Siemens Corporate PKI

Certificate Policy

Version:	1.17
Date:	29.01.2024
Classification:	Public / Unrestricted

Document History

Version	Date	Author	Change Comment
1.0	June 20, 2016	Michael Munzert Alexander Winnen	First released version
1.1	December 1, 2016	Rufus Buschart	Minor updated version
1.2	May 29, 2017	Rufus Buschart	Update new structure of the Siemens PKI hierarchy
1.3	July 31, 2017	Björn Hundertmarck	Update with chapter for Certificate Authority Authorization (CAA)
1.4	December 1, 2017	Florian Grotz	Revised Certificate Authority Authorization (CAA)
1.5	January 12, 2018	Rufus Buschart	Chapter „Document History" Added changed after ballots Chapter 1.3.2 No delegated third parties Chapter 2.1 URL of CRL and OCSP added Chapter 2.2 URL of CRL and OCSP removed Chapter 4.9.1 Revocation reasons removed Chapter 4.9.5 Certificate problem report added Chapter 5 Moved from CPS Root CA
1.6	January 31, 2018	Rufus Buschart	Chapter 4.9.1 Cross certification partner mentioned Chapter 4.9.9 OCSP specification detailed Chapter 5.4.1 Information about the scope of logging data added Chapter 5.4.8 Frequency clarified Chapter 8.2 Auditor needs to be qualified
1.7	February 6, 2018	Rufus Buschart	Chapter 9.10.2 Reliable party added Chapter 6 Technical controls checked against ETSI EN 319 411-1 / 319 401 Chapter 7.1 Reference to ETSI EN 319 412-2 added Chapter 4.7 Reuse of previously validated information is prohibited Licence changed to CC BY-SA4.0 as required by Mozilla Chapter 1.2 OID 1.3.6.1.4.1.4329.7 added
1.8	August 31, 2018	Markus Wichmann	Chapter 9 Update
1.9	December 21, 2018	Rufus Buschart	Chapter 5.2 adapted Chapter 1.5.2 updated Chapter 4.9.3 updated with CPR contact information
1.10	February 18, 2019	Rufus Buschart	All chapter „No stipulations" removed
1.11	January 30, 2020	Rufus Buschart	Chapter 9.6ff updated Minor editorial changes
1.12	February 17, 2021	Rufus Buschart	Chapter 1.3: Clarification in regards to the fleet of Siemens companies All chapter: Reflecting revocation of TLS CA
1.13	June 14, 2021	Mauricio Fernandez	Chapter 1.1 Added CA 2021 Hierarchy, minor updates through Chaper 1,7,8,9. Chapter 4 updated
1.14	July 27, 2021	Mauricio Fernandez	Chapter 7 updated – CRLs profiles details
1.15	February 17, 2022	Rufus Buschart	Chapter 1.5.4 Added check interval Chapter 4.9.9 Difference between OCSP and CRL state clarified
1.16	February 21, 2023	Rufus Buschart	Minor editorial changes
1.17	January 24, 2024	Ilias Cotoulas Marco Fechter	Adaptions over all chapters for SBR101 Minor format changes

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. Changes to the CA/B Baseline Requirements will be reflected after passing of the respective ballot into this document. 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 overarching Certificate Policy (CP) for the Siemens Certification Authority. The Siemens Certification Authority is responsible for the operation of the Siemens Root CA as well as for the Siemens Issuing CAs. The purpose of this document is to publicly disclose to Subjects and Relying Parties the business policies and practices under which the Siemens CAs operate.

The senior management of the CA 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 with version 1.17 and status "Released" has been classified as "Unrestricted" and published under the CC BY-SA4.0.

	Name	Department	Date
Author	Various authors, detailed information in document history		
Checked by	Tobias Lange Florian Grotz	Siemens LC Siemens GS IT HR 7 4	June 20, 2016 February 20, 2019
Authorization	Mauricio Fernandez	Siemens CYS INF NG	January 29, 2024

Table of Content

1 Introduction

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

1.1 Overview

This document describes the Certificate Policy of the Siemens CA. It describes the services provided by the Siemens CA as well as binding requirements that have to be fulfilled by service providers and other PKI participants. Moreover (together with the CPSs) it also defines the certification process as well as the cooperation, duties and rights of the PKI participants.

In addition to the requirements defined in this CP and the corresponding CPSs, Siemens IT systems are operated according to the Siemens internal InfoSec rules and respective execution guidelines, which define how IT systems must be operated securely. These InfoSec rules are part of an ISMS, which is defined and implemented according to ISO 27001.

For delegated tasks, the Siemens CA and any Delegated Service Providers may allocate liability between themselves contractually as they determine, but the CA remains fully responsible for the performance of all parties in accordance with these requirements, as if the tasks had not been delegated.

1.1.1 PKI hierarchy

The structure of the Siemens PKI hierarchy is shown in the following figuresFigure 1. Currently three separate hierarchies under the same Siemens Root v.3.0 CA 2016 exist:

Internal

Siemens CA PKI Hierarchy 2020

- the Siemens Root CA v3.2016 is a self-signed X.509 v3 certificate acting as internal trusted anchor; dedicated for Siemens internal use cases and
- Siemens Issuing CAs 2020

Siemens CA PKI Hierarchy 2021

- the Siemens Root CA v3.2016 is a self-signed X 509 v3 certificate acting as internal trusted anchor; dedicated for Siemens internal use cases;
- Siemens Intermediate CA 2021 and
- Siemens Issuing CAs 2021

Siemens CA PKI Hierarchy 2023

- the Siemens Root CA v3.2016 is a self-signed X.509 v3 certificate acting as internal trusted anchor; dedicated for Siemens internal use cases;
- Siemens Intermediate CA 2021 and
- Siemens Issuing CAs 2023

The Siemens Root CA v3 2016 exclusively issues CA certificates to the Intermediate CA and Issuing CAs.
Siemens PKI CAs are cross signed by two external Trusted Service Providers Certificates Authorities (Authorized cross signer).

External

- Entrust.net Root Certificate Authority (2048) and
- Quovadis Root CA 3 G3

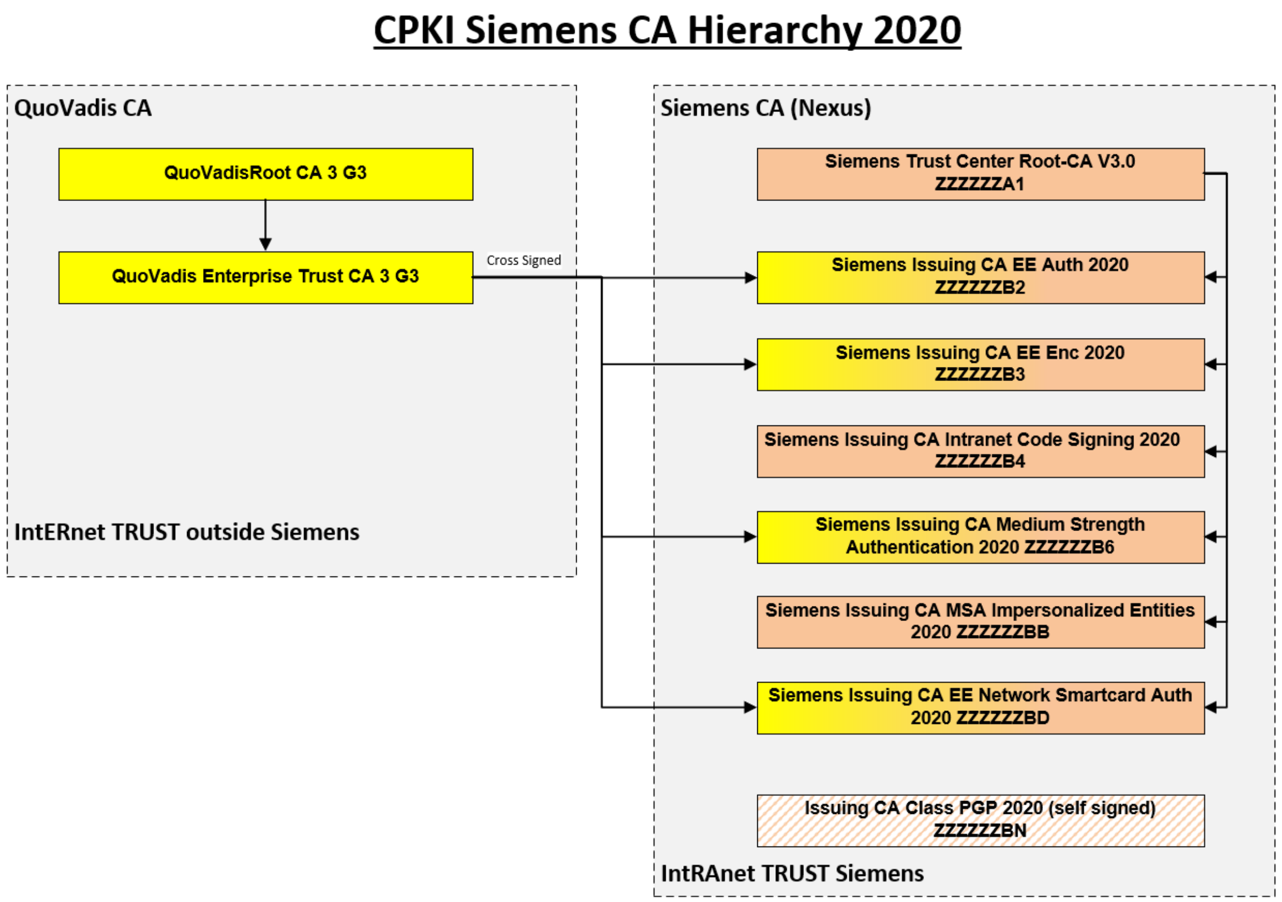
CPKI Siemens CA Hierarchy 2020
QuoVadis CA
QuoVadisRoot CA 3 G3
QuoVadis Enterprise Trust CA 3 G3
Cross Signed
IntERnet TRUST outside Siemens
Siemens CA (Nexus)
Siemens Trust Center Root-CA V3.0 ZZZZZZA1
Siemens Issuing CA EE Auth 2020 ZZZZZZB2
Siemens Issuing CA EE Enc 2020 ZZZZZZB3
Siemens Issuing CA Intranet Code Signing 2020 ZZZZZZB4
Siemens Issuing CA Medium Strength Authentication 2020 ZZZZZZB6
Siemens Issuing CA MSA Impersonalized Entities 2020 ZZZZZZBB
Siemens Issuing CA EE Network Smartcard Auth 2020 ZZZZZZBD
Issuing CA Class PGP 2020 (self signed) ZZZZZZBN
IntRAnet TRUST Siemens

