sub CA 01 and the ECB RSA AV Sub CA 02 providing certificate issuance for different purposes. The ECB RSA AV Sub CA 01 is used for issuance of advanced authentication, signature and encryption user-based certificates, while the ECB RSA AV Sub CA 02 is used to issue shard mailboxes and application account certificates (listed here for completeness).

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

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

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

Overview of the ECB RSA trust chain:



1.2 Document Name and Identification

This CP is called "**ECB Advanced Encryption Certificate Policy (CP)**" for the ECB PKI service. The Object Identifier (OID) representing this document is 1.3.6.1.4.1.41697.509.10.100.2.1.3. 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 trust chain identifier

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

X.509 OID –Environment

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

X.509 OID – Issuance Policies Namespace

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

X.509 OID – ECB NG Issuance Policy Reference

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

X.509 OID – ECB PKI CPS Reference

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

X.509 OID – ECB PKI Internal trust realm

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

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

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

X.509 OID – ECB PKI Issuing Authorities CP

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

X.509 OID – ECB PKI Directory signing realm

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

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

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

X.509 OID – ECB PKI Object signing realm

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

X.509 OID – ECB PKI ECB Subscriber CP

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

X.509 OID – ECB PKI CAF Compliant realm

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

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

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

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

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

X.509 OID – ECB PKI Advanced profile realm

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

X.509 OID –AV CP documentation

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

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

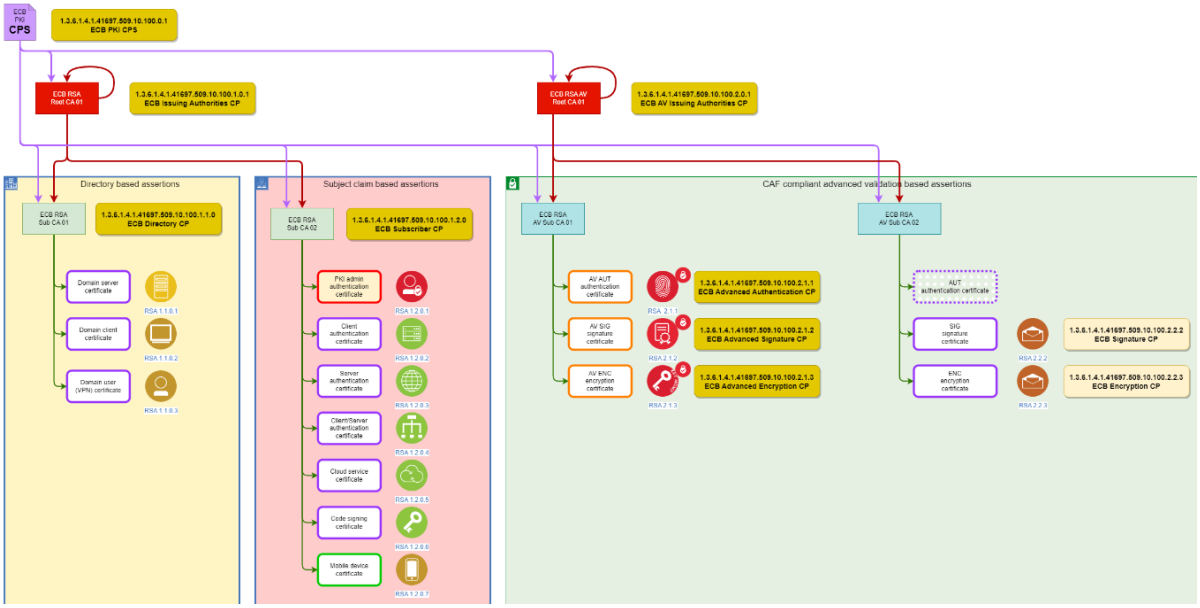
1.3.6.1.4.1.41697.509.10.100.2.**1.3** ECB Advanced Encryption Certificate Policy

