Siemens AG

Siemens
Product PKI Certificate Management Service – Central Certificate Policy

Document History

Version	Date	Author	Change Comment
1.0	June 6, 2020	Michael Munzert Antonio Vaira	First released version
1.1	Oct. 1, 2020	Michael Munzert	Adaption to new organization naming
1.2	Oct.19, 2020	Michael Munzert	Glossary and References adapted
1.3	Dec. 12, 2020	Michael Munzert	Comments from IT incorporated
1.4	Dec, 23, 2020	Michael Munzert	Final Comments incorporated
1.5	Feb. 9, 2021	Michael Munzert	Adaption of approval process (linkage with ACP process)
1.6	March 12, 2021	Michael Munzert	Minor editorial changes
1.7	July 20, 2021	Michael Munzert	Editorial changes
1.8	Jan. 14, 2022	Michael Munzert Antonio Vaira	First published version
1.9	October 11, 2022	Michael Munzert Antonio Vaira	New responsible for document authorization

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 Certificate Policy (CP) for the central parts of the Siemens Certificate Management Service, in the following called "Product PKI". The Product PKI is responsible for the operation of the Root CAs as well as for the CAs. Together with the Tenant specific Central CP it 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 Kuechler, Markus	Siemens LC Siemens IT	May, 2020 Jan, 2022
Authorization	Dr.Kind, Andreas	Head of Siemens T CST.	Oct., 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 Certificate Policy of the Siemens Product PKI Certificate Management Service (in the following called “Product PKI”).

It describes the services provided by the Product PKI as well as binding requirements that must be fulfilled by Product PKI participants. Moreover - together with the CPSs - it also defines 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” also called “Manufacturer Device Certificates” as well as "LDevID certificates" also called "Operational Certificates") that are stored on and used by Siemens products and solutions. The certificates might be used in bootstrapping or other operational scenarios for authentication purposes. Or the certificates might be used to proof that a 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.

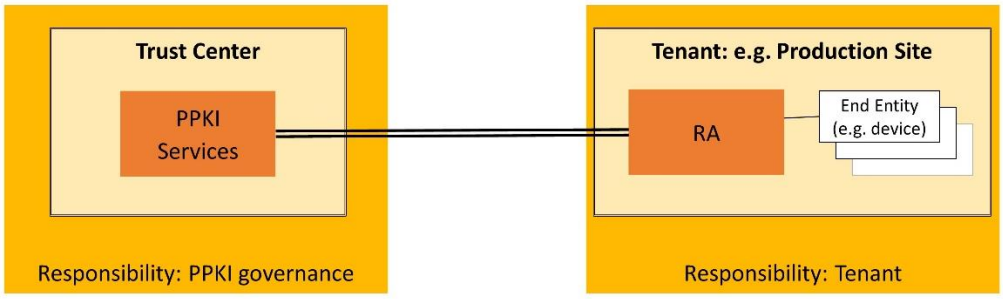

Figure 1: Stakeholders and typical responsibility split

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

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.

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:

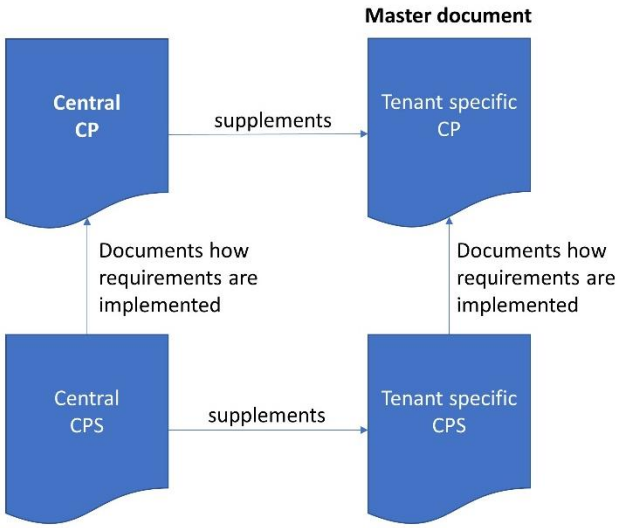

Figure 2: Document structure (CP and CPS)

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 Product PKI hosts several Root CAs and corresponding subordinate CAs. Every CA is associated to one Tenant.

The generic structure of the Product PKI hierarchy of Tenants is shown in Figure 3.

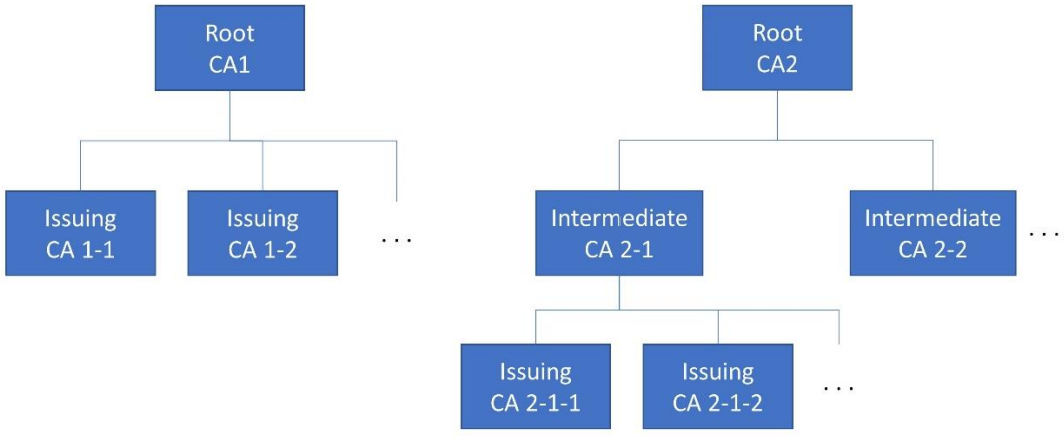

Figure 3: Product PKI hierarchy

The detailed Product PKI hierarchy of *Tenants* is described in the respective Tenant CP.

1.2 Document Name and Identification

This CP is referred to as the 'Central Certificate Policy'.