Figure 1: Siemens PKI hierarchy 2020

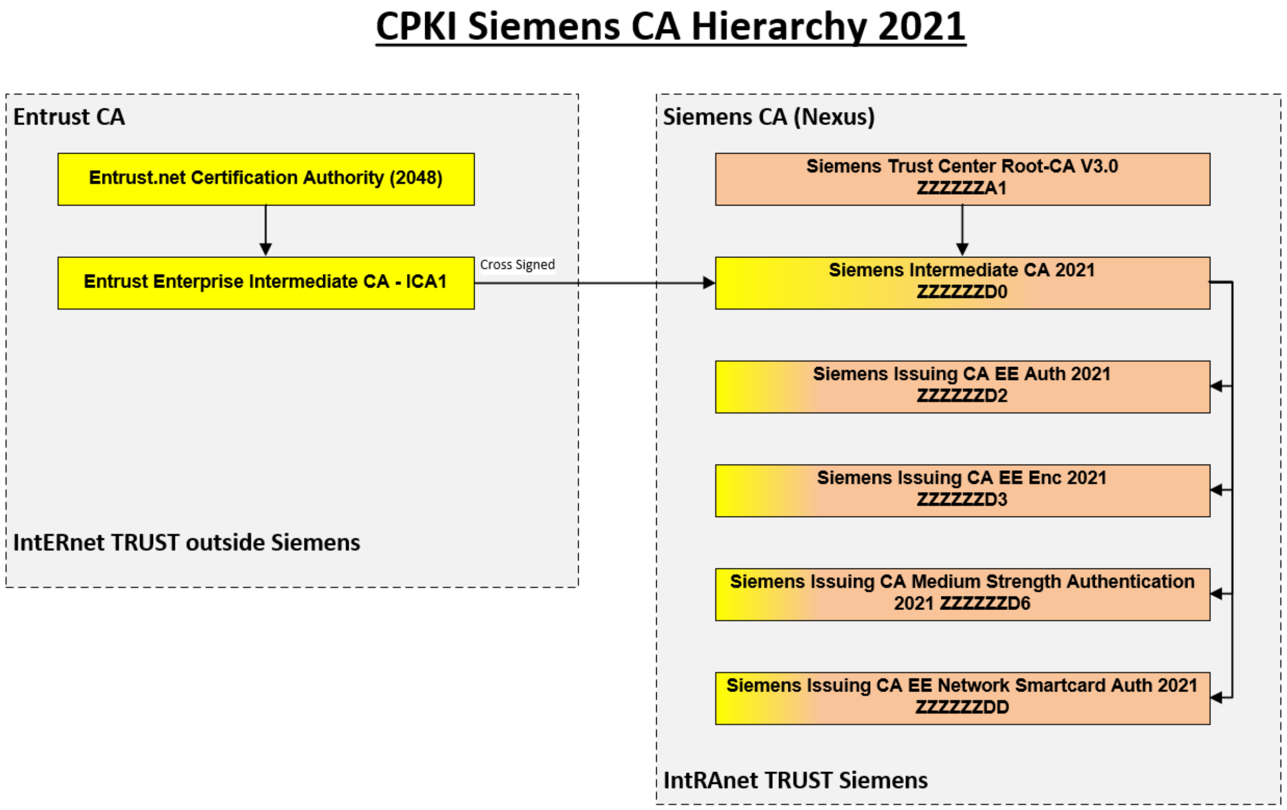
CPKI Siemens CA Hierarchy 2021
Entrust CA
Entrust.net Certification Authority (2048)
Entrust Enterprise Intermediate CA - ICA1
Cross Signed
IntERnet TRUST outside Siemens
Siemens CA (Nexus)
Siemens Trust Center Root-CA V3.0 ZZZZZZA1
Siemens Intermediate CA 2021 ZZZZZZD0
Siemens Issuing CA EE Auth 2021 ZZZZZZD2
Siemens Issuing CA EE Enc 2021 ZZZZZZD3
Siemens Issuing CA Medium Strength Authentication 2021 ZZZZZZD6
Siemens Issuing CA EE Network Smartcard Auth 2021 ZZZZZZDD
IntRAnet TRUST Siemens

Figure 2: Siemens PKI hierarchy 2021

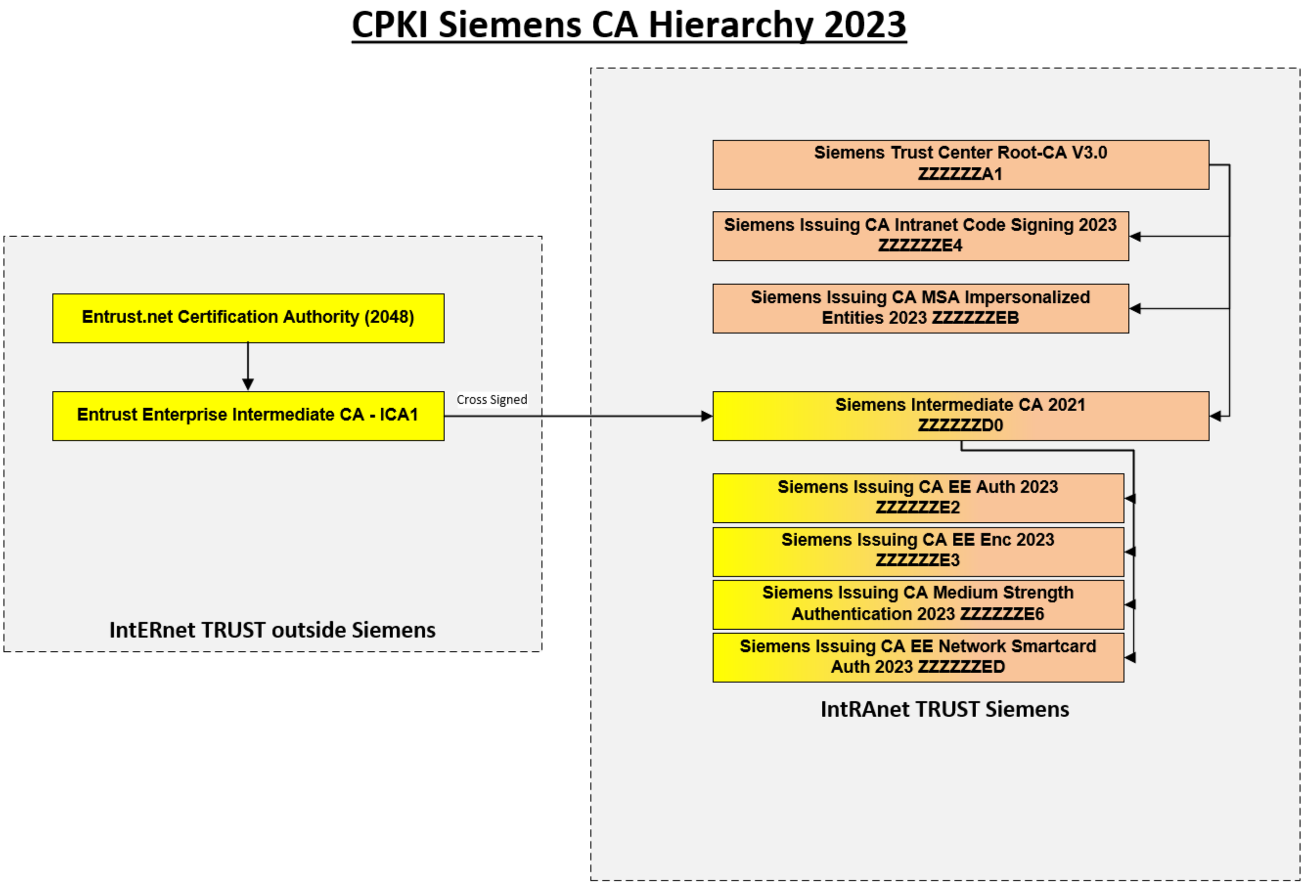
CPKI Siemens CA Hierarchy 2023
Siemens Trust Center Root-CA V3.0 ZZZZZZA1
Siemens Issuing CA Intranet Code Signing 2023 ZZZZZZE4
Siemens Issuing CA MSA Impersonalized Entities 2023 ZZZZZZEB
Entrust.net Certification Authority (2048)
Entrust Enterprise Intermediate CA - ICA1
Cross Signed
Siemens Intermediate CA 2021 ZZZZZZD0
Siemens Issuing CA EE Auth 2023 ZZZZZZE2
Siemens Issuing CA EE Enc 2023 ZZZZZZE3
Siemens Issuing CA Medium Strength Authentication 2023 ZZZZZZE6
Siemens Issuing CA EE Network Smartcard Auth 2023 ZZZZZZED
IntERnet TRUST outside Siemens
IntRAnet TRUST Siemens

Figure 3: Siemens PKI hierarchy 2023

All certificates issued by the above-mentioned CAs as a minimum comply with the ETSI requirements of NCP ETSI EN 319 411-1 [ex. ETSI TS 102 042].

1.1.2 Siemens Root v3 2016 CA, Entrust.net Certification Authority (2048)and Quovadis Root CA3 G3

The Siemens Root CA v3 2016 and the Entrust.net Certificate Authority (2048)[1] issue, manage, and revoke X.509v3 Certificates used by the corresponding Intermediate CAs. This includes:

- Generating Root Key Pairs
- Generating the self-signed Certificates for the Root CAs
- Generating Certificates for the Intermediates CAs
- Recertification of existing CA keys
- Revoking Intermediate CA Certificates
- Maintaining a Revocation List for CA Certificates (“CA-CRL”)

[1] The Entrust Root Certificate Authority (2048) and Entrust Enterprise CA – ICA are included for reference but not in scope of this CP and are managed under the Entrust CPS located at https://entrust.net/cps.

Quovadis Root CA 3 G3 and Quovadis Enterprise Trust CA 3 G3 are included for reference but not in the scope of this CP and are managed under the Digicert CPS located at https://www.quovadisglobal.com/repository

1.1.3 Intermediate CAs

The Siemens Intermediate CA 2021 is covered by this CP. In addition, the Siemens Intermediate CA 2021 is cross signed by the Entrust Enterprise Intermediate CA – ICA1 governed by the Entrust CPS.

The Siemens Intermediate CA2021 issues, manages, and revokes X.509 v3 certificates used by the corresponding Issuing CA.
This includes:

- ❑ Generating Intermediate CA Key Pairs
- ❑ Generating Certificates for Issuing CAs
- ❑ Revoking Issuing CA Certificates
- ❑ Maintaining a Revocation List for Intermediate CA Certificates (“ICA-CRL”)
- ❑ Managing OCSP responses for Issuing CAs

1.1.4 Issuing CAs

The Issuing [2]CAs together with other Siemens PKI Participants (such as Registration Authorities) issue, manage or revoke X.509v3 Public Key Certificates used for securing Siemens’ business processes either internally (e.g., Siemens’ employees) or externally (e.g., server certificates). The services offered include:

- ❑ Generating Issuing CA Key Pairs
- ❑ Generating Certificates for the end entities
- ❑ Revoking End-Entity Certificates
- ❑ Maintaining a Revocation List for End-Entity Certificates (“EE-CRL”)

1.2 Document Name and Identification

This CP is referred to as the ‘Certificate Policy’.

Title: Certificate Policy - Siemens Root CA v3 2016
OID: 1.3.6.1.4.1.4329.99.1.1.17.0
Expiration: This version of the document is the most current one until a subsequent release.

The set of all documents describing the Siemens PKI is referred to under the OID 1.3.6.1.4.1.4329.7.99

[2] The Issuing CAs 2020 are cross signed by QuoVadis Enterprise CA 3 G3 governed by the Digicert CPS located at https://www.quovadisglobal.com/repository.

The Issuing CAs 2021 are cross signed by Siemens Intermediate CA 2021 governed by the Entrust CPS located at https://entrust.net/cps.

