OPEN
INDUSTRIAL
PKI

Open industrial PKI (OiPKI)
Certificate Policy

Document History

Version	Date	Author	Change Comments
01.00	09. May 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 Introduction

1.1 Overview

This Certificate Policy (CP) document outlines the certificate policies for the Open industrial Public Key Infrastructure (OiPKI).

The OiPKI service include, but not limited to, issuing, managing, validating, revoking and renewing X.509 Certificates. OiPKI is operated in accordance with the requirements of these CP and consistent with the OiPKI Certification Practice Statement (CPS).

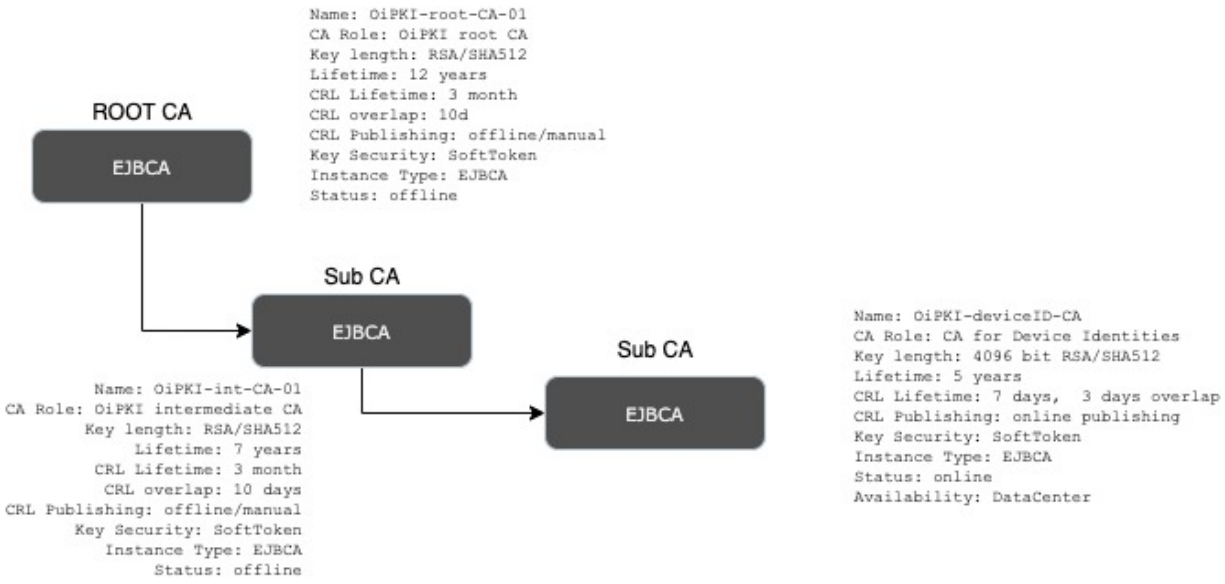
The OiPKI services are provided to pre-registered user with exceptions considered appropriate by the OiPKI Board Members or in accordance with relevant law.

OiPKI services are typically, but not exclusively, offered under the "Open industrial PKI" brand.

Other document related to the behavior and operation of the OiPKI, e.g., Subscriber Agreement or privacy policy can be found at: <LINK>

According to IETF PKIX RFC 3647, this CP is structured into nine parts that covering security controls, practices and procedures for the certification services provided by the OiPKI.

The following Certificates Authorities are covered und this CP:



```
Name: OiPKI-root-CA-01
CA Role: OiPKI root CA
Key length: RSA/SHA512
Lifetime: 12 years
CRL Lifetime: 3 month
CRL overlap: 10d
CRL Publishing: offline/manual
Key Security: SoftToken
Instance Type: EJBCA
Status: offline
```

```
Name: OiPKI-int-CA-01
CA Role: OiPKI intermediate CA
Key length: RSA/SHA512
Lifetime: 7 years
CRL Lifetime: 3 month
CRL overlap: 10 days
CRL Publishing: offline/manual
Key Security: SoftToken
Instance Type: EJBCA
Status: offline
```

```
Name: OiPKI-deviceID-CA
CA Role: CA for Device Identities
Key length: 4096 bit RSA/SHA512
Lifetime: 5 years
CRL Lifetime: 7 days,  3 days overlap
CRL Publishing: online publishing
Key Security: SoftToken
Instance Type: EJBCA
Status: online
Availability: DataCenter
```

1.2 Document name and identification

This is the OiPKI Certificate Policy. This document was approved by the OiPKI Board and it is available at https://www.open-industrial-pki.org/

1.3 PKI Participants

1.3.1 Certification Authorities

The Open-Industrial-PKI (OiPKI) uses a two-stage certification structure with a self-signed root certificate. This two-stage certification structure exist independent to any other certification structure operated by Open industrial PKI. The root CA is not cross signed.
The root CA certifies only SubCAs. SubCAs are used to create certificates for the subscribers named in section Subscribers.

