Certification Practice Statement

Siemens Root CAs

Document History

Version	Date	Author	Change Comment
1.0	June 10, 2016	Alexander Winnen, Michael Munzert	First final version
1.1	December 1, 2016	Rufus Buschart	Minor updated version
1.2	May 29, 2017	Rufus Buschart	Update new CA hierarchy

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

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

Scope and Applicability

This document constitutes the Certificate Practice Statement (CPS) for the Siemens Root Certificates (Root CA). The purpose of this document is to publicly disclose to subscribers and relying parties the business policies and practices under which this Root CA is operated.

Document Status

This document with version 1.0 and status Released has been classified as “Unrestricted“.

	Name	Department	Date
Author	Various authors, detailed information in document history		
Checked by	Tobias Lange Rufus Buschart	Siemens LS Siemens GS IT HR 7 4	June 10, 2016 June 14, 2017
Authorization	Markus Wichmann	Siemens GS IT ISEC	June 14, 2017

This CPS has been approved by the responsible Siemens information security officer on June 14, 2017.

Table of Content

1 Introduction

This document has been structured according to RFC 3647 “Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework” (Nov 2003) [RFC3647].

1.1 Overview

This Certification Practice Statement (CPS) defines

- measures and procedures in the context of the Certification Services performed by the Siemens Root CA
- minimum requirements demanded from all PKI participants

The CPS details the procedures and controls in place to meet the CP requirements. For identical topics the respective chapter in the CP is referenced.

The following picture shows the Siemens Root CAs together with the respective Issuing CAs:

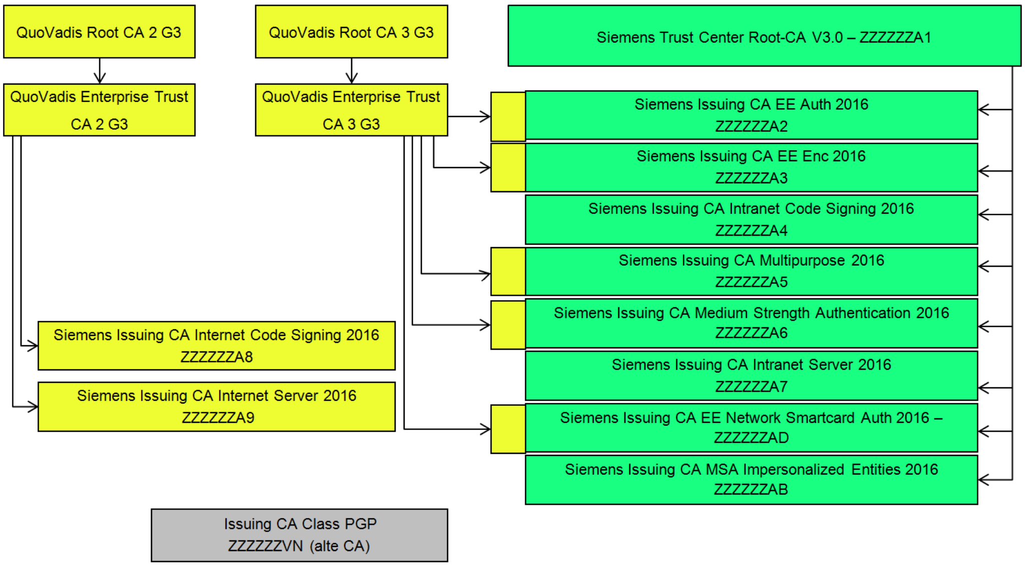
QuoVadis Root CA 2 G3
QuoVadis Root CA 3 G3
Siemens Trust Center Root-CA V3.0 – ZZZZZZA1
QuoVadis Enterprise Trust CA 2 G3
QuoVadis Enterprise Trust CA 3 G3
Siemens Issuing CA EE Auth 2016 ZZZZZZA2
Siemens Issuing CA EE Enc 2016 ZZZZZZA3
Siemens Issuing CA Intranet Code Signing 2016 ZZZZZZA4
Siemens Issuing CA Multipurpose 2016 ZZZZZZA5
Siemens Issuing CA Medium Strength Authentication 2016 ZZZZZZA6
Siemens Issuing CA Intranet Server 2016 ZZZZZZA7
Siemens Issuing CA EE Network Smartcard Auth 2016 – ZZZZZZAD
Siemens Issuing CA MSA Impersonalized Entities 2016 ZZZZZZAB
Siemens Issuing CA Internet Code Signing 2016 ZZZZZZA8
Siemens Issuing CA Internet Server 2016 ZZZZZZA9
Issuing CA Class PGP ZZZZZZVN (alte CA)

