
Siemens AG

# Product PKI Certificate Management Service – Certification Practice Statement for Siemens Product PKI Infrastructure Certificates

# Document History

| Version | Date | Author | Change Comment |
|---|---|---|---|
| 1.0 | 26.01.2022 | Michael Munzert, Antonio Vaira; T CST | First released version |

This document will be reviewed every year or in the event of an important ad-hoc change according to the Information Security update process for documents. Each new version will be approved by the respective management level before being released.

This document is published under www.siemens.com/pki.

# Scope and Applicability

This document constitutes the Certification Practice Statement (CPS) for the PKI service providing infrastructure certificates to Siemens Product PKI Tenant. The Product PKI is responsible for the operation of the Root CAs as well as for the Issuing CAs. Together with the Central CPS, this document discloses to interested parties the business policies and practices under which the Product PKI operates.

The Central PMA ensures that the certification practices established to meet the applicable requirements specified in the present document are properly implemented in accordance with Siemens' Information Security Policy.

# Document Status

This document has been classified as “Unrestricted”.

| | Name | Department | Date |
|---|---|---|---|
| **Author** | Various authors, detailed information see document history. | | |
| **Checked by** | Stenger, Meiko<br>Kuechler, Markus | Siemens LC<br>Siemens IT | May, 2020<br>Feb, 2022 |
| **Authorization** | Dr.Gaus, Norbert | Head of Siemens T RPD1 | Jan, 2022 |

# Content

# 1 Introduction

This document is structured according to RFC 3647 “Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework” [RFC3647].

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] even in case the keywords are not capitalized.

## 1.1 Overview

This document describes the Certification Practice Statement of the Siemens Product PKI Certificate Management Service (in the following called “Product PKI”) of the Tenant providing Infrastructure Certificates for all other Product PKI Tenants.

Together with the central CPS [CCPS] it describes the services provided by the Product PKI as well as binding requirements that must be fulfilled by Product PKI participants. In case there are no additional requirements defined by the tenant (in this document, i.e. Tenant CPS), the respective section will refer to the Central CP. In case specific requirements are listed they will apply in addition to the requirements set forth in the Central CP. Under no circumstances, provisions set forth in this document can weaken the requirements set forth in the Central CP.

Moreover - together with the CPSs – the CPs also define the certification process as well as the cooperation, duties and rights of the Product PKI participants.

The Product PKI is a PKI that provides and manages certificates (e.g. “IDevID certificates” or “Manufacturer Device certificates”) that are stored on and used by Siemens products and solutions. The private key might be used in bootstrapping scenarios for authentication purposes. Or the certificate might be used to proof that the device is a genuine Siemens device.

Unless otherwise stated, the term “Product PKI” or any of its entities, refer to “Siemens Product PKI Certificate Management Service”, or any of its respective entities, for the rest of this Certificate Policy.

Since different stakeholders are involved, also responsibilities are distributed between these stakeholders:

- **Product PKI Governance**: responsible for the Product PKI service is the organization listed in section 1.5 Policy Administration.
- **IT Services**: The central Product PKI service is hosted in the Siemens Trust Center that is operated and managed by Siemens IT department.
- **Tenant**: Tenant can be every Siemens AG organizational unit or any other legal entity that has a contract in place that covers Product PKI services. The Tenants typically operate and maintain the registrations authorities (e.g. within their production facilities or data center). Therefore, the Tenants are responsible for RA operation and End-Entity authentication.

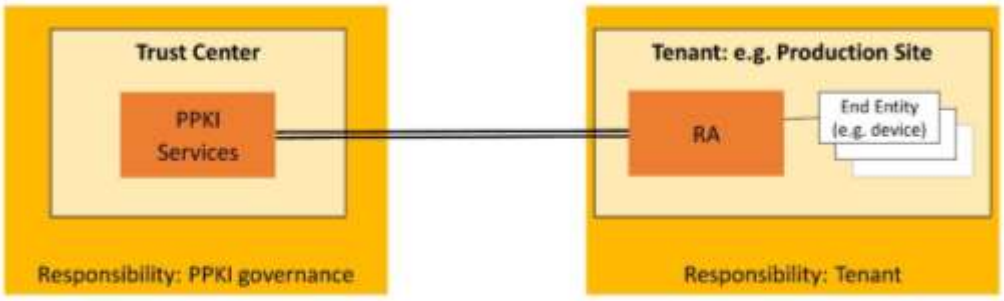



Figure 1: Stakeholders and typical responsibility split

In accordance with this responsibility split, there are two Certificate Policies, one for the central part of the Product PKI (Central CP) and additional ones for the Tenant specific aspects (this document).

The same holds for the corresponding Certification Practice Statements (CPSs).

The Tenant specific CP is always the master document. It defines all requirements for which the Tenant is responsible for. In particular, it comprises the management and operation of the RAs and/or LRAs, of publicly accessible repositories. Where appropriate, the Tenant specific CP will also refer to requirements valid for the operation of the central service. In that case the phrase "See also Central CP for central service aspects". In those sections that are not relevant for the Tenant, it is referred to the central CP by using the phrase "See central CP".

The Tenant specific CP is supplemented with the Central CP. In particular, the Central CP comprises all requirements for the management and operation of the Central PKI System including Root CA and Issuing CAs.

The Tenant CPS describes how the requirements defined in the Tenant CP are implemented.