1.3 PKI Participants

PKI Participants are Siemens Certification Authorities, Registration Authorities, Subjects, and Relying Parties. The Siemens PKI is intended for the use within the Siemens fleet of companies. Subscribers are either companies under direct control of Siemens or bound to Siemens with Long term Service Agreements. Subjects are either employees or business partners of the subscribers. The subscribers delegate parts of their duty to the subjects.

1.3.1 Certification Authorities

A graphical overview of the CA hierarchy is depicted in figures 1 – 3 .Figure 1: Siemens PKI hierarchy 2020.

1.3.1.1 Root CA

Siemens PKI architecture has a two and three-tier CA structure. This architecture allows the Root CA to be stored off-line.

- Siemens CA PKI 2020 – Two tiers
- Siemens CA PKI 2021 – Three tiers
- Siemens CA PKI 2023 – Three tiers

The Siemens Root CA performs the signing, issuance, and revocation of Certificates used to establish and authenticate a Siemens Intermediate CA. The Siemens Root CA only issues CA Certificates. The Siemens Root CA is also used for signing the CA's CRL.

1.3.1.2 Intermediate CAs – ICA’s

The Siemens Intermediate CA performs the signing, issuance, and revocation of certificates used to establish and authenticate a Siemens Issuing CAs. The Siemens Intermediate CA only issues CA Certificates. The Siemens Intermediate CA is also used for signing Issuing CA's CRL.

1.3.1.3 Issuing CAs

The Siemens Issuing CAs issue Certificates to End Entities and manage and revoke End Entity Certificates. The Siemens Issuing CA is also used for signing End Entities CRLs.

1.3.2 Registration Authorities

For person related certificates Siemens CA may delegate registration of End Entities to two types of RAs. The Enterprise RAs are part of the Siemens organization:

- Corporate ID Card Office (also called “Local Registration Authority” or “LRA”) generally for Identification and Authentication of initial Certificate Applicants;
- Electronic PKI Self-Service (“PKISS”) generally for Identification and Authentication of re-keying of existing Certificates.

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. Establishing an environment and procedure for distributing to Subjects their Activation Data, Key Pairs and Certificate on media (“Personal Security Environment” or “PSE”);
5. Validation of Certificate revocations; either at the Subject’s request or upon the CAs (or RAs) own initiative.
6. 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 (persons or functions) is not delegated to a third party.

1.3.3 Subscribers

Subscriber is either a Siemens as legal entity or a member of the Siemens fleet of companies, which applies for and owns the End Entity Certificates. Responsible for the key and the content of the End Entity Certificate is the subscriber. However, Siemens delegates rights to dedicated persons and functions that then act on behalf of Siemens (subjects). 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 contains incorrect information or Subscriber's Private Key or the Activation Data controlling its access has been lost or when Subscriber has reason to believe that the Private Key has been accessed by another individual or otherwise compromised;
3. acknowledgement of receipt or assent to Subscriber responsibilities.

1.3.4 Subject (End Entity)

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

The subject
(1) is named or identified in the respective element of the Certificate issued to this entity, and
(2) owns the Private Key that corresponds to the Public Key listed in that Certificate.

Subject's responsibilities include:

1. take all reasonable and necessary precautions to prevent loss, disclosure, modification or unauthorized use of Subject's Private Key or the Activation Data controlling its access;
2. use Certificates only for the purpose of doing business for or with Siemens, for the applications supported by the CA and for the duration of the Subject's employment or agency;
3. use only Key Pairs bound to valid Certificates; and
4. cease use of the Private Key after revocation or expiration of the Certificate.

1.3.5 Relying Parties

A "Relying Party" is a PKI Participant who uses a Certificate to obtain the Subject's Public Key and is in a position to rely on the assurances in the Certificate. When an individual is relying on a Certificate for his or her own business or personal use, the individual is the Relying Party. When an individual is acting on behalf of an employer or other principal, however, the employer or principal is the Relying Party. When a device and application relying on Certificates are under the control of an organization and individuals acting on behalf of the organization, then the Relying Party is the controlling organization.
For the purpose of this CP, the scope of Relying Parties is limited to persons (individuals or legal entities) who have entered into an applicable agreement defining and controlling the potential representations, warranties and liability of the Siemens Issuing CAs and other PKI Participants.

Relying Party responsibilities include:

1. perform cryptographic operations properly: verification of Digital Signatures by referring to Subject's Public Key listed in a valid 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 ("OSCP");
3. assent to the terms of an applicable agreement required as a condition to relying on the Certificate.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

The Certificates signed by the Siemens Root CA are approved for the following usages:

Certificate	Use
Root CA Certificate	This Certificate is signed by the Root CA itself and only approved for signing the CA Certificates of Issuing CA, the Root CA´s CRL and OCSP signer certificates.
Intermediate CA Certificates (ICAs)	This Certificate is signed by the Siemens Root CA itself or an authorized Cross Signer only approved for signing the CA Certificates of Intermediate CAs, the Intermediate CA´s CRL and OCSP signer certificates. In Figure 2 the current Authorized Cross signer are depicted.
Issuing CA Certificates	These Certificates are approved only for the signing of the End-Entity Certificates, the Issuing CA´s CRL and OCSP signer certificates.

The approved usages of keys and certificates signed by the respective Issuing CAs can be found in the respective CPSs.

1.4.2 Prohibited Certificate Usage

All Certificate usages not listed in 1.4.1 are prohibited.

1.5 Policy Administration

Siemens CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Siemens CA conforms to the current version of the Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates (“Code Signing Minimum Requirements”) published at https://aka.ms/csbr. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.5.1 Organization Administering the Document

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

Siemens Aktiengesellschaft (“Siemens AG”)
Cyber Security (“CYS”)
Otto-Hahn-Ring 6, 81739 Munich, GERMANY
E-mail: contact.pki@siemens.com
Website: https://www.siemens.com/pki

1.5.2 Contact Person

Questions about this CP may be sent to:

Siemens AG
CYS INF NG
Attn: Siemens PKI
Otto-Hahn-Ring 6, 81739 Munich, GERMANY
E-mail: contact.pki@siemens.com
Website: https://www.siemens.com/pki

Certificate Problem Reports shall be sent to: certificate-problem-report@siemens.com

1.5.3 Person Determining CP and CPS Suitability for the Policy

The Policy Management Authority (PMA) of Siemens in CP §1.5.1 and CP §1.5.2 determines CP and CPS suitability for the policy.

1.5.4 CP and CPS Approval Procedures

A risk assessment is carried out annually 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 CPSs will be reviewed annually regarding consistency with the actual PKI processes and services (see also §8).

This document is accepted and approved by the Head of Siemens CYS.

2 Publication and Repository Responsibilities

The Siemens CA makes its CP, CPSs, Certificate(s), CRL publicly available through the Siemens Website and additional appropriate communication channels.
In addition, it maintains an online accessible repository of Certificate revocation information.

The website can be reached at: http://www.siemens.com/pki.

2.1 Repositories

Siemens CA Repositories are operated either by Siemens CA itself or by trusted service provider(s).

The Repository responsibilities include:

1. accurately publishing information;
2. publishing and archiving Certificates;
3. publishing the status of Certificates;
4. availability to the CAs, RAs, Subjects and Relying Parties during the period of availability specified in Siemens PKI documentation;
5. promptness or frequency of publication; and
6. security of the Repository and controlling access to information published on the Repository to prevent unauthorized access and tampering.

Subjects and Relying Parties have access to:

- Certificate Revocation List (CRL) via:
  - HTTP: http://ch.siemens.net/pki? <GID of Issuing CA>.crl
  - LDAP: ldap://cl.siemens.net/CN=<GID of Issuing CA>,L=PKI?certificateRevocationList
  - LDAP: ldap://cl.siemens.com/CN=<GID of Issuing CA>,o=Trustcenter?certificateRevocationList

- Online certificate status information via:
  - HTTP: http://ocsp.siemens.com

2.2 Publication of Certification Information

The Siemens CA publishes the publicly available information at http://www.siemens.com/pki/.

At a minimum the following information is published:

❑ all required Certificates to trust the Root CAs

❑ all Intermediate and Issuing CA certificates,

❑ issued encryption certificates

❑ revocation information for Siemens Root, Intermediate and Issuing CA certificates and for End Entity certificates

❑ possible compromise of used algorithms or associated parameters

The following information is available for Siemens Community, Server Community and Business Partner Community.

The Siemens PKI conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org.

In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document. This applies to the S/MIME baseline requirements as well as the TLS baseline requirements to the extent possible. An S/MIME Certificate for the purposes of this be identified by the existence of an Extended Key Usage (EKU) for id-kp-emailProtection (OID: 1.3.6.1.5.5.7.3.4) and the inclusion of a rfc822Name or an otherName of type id-on-SmtpUTF8Mailbox in the subjectAltName extension.

2.3 Time or Frequency of Publication

Updates to the CP and the CPSs are published in accordance with the definitions in §9.12 of this document.

The CP/CPS will be updated and published at least once a year and updates will be reflected in an incremented version number.

Certificates are published upon issuance.

Certificate status information is published on a daily basis.

2.4 Access Controls on Repositories

Information published in the Repository (https://siemens.com/pki) is accessible with read-only access through the Siemens Intranet or Internet under existing procedures and policies.

Siemens CA 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 §7 of the respective CPS for each Certificate type.

3.1.2 Need of Names to be Meaningful

3.1.2.1 CA Names

The CN must be stated as the full name of the CA. A CA name indicates its purpose.

3.1.2.2 End Entity Names

EE Certificates contain commonly understood names permitting the determination of the identity of the individual.

3.1.3 Anonymity or Pseudonymity of Subjects

3.1.3.1 CA Names

The use of pseudonyms for CA names is not permitted.

3.1.3.2 End Entity Names

For personal EE Certificates anonyms or pseudonyms in the subject field of the certificate are not permitted, i.e. names must be the Subject’s true personal name. For functional EE Certificate’s the Subject must contain an unique e-mail address and serialnumber which allow to find an unique responsible person (sponsor).

3.1.4 Rules for Interpreting Various Name Forms

No special regulation.

3.1.5 Uniqueness of Names

3.1.5.1 CA Names

Siemens CA ensures that Root CA and Issuing CA names are unique.

3.1.5.2 End Entity Names

Siemens Issuing CAs shall ensure during the enrollment process that uniqueness of certificates is guaranteed.
This is realized by assigning a unique serial number to the X.509 certificates.

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. Siemens CA 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, Siemens CA may reject or suspend any Certificate Application or revoke issued certificates because of such dispute.

3.2 Initial Identity Validation

Applicants for certificates are end entities. The applicant always acts on behalf of the subscriber (Siemens).

A Certificate shall be issued to a Subject only when the Subject has submitted a Certificate Request and is able to prove to the CA possession of the corresponding Private Key.

3.2.1 Method to Prove Possession of Private Key

Certificate Requests are only accepted as PKCS#10 Certificate Requests. Signature verification of a PKCS#10 request constitute sufficient proof of possession of the corresponding Private Key.

If a Key Pair is generated by the Siemens CA on behalf of a Subject (e.g., where a pre-generated Key Pair for decryption is placed on a Secure Signature Creation Device such as a smart card), this requirement is not applicable.

3.2.2 Identification and Authentication of Organization Identity

Only applicants belonging to the Siemens organization can request certificates.