Figure 1: Siemens CA hierarchy as of June 2016

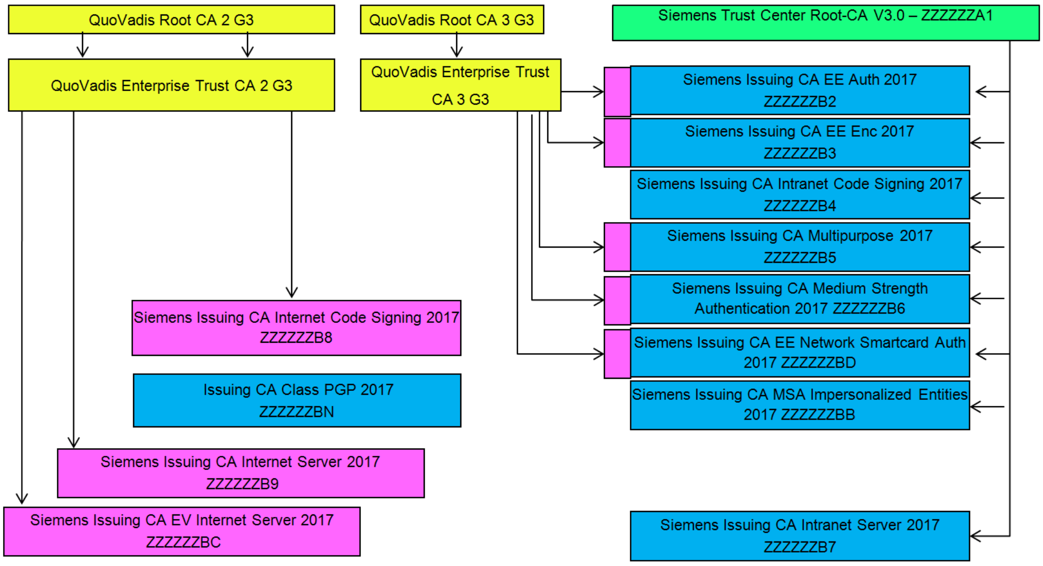
QuoVadis Root CA 2 G3
QuoVadis Root CA 3 G3
Siemens Trust Center Root-CA V3.0 – ZZZZZZA1
QuoVadis Enterprise Trust CA 2 G3
QuoVadis Enterprise Trust CA 3 G3
Siemens Issuing CA EE Auth 2017 ZZZZZZB2
Siemens Issuing CA EE Enc 2017 ZZZZZZB3
Siemens Issuing CA Intranet Code Signing 2017 ZZZZZZB4
Siemens Issuing CA Multipurpose 2017 ZZZZZZB5
Siemens Issuing CA Medium Strength Authentication 2017 ZZZZZZB6
Siemens Issuing CA EE Network Smartcard Auth 2017 ZZZZZZBD
Siemens Issuing CA MSA Impersonalized Entities 2017 ZZZZZZBB
Siemens Issuing CA Internet Code Signing 2017 ZZZZZZB8
Issuing CA Class PGP 2017 ZZZZZZBN
Siemens Issuing CA Internet Server 2017 ZZZZZZB9
Siemens Issuing CA EV Internet Server 2017 ZZZZZZBC
Siemens Issuing CA Intranet Server 2017 ZZZZZZB7

Figure 2: Siemens CA hierarchy as of 01.10.2017

The following table lists the currently operated Root CAs as well as their implemented requirements according to [ETSI 102 042]:

CA	Requirements		
	NCP+	OVCP	DVCP
ZZZZZZV0 Siemens Internet CA V1.0	X	-	-
ZZZZZZV1 Siemens Trust Center Root-CA V2.0	X	-	-
ZZZZZZA1 Siemens Trust Center Root-CA V3.0	X	-	-

Table 1: Root CA Implementation of ETSI requirements

1.2 Document Name and Identification

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

Title:	Certification Practice Statement of Siemens Root CAs
OID:	1.3.6.1.4.1.4329.99.2.1.1.1.0
Expiration:	This version of the document is the most current one until a subsequent release is published.

1.3 PKI Participants

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

1.3.1 Certification Authorities

Specified in the Certificate Policy.

