Siemens AG

Siemens
Product PKI Certificate Management Service – Central Certification Practice Statement

Document History

Version	Date	Author	Change Comment
1.0	Dec. 23, 2020	Michael Munzert Antonio Vaira	First released version
1.1	July 20, 2021	Michael Munzert	Editorial changes
1.2	Jan. 14, 2022	Michael Munzert Antonio Vaira	Reference for Central CP updated

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.

Scope and Applicability

This document constitutes the Central Certification Practice Statement (CPS) for the Siemens Product PKI. It details how the requirements documented in the Central Certificate Policy [CCP] are implemented. The purpose of this document is to publicly disclose to interested parties the business policies and practices under which the Siemens Product PKI operates.

The senior management of the Product PKI ensures that the certification practices established to meet the requirements specified in the Central Certificate Policy [CCP] 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 in document history.		
Checked by	Stenger, Meiko Kuechler, Markus	Siemens LC Siemens IT	May, 2020 Jan, 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

See Central Certificate Policy [CCP].

1.1.1 PKI hierarchy

See Central Certificate Policy [CCP].

1.2 Document Name and Identification

This CPS is referred to as the ‘Central Certification Practice Statement’.

Title: Siemens Product PKI Certificate Management Service – Central Certification Practice Statement

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

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

1.3 PKI Participants

See Central Certificate Policy [CCP].

1.3.1 Certification Authorities

Specified in the Central Certificate Policy [CCP].

1.3.2 Registration Authorities

Specified in the Central Certificate Policy [CCP].

1.3.3 Subscribers

Specified in the Central Certificate Policy [CCP].

1.3.4 Relying Parties

Specified in the Central Certificate Policy [CCP].

1.3.5 Other Participants

Specified in the Central Certificate Policy [CCP].

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

Specified in the Central Certificate Policy [CCP].

1.4.2 Prohibited Certificate Usage

Specified in the Central Certificate Policy [CCP].

1.5 Policy Administration

1.5.1 Organization Administering the Document

Specified in the Central Certificate Policy [CCP].

1.5.2 Contact Person

Specified in the Central Certificate Policy [CCP].

1.5.3 Person Determining CP and CPS Suitability for the Policy

Specified in the Central Certificate Policy [CCP].

1.5.4 CPS Approval Procedures

Specified in the Central Certificate Policy [CCP].

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	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements [RFC3647].
Certification Authority	Authority, that is entitled to certify public keys; compare section 1.3.1.
Certification Practice Statement	A statement of the practices which a certification authority employs in issuing certificates [RFC3647].
Distinguished Name	Sequence of data-fields uniquely identifying e.g. the issuer and the Subject within a certificate or a CRL. The format of a Distinguished Name is defined in the [X.520] standard.
EE certificate	See “End-Entity certificate”.
End-Entity	Equivalent to Subject; the identity of the End Entity is connected to the certificate and the related key-pair. 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 CAs are operated on behalf of a Tenant by a Trusted Operator whereas Tenants their self 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 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

See Tenant CP.

2.2 Publication of Certification Information

See Tenant CP.

2.3 Time or Frequency of Publication

Specified in the Central Certificate Policy [CCP].

2.4 Access Controls on Repositories

Specified in the Central Certificate Policy [CCP].

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Specified in the Central Certificate Policy [CCP].

3.1.2 Need of Names to be Meaningful

3.1.2.1 CA Names

See Tenant CP.

3.1.2.2 End Entity Names

See Tenant CP.

3.1.3 Anonymity or Pseudonymity of Subscribers

3.1.3.1 CA Names

Specified in the Central Certificate Policy [CCP].

3.1.3.2 End Entity Names

Specified in the Central Certificate Policy [CCP].

3.1.4 Rules for Interpreting Various Name Forms

Specified in the Central Certificate Policy [CCP].

3.1.5 Uniqueness of Names

Specified in the Central Certificate Policy [CCP].

3.1.6 Recognition, Authentication, and Roles of Trademarks

Specified in the Central Certificate Policy [CCP].