3.2.3 Identification and Authentication of Individual Identity

For all End Entity Certificates, Siemens CA shall cause the respective RA to confirm that:

- the Certificate Applicant is the person identified in the Certificate Application;
- the Certificate Applicant rightfully holds the Private Key corresponding to the Public Key to be listed in the Certificate; and
- the information to be included in the Certificate is accurate, except for non-verified Subject information.

In order to make this confirmation, RAs use information in the Siemens human resources databases to approve or reject Certificate Applications.

Prior to issuance of a Certificate, Certificate Applicants shall either be:

1. personally present before an authorized RA or its designated representative to check the identity of the Certificate Applicant against a well-recognized form of government-issued or corporate identification (e.g., a passport, driver’s license, or Siemens corporate identity card);
2. checked through appropriate Validation in the PKISS process via authentication on corporate Identity Provider;
3. electronic form-based process used by the server RA.

3.2.4 Non-verified Applicant Information

Only verified Application Information is included into the certificate.

3.2.5 Validation of Authority

If the applicant for a Certificate containing subject identity information is an organization, the RA will use a reliable method of communication to verify the authenticity of the applicant representative’s certificate request.

Applicants are limited to the closed group as described in 3.2.2, and may apply for:

- Personal certificates, only for their own identity.

- Team, group or organizational certificates by belonging to this community, proven by a reliable data source as described in the related CPS in 3.2.3.1.

- TLS certificates of pre-registered domains

Applicant MAY be allowed to specify the individuals who may request Certificates as delegates.

3.2.6 Criteria for Interoperation between Communities of Trusts

Siemens CA is member of the European Bridge CA and exchanges PKI related information with its partners.

A detailed description of the interoperation of CAs is described in ‘Certificate Policy Siemens CA 6/15/2021 1.13’.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Root CA

Before an Issuing CA Certificate expires, the Key Changeover Procedure shall be initiated. The procedure is performed by trusted personnel under dual control in a secured environment.

3.3.2 Intermediate CA

Before an Intermediate CA Certificate expires, the Key Changeover procedure shall be initiated. The procedure is performed by trusted personnel under dual control in a secured environment.

3.3.3 Issuing CA

Before an EE Certificate expires, the Re-key Procedure shall be initiated. A Certificate Request on the basis of the current EE Key Pair shall be send to the respective Issuing CA (via the Self-Service-Portal).

If the Certificate to be replaced has already expired or has been revoked, a new identification process shall be started.

3.4 Identification and Authentication for Revocation Requests

3.4.1 Root CA

Revocation of Issuing CA Certificates shall only be performed manually by Siemens CA trusted employees under dual control.

3.4.2 Intermediate CA

Revocation of Intermediate CA Certificates shall only be performed manually by Siemens CA trusted employees under dual control The procedure is performed by trusted personnel under dual control in a secured environment.

3.4.3 Issuing CA

The identification and authentication procedures for a revocation request of EE Certificates are the same as for initial identity validation.

4 Certificate Lifecycle Operational Requirements

This section addresses the administration of Siemens Root CA's, Intermediate and Issuing CAs' Key Pairs throughout the operational life cycle of the Root CA , Intermediate 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 CA

The Siemens CA management decides when a new Intermediate CA is to be created and to be signed by the Siemens Root CA.

4.1.1.2 Intermediate CA

The Siemens CA management decides when a new Issuing CA is to be created and to be signed by the Siemens Intermediate CA.

4.1.1.3 Issuing CAs

Certificate Applicants can only be member of the *Siemens Community or Business Partner*

Details are specified in the CPS for issuing CAs.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 Root CA

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

- ❑ A name for the Root CA in accordance with Regulations in section 3.1, "Naming", of this CP
- ❑ Duration of the Root CA Certificate
- ❑ Date of the request for the Root CA
- ❑ Certificate Profile of the new Root CA
- ❑ CPS for the new Root CA and Intermediates CA
- ❑ Profile of new Root CA is self-signed.

4.1.2.2 Intermediate CAs

For Intermediate CA Certificates to be generated, following information shall be documented:

- ❑ A name for the Intermediate CA in accordance with Regulations in section 3.1, "Naming", of this CP
- ❑ Date of the request of the Intermediate CA Certificate
- ❑ Duration of the Intermediate CA Certificate, which cannot exceed the duration of the Root/Intermediate CA's Certificate
- ❑ Certificate Profile of the new Intermediate CA
- ❑ Profile of the new Intermediate CA to be signed either by a new Root CA or a Trusted cross signer Intermediate CA.

4.1.2.3 Issuing CAs

For the Issuing CA Certificates to be generated, following information shall be documented:

- ❑ A name for the Issuing CA in accordance with Regulations in section 3.1, "Naming", of this CP
- ❑ Date of the request
- ❑ Duration of the Issuing CA Certificate, which cannot exceed the duration of the Intermediate CA's Certificate

- CPS for the new Issuing CA
- Certificate Profile of the new Issuing CA and
- Profiles of the end-entity Certificates to be signed by that new CA
- Profile of the new Issuing CA to be signed by a new or existing Intermediate CA.

4.1.2.4 End Entity Certificate Applicants

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
- demonstrating to the respective RA that the Certificate Applicant has possession of the Private Key corresponding to the Public Key included in the Certificate Application and
- notifying Certificate Applicants of the relevant Subject responsibilities for usage of the Private Key and Certificates

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

Siemens CA ensures that Certificate Applicants (= "subjects") are properly identified and authenticated.

1. Validation of mailbox authorization or control: The CA SHALL verify that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate by validating authority over mailbox via domain. The CA SHALL use only the approved methods in Section 3.2.2.4 of the TLS Baseline Requirements to perform this verification.

2. Authentication of organization identity: Completed validation of organization identity in accordance with Section 3.2.3 SHALL be obtained no more than 825 days prior to issuing the Certificate.

Validation of authority in accordance with Section 3.2.6 SHALL be obtained no more than 825 days prior to issuing the Certificate, unless a contract between the CA and the Applicant specifies a different term. For example, the contract MAY include the perpetual assignment of roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

3. Authentication of individual identity: Completed validation of Individual identity in accordance with Section 3.2.4 SHALL be obtained no more than 825 days prior to issuing the Certificate.

A prior validation SHALL NOT be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

4.2.2 Approval or Rejection of Certificate Application

After a Certificate Applicant submits a Certificate Application, Siemens CA shall approve or reject it.

Siemens CA verifies that the Certificate Application is complete, accurate and duly authorized. If validation fails, the Certificate Application is rejected.

For EE Certificates Siemens CA these tasks can be delegated to respective Siemens RAs.

4.2.3 Time to Process Certificate Applications

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

4.2.4 Certificate Authority Authorization (CAA)

Siemens has stopped the issuance of publicly trusted TLS certificates as of October 1, 2019. Until then Siemens checked for a Certificate Authority Authorization (CAA) record for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for any records found. If Siemens issues, it does so within the TTL of the CAA record, or 8 hours, whichever is greater. When processing CAA records, Siemens processes the issue and issue wild records as specified in RFC 6844. Siemens will not issue a Certificate if an unrecognized property is found with the critical flag.

Siemens may not check CAA records for the following exceptions:

(I) For Certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
(II) For Digital Certificates issued by a Technically Constrained Subordinate CA Certificate, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
(III) If the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

Siemens treats a record lookup failure as permission to issue if:

(I) the failure is outside the CA's infrastructure.
(II) the lookup has been retried at least once; and
(III) the domain's zone does not have a DNSSEC validation chain to the ICANN root.
Siemens documents potential issuances that were prevented by a CAA record and will dispatch reports of such issuance requests to the contact stipulated in the CAA iodef record(s), if present.
Siemens support mailto: and https: URL schemes in the iodef record. The identifying CAA domain for Siemens is 'siemens.com'. CAA record checking results are logged in the Siemens Server Registry Authority (ServerRA).

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

4.3.1.1 Root and Intermediate CA actions during Certificate issuance

To ensure proper security of the Root CA Key Pair, the computer running Root CA services is not connected to the network and is kept in an offline security vault which complies with security standards for cryptographic modules set forth in chapter 6.2.1.

Procedures are established and approved in order to ensure integrity and non-repudiation of Certificate Requests and Certification of the Issuing CA's Public Key. Access to Siemens Root CA devices is granted only for authorized personnel. Furthermore, M*N authentication is used to ensure proper access to the Root CA services.

4.3.1.2 Issuing CA actions during Certificate issuance

A Certificate is created and issued using secure means after the approval of a Certificate Application. Siemens CA shall:

1. generate for the Subject a Certificate based on the information in the Certificate Application after its approval
2. check authorization of the respective RA through a secure server and
3. deliver the Certificate, Key Pairs and Activation Data (collectively "Personal Security Environment" or "PSE") to Subject through the respective RA using secure means. If a PKCS#10 Request was received only the Certificate is delivered to Subject

These procedures are also used for the issuance of Certificates in connection with the submission of a request to replace (i.e., re-key) a Certificate.

4.3.2 Notification to Subject by the CA of Certificate Issuance

Upon Certificate generation, the respective CA/RA has to inform Subjects that their Certificates are available and the means for securely obtaining their Certificates.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

4.4.1.1 Root CA

Certificate acceptance shall take place as part of or because of the CA Creation Ceremony.

4.4.1.2 Intermediate CA

Same as described in section 4.4.1.1

4.4.1.3 Issuing CA

Upon issuance of Certificates, Activation Data (e.g., Subject's PIN) shall be made available to Subjects, through a message (e-mail or otherwise). The Subject shall securely obtain the Key Pair and/or Certificate through the respective RA.

4.4.2 Publication of the certificate by the CA

CA Certificates will be published according to their distribution point (AIA), as outlined in the certificate profile.

The publication of End Entity Certificate is stipulated in the CPS of the issuing CA.

4.4.3 Notification of Certificate issuance by the CA to other entities

Siemens CA is member of the European Bridge CA and provides certificate issuance information to its partners.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

4.5.1.1 Root CA Private Key and Certificate Usage

The Root CA Private Key is only used for:

- ❑ Issuance of Siemens Root CA's Certificates
- ❑ Issuance of Siemens Root CA's CRLs
- ❑ Issuance of Siemens Intermediate CA Certificates
- ❑ Issuance of Siemens Intermediate CA's CRLs
- ❑ Issuance of OCSP signer certificates

4.5.1.2 Intermediate CA Private Key and Certificate Usage

The Intermediate CA Private Key is only used for:

- ❑ Issuance of Siemens Issuing Certificates
- ❑ Issuance of Siemens Issuing CA's CRLs
- ❑ Issuance of OCSP signer certificates

4.5.1.3 Issuing CA Private Key and Certificate Usage

The Issuing CA Private Key is only used for:

- ❑ Issuance of Certificates to End Entities
- ❑ Issuance of Siemens Issuing CA's CRLs
- ❑ Issuance of OCSP signer certificates
- ❑ Protection (encryption) of centrally generated private keys

4.5.1.4 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 Siemens Root CA Certificate, Intermediate and the Issuing CA Certificate and any other Certificates within the corresponding Certificate Chain and
- ❑ securely obtain and verify the validity, suspension or revocation of the certificate 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 with an extended validity to an entity without changing the Public Key or any other information in the Certificate.

As a matter of principle Certificate Renewal is not offered for Siemens Internal PKI.

4.6.1 Circumstance for Certificate Renewal

Not supported for Siemens Internal PKI.

