EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB PKI

Certificate Policy (CP) Standard Authentication OID:1.3.6.1.4.1.41697.509.10.100.1.3.1

Table of Contents

Document control

Basic Description

Document title	ECB PKI Certificate Policy (CP) Standard Authentication OID:1.3.6.1.4.1.41697.509.10.100.1.3.1
Topic	Certificate Policy for the ECB PKI Service based on RFC 3647
Version	1.0
Status	Published release related to introduction of the new ECB PKI and for certification for CAF compliancy
Document OID	1.3.6.1.4.1.41697.509.10.100.1.3.1
Supersedes Document	-
Authors	Daniela Puiu
ECB responsible contact	Daniela Puiu

Version History

Version	Version Date	Comment
1.0	05.02.2025	Initial Draft
1.0		First version submitted for approval

Document Review and Signoff

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

Related Documents

Document title	ECB PKI Certification Practice Statement (CPS)
Document Name	2025-02-05 ECB PKI Certification Practice Statement (CPS) (OID:1.3.6.1.4.1.41697.509.10.100.0.1) v1.2.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	V1.2
Last changed	28.02.2025

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

Document title	ECB PKI IANA PEN Namespace
Document Name	ECB PKI IANA PEN Namespace
Description	Overview of the ECB PKI related IANA PEN Namespace
Latest available version	v2.1
Last changed	10.02.2025

Document title	ECB PKI Operational Concept v1.0
Document Name	ECB PKI Operational Concept v1.0
Description	Overview of the ECB PKI operational processes and procedures
Latest available version	V1.0
Last changed	18.02.2025

1 Introduction

This document is 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 Sub CA 03 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 Root CAs, and issuing subordinate CAs certified by it. The Root CA and Issuing subordinate CAs define the whole CA certificate chain.

