



Certificate Policy

Siemens CA

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)

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

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

Scope and Applicability

This document constitutes the 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 1.4 and status "Released" has been classified as "Unrestricted".

	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 December 1, 2017
Authorization	Markus Wichmann in representation of the Head of Siemens ISEC Udo Wirtz	Siemens GS IT ISEC	December 1, 2017

This CP has been approved by Markus Wichmann in representation of the Head of Siemens ISEC on December 1, 2017.

Table of Content

Scope and Applicability	2
Document Status	2
1 Introduction	8
1.1 Overview	8
1.1.1 PKI hierarchy	8
1.1.2 Siemens Root CA and QuoVadis Root CA	8
1.1.3 Issuing CAs	9
1.2 Document Name and Identification	9
1.3 PKI Participants	9
1.3.1 Certification Authorities	9
1.3.1.1 Root CA	9
1.3.1.2 Issuing CAs	9
1.3.2 Registration Authorities	9
1.3.3 Subscribers	10
1.3.4 Subject (End Entity)	10
1.3.5 Relying Parties	10
1.4 Certificate Usage	11
1.4.1 Appropriate Certificate Usage	11
1.4.2 Prohibited Certificate Usage	11
1.5 Policy Administration	11
1.5.1 Organization Administering the Document	11
1.5.2 Contact Person	11
1.5.3 Person Determining CP and CPS Suitability for the Policy	11
1.5.4 CP and CPS Approval Procedures	12
2 Publication and Repository Responsibilities	13
2.1 Repositories	13
2.2 Publication of Certification Information	13
2.3 Time or Frequency of Publication	13
2.4 Access Controls on Repositories	13
3 Identification and Authentication	15
3.1 Naming	15
3.1.1 Types of Names	15
3.1.2 Need of Names to be Meaningful	15
3.1.2.1 CA Names	15
3.1.2.2 End Entity Names	15
3.1.3 Anonymity or Pseudonymity of Subjects	15
3.1.3.1 CA Names	15
3.1.3.2 End Entity Names	15
3.1.4 Rules for Interpreting Various Name Forms	15
3.1.5 Uniqueness of Names	15
3.1.5.1 CA Names	15
3.1.5.2 End Entity Names	15
3.1.6 Recognition, Authentication, and Roles of Trademarks	15
3.2 Initial Identity Validation	15

3.2.1	Method to Prove Possession of Private Key.....	15
3.2.2	Identification and Authentication of Organization Identity.....	16
3.2.3	Identification and Authentication of Individual Identity.....	16
3.2.4	Non-verified Applicant Information.....	16
3.2.5	Validation of Authority.....	16
3.2.6	Criteria for Interoperation between Communities of Trusts.....	16
3.3	Identification and Authentication for Re-key Requests.....	16
3.3.1	Root CA.....	16
3.3.2	Issuing CA.....	16
3.4	Identification and Authentication for Revocation Requests.....	16
3.4.1	Root CA.....	16
3.4.2	Issuing CA.....	16
4	Certificate Lifecycle Operational Requirements.....	17
4.1	Certificate Application.....	17
4.1.1	Who can submit a certificate application?.....	17
4.1.1.1	Root CA.....	17
4.1.1.2	Issuing CAs.....	17
4.1.2	Enrollment Process and Responsibilities.....	17
4.1.2.1	Root CA.....	17
4.1.2.2	Issuing CAs.....	17
4.2	Certificate Application Processing.....	17
4.2.1	Performing identification and authentication functions.....	17
4.2.2	Approval or Rejection of Certificate Applications.....	17
4.2.3	Time to Process Certificate Applications.....	18
4.2.4	Certificate Authority Authorization (CAA).....	18
4.3	Certificate Issuance.....	18
4.3.1	Root CA actions during Certificate issuance.....	18
4.3.2	Issuing CA actions during Certificate issuance.....	18
4.3.3	Notification to Subject by the CA of Certificate Issuance.....	18
4.4	Certificate Acceptance.....	19
4.4.1	Root CA.....	19
4.4.2	Issuing CA.....	19
4.4.3	Notification of Certificate issuance by the CA to other entities.....	19
4.5	Key Pair and Certificate Usage.....	19
4.5.1	Root CA Private Key and Certificate Usage.....	19
4.5.2	Issuing CA Private Key and Certificate Usage.....	19
4.5.3	Subject Private Key and Certificate Usage.....	19
4.5.4	Relying Party Public Key and Certificate Usage.....	19
4.6	Certificate Renewal.....	19
4.6.1	Circumstance for Certificate Renewal.....	19
4.6.2	Who may request renewal?.....	20
4.6.3	Processing Certificate Renewal Request.....	20
4.6.4	Notification of new Certificate Issuance to Subject.....	20
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	20
4.6.6	Publication of the Renewal Certificate by the CA.....	20
4.6.7	Notification of Certificate Issuance by the CA to the Entities.....	20
4.7	Certificate Re-key.....	20
4.7.1	Circumstances for Certificate Re-key.....	20
4.7.2	Who may request certification of a new Public Key?.....	20
4.7.2.1	Re-keying of a Issuing CA Certificate.....	20
4.7.2.2	Re-keying of End Entity Certificates.....	20