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organization Identity

The authentication of the organization identity is part of a defined onboarding process in which (among others) also the identity of the organization as well as of the persons requesting the onboarding will be verified using digital signatures as well as the companywide services Siemens Corporate directory (SCD) and Siemens Corporate Organization (SCO).

3.2.3 Authentication of Individual Identity

See Tenant CPS.

3.2.4 Non-verified Subscriber Information

Specified in the Central Certificate Policy [CCP].

3.2.5 Validation of Authority

See Tenant CPS.

3.2.6 Criteria for Interoperation

Specified in the Central Certificate Policy [CCP].

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Specified in the Central Certificate Policy [CCP].

3.3.2 Identification and Authentication for Re-Key After Revocation

Not supported.

3.4 Identification and Authentication for Revocation Requests

Revocation of Intermediate CA and Issuing CA certificates can be submitted digitally signed by the Tenant PMA.

Revocation requests for EE certificates require either a digitally signed request (via CMP) by an authorized RA or can be submitted digitally signed by the contract owner (or from the line manager of the contract owner) or the technical contact e.g. via signed email.

Details how to request certificate revocation by relying parties are specified in the Tenant CPS.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

As part of an onboarding process a checklist must be provided and (digitally) signed by the requesting organization.

This checklist includes (but is not limited to)

- PKI hierarchy that needs to be set up
- Certificate profiles for CA and EE Certificates
- Named persons that are authorized to represent the Tenant.

These named persons are later allowed to request changes in the configuration of issuing CAs.

During regular operations, only authorized RAs will be accepted for submitting certificate applications. For example, if CMP is used as enrolment protocol, the Issuing CA will accept only certification requests for EE certificates that are signed by the RA with the correct CMP signer certificate and are sent via the correct mutual authenticated TLS channel.

4.1.2 Enrollment Process and Responsibilities

Based on the checklist (see section 4.1.1) the Root CA, Sub-ordinated CA(s) (if specified in the checklist) and Issuing CA(s) are securely generated as part of a ceremony under at least dual control. Beside two administrators of the trusted service provider, also persons representing the Tenant might participate in that ceremony. All steps are documented and later signed by the persons that performed the ceremony.

As part of the onboarding, credentials required for the communication between RA and CA will be securely generated and distributed. For example, if CMP will be used as enrolment protocol, as part of the onboarding process, CMP and TLS certificates for the Tenant RA(s) are generated which are securely transferred to the Tenant. The keys are securely transmitted (e.g. PKSC#12 container) to one named person (technical contact one from checklist). The credentials to access the keys are send to a different named person (technical contact two from checklist). For further enrolment protocols, like EST or ACME, protocol specific means will be used to authorize certification requests.

Processes and responsibilities for enrolment of EE certificates are described in the Tenant CPS.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

Before the ceremony for setting up the PKI hierarchy takes place, the signed checklist (see section 4.1.1) will be checked by the trusted service operator thereby guaranteeing that only allowed parties will be “onboarded”.

Identification and authentication of end entities is performed by the Tenant (see Tenant CPS).

Only authorized certification requests for EE certificates are accepted. For example, if CMP is used as enrolment protocol, certification requests for EE certificates that are signed by the correct CMP signer certificate and are sent via the correct mutual authenticated TLS channel are accepted. If other enrolment protocols, such as EST or ACME, respective protocol specific means will be applied to identify and authenticate certification requests.

4.2.2 Approval or Rejection of Certificate Applications

The requester is informed about approval or rejection via, either protocol specific means, e.g. CMP or via organizational means, e.g. communication via email.

Only requests conforming to the respective certificate profile will be processed by the issuing CA.

4.2.3 Time to Process Certificate Applications

Officially ordered and complete application requests for a new Tenant will be checked and performed within 10 weeks.

Requests for EE certificates will be executed immediately (typically within five seconds).

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The Issuing CA informs the (subscriber's) RA via the used certificate management protocol.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

CA certificate acceptance is constituted as result of the CA Creation Ceremony, which is performed at least under dual control.

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

Specified in the Central Certificate Policy [CCP].

4.5.1 Subject Private Key and Certificate Usage

Specified in the Central Certificate Policy [CCP].