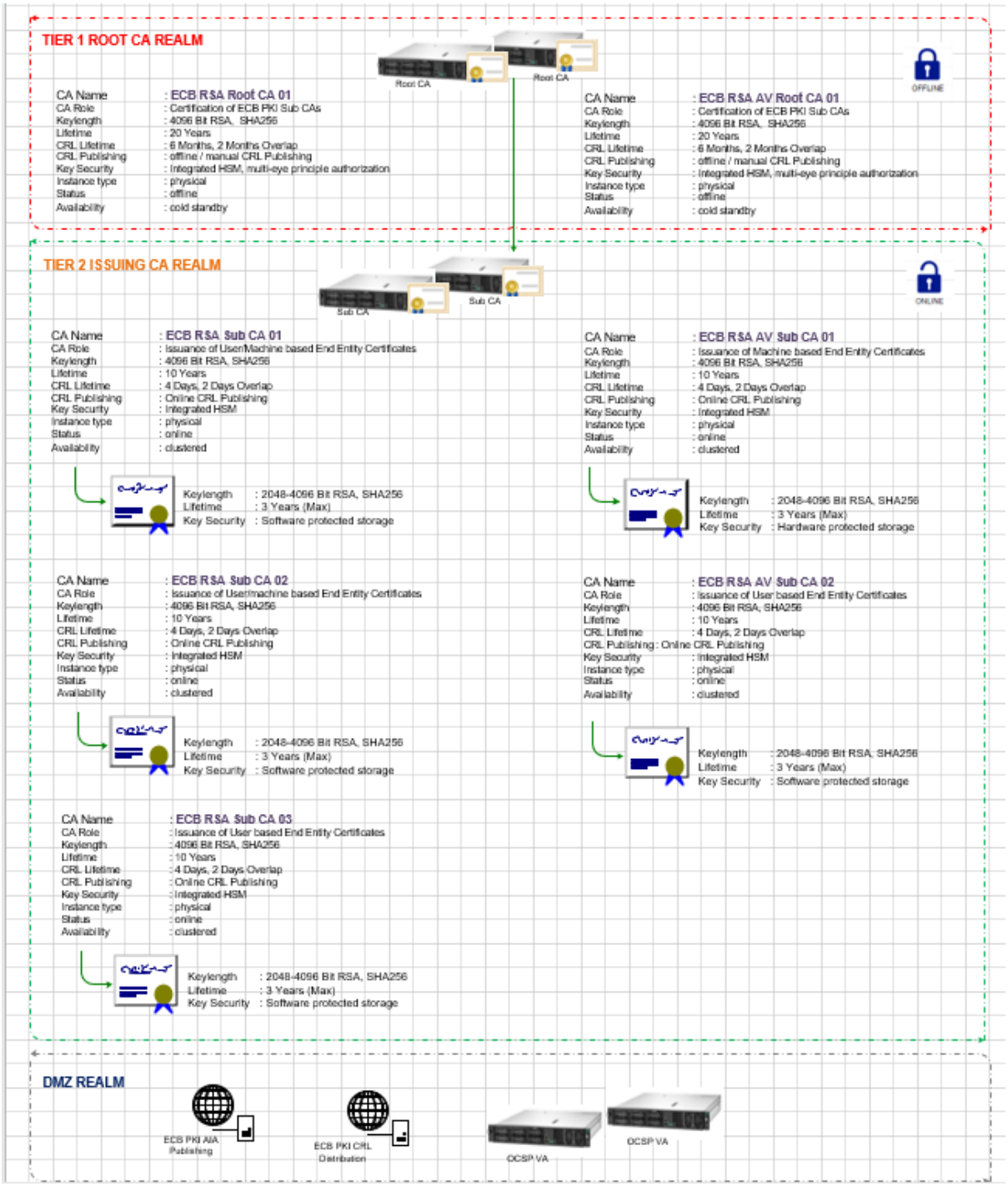
The ECB PKI environment is comprised of ECB RSA Root CA 01 and ECB RSA AV Root CA 01 as the trust anchors and, on the subordinate level, the ECB RSA Sub CA 01, ECB RSA Sub CA 02, ECB RSA Sub CA 03, ECB RSA AV Sub CA 01 and the ECB RSA AV Sub CA 02, each providing certificate issuance for different purposes. The ECB RSA Sub CA 01 is used for issuance of domain-joined machine or user certificates following directory based assertions, ECB RSA Sub CA 02 is used for issuance of user or machine certificates for authentication, signature or encryption following subject claim based assertions, and the ECB RSA Sub CA 03 is used to issue standard authentication, encryption or signature certificates for users. The ECB RSA AV Sub CA 01 is used for issuance of advanced authentication, signature and encryption user-based certificates, while the ECB RSA AV Sub CA 02 is purposed to issue advanced authentication application certificates.

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

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

The other components in the PKI are built from multi-tenant capable centralized components like certificate validation services 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 Standard Authentication Certificate Policy (CP)**" for the ECB PKI service. The Object Identifier (OID) representing this document is 1.3.6.1.4.1.41697.509.10.100.1.3.1. 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 Standard realm