4.7.3	Processing Certificate Re-keying Requests.....	20
4.7.4	Notification of new Certificate Issuance to Subject	20
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate	20
4.7.6	Publication of the Re-keyed Certificate by the CA	20
4.7.7	Notification of Certificate Issuance by the CA to other Entities.....	21
4.8	Certificate Modification	21
4.8.1	Circumstance for Certificate Modification	21
4.8.2	Who may request Certificate modification?	21
4.8.3	Processing Certificate Modification Requests.....	21
4.8.4	Notification of new Certificate Issuance to Subject	21
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	21
4.8.6	Publication of the Modified Certificate by the CA.....	21
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	21
4.9	Certificate Revocation and Suspension	21
4.9.1	Circumstances for Revocation.....	21
4.9.1.1	Revocation of Issuing CA certificates	21
4.9.1.2	Revocation of End Entity Certificates.....	21
4.9.1.3	Other Reasons for Revocation of Certificates	22
4.9.2	Who can request revocation?	22
4.9.3	Procedure for Revocation Request	22
4.9.4	Revocation Request Grace Period.....	22
4.9.5	Time within which CA must Process the Revocation Request	22
4.9.6	Revocation Checking Requirement for Relying Parties	22
4.9.7	CRL Issuance Frequency	23
4.9.8	Maximum Latency for CRLs	23
4.9.9	On-line Revocation/Status Checking Availability	23
4.9.10	On-line Revocation Checking Requirements	23
4.9.11	Other Forms of Revocation Advertisements Available.....	23
4.9.12	Special Requirements for Private Key Compromise	23
4.9.13	Circumstances for Suspension.....	23
4.10	Certificate Status Services	23
4.10.1	Operational Characteristics	23
4.10.2	Service Availability	23
4.10.3	Optional Features	23
4.11	End of Subscription	23
4.12	Key Escrow and Recovery	23
5	Management, Operational, and Physical Controls.....	24
5.1	Physical Security Controls.....	24
5.2	Procedural Controls	24
5.3	Personnel Security Controls.....	24
5.4	Audit Logging Procedures	24
5.5	Records Archival	24
5.6	Key Changeover	24
5.7	Compromise and Disaster Recovery.....	24
5.8	CA Termination.....	24
6	Technical Security Controls	25
6.1	Key Pair Generation and Installation.....	25