1.3.2 Registration Authorities

The registration authorities (RA) are responsible for:

- verifying the identity and authenticity of subscribers,
- registration procedure,
- documentation of registration procedure and
- suspension and revocation of certificates

The registration process is typically, but not exclusively, done via an online process. The registration process is described in section Identification and Authentication.

1.3.3 Subscribers

Subscribers are natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

1.3.4 Relying Party

Any natural person or Legal Entity that relies on a Valid Certificate. An Application Hardware & Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The main objective of the certificates issued, is to enable efficient and secure electronic communication, while addressing the user's concerns about the trustworthiness of certificates. This also helps to identify the user and to make decisions based on the certificate.

1.4.2 Prohibited Certificate Uses

No stipulation.

1.5 Policy administration

1.5.1 Organization Administering the Document

This CP is maintained by the operator of the Open industrial PKI Board Members.

1.5.2 Contact Person

The Open Industrial PKI can be contacted at:

Campus Schwarzwald
(Centrum für Digitalisierung, Führung und Nachhaltigkeit Schwarzwald gGmbH)
Herzog-Eberhard-Straße 56
72250 Freudenstadt

Issues can be filed in via the GitHub repository where the CP is maintained: https://github.com/Open-Industrial-PKI/cp-cps

1.5.3 Person determining CPS Suitability for the Policy

CPs are always verified by the Open industrial PKI Board Members. The Open industrial PKI Board Members is the high level management body in case of the PKI.
The responsible unit verifies that each CPS complies with the guidelines in the respective CP.

1.5.4 CPS Approval Procedures

This CP will be published on the Open industrial PKI website.
The Open industrial PKI Board Members approves any revisions to the OiPKI CPS after formal review.
The documents will not be passed on to any other Organizations for validation.

1.5.5 Definitions and Acronyms

See section Abbreviations

2 Publication and Repository Responsibilities

2.1 Repositories

The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy.

2.2 Publication of Certification Information

The OiPKI publishes the following information :

- Root CA certificates with fingerprints
- CA certificates with fingerprints
- CRLs
- CPs and CPSs

The OiPKI host a test infrastructure that allows Application Hardware & Software suppliers to test their software with subscriber Certificates.

2.3 Time and Frequency of Publication

Publication dates for CA/root CA certificates, CRLs, CP and CPS are as follows:

- CA/root CA certificates with fingerprints: as soon as they are generated
- CRLs: after revocation, otherwise on a regular schedule see Certificate Life Cycle Operational Requirements.
- CPs and CPSs: after generation / updates

2.4 Access Controls on Repositories

Read access to the information listed under points *Repositories* and *Publication of Certification Information* is not restricted.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of names

The permitted types of name must be documented in the CPS.
Optionally, certificates can contain Subject Alternative Names (SAN).

3.1.2 Need for Names to be Meaningful

The name of the certificate issued (DN) must uniquely identify the subscriber within the BBk- PKI-Advanced.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

No stipulation.

3.1.6 Recognition, Authentication and Role of Trademarks

OiPKI has no procedures for resolving brand disputes trademarks violation and other IP related issues.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The respective method must be documented in the CPS.

3.2.2 Authentication of Organisation Identity

CA SHALL verify the identity of the applicant and the authenticity of the certificate application of the applicant's representative using a verification process that meets the requirements of this section and is described in the CA's certification policy and/or certification practice statement. The CA SHALL check each document relied upon under this clause for modifications or falsification.