4.6.2 Who may request renewal?

No supported for Siemens Internal PKI.

4.6.3 Processing Certificate Renewal Request

No supported for Siemens Internal PKI.

4.6.4 Notification of new Certificate Issuance to Subject

No supported for Siemens Internal PKI.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No supported for Siemens Internal PKI.

4.6.6 Publication of the Renewal Certificate by the CA

No supported for Siemens Internal PKI.

4.6.7 Notification of Certificate Issuance by the CA to the Entities

No supported for Siemens Internal PKI.

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 replaces an existing Key Pair.

For Certificate Re-keying the same requirements apply as for §4.3. Certificate Issuance. Previously validated information must not be reused.

4.7.1 Circumstances for Certificate Re-key

The Re-key Process must only be requested if the ownership of the affected Certificate is documented by a Certificate that is still valid.

4.7.2 Who may request certification of a new Public Key?

I. Re-keying of an Intermediate CA Certificate
Rekeying of Intermediate CA Certificates must not be performed.

II. Re-keying of an Issuing CA Certificate
Rekeying of Issuing CA Certificates must not be performed.

III. Re-keying of End Entity Certificates
No additional stipulation.

4.7.3 Processing Certificate Re-keying Requests

No additional stipulation.

4.7.4 Notification of new Certificate Issuance to Subject

No additional stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No additional stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

No additional stipulation.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

No additional stipulation.

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.

Certificate modification shall not be performed.

4.8.1 Circumstance for Certificate Modification

Not applicable.

4.8.2 Who may request Certificate modification?

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of new Certificate Issuance to Subject

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for revoking a subscriber certificate

Siemens will follow the terms and conditions of its cross-signing partner. Furthermore, there can be the following technical reasons for revoking a Certificate:

- ❑ the key lengths or algorithms used no longer seem secure enough
- ❑ a change in the CA hierarchy is necessary, and
- ❑ the Policy Management Authority recognizes an acute threat of a yet unknown technical nature

Furter stipulation may be added in CPS.

4.9.1.2 Reasons for revoking a subordinate CA certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies the Issuing CA that the original Certificate Request was not authorized and does not retroactively grant authorization;

3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;

4. The Issuing CA obtains evidence that the Certificate was misused;

5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable CP and/or CPS;

6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;

7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or

9. Revocation is required by the Issuing CA's CP and/or CPS.

4.9.2 Who can request revocation?

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties MAY submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke a Certificate.

4.9.3 Procedure for Revocation Request

Siemens CA supports the secure and authenticated revocation of EE Certificates and provides a means of rapid communication of such revocation through the issuance of CRLs published on an as-needed basis. Contact information for Certificate Problem Reports are to be found in CP §1.5.2.

Upon the revocation of an Issuing CA Certificate or EE Certificate, the newly revoked Certificate is recorded in a CRL that is published within 24 hours.

A requestor of revocation of an EE Certificate is required to communicate the request to Siemens CA through its respective RA to initiate revocation of the Certificate, which shall be performed promptly. Communication of such revocation request shall be in accordance with CP §3.4.

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

Siemens CA processes the revocation request and any certificate problem report within 24 hours after its submission.

Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the Certificate will be revoked, and if so, a date on which the CA will revoke the Certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation SHALL NOT exceed the time frame set forth in Section 4.9.1. The date selected by the CA SHOULD consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);

2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);

3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;

4. The entity making the complaint (for example, a complaint from a law enforcement official should be addressed with higher priority); and

5. Relevant legislation.

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency

For the status of Subscriber Certificates: the CA SHALL update and reissue CRLs every 24 hours, and the value of the nextUpdate field SHALL NOT be more than ten days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates: the CA SHALL update and reissue CRLs at least:

1. once every twelve months; and

2. within 24 hours after revoking a Subordinate CA Certificate.

The value of the nextUpdate field SHALL NOT be more than twelve months beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

CRLs shall be posted to the repository within a reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-line Revocation/Status Checking Availability

A Certificate status checking service based on OCSP-Responder implementing RFC2560, RFC5019 and RFC6960 may be offered. When provided, the OCSP responder supports HTTP GET operation for requesting the status of a certificate. The returned status is always based either on the latest available CIL or directly on information within the CA databases. This implementation can lead to the situation, that according to the OCSP responder a certificate is “revoked” but not listed as revoked on the CRL at that moment. Eventually after a maximum of 24 hours, the responses will be similar. The OCSP responder receives a request for the status of a certificate that has not been issued, then the responder answers according to the RFC6960. Siemens Issuing CAs monitors the OCSP responders log files for signs of unauthorized certificates.

4.9.10 On-line Revocation Checking Requirements

Relying Parties shall check Certificate status by consulting the most recent CRL published by Siemens CA or the OCSP responder.

OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds SHALL be equal to one hour, and a difference of 86,400 seconds SHALL be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates:

1. OCSP responses SHALL have a validity interval greater than or equal to eight hours;

2. OCSP responses SHALL have a validity interval less than or equal to ten days;

3. For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate; and

4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates, the CA SHALL update information provided via OCSP:

1. at least every twelve months; and

2. within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for the status of a Certificate serial number that is "unused", then the responder SHOULD NOT respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5, the responder SHALL NOT respond with a "good" status for such requests.

The CA SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

A Certificate serial number within an OCSP request is "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject, or "unused" if otherwise.

4.9.11 Other Forms of Revocation Advertisements Available

Additional forms or revocation advertisements are only available in certain situations if necessary.

4.9.12 Special Requirements for Private Key Compromise

If Siemens CA has reason to believe there has been a compromise of a CA's Private Key, it shall notify potential Relying Parties and Cross Signing parties will be notified by established mechanisms.

If a Subject has a reason to believe that there has been a compromise of an EE Private Key, then it will notify its respective RA to take appropriate action, including request for revocation.

4.9.13 Circumstances for Suspension

Certificate Suspension for Certificates issued by Siemens CA is not provided.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.

As well compare chapter 4.9.9.

4.10.2 Service Availability

The OCSP service and the CRLs shall be available twenty-four (24) hours a day, seven (7) days a week, except in case of Force Majeure Events (CP §9.16.5). The OCSP service is constantly being monitored to ensure that the response time stays below ten (10) seconds per request.

For high-priority Certificate Problem Reports compare CP §4.9.3.

4.10.3 Optional Features

No optional features are supported.

4.11 End of Subscription

As the only subscriber of the Siemens CA is Siemens, the Siemens CA ceases operation in case the Subscription ends.

4.12 Key Escrow and Recovery

Key Escrow is only performed for end-entity encryption keys.

The Subject’s Private Key can be recovered for the Subject or for a third party under following conditions:

- The subject can request recovery at any time
- The supervisor of a Subject can request recovery if the Subject has left the company
- Compliance or Legal office can request recovery with consent of the PMA

5 Management, Operational, and Physical Controls

Management, operational, and physical controls are defined in accordance with [ETSI EN 319 411-1] and [ETSI EN 319 401].

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

Siemens CA is operated according to the Information Security Management System ("ISMS") of Siemens, which supports the security requirements of this CPS. This ISMS is based on ISO27001. The following gives an overview of the security requirements for the Siemens Root CA.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The site is certified according to TÜV Trusted Site Infrastructure Level 4.

5.1.2 Physical Access

The site is certified according to TÜV Trusted Site Infrastructure Level 4.

5.1.3 Power and Air Conditioning

The site is certified according to TÜV Trusted Site Infrastructure Level 4.

5.1.4 Water Exposure

The site is certified according to TÜV Trusted Site Infrastructure Level 4.

5.1.5 Fire Prevention and Protection

The site is certified according to TÜV Trusted Site Infrastructure Level 4.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored in specially secured areas at 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).

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

Routine backups of critical system data, audit log data, and other sensitive information are performed. Offsite backup media are stored in a physically secure manner using the Siemens disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Roles for Siemens Root CA's operation include all personnel, who have access to or control of Root CA "back end" operations that may materially affect:

- ❑ the validation of information in Certificate Applications;
- ❑ the acceptance, rejection, or other processing of Certificate Applications, Re-key or Revocation Requests, or Enrollment Information, and
- ❑ the Issuance or Revocation of Certificates, including access to restricted portions of the Repository.

Personnel in trusted roles in the Root CA operation include, without limitation:
Trusted Roles as defined in ETSI TS 319 401 V2.2.1 / REQ-7.2-15:

- ❑ Security Officers
- ❑ System Administrators
- ❑ System Operators
- ❑ System Auditors

Additional Trusted Roles at Siemens CA:

- ❑ Data Protection Officer
- ❑ Corporate Information Security Officer (CISO)

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 require at a minimum, that two trusted employees have either physical or logical access to the device or location:

- ❑ 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.

5.2.3 Identification and Authentication for each Role

Identification and Authentication of persons to safety-relevant areas is performed by two-factor-authentication. Access to critical systems is controlled by smart cards. In the control systems the authorization of the users are managed by roles. Controls are implemented to protect against equipment, information, media and software relating to the CA services being taken off-site without authorization.

5.2.4 Roles Requiring Separation of Duties

Any Trusted Role for Siemens CA operations requires the presence and participation of at least two trusted employees. Therefore, no stipulation for separation of duties within one role is necessary.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Persons seeking employment for Trusted 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.

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 Role.

5.3.3 Training Requirements

All personnel performing managerial duties with respect to the operation of the Siemens CA 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.

5.3.4 Retraining Frequency and Requirements

Personnel in Trusted 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.

5.3.5 Job Rotation Frequency and Sequence

No stipulation regarding job rotation frequency and sequence are set forth.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

No independent contractors, external consultants or apprentices shall be employed for Siemens CA operation to fill Trusted 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 Roles.

5.3.8 Documents Supplied to Personnel

Personnel in Trusted Roles shall be provided with the Siemens AG's "Corporate Information Security Guide", 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 check of parameter modifications, configuration changes, etc. to the components of the CA systems. The logging processes focus particularly on the following:

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

The data collected is analyzed automatically. The collected data can be accessed via the Card Management System (for Certificate lifecycle data) or file based (for CA key lifecycle data).

5.4.1 Types of Events Recorded

Siemens CA 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 CA records 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 person making the journal entry; and
3. Description of the entry.

5.4.2 Frequency of Processing Audit Logging Information

Audit und logging data have to be controlled by the PMA after all CA events. Siemens CA make the records generated under §5.4.1 available to its Qualified Auditor as proof of the CA’s compliance with these Requirements.

5.4.3 Retention Period for Audit Logging Information

Audit logs are retained onsite unlimited. At termination of the Siemens CA, all data will be transferred to the Siemens central archiving service and deleted after 30 years.

5.4.4 Protection of Audit Logs

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering. Manual audit information shall be protected from unauthorized viewing, modification and destruction.

5.4.5 Backup Procedures for Audit Logging Information

A full backup is performed after each CA Ceremony. After that the system remains offline.

5.4.6 Collection System for Monitoring Information (internal or external)

The collection and storage of audit and technical log data is located in the secure facilities.

5.4.7 Notification to Event-causing Subject

If a person or a device under the person’s control causes an audit event, which results in an alarm, or creates another anomalous audit log entry or is otherwise detected, the first response is to prevent any further intrusion by the person or device.

The audit event will be analyzed in order to identify the intruding person or device as quickly as possible. This analysis includes close scrutiny of all relevant audit events. Actions according to the Siemens Incident Management Processes shall be taken.