6.2	Private Key Protection and Cryptographic Module Engineering Controls	25
6.3	Other Aspects of Key Pair Management	25
6.4	Activation Data	25
6.5	Computer Security Controls	25
6.6	Life Cycle Security Controls	25
6.7	Network Security Controls	25
6.8	Time Stamp Process	25
7	<i>Certificate, CRL, and OCSP Profiles</i>	26
7.1	Certificate Profile	26
7.2	CRL Profile	26
7.3	OCSP Profile	26
8	<i>Compliance Audit and Other Assessment</i>	27
8.1	Frequency or Circumstances of Assessment	27
8.2	Identity / Qualifications of Assessor	27
8.3	Assessor’s Relationship to Assessed Entity	27
8.4	Topics Covered by Assessment	27
8.5	Actions Taken as a Result of Deficiency	27
8.6	Communication of Results	28
9	<i>Other Business and Legal Matters</i>	29
9.1	Fees	29
9.2	Financial Responsibility	29
9.3	Confidentiality of Business Information	29
9.3.1	Scope of Confidential Information	29
9.3.2	Information not within the Scope of Confidential Information	29
9.3.3	Responsibility to Protect Confidential Information	29
9.4	Privacy of Personal Information	30
9.5	Intellectual Property Rights	30
9.5.1	Intellectual Property Rights in Certificates and Revocation Information	30
9.5.2	Intellectual Property Rights in CP	30
9.5.3	Intellectual Property Rights in Names	30
9.5.4	Property rights of Certificate Owners	30
9.6	Representations and Warranties	30
9.7	Disclaimers of Warranties	31
9.8	Limitations of Liability	31
9.9	Indemnities	31
9.10	Term and Termination	31
9.10.1	Term	31
9.10.2	Termination	31
9.10.3	Effect of Termination and Survival	31
9.11	Individual Notices and Communication with Participants	31

9.12	Amendments	32
9.12.1	Procedure for Amendment.....	32
9.12.2	Notification Mechanism and Period	32
9.12.3	Circumstances under which OID must be changed	32
9.13	Dispute Resolution Provisions	32
9.14	Governing Law	32
9.15	Compliance with Applicable Law	32
9.16	Miscellaneous Provisions	32
9.16.1	Entire Agreement	32
9.16.2	Assignment	33
9.16.3	Severability	33
9.16.4	Enforcement (attorneys' fees and waiver of rights)	33
9.16.5	Force Majeure.....	33
9.17	Other Provisions	33
9.17.1	Order of Precedence of CP	33
10	References	34
Annex A: Acronyms and Definitions		35
A.1	Definitions	35
A.2	Abbreviations	36

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 *Figure 1*.

Currently two separate active root CAs exist:

- the Siemens Root CA dedicated for Siemens internal use cases and
- the QuoVadis Root CA (cross certification partner for external trust) for use cases which require external recognition of the certificates

The Root CAs exclusively issue CA certificates to the Issuing CAs.

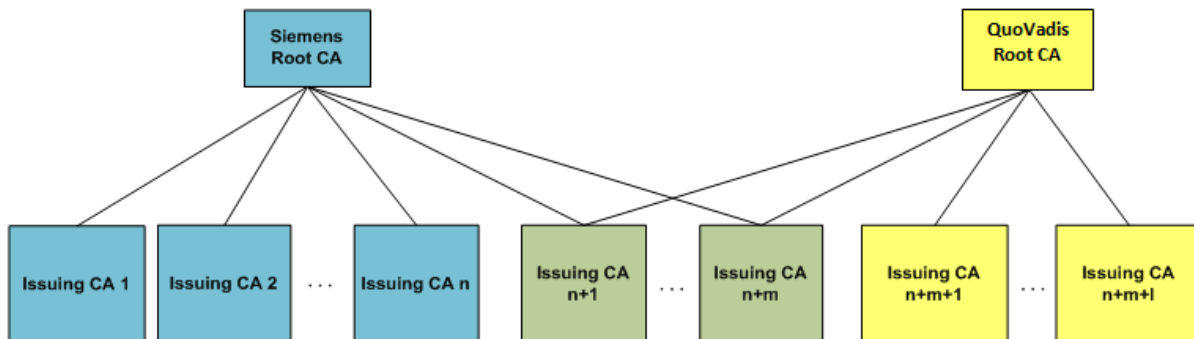


Figure 1: Siemens PKI hierarchy

All certificates issued by the above mentioned CAs as a minimum comply with the ETSI requirements of NCP [ETSI TS 102 042].

Where appropriate, additional specifications (beyond NCP) are defined in the respective CPSs.

