OPEN
INDUSTRIAL
PKI

Open industrial PKI (OiPKI)

Central Certificate Practice Statement

Document History

Version	Date	Author	Change Comments
00.01	05.04.2023	A. Philipp	Initial version

This document will be reviewed every year or in the event of an important ad-hoc change request. Each new version will be approved by the OiPKI Board.

Document Status

This document has been classified as “Unrestricted“.

	Name	Dep.	Date
Author	Various authors, detailed in formation in document history		
Checked by	Andreas Philipp Florian Handke	Keyfactor Campus Schwarzwald	2023-06-21 2023-06-21
Authorization	Florian Handke	Campus Schwarzwald	2023-06-21

Content

1 Scope and Applicability

This document constitutes the Central Certification Practice Statement (CPS) for the Open industrial PKI (OiPKI). The purpose of this document is to publicly disclose to interested parties the business policies and practices under which the OiPKI operates.

2 Introduction

The structure of this document follows the template specified in the RFC 3647 standard.
This work is licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0). (To view a copy of the license, visit https://creativecommons.org/licenses/by/4.0/.

2.1 Overview

See OiPKI Certificates Policy (OiPKI CP).

2.2 PKI Participants

See OiPKI Certificates Policy (OiPKI CP).

2.2.1 Certification Authorities

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.2.2 Registration Authorities

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.2.3 Subscribers

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.2.4 Relying Party

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.2.5 Other Participants

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.3 Certificate Usage

2.3.1 Appropriate Certificate Uses

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.3.2 Prohibited Certificate Uses

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.4 Policy administration

2.4.1 Organization Administering the Document

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.4.2 Contact Person

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.4.3 Person determining CPS Suitability for the Policy

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.4.4 CPS Approval Procedures

Specified in the OiPKI Certificates Policy (OiPKI CP).

2.4.5 Definitions and Acronyms

See section Abbreviations

3 Publication and Repository Responsibilities

3.1 Repositories

Specified in the OiPKI Certificates Policy (OiPKI CP) and application related Tenant CPS

3.2 Publication of Certification Information

Specified in the OiPKI Certificates Policy (OiPKI CP) and application related Tenant CPS

3.3 Time and Frequency of Publication

Specified in the OiPKI Certificates Policy (OiPKI CP) and application related Tenant CPS

3.4 Access Controls on Repositories

Specified in the OiPKI Certificates Policy (OiPKI CP) and application related Tenant CPS

4 Identification and Authentication

4.1 Naming

4.1.1 Type of names

Specified in the OiPKI Certificates Policy (OiPKI CP).

4.1.2 Need for Names to be Meaningful

Specified in the OiPKI Certificates Policy (OiPKI CP).

4.1.3 Anonymity or Pseudonymity of Subscribers

Specified in the OiPKI Certificates Policy (OiPKI CP).

4.1.4 Rules for Interpreting Various Name Forms

Specified in the OiPKI Certificates Policy (OiPKI CP).

4.1.5 Uniqueness of Names

Specified in the OiPKI Certificates Policy (OiPKI CP).

4.1.6 Recognition, Authentication and Role of Trademarks

Specified in the OiPKI Certificates Policy (OiPKI CP).

4.2 Initial Identity Validation

4.2.1 Method to Prove Possession of Private Key

The method to proof private key possession is described in the application specific Tenant CPS.

4.2.2 Authentication of Organization Identity

The authentication of the organization identity is part of the onboarding process in which also the identity of the organization as well as of the persons requesting the onboarding will be verified. During the authentication process the following steps are processed:

- validation of the given email and phone number during a initial communication channel
- validation of the given company Identification Number against a third party database from a reliable Data Source,
- cross check references with social Networks
- we will reserve the right, in unclear situations, to arrange a meeting with the requesting person to validate the identity. The meeting can take place both on site and virtually.

4.2.2.1 Authentication of Identity

Specified in the OiPKI Certificates Policy (OiPKI CP) and application related Tenant CPS

4.2.2.2 Verification of the Country

Specified in the OiPKI Certificates Policy (OiPKI CP) and application related Tenant CPS

4.2.3 Non-verified Subscriber Information

Specified in the OiPKI Certificates Policy (OiPKI CP) and application related Tenant CPS

4.2.4 Validation of Authority

Specified in application related Tenant CPS

4.2.5 Criteria for Interoperation

Specified in the OiPKI Certificates Policy (OiPKI CP) and application related Tenant CPS

4.3 Identification and Authentication for Re-key Requests

4.3.1 Identification and Authentication for Routine Re-key

Specified in the OiPKI Certificates Policy (OiPKI CP)

4.3.2 Identification and Authentication for Re-key after Revocation

Not supported.