X.509 OID – ECB PKI Standard profile realm

1.3.6.1.4.1.41697.509.10.100.2.**2**	ECB PKI Standard profile realm

X.509 OID –CP documentation

1.3.6.1.4.1.41697.509.10.100.2.2.**1**	ECB PKI Authentication CP
1.3.6.1.4.1.41697.509.10.100.2.2.**2**	ECB PKI Signature CP
1.3.6.1.4.1.41697.509.10.100.2.2.**3**	ECB PKI Encryption CP



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

1.3 PKI Participants

1.3.1 Certification Authorities

The ECB PKI CAs involved in the trust chain issuing certificates under this ECB Advanced Authentication CP are:

- Policy root CA:
  - ECB RSA AV Root CA 01
- Issuing sub CA:
  - ECB RSA AV Sub CA 01

- ECB RSA AV Sub CA 02

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.

User encryption certificates issued under this policy must be approved by upstream HR systems and procedures including ECB security clearance and background checks. Thus, the RA role is delegated to the IT service division in charge of producing and issuing the smart card tokens bearing the resulting certificates in conjunction with the inherited assertions attached to the subject by upstream HR procedures

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 Field Services team according to the rules and procedures defined for the ECB employees and contractors.

1.3.3 Subscribers

Subscribers for certificates governed by this CP are ECB employees, contractors and identities having an active account in the ECB Active Directory

The subscriber holds a private key that corresponds to the public key listed in that certificate. Subscribers of the ECB PKI are internal users, as well as approved partners 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 and may or may not be a Subscriber within PKI. 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 under this CP are as follows:

Certificates issued by ECB RSA AV Sub CA 01

ECB RSA AV User encryption certificate	ECB Advanced User Encryption
ECB OCSP Signing	OCSP response signing

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

See section 1.4 on ECB PKI CPS.

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.

Advanced Validation user encryption certificates must only be used for smart card based key/data encryption purposes including secure e-mail.

1.4.2 Prohibited certificate uses

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

The certificate explicitly MUST NOT be used

- to sign lower tier CA certificates,
- for different purposes other than outlined in the certification request,
- outside of their given validity period or after revocation,
- to use subscriber end entity certificates after revocation by the ECB PKI,
- for non-ECB and on non-certified partner subjects, and
- for the usage 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 Director / 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

Term	Alias	Definition
Certificate	public key certificate	A data structure containing the public key of an electronic identity and additional information. A certificate is digitally signed using the private key of the issuing CA binding the subject's identity to the respective public key
Certificate Management over CMS	CMC	Transport mechanism that can be used for obtaining X.509 digital certificates in a PKI
Certificate Policy	CP	A document containing the rules that indicate the applicability and use of certificates issued to ECB PKI subscribers
Certificate Signing Request	CSR	A request from a Subscriber to an RA to create and sign a certificate for a subject with certain attributes specified in the request

Term	Alias	Definition
Certification Authority	CA	The unit within ECB PKI to create, assign and revoke public key certificates
Certification Practices Statement	CPS	A document containing the practices that ECB PKI certification authority employs in issuing certificates and maintaining PKI related operational status
Common Name	CN	An identifier for an end entity (subject)
Directory		A database containing information and data related to identities, certificates and CAs
Encryption		Cryptographic transformation of data (called plaintext) into a form (called cipher text) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called decryption, which is a transformation that restores encrypted data to its original state.
End-Entity		An entity that is a subscriber, a relying party, or both
FIPS 140		FIPS 140 is the (US) Federal Information Processing Standard that outlines security requirements for cryptographic modules. FIPS 140 is one of several cryptographic standards maintained by the Computer Security Division of NIST (National Institute for Standards and Technology)
Hardware Security Module	HSM	A hardware encryption device that is connected to a server at the device level via direct physical interfaces.
Internet Assigned Numbers Authority	IANA	A standards organization that oversees global Internet Protocol–related symbols and Internet numbers
Machine Readable Zone	MRZ	The visual part of an official identity or travel document designed to be interpreted using optical character recognition