1.1.2 Siemens Root CA and QuoVadis Root CA

The Siemens Root CA and the QuoVadis Root CA issue, manage, and revoke X.509v3 Certificates used by the corresponding Issuing CAs. This includes:

- ❑ Generating Root CA Key Pairs
- ❑ Generating the self-signed Certificates for the Root CAs
- ❑ Generating Certificates for the Issuing CAs
- ❑ Recertification of existing CA keys
- ❑ Revoking Issuing CA Certificates
- ❑ Maintaining a Revocation List for CA Certificates ("CA-CRL")

1.1.3 Issuing CAs

The Issuing 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 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 CAs and Issuing CAs
OID: 1.3.6.1.4.1.4329.99.1.1.1.1.0
Expiration: This version of the document is the most current one until a subsequent release.

1.3 PKI Participants

PKI Participants are Siemens Certification Authorities, Registration Authorities, Subjects, and Relying Parties.

1.3.1 Certification Authorities

A graphical overview of the CA hierarchy is depicted in *Figure 1: Siemens PKI hierarchy*.

1.3.1.1 Root CA

Siemens PKI architecture is based on a two-tier CA structure. This architecture allows the Root CA to be stored off-line. The Siemens Root CA performs the signing, issuance, and revocation of Certificates used to establish and authenticate a Siemens Issuing 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 Issuing CAs

The Siemens Issuing CAs issue Certificates to End Entities and manage and revoke End Entity Certificates.

1.3.2 Registration Authorities

For person related certificates Siemens CA may delegate registration of End Entities to two types of RAs:

- 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.

For the *server related and code signing certificates* Siemens CA may delegate registration to a single RA:

- The Server RA is responsible for Identification and Authentication of the responsible person for a server. The Certificate Applicant, who is responsible for the server, must be a Siemens employee or a Business Partner.

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.

1.3.3 Subscribers

Subscriber is always Siemens as legal entity, 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 or servers represented by named Siemens employees) 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.
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")
Global Service ("GS") Information Technology ("IT"), Information Security ("ISEC")
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
GS IT ISEC
Attn: Siemens PKI
Otto-Hahn-Ring 6, 81739 Munich, GERMANY
E-mail: contact.pki@siemens.com
Website: <https://www.siemens.com/pki/>

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

An annual risk assessment is carried out to evaluate business requirements and determine the security requirements to be included in the certificate policy for the stated community and applicability. In addition the CP as well as the 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 ISEC.

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.

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 Issuing CA Certificates, and
- ❑ issued encryption certificates
- ❑ revocation information for root CA and Issuing CA certificates and for end entity certificates

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

Subjects and Relying Parties will have access to:

- Siemens Issuing CAs via:
 - HTTP: <http://www.siemens.com/pki/>
 - LDAP: `ldap://al.siemens.net/CN=<GID of Issuing CA>,L=PKI?cACertificate`
- Certificate Revocation List (CRL) via:
 - HTTP: [http://ch.siemens.net/pki? <GID of Issuing CA>.crl](http://ch.siemens.net/pki?<GID of Issuing CA>.crl)
 - LDAP: `ldap://cl.siemens.net/CN=<GID of Issuing CA>,L=PKI?certificateRevocationList`
- Online certificate status information via:
 - HTTP: <http://ocsp.pki-services.siemens.com>

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.

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 is accessible with read-only access through the Siemens Intranet or Internet under existing procedures and policies.

Certificate Policy

As a condition to accessing Certificates, Certificate status information or CRLs in the Repository, Siemens CA may require persons to agree to a Relying Party agreement. 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, i.e., names other than Subject's true personal name, are not permitted.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

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 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 or other Siemens CA-approved methods. 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;
3. electronic form based process used by the server RA.

3.2.4 Non-verified Applicant Information

No stipulation.

3.2.5 Validation of Authority

No stipulation.

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.

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 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 sent 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 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 and Issuing CAs' Key Pairs throughout the operational life cycle of the Root CA 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 Issuing CA is to be created and to be signed by the Root CA.

4.1.1.2 Issuing CAs

Certificate Applicants can 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 CA in accordance with Regulations in section 3.1, "Naming", of this CP
- Date of the request
- Duration of the CA Certificate, which cannot exceed the duration of the Root-CA's Certificate;
- CPS for the new Issuing CA of this Root CA
- Certificate Profile of the new Issuing CA and
- Profiles of the end-entity Certificates to be signed by that new Issuing CA

4.1.2.2 Issuing CAs

End Entity Certificate Applicants undergo an enrollment process consisting of:

- generating, or arranging to have generated, a Key Pair
- completing a Certificate Application and providing the required information
- 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.