4.4 Identification and Authentication for Revocation Request

Revocation requests for EE certificates require either a digitally signed request via the given interface by an authorized RA or can be submitted digitally signed by the Tenant registered contact person via signed email.
Details how to request certificates revocation are specified in the application relevant Tenant CPS.

5 Certificate Life Cycle Operational Requirements

5.1 Certificate Application

5.1.1 Who Can Submit a Certificate Application

As part of the onboarding process a checklist must be generated. This checklist includes (but not limited to):

- Name of the Person that are authorized to represent the Tenant.
- Second name of a Person that are authorized to represent the Tenant.
- Organization identification of the Tenant.
- Contact Details.

These named persons are later allowed to request changes and issues.
During the regular operations, only authorized RAs will be accepted for submitting certificate releated request. Therefore, the Issuing CA will issue during the onboarding process a RA Token for the Tenant. Only request that are signed by the RA Token are accepted by the Issuing CA.

5.1.2 Enrollment process and responsibilities

As part of the onboarding process, credentials that are required will be either provide by the Tenant or securely generated and distributed. For example, RA Certificates and the TLS Certificates for the Tenants are generated and securely transferred to the Tenant. The keys are securely send (e.g. PKCS#12 container) to the named Tenant contact person (from the Checklist). The credential to access the keys are send the second contact person of the Tenant.

Processes and responsibilities for enrolment of End Entities certificates are described in the application specific Tenant CPS.

5.2 Certificate Application Processing

5.2.1 Performing identification and authentication function.

Only authorized certificate requests for EE certificates are accepted.

5.2.2 Approval or Rejection of Certificate Applications

The requester is informed about the approval or rejection either protocol specific, or via email.
Only requests conforming to the respective certificate profile will be processed by the issuing CA.

5.2.3 Time to Process Certificate Applications

A request for a new Tenant will be processed within one (1) week. Requests for EE certificates will be executed immediately (typically within 10 second).

5.3 Certificate Issuance

5.3.1 CA Actions during Certificate Issuance

The certification requests for EE Certificates are validated by the issuing CA to guarantee conformance with the respective certificate profile.

5.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The issuing CA informs the tenant RA via the used certificate management protocol.

5.3.3 Conduct constituting certificate acceptance.

The certificate is considered accepted as soon as an acknowledgement of receipt has been received or the certificate has been used.

5.4 Key Pair and Certificate Usage

5.4.1 Subscriber Private Key and Certificate Usage

Specified in the OiPKI Certificates Policy (OiPKI CP)

5.4.2 Relying Party Public Key and Certificate Usage

Specified in the OiPKI Certificates Policy (OiPKI CP).

5.5 Certificate Renewal

Unless otherwise stated in the Tenant CPS, certificates renewal are specified in the OiPKI Certificate Policy (OiPKI).

5.5.1 Circumstances for Certificate Renewal

The renewal procedure must be documented in the Tenant CPS.

5.5.2 Who may request renewal

The request condition must be documented in the Tenant CPS

5.5.3 Processing certificate renewal requests

Not supported unless otherwise stated in the Tenant CP.

5.5.4 Notification of new certificate issuance to subscriber

Not supported unless otherwise stated in the Tenant CP.

5.5.5 Conduct constituting acceptance of a renewal certificate

Not supported unless otherwise stated in the Tenant CP.

5.5.6 Publication of the renewal certificate by the CA

Not supported unless otherwise stated in the Tenant CP.

5.5.7 Notification of certificate issuance by the CA to other entities

Not supported unless otherwise stated in the Tenant CP.

5.6 Certificate re-key

5.6.1 Circumstance for certificate re-key

The Re-key Process can only be requested if the ownership of the affected certificate that is still valid is proved by the certificate applicant.

5.6.2 Who may request certification of a new public key

5.6.2.1 Re-keying of Issuing CA certificates

Re-keying of Issuing CA certificates is not supported.

5.6.2.2 Re-keying of End Entity certificates

For re-keying of EE certificates, the same requirements apply as for certificate Issuance (see section 5.2).