In addition, the Central CPS supplements how the requirements defined in the Central CP are implemented.

The different documents and their interrelation are depicted in the following figure:

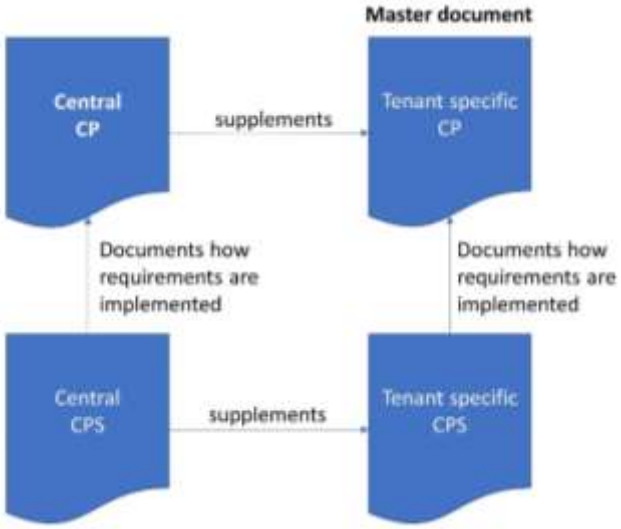
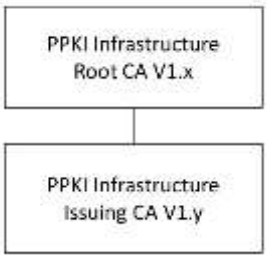



Figure 2: Document structure (CP and CPS)

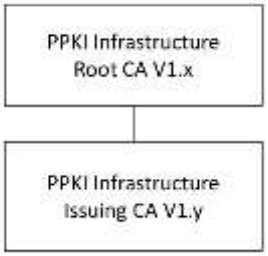
In addition to the requirements defined in this CP and the corresponding CPSs, Siemens IT systems are operated according to the Siemens internal information security rules and respective execution guidelines, which define how IT systems must be operated securely. The corresponding documents can be retrieved on request.

These rules are part of a Siemens ISMS [ISMS], which is defined and implemented according to ISO 27001.

### 1.1.1 PKI hierarchy




The specific PKI hierarchy is shown in Figure 3.




366

367 **Figure 3: PPKI hierarchy for Infrastructure Certificates**

368 The Issuing CA for Siemens Product PKI Infrastructure Certificates issues certificates that are used (together with
369 the corresponding private keys) to identify and authenticate the different Tenants to provide the right, Tenant
370 specific services (e.g. issuing CAs). These certificates are typically deployed on Local RAs, managed by the Tenants,
371 but also on PPKI core components to correctly identify them and guarantee authenticated and integrity protected
372 connections between the Tenants and the PPKI component, e.g. CMP gateway, or any generic PPKI servers.

## 1.2 Document Name and Identification

This CP is referred to as Certificate Policy for the 'Siemens Product PKI Infrastructure Certificates'.

Title: Product PKI Certificate Management Service – Certification Practice Statement for Siemens Product PKI Infrastructure Certificates

OIDs: 1.3.6.1.4.1.4329.99.1.2.1000.1

Expiration: This version of the document is the most current one until a subsequent release.

The set of all documents describing the Siemens Product PKI is referred to under the OID 1.3.6.1.4.1.4329.99.1.2.

## 1.3 PKI Participants

See Central CP.

### 1.3.1 Certification Authorities

A graphical overview of the CA hierarchy is depicted in Figure 3: PPKI hierarchy for Infrastructure Certificates.

#### 1.3.1.1 Root CA

See Central CP.

#### 1.3.1.2 Intermediate CA

See Central CP.

#### 1.3.1.3 Issuing CAs

See Central CP.

### 1.3.2 Registration Authorities

See Central CP.

### 1.3.3 Subscribers

See Central CP.

### 1.3.4 Relying Parties

See Central CP.

### 1.3.5 Other Participants

#### 1.3.5.1 Subject (End-Entity)

See Central CP.

## 1.4 Certificate Usage

### 1.4.1 Appropriate Certificate Usage

See Central CP.

### 1.4.2 Prohibited Certificate Usage

See Central CP.

## 1.5 Policy Administration

### 1.5.1 Organization Administering the Document

The organization responsible for drafting, maintaining, and updating this CP is:

Siemens Aktiengesellschaft ("Siemens AG")

Technology (“T”) Research & Predevelopment 1 (“RPD1”)

Otto-Hahn-Ring 6, 81739 Munich, GERMANY

E-mail: contact.pki (at) siemens.com

Website: https://www.siemens.com/pki

### 1.5.2 Contact Person

Questions about this CP may be sent to:

Siemens AG

T RDA CST

Attn: Product PKI

Otto-Hahn-Ring 6, 81739 Munich, GERMANY

E-mail: contact.pki (at) siemens.com

Certificate Problem Reports shall be sent to: contact.pki (at) siemens.com

### 1.5.3 Person Determining CP and CPS Suitability for the Policy

The Policy Management Authority (Tenant PMA) in section 1.5.1 determines suitability of this document and the respective CPS.

### 1.5.4 CPS Approval Procedures

An annual risk assessment is carried out to evaluate business requirements and determine the security requirements to be included in the certificate policy for the stated community and applicability. In addition, the CP as well as the CPS will be reviewed every year regarding consistency with the actual PKI processes and services (see also section 8).