For EE Certificates Siemens CA delegates these tasks to respective RAs.

4.2.2 Approval or Rejection of Certificate Applications

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.

Certificate Policy

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

4.2.3 Time to Process Certificate Applications

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

4.2.4 Certificate Authority Authorization (CAA)

Siemens checks 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 issuewild 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 Root 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 located in 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.

4.3.2 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.

4.3.3 Notification to Subject by the CA of Certificate Issuance

Upon Certificate generation, the respective 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 Root CA

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

4.4.2 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.

4.4.3 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 partners.

4.5 Key Pair and Certificate Usage

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

4.5.2 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

4.5.3 Subject Private Key and Certificate Usage

Subject Private Keys and Certificates shall only be used for the purposes as specified in the Certificate.

4.5.4 Relying Party Public Key and Certificate Usage

Before any act of reliance, Relying Parties shall

- take account of any limitations on the usage and liability limits of the Certificate as indicated in the applicable CP
- securely obtain the Siemens Root CA Certificate, the Issuing CA Certificate and any other Certificates within the corresponding Certificate Chain and
- securely obtain the revocation status of all certificates in the certificate chain

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

4.6 Certificate Renewal

Certificate Renewal is the issuance of a new Certificate to an entity without changing the Public Key or any other information in the Certificate.

As a matter of principle Certificate Renewal is not offered.

4.6.1 Circumstance for Certificate Renewal

No stipulation.

Certificate Policy

4.6.2 Who may request renewal?

No stipulation.

4.6.3 Processing Certificate Renewal Request

No stipulation.

4.6.4 Notification of new Certificate Issuance to Subject

No stipulation.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to the Entities

No stipulation.

4.7 Certificate Re-key

“Re-key” addresses the generating of a new Key Pair and applying for the issuance of a new Certificate and replaces an existing Key Pair.

Generally, for Certificate Re-keying the same requirements apply as for §4.3. Certificate Issuance.

4.7.1 Circumstances for Certificate Re-key

The Re-key Process shall 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?

4.7.2.1 *Re-keying of a Issuing CA Certificate*

Rekeying of Issuing CA Certificates should not be performed.

4.7.2.2 *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 Revocation of Issuing CA certificates

Siemens CA shall revoke without delay a Certificate in the following circumstances:

- the Private Key corresponding to the Public Key in the Certificate has been lost, disclosed without authorization, stolen or compromised in any way
- the Certification Service of a CA is discontinued
- the Policy Management Authority discontinues the certification service for yet unknown higher reasons

4.9.1.2 Revocation of End Entity Certificates

Siemens CA shall revoke EE Certificates in the following circumstances:

- Siemens CA becomes aware that the Private Key corresponding to the Public Key in the Certificate has been lost, disclosed without authorization, stolen or compromised in any way
- Siemens CA suspects or finds out that the Certificates are not being used in accordance with the CP referenced in the Certificate

- ❑ Siemens CA suspects that the Certificates were not generated securely in accordance with the CP
- ❑ Subject's employment or agency with the organization responsible for requesting Subject's Certificate has been terminated or has otherwise ended
- ❑ Siemens CA has reason to believe that the Certificate was issued
 - in a manner not materially in accordance with the procedures required by this CP
 - to an entity other than the one named as the Subject of the Certificate or
 - without the authorization of the entity named as the Subject of such Certificate
- ❑ Siemens CA has reason to believe that a material fact in the Certificate Application is false
- ❑ Siemens CA determines that a material prerequisite to Certificate issuance was neither satisfied nor waived
- ❑ the information within the Certificate, other than non-verified Applicant Information, is incorrect or has changed or
- ❑ the Subject requests revocation of the Certificate

4.9.1.3 *Other Reasons for Revocation of Certificates*

More technical reasons for revoking a Certificate can be:

- ❑ 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

Additional reasons for revoking a CA Certificate can be specified in the CPSs.