5.6.3 Processing certificate re-keying requests

See section 5.3.

5.6.4 Notification of new certificate issuance to subscriber

See section 5.3.2.

5.6.5 Conduct constituting acceptance of a re-keyed certificate

See section 5.3.3.

5.7 Certificate modification

Certificate modification is not supported

5.8 Certificate Revocation and Suspension

5.8.1 Circumstances for Revocation

Specified in the OiPKI Certificates Policy (OiPKI CP).

5.8.2 Who can Request Revocation

Specified in the OiPKI Certificates Policy (OiPKI CP).

5.8.3 Procedure for Revocation Request

The procedure for revocation of EE certificates is described in the Tenant CPS.
Only authorized revocation request are executed by the Device PKI. Such requests either need to be signed by authorized Tenant Person listed in the onboarding Checklist or they can be send by authorized RA via the used management protocol.

5.8.4 Revocation Request Grace Period

Specified in the OiPKI Certificates Policy (OiPKI CP).

5.8.5 Time within which CA must process the revocation request

In case of interest Device PKI will revoke certificates without any delay. In case an appropriate certificates management protocol is used the revocation request will be carried out automatically. In case of a signed request, performend by an authorized person, it will be carried out during the normal business hour of the OiPKI.

5.8.6 Revocation checking requirement for relying parties

See Tenant CPS.

5.8.7 CRL issuance frequency

Specified in the OiPKI Certificates Policy (OiPKI CP).

5.8.8 Maximum Latency for CRLs

Specified in the OiPKI Certificates Policy (OiPKI CP).

5.8.9 Online revocation/status checking availability

Specified in the OiPKI Certificates Policy (OiPKI CP)..

5.8.10 Online revocation checking Requirements

Specified in the OiPKI Certificates Policy (OiPKI CP)..

5.8.11 Other forms of revocations advertisements available

No stipulation.

5.8.12 Special requirements re-key Compromise

In case the private key of the issuning CA is compromised or it is suspected, OiPKI will inform the affected Tenant (contact person listed in the Checklist) via signed email.

5.8.13 Circumstances for suspension

No stipulation.

5.8.14 Who can request suspension

No stipulation.

5.8.15 Procedure for suspension request

No stipulation.

5.8.16 Limits on suspension Period

No stipulation.

5.9 Certificate Status Service

5.9.1 End of Subscription

No stipulation.

5.9.2 Key Escrow and Recovery

No stipulation.

6 Facility, Management, and Operational Controls

6.1 Physical Controls

6.1.1 Site Location and Construction

For centrally operated and managed components see OiPKI CP.
Controls under Tenant policy are specified in the respective Tenant CPS.

6.1.2 Physical Access

For centrally operated and managed components see OiPKI CP.
Controls under Tenant policy are specified in the respective Tenant CPS.

6.1.3 Power and Air Conditioning

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.1.4 Water Exposures

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.1.5 Fire Prevention and Protection

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.1.6 Media Storage

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.1.7 Waste Disposal

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.1.8 Off-Site Backup

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.2 Procedural Controls

6.2.1 Trusted Roles

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.2.2 Number of Persons Required per Task

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS

6.2.3 Identification and Authentication for Each Role

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.2.4 Roles Requiring Separation of Duties

No stipulation.

6.3 Personnel Controls

6.3.1 Qualifications, Experience, and Clearance Requirements

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.3.2 Background Check Procedures

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.3.3 Training Requirements

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.3.4 Retraining Frequency and Requirements

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.3.5 Job Rotation Frequency and Sequence

No stipulation.

6.3.6 Sanctions for Unauthorized Actions

For centrally operated and managed components see OiPKI CP.

Controls under Tenant policy are specified in the respective Tenant CPS.

6.3.7 Independent Contractor Requirements

For centrally operated and managed components see OiPKI CP.

6.3.8 Documentation Supplied to Personnel

For centrally operated and managed components see OiPKI CP.

6.4 Audit Logging Procedures

For centrally operated and managed components see OiPKI CP.

6.4.1 Types of Events Recorded

For centrally operated and managed components see OiPKI CP.

6.4.2 Frequency of Processing Log

For centrally operated and managed components see OiPKI CP.

6.4.3 Retention Period for Audit Log

For centrally operated and managed components see OiPKI CP.

6.4.4 Protection of Audit Log

For centrally operated and managed components see OiPKI CP.