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

X.509 OID –CP documentation

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

1.3.6.1.4.1.41697.509.10.100.1.3.**2** ECB Standard Encryption CP

1.3.6.1.4.1.41697.509.10.100.1.3.**3** ECB Application Authentication CP

X.509 OID – ECB PKI CAF Compliant Advanced realm

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

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

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

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

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

X.509 OID – ECB PKI Advanced profile realm

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

X.509 OID –AV CP documentation

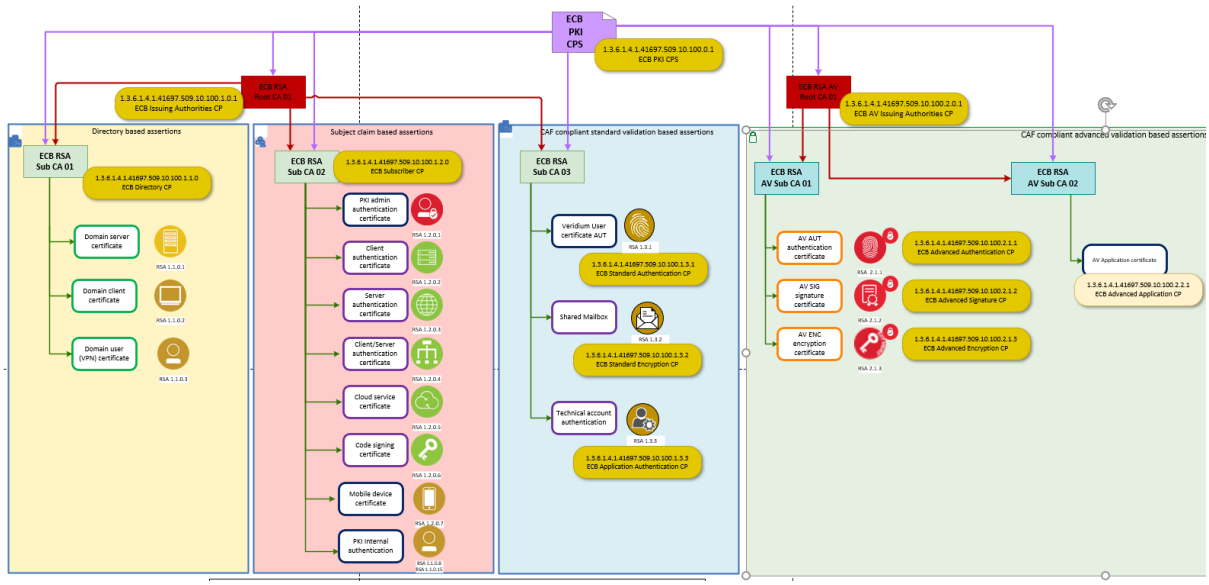
1.3.6.1.4.1.41697.509.10.100.2.**1.1** ECB Advanced Authentication Certificate Policy

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

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

X.509 OID – ECB PKI Advanced application profile realm

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



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

1.3 PKI Participants

1.3.1 Certification Authorities

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

- Policy root CA:
  - ECB RSA Root CA 01

- Issuing sub CA:
  - ECB RSA Sub CA 01
  - ECB RSA Sub CA 02
  - ECB RSA Sub CA 03

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 three 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 authentication certificates issued under this policy are approved by ECB Identity Governance and Access management system following HR procedures including ECB security clearance and background checks. Thus, the RA role is delegated to the Veridium RA system, which is a part of ECB Identity Governance and Access Management service and is in charge of requesting certificates on behalf of the user after their successful identification and authorization through the ECB identity Governance and access management processes.

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.

See also section 1.3.3 on ECB PKI CPS.

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 Sub CA 03

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

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.

Standard validation user authentication certificates must only be used for software-based authentication purposes.

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.
Veridium		Integrated Passwordless Platform (https://www.veridiumid.com/)
VeridiumID Authenticator		Mobile application integrated with Veridium server to provide user identification and authorization

2 Publication and Repository Responsibilities

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 Root CA 01**

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

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

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

CA certificate naming of the **ECB RSA AV Sub CA 03**

Attribute	Value
Subject Name	CN = ECB RSA Sub CA 03 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 03 OCSP Validation Authority Internal O = European Central Bank C = EU
Subject Alternative Name (DNS)	None

Subscriber certificate naming of **ECB RSA Veridium User Authentication certificate**

Attribute	Value
Subject Name	CN = <First Name>.<Last Name> [AUT:S] O = European Central Bank C = EU
Subject Alternative Name (UPN)	<UPN 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.

3.2.2 Authentication of organization identity

Not applicable.