3.2.2.1 Authentication of Identity

The type of authentication and the type of proof given must be documented in the CPS of the SubCAs. During the pre Registration process the subscriber applicant will be authenticated and identified by the OiPKI, at least one of the following:

- validation of the given email and phone number during a communication channel validation
- validation of the given company Identification Number against a third party database from a reliable Data Source,
- cross check references with social Networks
- a site visit by members or reliable partners who is acting as an agent for the OiPKI

3.2.2.2 Verification of the Country

If the subject Country Name is present, OiPKI SHALL verify the country associated with the subject by using one of the following :

- Matching the IP address of the specified company website with specified country name
- Matching the Country Name with the registered Company Address

3.2.3 Non-verified Subscriber Information

Only information required to authenticate and identify the subscriber is verified. All other subscriber information is ignored.

3.2.4 Validation of Authority

This procedure is described in the respective CPS.

3.2.5 Criteria for Interoperation

No stipulation. No cross-certification with other organizations is planned or present.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

No stipulation.

3.3.2 Identification and Authentication for Re-key after Revocation

If a certificate is revoked, a new application is required.

3.4 Identification and Authentication for Revocation Request

Applicants (natural persons) must uniquely authenticate by the OiPKI , at least with one of the following:

- validation of the given email and phone number during a communication channel validation
- validation of the given company Identification Number against a third party database from a reliable Data Source,
- cross check references with social Networks
- a site visit by members or reliable partners who is acting as an agent for the OiPKI

If a uniquely authentication of the applicant is not possible certificate will be suspended.
The applicant's identity is documented in the event of a revocation request.
Reason and way of submitting of revocation request is documented.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Only Subscribers, as defined above, who have passed the registration and who are obtaining an identification token from the CA could apply for certificates.

4.1.2 Enrollment process and responsibilities

An application for certificates involves a multistage registration process to the responsible unit. The following checks are made:

- Is the applicant authorized?
- Is the application complete, and correct? (The respective method must be documented in the CPS.)

4.2 Certificate Application Processing

Subscribers are identified and authenticated as described in section Identification and Authentication

4.2.1 Approval or Rejection of Certificate Applications

Meeting the formal requirements does not constitute an entitlement to issuance of a certificate. The decision to issue certificates is entirely at the discretion of the OiPKI.
A certificate application must be rejected if the requirements defined in section Identification and Authentication and Certificate Life Cycle Operational Requirements are not fulfilled.
Acceptance or rejection must be documented.

4.2.2 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

SubCAs must guarantee that certificates are only issued for the intended subscribers after checking their application. The issuing procedure and the tasks involved in issuing certificates must be documented in the CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The form of notification and the applicable rules must be documented in the SubCAs CPS.

4.4 Certificate Acceptance

4.4.1 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.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Only the subscriber is entitled to use the private key.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are IT systems and/or IT processes which use the certificate only for the purposes stated therein. The relying party also checks the trust of certificate chain and validity period of the certificate. Any limitation on the usage of certificates must be taken account.

4.6 Certificate Renewal

A certificate could be renewed based on the existing key pair or with new generated key pairs. The renewal procedure must be documented in the CPS.

4.6.1 Circumstances for Certificate Renewal

The renewal procedure must be documented in the CPS.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.6.8 Certificate re-key

4.6.9 Circumstance for certificate re-key

No stipulation.

4.6.10 Who may request certification of a new public key

No stipulation.

4.6.11 Processing certificate re-keying requests

No stipulation.

4.6.12 Notification of new certificate issuance to subscriber

No stipulation.

4.6.13 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.6.14 Publication of the re-keyed certificate by the CA

No stipulation.

4.6.15 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate modification

Within the framework of the OiPKI, a certificate can only be changed if it has been revoked in advance.

4.8 Certificate Revocation and Suspension

4.8.1 Circumstances for Revocation

A certificate must be revoked if a at least one of the following circumstances arises.

- Information in the certificate is no longer valid.
- The private key has been compromised.
- The subscriber is no longer authorized to use the certificates.
- The subscriber no longer requires the certificate.
- The private key of the issuing CA or the RootCA has been compromised. In this case, all certificates issued by this CA are revoked as well.

- The algorithms, key sizes or validity periods of the certificates no longer provides sufficient security. The responsible unit reserves the right to revoke the certificates in question.

4.8.2 Who can Request Revocation

The Subscriber, the RA or the issuing CA can trigger the revocation. In addition, Subscribers, trusted parties, and other third parties, can submit reports of certificate problems and inform the issuing CA of reasonable causes for revoking the certificate.

4.8.3 Procedure for Revocation Request

The revocation request is documented in the RA system of the individual CA. More detailed information is entered in the CPS of the SubCAs.