Title: Siemens Product PKI Certificate Management Service - Central Certificate Policy

OID: 1.3.6.1.4.1.4329.99.1.2.0.1

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

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

1.3 PKI Participants

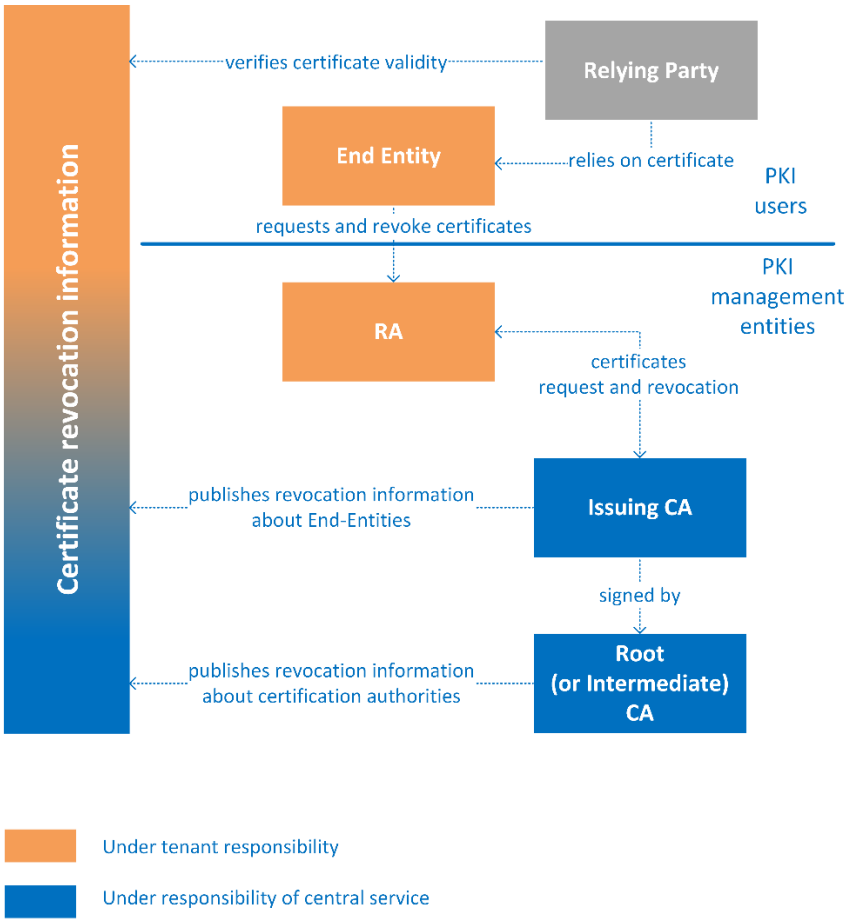

Figure 4: Product PKI Participants Overview

PKI Participants are Certification Authorities, Registration Authorities, Subjects (End-Entities), and Relying Parties (see also section 1.6).

1.3.1 Certification Authorities

A graphical overview of the CA hierarchy is depicted in *Figure 3: Product PKI* hierarchy.

1.3.1.1 *Root CA*

The Product PKI architecture is based on a multi-tier CA structure. This architecture allows the Root CAs to be stored off-line.

The Root CAs are primarily used to issue, manage, and revoke X.509v3 certificates of the corresponding Intermediate and Issuing CAs. The main tasks include:

- Generating Root CA Key Pairs
- Generating the self-signed certificates for the Root CAs

- ❑ Generating certificates for Intermediate and Issuing CAs
- ❑ Recertification of existing CA keys
- ❑ Revoking CA certificates
- ❑ Maintaining a Revocation List for CA certificates (“ARL”)

1.3.1.2 *Intermediate CA*

The Intermediate CAs issue, manage, or revoke X.509v3 certificates of subordinate Intermediate or Issuing CAs.

The usage of Intermediate CAs is optional.

The services offered include:

- ❑ Generating certificates for subordinate CAs
- ❑ Revoking certificates of subordinate CAs
- ❑ Maintaining a Revocation List for subordinate CA certificates (“ARL”)

1.3.1.3 *Issuing CAs*

Issuing CAs issue, manage or revoke X.509v3 End-Entity certificates that e.g. are used by Siemens devices.
The services offered include:

- ❑ Generating certificates for the End-Entities
- ❑ Revoking End Entity certificates
- ❑ Maintaining a certificate status information for End Entity certificates (e.g. “EE-CRL”)

1.3.2 Registration Authorities

RA responsibilities include:

1. Establishing an environment and procedure for certificate applicants to submit their certificate applications;
2. “Identification and authentication” of certificate applicants;
3. Approval or rejection of certificate applications;
4. Approval of certificate revocation requests either at the Subject’s (see 1.3.5.1) request or upon other RAs initiative;
5. Identification and authentication of Subjects submitting requests seeking a new certificate following a re-keying process and for certificates issued in response to approved re-keying requests.

Registration of Subjects (e.g. devices) may be delegated to Tenants. However, in such a case the Tenant also will take over the above-mentioned responsibilities.

1.3.3 Subscribers

Subscriber is always a Tenant, who is responsible for the procedures of the Registration Authority applying for End-Entity certificates. Responsible for the key and the content of the End-Entity certificate is the Subscriber. However, the Tenant may delegate rights to dedicated persons and functions that then act on his behalf. Examples for such persons and functions are administrators or employees.

Subscriber’s responsibilities include:

1. provide complete, accurate and truthful information in a certificate application;
2. request the revocation of Subject’s certificate when the certificate e.g. contains incorrect information or when Subscriber has reason to believe that the private key has been compromised;
3. acknowledgement of receipt or assent of issued EE certificates.

1.3.4 Relying Parties

A “Relying Party” is a PKI Participant who uses a certificate to obtain the Subject’s public key and is in the position to rely on the assurances in the certificate.

In the event in which a certificate is issued to a device, application, service or any other entity which does not

constitute a physical person then the term "Relying Party" designates the legal entity responsible for it.

Relying Party responsibilities include:

1. perform cryptographic operations properly: verification of digital signatures by referring to Subject's public key listed in a certificate and verification whether there is a certificate path to a trusted CA;
2. check the status of certificates before relying on it, including the revocation status in the Certificate Revocation List ("CRL") or by the use of the Online Certificate Status Protocol ("OCSP");
3. assent to the terms of an applicable agreement required as a condition to relying on the certificate.

1.3.5 Other Participants

1.3.5.1 *Subject (End Entity)*

The Subject is the entity that is authenticated by the private key and has control over its use.

The *Subject*:

(1) is named or identified in the respective elements of the certificate issued to this entity, and

(2) controls the private key that corresponds to the public key listed in that certificate.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

The certificates signed by the Product PKI are approved for the following usages:

Certificate Type	Certificate Usage
Root CA certificate	This certificate is signed by the private key of the Root CA itself and only approved for signing the CA certificates of subordinate CAs, the Root CA´s CRL, and OCSP signer certificates.
Intermediate CA certificates	These certificates are approved only for signing of subordinate CA certificates (e.g. Issuing CA certificates), the Intermediate CA´s CRL, and OCSP signer certificates.
Issuing CA certificates	These certificates are approved only for signing of End Entity certificates, the Issuing CA´s CRL, OCSP signer certificates, and CMP messages.
End-Entity certificates	These certificates are approved only for usage in accordance with the "key usage" and "extended key usage" fields set in the End Entity certificate

Table 1: Certificate Usage

The approved usages of keys and certificates signed by the respective *Issuing CA*s can be found in the respective Tenant CPS.