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

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:

- Software Certificates for individual subscribers (ECB 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.
- Veridium Credential Provider together with Veridium mobile application are deployed centrally by the ECB IT Department to all ECB devices (laptops, respectively mobile devices). When a user wants to login to the ECB laptop via VeridiumID Authenticator authentication method, he/she needs to perform an initial registration of the mobile device to Veridium server via a QR code. During the registration, the user needs to accept the End User Licence Agreement together with ECB terms and conditions. Upon successful registration, the user can login using Veridium mobile app and the challenge response process after being identified and authenticated by the Veridium server which confirms the status of the user in Active Directory. During the logon process, the certificate request is triggered to Veridium RA by the Veridium Credential provider. The request is authorized by the Veridium mobile app, at which time the software certificate is created and automatically installed on the user's laptop in their Personal Store. Certificate acceptance is corroborated by the use of the software certificate (see section 4.4).
- When a user has accidentally deleted the software certificate, a new certificate is automatically provisioned for the user upon successful authentication via Veridium mobile app. Certificate acceptance is corroborated by use of the software certificate (see 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 standard user authentication certificates. This is validated by establishing a unique mapping between

the user's identity and their 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 Re-key process does not apply for certificates issued under this CP, all certificate requests are treated as new enrollment requests and the process described in section 3.2 applies.

3.3.1 Identification and authentication for routine re-key

Not applicable.

3.3.2 Identification and authentication for re-key after revocation

Not applicable.

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

Standard User authentication certificate applications are submitted by the Veridium RA acting on behalf of the subscriber from within the certificate 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 is required.

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

- Standard User Authentication certificates under this CP are generated on the subscriber's laptop upon logon and after successful registration in Veridium and identification and authorization by Veridium Server through Veridium mobile app. Any user holding an active account in Active Directory and registered with Veridium system is eligible and authorized to receive such a certificate.
- The user accepts the terms and conditions at the time of registration with Veridium Server
- OCSP Responder certificates to machine subscribers are enrolled automatically via OCSP responder machine and OCSP responder configuration.

Responsibilities

- For user software certificates under this CP, the Veridium Server is responsible (see also section 3.2.3 for an overview of the overall process) to verify the user's identity against the ECB Active Directory and to ensure a mapping between user identity and their registered mobile devices. At the same time, Veridium server authorizes the Veridium Credential Provider to request a certificate to the Veridium RA server
- Veridium RA server receives the certificate requests from Veridium Credential Provider and is responsible for sending the CSR to the CA on behalf of the user. Veridium RA receives the signed certificate from the CA and returns the certificate to the Veridium Credential Provider which then installs the certificate onto the user's store.
- Veridium Credential Provider is responsible for submitting the certificate request to the Veridium RA and installing the signed certificate onto the user store. In case a user is offline, Credential Provider performs the logon of the user with the software certificate which was previously issued. For online logon cases, Credential Provider performs the user logon based on challenge-response leveraging the Veridium Mobile app.

4.2 Certificate application processing

For both new and existing users the certificate request process is triggered when the user selects VeridiumID Authenticator as logon mechanism and scans the QR code presented on the logon screen. Veridium Credential provider sends the certificate request to Veridium RA server which validates the request and forwards it to the CA. User is authenticated and authorized by Veridium server via Veridium mobile app, leading to successful issuance of the certificate.

Veridium Credential Provider and Veridium mobile application have been centrally deployed to all ECB laptops and mobile devices therefore all users can register and are eligible for such certificates.

4.2.1 Performing identification and authentication functions

Identification and authentication of users is done by the Veridium Server verifying the requester's identity in ECB Active Directory and establishing the unique mapping between the user's identity and the Active Directory-based user account.

4.2.2 Approval or rejection of certificate applications

Every user of ECB internal systems, i.e. ECB staff and contractors having an account in the ECB's Active Directory, is eligible to obtain user software certificates 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 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

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

4.3 Certificate Issuance

Software Certificates for individual users are being requested whenever a user selects VeridiumID Authenticator as logon mechanism and scans the QR code presented on the logon screen. Veridium Credential provider sends the certificate request to Veridium RA server which validates the request and forwards the request to the CA. User is authenticated and authorized by Veridium Server via Veridium mobile app, leading to successful issuance of the certificate. If the user has already been issued with such a certificate, the offline logon action will be done using the existing certificate and no new certificate is being issued; online logon is performed through challenge-response authentication. Any user holding an active account in Active Directory is eligible to obtain the software

certificate. The certificate request process is concluded with the installation of the certificate in the Personal User store. The same process applies in case the certificate has been deleted or revoked.