1.3.2 Registration Authorities

Specified in the Certificate Policy.

1.3.3 Subscribers

Specified in the Certificate Policy.

1.3.4 Relying Parties

Specified in the Certificate Policy.

1.3.5 Other participants

Specified in the Certificate Policy.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

Specified in the Certificate Policy.

1.4.2 Prohibited Certificate Usage

Specified in the Certificate Policy.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Specified in the Certificate Policy.

1.5.2 Contact Person

Specified in the Certificate Policy.

2 Publication and Repository Responsibilities

2.1 Repositories

Specified in the Certificate Policy.

2.2 Publication of Certification Information

Specified in the Certificate Policy.

2.3 Time or Frequency of Publication

Specified in the Certificate Policy.

2.4 Access Controls on Repositories

Specified in the Certificate Policy.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Specified in the Certificate Policy.

3.1.2 Need of Names to be Meaningful

Specified in the Certificate Policy.

3.1.3 Anonymity or Pseudonymity of Subscribers

Specified in the Certificate Policy.

3.1.4 Rules for Interpreting Various Name Forms

Specified in the Certificate Policy.

3.1.5 Uniqueness of Names

Specified in the Certificate Policy.

3.1.6 Recognition, Authentication, and Roles of Trademarks

Specified in the Certificate Policy.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Specified in the Certificate Policy.

3.2.2 Identification and Authentication of Organization Identity

Specified in the Certificate Policy.

3.2.3 Identification and Authentication of Individual Identity

Specified in the Certificate Policy.

3.2.4 Non-verified Subscriber Information

Specified in the Certificate Policy.

3.2.5 Validation of Authority

Specified in the Certificate Policy.

3.2.6 Criteria for Interoperation between Communities of Trusts

Specified in the Certificate Policy.

3.3 Identification and Authentication for Re-key Requests

Specified in the Certificate Policy.

3.4 Identification and Authentication for Revocation Requests

Specified in the Certificate Policy.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Specified in the Certificate Policy.

4.1.2 Enrollment Process and Responsibilities

Specified in the Certificate Policy.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

Specified in the Certificate Policy.

4.2.2 Approval or Rejection of Certificate Applications

Specified in the Certificate Policy.

4.2.3 Time to Process Certificate Applications

Specified in the Certificate Policy.

4.3 Certificate Issuance

4.3.1 Root CA actions during Certificate issuance

Specified in the Certificate Policy.

4.3.2 Notification to Subscriber by the CA of Certificate issuance

Specified in the Certificate Policy.

4.4 Certificate Acceptance

4.4.1 Conduct constituting Certificate acceptance

Specified in the Certificate Policy.

4.4.2 Publication of the Certificate by the CA

Specified in the Certificate Policy.

4.4.3 Notification of Certificate issuance by the CA to other entities

Specified in the Certificate Policy.

4.5 Key Pair and Certificate Usage

4.5.1 Subject Private Key and Certificate Usage

Specified in the Certificate Policy.

4.5.2 Relying Party Public Key and Certificate Usage

Specified in the Certificate Policy.

4.6 Certificate Renewal

Specified in the Certificate Policy.

4.6.1 Circumstance for Certificate Renewal

Specified in the Certificate Policy.

4.6.2 Who may request renewal?

Specified in the Certificate Policy.

4.6.3 Processing Certificate Renewal Request

Specified in the Certificate Policy.

4.6.4 Notification of new Certificate Issuance to Subject

Specified in the Certificate Policy.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Specified in the Certificate Policy.

4.6.6 Publication of the Renewal Certificate by the CA

Specified in the Certificate Policy.

4.6.7 Notification of Certificate Issuance by the CA to the Entities

Specified in the Certificate Policy.

4.7 Certificate Re-key

Specified in the Certificate Policy.

4.7.1 Circumstances for Certificate Re-key

Specified in the Certificate Policy.

4.7.2 Who may request certification of a new Public Key?

Specified in the Certificate Policy.

4.7.3 Processing Certificate Re-keying Requests

Specified in the Certificate Policy.

4.7.4 Notification of new Certificate Issuance to Subscriber

Specified in the Certificate Policy.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Specified in the Certificate Policy.

4.7.6 Publication of the Re-keyed Certificate by the CA

Specified in the Certificate Policy.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

Specified in the Certificate Policy.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Specified in the Certificate Policy.

4.8.2 Who may request Certificate modification?

Specified in the Certificate Policy.