1.4.2 Prohibited Certificate Usage

All certificate usages not listed in 1.4.1 are prohibited.

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") Cyber Security Technology ("CST")

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 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: certificate-problem-report (at) siemens.com

1.5.3 Person Determining CP and CPS Suitability for the Policy

The Policy Management Authority (Central 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	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

ACP	Asset Classification and Protection
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

Product PKI provides the Central CP, the Central CPSs, certificate(s), OCSP(s) and CRLs.

Further details regarding publication are specified in the Tenant CP and Tenant CPS.

2.1 Repositories

Siemens central PPKI repositories are operated either by Siemens PPKI itself or by trusted service operators.

The repository responsibilities include:

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

See also Tenant CPs for Tenant specific repositories.

2.2 Publication of Certification Information

Siemens central PPKI publishes CP and CPS on the web site specified in section 1.5.1.

See also Tenant CPs for Tenant specific aspects.

2.3 Time or Frequency of Publication

Updates to this CP are published in accordance with the definitions in section 9.12 of this document.

See also Tenant CP.

2.4 Access Controls on Repositories

Product PKI requires its repository operator(s) to implement technical and organizational security measures to prevent misuse by authorized persons or prevent unauthorized persons from adding, deleting, or modifying entries in the repository.

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, in the respective Certificate Profile documentation, for each certificate type.

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*

The use of pseudonyms for CA names is not permitted.

3.1.3.2 *End Entity Names*

The use of pseudonyms for End Entity names is not permitted unless otherwise stated in the *Tenant* CP.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

3.1.5.1 *CA Names*

Product PKI ensures that Root CA, Intermediate CA and Issuing CA names are unique within the scope of the respective CA signing the certificate.

3.1.5.2 *End Entity Names*

The Issuing CAs ensure during the enrollment process that uniqueness of certificates is guaranteed within the scope of the respective CA signing the certificate.

3.1.6 Recognition, Authentication, and Roles of Trademarks

Certificate applicants are prohibited from using names in their certificate applications that infringe upon the Intellectual Property Rights of others. *Product PKI,* however, does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application or resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. Without liability to any certificate applicant, *Product PKI* may reject or suspend any certificate application because of such dispute.

3.2 Initial Identity Validation

Applicants for certificates are End Entities. The applicant always acts on behalf of the Subscriber (Tenant).

A certificate shall be issued to a Subject only when

- the Subject has submitted a certificate request and
- the Subject or the RA confirm private key possession.

3.2.1 Method to Prove Possession of Private Key

Certificate requests are only accepted according to Product PKI approved methods.

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

3.2.2 Authentication of Organization Identity

Certificates will be issued only to Tenants.

3.2.3 Authentication of Individual Identity

See Tenant CP.

3.2.4 Non-verified Subscriber Information

Only verified Information is included into the certificate.

3.2.5 Validation of Authority

See Tenant CP.

3.2.6 Criteria for Interoperation

No interoperation with other communities of trust is foreseen, unless otherwise stated in the Tenant CP.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Re-key procedure shall be only possible after successful authentication with a valid certificate.

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 must be authorized by the Tenant PMA.

Revocation of Intermediate CA and Issuing CA certificates shall only be performed manually by Product PKI trusted employees under dual control.

Revocation request of End-Entity certificates can be performed by Product PKI trusted employees (manually) and the corresponding authorized RA (automatically).

4 Certificate Lifecycle Operational Requirements

This section addresses the administration of Product PKI Root CA's, Intermediate CA's and Issuing CA's key pairs throughout the operational life cycle of the Root CAs, Intermediate CAs and the Issuing CAs, including how

- the public and private keys are generated and/or re-generated (i.e. re-keying)
- the private key(s) are stored, protected and eventually destroyed
- the public key(s) are distributed and archived.

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

4.1.1.1 *Root and Intermediate CA*

The Product PKI PMA decides if a new Intermediate or Issuing CA is to be created and to be signed by the respective Root or Intermediate CA.

4.1.1.2 *Issuing CAs*

All certification requests for EE certificates from authorized RAs shall be processed.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 *CA Certificates*

For CA certificates to be generated, following information shall be documented:

- ❑ A name for the CA in accordance with regulations in section 3.1, “Naming”, of this CP
- ❑ Date of the request
- ❑ Duration of the CA certificate, which cannot exceed the duration of the Root CA’s certificate
- ❑ Certificate profile of the new CA and
- ❑ Profiles of the End Entity certificates to be signed by that new CA, in case of an Issuing CA

4.1.2.2 *End Entity Certificate*

End-Entity certificate applicants undergo an enrollment process consisting of:

- generating, or arranging to have generated, a key pair
- completing a certificate application and providing the required information
- either demonstrating to the respective RA or CA that the certificate applicant has possession of the private key corresponding to the public key included in the certificate application

  or guaranteeing by comparable measure that the certification request is originating from a legitimate End-Entity and that the End-Entity controls the private key.

Certificate applications are submitted for processing, either approval or rejection, to the respective RA.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

Product PKI ensures that certificate applicants (= “Subjects”) are properly identified and authenticated.

For EE certificates, the Product PKI delegates these tasks to respective RAs.

4.2.2 Approval or Rejection of Certificate Applications

After a certificate applicant submits a certificate application, Product PKI shall approve or reject it.

Product PKI verifies that the certificate application is complete, accurate and duly authorized. If validation fails, the certificate application is rejected.

For EE certificates these tasks can be delegated to respective RAs.

4.2.3 Time to Process Certificate Applications

Certificate applications shall be approved or rejected in a timely manner.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued using secure means after the approval of a certificate application.

Product PKI shall:

1. check authorization of the respective RA by validating the signature of the certification request,
2. generate for the Subject a Certificate based on the information in the certificate application after its validation, and
3. deliver the Certificate through the respective RA.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The CA informs the RA whether an EE Certificate has been generated or that the certification request could not be successfully executed.

The notification of the Subscriber is detailed in the Tenant CP.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

CA certificate acceptance shall take place as part of or as a result of the CA Creation Ceremony.

The Subjects shall securely obtain the Certificate through the respective RA.

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

The Root CA private key is only used for:

- Issuance of Root CA's certificates
- Issuance of Intermediate or Issuing CA certificates
- Issuance of Root CA's CRLs
- Issuance of CRL signer certificates or OCSP signer certificates

The Issuing CA private key is only used for:

- Issuance of certificates to End-Entities
- Issuance of Issuing CA's CRLs
- Issuance of CRL signer certificates and OCSP signer certificates
- Signing of CMP messages sent to the RA

4.5.1 Subject Private Key and Certificate Usage

Subject private keys and certificates shall only be used for the purposes as specified in the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Before any act of reliance, Relying Parties shall

- securely obtain the Root CA certificate,
- obtain and verify the validity, suspension or revocation of all subordinate CA and EE certificates using current revocation status information as indicated to the Relying Party of all certificates in the certificate chain
- take account of any limitations on the usage and liability limits of the certificate indicated to the Relying Party in this CP

Relying parties are responsible to validate certificates including certificate chain and revocation status.