This document is accepted and approved by the Central PMA. Acceptance of the Siemens ACP process (which is part of the Siemens ISMS) constitutes acceptance of this document which therefore will not be explicitly signed. However, in case minor changes of this document will be necessary (see also 9.12.3), a new version will be published after release and official approval will be part of the next Siemens ACP process review.

## 1.6 Definitions and Acronyms

### 1.6.1 Definitions

| | |
|---|---|
| Authority Revocation List | Certificate Revocation List containing CA certificates. |
| CA certificate | Certificate for a Certification Authority's public key. |
| Central PMA | PMA that is responsible for the management and operation of the Central Product PKI Certificate Management service. |
| Central Product PKI System | Technical components of the Product PKI Certificate Management System that are managed and operated in the Siemens Trust Center facility. |
| Certificate Policy (CP) | Compare section 1.1. |
| Certification Authority (CA) | Authority, that is entitled to certify public keys; compare section 1.3.1. |
| Distinguished Name | Sequence of data-fields uniquely identifying e.g. the issuer and the Subject within a certificate or a CRL.<br>The format of a Distinguished Name is defined in the [X.520] standard. |
| EE certificate | See “End-Entity certificate”. |
| End-Entity | Equivalent to Subject;<br>the identity of the End-Entity is connected to the certificate and the related key-pair.<br>See also section 1.3.3. |
| End-Entity certificate | A digital certificate is used to prove ownership of a public key and the corresponding private key. It must not be used for certifying and issuing CRLs or other certificates. |
| End-User certificate | See “End-Entity certificate”. |
| HSM | Hardware Security Modul that can be used for random number generation and generation and storage of secret keys. The HSM can use the keys for digital signatures and for other PKI-applications. |
| Intermediate CA | Entity that issues and manages certificates of further Intermediate CAs or Issuing CAs and has a certificate signed by either a Root CA or by an Intermediate CA. |
| Issuing CA | Entity that issues and manages certificates of End Entities and has a certificate signed by either a Root CA or by an Intermediate CA. |
| Issuing CA System | Technical components (hardware and software) hosting Issuing and Intermediate CAs. |
| Multi-person Control | Sensitive activities typically are carried out by more than one person holding a trusted role. This is called Multi-person control. |
| Policy Management Authority | A body (of Siemens) that is responsible for setting, implementing and administering policy decisions regarding this CP and related documents and agreements in the Product PKI |
| Product PKI | Term used in this document for the Siemens Product PKI Certificate Management Service (due to ease of readability). |
| Product PKI System | Technical components (central and local) that are necessary to manage and operate the Product PKI Certificate Management System. |
| Qualified Auditor | Auditor who has appropriate knowledge in order to evaluate and assess and confirm the requirements and corresponding implementation of measures defined in the Certificate Policy documents and the Certification Practice Statements, respectively. |

| | |
|---|---|
| Registration Authority (RA) | PKI-incorporated facility for participant-authentication. See also section 1.3.2. |
| Relying Party | Individual or legal entity that uses certificates; see also section 1.3.5. |
| Root CA | Entity that issues and manages certificates of Intermediate or Issuing CAs (in case there do not exist Intermediate CAs). The certificate of the Root CA is self-signed. |
| Root CA System | Technical components (hardware and software) hosting Root and (optionally) Intermediate CAs. |
| Secure Device | A component (such as a Smart Card or HSM) that substantiated to protect the private key stored in that device. All cryptographic operations using the private key are performed inside this Secure Device. |
| Siemens Product PKI Certificate Management Service | Siemens internal organization that issues and manages certificates. This organization operates the Root CA System as well as the Issuing CA systems. |
| Smart Card | Integrated circuit card including a micro-processor that can be used for random number generation and generation and storage of secret keys. A Smart Card can use the keys for the generation of digital signatures and for other PKI-applications |
| Subject | End-Entity that uses the private End-Entity key (EE key). The End-Entity may differ from the Subscriber. |
| Subscriber | Subscriber for all certificates issued by the Product PKI is the respective Tenant as legal entity. See also section 1.3.3. |
| Tenant | Tenant can be every Siemens AG organizational unit or any other legal entity that has a contract in place that covers Product PKI services. The Tenants typically operate and maintain the Registration Authorities (e.g. within their production facilities or data center). In such a case the Tenants are responsible for RA operation and End-Entity authentication. |
| Tenant PMA | PMA that is responsible for the management and operation of the local Product PKI Certificate Management components such as RA and/or LRA as well as for identification of End-Entities. |
| Token | Transport-medium for certificates and keys |
| Trust Center | The term “Trust Center” refers to assets and components that are centrally operated and maintained at the Trust Center location as well to the respective processes. |
| Trusted Operator | Product PKI has the overall responsibility of issuing certificates to Subjects and managing and revoking certificates. Tenants delegate may delegate parts or these functions to the Central Product PKI Certificate Management Service or to other internal Service Providers of Siemens, which are called Trusted Operators |