4.8.4 Revocation Request Grace Period

As soon as a circumstance for revocation arises, subscribers must immediately arrange for the certificate to be revoked.
If special events occur which require the revocation of a Sub-CA, the assessment by a security officer and revocation of the Sub-CA must take place within 24 hours after the event has been recognized.

4.8.5 Time within which CA must process the revocation request

After receiving a certificate request or a certificate problem, the CA should investigate the facts and the circumstances related to the reported problem and should reply with a preliminary report as soon as possible. The CA SHOULD revoke a certificate within **24 hours** and MUST revoke a Certificate within 5 days.

4.8.6 Revocation checking requirement for relying parties

No stipulation.

4.8.7 CRL issuance frequency

Root CA CRLs is issued with a validity period of 180 days. A new list is issued one week prior to expiry of the most recent CRL. Rules governing the publication of CRLs of SubCAs can be found in the respective CA's CPS.
If the revocation of a certificate leads to the creation of a new CRL, this is published immediately and replaces the prevailing CRL irrespective of its original duration.
A new CRL contains the information about revoked certificates until those certificates have expired.

4.8.8 Maximum Latency for CRLs

CRLs must be published as soon as they have been created.

4.8.9 Online revocation/status checking availability

CRLs from the responsible unit are published via the CRL Distribution Points feature. CDPs must be selected in such a way that all the designated subscribers have access to them.

4.8.10 Online revocation checking Requirements

No stipulation.

4.8.11 Other forms of revocations advertisements available

No stipulation.

4.8.12 Special requirements re-key Compromise

If a subscriber's private key is compromised, the corresponding certificate must be revoked immediately. If a CA's private key is compromised, the CA certificate and all certificates that it has issued must be revoked.

4.8.13 Circumstances for suspension

No stipulation.

4.8.14 Who can request suspension

No stipulation.

4.8.15 Procedure for suspension request

No stipulation.

4.8.16 Limits on suspension Period

No stipulation.

4.8.17 Certificate Status Service

The responsible unit can provide a certificate status request service.

4.8.18 End of Subscription

No stipulation.

4.8.19 Key Escrow and Recovery

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The central (IT) components of the SubCAs are operated in an access-protected areas within a Datacenter (DC). The OiPKI operates his CA Services in a DataCenter that is at least certified to DIN EN ISO 9001 as well as DIN ISO EC 27001.

The root CA is operated offline (without connection to a LAN). Outside the operating hours, all components of the Root CA are stored in a vault. The access to the components is protected.

5.1.2 Physical Access

Physical access must be only for authorized person only.

5.1.3 Power and Air Conditioning

The power supply must meet the required standards.

5.1.4 Water Exposures

The rooms must have adequate protection from exposure to water.

5.1.5 Fire Prevention and Protection

Fire prevention and fire alarm regulations must be observed.

5.1.6 Media Storage

No stipulation.

5.1.7 Waste Disposal

Waste disposal must comply with the local policy. Sensitive waste material (i.e., documentation) shall be disposed of in a secure fashion (e.g., shredding or burning).

5.1.8 Off-Site Backup

There is not an off-site data backup external to the data centers (e.g. at other service providers).

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles must be established to ensure that individuals are not able to change any of the security-critical components or view, generate or manipulate certificates or private keys without being noticed. SubCAs must document established roles in their CPS.

5.2.2 Number of Persons Required per Task

The CA should be operated by personnel in trusted roles.

5.2.3 Identification and Authentication for Each Role

The trusted roles approach is implemented using a few technical and organizational measures. Roles are identified and authenticated by using user IDs and passwords.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

In its operations, the responsible unit shall use experienced personnel who have the necessary IT expertise and specific knowledge of CA operations.

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

Personnel operating CAs for the responsible unit receive regular and ad hoc training. They are sensitized to the security relevance of their work.

5.3.4 Retraining Frequency and Requirements

Retraining is provided when new or amended directives, IT systems and/or IT processes are implemented.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Independent Contractor Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

No stipulation.

5.4 Audit Logging Procedures

All IT systems needed to operate the OiPKI should be synchronized with a master timer. This time source should access an external time signal such as DCF77.

5.4.1 Types of Events Recorded

SubCAs must monitor and document the following processes.

- System initialization
- Certification applications
- Issuance of Certificates
- Generation of CRL
- Publication of a CRL

Any malfunctions or one-off operating situations are also recorded. Retention period is documented in point Retention Period for Audit Log.

