



Certification Practice Statement

Siemens Issuing CAs

Document History

Version	Date	Author	Change Comment
1.0	June 10, 2016	Alexander Winnen, Michael Munzert	First version
1.1	December 1, 2016	Rufus Buschart	Minor updated version
1.2	May 26, 2017	Rufus Buschart	Update Issuing CAs 2017
1.3	July 31, 2017	Björn Hundertmarck	Update with chapter for 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 Certification Practice Statement (CPS) for the Siemens Issuing Certification Authorities (Issuing CAs). The purpose of this document is to publicly disclose to subscribers and relying parties the business policies and practices under which these Issuing CAs are operated.

Document Status

This document with version 1.3 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 August 23, 2017
Authorization	Markus Wichmann	Siemens GS IT ISEC	August 23, 2017

This CPS has been approved by the responsible Siemens information security officer on August 23, 2017.

Table of Content

Scope and Applicability	2
Document Status	2
1 Introduction	8
1.1 Overview	8
1.2 Document Name and Identification	10
1.3 PKI Participants	10
1.3.1 Certification Authorities	10
1.3.2 Registration Authorities	10
1.3.3 Subscribers	10
1.3.4 Relying Parties	10
1.3.5 Other participants	10
1.4 Certificate Usage	10
1.4.1 Appropriate Certificate Usage	10
1.4.2 Prohibited Certificate Usage	10
1.5 Policy Administration	10
1.5.1 Organization Administering the Document	10
1.5.2 Contact Person	10
2 Publication and Repository Responsibilities	11
2.1 Repositories	11
2.2 Publication of Certification Information	11
2.3 Time or Frequency of Publication	11
2.4 Access Controls on Repositories	11
3 Identification and Authentication	12
3.1 Naming	12
3.1.1 Types of Names	12
3.1.2 Need of Names to be Meaningful	12
3.1.3 Anonymity or Pseudonymity of Subscribers	12
3.1.4 Rules for Interpreting Various Name Forms	12
3.1.5 Uniqueness of Names	12
3.1.6 Recognition, Authentication, and Roles of Trademarks	12
3.2 Initial Identity Validation	12
3.2.1 Method to Prove Possession of Private Key	12
3.2.2 Identification and Authentication of Organization Identity	12
3.2.3 Identification and Authentication of Individual Identity	12
3.2.4 Non-verified Subscriber Information	12
3.2.5 Validation of Authority	12
3.2.6 Criteria for Interoperation between Communities of Trusts	12
3.3 Identification and Authentication for Re-key Requests	12
3.4 Identification and Authentication for Revocation Requests	13

4 Certificate Lifecycle Operational Requirements 14

- 4.1 Certificate Application 14
 - 4.1.1 Who can submit a certificate application? 14
 - 4.1.2 Enrollment Process and Responsibilities 14
- 4.2 Certificate Application Processing 15
 - 4.2.1 Performing identification and authentication functions 15
 - 4.2.2 Approval or Rejection of Certificate Applications 15
 - 4.2.3 Time to Process Certificate Applications 15
 - 4.2.4 Certificate Authority Authorization (CAA) 15
- 4.3 Certificate Issuance 15
 - 4.3.1 Issuing CA actions during Certificate issuance 15
 - 4.3.2 Notification to Subscriber by the CA of Certificate issuance 15
- 4.4 Certificate Acceptance 15
 - 4.4.1 Conduct constituting Certificate acceptance 15
 - 4.4.2 Publication of the Certificate by the CA 15
 - 4.4.3 Notification of Certificate issuance by the CA to other entities 16
- 4.5 Key Pair and Certificate Usage 16
 - 4.5.1 Subject Private Key and Certificate Usage 16
 - 4.5.2 Relying Party Public Key and Certificate Usage 16
- 4.6 Certificate Renewal 17
 - 4.6.1 Circumstance for Certificate Renewal 17
 - 4.6.2 Who may request renewal? 17
 - 4.6.3 Processing Certificate Renewal Request 17
 - 4.6.4 Notification of new Certificate Issuance to Subject 17
 - 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 17
 - 4.6.6 Publication of the Renewal Certificate by the CA 17
 - 4.6.7 Notification of Certificate Issuance by the CA to the Entities 17
- 4.7 Certificate Re-key 17
 - 4.7.1 Circumstances for Certificate Re-key 18
 - 4.7.2 Who may request certification of a new Public Key? 18
 - 4.7.3 Processing Certificate Re-keying Requests 18
 - 4.7.4 Notification of new Certificate Issuance to Subscriber 18
 - 4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 18
 - 4.7.6 Publication of the Re-keyed Certificate by the CA 18
 - 4.7.7 Notification of Certificate Issuance by the CA to other Entities 18
- 4.8 Certificate Modification 18
- 4.9 Certificate Revocation and Suspension 19
 - 4.9.1 Circumstances for Revocation 19
 - 4.9.2 Who can request revocation? 19
 - 4.9.3 Procedure for Revocation Request 19
 - 4.9.4 Revocation Request Grace Period 19
 - 4.9.5 Time within which CA must Process the Revocation Request 19
 - 4.9.6 Revocation Checking Requirement for Relying Parties 19