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.

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

"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

The Re-key Process shall 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*

Rekeying 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 4.3).

No previously validated information shall be reused.

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.

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

There can be the following technical reasons for revoking a certificate:

- identification information in the certificate become invalid
- the Subject is found to be in violation of its agreement terms
- private key material connected to a certificate is suspected of compromise
- the key lengths or algorithms used no longer seem secure enough
- a change in the CA hierarchy is necessary, and
- the Central PMA or the Tenant PMA recognizes an urgent threat of a yet unknown technical nature.

4.9.2 Who can request revocation?

Only the Tenant PMA can request revocation of Root CA certificates, Intermediate CA and Issuing CA certificates as well as EE certificates.

4.9.3 Procedure for Revocation Request

Only authorized requests coming from an RA or the Tenant PMA will be accepted.

4.9.4 Revocation Request Grace Period

Revocation Requests shall be submitted by the requestor as soon as having reason to believe that there is a circumstance for certificate revocation.

4.9.5 Time within which CA must Process the Revocation Request

Product PKI processes the revocation request and any certificate problem report within the time frame, defined in the respective SLA, after its submission.

4.9.6 Revocation Checking Requirement for Relying Parties

See Tenant CP.

4.9.7 CRL Issuance Frequency

See Tenant CP.

4.9.8 Maximum Latency for CRLs

See Tenant CP.

4.9.9 On-line Revocation/Status Checking Availability

See Tenant CP.

4.9.10 On-line Revocation Checking Requirements

See Tenant CP.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements for Private Key Compromise

If Product PKI has reason to believe there has been a compromise of a CA's private key, it shall initiate the Siemens Incident Handling process and notify the respective Tenant.

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 Tenant CP.

4.10.3 Optional Features

See Tenant CP.

4.11 End of Subscription

In case the Subscriber ends subscription, a migration strategy shall be negotiated between the Tenant PMA and Central PMA. In case no migration strategy is defined, all still valid certificates will be revoked.

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

Management, operational, and physical controls of the Central Product PKI systems are defined in accordance with [ETSI 411] and [ETSI 401].

The Product PKI's trustworthy systems and products in use are protected against modification to ensure the technical and cryptographic security of the process supported by them.

Product PKI is operated according to the Information Security Management System of Siemens [ISMS], which supports the security requirements of this CP. This ISMS is based on ISO 27001 [ISO27001] and can be provided to a Qualified Auditor, as well as any other document that is deemed necessary by the Qualified Auditor, upon request to the PMA.

Each subsection of this chapter sets forth non-technical security controls for **central components** such as the Root CAs, Intermediate CAs, or typically also for Issuing CAs. Those controls will be fulfilled by the Siemens Trust Center and the Trusted Operator role holders operating it.

These non-technical security controls are critical to trusting the End-Entity certificates since lack of security may compromise CA operations. The level of trust for End-Entity certificate shall be assessed considering requirements expressed in the Central CP [this document] as well as requirements expressed in the Tenant CP. Should a requirement be expressed in both the Central CP and the Tenant CP then, the overall resulting level of trust will be at most equivalent to the level of trust derived from the less restrictive requirement.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The Trust Center, including all the Product PKI's systems, site location and construction shall be compliant with the requirements defined in TÜV Trusted Site Infrastructure Level 4 [TÜV].

Site specific security controls are defined in the respective Tenant CP.

5.1.2 Physical Access

The Trust Center, including all the Product PKI's systems, physical access shall be compliant with the requirements defined in TÜV Trusted Site Infrastructure Level 4 [TÜV].

Site specific security controls are defined in the respective Tenant CP.

5.1.3 Power and Air Conditioning

The Trust Center, including all the Product PKI's systems, power and air conditioning shall be compliant with the requirements defined in TÜV Trusted Site Infrastructure Level 4 [TÜV].

Site specific security controls are defined in the respective Tenant CP.

5.1.4 Water Exposure

The Trust Center, including all the Product PKI's systems, water exposure countermeasures shall be compliant with the requirements defined in TÜV Trusted Site Infrastructure Level 4 [TÜV].

Site specific security controls are defined in the respective Tenant CP.

5.1.5 Fire Prevention and Protection

The Trust Center, including all the Product PKI's systems, fire prevention and protection shall be compliant with the requirements defined in TÜV Trusted Site Infrastructure Level 4 [TÜV].

Site specific security controls are defined in the respective Tenant CP.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information shall be stored in designated secured areas either in multiple locations or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic exposure).

Site specific security controls are defined in the respective Tenant CP.

5.1.7 Waste Disposal

Sensitive documents and materials shall be shredded, in compliance with DIN66933, before disposal. Media used to collect or transmit sensitive information shall be rendered unreadable before disposal. Cryptographic devices shall be physically destroyed or zeroized in accordance with the manufacturers' guidance, and in compliance DIN66933 where applicable, prior to disposal.

Site specific security controls are defined in the respective Tenant CP.

5.1.8 Off-site Backup

Backups of critical system data, audit log data, and other sensitive information shall be routinely performed at defined intervals, as described in the respective CPS. Backup medias shall be securely stored offsite in a Siemens disaster recovery facility.

Site specific security controls are defined in the respective Tenant CP.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. Trusted role operations include:

- The validation, authentication, and handling of information in certificate applications,
- The acceptance, rejection, or other processing of certificate applications, revocation requests, renewal requests, or enrollment information,
- The issuance, or revocation of certificates, including personnel having access to restricted portions of its repository,
- Access to safe combinations and/or keys to security containers that contain materials supporting production services,
- Access to hardware security modules (HSMs), their associated keying material,
- Installation, configuration, and maintenance of the CA and of RA systems

Personnel holding a trusted role include, and it is not limited to:

- Trusted Operator roles as defined in [ETSI 401] (REQ-7.2-15):
- Security Officers
- System Administrators and System Operators
- System Auditors
- Data Protection Officer
- Corporate Information Security Officer (CISO)

Site specific security controls are defined in the respective Tenant CP.

5.2.2 Numbers of Persons Required per Task

Establishment and maintenance of rigorous control procedures ensure the segregation of duties based on job responsibility. Multiple Trusted Persons are required to perform sensitive tasks.

The following activities shall be performed at least by two trusted roles:

- Access to the high-security facilities;
- Logical and physical access to HSMs;
- Physical access to data archive, and
- Logical access to central, sensitive or critical systems of Siemens Root CA and its backup systems.

Site specific security controls are defined in the respective Tenant CP.