5.4.2 Frequency of Processing Log

No stipulation.

5.4.3 Retention Period for Audit Log

The retention period is one year.

5.4.4 Protection of Audit Log

No stipulation.

5.4.5 Audit Log Backup Procedures

No stipulation.

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

CA's MUST include an annual Risk Assessment that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, modification, or destruction of certificate data;
- Evaluates the adequacy of the policies, procedures, information systems, technologies, and other precautions taken by the certification body to address such threats.

5.5 Records Archival

The CA and each Delegated Party SHALL archive all audit logs (as set forth in Section 5.4.1).Types of Records Archived

5.5.1 Retention period for Archive

The retention periods are defined in point 5.4.3.

5.5.2 Protection of Archive

The archives must be protected against unauthorized access, manipulation and destruction.

5.5.3 Archive Backup Procedures

No stipulation.

5.5.4 Requirements for Time-Stamping of Records

No stipulation.

5.5.5 Archive Collection System (internal or external)

No stipulation.

5.5.6 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key changeover

The CA shall change the key whenever the validity of a user certificate to be issued would exceed the remaining term of the CA.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CA organization shall have an Incident Response Plan.

5.7.2 Computing Resources, Software, and/or Data are corrupted

If it is discovered that the CA has faulty or manipulated computing resources, software and/or data that have an impact on the processes conducted by this entity, the system in question must be stopped immediately.

The system must be reset using software and data backups, and – after checks in safe mode – it is to be put back into operation. The faulty or modified system must be analyzed. If there is a suspicion of willful action, legal steps may be taken.

If certificates have been generated using incorrect data, the subscriber or the person responsible for the IT system and/or the IT process must be informed immediately, and the certificate must be revoked by the certification authority.

5.7.3 Entity Private key compromise Procedures

If a CA's private key is compromised, the corresponding certificate must be revoked immediately. All certificates issued by this certification authority must be revoked at the same time. All subscribers affected are to be notified immediately.

The entity in question is set up as a new CA with a new key pair. The certificate of the new CA is published.

5.7.4 Business Continuity Capabilities after a Disaster

See CPS of the SubCAs.

5.8 CA or RA Termination

If the operations of the responsible unit or of a SubCA are terminated, the following measures must be taken.

- Notification of all subscribers as well as relying parties with a lead time of at least three months.
- Revocation of all user certificates as well as all certificates issued by the CA.
- Destruction of the CA's private keys.
- Publication of the corresponding CA and root CA CRLs.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 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.

6.1.2 Private Key delivery to subscriber

Parties other than the Subscriber MUST NOT obtain the Subscriber's private key without the Subscriber's permission.
The prerequisites are defined in the corresponding CPS of the SubCA.

6.1.3 Public Key delivery to Certificate Issuer

The subscriber delivers the public key in a Certificate Signing Request. The technical process of delivery must be described in the CPS.

6.1.4 CA public key delivery to relying parties

No stipulation.

6.1.5 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.

6.1.6 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]

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

For SubCAs, the key usage purposes are

- signing certificates and
- signing CRLs.

6.1.8 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.

6.1.9 Cryptographic module standards and controls

No stipulation.

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

No stipulation.

6.1.11 Private key escrow

No stipulation.

6.1.12 Private key backup

See Section 5.2.2.

6.1.13 Private key archival

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

6.1.14 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 organizatuin then the CA shall revoke all certificates that include the corresponding public key.

6.1.15 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.

6.1.16 Activating Private Keys

No stipulation.

6.1.17 Deactivating Private Keys

No stipulation.

6.1.18 Destroying Private Keys

No stipulation.

6.1.19 Cryptographic Module Capabilities

No stipulation.

6.2 Other Aspects of Key Pair Management

6.2.1 Public Key Archival

No stipulation.

6.2.2 Certificate Operational Periods and Key Pair Usage Periods

The certificates issued by the OiPKI have the following validity periods.

- Root CA certificates: maximum of 12 years
- CA certificates: maximum of 6 years
- User certificates: maximum of 3 years

6.3 Activation Data

6.3.1 Activation Data Generation and Installation

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

6.3.2 Activation Data Protection

Activation Data has to be kept private and protected.

6.3.3 Other Aspects of Activation Data

No stipulation.

6.4 Computer security controls

6.4.1 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.

6.4.2 Computer security rating

No stipulation.

6.5 Life cycle technical controls

6.5.1 System development controls

No stipulation.