### 1.6.2 Acronyms

| | |
|---|---|
| ARL | Authority Revocation List |
| CA | Certification Authority |
| CISO | Chief Information Security Officer |
| CMP | Certificate Management Protocol (RFC 4210) |
| CN | Common Name |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| DN | Distinguished Name |
| EE | End-Entity |
| FIPS | Federal Information Processing Standard |
| FQDN | Fully qualified domain name |
| HSM | Hardware Security Module |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IDevID | Initial Device Identifier (IEEE 802.1AR) |
| ISO | International Organization for Standardization |
| ISMS | Information Security Management System |
| LDevID | Locally significant Device Identifier (IEEE 802.1AR) |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PPKI | Product PKI |
| PMA | Policy Management Authority |
| RA | Registration Authority |
| RFC | Request for Comment |
| SLA | Service Level Agreement |
| URL | Uniform Resource Locator |
| UTF8 | Unicode Transformation Format-8 |

# 2 Publication and Repository Responsibilities

## 2.1 Repositories

Tenant specific Product PKI Repositories are operated by trusted service provider(s).

The repository responsibilities include:

1. accurately publishing information;
2. publishing the status of certificates;
3. promptness or frequency of publication; and
4. security of the repository and controlling access to information published on the repository to prevent unauthorized access and tampering.

Subjects and Relying Parties have access to:

- Certificate Revocation List (CRL)
- and OCSP responder

via: ppki-va.siemens.com .

## 2.2 Publication of Certification Information

The Tenant publishes certificate status information at ppki-va.siemens.com .

The CP is published on the website specified in section 1.5.1 Organization Administering the Document.

## 2.3 Time or Frequency of Publication

Updates to this CPS and the Central CPS are published in accordance with the definitions in section 9.12 of this document.

## 2.4 Access Controls on Repositories

Information published in the repository can be accessed with read-only access.

Administration of the published information shall be carried out only by trusted roles with adequate access control restrictions.

# 3 Identification and Authentication

## 3.1 Naming

### 3.1.1 Types of Names

The complete policy of specifying names and CA certificate profiles is documented for each certificate type in the respective Certificate Profile Documentation [PROF], which can be retrieved on request.

### 3.1.2 Need of 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 Certificate Profile Documentation [PROF].

### 3.1.3 Anonymity or Pseudonymity of Subscribers

#### 3.1.3.1 CA Names

See Central CP.

#### 3.1.3.2 End-Entity Names

See Central CP.

### 3.1.4 Rules for Interpreting Various Name Forms

See Central CP.

### 3.1.5 Uniqueness of Names

#### 3.1.5.1 CA Names

See Central CP.

#### 3.1.5.2 End-Entity Names

See Central CP.

### 3.1.6 Recognition, Authentication, and Roles of Trademarks

See Central CP.

## 3.2 Initial Identity Validation

See also Central CP.

### 3.2.1 Method to Prove Possession of Private Key

The key pairs are either generated by the corresponding issuing CA or by the End-Entity in case of automatic certificate update. In the latter case proof of private key possession is realized via state-of-the-art certificate management protocol, e.g. CMP.

### 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 Individual Identity

The individual identity of the corresponding (L)RA, or End-Entity, is determined within the onboarding process.

### 3.2.4 Non-verified Subscriber Information

See Central CP.

#### 3.2.5 Validation of Authority

The authority of the requester is checked as part of the onboarding process.

#### 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 central CP.

#### 3.3.2 Identification and Authentication for Re-Key After Revocation

Not supported.

## 3.4 Identification and Authentication for Revocation Requests

Revocation requests can be initialized either manually via MyIT portal or by the (L)RA. In the first case only requests from such persons listed in the onboarding checklist will be accepted. In the second case only revocation requests from a specific RA for its own keys are accepted.

# 4 Certificate Lifecycle Operational Requirements

## 4.1 Certificate Application

### 4.1.1 Who can submit a certificate application?

#### 4.1.1.1 Root and Intermediate CA

See Central CP.

#### 4.1.1.2 Issuing CAs

See Central CP.

#### 4.1.1.3 End-Entity Certificates

EE certificates (for examples, certificates used by RAs or by PPKI service internal components to authenticate against the central services) are generated as part of the onboarding process.

### 4.1.2 Enrollment Process and Responsibilities

#### 4.1.2.1 CA Certificates

See Central CP.

#### 4.1.2.2 End-Entity Certificate

The End-Entity certificate and the corresponding private key is generated by the central service. The private key material is securely transported via a PKCS#12 container.

## 4.2 Certificate Application Processing

### 4.2.1 Performing identification and authentication functions

Identity information is checked as part of the onboarding process.

### 4.2.2 Approval or Rejection of Certificate Applications

See Central CP and section 4.2.1.

### 4.2.3 Time to Process Certificate Applications

See Central CP.

## 4.3 Certificate Issuance

### 4.3.1 CA Actions during Certificate Issuance

See Central CP.

### 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The End-Entity (e.g., the operator of a BU RA), for which the subscriber has requested a certificate, is notified via email w.r.t. the status of certificate issuance. The initial key material as PKCS#12 container is securely sent via encrypted and signed email to the first technical contact listed in the onboarding check list. The passphrase for the PKCS12 container is sent via signed and encrypted email to the second technical contact listed in the onboarding checklist.

## 4.4 Certificate Acceptance

### 4.4.1 Conduct constituting certificate acceptance

See Central CP.

#### 4.4.2 Publication of the certificate by the CA

Relying parties of the Infrastructure CA are the BUs. Terms and conditions are made available to the relying parties as part of the ordering process.