5.2.3 Identification and Authentication for Each Role

Identification and Authentication of persons to sensitive areas shall rely on multi-factor-authentication. Access to critical systems shall be granted only to trusted roles that authenticate with unique credentials that in turn are stored on secure crypto-tokens, e.g. smartcards. Role-based authorization of the users shall be enforced, in control systems.

Additional controls shall be implemented to protect against equipment, information, media and CA software being taken off-site without authorization.

Site specific security controls are defined in the respective Tenant CP.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Persons seeking employment for Trusted Operator roles must present proof of the requisite background, credentials and experience needed to perform prospective job responsibilities competently and satisfactorily, as well as proof of government clearances, if any, necessary to perform certification services under government contracts.

Site specific security controls are defined in the respective Tenant CP.

5.3.2 Background Check Procedures

Background verification checks on all candidates for employment (contractors and external users) are carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Police criminal record checks or equivalent background clearances are repeated at regular intervals.

All personnel who fail an initial or periodic investigation will not serve or continue to serve in a *Trusted Operator* role.

Site specific security controls are defined in the respective Tenant CP.

5.3.3 Training Requirements

All personnel performing management activities, with respect to the operation of the Product PKI, shall 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.

Site specific security controls are defined in the respective Tenant CP.

5.3.4 Retraining Frequency and Requirements

Personnel in *Trusted Operator* roles shall receive refresher training and updates to the extent and with the frequency 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 shall be provided on an ongoing basis.

Site specific security controls are defined in the respective Tenant CP.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

No independent contractors, external consultants or apprentices shall be employed for Product PKI operation to fill Trusted Operator roles.

If the cooperation with independent contractors, consultants or apprentices is necessary, they shall be permitted to have access to secure facilities only to the extent they are escorted and directly supervised by authorized personnel in Trusted Operator roles.

5.3.8 Documents Supplied to Personnel

Personnel in Trusted Operator roles shall be provided with the rules and regulations laid down in the Siemens Information Security Management System [ISMS], and other documentation, which are binding on all personnel performing trusted roles.

This information is needed for employees to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

The purpose of logging is the continuous documentation of parameter modifications, configuration changes, etc. to the components of the central Product PKI Systems. The logging processes focus particularly on the following:

- Any activities taking place on the administrative components, and
- Any intervention in the applications, e.g., Firewall, Webserver, Database, Authentication, Certification Authority.

5.4.1 Types of Events Recorded

Product PKI records details of the actions taken to process a certificate request and to issue a certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved.

The Product PKI shall record at least the following events:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of certificates; and
    f. Generation of certificate Revocation Lists and OCSP entries.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;

e. Firewall and router activities; and

f. Entries to and exits from the CA facility.

Log entries include the following elements:

1. Date and time of entry;
2. Identity of the entity, person or technical component making the journal entry; and
3. Description of the entry.

5.4.2 Frequency of Processing Log

Audit and logging data shall be available to be controlled by the Central PMA and the Tenant PMA. Product PKI shall make the records, generated under section 5.4.1, available to Qualified Auditors as proof of the Central Product PKI System compliance with requirements defined in the Certificate Policy [this document and Tenant CP] under which the CA operates.

In addition, logs are regularly checked automatically by a monitoring system or manually by trusted roles on demand.

Internal audits shall be performed whenever there is indication or suspicion of misconduct.

5.4.3 Retention Period for Audit Log

Product PKI shall retain any audit logs generated for at least ten (10) years.

Site specific audit logs (in particular of the (L)RAs at the Tenant site) shall be retained for a time period specified in the Tenant CP.

The CA shall make these audit logs available to its Qualified Auditor upon request. Every retention period is subject to the local data privacy law and may be changed without further notice to reflect changing legal requirements.

5.4.4 Protection of Audit Log

Automatically created audit logs shall be integrity protected. Audit logs shall be protected from unauthorized viewing, modification, destruction, or any other form of tampering.

5.4.5 Audit Log Backup Procedures

Audit logs are backed up and archived as defined in section 5.5

5.4.6 Audit Collection System (Internal vs. External)

Accumulation system used to collect and securely store audit logs shall be located at a secure facility which is operated at a security level comparable with the security level of the facility that hosts the CA.

5.4.7 Notification to Event-Causing Subject

This CP does not set forth any requirements on notification of event-causing Subject.

Additionally, this CP requires that: if an audit event, which results in an alarm, or an anomalous audit log entry is otherwise detected, an adequate countermeasure shall be initiated to avoid further intrusion, damage or tampering.

5.4.8 Vulnerability Assessments

Vulnerability of the CA shall be assessed, at the minimum, annually as part of annual Siemens-internal security assessments. CA vulnerabilities shall be documented following the standard Siemens risk assessment process, in accordance with ISMS [ISMS] regulations.

Site specific vulnerability assessments are defined in the respective Tenant CP.

5.5 Records Archival

5.5.1 Types of Records Archived

The types of records that shall be archived include the following:

- Technical Log Data
  Technical Log Data are used for Operational Status Monitoring events and provide the basis for corrective actions. Technical Log Data are generated automatically and electronically from CA system functions, and are stored and archived automatically;
- Audit Data
  Audit Data are generated automatically or manually, used for Access and Non-repudiation events and are required by *Product PKI* for commercial, legal or organizational purposes.
  - *Automatic Audit Data* consists of audit and statistical information
    Audit information provides evidence of events to show whether actions were performed in accordance with the agreed procedures and to show to what extent identifiable tasks are being performed and completed;
    Statistical information shows whether the SLA requirements are met and provides data for a quantitative and preventive systems analysis.
  - *Manual Audit Data* consists of procedure information that is kept in handwritten form as an original and signed where appropriate for evidentiary purposes. Such data includes log book records, release documents, update instructions etc.

5.5.2 Retention Period for Archived Audit Logging Information

The retention period for Technical Log Data as defined in section 5.5.1 is at least six weeks. The retention period for Automatic Audit Data in section 5.5.1 is at least ten years. Manual Audit Data is retained for at least ten years. Every retention period is subject to local data privacy law and may be changed without further notification to reflect changing legal requirements.

Site specific retention periods for archived audit logs are defined in the respective Tenant CP.

5.5.3 Protection of Archive

Protection of archived records shall be performed in accordance with Siemens ISMS [ISMS]. No unauthorized user shall be permitted to write to, modify, or delete the archive.

Archived records shall be hosted in multiple locations. These locations shall be equipped with adequate monitoring and protected against theft or unauthorized destruction, alteration or loss, as set forth in the ISMS [ISMS] regulations.

Site specific security controls are defined in the respective Tenant CP.

5.5.4 Archive Backup Procedures

Archive backup procedures are implemented according to Siemens ISMS Regulations [ISMS]. For technical log data and automatic audit data, a daily incremental backup and a weekly complete backup are performed. Manual audit data are stored whenever it has been generated. Before a system upgrade, a complete backup is made of all technical log data, automatic audit data, and related software.