Term	Alias	Definition
Object Identifier	OID	An identification mechanism jointly developed by ITU-T and ISO/IEC for naming any type of object, concept or "thing" with a globally unambiguous name
Personal Identification Number	PIN	In practice a (chiefly numeric) password to authenticate a user upon smart card access
Policy Management Authority	PMA	This management authority sets the overall policies of the ECB PKI and approves the policies and procedures of trust domains within the PKI
Private Enterprise Number	PEN	IANA assigned Private Enterprise Numbers are identifiers that can be used in SNMP configurations, in LDAP configurations, and wherever the use of an ASN.1 object identifier (OID) is appropriate
Public Key Cryptography Standards	PKCS	Are a group of public key cryptography standards published by RSA Security LLC
Public Key Infrastructure	PKI	Framework of technical components and related organizational processes for the distribution and management of private keys, public keys and corresponding certificates
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
Subject		Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

Term	Alias	Definition
Subscriber		Entity subscribing with a Certification Authority on behalf of one or more subjects. It is the subject named or identified in a certificate and holds the private key that corresponds to the associated certificate.

2 Publication and Repository Responsibilities

2.1 Repositories

The central repository for the ECB PKI CA, CRL and CP/CPS documentation is the ECB PKI Web site located at http://cpki.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 http://cpki.ecb.europa.eu

All documents, CPs and CPS, are subject of the regulations in place at the ECB defined in the internal rules.

See section 2.1 on ECB PKI CPS.

2.2 Publication of Certification Information

See section 2.2 on ECB PKI CPS.

2.3 Time or Frequency of Publication

See section 2.3 on ECB PKI CPS.

2.4 Access Controls on Repositories

See section 2.4 on ECB PKI CPS.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

ECB PKI Trust Chain

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

CA certificate naming of the **ECB RSA AV Root CA 01**

Attribute	Value
Subject Name	CN = ECB RSA AV Root CA 01 O = European Central Bank C = EU
Subject Alternative Name	None

CA certificate naming of the **ECB RSA AV Sub CA 01**

Attribute	Value
Subject Name	CN = ECB RSA AV Sub CA 01 O = European Central Bank

	C = EU
Subject Alternative Name	None

CA certificate naming of the **ECB RSA AV Sub CA 02** (listed here for completeness)

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

Subscriber certificate naming of **ECB OCSP Signer Certificate**

Attribute	Value
Subject Name	CN = CN=ECB RSA AV 01 OCSP Validation Authority Internal
Subject Alternative Name (DNS)	None

Currently issued subscriber certificate naming of **ECB RSA AV User Authentication**

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

Currently issued subscriber certificate naming of **ECB RSA AV User Encryption**

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

Currently issued subscriber certificate naming of **ECB RSA AV User Signature**

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

3.1.2 Need for names to be meaningful

Names are required to be meaningful in the term that the name form has commonly understood semantics to determine the identity of a person.

3.1.3 Anonymity or pseudonymity of subscribers

ECB PKI supports neither anonymous users nor pseudonyms for users.

3.1.4 Rules for interpreting various name forms

See section 3.1.4 on ECB PKI CPS.

3.1.5 Uniqueness of names

For user certificates the entity distinguished name must be unique over the lifetime of the CA

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 internal 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 subscriber must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be the PKCS#10 or CMC[1] compliant certificate request (CSR). This request is signed with the corresponding private key of the certificate subscriber.

This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber.

3.2.2 Authentication of organization identity

Not applicable.

3.2.3 Authentication of individual identity

Certificate requests under this CP 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

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

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[2] 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)[3]. The users are instructed to change the initial PIN at first use, and are handed over the terms & conditions. Certificate acceptance is corroborated by the use of the USB-based smart card (see section 4.4).
b. 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 first 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).

In the above-mentioned cases, 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.

3.2.4 Non-verified subscriber information

Any enrollment request that holds non-verifiable information and / or information that cannot be validated shall be discarded without any further notice.