#### 4.4.3 Notification of Certificate issuance by the CA to other entities

No stipulation.

## 4.5 Key Pair and Certificate Usage

See Central CP

#### 4.5.1 Subject Private Key and Certificate Usage

See Central CP.

#### 4.5.2 Relying Party Public Key and Certificate Usage

See Central CP.

## 4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to an entity without changing the public key or any other information in the certificate.

Not supported.

#### 4.6.1 Circumstance for Certificate Renewal

No stipulation.

#### 4.6.2 Who may request renewal?

No stipulation.

#### 4.6.3 Processing Certificate Renewal Request

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

"Re-key" addresses the generating of a new Key Pair and applying for the issuance of a new certificate and replacing the existing Key Pair.

#### 4.7.1 Circumstances for Certificate Re-key

See Central CP.

#### 4.7.2 Who may request certification of a new Public Key?

##### 4.7.2.1 Re-keying of an Issuing CA certificate

See Central CP.

#### 4.7.2.2 Re-keying of End-Entity certificates

The End-Entity, prior to the expiration of its certificate, will authenticate against the CA with its still valid certificate and initiate the issuance of a new certificate.

### 4.7.3 Processing Certificate Re-keying Requests

See section 4.3.1

### 4.7.4 Notification of new Certificate Issuance to Subscriber

See section 4.3.2

### 4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See section 4.4.1

### 4.7.6 Publication of the Re-keyed Certificate by the CA

See section 4.4.2

### 4.7.7 Notification of Certificate Issuance by the CA to other Entities

See section 4.4.3

## 4.8 Certificate Modification

Certificate modification means that the keys of a certificate remain unchanged, but more certificate information than for a certificate renewal is changed.

Not supported.

### 4.8.1 Circumstance for Certificate Modification

No stipulation.

### 4.8.2 Who may request Certificate modification?

No stipulation.

### 4.8.3 Processing Certificate Modification Requests

No stipulation.

### 4.8.4 Notification of new Certificate Issuance to Subscriber

No stipulation.

### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

### 4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## 4.9 Certificate Revocation and Suspension

### 4.9.1 Circumstances for Revocation

See Central CP.

### 4.9.2 Who can request revocation?

RA owners can request revocation of the EE certificates that have been issued for their RA.

#### 4.9.3 Procedure for Revocation Request

RA owners can request revocation of their EE certificates either manually by generating a ticket in MyIT or via the RA using CMP.

See also section 3.4.

#### 4.9.4 Revocation Request Grace Period

See Central CP.

#### 4.9.5 Time within which CA must Process the Revocation Request

See Central CP.

#### 4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties shall check the status of certificates on which they wish to rely by consulting the most recent CRL or using another applicable method.

#### 4.9.7 CRL Issuance Frequency

ARLs are regularly issued every 6 month or in exceptional cases when a specific CA certificate needs to be revoked.

CRLs are regularly issued once per day or in exceptional cases when a specific EE certificate needs to be revoked.

#### 4.9.8 Maximum Latency for CRLs

CRLs shall be posted to the repository within a reasonable time after generation.

#### 4.9.9 On-line Revocation/Status Checking Availability

Not supported.

#### 4.9.10 On-line Revocation Checking Requirements

No stipulation.

#### 4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

#### 4.9.12 Special Requirements for Private Key Compromise

Beside issuing a new ARL the RA owners will be informed via signed email.

If the RA operator has a reason to believe that there has been a compromise of an EE private key, then it shall notify the respective Issuing CA to take appropriate action, including request for revocation.

See also central CP for central service aspects.

#### 4.9.13 Circumstances for Suspension

Not supported.

#### 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 Services

#### 4.10.1 Operational Characteristics

See section 4.9.

### 4.10.2 Service Availability

The service to retrieve CRLs shall be available twenty-four (24) hours a day, seven (7) days a week, except in case of Force Majeure Events (CP section 9.16.5).

### 4.10.3 Optional Features

No stipulation.

## 4.11 End of Subscription

See Central CP.

## 4.12 Key Escrow and Recovery

Not supported.

### 4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

### 4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

# 5 Management, Operational, and Physical Controls

As this tenant for providing key material and certificates to securely connect RAs with the Central Product PKI service is operated as part of the Central PPKI service, all relevant requirements are set forth in the Central CP [CP].

## 5.1 Physical Security Controls

### 5.1.1 Site Location and Construction

See Central CPS [CCPS]

### 5.1.2 Physical Access

See Central CPS [CCPS].

### 5.1.3 Power and Air Conditioning

See Central CPS [CCPS].

### 5.1.4 Water Exposure

See Central CPS [CCPS].

### 5.1.5 Fire Prevention and Protection

See Central CPS [CCPS].

### 5.1.6 Media Storage

See Central CPS [CCPS].

### 5.1.7 Waste Disposal

See Central CPS [CCPS].

### 5.1.8 Off-site Backup

See Central CPS [CCPS].

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

See Central CPS [CCPS].

### 5.2.2 Numbers of Persons Required per Task

See Central CPS [CCPS].

### 5.2.3 Identification and Authentication for Each Role

See Central CPS [CCPS].

### 5.2.4 Roles Requiring Separation of Duties

See Central CPS [CCPS].

## 5.3 Personnel Controls

### 5.3.1 Qualifications, Experience and Clearance Requirements

See Central CPS [CCPS].

