Open industrial PKI (OiPKI) Certificate Practice Statement

Device ID PKI

Document History

Version	Date	Author	Change Comments
00.01	22.12.2022	A. Philipp	Initial version
00.02	03.04.2023	A. Philipp	Ready for review 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	Keyfactor	2023-06-21
	Florian Handke	Campus Schwarzwald	2023-06-21
Authorization	Florian Handke	Campus Schwarzwald	2023-06-21

Content

1 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/.

1.1 Overview

This document describes the Certification Practice Statement of the OiPKI Device ID PKI (in the following called “Device ID PKI”) to provide Device Identity Certificates.
Together with the Open industrial PKI Certificate Policy it describes the services provided by the Device ID PKI, as well as binding requirements that must be fulfilled by Device ID PKI participants.
The Device ID PKI is a PKI that provides and manages certificates (e.g. “IDevID certificates” or LDevID certificates”) that are stored and used by tenants products and solutions. The private key might be used in bootstrapping scenarios for authentication purposes.
The following stakeholders are involved in the issuing process:

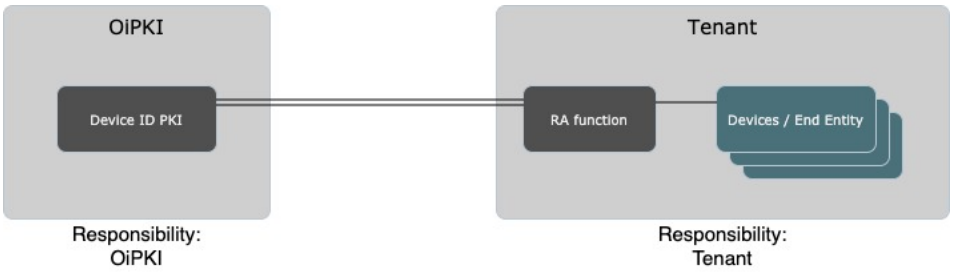

Figure 1 Stakeholder and typical responsibilities.

OiPKI: Responsible for the PKI Service is the organization listed in the central OiPKI CP.
Tenant: Tenant can be every registered and authorized entity that covers the Device ID PKI service. The Tenants has to operate the registration authorities (RA) within their facilities or data center. Therefore, the Tenants are responsible for RA operation and End-Entity authentication.
In accordance with this responsibility split, there are two Certificate Practice Statements on for the central part of the OiPKI PKI (Central Certificate Practice Statement) and one for the Tenant specific aspects (this document)

Right now, there is no specific Tenant CP as a supplement to the Central OiPKI CP. The implementation Document are only for the central side the Central Certificate Practice Statement and the Tenant specific CPS (this document)

1.1.1 PKI hierarchy

The specific PKI hierarchy is show in figure below:

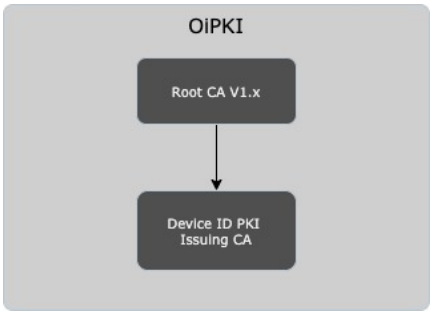

Figure 2 OiPKI Device ID PKI hierarchy

The Issuing CA for the OiPKI Device ID PKI issues certficates that are used (together with the corresponding private key) to identify and authenticate the different Tenants Devices. These certificates are typically deployed on local RAs, managed by the Tenants, but also on the OiPKI side, to correctly identify them and guarantee authenticated and integrity protected connection between the Tenants and the OiPKI Device ID PKI.

1.2 Document name and identification

This CPS is referred to 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

See OiPKI CP.

1.3.1 Certification Authorities

The graphical overview of the CA hierarchy is given in Figure 2

1.3.2 Registration Authorities

See OiPKI CP.

1.3.3 Subscribers

See OiPKI CP.

1.3.4 Relying Party

See OiPKI CP.

1.3.5 Other Participants

See OiPKI CP.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

See OiPKI CP

1.4.2 Prohibited Certificate Uses

See OiPKI CP.

1.5 Policy administration

1.5.1 Organization Administering the Document

This CPS 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

See OiPKI CP.

1.5.4 CPS Approval Procedures

See OiPKI CP.

1.5.5 Definitions and Acronyms

See section Abbreviations

2 Publication and Repository Responsibilities

2.1 Repositories

Tenant specific Device ID PKI repositories are operated by the Tenant itself. The responsibility shall include:

- Accurately publishing information
- Publishing the status of certificates

2.2 Publication of Certification Information

The Tenant shall publish certificates status information at his own operated infrastructure. OiPKI is not responsible for any information in that system.

2.3 Time and Frequency of Publication

The Tenant is responsible for the definition of time and frequency of publishing.

2.4 Access Controls on Repositories

The Tenant is responsible for.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of names

The complete documentation is specified in a separate document (Device ID Certificate Profil) and can be retrieved on request.

3.1.2 Need for Names to be Meaningful

3.1.2.1 CA Names

The CN must be stated as the full name of the CA.

3.1.2.2 End-Entity Names

For details see Device ID Certificate Profile Documentation.

3.1.3 Anonymity or Pseudonymity of Subscribers

See OiPKI CP.