Site specific security controls are defined in the respective Tenant CP.

5.5.5 Requirements for Time-Stamping of Record

Archived records, as defined in section 5.5.1, shall be time-stamped upon creation.

5.5.6 Archive Collection System (internal or external)

All archived data shall be stored as described in section 5.5.3.

5.5.7 Procedures to Obtain and Verify Archived Information

Procedures, to obtain and verify archived records, shall be implemented in accordance to ISMS regulations. Backup procedures shall include automated control steps to confirm that stored audit logging information can later be accessed and read.

5.6 Key Changeover

In the event of a CA key changeover, the new CA public key shall be published in accordance with the publication requirements set forth in the Tenant CP.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

In the event of an incidents or a compromise during regular operation of the Product PKI, the PMA shall be timely informed, initiate the Incident Handling Process [IHP] and, an Incident Response Team shall be assembled in accordance with the ISMS [ISMS] regulations. The Incident Response Team is tasked with:

- Gathering relevant information;
- Assessing risks connected with the incident;
- Developing a recovery procedure, and
- To propose and implement a recovery procedure with approval from the Tenant PMA and the Central PMA.

The Incident Response Team, while defining the recovery procedure, shall consider several aspects, including but not limited to:

- The consequences of the specific incident or compromise, and
- Any resulting allocation of liability among the PKI Participants under or relevant SLA or governing law.

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

If the Product PKI´s computing resources, software or data are corrupted (e.g., by natural disaster or hostile attack), the Product PKI will report such occurrence to the PMA. Handling procedures shall be implemented for actual or threatened hostile attacks, as described in section 5.7.1.

In the event of a natural disaster and, if only the Root CA is affected, the Issuing CA can continue to operate, because:

(i) replacement hardware will be quickly procured;

(ii) the Software of Root CA System is available;

(iii) the Root CA's private key and the CRL are kept separately and in secure locations, and

(iv) if items (i)-(iii) are available, the Root CA System can be re-activated on short notice.

If the Issuing CA is affected, the respective Tenant PMA shall be immediately informed, and the incident handling process shall be initiated.

The responsibility to inform Relying Parties lies with the Tenant, therefore it is detailed in the Tenant CP.

5.7.3 Entity Private Key Compromise Procedures

If Product PKI private key, up to the Root CA, is compromised or suspected to be compromised, following procedures shall be performed:

- Inform the respective Tenant PMA;
- inform the Central PMA;
- indicate that certificates and revocation status information issued using this CA key may no longer be valid;
- terminate the certificate and CRL Distribution Service for certificates and CRLs issued using the compromised private key.

In addition, in case of End-Entities', Issuing CAs' or Intermediate CAs' private key compromise the revocation of all affected certificates will be requested in alignment with the respective Tenant.

In addition, in case of Root CAs' private key compromise its private key shall be disposed upon agreement with the Tenant PMA. Whether and how to inform the Relying Parties, about the Root CA key is under the Tenant responsibility and therefore detailed in the Tenant CP.

5.7.4 Business Continuity Capabilities After a Disaster

The High Availability of Certificate Life Cycle Management services of the Product PKI shall be guaranteed by a redundant installation of the system.

In the event of a corruption or loss of computing resources, software or data, an appropriate Disaster Recovery and Business Continuity Plan shall be started, in accordance with the ISMS [ISMS] regulations. The CA services shall be resumed in a secure facility located in a different area and that is capable of hosting CA services.

Full CA functionality (recovery time objective) shall be provided within 30 days. Re-establishment of critical services like certificate revocation, certificate validation, and publication of CRLs shall be done as soon as possible.

5.8 CA or RA Termination

In the event that the Product PKI needs to revoke a CA or RA certificate operated on behalf of a Tenant – therefore terminate the corresponding service – the Central PMA and the Tenant PMA shall jointly approve the procedure as well as take measures to mitigate the impact. The grace period prior to the CA termination shall be reasonable and commensurate with the termination reason: e.g. end of subscription shall trigger a termination notification at least (6) six months before.

For example, in the event of a termination of a CA service, the following termination plan can be adopted to minimize disruption to Relying Parties:

- The respective Tenant should publish a notification to parties affected by the termination;
- Revocation of the certificate issued to Issuing CAs;
- Preservation of the CA's archives and records for the time periods required in this CP;
- Continuation of Customer Support and Help Desk services;
- Continuation of Revocation Services, such as the issuance of CRLs;
- Disposition of the Root CA's private key, and
- Provisions needed for the transition of actual Root CA's services to a successor Root CA.

If it shall be necessary to terminate an RA service, Product PKI should:

- Notify Relying Parties and other affected entities in advance of the RA termination;
- Revoke the certificates issued to the RA;
- Initiate the enrollment of a new RA service if required.

Site specific security controls are defined in the respective Tenant CP.

6 Technical Security Controls

Technical security controls and measures taken by the CAs, RAs, *Subjects* and repositories to protect their keys and activation data (PIN, passwords or key shares) are defined in accordance with [ETSI 411] and [ETSI 401].

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The Key Pairs of the Root CAs and Issuing CAs shall be generated in a hardware security module ("HSM"), which is certified in accordance with FIPS 140-2 level 3 [FIPS]. The key storage is restricted to the module where the key was generated. CA Key Pair Generation shall be executed by multiple persons holding a trusted role in a secure environment, as defined in chapter 5.

This CP does not set forth specific requirements for RAs and Subject Key Pair generation. RA entities shall follow Key Pair generation requirements equivalent or more restrictive than Subject Key Pair generation requirements.

See Tenant CP for requirements of RA and Subject Key Pair generation.

6.1.2 Private Key Delivery to Subscriber

CAs shall generate their own private keys; therefore, no private key delivery is required in this case. In case a Subscriber requests an RA to generate a Key Pair on its behalf, delivery of the private key shall be secured via technical or organizational means.

6.1.3 Public Key Delivery to Certificate Issuer

Subject's public key, together with its identity, shall be securely delivered to the certificate issuer to allow the binding of the Subject identity with its public key. If the public key is delivered electronically then, the transmission of the cryptographic material shall be integrity protected according to state-of -the-art.

6.1.4 CA Public Key Delivery to Relying Parties

Root CA and Issuing CA public keys shall be securely and reliably distributed to Subscribers and Relying Parties. Acceptable distribution methods include, but are not limited to:

- Secure out-of-band delivery;
- Secure delivery in a device at manufacturing time;
- Publication on a secure website.

6.1.5 Key Sizes

Minimum requirements for key sizes and algorithms are defined in accordance with [ECRYPT] and [NIST]. Additional requirements towards allowed key sizes and algorithms are set forth in the respective Tenant CP(s).

6.1.6 Public Key Parameters Generation and Quality Checking

The CAs and *Subscribers* shall generate Key Pairs using secure algorithms and parameters based on state-of-the-art cryptography and industry standards.