### 5.3.2 Background Check Procedures

See Central CPS [CCPS].

#### 5.3.3 Training Requirements

See Central CPS [CCPS].

#### 5.3.4 Retraining Frequency and Requirements

See Central CPS [CCPS].

#### 5.3.5 Job Rotation Frequency and Sequence

See Central CPS [CCPS].

#### 5.3.6 Sanctions for Unauthorized Actions

See Central CP.

#### 5.3.7 Independent Contractor Requirements

See Central CP.

#### 5.3.8 Documents Supplied to Personnel

See Central CP.

## 5.4 Audit Logging Procedures

#### 5.4.1 Types of Events Recorded

See Central CPS [CCPS].

#### 5.4.2 Frequency of Processing Log

See Central CP.

#### 5.4.3 Retention Period for Audit Log

See Central CPS [CCPS].

#### 5.4.4 Protection of Audit Log

See Central CPS [CCPS].

#### 5.4.5 Audit Log Backup Procedures

See Central CPS [CCPS].

#### 5.4.6 Audit Collection System (Internal vs. External)

See Central CPS [CCPS].

#### 5.4.7 Notification to Event-Causing Subject

See Central CP.

#### 5.4.8 Vulnerability Assessments

See Central CPS [CCPS].

## 5.5 Records Archival

#### 5.5.1 Types of Records Archived

CPS: See Central CPS [CCPS].

#### 5.5.2 Retention Period for Archived Audit Logging Information

See Central CPS [CCPS].

#### 5.5.3 Protection of Archive

See central CP.

See Central CPS [CCPS].

#### 5.5.4 Archive Backup Procedures

See Central CPS [CCPS].

#### 5.5.5 Requirements for Time-Stamping of Record

See Central CP.

#### 5.5.6 Archive Collection System (internal or external)

See Central CPS [CCPS].

#### 5.5.7 Procedures to Obtain and Verify Archived Information

See Central CP.

## 5.6 Key Changeover

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

For example, if a EE certificate is valid for 1 year, the issuing CA certificate for 5 years and the root CA certificate is valid for 20 years then the issuing CA should be renewed not later than 15 months before the expiration of its certificate. The root CA certificate should be renewed not later than 5.25 years before the expiration of its certificate.

## 5.7 Compromise and Disaster Recovery

#### 5.7.1 Incident and Compromise Handling Procedures

See Central CP.

#### 5.7.2 Corruption of Computing Resources, Software, and/or Data

See Central CP.

#### 5.7.3 Entity Private Key Compromise Procedures

See Central CP.

#### 5.7.4 Business Continuity Capabilities After a Disaster

See Central CP.

## 5.8 CA or RA Termination

See central CP.

# 6 Technical Security Controls

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key Pair Generation

Private keys for infrastructure certificates are created by used PKI software. In case of automated re-keying the private key is created by the End-Entity starting from the first re-key.

### 6.1.2 Private Key Delivery to Subscriber

The centrally generated private keys are securely distributed via signed and encrypted email within PKCS#12 containers to the first technical contact listed in the onboarding checklist. The corresponding passphrase for the PKCS#12 container is sent via signed and encrypted email to the second technical contact listed in the onboarding checklist.

The PKCS#12 container, together with its password, are deleted upon sending them to the tenants.

### 6.1.3 Public Key Delivery to Certificate Issuer

See Tenant specific CP [TCP].

### 6.1.4 CA Public Key Delivery to Relying Parties

Relying party is only the central PPKI service. The delivery of CA public keys is performed as part of the initial key event (set-up of issuing CA).

See also Central CP [CCP].

### 6.1.5 Key Sizes

See Central CP.

### 6.1.6 Public Key Parameters Generation and Quality Checking

See Central CP.

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

See Central CP.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic Module Standards and Controls

It is strongly recommended that end-entities securely store the private key (e.g. within a TPM if possible).

See also central CP for central service aspects.

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

4 eyes principle is applied for private keys of end entities (see 6.1.2 Private Key Delivery to Subscriber).

See also central CP for central service aspects.

### 6.2.3 Private Key Escrow

No supported.

### 6.2.4 Private Key Backup

See Central CP.

### 6.2.5 Private Key Archival

No stipulation.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

Not supported for End-Entity keys.

See also central CP for central service aspects.

#### 6.2.7 Private Key Storage on Cryptographic Module

End-Entity keys shall be stored in a security module if technically feasible.

See also central CP for central service aspects.

#### 6.2.8 Method of Activating Private Key

End-Entity private keys are automatically active after generation.

See also central CP for central service aspects.

#### 6.2.9 Method of Deactivating Private Key

Deactivating Private Keys is not supported.

#### 6.2.10 Method of Destroying Private Key

In case of resetting an End-Entity, the administrator in control of the End-Entity executes adequate measures to securely delete the formerly used private keys if possible.

See also central CP for central service aspects.

#### 6.2.11 Cryptographic Module Rating

See section 6.2.1.

## 6.3 Other Aspects of Key Pair Management

#### 6.3.1 Public key archival

Public key and related certificate shall be archived in accordance with Section 5.5.