6.5.2 Security management controls

No stipulation.

6.5.3 Life cycle security controls

No stipulation.

6.6 Network security controls

No stipulation.

6.7 Time-stamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate profile

7.1.1 Version Numbers

The OiPKI issued certificates are in line with the X509v3 standard.

7.1.2 Certificate Extensions

Sub CAs must document the certificate extensions used in the CPS.

7.1.3 Algorithm Object Identifiers

The RSA (OID 1.2.840.113549.1.1.1) algorithm is used in the certificates issued by the OiPKI.

The ECDSA (OID: 1.2.840.10045.2.1) algorithm is used in the certificates issued by the OiPKI.

The parameter must use the namedCurves encoding:

- For P-256 keys, the namedCurve MUST be secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the namedCurve MUST be secp384r1 (OID: 1.3.132.0.34).
- For P-521 keys, the namedCurve MUST be secp521r1 (OID: 1.3.132.0.35).

7.1.4 Name Forms

See section 3.1.1 and 3.1.2.

7.1.5 Name Constraints

See point 3.1.

7.1.6 Certificate Policy Object Identifier (OID)

The Certificate policy OID is defined in the SubCAs CPS.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

The OiPKI issues CRLs in line with the x.509 norm, version 2.

7.2.2 CRL and CRL Entry Extensions

A CRL distribution point (CRLDP) is contained in the user certificates.

7.2.3 OCSP Profile

No stipulation.

8 Compliance Audit and Other Assessments

No stipulation.

8.1 Frequency or Circumstances of Assessment

No stipulation.

8.2 Identity/Qualifications of Assessor

No stipulation.

8.3 Assessor’s Relationship to Assessed Entity

No stipulation.

8.4 Topics Covered by Assessment

No stipulation.

8.5 Actions Taken as a Result of Deficiency

No stipulation.

8.6 Communication of Results

No stipulation.

9 Other Business and Legal Matters

9.1 Fees

No fees will be charged.

9.2 Financial Responsibility

The OiPKI assume no financial responsibility or liability for certificates issued by SubCAs under this CP.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information and data about OiPKI subscribers and participants that are not covered by point 9.3.2 are considered confidential.

9.3.2 Information not within the Scope of Confidential Information

All information and data that are contained in published certificates and CRLs, either explicitly (e.g. e-mail addresses) or implicitly (e.g. data about certification), or that can be derived from them, are not considered confidential.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

The OiPKI owns the intellectual property rights on this document. The document can be passed on to third parties as it stands.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

The OiPKI undertakes to follow the provisions of the CP.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

Prior to the issuance of a Certificate, the CA shall obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

- The Applicant's agreement to the Subscriber Agreement with the CA, or
- The Applicant's acknowledgement of the Terms of Us

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

As a rule, no warranties are assumed. The OiPKI does not guarantee availability of the PKI services.

9.8 Limitations and Liability

If the CA has issued and managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's Certificate Policy and/or Certification Practice Statement.

9.9 Indemnities

If the certificate and the corresponding private key are improperly used or if the use of key material is based on information that was incorrectly provided during the application process, the OiPKI is released from liability.

9.10 Term and Termination

9.10.1 Term

This CP comes into force on the day it is published.

9.10.2 Termination

This document is valid until it is replaced by a new version or until the OiPKI operations are terminated.

9.10.3 Effect of Termination and survival

The responsibility to protect confidential and personal information remains unaffected by the consequences of terminating this CP.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to the CP are published in a timely manner prior to entering into force.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Serverability

If individual provisions of this CP/CPS are or become invalid, this shall not affect the remaining provisions of this CP/CPS. Likewise, if a provision is missing, this shall not affect the validity of the CP/CPS. In place of the ineffective provision, an effective provision shall be deemed to be agreed that comes closest to the original intention or that would have been determined in line with the meaning and purpose of the CP/CPS had this point been covered therein.

9.16.4 Enforcement

Any legal disputes arising from the OiPKI operations are subject to the laws of the Federal Republic of Germany.
The place of enforcement and jurisdiction is Stuttgart.

9.16.5 Force Majeure

The Open industry PKI accepts no liability for the violation of an obligation, for default or for non-fulfilment under this CP if this results from an underlying event that is beyond its control (e.g. force majeure, war, network outage, fire, earthquake or other catastrophes).

9.17 Other Provisions

No stipulation.

10 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