3.2.5 Validation of authority

Subscribers must be ECB employees or ECB contractors to be eligible for enrolling with the ECB PKI for AV user authentication certificates. This is validated by establishing a unique mapping between the

[2] 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] 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.

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.

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 expires via 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.

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.

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

See section 3.4 in ECB PKI CPS.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

AV User encryption certificate applications must be submitted by the smart card management RA acting on behalf of the subscriber from within the smart card issuance validation process. Certificate applicants must be ECB employees or approved partners of ECB to submit a certificate application.
A valid ECB Directory user account and appropriate authorization according to the applicant's role is required. 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.

Machine/device requests for ECB OCSP Response Signing certificates are handled in an automatic enrolment scenario.

4.1.2 Enrolment process and responsibilities

Enrolment process

- AV User Encryption certificates under this CP, issued to subscribers are enrolled on a cryptographic USB-based smartcard of the user according to the ECB PKI certificate enrolment processes and procedures in combination with the ECB Registration Authority Officer using the certificate management portal. If the user does not have a USB-based smartcard a new one is issued.
- OCSP Responder certificates to machine subscribers are enrolled automatically via OCSP responder machine and OCSP responder configuration.

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 remote activities) 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.

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.

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.

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. 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.

4.2.3 Time to process certificate applications

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

- ECB IT Certificate Services Operational Level Agreement, or
- ECB IT change management Operational Level Agreement (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 account in Active Directory is eligible and authorized to obtain the device with corresponding certificates. The request is either

- executed by the Registration Authority Officer on behalf of the user, before the user arrives for 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
- executed by the Registration Authority Officer to replace a lost/stolen/forgotten/broken USB-based smartcard, with the user personally present, with the new certificates issued on the spot.

4.3.1 CA actions during certificate issuance

- See section 4.3.1 on ECB PKI CPS.

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 beginning of the enrolment process through a self-service component notification requesting them to go through the renewal process, and also at the end of the enrolment process by the successful issuance notification.

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 or re-keyed 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.

4.4.1 Conduct constituting certificate acceptance

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).

4.4.2 Publication of the certificate by the CA

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 certificates regulated by this CP may be used only to provide the following security services:

- Authentication certificates: authentication of the subscriber.

4.5.2 Relying party public key and certificate usage

See section 4.5.2 on ECB PKI CPS.

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.

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

4.8.1 Circumstance for Certificate Modification

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 RSA AV Root CA 01	20 years	14 years
ECB RSA AV Sub CA 01	10 years	7 years
ECB RSA AV 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 smartcard is lost by accident and any recovery procedure if applicable is not successful, or
- After a subscriber's certificate is deleted
- After modification of the data contained in the certificate
- When the keys are compromised or are no longer fully reliable

4.8.2 Who may request certificate modification

The ECB subscriber must request a certificate modification with re-key in the following cases:

- Modification of data contained in the certificate
- When the keys are compromised
- When the smartcard is lost or broken

The request must be done still within the validity period of the existing certificate[4]. 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-datedness 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.

In case of end of validity period for existing certificates, the certificate modification request is being initiated by the ECB certificate management system on behalf of the subscriber, still within the validity period of existing certificate, and the process is then finalized by the subscribers themselves.

4.8.3 Processing certificate modification requests

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

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.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

See section 4.9.1 on ECB PKI CPS.

4.9.2 Who can request revocation

See section 4.9.2 on ECB PKI CPS.

4.9.3 Procedure for revocation request

See section 4.9.3 on ECB PKI CPS.

[4] 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.

4.9.4 Revocation request grace period

There is no revocation request grace period. All revocation requests are considered effective with the request reaching the ECB Service Desk or ECB PKI operations staff and appropriate measures are started to be applied immediately according to the ECB PKI service level agreement.

4.9.5 Time within which CA must process the revocation request

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

4.9.6 Revocation checking requirement for relying parties

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

4.9.7 CRL issuance frequency

See section 4.9.7 on ECB PKI CPS.