4.5.2 Relying Party Public Key and Certificate Usage

Specified in the Central Certificate Policy [CCP].

4.6 Certificate Renewal

Unless otherwise stated in the Tenant CP, certificate renewal is not supported.

4.6.1 Circumstance for Certificate Renewal

Not supported unless otherwise stated in the Tenant CP.

4.6.2 Who may request renewal?

Not supported unless otherwise stated in the Tenant CP.

4.6.3 Processing Certificate Renewal Request

Not supported unless otherwise stated in the Tenant CP.

4.6.4 Notification of new Certificate Issuance to Subscriber

Not supported unless otherwise stated in the Tenant CP.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not supported unless otherwise stated in the Tenant CP.

4.6.6 Publication of the Renewal Certificate by the CA

Not supported unless otherwise stated in the Tenant CP.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

Not supported unless otherwise stated in the Tenant CP.

4.7 Certificate Re-key

4.7.1 Circumstances for Certificate Re-key

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

4.7.2 Who may request certification of a new Public Key?

4.7.2.1 Re-keying of an Issuing CA certificate

Re-keying of Issuing CA certificates is not supported.

4.7.2.2 Re-keying of End Entity certificates

For re-keying of EE certificates, the same requirements apply as for certificate Issuance (see section 4.2).

4.7.3 Processing Certificate Re-keying Requests

See section 4.2.

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

Unless otherwise stated in the Tenant CP, certificate modification is not supported.

4.8.1 Circumstance for Certificate Modification

Not supported unless otherwise stated in the Tenant CP.

4.8.2 Who may request Certificate modification?

Not supported unless otherwise stated in the Tenant CP.

4.8.3 Processing Certificate Modification Requests

Not supported unless otherwise stated in the Tenant CP.

4.8.4 Notification of new Certificate Issuance to Subscriber

Not supported unless otherwise stated in the Tenant CP.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not supported unless otherwise stated in the Tenant CP.

4.8.6 Publication of the Modified Certificate by the CA

Not supported unless otherwise stated in the Tenant CP.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not supported unless otherwise stated in the Tenant CP.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Specified in the Central Certificate Policy [CCP].

4.9.2 Who can request revocation?

Specified in the Central Certificate Policy [CCP] and in the respective Tenant Certificate Policy.

4.9.3 Procedure for Revocation Request

The procedure for revocation of EE certificates is described in the Tenant CPS.

Only authorized revocation requests are executed by Siemens PPKI. Such requests either need to be signed by the authorized persons specified in the checklist, or they can be sent by the authorized RA using a secure certificate management protocol.

Revocation of CA certificates is performed in two steps. (1) The impacted issued EE certificates are revoked by creating a long lasting CRL which includes the impacted EE certificates. (2) An ARL with the respective CA certificate is created.

More details as well as revocation of Root CA certificates are described in the Tenant CPS.

4.9.4 Revocation Request Grace Period

Specified in the Central Certificate Policy [CCP].

4.9.5 Time within which CA must Process the Revocation Request

In case of legitimate interest Siemens PPKI will revoke certificates without any delay. In case a CMP request is submitted by an authorized RA the revocation request will be carried out automatically. In case of a signed request, performed by the authorized person, it will be carried out within the time period specified in the Service Level Agreement [SLA].

4.9.6 Revocation Checking Requirement for Relying Parties

See Tenant CPS.

4.9.7 CRL Issuance Frequency

See Tenant CPS.

4.9.8 Maximum Latency for CRLs

See Tenant CPS.

4.9.9 On-line Revocation/Status Checking Availability

See Tenant CPS.

4.9.10 On-line Revocation Checking Requirements

See Tenant CPS.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements for Private Key Compromise

In case private key compromise of CA keys or of keys used for authentication is suspected, the Siemens Incident Handling process is started and the affected Tenant (contact persons listed in the Checklist) will be informed via signed email.

4.9.13 Circumstances for Suspension

Not supported.

4.9.14 Who can request suspension?

Not supported.

4.9.15 Procedure for suspension request

Not supported.

4.9.16 Limits on suspension period

Not supported.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

See section 4.9.

4.10.2 Service Availability

See [SLA].