6.4.5 Audit Log Backup Procedures

For centrally operated and managed components see OiPKI CP.

6.4.6 Audit Collection System (Internal vs. External)

For centrally operated and managed components see OiPKI CP.

6.4.7 Notification to Event-Causing Subject

For centrally operated and managed components see OiPKI CP.

6.4.8 Vulnerability Assessments

For centrally operated and managed components see OiPKI CP.

6.5 Records Archival

6.5.1 Retention period for Archive

For centrally operated and managed components see OiPKI CP.

6.5.2 Protection of Archive

For centrally operated and managed components see OiPKI CP.

6.5.3 Archive Backup Procedures

No stipulation.

6.5.4 Requirements for Time-Stamping of Records

No stipulation.

6.5.5 Archive Collection System (internal or external)

No stipulation.

6.5.6 Procedures to Obtain and Verify Archive Information

No stipulation.

6.6 Key changeover

See OiPKI CP.

6.7 Compromise and Disaster Recovery

See OiPKI CP.

6.8 CA or RA Termination

See OiPKI CP.

7 Technical Security Controls

7.1 Key pair generation and installation

7.1.1 Key pair generation

For CA Key Pairs that are either used as a CA Key pair for the Root CA or the SubCAs, the CA shall:

- Prepare and follow a Key Generation Script
- Should have a trusted third party designated to oversee and attest to the process.

In all cases, the CA shall:

- generate the CA Key Pair in a physically secured environment.
- log its CA Key Pair generation activities.

7.1.2 Private Key delivery to subscriber

For centrally operated and managed components see OiPKI CP.
Controls under Tenant policy are specified in the respective Tenant CPS.

7.1.3 Public Key delivery to Certificate Issuer

The subscriber delivers the public key in a Certificate Signing Request. Therefore a secure certificates management protocol applied.

7.1.4 CA public key delivery to relying parties

See Tenant CPS.

7.1.5 Key sizes

For RSA key pairs the CA shall:

- Ensure that the modulus size, when encoded is at least 2048bits
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, the CA shall:

- Ensure that the key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

No other algorithms or key sizes are permitted.

7.1.6 Public key parameters generation and quality checking

RSA: The CA shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between 2^16 + 1 and 2^256 - 1. The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: The CA should confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

7.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

See OiPKI CP.

7.1.8 Private Key Protection and Cryptographic Module Engineering Controls

The CA shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the protected operational system must consist of either physical key protection or encryption mechanism or a combination of both, implemented in a manner that prevents disclosure of the Private Key.

7.1.9 Cryptographic module standards and controls

No stipulation.

7.1.10 Private key (n out of m) multi-person control

No stipulation.

7.1.11 Private key escrow

No stipulation.

7.1.12 Private key backup

See Section 5.2.2.

7.1.13 Private key archival

Parties other than the Subordinate CA shall not archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

7.1.14 Private key transfer into or from a cryptographic module

If the key transportation required that the CA shall encrypt the private key for transport purposes. If the CA becomes aware that the private Key has been opened to an unauthorized person or an organization then the CA shall revoke all certificates that include the corresponding public key.

7.1.15 Private key storage on cryptographic module

The CA should protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

7.1.16 Activating Private Keys

No stipulation.

7.1.17 Deactivating Private Keys

No stipulation.

7.1.18 Destroying Private Keys

No stipulation.

7.1.19 Cryptographic Module Capabilities

No stipulation.

7.2 Other Aspects of Key Pair Management

7.2.1 Public Key Archival

No stipulation.

7.2.2 Certificate Operational Periods and Key Pair Usage Periods

See OiPKI CP.

7.3 Activation Data

7.3.1 Activation Data Generation and Installation

Activation Data for CA private Keys must be at least PIN protected.

7.3.2 Activation Data Protection

Activation Data has to be kept private and protected.

7.3.3 Other Aspects of Activation Data

No stipulation.

7.4 Computer security controls

7.4.1 Specific computer security technical requirements

All of the responsible unit's IT systems must be run according to the applicable IT security guidelines and must be competently protected against manipulation and espionage.

7.4.2 Computer security rating

No stipulation.

7.5 Life cycle technical controls

7.5.1 System development controls

No stipulation.

7.5.2 Security management controls

No stipulation.

7.5.3 Life cycle security controls

No stipulation.

7.6 Network security controls

No stipulation.

7.7 Time-stamping

No stipulation.