- 4.9.7 CRL Issuance Frequency..... 19
- 4.9.8 Maximum Latency for CRLs..... 19
- 4.9.9 On-line Revocation Checking Requirements 19
- 4.9.10 Other Forms of Revocation Advertisements Available 19
- 4.9.11 Special Requirements for Private Key Compromise..... 19
- 4.9.12 Circumstances for Suspension..... 19
- 4.10 Certificate Status Services 20
 - 4.10.1 Operational Characteristics 20
 - 4.10.2 Service Availability..... 20
 - 4.10.3 Optional Features 20
- 4.11 End of Subscription..... 20
- 4.12 Key Escrow and Recovery 20
- 5 Management, Operational, and Physical Controls..... 21**
 - 5.1 Physical Security Controls..... 21
 - 5.1.1 Site Location and Construction 21
 - 5.1.2 Physical Access 21
 - 5.1.3 Power and Air Conditioning 21
 - 5.1.4 Water Exposure 21
 - 5.1.5 Fire Prevention and Protection 21
 - 5.1.6 Media Storage 21
 - 5.1.7 Waste Disposal 21
 - 5.1.8 Off-site Backup..... 21
 - 5.2 Procedural Controls..... 21
 - 5.2.1 Trusted Roles..... 21
 - 5.2.2 Numbers of Persons Required per Task..... 21
 - 5.2.3 Identification and Authentication for each Role 21
 - 5.2.4 Roles Requiring Separation of Duties 21
 - 5.3 Personnel Security Controls..... 22
 - 5.3.1 Qualifications, Experience and Clearance Requirements..... 22
 - 5.3.2 Background Check Procedures 22
 - 5.3.3 Training Requirements..... 22
 - 5.3.4 Retraining Frequency and Requirements 22
 - 5.3.5 Job Rotation Frequency and Sequence..... 22
 - 5.3.6 Sanctions for Unauthorized Actions 22
 - 5.3.7 Independent Contractor Requirements 22
 - 5.3.8 Documents Supplied to Personnel 22
 - 5.4 Audit Logging Procedures 22
 - 5.4.1 Types of Events Recorded 22
 - 5.4.2 Frequency of Processing Audit Logging Information..... 22
 - 5.4.3 Retention Period for Audit Logging Information 22
 - 5.4.4 Protection of Audit Logs 22
 - 5.4.5 Backup Procedures for Audit Logging Information..... 22
 - 5.4.6 Collection System for Monitoring Information (internal or external)..... 22

5.4.7	Notification to Event-causing Subject	22
5.4.8	Vulnerability Assessments	23
5.5	Records Archival	23
5.5.1	Types of Records Archived	23
5.5.2	Retention Period for Archived Audit Logging Information	23
5.5.3	Protection of Archived Audit Logging Information	23
5.5.4	Archive Backup Procedures	23
5.5.5	Requirements for Time-Stamping of Record	23
5.5.6	Archive Collection System (internal or external)	23
5.5.7	Procedures to Obtain and Verify Archived Information	23
5.6	Key Changeover	23
5.7	Compromise and Disaster Recovery	24
5.7.1	Incident and Compromise Handling Procedures	24
5.7.2	Corruption of Computing Resources, Software, and/or Data	24
5.7.3	Entity Private Key Compromise Procedures	24
5.7.4	Business Continuity Capabilities After a Disaster	24
5.8	CA Termination	24
6	Technical Security Controls	25
6.1	Key Pair Generation and Installation	25
6.1.1	Key Pair Generation	25
6.1.2	Private Key Delivery to Subject	25
6.1.3	Public Key Delivery to Certificate Issuer	25
6.1.4	CA Public Key delivery Relying Parties	25
6.1.5	Key Sizes	25
6.1.6	Public Key Parameters Generation and Quality Checking	25
6.1.7	Key Usage Purposes	25
6.2	Private Key Protection and Cryptographic Module Engineering Controls	25
6.2.1	Cryptographic Module Standards and Controls	25
6.2.2	Private Key (n out of m) Multi-person Control	25
6.2.3	Private Key Escrow	25
6.2.4	Private Key Backup	26
6.2.5	Private Key Archival	26
6.2.6	Private Key Transfer into or from a Cryptographic Module	26
6.2.7	Storage of Private Keys on the Cryptographic Module	26
6.2.8	Method of Activating Private Key	26
6.2.9	Method of Deactivating Private Key	26
6.2.10	Method of Destroying Private Key	26
6.2.11	Cryptographic Module Rating	26
6.3	Other Aspects of Key Pair Management	27
6.3.1	Public Key Archival	27
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	27
6.4	Activation Data	27
6.4.1	Activation Data Generation and Installation	27