4.10.3 Optional Features

See Tenant CP.

4.11 End of Subscription

See Central Certificate Policy [CCP].

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

5.1 Physical Security Controls

5.1.1 Site Location and Construction

For centrally operated and managed components see Central Certificate Policy [CCP].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.1.2 Physical Access

For centrally operated and managed components see Central Certificate Policy [CCP]. Additional details are described in the Asset Handling Concept [AHC].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.1.3 Power and Air Conditioning

For centrally operated and managed components see Central Certificate Policy [CCP].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.1.4 Water Exposure

For centrally operated and managed components see Central Certificate Policy [CCP].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.1.5 Fire Prevention and Protection

For centrally operated and managed components see Central Certificate Policy [CCP].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.1.6 Media Storage

For centrally operated and managed components see Central Certificate Policy [CCP]. Additional details are described in the Asset Handling Concept [AHC].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.1.7 Waste Disposal

For centrally operated and managed components see Central Certificate Policy [CCP].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.1.8 Off-site Backup

For centrally operated and managed components see Central Certificate Policy [CCP]. Additional details are described in the Asset Handling Concept [AHC].

Controls implemented on components under Tenant responsibility are specified in the respective Tenant CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

For centrally operated and managed components see Central Certificate Policy [CCP]. Additional details are described in the Asset Handling Concept [AHC].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.2.2 Numbers of Persons Required per Task

At least two persons are required to perform the following trusted role activities (dual control):

- Access to the high-security facilities of the Siemens Trust Center;
- Logical and physical access to HSMs;
- Logical and physical access to data archive, and

- Logical and physical access to central, sensitive or critical systems of Siemens Root CA and its backup systems.

Additional details are described in the Asset Handling Concept [AHC].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.2.3 Identification and Authentication for Each Role

Identification and Authentication of persons to sensitive areas relies on multi-factor-authentication.

Access to critical systems is granted only to trusted roles that authenticate with unique credentials stored on smartcards. Role-based authorization of the users is enforced, in control systems.

Additional details are described in the Asset Handling Concept [AHC].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Specified in the Central Certificate Policy [CCP].

Additional details are described in the Asset Handling Concept [AHC].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.3.2 Background Check Procedures

Specified in the Central Certificate Policy [CCP].

Controls implemented on component under Tenant responsibility are specified in the respective Tenant CPS.

5.3.3 Training Requirements

All personnel performing management activities, with respect to the operation of the Product PKI, receive comprehensive training in:

- security principles and mechanisms;
- security awareness;
- all software versions in use;
- all duties they are expected to perform, and
- disaster recovery and business continuity procedures.

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

5.3.4 Retraining Frequency and Requirements

Personnel in Trusted Operator roles receive annual refresher training and updates to the extent required to ensure maintenance of the required level of proficiency to perform their job responsibilities competently and satisfactorily. Data security and data privacy protection training is provided on an ongoing basis.

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of information security and data privacy protection policies and procedures that are commensurate with the frequency and severity of the unauthorized actions. Disciplinary actions that are taken including measures up to employment termination.

5.3.7 Independent Contractor Requirements

Specified in the Central Certificate Policy [CCP].

5.3.8 Documents Supplied to Personnel

Specified in the Central Certificate Policy [CCP].

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Specified in the Central Certificate Policy [CCP].

5.4.2 Frequency of Processing Log

Specified in the Central Certificate Policy [CCP].

5.4.3 Retention Period for Audit Log

Specified in the Central Certificate Policy [CCP].

5.4.4 Protection of Audit Log

Automatically created audit logs are integrity protected applying digital signatures at creation time. Access to audit logs is only granted for authorized roles.

5.4.5 Audit Log Backup Procedures

Specified in the Central Certificate Policy [CCP].

5.4.6 Audit Collection System (Internal vs. External)

Audit logs are securely stored as part of the backup procedure, that is performed daily.

5.4.7 Notification to Event-Causing Subject

Specified in the Central Certificate Policy [CCP].

5.4.8 Vulnerability Assessments

Specified in the Central Certificate Policy [CCP].

5.5 Records Archival

5.5.1 Types of Records Archived

Specified in the Central Certificate Policy [CCP].