5.4.8 Vulnerability Assessments

As part of annual Siemens-internal security assessments, the potential vulnerability of the Siemens CA is checked. Furthermore, the current vulnerability status is documented with the help of risk assessment, which is documented and treated in accordance with ISMS Regulations.

5.5 Records Archival

5.5.1 Types of Records Archived

The types of records that are archived include the categories of audit log information listed below:

- ❑ 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 Siemens CA for commercial, legal or organizational purposes.
  - *Automatic Audit Data* consists of audit, billing 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;

    Billing information provides the basis for charging for the services rendered in accordance with the services level agreement(s) ("SLA") and also provides quantitative revenue information;

    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 §5.5.1 is at least six weeks. The retention period for Automatic Audit Data in §5.5.1 is at least ten years, subject to differing contractual requirements and to the clarification that statistical information is retained for at least one year. Manual Audit Data is retained for at least ten years. Every retention period is subject to German data privacy law and may be changed without further to reflect changing legal requirements.

5.5.3 Protection of Archived Audit Logging Information

Protection of archived records is performed in accordance with Siemens ISMS. Archived records are located in multiple locations. The security infrastructure at these locations and special monitoring of the backup facilities and archived records includes different methods to protect against theft or unauthorized destruction, alteration or loss, which are set forth in detail in the ISMS Regulations.

5.5.4 Archive Backup Procedures

Archive Backup Procedures are implemented according to ISMS Regulations. 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 and Automatic Audit Data and related software.

5.5.5 Requirements for Time-Stamping of Record

No special stipulation.

5.5.6 Archive Collection System (internal or external)

All archived data is stored internally and on an off-site data storage for disaster recovery.

5.5.7 Procedures to Obtain and Verify Archived Information

The procedures to obtain and verify saved records are implemented according to ISMS Regulations. Automated saving procedures contain control steps that confirm that stored audit logging information can later be accessed and read again.

5.6 Key Changeover

Details are described in the respective CPSs.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

When emergency incidents and compromises occur during operation of the CA, an Emergency Team is established in accordance with the ISMS Regulations. This Emergency Team gathers information, assesses the risks, develops a procedure, and proposes and implements that procedure with approval from Siemens CISO. The considerations about which procedure is most appropriate focus on the consequences of the specific incident or compromise and any resulting allocation of liability among the PKI Participants under the law or contract.

The ‘Siemens PKI emergency handbook’ covers the topics as listed below:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA’s plan to maintain or restore the CA’s business operations in a timely manner following interruption to or failure of critical business processes
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA’s main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.”

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

If the Siemens CA´s computing resources, software or data are corrupted (e.g., by natural disaster or hostile attack), the Siemens CA will report such occurrence to the PMA. Handling procedures will be implemented for actual or threatened hostile attacks.

If only the Root CA is affected, the Issuing CA can continue to operate, because:

(i) replacement hardware will likely 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.

5.7.3 Entity Private Key Compromise Procedures

If Siemens Root CA’s Private Key is compromised or suspected to be compromised, following procedures shall be performed:

- ❑ inform Subjects, Relying Parties and European Bridge CA and cross signing CA partners;
- ❑ indicate that certificates and revocation status information issued using this Root CA key may no longer be valid;
- ❑ terminate the Certificate and CRL Distribution Service for Certificates and CRLs issued using the compromised Private Key, and

- ❑ request the revocation of all affected Certificates.

5.7.4 Business Continuity Capabilities After a Disaster

The High Availability of Certification Services provided by Siemens CA is guaranteed by the implementation of the redundant installation of the system.

In the event of the corruption or loss of computing resources, software or data, an appropriate Disaster Recovery and Business Continuity Plan according to the ISMS Regulations shall rendered operational in a facility located in a separated area that is capable of providing CA services.

Re-establishment of critical services like Certificate Suspension/Revocation, Certificate Validation and Publication of CRLs will be done within a time scale of twenty-four (24) hours max. Full functionality will be provided within 30 days.

5.8 CA Termination

In the event that it is necessary for Siemens to terminate the CA service, Siemens CA shall notify Relying Parties, and other affected entities in advance of the CA termination via its website. Following termination plan should minimize disruption to Relying Parties:

- Publication of a notification to parties affected by the termination incl. European Bridge CA and cross signing CA partners;
- Revocation of the Certificate issued to Issuing CAs;
- Preservation of the CA's archives and records for the time periods required in this CPS;
- 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.

6 Technical Security Controls

Technical security controls are defined in accordance with [ETSI EN 319 411-1] and [ETSI EN 319 401].

Details are described in the CPS.

6.1 Key Pair Generation and Installation

Details are described in the CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Details are described in the CPS.

6.3 Other Aspects of Key Pair Management

Details are described in the CPS.

6.4 Activation Data

Details are described in the CPS.

6.5 Computer Security Controls

Details are described in the CPS.

6.6 Life Cycle Security Controls

Details are described in the CPS.

6.7 Network Security Controls

Details are described in the CPS.

6.8 Time Stamp Process

Details are described in the CPS.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificate Profile definitions for Siemens Issuing CA itself and the Subject Certificates issued by it and Certificate content requirements for issued Certificates are in accordance with

- ITU-T Recommandation [X.509 Version 3] and
- [RFC 5280]
- [ETSI EN 319 412-2]

Details are described in the CPS.

7.2 CRL Profile

Details are described in the CPS.

7.3 OCSP Profile

Details are described in the CPS.

8 Compliance Audit and Other Assessment

Siemens CA’s compliance to this CP and the CPSs will be checked annually. In addition, an annual asset classification of the PKI services and its components takes place, which is performed in accordance with the Siemens Enterprise Risk Management Process. This asset classification might lead to an adaption of the implemented security mechanisms and controls and to respective changes in CP and CPSs.

8.1 Frequency or Circumstances of Assessment

The Siemens CAs shall be audited and certified in compliance with ETSI EN 319 411-1. Audits are performed on an annual basis.

In addition to compliance audits, Siemens CA may perform or cause to be performed other assessments to ensure the trustworthiness of its trusted service providers or PKI Participants, including without limitation:

- At its sole discretion, Siemens CA may perform at any time an assessment on itself or RA or other PKI Participant in the event Siemens CA has reason to believe that the audited entity has not operated in accordance with stated security policies or procedures in PKI documentation.
- Siemens CA 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
- ❑ (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403 or ETSI EN 319 403-1
- ❑ Bound by law, government regulation, or professional code of ethics; and
- ❑ Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor’s Relationship to Assessed Entity

The assessor shall be organizationally independent of the assessed entity’s operational and policy authorities.

8.4 Topics Covered by Assessment

The scope of the compliance audit or other assessment of Siemens CA or other Siemens PKI Participants is the review of the design and operational effectiveness of the assessed entity’s controls covering a specified 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. Siemens CA 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 Siemens PKI, a corrective action plan shall be developed 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, Siemens CA shall evaluate the significance of such issues and determine the appropriate response.

Possible actions taken include those set forth in [RFC3647]:

- ❑ 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

Summary reports of the compliance audit shall be published together with the audit certificate.

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1. The CA SHALL make the Audit Report publicly available.

The CA SHALL make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, the CA SHALL provide an explanatory letter signed by the Qualified Auditor.

The Audit Report SHALL contain at least the following clearly-labelled information:

1. Name of the organization being audited;

2. Name and address of the organization performing the audit;

3. The SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;

4. Audit criteria, with version number(s), that were used to audit each of the Certificates (and associated keys);

5. A list of the CA policy documents, with version numbers, referenced during the audit;

6. Whether the audit assessed a period of time or a point in time;

7. The start date and end date of the Audit Period, for those that cover a period of time;

8. The point in time date, for those that are for a point in time;

9. The date the report was issued, which will necessarily be after the end date or point in time date;

10. (For audits conducted in accordance with any of the ETSI standards) a statement to indicate if the audit was a full audit or a surveillance audit, and which portions of the criteria were applied and evaluated, e.g., ETSI EN 319 401, ETSI EN 319 411-1 policy LCP, NCP or NCP+, ETSI EN 319 411-2 policy QCP-n, QCP-n-qscd, QCP-l or QCP-l-qscd; and

11. (For audits conducted in accordance with any of the ETSI standards) a statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as this document, and the version used.

An authoritative English language version of the publicly available audit information SHALL be provided by the Qualified Auditor and the CA SHALL ensure that it is publicly available.

The Audit Report SHALL be available as a PDF, and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report SHALL be uppercase letters and SHALL NOT contain colons, spaces, or line feeds. See https://www.ccadb.org/policy#51-audit-statement-content for more information.

8.7 Self-Audits

Siemens CA monitors adherence to its Certificate Policy, Certification Practice Statement, and the CA/B BRGs and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

8.8 Review of delegated parties

Not applicable.

9 Other Business and Legal Matters

Other business and legal matters generally address:

- fees to be charged for CA-related services (CP §9.1)
- financial responsibility of Siemens PKI Participants for:
  - (i) maintaining resources for ongoing operations and
  - (ii) paying judgments, awards, or settlements in response to claims asserted against them, including third party insurance coverage (CP/CPS §9.2)
- legal responsibilities and allocation of potential liability and risks among PKI Participants (CP/CPS §9.3 to CP/CPS §9.17)

9.1 Fees

For the Siemens Community, fees are charged for Certificate-related services and paid by the responsible Siemens entity. For the Business Partner Community, fees are charged for Certificate-related services and may be paid either by the Business Partner or by the Siemens Sponsor or Siemens entity doing, or planning to do, business with the Business Partner. For Server Community, fees are charged for Certificate-related services and paid by the responsible Siemens entity.

In all cases, the contractual agreement with the Siemens CA is decisive with regard to the fees.

9.2 Financial Responsibility

Unless otherwise explicitly agreed or explicitly provided for in a CP/CPS approved by Siemens CIO, Siemens CA´s liability to Relying Parties and any other entities, is limited against claims of any kind to the highest extend permitted by applicable law, including those of contractual nature, on a per Certificate basis regardless of the number of transactions, digital signatures, or causes of action arising out of or related to such Certificate or any services provided in respect of such Certificate and on a cumulative basis.
Subject to the foregoing limitations, Siemens CA's liability limit towards Relying Parties and any other entities for the whole of the validity period of a Certificate issued by Siemens CA (e.g. 6 years unless revoked) towards all persons with regard to such Certificate is limited by an amount defined by Siemens CIO, if not otherwise defined in the applicable contractual agreement.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information used by or transmitted to Siemens CA shall be classified according to Siemens Information Security Management System.

As a minimum the following information shall be treated confidential:

- ❑ Centrally generated EE Private Keys and Activation Data needed to use such Private Keys
- ❑ Transactional records (both full records and the audit trail of transactions)
- ❑ Audit records created or retained by Siemens CA, RA, or auditor
- ❑ Contingency planning and disaster recovery plans
- ❑ Security measures controlling the operations of Root CA and Siemens Issuing CA hardware and software and the administration of Certificate services and designated enrollment services
- ❑ Not specially marked information shall be considered confidential if it obviously contains business secrets or other Confidential Information

9.3.2 Information not within the Scope of Confidential Information

Information in Certificates, CRLs and other status information in the Repository are not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

Siemens CA and respective RA shall require its employees or contractors to observe the obligations to keep Confidential Information confidential, subject to CP §9.3.1. Subjects shall comply with applicable portions of CP §9.3.1.