6.4.2	Activation Data Protection	27
6.4.3	Other Aspects of Activation Data	27
6.5	Computer Security Controls	27
6.6	Life Cycle Security Controls	28
6.6.1	System Development Controls.....	28
6.6.2	Security Management Controls.....	28
6.6.3	Life Cycle of Security Controls.....	28
6.7	Network Security Controls.....	28
6.8	Time Stamp Process	28
7	Certificate, CRL, and OCSP Profiles.....	29
7.1	Certificate Profile	29
7.2	CRL Profile	29
7.3	OCSP Profile.....	29
8	Compliance Audit and Other Assessment	30
9	Other Business and Legal Matters.....	31
10	References	32
Annex A: Acronyms and Definitions		33
A.1	Definitions.....	33
A.2	Abbreviations.....	33

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 Issuing CAs
- 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.

If new Issuing CAs may be introduced in the future additional CPS documents may be created, to cover special requirements.

The picture of the Siemens PKI hierarchy can be found in the Siemens Root CA CPS.

The following table lists the currently operated Issuing CAs as well as the requirements upon their issued certificates according to [ETSI 102 042] including the respective secure devices. Minimum requirement is NCP.

Issuing CA	Requirements for issued certificates						
	ETSI quality level			Secure device			
	NCP+	OVCP	DVCP	SmartCard	SmartPhone	HSM	NwSC
ZZZZZA2 Siemens Issuing CA EE Auth 2016	X			X			
ZZZZZA3 Siemens Issuing CA EE Enc 2016	X			X	X		X
ZZZZZA4 Siemens Issuing CA Intranet Code Signing 2016							
ZZZZZA5 Siemens Issuing CA Multipurpose 2016							
ZZZZZA6 Siemens Issuing CA Medium Strength Authentication 2016							
ZZZZZA7 Siemens Issuing CA Intranet Server 2016		X	X				
ZZZZZB7 Siemens Issuing CA Intranet Server 2017		X	X				
ZZZZZA8 Siemens Issuing CA Internet Code Signing 2016							
ZZZZZA9 Siemens Issuing CA Class Internet Server 2016		X	X				
ZZZZZB9 Siemens Issuing CA Class Internet Server 2017		X	X				
ZZZZZAD Siemens Issuing CA EE Network Smartcard Auth 2016							X
ZZZZZAB Siemens Issuing CA MSA Impersonalized Entities 2016							
ZZZZZY2 Siemens Issuing CA EE Auth 2013	X			X			
ZZZZZY3 Siemens Issuing CA EE Enc 2013	X			X	X		X
ZZZZZY4 Siemens Issuing CA Intranet Code Signing 2013							
ZZZZZY5 Siemens Issuing CA Multipurpose 2013							
ZZZZZY6 Siemens Issuing CA Medium Strength Authentication 2013							
ZZZZZY7 Siemens Issuing CA Intranet Server 2013		X	X				
ZZZZZY8 Siemens Issuing CA Internet Code Signing 2013							
ZZZZZY9 Siemens Issuing CA Class Internet Server 2013		X	X				
ZZZZZYB Siemens Issuing CA MSA Impersonalized Entities 2013							
ZZZZZV2 Siemens Issuing CA EE Auth 2011	X			X			
ZZZZZV3 Siemens Issuing CA EE Enc 2011	X			X	X		X
ZZZZZV4 Siemens Issuing CA Intranet Code Signing 2011							
ZZZZZV6 Siemens Issuing CA Medium Strength Authentication 2011							
ZZZZZV8 Siemens Issuing CA Internet Code Signing 2011							
ZZZZZVN Siemens Issuing CA Class PGP							

Table 1: Issuing CA Implementation of ETSI requirements

Siemens Issuing CAs issue Certificates to the below-specified groups of End Entities or class of applications with common security requirements ("Communities").