5.5.2 Retention Period for Archived Audit Logging Information

Specified in the Central Certificate Policy [CCP].

5.5.3 Protection of Archive

Specified in the Central Certificate Policy [CCP].

5.5.4 Archive Backup Procedures

Specified in the Central Certificate Policy [CCP].

5.5.5 Requirements for Time-Stamping of Record

Specified in the Central Certificate Policy [CCP].

5.5.6 Archive Collection System (internal or external)

Specified in the Central Certificate Policy [CCP].

5.5.7 Procedures to Obtain and Verify Archived Information

Specified in the Central Certificate Policy [CCP].

5.6 Key Changeover

See Central Certificate Policy [CCP].

5.7 Compromise and Disaster Recovery

Compromise and Disaster Recovery is described in [DRP].

5.7.1 Incident and Compromise Handling Procedures

See section 5.7.

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

See section 5.7.

5.7.3 Entity Private Key Compromise Procedures

Specified in the Central Certificate Policy [CCP].

5.7.4 Business Continuity Capabilities After a Disaster

See section 5.7.

5.8 CA or RA Termination

Specified in the Central Certificate Policy [CCP].

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Critical key pairs, such as the key pairs of the Root CAs, Intermediate CAs and Issuing CAs, are generated with a hardware security module ("HSM"), which is certified in accordance with FIPS 140-2 level 3.

The key material, for protecting the infrastructure, e.g.:

- TLS servers (CMP gateway, CA web interfaced for administrating purposes, etc.),
- TLS clients (e.g. RAs),
- CMP clients (e.g. RAs),

is generated in the CA system for the initial enrolment and the manual enrolments.

Subsequent renewals procedures are described in the Tenant CPS.

6.1.2 Private Key Delivery to Subscriber

See Central Certificate Policy [CCP] for private key delivery for CA and RA keys.

See Tenant CPS for private key delivery for end entities.

6.1.3 Public Key Delivery to Certificate Issuer

The public key is transmitted from the RA to the CA within the secure certificate management protocol applied, for example using signed CMP messages.

6.1.4 CA Public Key Delivery to Relying Parties

See Tenant CPS.

6.1.5 Key Sizes

Algorithms, parameters, and key lengths are defined in the respective Tenant CP.

6.1.6 Public Key Parameters Generation and Quality Checking

Keys, if applicable, are validated by the CA and are checked against a blacklist of weak keys.

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

See Central Certificate Policy [CCP].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The Cryptographic Module (HSM) used to operate the Product PKI CA is certified according to FIPS 140-2 level 3. The HSMs are hosted in the Siemens Trust Center, they are additionally shielded against electromagnetic radiation, and they are accessed and operated only by named trusted roles.

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

Technical and procedural mechanisms that require the participation of multiple trusted employees to perform sensitive Root CA cryptographic operations are implemented. In order to gain access to the Private Keys, 2 persons holding a trusted role are required. No single person has all the activation data needed for accessing any of the Siemens CA Private Keys.

6.2.3 Private Key Escrow

Private Key Escrow is not being performed for Root and Issuing CAs.

6.2.4 Private Key Backup

Siemens Root CA´s Private Key will be backed up and securely stored, at separate sites, for the unlikely event of key loss, for example, due to hardware failure. Key backup will occur as part of CA key generation ceremony. Backed up CA Private Key remains secret and their integrity and authenticity is retained.

6.2.5 Private Key Archival

See Central Certificate Policy [CCP].

6.2.6 Private Key Transfer into or from a Cryptographic Module

Siemens Root and Issuing CA´s Key Pairs are generated in the HSM modules in which the keys will be used.

6.2.7 Private Key Storage on Cryptographic Module

Root and Issuing CA´s Private Keys are held in HSMs in encrypted form and backed up in encrypted files that can be restored only under dual control. In addition, the private keys are marked as not extractable, which prevents the export of these keys and they can "only" be used on the HSM.

6.2.8 Method of Activating Private Key

Root and Issuing CA´s Private Key are already active at creation time, see section 6.2.2.