8 Certificate, CRL, and OCSP Profiles

8.1 Certificate profile

8.1.1 Version Numbers

See OiPKI CP.

8.1.2 Certificate Extensions

See OiPKI CP.

8.1.3 Algorithm Object Identifiers

See OiPKI CP.

8.1.4 Name Forms

See OiPKI CP.

8.1.5 Name Constraints

See OiPKI CP.

8.1.6 Certificate Policy Object Identifier (OID)

See OiPKI CP.

8.1.7 Usage of Policy Constraints Extension

See OiPKI CP.

8.1.8 Policy Qualifiers Syntax and Semantics

See OiPKI CP.

8.1.9 Processing Semantics for the Critical Certificate Policies Extension

See OiPKI CP.

8.2 CRL Profile

8.2.1 Version Number(s)

See OiPKI CP.

8.2.2 CRL and CRL Entry Extensions

See OiPKI CP.

8.2.3 OCSP Profile

No stipulation.

9 Compliance Audit and Other Assessments

No stipulation.

9.1 Frequency or Circumstances of Assessment

No stipulation.

9.2 Identity/Qualifications of Assessor

No stipulation.

9.3 Assessor’s Relationship to Assessed Entity

No stipulation.

9.4 Topics Covered by Assessment

No stipulation.

9.5 Actions Taken as a Result of Deficiency

No stipulation.

9.6 Communication of Results

No stipulation.

10 Other Business and Legal Matters

10.1 Fees

See OiPKI CP.

10.2 Financial Responsibility

See OiPKI CP.

10.3 Confidentiality of Business Information

10.3.1 Scope of Confidential Information

See OiPKI CP.

10.3.2 Information not within the Scope of Confidential Information

See OiPKI CP.

10.3.3 Responsibility to protect confidential information

No stipulation.

10.4 Privacy of personal information

10.4.1 Privacy plan

See OiPKI CP.

10.4.2 Information treated as private

See OiPKI CP.

10.4.3 Information not deemed private

See OiPKI CP.

10.4.4 Responsibility to protect private information

See OiPKI CP.

10.4.5 Notice and consent to use private information

See OiPKI CP.

10.4.6 Disclosure pursuant to judicial or administrative process

See OiPKI CP.

10.4.7 Other information disclosure circumstances

See OiPKI CP.

10.5 Intellectual property rights

See OiPKI CP

10.6 Representations and Warranties

10.6.1 CA representations and warranties

See OiPKI CP.

10.6.2 RA representations and warranties

See OiPKI CP.

10.6.3 Subscriber representations and warranties

See OiPKI CP

10.6.4 Relying party representations and warranties

See OiPKI CP.

10.6.5 Representations and warranties of other participants

See OiPKI CP.

10.7 Disclaimers of warranties

See OiPKI CP.

10.8 Limitations and Liability

See OiPKI CP.

10.9 Indemnities

See OiPKI CP.

10.10 Term and Termination

10.10.1 Term

See OiPKI CP.

10.10.2 Termination

See OiPKI CP.

10.10.3 Effect of Termination and survival

See OiPKI CP.

10.11 Individual notices and communications with participants

See OiPKI CP.

10.12 Amendments

10.12.1 Procedure for Amendment

See OiPKI CP.

10.12.2 Notification mechanism and period

See OiPKI CP.

10.12.3 Circumstances under which OID must be changed

See OiPKI CP.

10.13 Dispute resolution provisions

See OiPKI CP.

10.14 Governing law

See OiPKI CP.

10.15 Compliance with applicable law

See OiPKI CP.

10.16 Miscellaneous provisions

10.16.1 Entire agreement

See OiPKI CP.

10.16.2 Assignment

See OiPKI CP.

10.16.3 Severability

See OiPKI CP.

10.16.4 Enforcement

See OiPKI CP.

10.16.5 Force Majeure

See OiPKI CP.

10.17 Other Provisions

See OiPKI CP.

11 Abbreviations

OiPKI	Open industry PKI
CA	Certificate Authority
Certificate	Secure assignment of public keys to a subscriber
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CRL DP	CRK distribution Point
DC	Data Center
HSM	Hardware Security Module
OID	Object identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RFC	Request for Comment, documents for global standardization
RFC3647	This RFC describes documents that outline PKI operations
Root CA	Highest CA of a PKI
SHA	Secure Hash Algorithm
X.509	Certification Standard