4.9.8 Maximum latency for CRLs

The maximum time allowed between generation of the CRLs and their publication in the repository is 1 hour.

4.9.9 On-line revocation/status checking availability

See section 4.9.9 on ECB PKI CPS.

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 the action that renders a certificate invalid for a period of time prior to its expiry date. The main effect of suspension with regards to the certificate is that the certificate becomes invalid until it is reactivated again.

Certificate suspension is not supported by the ECB certificate management system for individual smartcards on the user USB token / smartcard certificate package.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable

4.9.16 Limits on suspension period

Not applicable

4.10 Certificate Status Services

See section 4.10 on ECB PKI CPS.

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

Procedure for Key recovery with the participation of the certificate subscriber will be as follows:

- The subscriber visits ECB Service Desk and requests the recovery of their encryption certificate
- The request is triggered by ECB Service Desk in the ECB certificate management portal
- Once an existing token already assigned to the subscriber is inserted, the process is finalized and the respective ENC certificate is installed on the cryptographic token, all existing certificates remain on the token and they are not updated

Procedure for Key recovery without participation of the certificate subscriber is as follows:

Key recover process

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

Four-eye principle will always be complied with, i.e., K will always be equal or greater than 2.

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.

See also section 5.1 on ECB PKI CPS.

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.

See also section 5.1.1 on ECB PKI CPS.

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.

See also section 5.1.2 on ECB PKI CPS.

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), Security Officer, 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 RSA AV Root CA 01 must involve multi-person control.

See also section 5.2.2 on ECB PKI CPS.

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.

See also section 5.2.3 on ECB PKI CPS.

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

See section 5.4.3 on ECB PKI CPS.

5.4.4 Protection of audit log

See section 5.4.4 on ECB PKI CPS.

5.4.5 Audit log backup procedures

See section 5.4.5 on ECB PKI CPS.

5.4.6 Audit collection system (internal vs. external)

See section 5.4.6 on ECB PKI CPS.

5.4.7 Notification to event-causing subject

Not applicable.

5.4.8 Vulnerability assessments

See section 5.4.8 on ECB PKI CPS.

5.5 Records Archival

5.5.1 Types of records archived

See section 5.5.1 on ECB PKI CPS.

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

See section 5.5.3 on ECB PKI CPS.

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 RSA AV Root CA 01	20 years	14 years
ECB RSA AV Sub CA 01	10 years	7 years
ECB RSA AV Sub CA 02	10 years	7 years

See section 5.6 on ECB PKI CPS for further details.

5.7 Compromise and Disaster Recovery

See section 5.7 on ECB PKI CPS.

5.7.1 Incident and compromise handling procedures

See section 5.7.1 on ECB PKI CPS for details.

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

See section 5.7.2 on ECB PKI CPS for details.

5.7.3 Entity private key compromise procedures

See section 5.7.3 on ECB PKI CPS for details.

5.7.4 Business continuity capabilities after a disaster

See section 5.7.4 on ECB PKI CPS for details.

5.8 CA or RA Termination

See section 5.8 on ECB 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

User key pairs for encryption are generated on smartcards certified according to CC EAL 4+ or 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 CC EAL 4+ or FIPS 140-2 level 3. A copy of the key pair generated by the CA may be retained for private key archival/backup/escrow.

See section 6.1.1 on ECB PKI CPS.

6.1.2 Private Key delivery to subscriber

User private keys for authentication 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 PKI CPS.

6.1.3 Public key delivery to certificate issuer

Established message standards should be followed.

See section 6.1.3 on ECB PKI CPS.

6.1.4 CA public key delivery to relying parties

See section 6.1.4 on ECB PKI CPS.