#### 6.3.2 Certificate operational periods and key pair usage periods

The respective maximum validity periods for keys are:

| Certified Entity | Validity Period |
|---|---|
| **PPKI Infrastructure Root CA** | Up to two years |
| **PPKI Infrastructure Issuing CA** | Up to two years |
| **CMP certificate** | Up to one year |
| **TLS certificate** | Up to one year |

Table 1: Maximum validity periods

See also central CP.

## 6.4 Activation Data

#### 6.4.1 Activation Data Generation and Installation

Passphrase for PKCS#12 container is defined during the onboarding and securely delivered to the Tenant.

See also central CP for central service aspects.

#### 6.4.2 Activation Data Protection

See Central CP.

#### 6.4.3 Other Aspects of Activation Data

See Central CP.

## 6.5 Computer Security Controls

### 6.5.1 Specific Computer Security Technical Requirements

Specific computer security requirements for RAs are defined in [ISMS].

See also central CP for central service aspects.

### 6.5.2 Computer Security Rating

No stipulation.

## 6.6 Life Cycle Security Controls

### 6.6.1 System Development Controls

See Central CP.

### 6.6.2 Security Management Controls

RA security management controls shall follow regulations equivalent to Siemens ISMS [ISMS].

See also central CP for central service aspects.

### 6.6.3 Life Cycle Security Controls

See Central CP.

## 6.7 Network Security Controls

The (L)RA network security controls shall follow regulations equivalent to Siemens ISMS [ISMS].

See also central CP for central service aspects.

## 6.8 Time Stamp Process

See Central CP.

# 7 Certificate, CRL, and OCSP Profiles

## 7.1 Certificate Profile

Details of the tenant specific certificate profile can be found in [PROF].

See also central CP.

### 7.1.1 Version Number(s)

See Central CP.

### 7.1.2 Certificate Extensions

See Central CP.

### 7.1.3 Algorithm Object Identifiers

See Central CP.

### 7.1.4 Name Forms

See Central CP.

### 7.1.5 Name Constraints

No stipulation.

### 7.1.6 Certificate Policy Object Identifier

The Issuing CA certificates contain the “any policy” OID.

Following OIDs are included in the Subject certificates:

1.3.6.1.4.1.4329.38.1000.3.2

1.3.6.1.4.1.4329.99.1.2.0.1

### 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

Critical Certificate Policy extension shall conform to IETF RFC 5280 [RFC5280].

## 7.2 CRL Profile

### 7.2.1 Version number(s)

See Central CP.

### 7.2.2 CRL and CRL entry extensions

See Central CP.

## 7.3 OCSP Profile

### 7.3.1 Version Number(s)

See Central CP.

### 7.3.2 OCPS Extension

See Central CP.

# 8 Compliance Audit and Other Assessment

## 8.1 Frequency or Circumstances of Assessment

Compliance to this CP and the relevant CPSs shall be checked on a yearly basis. In addition, an bi-annual asset classification of the PKI components takes place. The asset classification is performed in accordance with the Siemens Enterprise Risk Management Process [ERM]. A possible outcome of either the audit or the asset classification is the adaption of the implemented security mechanisms and controls, which may result in changes in CP and CPSs.

## 8.2 Identity / Qualifications of Assessor

Compliance audits shall be performed by a qualified auditor.

See also central CP for central service aspects.

## 8.3 Assessor's Relationship to Assessed Entity

The assessor shall be organizationally independent from the assessed entity's operational authority.

See also central CP for central service aspects.

## 8.4 Topics Covered by Assessment

See Central CP.

## 8.5 Actions Taken as a Result of Deficiency

If a compliance audit or other assessments show deficiencies of the assessed entity, a determination of actions to be taken shall be made. This determination is made by Tenant PMA with input from the auditor/assessor. Tenant PMA is responsible for developing and implementing a corrective action plan.

If Tenant PMA determines that such deficiencies pose an immediate threat to the security or integrity of the Product PKI or the respective Tenant, a corrective action plan shall be developed in accordance with the incident response procedures described in section 5.7.1 within thirty (30) days and implemented within a commercially reasonable period of time, and a re-assessment is to be performed within thirty (30) days after completion of the corrective action. For less serious deficiencies, Tenant PMA shall evaluate the significance of such issues and determine the appropriate response.

Possible actions taken include but are not limited to:

- ❑ temporary suspension of operations until deficiencies are corrected
- ❑ revocation of certificates issued to the assessed entity
- ❑ changes in personnel
- ❑ triggering special investigations or more frequent subsequent compliance assessments, and
- ❑ claims for damages against the assessed entity

## 8.6 Communication of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, shall be provided to the Tenant PMA.

# 9 Other Business and Legal Matters

All business and legal matters will be regulated within specific contracts if necessary.

## 9.1 Fees

### 9.1.1 Certificate Issuance or Renewal fees

No stipulation.

### 9.1.2 Certificate Access fees

No stipulation.

### 9.1.3 Revocation or Status Information Access fees

No stipulation.

### 9.1.4 Fees for other Services

No stipulation.

### 9.1.5 Refund Policy

No stipulation.

## 9.2 Financial Responsibility

No stipulation.

### 9.2.1 Insurance Coverage

No stipulation.

### 9.2.2 Other Assets

No stipulation.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

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.

#### 9.5.1 Intellectual Property Rights in Certificates and Revocation Information

No stipulation.

#### 9.5.2 Intellectual Property Rights in CP

No stipulation.

#### 9.5.3 Intellectual Property Rights in Names

No stipulation.