3.1.4 Rules for Interpreting Various Name Forms

See OiPKI CP.

3.1.5 Uniqueness of Names

See OiPKI CP.

3.1.6 Recognition, Authentication and Role of Trademarks

See OiPKI CP.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The key pairs are generated by the End-Entity and the private key proof of possession is realized via state of the art certificate management protocol.

3.2.2 Authentication of Organization Identity

The identity of the requesting organization is checked as part of the onboarding process.

3.2.3 Authentication of Identity

The identity of the requesting Tenant is checked as followed:

- 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
- optional: Site visit by members or reliable partners who is acting as an agent for the OiPKI

3.2.4 Non-verified Subscriber Information

See OiPKI CP.

3.2.5 Validation of Authority

The authority of the requested Tenant is check during the onboarding process as described in 3.2.2.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

See OiPKI CP.

3.3.2 Identification and Authentication for Re-key after Revocation

See OiPKI CP.

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

See OiPKI CP.

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 corresponding the the Device ID Certificate Profil Documenation.

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

See OiPKI CP.

4.2.2 Time to Process Certificate Applications

See OiPKI CP.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The Certificate request information is send in a signed format according to a state-of-the art certificate management protocol. The Issuing CA only accepted request that are sing with pre-registered members.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Only the build mechanism of the used state-of-the art certificate management protocol notification services are supported.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

See OiPKI CP.

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

See OiPKI CP.

4.5.2 Relying Party Public Key and Certificate Usage

See OiPKI CP.

4.6 Certificate Renewal

Certificate renewal (issuance of a new certificate to an entity without changing the public key or any other information in the certificate) is not supported.

4.6.1 Circumstances for Certificate Renewal

No stipulation.

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.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate Modification

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

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

See OiPKI CP.

4.9.2 Who can Request Revocation?

The Tenant RA can request revocation of the EE certificates that been issued for their RA.

4.9.3 Procedure for Revocation Request

Tenant RA owner can request revocation of their EE certficates via the RA using stat-of the art management protocol. If the protocol doesn’t support revocation functionality, it isn’t possible.

4.9.4 Revocation Request Grace Period

See OiPKI CP.

4.9.5 Time within which CA must process the revocation request

See OiPKI CP.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

4.9.7 CRL issuance frequency

See OiPKI CP.

4.9.8 Maximum Latency for CRLs

See OiPKI CP.

4.9.9 Online revocation/status checking availability

See OiPKI CP.

4.9.10 Online revocation checking Requirements

No stipulation.

4.9.11 Other forms of revocations advertisements available

No stipulation.

4.9.12 Special requirements re-key Compromise

See OiPKI CP.

4.9.13 Circumstances for suspension

No stipulation.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension Period

No stipulation.

4.10 Certificate Status Service

See OiPKI CP.

4.11 End of Subscription

See OiPKI CP.

4.12 Key Escrow and Recovery

See OiPKI CP.

5 Facility, Management, and Operational Controls

As the Tenant is responsible for generating key material and operating certificates to securely connect to the Device ID PKI, he shall define his own operation scenarios or should be in line with the OiPKI controls.

5.1 Key changeover

In the event of a CA key changeover, the new CA public key should be published early enough to the Tenant.

5.2 Compromise and Disaster Recovery

5.2.1 Incident and Compromise Handling Procedures

See OiPKI CP.

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

See OiPKI CP.

5.2.3 Entity Private key compromise Procedures

See OiPKI CP.

5.3 CA or RA Termination

See OiPKI CP.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key-pairs for Device ID certificates are created by the Tenant localy.

6.1.2 Private Key delivery to subscriber

The Private Key material never send to the Issuing CA. It should be owned by the Tenant.

6.1.3 Public Key delivery to Certificate Issuer

The subscriber delivers the public key in a Certificate Signing Request. Therefore the provides Toolsets or an supported certificates protocol could be used. (A list of supported protocols could obtain via email request).

6.1.4 CA public key delivery to relying parties

No stipulation.

6.1.5 Key sizes

See OiPKI CP.

6.1.6 Public key parameters generation and quality checking

See OiPKI CP.

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

- Identification and Authentication.

6.1.8 Private Key Protection and Cryptographic Module Engineering Controls

See OiPKI CP.

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 OiPKI CP.

6.1.13 Private key archival

See OiPKI CP.

6.1.14 Private key transfer into or from a cryptographic module

Not supported for End-Entity keys.

6.1.15 Private key storage on cryptographic module

End-Entity keys shall be stored in a security module if feasible. Or they shall be protected in software token e.g. PKCS#12.

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

See OiPKI CP.

6.3 Activation Data

6.3.1 Activation Data Generation and Installation

See OiPKI CP.

6.3.2 Activation Data Protection

See OiPKI CP.

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 and 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

See OiPKI CP

6.6 Network security controls

No stipulation.

6.7 Time-stamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate profile

Details of Tenant Device ID Certificate Profiles could be found in the Documenation.

7.2 CRL Profile

7.2.1 Version Number(s)

See OiPKI CP.

7.2.2 CRL and CRL Entry Extensions

See OiPKI CP.

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 stipulation.

9.2 Financial Responsibility

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

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

No stipulation.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation

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

No stipulation.

9.8 Limitations and Liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 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