4.9.2 **Who can request revocation?**

The revocation of Issuing CA Certificates may be requested by the PMA.

The following entities may request revocation of an EE Certificate.

- Individual End Entity Subjects may request revocation of their own individual Certificates
- Only duly authorized representative of the organization (i.e., Authorized Party or Siemens Sponsor, CP/CPS §4.1.1) may request the revocation of Certificates issued to the organization

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.

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 within 24 hours after its submission.

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.

Certificate Policy

4.9.7 CRL Issuance Frequency

The CRLs are issued every 24 hours.

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 is offered.

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.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

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 via its website.

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

No stipulation.

4.10.2 Service Availability

The service 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).

4.10.3 Optional Features

No stipulation.

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 TS 102042].

Details are described in the respective CPSs.

5.1 Physical Security Controls

Details are described in the respective CPSs.

5.2 Procedural Controls

Details are described in the respective CPSs.

5.3 Personnel Security Controls

Details are described in the respective CPSs.

5.4 Audit Logging Procedures

Details are described in the respective CPSs.

5.5 Records Archival

Details are described in the respective CPSs.

5.6 Key Changeover

Details are described in the respective CPSs.

5.7 Compromise and Disaster Recovery

Details are described in the respective CPSs.

5.8 CA Termination

Details are described in the respective CPSs.

6 Technical Security Controls

Technical security controls are defined in accordance with [ETSI TS 102042].

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 Recommendation X.509 Version 3 and
- RFC 5280

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 TS 102 042. 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 auditor who:

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

8.3 Assessor's Relationship to Assessed Entity

The assessor shall be organizationally independent 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.

Certificate Policy

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.

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 extent 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.

9.5 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 grants permission to reproduce and distribute 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

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 AG disclaims any

- ❑ representations (which usually refer to the correctness of statement or the existence of a state of affairs as of a past or a present time) and

- ❑ warranties (which usually refer to a continuation of correctness or the continued existence of a state of affairs into the future), whether express or implied.

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 CA excludes the recovery from Siemens Root CA, Siemens Issuing CAs, its trusted service providers or respective RA or Repository for damages, punitive damages, loss of profits or revenue, loss of use or production to the highest extent permitted by applicable law, except in cases of willful misconduct or gross negligence.

9.9 Indemnities

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 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
- 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 and survival.

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 the *Siemens Community*, 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.
- ❑ For the *Business Partner Community*, any 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 Business Partner.

9.14 Governing Law

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

- ❑ For the Siemens Community, this CP and its subject matter shall be governed by and interpreted in accordance with the laws of Germany for all PKI Participants.
- ❑ For the Business Partner Community, 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 Business Partner, 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 "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 stipulation.

Certificate Policy

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No 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>
- [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)
- [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)
- [TRUST_SITE] Sichere Infrastrukturen für IT-Systeme, Trusted Site Infrastructure, TÜViT, 2016

Annex A: Acronyms and Definitions

A.1 Definitions

Business Partner	Persons or legal entities not belonging to Siemens but having a contractual relationship to Siemens. Examples are external consultants, sub-contractors or components suppliers.
CA-certificate	Certificate for a Certification Authority's public key
Certificate Policy (CP)	Compare section 1.1
Certification Authority (CA)	Authority, that is entitled to certify public keys; compare chapter 1.3.1.
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.
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
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.
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	Persons that belong to Siemens and can request a Siemens certificate. Examples are employees or administrators.
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.

Certificate Policy

Subscriber	<p>Subscriber for all certificates issued by the Siemens PKI is Siemens as legal entity.</p> <p>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.</p> <p>See also chapter 1.3.3.</p>
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

A.2 Abbreviations

BRG	Baseline Requirements Guidelines
CA	Certification Authority
CAB	CA Browser Forum
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
FG	Function Group
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name
HSM	Hardware Security Module
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
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Personal Unblocking Key
RA	Registration Authority
RFC	Request for Comment
PSE	Personal Security Environment
SSCD	Secure Signature Creation Device
SUD	Secure User Device
URL	Uniform Resource Locator
UTF8	Unicode Transformation Format-8 Policy Management