CA Key Pairs shall be generated in Hardware Security Modules certified according to FIPS 140-2 level 3, hence guaranteeing sufficient quality of the parameters used and the overall Key Pair generation procedure.

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

Key Usage and Extended Key Usage extension fields of Product PKI certificates shall be specified in accordance with RFC 5280 [RFC5280].

For additional requirements see Tenant CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CA Key Pair shall be generated and hosted in Hardware Security Modules, certified at FIPS 140-2 level 3. Additional controls, on the cryptographic module include but are not limited to:

- Multi-Person control required to access the hosting facility and to manage the cryptographic modules

(see section 6.2.2);
- ❑ Cryptographic modules shall be hosted in a physically secured facility (see section 5.1);
- ❑ Cryptographic modules shall make use only state of the art cryptographic algorithms and industry standards.

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

Technical and procedural mechanisms shall be put in place to enforce Multi-person Controls and to ensure that only Trusted Operator roles can perform sensitive CA cryptographic operations. For example, in order to gain access to the private keys, N out of M persons shall be required. At all time, no single person shall be in possession of all the activation data needed for accessing any of the CA private keys.

6.2.3 Private Key Escrow

Not supported for CA keys.

6.2.4 Private Key Backup

This CP supports CA private key backup. Under no circumstances shall a Subject private key be backed up.
CAs' private key shall be backed up and securely stored to mitigate risks and potential disruptions connected to key loss. Backed up private key shall be stored in a site different from where the CA is hosted during operations.
Backup and restore procedure shall be executed by Trusted Operator roles, enforcing Multi-person Controls, and only be stored in encrypted form in a secure location (see section 6.2.1).
Backup and restore procedure shall be executed only in locations operated at the same security level as the location hosting the CA during operations (see section 5.1).

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys shall be generated in Cryptographic Modules, as defined in section 6.2.1. Transferring private keys between two Cryptographic modules shall be performed only as part of a backup procedure. CA private keys shall be backed up as described in section 6.2.4.

6.2.7 Private Key Storage on Cryptographic Module

CA private key shall be always stored, encrypted, on Cryptographic Modules that are compliant with the requirements defined in section 6.2.1.

6.2.8 Method of Activating Private Key

CA private key shall be activated by authenticated Trusted Operator roles and Multi-person Control shall be enforced as described in section 6.2.2. Acceptable means of authentication include but are not limited to passphrases and PINs compliant with the Siemens ISMS [ISMS].

6.2.9 Method of Deactivating Private Key

Deactivating Private Keys is not supported.

6.2.10 Method of Destroying Private Key

Private Keys shall be destroyed if they are no longer needed, or when the certificates to which they correspond expire or are revoked. CA private key destruction shall be performed by Trusted Operator roles in a Multi-person Control regime. Private Keys shall be destroyed to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use. Private Key destruction shall be logged by technical and/or procedural means.

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 operational period of a certificate ends upon its expiration or revocation. The operational period for Key Pairs is the same as the operational period for the associated certificates, except that they may continue to be used for signature verification. The maximum expiration period allowed per certificate type is defined in the Tenant CP.

The applicability of cryptographic algorithms and parameters is constantly supervised by the Tenant PMA. If an algorithm or the appropriate key length offers insufficient security during the validity period of a certificate, the concerned certificate shall be revoked, and new certificate application initiated.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CA Activation Data values shall be intended as values required to operate Cryptographic Modules storing CA private key. Activation Data shall have a level of strength adequate to protect the private key material that is intended to be activated with. When transmission of Activation Data is required a secure channel shall be used. If a secure channel cannot be established via technical means then procedures that guarantee a comparable security level shall be used, e.g. Multi-person Control and physically secure locations can be used to establish a secure and confidential channel.

6.4.2 Activation Data Protection

Activation Data shall be protected at a security level comparable with the private key that is activated with. If private key material is secured with Multi-person Control this shall apply also to Activation Data. Activation Data shall not be stored in the same place with the private key that is activated with. Activation Data shall be stored in a physically protected location.

6.4.3 Other Aspects of Activation Data

Activation Data shall be periodically refreshed. At the minimum it shall be changed when the private key, that is protected with, is changed.

6.5 Computer Security Controls

Product PKI Computer Security Controls are established and documented in accordance with the ISMS [ISMS] regulations.

6.5.1 Specific Computer Security Technical Requirements

Product PKI shall enforce the following Computer Security Controls:

- Multi-factor Authentication on CA System components;
- Secure audit capability;
- Secure communication with CA System components, this includes but it is not limited to databases and repositories;
- CA System components shall be subject to continuous monitoring;
- Multi-person control shall be enforced to perform configuration changes on the CA system.

(L)RA specific requirements are defined in the Tenant CP.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

Software used by the Product PKI shall be developed by trusted software supplier(s) and rigorously documented. Software and Hardware used by the *Product PKI* shall be exclusively dedicated to PKI usage and a proper maintenance and update of software and hardware procedure shall be established.

6.6.2 Security Management Controls

Product PKI's security management controls shall follow Siemens ISMS [ISMS].

6.6.3 Life Cycle Security Controls

All security management controls shall be periodically audited, and potential shortcomings shall be reported to the PMA.

6.7 Network Security Controls

Root CA shall be kept offline and shall not at any point in time be connected to a network with external access.

Issuing CA network security controls shall be enforced to maintain a trustworthy infrastructure. Network security controls shall be operated by Trusted Operator roles only, as specified in the ISMS [ISMS] standards. Network security controls includes, but are not limited to:

- Firewall and other controls, employed to protect the integrity of the PKI networks and prevent intrusions;
- sufficiently strong authentication to ensure that only authorized entities are communicating;
- integrity mechanisms, to ensure that the information being exchanged are not tampered with;
- confidentiality mechanisms to ensure that information exchanged among the PKI Participant is protected from unauthorized access;
- mechanisms to prevent damage from denial-of-service attacks.

PKI network shall be subject to periodical penetration test to ensure that Network Security Controls are operated correctly and that they are still state of the art in terms of security. Penetration tests results shall be communicated to the PMA.

(L)RA network security controls are defined in the Tenant CP.

6.8 Time Stamp Process

Certificates, audit trails (as defined in section 5.4.1), CRLs and other revocation database entries shall include trustworthy and accurate time and date information.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificate Profile definitions for CAs and the Subject certificates issued by it and certificate content requirements for issued certificates are in accordance with, e.g.,

- ITU-T Recommendation X.509 Version 3 [X.509] and
- RFC 5280 [RFC5280].

7.1.1 Version Number(s)

Typically, certificates are of type X.509 v3 [X.509].

Details of the CA Certificate Profiles are defined in the Tenant CP.