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

The first enrolment of certificates under this CP takes place after the registration of the user's mobile device with Veridium Server. During the registration, the user is presented with, and needs to accept the End User License Agreement together with the ECB Terms and Conditions for the certificate usage. The standard user certificates are short lived and a new certificate is issued automatically ten days before certificate expiration. Users are not notified when the certificate is being renewed.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

Receiving the certificate is integrated into a workflow which

- Generates new key pairs,
- Informs the user about the terms and conditions set out in the ECB internal rules during device registration,
- Requests the actual issuance of the certificate, and
- Generates the certificate on the user's laptop.

Completion of this process, together with installation of the certificate in the user's store and successful logon, 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.

Certificate Renewal process does not apply for certificates issued under this CP, all certificate requests are treated as new enrollment requests and the process described in section 3.2 applies.

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.

Certificate Re-key process does not apply for certificates issued under this CP, all certificate requests are treated as new enrollment requests and the process described in section 3.2 applies.

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 for most use cases 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.

Certificate Modification with re-key process does not apply for certificates issued under this CP, all certificate requests are treated as new enrollment requests and the process described in section 3.2 applies

4.8.1 Circumstance for Certificate Modification

CA 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 Root CA 01	20 years	14 years
ECB RSA Sub CA 01	10 years	7 years
ECB RSA Sub CA 02	10 years	7 years
ECB RSA Sub CA 03	10 years	7 years

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

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.

4.9.4 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 user software certificates.

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 Root CA 01 certificate is expired or the respective Root CA service is terminated.
- CRL and OCSP of ECB RSA Sub CA 01 subscription ends, when the ECB RSA Sub CA 01 certificate is expired or the ECB RSA Sub CA 01 service is terminated.
- CRL and OCSP of the ECB RSA Sub CA 02 subscription ends, when the ECB RSA Sub CA 02 certificate is expired or the ECB RSA Sub CA 02 service is terminated.
- CRL and OCSP of the ECB RSA Sub CA 03 subscription ends, when the ECB RSA Sub CA 03 certificate is expired or the ECB RSA Sub CA 03 service is terminated.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

No key recovery or escrow is supported for standard user software authentication certificates.

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 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 must be modified and re-keyed before their expiration to guarantee the continuity of offered services. New CA key pairs must 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 Root CA 01	20 years	14 years
ECB RSA Sub CA 01	10 years	7 years
ECB RSA Sub CA 02	10 years	7 years
ECB RSA Sub CA 03	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 standard authentication are generated by the ECB PKI Issuing CA, and are stored in a file conformant to the PKCS#12 specification.

See section 6.1.1 on ECB PKI CPS.

6.1.2 Private Key delivery to subscriber

User private keys for standard user authentication under this CP are generated on the Veridium RA server and their delivery to the Veridium Credential Provider is performed via encrypted channels, both in transit and at rest.

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 Root CA 01	4096 Bit RSA
ECB RSA Sub CA 01	4096 Bit RSA
ECB RSA Sub CA 02	4096 Bit RSA
ECB RSA Sub CA 03	4096 Bit RSA
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 Sub CA 03 under this CP:

- digitalSignature

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

User key pairs for standard user authentication are stored in a FIPS 140-2 Level 1 compliant software cryptographic provider.

See section 6.2.8 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 are 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

Private Key escrow is not supported for the certificates issued under this CP.