6.2.9 Method of Deactivating Private Key

Deactivating Private Keys is not supported.

6.2.10 Method of Destroying Private Key

CA private keys are stored as defined in 6.2.7. Their destruction (in case they are no longer needed) requires the participation of 2 persons holding trusted roles. When performed, the destruction process is documented.

In case End Entity private keys are no longer needed, the corresponding certificate will be revoked.

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

CA Public Keys are backed up and archived as part of the routine backup procedures.

6.3.2 Certificate operational periods and key pair usage periods

See Central Certificate Policy [CCP].

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation date generation and installation takes place as part of the process of creation of the Root and Issuing CA's Private Keys. See section 6.2.

6.4.2 Activation Data Protection

See section 6.4.1.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

All PPKI computers are subject to constant monitoring. Monitoring results are available 24 hours, 7 days a week.

The configuration of system components may only be performed under dual control by operators who have identified with two-factor-authentication.

6.5.2 Computer Security Rating

See Central Certificate Policy [CCP].

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

Product PKI software is developed and maintained by a best-in-bread PKI SW vendor.

This vendor has been chosen as result of a vendor selection process, where trustworthiness of the supplier was one of main selection criteria.

Furthermore, the used software has been pen-tested by independent Siemens pen-testers.

6.6.2 Security Management Controls

See Central Certificate Policy [CCP].

6.6.3 Life Cycle Security Controls

All security management controls are annually audited. Any shortcomings will be reported to the PMA, which will trigger adequate follow-up activities.

6.7 Network Security Controls

The Root CAs are maintained off-line and are not networked with any external components.

A complete documentation of the network is available and can be retrieved upon request to the PMA.

Penetration tests are performed annually. Corresponding findings will be communicated to the PMA and corresponding action plan will be defined to mitigate these findings.

6.8 Time Stamp Process

Logfiles contain an embedded time stamp. CA event protocols are being signed and time stamped.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The certificate profiles are defined during the onboarding process. Peer-review ensures that certificate profiles comply with the requirements set forth in the Central Certificate Policy [CCP].

7.1.1 Version Number(s)

See Central Certificate Policy [CCP].

7.1.2 Certificate Extensions

See Central Certificate Policy [CCP].

7.1.3 Algorithm Object Identifiers

See Central Certificate Policy [CCP].

7.1.4 Name Forms

See Central Certificate Policy [CCP].

7.1.5 Name Constraints

See Central Certificate Policy [CCP].

7.1.6 Certificate Policy Object Identifier

See Central Certificate Policy [CCP].

7.1.7 Usage of Policy Constraints Extension

See Central Certificate Policy [CCP].

7.1.8 Policy Qualifiers Syntax and Semantics

See Central Certificate Policy [CCP].

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

See Central Certificate Policy [CCP].

7.2 CRL Profile

7.2.1 Version number(s)

See Central Certificate Policy [CCP].

7.2.2 CRL and CRL entry extensions

See Central Certificate Policy [CCP].

7.3 OCSP Profile

7.3.1 Version Number(s)

See Central Certificate Policy [CCP].

7.3.2 OCPS Extension

See Central Certificate Policy [CCP].

8 Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Assessment

See Central Certificate Policy [CCP].

8.2 Identity / Qualifications of Assessor

See Central Certificate Policy [CCP].

8.3 Assessor's Relationship to Assessed Entity

The assessment is performed by an independent organization.

8.4 Topics Covered by Assessment

See Central Certificate Policy [CCP].

8.5 Actions Taken as a Result of Deficiency

See Central Certificate Policy [CCP].

8.6 Communication of Results

See Central Certificate Policy [CCP].

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal fees

See Central Certificate Policy [CCP].

9.1.2 Certificate Access fees

See Central Certificate Policy [CCP].

9.1.3 Revocation or Status Information Access fees

See Central Certificate Policy [CCP].

9.1.4 Fees for other Services

See Central Certificate Policy [CCP].

9.1.5 Refund Policy

See Central Certificate Policy [CCP].

9.2 Financial Responsibility

See Central Certificate Policy [CCP].

9.2.1 Insurance Coverage

See Central Certificate Policy [CCP].