9.4 Privacy of Personal Information

Siemens CA, and respective RAs, shall protect “Personal Data” of Certificate Applicants under applicable law and, if applicable, the "Binding Corporate Rules (BCR) for Siemens Group Companies and Other Adopting Companies for the Protection of Personal Data" with Circular No. 216 (“Binding Corporate Rules”).
Siemens CA and respective RA shall comply or cause its trusted service providers to comply with requirements of applicable national data privacy protection law when processing Personal Data in the Certificate Application or Certificate, including the law of a Member State implementing the European Union Directive 95/46/EC on Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data [EU95/46/EC].
Anonymous, pseudonymous, or other otherwise non-personal Data in Certificate Applications, Certificates, CRL and other status information in the Repository is not deemed private within the PKI.
Siemens CA will use suitable organizational and technical information security measures to protect Personal Data of Certificate Applicants against misuse or accidental or unlawful destruction, loss or alteration and unauthorized disclosure or access.

Personal Data of a Certificate Applicant or Subject that is necessary for important public interest grounds or for the establishment, exercise or defense of legal claims may be transferred in accordance with applicable data privacy protection law. The party to whom such Personal Data are transferred shall be advised that the Personal Data transferred may be processed or used only for the purpose for which they were transferred.

Siemens CA will cause its trusted service providers to ensure that Personal Data is factually correct and – if necessary, up-to-date – and that appropriate measures are taken to assure that inaccurate or incomplete information is corrected or deleted and that Certificate Applicant’s and Subject’s right to information, rectification, erasure, blocking and objection are respected as provided under applicable data protection law or Corporate Guidelines.

9.4.1 Privacy plan

CA data privacy practices are documented here: https://www.siemens.com/global/en/general/privacy-notice.html .

9.4.2 Information treated as private

The CA or RA SHALL treat all personal information about an Individual that is not publicly available in the contents of a Certificate as private information. This includes information that links a Pseudonym to the real identity of the Subject Individual.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

The CA or RA SHALL protect private information using appropriate safeguards and a reasonable degree of care.
The CA or RA SHALL require the same from any service providers who handle private information on behalf of the CA or RA.

9.4.5 Notice and consent to use private information

The CA or RA shall provide appropriate notices to, and receive the necessary consent, from Subject Individuals before using private information for any purpose other than providing services related to the issuance and management of Certificates. The CA or RA shall require the same from any service providers who handle private information on behalf of the CA or RA.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual Property Rights

The allocation of Intellectual Property Rights (e.g., copyright, trademark) in this CP, Certificates, and Key Pairs among Siemens PKI Participants (other than Subjects and Relying Parties) is governed by the applicable agreements, which shall at all times prevail over this §9.5. For Subjects and Relying Parties, the allocation of Intellectual Property Rights is addressed in CP §9.5.1-9.5.4 below.

9.5.1 Intellectual Property Rights in Certificates and Revocation Information

Siemens AG retains all Intellectual Property Rights in and to the Certificates and Revocation Information issued by Siemens Root CA and corresponding Issuing CAs. Siemens AG limits reproduction and distribution of certificates on a nonexclusive royalty-free basis in the Repository or otherwise, provided that the Certificates are reproduced in full, unless use of Certificates is otherwise subject to an applicable agreement. Siemens AG may grant permission to use Revocation Information to perform Relying Party functions in an applicable agreement, e.g., by checking CRL(s).

9.5.2 Intellectual Property Rights in CP

Siemens AG retains all Intellectual Property Rights in and to this CP and related basic Siemens PKI documents.

9.5.3 Intellectual Property Rights in Names

Certificate Applicant retains all rights it has (if any) in any trademark or trade name contained in any Certificate Application and “Subject Name” within any Certificate issued to such Certificate Applicant as Subject. Siemens CA is not responsible for resolving disputes among competing claimants to the Intellectual Property Rights in or to such names.

9.5.4 Property rights of Certificate Owners

Any information gained with the help of a CA’s Certificates remains the property of the respective Certificate owner.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

By issuing a Certificate, the CA makes the warranties listed herein to the following Certificate Beneficiaries:
1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
2. All Application Software Suppliers with whom the Siemens Root CA has entered into a contract for inclusion of its Siemens Root CA Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its CP and/or CPS in issuing and managing the Certificate.

9.6.1.1 Limited warranty

Siemens AG provides the following limited warranty to the Certificate Beneficiaries at the time of Certificate issuance: (a) it issued the Certificate substantially in compliance with this CPS; b) the information contained within the Certificate accurately reflects the information provided to Siemens AG by the Applicant in all material respects; and (c) it has taken reasonable steps to verify that the information within the Certificate is accurate. The steps Siemens AG takes to verify the information contained in a Certificate are set forth in this CPS.

9.6.1.2 Warranties and Obligations relating to the CPS

Siemens AG will apply CA Browser Forum’s S/MIME baseline requirements to the extent applicable. By issuing such a Certificate, Siemens AG represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, Siemens AG has complied with this Section and its CPS in issuing and managing the Certificate.

9.6.2 RA representations and warranties

No further stipulation as there are no additional RAs except of the Siemens CA.

9.6.3 Applicant's representations and warranties

As part of the Subscriber Agreement agreed to by all Subscribers, the following commitments and warranties are made for the express benefit of Siemens and all Relying Parties and Application Software Suppliers:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to Siemens, both in the Certificate Request and as otherwise requested by Siemens in connection with the issuance of the Certificate(s) to be supplied by Siemens;
- Protection of Private Key: An obligation and warranty by the Subscriber or a subcontractor (e.g. hosting provider) to take all reasonable measures necessary to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated access information or device such as a password or token);
- Acceptance of Certificate: An obligation and warranty that it will not install and use the Certificate(s) until it has reviewed and verified the accuracy of the data in each Certificate;
- Use of Certificate: An obligation and warranty to:
    - Server Certificates: install the Certificate only on the server accessible at the domain name listed on the Certificate,
    - Code Signing Certificates: not use the Certificate to digitally sign hostile code, spyware or other malicious software (or to disable antispyware and other protective measures or provide false or misleading descriptions of the signed code’s functions or features), and to use the Certificate solely in compliance with all applicable laws, solely for authorized company business and solely in accordance with the Certificate Holder Agreement; and
    - Other Certificates: use the Certificate in accordance with all applicable laws, solely in accordance with the Certificate Holder Agreement and as may be reasonably used for its intended purpose.
- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request that Siemens revoke the Certificate, in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Certificate Holder’s Private Key associated with the Public Key listed in the Certificate; and
- Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of that Certificate.
- Responsiveness An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within three working days.
- An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the CA's CP, CPS, or the Baseline Requirements.

Without limiting other Subscribers obligations stated in this CP/CPS, Subscribers are solely liable for any misrepresentations they make in Certificates to third parties that reasonably rely on the representations contained therein.

Upon accepting a Certificate the Siemens represents to Siemens and to Relying Parties that at the time of acceptance and until further notice:

- The Subscriber retains control of the Subscriber’s private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use and that no unauthorized person has ever had access to the Subscriber’s private key.
- All representations made by the Subscriber to Siemens regarding the information contained in the Certificate are accurate and true to the best of the Subscriber’s knowledge or to the extent that the Subscriber receives notice of such information, the Subscriber shall act promptly to notify Siemens of any material inaccuracies contained in the Certificate.
- The Certificate is used exclusively for authorized and legal purposes, consistent with this CP/CPS, and that the Subscriber will use the Certificate only in conjunction with the entity named in the organization field of the Certificate.
- The Subscriber agrees with the terms and conditions of this CP/CPS and other agreements and policy statements of Siemens.

9.6.4 Relying party representations and warranties

Relying Parties represent and warrant that:

- They will collect enough information about a Digital Certificate and its Corresponding Holder to make an informed decision as to the extent to which they can rely on the Digital Certificate.
- That they are solely responsible for making the decision to rely on a Digital Certificate.
- That they shall bear the legal consequences of any failure to perform Relying Party obligations under the terms of this CP/CPS and the Relying Party agreement.

9.7 Disclaimers of Warranties

Except as expressly otherwise provided in an applicable agreement or equivalent documentation provided in accordance with employment law and practice applicable to the respective Siemens PKI Participants, Siemens Root CA disclaims all representations, warranties (whether express or implied) and liability, except in cases of willful misconduct or gross negligence.

9.8 Limitations of Liability

Except as expressly otherwise provided in an applicable agreement or equivalent documentation provided in accordance with employment law and practice applicable to the respective Siemens PKI Participants, Siemens’ liability for damages based on whatever legal reason, including infringement of duties arising in connection with the contract or tort, is excluded.

This does not apply if liability is based on:

(a) the German Product Liability Act ("Produkthaftungsgesetz");

(b) intent;

(c) gross negligence on the part of the owners, legal representatives or executives;

(d) fraud;

(e) failure to comply with a guarantee granted;

(f) negligent injury to life, limb or health; or

(g) negligent breach of a fundamental condition of contract ("*wesentliche Vertragspflichten*").

However, claims for damages arising from a breach of a fundamental condition of contract shall be limited to the foreseeable damage which is intrinsic to the contract, provided that no other of the above case applies.

The above provision does not imply a change in the burden of proof to the detriment of the claiming party.

9.9 Indemnities

Notwithstanding above sec. 9.8 and except as expressly otherwise provided in an applicable agreement or equivalent documentation provided in accordance with employment law and practice applicable to the respective Siemens PKI Participants, there is no obligation to make one PKI Participant whole for losses or damages incurred by that PKI Participant, which arise out of another PKI Participant's conduct with respect to third party claims, i.e., there is no indemnity.

9.10 Term and Termination

9.10.1 Term

The Term of this CP commences on effective date published in CP §1.2 and continues until terminated as provided in CP §9.10.2.

9.10.2 Termination

This CP terminates if the Validity Period of the Siemens Root CA Certificates or Siemens Issuing CA Certificates expire and are not renewed, if this CP is replaced with a new version, if Siemens' -PKI operations are terminated or if it is otherwise necessary to terminate operation for any reason.

Before Siemens CA terminates its services at least the following procedures shall be executed:

- Siemens CA shall inform the following of the termination: all subscribers and other entities with which Siemens CA has agreements or other form of established relations, among which relying parties and Siemens CA. In addition, this information shall be made available to other relying parties
- Siemens CA shall terminate all authorization of subcontractors to act on behalf of Siemens CA in the performance of any functions related to the process of issuing certificates
- Siemens CA shall perform necessary undertakings to transfer obligations for maintaining registration information, revocation status information and event log archives for their respective period of time as indicated to the subscriber and relying party, to a reliable party
- Siemens CA shall destroy, or withdraw from use, its private keys

9.10.3 Effect of Termination and Survival

Prior to termination, Siemens CA will make commercially reasonable efforts to prepare and implement a termination plan set forth in CP §5.8 to address the effects of termination. Where possible Siemens CA will make arrangements to transfer provision of trust services, including its public keys, for its existing customers to another CA.

9.11 Individual Notices and Communication with Participants

Individual notices and communication shall be performed via email except as otherwise set forth in the applicable agreement.

9.12 Amendments

9.12.1 Procedure for Amendment

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

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

9.12.2 Notification Mechanism and Period

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

The new version of the CP/CPS will be published after its release on the following website: https://www.siemens.com/pki/.