6.1.5 Key Sizes

Acceptable Key Size and Algorithms for certificates issued under this CP:

Certification Authority	Key Size and Key Algorithm
ECB RSA AV Root CA 01	4096 Bit RSA
ECB RSA AV Sub CA 01	4096 Bit RSA
ECB RSA AV Sub CA 02	4096 Bit RSA
Subscriber	2048 Bit RSA 3072 Bit RSA 4096 Bit RSA

6.1.6 Public key parameters generation and quality checking

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

See section 6.1.6 on ECB 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.

Acceptable key usage purposes for certificates issued by ECB RSA AV Sub CA 01 under this CP:

- keyEncipherment

See section 6.1.7 on ECB PKI CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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 RSA Root CAs
- All direct Sub CAs of the ECB RSA Root CAs
- All OCSP response signing keys of direct Sub CAs of the ECB RSA Root CAs

ECB PKI advanced subscriber key pairs for encryption shall be generated in FIPS 140-2 Level 3 compliant HSMs and must be imported into CC EAL 4+ or FIPS 140-2 level 3 or above compliant hardware smart cards.

See section 6.2.1 on ECB PKI CPS.

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

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

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

See section 6.2.2 on ECB PKI CPS.

6.2.3 Private Key escrow

The private keys of CAs are escrowed encrypted by one of the corresponding CA's HSM protected public keys (master backup keys). The escrow system requires a 3 out of 5 OCS quorum acting as the escrow agent to decipher the corresponding CA certificate private key.

6.2.4 Private Key backup

The private keys of the ECB PKI Root CAs and their Sub CAs must be backed up in such a way that the private key is protected by cryptographic controls and multi-person authorization.

Private key backup for user certificates for encryption is backed up encrypted by one of the corresponding CA's HSM protected public keys. The backup system allows an automated restore onto the subscriber's smart card with the smart card RA acting as the backup agent on the subscriber's behalf

See section 6.2.4 on ECB PKI CPS.

6.2.5 Private Key archival

Private key archival for user certificates for encryption is archived encrypted by one of the corresponding CA's HSM protected public keys. The archive retrieval system allows a conditional automated restore onto the subscriber's smart card with the smart card RA acting as the retrieval agent on the subscriber's behalf. If the subscriber assigned smart card cannot hold additional historic encryption certificate private keys, ECB PKI may choose to supply encrypted keystore container formats to the subscriber. Such soft-token must not be issued for the newest certificates that can be stored in cryptographic hardware smart cards. The usage of dedicated cryptographic smart cards or other HSM to hold revoked/invalid encryption certificates is recommended.

See section 6.2.5 on ECB 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. Private keys may be generated in a trusted secure environment and transferred into approved smart cards via encrypted transfer channels.

6.2.7 Private Key storage using cryptographic module

See section 6.2.1 of this CP.

See section 6.2.7 on ECB PKI CPS.

6.2.8 Method of activating private key

The private key for user authentication certificates under this CP, must be activated by inserting the smart card token and entering the PIN upon access by an application. See also section 6.2.1 on ECB PKI CPS.

6.2.9 Method of deactivating private keys

The private key is deactivated by logging out of the operating system, turning off the power of the equipment, removing the smart card token and when the cryptographic context the key has been activated in times out. See section 6.2.9 on ECB PKI CPS.

6.2.10 Method of destroying private keys

The private key is destroyed by overwriting the key, token surrender or in case of failure on overwriting the key physically destroying the token.

See section 6.2.10 on ECB 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

The following certificate operational periods and key pair usage periods are defined under this policy.

Certificate Type	Certificate Operational Period	Key Pair Usage Period
ECB AV User encryption certificates	no stipulation	3 years

6.4 Activation Data

6.4.1 Activation data generation and installation

See section 6.4.1 on ECB PKI CPS.

6.4.2 Activation data protection

See section 6.4.2 on ECB PKI CPS.

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.

See section 6.5.1 on ECB PKI CPS.

6.5.2 Computer security rating

See section 6.5.2 on ECB PKI CPS.

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

See section 6.6.2 on ECB PKI CPS.

6.6.3 Life cycle security controls

See section 6.6.3 on ECB PKI CPS.