9.2.2 Other Assets

See Central Certificate Policy [CCP].

9.2.3 Insurance or Warranty Coverage for End-Entities

See Central Certificate Policy [CCP].

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

See Central Certificate Policy [CCP].

9.3.2 Information not within the Scope of Confidential Information

See Central Certificate Policy [CCP].

9.3.3 Responsibility to Protect Confidential Information

See Central Certificate Policy [CCP].

9.4 Privacy of Personal Information

9.4.1 Privacy plan

See Central Certificate Policy [CCP].

9.4.2 Information treated as private

See Central Certificate Policy [CCP].

9.4.3 Information not deemed private

See Central Certificate Policy [CCP].

9.4.4 Responsibility to protect private information

See Central Certificate Policy [CCP].

9.4.5 Notice and consent to use private information

See Central Certificate Policy [CCP].

9.4.6 Disclosure pursuant to judicial or administrative process

See Central Certificate Policy [CCP].

9.4.7 Other information disclosure circumstances

See Central Certificate Policy [CCP].

9.5 Intellectual Property Rights

9.5.1 Intellectual Property Rights in Certificates and Revocation Information

See Central Certificate Policy [CCP].

9.5.2 Intellectual Property Rights in CP

See Central Certificate Policy [CCP].

9.5.3 Intellectual Property Rights in Names

See Central Certificate Policy [CCP].

9.5.4 Property rights of Certificate Owners

See Central Certificate Policy [CCP].

9.6 Representations and Warranties

9.6.1 CA representations and warranties

See Central Certificate Policy [CCP].

9.6.2 RA representations and warranties

See Tenant CP.

9.6.3 Subscriber representations and warranties

See Central Certificate Policy [CCP].

9.6.4 Relying party representations and warranties

See Central Certificate Policy [CCP].

9.6.5 Representations and warranties of other participants

See Central Certificate Policy [CCP].

9.7 Disclaimers of Warranties

See Central Certificate Policy [CCP].

9.8 Limitations of Liability

See Central Certificate Policy [CCP].

9.9 Indemnities

See Central Certificate Policy [CCP].

9.10 Term and Termination

9.10.1 Term

See Central Certificate Policy [CCP].

9.10.2 Termination

See Central Certificate Policy [CCP].

9.10.3 Effect of Termination and Survival

See Central Certificate Policy [CCP].

9.11 Individual Notices and Communication with Participants

See Central Certificate Policy [CCP].

9.12 Amendments

9.12.1 Procedure for Amendment

See Central Certificate Policy [CCP].

9.12.2 Notification Mechanism and Period

See Central Certificate Policy [CCP].

9.12.3 Circumstances under which OID must be changed

See Central Certificate Policy [CCP].

9.13 Dispute Resolution Provisions

See Central Certificate Policy [CCP].

9.14 Governing Law

See Central Certificate Policy [CCP].

9.15 Compliance with Applicable Law

See Central Certificate Policy [CCP].

9.16 Miscellaneous Provisions

See Central Certificate Policy [CCP].

9.16.1 Entire Agreement

See Central Certificate Policy [CCP].

9.16.2 Assignment

See Central Certificate Policy [CCP].

9.16.3 Severability

See Central Certificate Policy [CCP].

9.16.4 Enforcement (attorneys' fees and waiver of rights)

See Central Certificate Policy [CCP].

9.16.5 Force Majeure

See Central Certificate Policy [CCP].

9.17 Other Provisions

9.17.1 Order of Precedence of CP

See Central Certificate Policy [CCP].

10. References

[AHC] Asset Handling Concept

[CCP] Siemens Product PKI Certificate Management Service – Central Certificate Policy; Version 1.7; July. 20, 2021.

[DRP] Disaster and Recovery Plan (Notfall Handbuch PKI Services).

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

[FIPS] National Institute of Standards and Technology; SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES; May 25, 2001; https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

[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

[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; Nov. 2003.

[RFC5280] IETF; RFC 5280; Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; May 2008.

[RFC8174] IETF; RFC 8174; Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words; May 2017.

[SLA] SLA Product PKI - Service Level Agreement, v3.0, May 25, 2020.

[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