7.1.2 Certificate Extensions

Certificate extensions shall be compatible with RFC 5280 [RFC5280]. Critical extensions that are included by the CA in the Subject certificate shall be specifically requested by the Tenant. Any optional, additional or Subject specific extension shall be flagged as non-critical.

7.1.3 Algorithm Object Identifiers

Product PKI shall issue Subject certificates using only algorithms that are compatible with section 6.1.5.

7.1.4 Name Forms

Product PKI shall only issue Subject certificates whose Issuer and Subject information is consistent with the Tenant CP.

7.1.5 Name Constraints

Name Constraints set by Product PKI in Subject certificates shall be consistent with the Tenant CP.

7.1.6 Certificate Policy Object Identifier

Subordinate CA certificates and Subject certificates issued under this CP shall assert one or more of the Certificate Policy OIDs listed in section 1.2 of Certificate Policy. Issuing CA certificates shall contain the policy OIDs of all policies under which it issues certificates as defined in the Tenant CP.

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)

Product PKI shall issue X.509 version two (v2) CRLs.

7.2.2 CRL and CRL entry extensions

CRL critical extensions shall be interoperable among the relying parties.

7.3 OCSP Profile

7.3.1 Version Number(s)

Requests and responses version number shall be set to one (v1).

7.3.2 OCPS Extension

No stipulation.

8 Compliance Audit and Other Assessment

Product PKI's compliance to this CP and the relevant CPSs shall be checked at least on a biannual basis. In addition, a bi-annual asset classification of the Product PKI services and its components takes place. The Asset Classification and Protection [ACP] process 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.

8.1 Frequency or Circumstances of Assessment

Tenants can request a certification of the Product PKI service (e.g. in compliance with [ETSI 411]). In such a case audits are performed at least on an annual basis.

In addition to compliance audits, Product PKI may perform or request to perform assessments to ensure the trustworthiness of its trusted service providers, including without limitation:

- At its sole discretion, Product PKI may perform at any time an assessment on itself in case Product PKI has reason to believe that the audited entity has not operated in accordance with stated security policies or procedures in PKI documentation.
- Product PKI may perform supplemental assessments on itself or RA or other PKI Participant following incomplete or exceptional findings in a compliance audit or as part of the overall risk management process in the ordinary course of business.

8.2 Identity / Qualifications of Assessor

Compliance audits are performed by an external qualified auditor who:

- ❑ demonstrates proficiency in PKI technology, information security tools and techniques, security auditing, and the third-party attestation function
- ❑ is accredited by a recognized professional organization or association, which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education

8.3 Assessor's Relationship to Assessed Entity

The assessor shall be organizationally independent from the assessed entity's operational and policy authorities.

8.4 Topics Covered by Assessment

The scope of the compliance assessment, of the Product PKI, includes the review of the design and operational effectiveness of the assessed entity's controls over a defined period of time. The audit, or other assessment, should be performed using appropriate criteria covering environmental, key management and certificate life cycle management controls of the assessed entity. The purpose of the audit, or other assessment, is to assess whether the implemented controls are effective and in accordance with the defined business practices as expressed in relevant security policies and procedures.

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 PMA with input from the auditor/assessor. Product PKI is responsible for developing and implementing a corrective action plan.

If PMA determines that such deficiencies pose an immediate threat to the security or integrity of the Product PKI, 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, Product PKI 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 Central and Tenant PMAs.

9 Other Business and Legal Matters

Fees and other business aspects as well as legal aspects between Service Provider and Tenant are regulated in separate, bilateral contracts.

Tenant specific business and legal matters will be addressed in the specific Tenant CP.

9.1 Fees

9.1.1 Certificate Issuance or Renewal fees

Not applicable.

9.1.2 Certificate Access fees

Not applicable.

9.1.3 Revocation or Status Information Access fees

Not applicable.

9.1.4 Fees for other Services

Not applicable.

9.1.5 Refund Policy

Not applicable.

9.2 Financial Responsibility

Not applicable.

9.2.1 Insurance Coverage

Not applicable.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Not applicable.

9.3.2 Information not within the Scope of Confidential Information

Not applicable.

9.3.3 Responsibility to Protect Confidential Information

Not applicable.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

Not applicable.

9.4.2 Information treated as private

Not applicable.

9.4.3 Information not deemed private

Not applicable.

9.4.4 Responsibility to protect private information

Not applicable.

9.4.5 Notice and consent to use private information

Not applicable.

9.4.6 Disclosure pursuant to judicial or administrative process

Not applicable.

9.4.7 Other information disclosure circumstances

Not applicable.

9.5 Intellectual Property Rights

Not applicable.

9.5.1 Intellectual Property Rights in Certificates and Revocation Information

Not applicable.

9.5.2 Intellectual Property Rights in CP

Not applicable.

9.5.3 Intellectual Property Rights in Names

Not applicable.

9.5.4 Property rights of Certificate Owners

Not applicable.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

Not applicable.

9.6.2 RA representations and warranties

See Tenant CP.

9.6.3 Subscriber representations and warranties

Not applicable.

9.6.4 Relying party representations and warranties

See Tenant CP.

9.6.5 Representations and warranties of other participants

See Tenant CP.

9.7 Disclaimers of Warranties

Not applicable.

9.8 Limitations of Liability

Not applicable.

9.9 Indemnities

Not applicable.

9.10 Term and Termination

9.10.1 Term

Not applicable.

9.10.2 Termination

Not applicable.

9.10.3 Effect of Termination and Survival

Not applicable.

9.11 Individual Notices and Communication with Participants

Not applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

Not applicable.

9.12.2 Notification Mechanism and Period

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

The new version of the CP/CPS will be published within 24 hours 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, will lead to a corresponding change in the CP OID.

9.13 Dispute Resolution Provisions

Not applicable.

9.14 Governing Law

Not applicable.

9.15 Compliance with Applicable Law

Not applicable.

9.16 Miscellaneous Provisions

Not applicable.

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

Not applicable.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

SIEMENS ACCEPTS NO LIABILITY FOR ANY BREACH OF WARRANTY, DELAY, OR FAILURE IN PERFORMANCE THAT RESULTS FROM EVENTS BEYOND ITS CONTROL SUCH AS ACTS OF GOD, ACTS OF WAR, ACTS OF TERRORISM, EPIDEMICS, POWER OR TELECOMMUNICATION SERVICES FAILURE, FIRE, AND OTHER NATURAL DISASTERS.

9.17 Other Provisions

9.17.1 Order of Precedence of CP

This CP provides baseline requirements that are applicable to all CAs operated by the Product PKI. In the event of a conflict between this CP and any other document, 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. Tenant CP that is applicable to a Tenant operated by the Product PKI
2. Product PKI Central CP [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 entity authentication) as defined in section 1.1:

1. Tenant CP that is applicable to a Tenant operated by the Product PKI
2. Product PKI Central CP [this document]
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 Siemens internal documents can be retrieved on request.

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

[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

[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

[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