6.7 Network Security Controls

See section 6.7 on ECB PKI CPS.

6.8 Time-stamping

See section 6.8 on ECB PKI CPS.

7 Certificate, CRL, and OCSP Profiles

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

7.1 Certificate Profile

See section 7.1 on ECB PKI CPS.

7.1.1 Version number(s)

See section 7.1.1 on ECB PKI CPS.

7.1.2 Certificate extensions

Extension	OID	critical	Value
Authority Key Identifier	2.5.29.35	-	Issuing CA fingerprint
Subject Key Identifier	2.5.29.14	-	Subject fingerprint
Key Usage	2.5.29.15	critical	keyEncipherment
Certificate Policies	2.5.29.32	-	CP: 1.3.6.1.4.1.41697.509.10.100.2.1.3 CPS: 1.3.6.1.4.1.41697.509.10.100.0.1
Subject Alternative Name	2.5.29.17	-	RFC822 Name=FirstName.LastName@ecb.europa.eu
Basic Constraints	2.5.29.19	critical	Subject Type = End Entity
Extended Key Usage	2.5.29.37	-	1.3.6.1.4.1.311.80.1 Document Encryption 1.3.6.1.4.1.311.67.1.1 BitLocker Drive Encryption 1.3.6.1.5.5.7.3.4 Email Protection 1.3.6.1.4.1.311.10.3.4 MS Encrypted File System (EFS)
CRL Distribution Points	2.5.29.31	-	http://cpki.ecb.europa.eu/cdp/ECB-RSA-AV-Sub-CA-01-2033.crl
Authority Information Access	1.3.6.1.5.5.7.1.1	-	http://cpki.ecb.europa.eu/aia/ECB-RSA-AV-Sub-CA-01-2033.cer http://ocsp.ecb.europa.eu

See section 7.1.2 on ECB PKI CPS.

7.1.3 Algorithm object identifiers

See section 7.1.3 on ECBPKI CPS.

7.1.4 Name forms

ECB PKI Issuer and Subject Distinguished Names are set in the following order:

CN=[common name],O=[organization],C=[country]

For certificate types under this CP the subject CN will be suffixed by ' [ENC]'.

See also section 7.1.4 on ECB PKI CPS.

7.1.5 Name constraints

ECB RSA AV Sub CA 01 shall add the " [ENC]" suffix to the subject CN of AV User encryption certificates.
Certificate policy object identifier

All certificates issued under this CP bear the Certificate Policies extension (OID 2.5.29.32) including

Document Reference	**OID**
This Certificate Policy document	1.3.6.1.4.1.41697.509.10.100.2.1.3
The ECB PKI Certification Practice Statement	1.3.6.1.4.1.41697.509.10.100.0.1

7.1.6 Usage of Policy Constraints extension

Not applicable.

7.1.7 Policy qualifiers syntax and semantics

See section 7.1.8 on ECB PKI CPS.

7.1.8 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL Profile

See section 7.2 on ECB PKI CPS.

7.2.1 Version Number(s)

See section 7.2.1 on ECB PKI CPS.

7.2.2 CRL and CRL Entry Extensions

See section 7.2.2 on ECB PKI CPS.

7.3 OCSP Profile

See section 7.3 of the ECB PKI CPS.

7.3.1 Version number(s)

See section 7.3.1 on ECB PKI CPS.

7.3.2 OCSP extensions

See section 7.3.2 on ECB 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 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 PKI CPS.

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

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

See section 8.4 on ECB 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 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

See section 9.3.2 on ECB PKI CPS.

9.3.3 Responsibility to protect confidential information

See section 9.3.3 on ECB 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

See section 9.4.2 on ECB PKI CPS.

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.

See section 9.4.4 on ECB PKI CPS.

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

See section 9.10.1 on ECB PKI CPS.

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

See section 9.13 on ECB PKI CPS.

9.14 Governing Law

See section 9.14 on ECB PKI CPS.

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 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.