#### 9.5.4 Property rights of Certificate Owners

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 of Liability

No stipulation.

## 9.9 Indemnities

No stipulation.

## 9.10 Term and Termination

### 9.10.1 Term

No stipulation.

### 9.10.2 Termination

No stipulation.

### 9.10.3 Effect of Termination and Survival

No stipulation.

## 9.11 Individual Notices and Communication with Participants

No stipulation.

## 9.12 Amendments

### 9.12.1 Procedure for Amendment

In the case of CP amendments, change procedures may include:

- a notification mechanism to provide notice of proposed amendments to affected Product PKI Participants
- a comment period; a mechanism by which comments are received, reviewed and incorporated into the document and
- a mechanism by which amendments become final and effective

### 9.12.2 Notification Mechanism and Period

A modification or amendment of the CP/CPS leads to a new version of the CP/CPS.

The new version of the CP/CPS will be published after its release on the website stated in section 1.5.1.

### 9.12.3 Circumstances under which OID must be changed

Changes, which will not materially reduce the assurance that the CP or its implementation provides and will be judged by the Policy Management Authority (CP section 1.5) to have an insignificant effect on the acceptability of certificates, do not require a change in the CP OID.

Changes, which will materially change the acceptability of certificates for specific purposes, may require corresponding changes to the CP OID.

## 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

No stipulation.

#### 9.16.1 Entire Agreement

No stipulation.

#### 9.16.2 Assignment

No stipulation.

#### 9.16.3 Severability

No stipulation.

#### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

#### 9.16.5 Force Majeure

Siemens shall be not held liable for violations of this CP due to causes that are reasonably beyond its control, including but not limited to, an event of Force Majeure, act of the authority, failure of equipment, failure of telecommunications lines, failure of internet access or any unforeseeable events.

## 9.17 Other Provisions

#### 9.17.1 Order of Precedence of CP

This CP provides baseline requirements that are applicable to all CAs operated in the name of the Tenant. In the event of a conflict between this CP and any other documents, the following documents shall be given precedence with the same order of the list:

For the scope of applicability for the Product PKI as defined in section 1.1:

1. Product PKI Central CP
2. Tenant CP that is applicable to a Tenant operated by the Product PKI [this document]
3. Documentation executed or expressly authorized by respective PMA

For the scope of applicability for the Tenant specific parts (in particular (L)RA operation and End-Entity authentication) as defined in section 1.1:

1. Tenant CP that is applicable to a Tenant operated by the Product PKI [this document]
2. Product PKI Central CP
3. Documentation executed or expressly authorized by respective PMA

# 10. References

In case of legitimate interest, Siemens internal regulations and guidelines as well as other internal documents can be retrieved on request.


[ACP] Asset Classification & Protection; https://intranet.siemens.com/acp

[CCP] Siemens Product PKI Certificate Management Service – Central Certificate Policy; Jan. 14, 2022, Version 1.8, www.siemens.com/pki.

[CCPS] Siemens Product PKI Certificate Management Service – Central Certification Practice Statement; Jan. 14, 2022, Version 1.2, www.siemens.com/pki.

[ECRYPT] ECRYPT-CSA; Algorithms, Key Size and Protocols Report; February 2018; https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

[ERM] Siemens Enterprise Risk Management; "Enterprise Risk Management – Integrated Framework"; https://intranet.for.siemens.com/cms/054/en/about/org/Pages/cf-a-erm-org.aspx and https://intranet.for.siemens.com/cms/080/de/processes/office/Pages/ric-ch-erm.aspx

[ETSI 401] ETSI EN 319 401; Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers; August 2017

[ETSI 411] ETSI EN 319 411-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements; August 2017

[FIPS] National Institute of Standards and Technology; SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES; May 2001; https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[IEEE802.1AR] IEEE 802.1AR; IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity; June 2018; https://standards.ieee.org/standard/802_1AR-2018.html

[IHP] The Siemens Incident Handling process as part of the ISMS; https://www.cert.siemens.com/incident-response/process/

[ISMS] SFeRA - Security Framework and Regulations Application; https://webapps.siemens.com/sfera

[ISO27001] ISO/IEC 27001; Information technology — Security techniques — Information security management systems — Requirements; October 2013

[NIST] Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5 (Draft), NIST, 10/2019; https://www.nist.gov/news-events/news/2019/10/recommendation-key-management-part-1-general-draft-nist-sp-800-57-part-1

[PROF] Certificate Profile Naming Convention for Infrastructure Certificates, https://wiki.ct.siemens.de/display/ProductPKI/PPKI+Naming+Conventions

[RFC2119] IETF; RFC 2119; Key words for use in RFCs to Indicate Requirement Levels; March 1997.

[RFC3647] IETF; RFC 3647; Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework; November 2003.

[RFC5280] IETF; RFC 3647; Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; May 2008; https://tools.ietf.org/html/rfc5280

[TCP] Tenant CP, IT_Infrastructure_Certificates__CP_v1.0

[TÜV] TÜV IT; Sichere Infrastrukturen für IT-Systeme – Trusted Site Infrastructure; Version 4.0; https://www.tuvit.de/fileadmin/user_upload/TUEViT_TSI_V4_0.pdf

[X.520] ITU-T; X520 Information technology – Open Systems Interconnection – The Directory: Selected attribute type