4.8.3 Processing Certificate Modification Requests

Specified in the Certificate Policy.

4.8.4 Notification of new Certificate Issuance to Subject

Specified in the Certificate Policy.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Specified in the Certificate Policy.

4.8.6 Publication of the Modified Certificate by the CA

Specified in the Certificate Policy.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Specified in the Certificate Policy.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Specified in the Certificate Policy.

4.9.2 Who can request revocation?

Specified in the Certificate Policy.

4.9.3 Procedure for Revocation Request

Specified in the Certificate Policy.

4.9.4 Revocation Request Grace Period

Specified in the Certificate Policy.

4.9.5 Time within which CA must Process the Revocation Request

Specified in the Certificate Policy.

4.9.6 Revocation Checking Requirement for Relying Parties

Specified in the Certificate Policy.

4.9.7 CRL Issuance Frequency

Specified in the Certificate Policy.

4.9.8 Maximum Latency for CRLs

Specified in the Certificate Policy.

4.9.9 On-line Revocation/Status Checking Availability

Specified in the Certificate Policy.

4.9.10 Other Forms of Revocation Advertisements Available

Specified in the Certificate Policy.

4.9.11 Special Requirements for Private Key Compromise

Specified in the Certificate Policy.

4.9.12 Circumstances for Suspension

Specified in the Certificate Policy.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Specified in the Certificate Policy.

4.10.2 Service Availability

Specified in the Certificate Policy.

4.10.3 Optional Features

Specified in the Certificate Policy.

4.11 End of Subscription

Specified in the Certificate Policy.

4.12 Key Escrow and Recovery

Specified in the Certificate Policy.

5 Management, Operational, and Physical Controls

Management, operational, and physical controls are defined in accordance with [ETSI-F].

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 102 042 V2.4.1 (2013-02):

- ❑ 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.

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 Root 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.

5.4.1 Types of Events Recorded

The following types of data shall be recorded, which include information about events of the Root CA operation:

- ❑ Monitoring data
  Data present an ongoing overview of Root CA's operations and includes information of system status, penetration attempts and current warnings.
- ❑ Logging data
  Access to the Root CA secure facilities is traced by this data, also entry and exit from additional secure rooms (e.g. backup facilities). Access to computer systems is traced in system log files.
- ❑ Audit data
  Root CA operations are recorded in the audit documentation of the events: Audit data of Certificate Life Cycle relevant events are generated with the issuing, transfer and revocation of Certificates and the related key material. Audit data is collected and stored for a longer period of time than monitoring data. Furthermore, changes of hardware and/or software components are also documented. The documentation is regularly checked as part of the Compliance Audit Procedures.

5.4.2 Frequency of Processing Audit Logging Information

Audit und logging data have to be controlled by the PMA after all CA events.

5.4.3 Retention Period for Audit Logging Information

Audit logs are retained onsite unlimited.

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 regular 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 is at least six weeks. The retention period for Automatic Audit Data 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.

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 stipulation.

5.5.6 Archive Collection System (internal or external)

No stipulation.

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

Keys expire at the same time as their associated Certificates. Key Changeover must occur before the expiration of its Certificates (stop issuance date) and shall be performed manually.

CA	Validity period	Operational period (Stop Issuance Date)
Siemens Root CAs	12 years	6 years

At "Stop Issuance Date" Siemens CA stops issuing Certificates with old key and initiate generation of new keys. The new Certificate of the new Public Key is published. Certificate Requests received after the "Stop Issuance Date," will be signed with the new CA Private Key.

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.

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;
- ❑ 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;
- ❑ 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-TS 102042].

The technical security controls address:

- ❑ the security measures taken by the Siemens CA to protect its Root Key Pairs and Activation Data (e.g. passwords)
- ❑ other technical security controls used to perform securely the functions listed in CP § 1.1, including technical controls such as life-cycle security controls (e.g., software development environment security, trusted software development methodology) and operational security controls.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The Key Pairs of the Root CAs and Issuing CAs are currently generated with a hardware security module ("HSM"), which is certified in accordance with FIPS 140-2 level 3.

6.1.2 Private Key Delivery to Subject

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

Not applicable.

6.1.4 CA Public Key delivery Relying Parties

The Certificates of Siemens CA are distributed to Relying Parties for Certificate path validation purposes. Siemens CAs' Public Keys are published at the Siemens PKI Website.