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 §1.5) to have an insignificant effect on the acceptability of Certificates, do not require a change in the CP OID. Changes, which will materially change the acceptability of Certificates for specific purposes, may require corresponding changes to the CP OID.

9.13 Dispute Resolution Provisions

Any dispute or claim arising out of or relating to this CP, or the CPSs, or its subject matter shall be finally resolved as follows.

- ❑ For disputes between Siemens AG and/or its affiliates, any dispute or claim arising out of or relating to this CP/CPS or its subject matter shall be finally resolved in accordance with any dispute resolution procedures of the Siemens Group, Region or Operating Company employing the Subject or of an applicable agreement.
- ❑ Any other dispute or claim arising out of or relating to this CP/CPS or its subject matter is to be finally resolved in accordance with the dispute resolution procedures in an applicable agreement between the Siemens entity and the claiming party. If there is no applicable agreement the following dispute resolution provisions shall apply:

  1. Negotiations
  1.1 If a dispute arises out of or in connection with this CP, or the CPSs, or its subject matter , the responsible representatives of the parties shall attempt to settle such dispute. Upon request of a Party a senior management representative of each party shall participate in the negotiations. Each party shall be entitled to terminate these negotiations by written notification to the other party(-ies) at any time.
  1.2 Nothing in this and the following sections shall limit the right of the Parties to seek relief intended to preserve the status quo or interim measures in any court of competent jurisdiction, from an emergency arbitrator or arbitral tribunal.

  2. Arbitration
  2.1 All disputes arising out of or in connection with this this CP, or the CPSs, or its subject matter which are not resolved pursuant to above section 1 (Negotiations), including any question regarding the termination or any subsequent amendment of this CP, shall be finally settled in accordance with the Rules of Arbitration (“Rules”) of the International Chamber of Commerce (“ICC”).
  2.2 If the value of the total matter in dispute, including the value of any counterclaims, is € 1 million or above, the expedited procedure provisions of the Rules shall not apply and the arbitral tribunal shall consist of three arbitrators.
  If the tribunal consists of three arbitrators, each party shall nominate one arbitrator for confirmation by the ICC. Both arbitrators shall agree on the third arbitrator within thirty (30) days after their appointment. Should the two arbitrators fail to reach agreement on the third arbitrator within the thirty-day period, the ICC shall select and appoint the third arbitrator.
  2.3 The seat of arbitration shall be Munich, Germany. The law applicable to the dispute resolution clause shall be the law of the seat of arbitration.
  2.4 The language to be used in the arbitration shall be English.
  2.5 Any order for the production or disclosure of documents shall be limited to the documents on which each party specifically relies in its submission(s).
  2.6 Consolidation of arbitrations pending under the Rules into a single arbitration shall only be possible if all parties have agreed to consolidation.

2.7 Upon request of a party, the arbitral tribunal shall order any claiming or counterclaiming party to provide security for the legal and other costs of any other party related to that claim or counterclaim, by way of bank guarantee or in any other manner and upon such terms as the arbitral tribunal considers appropriate.

9.14 Governing Law

The substantive law applicable to this CP or its subject matter is as follows, excluding conflict of law rules.

❑ Any matter related to this CP or its subject matter is to be governed by and interpreted in accordance with the laws agreed in an applicable agreement between the Siemens entity and the claiming party, and if no such agreement is concluded, the laws of Germany.

9.15 Compliance with Applicable Law

The use of Siemens Certificates shall always comply with applicable law, especially regulation of export, import or use of encryption hardware, software or technology.

9.16 Miscellaneous Provisions

The so-called called "boilerplate” provisions below, which apply to this CP or other Siemens PKI documents, will be addressed in the applicable agreements.

9.16.1 Entire Agreement

No further stipulation.

9.16.2 Assignment

No further stipulation.

9.16.3 Severability

No further stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No further stipulation.

9.16.5 Force Majeure

No further stipulation.

9.17 Other Provisions

9.17.1 Order of Precedence of CP

In the event of a conflict between the following documents, these documents shall prevail in the following order:

1. This CP
2. Root CA CPS
3. Documentation executed or expressly authorized by Siemens CA
4. Issuing CA CPS
5. Any other Siemens PKI policy, practices, procedure or plans documentation

10 References

[CAB_Forum]	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates; CA / Browser Forum; http://www.cabforum.org
[CertProfile]	Siemens Trust Center PKI- CA Hierarchy Policy 2023 available on www.siemens.com/pki
[ETSI EN 319 411-1]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI EN 319 412-2]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[ETSI EN 319 401]	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI TS 102042]	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (Feb. 2013)
[ISO27001]	Information technology - Security techniques - Information security management systems – Requirements (March 2015)
[Issuing CA CPS]	Siemens Issuing CA Certification Practice Statement; published at www.siemens.com/pki
[InterCaMan]	Siemens Inter CA and HSM management manual
[NSSSR]	Network and Certificate System Security Requirements in Version 1.5 – effective October 2020; CA / Browser Forum; published at: Network Security Working Group – CAB Forum
[RFC3647]	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Network Working Group: S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu (November 2003)
[RFC5280]	Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile, Network Working Group: R. Housley, W. Polk, W. Ford, D. Solo (May 2008)
[RFC6960]	Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile, Network Working Group: R. Housley, W. Polk, W. Ford, D. Solo (May 2008)
[RFC8399]	Internationalization Updates to RFC5280: R. Housley (May 2018)
[Root CA CPS]	Siemens Root CA Certification Practice Statement published at www.siemens.com/pki
[SBR 101]	Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates; CA / Browser Forum; Version 1.0.1; https://cabforum.org/smime-br/ (August 11, 2023)
[Siemens CP]	Siemens CA Certificate Policy published at www.siemens.com/pki
[TRUST_SITE]	Sichere Infrastrukturen für IT-Systeme, Trusted Site Infrastructure, TÜViT, (2016)
[X.509 Version 3]	ITU-T Recommandation X.509 Version 3

Annex A: Acronyms and Definitions

A.1 Definitions

Applicant	Natural or legal person that is raising the certificate request.
Application Software Supplier	A supplier of email client software or other relying-party application software such as mail user agents (web-based or application based) and email service providers that process S/MIME Certificates
Business Partner	Persons or legal entities not belonging to Siemens but having a contractual relationship to Siemens. Such as contractors and divested entities.
CA-certificate	Certificate for a Certification Authority's public key
CA Key Pair	A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s)
Certificate	An applicant of a public key require confidence that the associated private key is owned by the correct remote subject (person or system) with which an encryption or digital signature mechanism will be used. This confidence is obtained through the use of public key certificates, which are data structures that bind public key values to subjects
Certificate Policy (CP)	Compare section 1.1
Certification Authority (CA)	Authority, that is entitled to certify public keys; compare chapter 1.3.1
Certificate Issuance List (CIL)	It’s a growing list under the control of a Siemens Issuing CA containing the serial numbers of all valid X.509 v3 certificates issued.
Cross-certificate	Certificate used to affirm a trusted relationship between two CAs
Directory Service	PKI-service for online access to certificates and CRLs; commonly realized through the Light Weight Directory Access Protocol (LDAP)
Distinguished Name	Sequence of data-fields describing the CA issuer and/or the subject uniquely. The format of a Distinguished Name is defined in the [X.501] 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 chapter 1.3.3.
End-entity-certificate	Certificate that must not be used for certifying and issuing CRLs or other certificates.
End-User-certificate	Certificate that may not be used to certify and issue other certificates or CRLs
Function Group	A function group represents a non-personal function, e.g. mailbox with a special purpose, team mailbox, service desk. More than one person can have access to a function group.
Intermediate Certification Authority	A Technical Certification Authority signed by a trusted Root CA, is entitled to certify public keys; compare chapter 1.3.1
Key Pair	The Private Key and its associated Public Key
Object Identifier (OID)	An object identifier is a string of decimal numbers that uniquely identifies an object
Policy Management Authority	A body of Siemens AG that is responsible for setting, implementing and administering policy decisions regarding this CP and related documents and agreements in the Siemens PKI
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used
	to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key
Public Key	The key of a Key Pair that can be publicly disclosed by the holder of the corresponding

Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder’s corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder’s corresponding Private Key

Registration Authority (RA)

PKI-incorporated facility for participant-authentication.
See also chapter 1.3.2.

Relying parties

Individual or legal entity that uses certificates;
see also chapter 1.3.5.

Revocation Information:

CAs are responsible for indicating the revocation status of the certificates that they issue. Revocation status information may be provided using the Online Certificate Status Protocol (OCSP) [RFC2560], certificate revocation lists (CRLs), or some other mechanism. In general, when revocation status information is provided using CRLs, the CA is also the CRL issuer. However, a CA may delegate the responsibility for issuing CRLs to a different entity

Secure Device

A component (such as a smart card) 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 Certification Authority

Siemens internal organization that issues and manages certificates. This organization operates the Siemens Root CAs as well as the Siemens Issuing CAs.

Siemens Community

Employees of Siemens corporation and its subsidiaries and affiliates.

Siemens Issuing CA

Technical components (hardware and software) that sign user certificates and related information such as revocation lists or OCSP signer certificates.

Siemens Root CA

Technical components (hardware and software) that sign certificates of Siemens Issuing CAs and related information such as revocation lists or OCSP signer certificates.

Smart Card

Integrated circuit card including a micro-processor that can be used 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 Siemens PKI is **Siemens as legal entity**.
During the lifetime of the certificate Siemens delegates rights to dedicated persons or functions. E.g. when the employee requests an EE certificate, Siemens has delegated the right to act as subscriber to this employee. The same holds for business partner certificates. In this case Siemens delegates the right to the business partner to requests a certificate.
See also chapter 1.3.3.

Token

Transport-medium for certificates and keys

Trusted Operator

Siemens CA has the overall responsibility of issuing Certificates to Subjects and managing and revoking Certificates. Siemens CA may delegate part or all of these functions in exercising its overall responsibility to RAs or to other internal Service Providers of Siemens, which are called Trusted Operators

Valid Certificate

A Certificate that passes the validation procedure specified in RFC 5280

A.2 Abbreviations

BRG	Baseline Requirements Guidelines
CA	Certification Authority
CAB	CA Browser Forum
CARL	Certificate Authority Revocation List
CISO	Chief Information Security Officer
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DVCP	Domain Validated Certificate Policy
EE	End entity
EFS	Encrypting File System
FG	Function Group
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name
HSM	Hardware Security Module
ICA	Intermediate Certificate Authority
IODEF	The Incident Object Description Exchange Format (RFC 5070)
ISO	International Organization for Standardization
ISMS	Information Security Management System
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
NetSec-CAB	Network Security Requirements- CA/Browser Forum
NCP	Normalized Certificate Policy
NCP+	Normalized Certificate Policy requiring a secure user device
NSC	Network-Smartcard
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKISS	Electronic PKI Self-Service
PMA	Policy Management Authority
PUK	Personal Unblocking Key
RA	Registration Authority
RFC	Request for Comment
PSE	Personal Security Environment
SBR	S/MIME Baseline Requirements
SSCD	Secure Signature Creation Device
SUD	Secure User Device
URL	Uniform Resource Locator
UTF8	Unicode Transformation Format-8 Policy Management
VSC	Virtual-Smartcard