6.2.4 Private Key backup

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

Veridium user standard authentication certificates including their corresponding private keys are cached in the Veridium RA server to reduce the load on the PKI and to be provided to the user at the next login. The cached certificates are stored on the RA server in an SQL lite database encrypted with the machine key.

See section 6.2.4 on ECB PKI CPS.

6.2.5 Private Key archival

Private key archival for user certificates for authentication is prohibited.

See section 6.2.5 on ECB PKI CPS.

6.2.6 Private Key transfer into or from a cryptographic module

Not applicable.

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 standard user authentication certificates under this CP, are activated by user's successful offline logon to Windows using VeridiumID Authenticator authentication method. See also section 6.2.8 on ECB PKI CPS.

6.2.9 Method of deactivating private keys

The private key is deactivated by logging out of the operating system and/or turning off the equipment. See section 6.2.9 on ECB PKI CPS.

6.2.10 Method of destroying private keys

The private key is destroyed by deletion, which is performed by the Credential Provider, or by certificate revocation.

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 RSA Veridium User authentication certificates	no stipulation	40 days

Certificate Type	Certificate Operational Period	Key Pair Usage Period
ECB RSA Shared Mailbox	No stipulation	2 years
ECB RSA Service Account Authentication	No stipulation	2 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

ECB PKI end-entity certificate profile under this CP:

ECB RSA Veridium User Authentication	
X.509 Version	V3
Serial Number	present
Signature Algorithm	sha256RSA
Issuer	CN = ECB RSA Sub CA 03 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 = firstname.lastname [AUT:S] O = European Central Bank C = EU
Key Usage (critical)	Digital Signature
Basic Constraints (critical)	Subject Type=CA, Path Length Constraint=0
Subject Key Identifier	present
Authority Key Identifier	fba080552eac4db33250e60095527e427d2684ae
CRL Distribution Points	http://cpki.ecb.europa.eu/cdp/ECB-RSA-Sub-CA-03-2035.crl
Authority Information Access	http://cpki.ecb.europa.eu/aia/ECB-RSA-Sub-CA-03-2035.cer
Subject Alternative Name	Other Name:Principal Name=firstname.lastname@ecb.europa.eu
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Smart Card Log-on (1.3.6.1.4.1.311.20.2.2)

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	digitalSignature
Certificate Policies	2.5.29.32	-	CPS: 1.3.6.1.4.1.41697.509.10.100.0.1 CP: 1.3.6.1.4.1.41697.509.10.100.1.3.1
Subject Alternative Name	2.5.29.17	-	Other Name: Principal Name=<FirstName.LastName@ecb.europa.eu>
Basic Constraints	2.5.29.19	critical	Subject Type = End Entity
Extended Key Usage	2.5.29.37	-	1.3.6.1.5.5.7.3.2 Client Authentication 1.3.6.1.4.1.311.20.2.2 MS Smart Card Logon
CRL Distribution Points	2.5.29.31	-	http://cpki.ecb.europa.eu/cdp/ECB-RSA-Sub-CA-03-2035.crl
Authority Information Access	1.3.6.1.5.5.7.1.1	-	http://cpki.ecb.europa.eu/aia/ECB-RSA-Sub-CA-03-2035.cer http://ocsp.ecb.europa.eu
Microsoft SID	1.3.6.1.4.1.311.25.2	-	provided by subscriber

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

See section 7.1.4 on ECB PKI CPS.

7.1.5 Name constraints

ECB RSA Sub CA 03 shall add the "[AUT:S]" suffix to the subject CN of Veridium User authentication certificates.

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

Document Reference	OID
This Certificate Policy document	1.3.6.1.4.1.41697.509.10.100.1.3.1
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 standard authentication certificate

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 software certificate 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 certificate;
- 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;
- Not transfer or delegate to third parties the obligations pertaining to the certificate assigned to you;
- Ensure that your certificate contains accurate and complete information about you as a person, and notify the ECB of changes of such information;
- Acknowledge and accept that the CA is entitled to revoke a certificate immediately if the subscriber/user breaches this agreement.