6.1.5 Key Sizes

The algorithms and key lengths allowed by Siemens CA are defined in the Certificate Profile document available on www.siemens.com/pki.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes

"KeyUsage" extension fields of Siemens CA Certificates are specified in accordance RFC 5280 and defined in the Certificate Profile document.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The Cryptographic Module (HSM) used to operate the Siemens CA is certified to FIPS 140-2 level 3 and the Common Criteria ("CC"), Evaluation Assurance Level (" EAL") 4+, which is generally equivalent to Information Technology Security Evaluation Criteria (ITSEC) assurance level E3.

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

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

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

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

Private Keys will be re-generated using a key regeneration card set. Key re-generation procedure is documented and must be done under dual control in a physically secure site.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

6.2.7 Storage of Private Keys on the Cryptographic Module

Siemens Root CA´s Private Key is held in HSM backup modules in encrypted form.

6.2.8 Method of Activating Private Key

Siemens Root CA´s Private Key can be activated by introducing the pre-defined number of Operator Cards in the HSM. Root CA Private Key activation requires entry and validation of a PIN/passphrase compliant with specified security parameters.

6.2.9 Method of Deactivating Private Key

After use, the Private Keys shall be deactivated by taking the Operator Cards out of the HSM.

6.2.10 Method of Destroying Private Key

Private Keys shall be destroyed if they are no longer needed, or when the Certificates to which they correspond expire or are revoked. CA Private Key destruction requires the participation of at least three trusted employees. Private Keys shall be destroyed in a way that prevents their loss, theft, modification, unauthorized disclosure, or unauthorized use.

When performed, the destruction process is logged.

6.2.11 Cryptographic Module Rating

In general the HSMs are operated with firmware levels that are certified according to FIPS 140-2 Level 3. Siemens reserves the right to operate its HSMs with OEM firmware at levels or configurations that are not certified according to FIPS 140-2 Level 3 if there is an operational or security need for it and if there is no newer FIPS certified firmware or configuration available.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The operational period of a Certificate ends upon its expiration or revocation. The operational period for Key Pairs is the same as the operational period for the associated Certificates, except that they may continue to be used for signature verification. The maximum operational periods for Root CA Certificates are set forth in table below.

Certificate	Validity Period
Siemens Root CA Certificate	Up to twelve (12) years

The applicability of cryptographic algorithms and parameters is constantly supervised by the PMA. If an algorithm or the appropriate key length offers no sufficient security during validity period of the Certificate, the concerned Certificate will be revoked and new Certificate Application will be initiated.

6.4 Activation Data

Activation Data refer to data values required to operate Cryptographic Modules such as a PIN, pass phrase. Activation data protection complies with FIPS 140-1, level 3.

6.4.1 Activation Data Generation and Installation

No stipulation.

6.4.2 Activation Data Protection

No stipulation.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

All computer security technical controls implemented for the Siemens CAs and Certificate Validation Service are established and documented in accordance to the ISMS Regulations.
All computers at the Siemens CA are subject to constant monitoring. Monitoring results are available 24 hours, 7 days a week. The configuration of system components may only be performed under dual control.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

System development controls are provided in accordance with systems development and change management standards of ISMS. Systems development is performed by trusted software supplier(s) in accordance with specifications for secure programming.

6.6.2 Security Management Controls

Siemens CA's security management controls are provided in compliance with Siemens ISMS.

6.6.3 Life Cycle of Security Controls

All Security Controls are audited annually by an external auditor.

6.7 Network Security Controls

The Siemens Root CA is maintained off-line and is not networked with any external components.

6.8 Time Stamp Process

No stipulation.

7 Certificate, CRL, and OCSP Profiles

All digital Certificates issued by the root CAs comply with digital Certificate and CRL profiles as described in [RFC 5280].

7.1 Certificate Profile

Detailed description of the Root CA profiles can be downloaded on http://www.siemens.com/pki

7.2 CRL Profile

Detailed description of the CRL profiles can be downloaded on http://www.siemens.com/pki

7.3 OCSP Profile

Detailed description of the OCSP profiles can be downloaded on http://www.siemens.com/pki

8 Compliance Audit and Other Assessment

Specified in the Certificate Policy.

9 Other Business and Legal Matters

Specified in the Certificate Policy.

10 References

Specified in the Certificate Policy.

Annex A: Acronyms and Definitions

A.1 Definitions

Specified in the Annex of the Certificate Policy.

A.2 Abbreviations

Specified in the Annex of the Certificate Policy.