For Siemens PKI the following Communities exist:

- Siemens Employee (S-E)
- Functional Group (FG)
- Business Partner (BP)
- Device (e.g. Server - SRV)

1.2 Document Name and Identification

This CPS is referred to as the 'Certification Practice Statement of Siemens Issuing CAs'.

Title: Certification Practice Statement of Siemens Issuing CAs
OID: 1.3.6.1.4.1.4329.99.2.2.1.1.0
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

Fehler! Hyperlink-Referenz ungültig.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

The table below sets forth the responsibilities for each type of Subscriber and Certificate Authentication/Digital Signatures (“A/D Certificate”); Encryption (“E Certificate”); and server Certificate (S Certificate)). For End Entity Certificates, Siemens Issuing CA does not provide “Renewal” and “Modification” operations, because these are covered by the “Re-key” process.

Abbreviations:

“End Entity” = EE; “Authorized Party” = AP; “Siemens Sponsor” = SS; PKI Self Service = PKISS

Certificate holder		Certificate lifecycle				
Community	Subscriber	Initial Application	Renewal	Re-Key	Modification	Revocation
Siemens Community	Siemens Employee <ul style="list-style-type: none"> • A/D Certificate • E Certificate • EFS Certificate 	AP via RA	No stipulation	EE or AP via RA or PKISS	No stipulation	EE or AP via RA or PKISS (only for E Cert)
	• Siemens Functional Group <ul style="list-style-type: none"> • A/D Certificate • E Certificate • Code Signing 	AP via RA	No stipulation	AP or SS via RA	No stipulation	AP or SS via RA
Business Partner Community	Business Partner <ul style="list-style-type: none"> • A/D Certificate • E Certificate • Multi Purpose Certificate 	SS or AP via RA	No stipulation	EE, or AP via RA or PKISS	No stipulation	AP or SS via RA and EE via PKISS
Server Community	Server <ul style="list-style-type: none"> • S Certificate 	AP via RA	No stipulation	AP via RA	No stipulation	AP via RA

Table 2: Certificate lifecycle for Siemens Issuing CAs

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Members of the Siemens Community and Business Partner Community and Server Community can act as Certificate Applicants.

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.

4.2.4 Certificate Authority Authorization (CAA)

Specified in the Certificate Policy.

4.3 Certificate Issuance

4.3.1 Issuing 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

Subscriber Certificates will be published in the Repository according to the following table.

	Siemens SCD	Siemens AD	External Repository
Repository Classification	internal	Internal	External
Authentication Certificates	No	No	No
Encryption Certificates	Yes	Yes	Yes
Multipurpose Certificates	No	No	Yes
EFS Certificates	No	No	No
Code Signing Certificates	No	No	No
Server Certificates	No	No	No

Table 3: Publication of Subscriber Certificates

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

For the Siemens Community Subjects (Siemens employees and Functional Groups): the Siemens Issuing CAs or the respective RAs have the responsibility of informing each Subjects of these responsibilities and any applicable limitations on the use of Certificates and Key Pairs imposed by Siemens-internal policies in accordance with employment law and practice governing the respective RA.

For the Business Partner Community Subjects, who are individuals and independent contractors: the Siemens Sponsor or its RA is responsible for informing Subjects of these responsibilities and any such limitations on use imposed by Siemens-internal policies in accordance with employment law and practice. For the Business Partner Community Subjects, who are employees or agents of legal entities which are Business Partners, the respective RA of the Business Partner has the responsibility of informing each Subject of these responsibilities and any applicable limitations on use imposed by the Business Partner-internal policies in accordance with employment law and practice governing the respective RA.

For the Server Community Subjects: the Siemens Issuing CAs or the respective RAs have the responsibility of informing each Subject of these responsibilities and any applicable limitations on the use of Certificates and Key Pairs imposed by Siemens-internal policies in accordance with employment law and practice governing the respective RA.

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

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 Checking Requirements

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

Specified in the Root CA CPS.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

Specified in the Root CA CPS.

5.1.2 Physical Access

Specified in the Root CA CPS.

5.1.3 Power and Air Conditioning

Specified in the Root CA CPS.

5.1.4 Water Exposure

Specified in the Root CA CPS.

5.1.5 Fire Prevention and Protection

Specified in the Root CA CPS.

5.1.6 Media Storage

Specified in the Root CA CPS.

5.1.7 Waste Disposal

Specified in the Root CA CPS.

5.1.8 Off-site Backup

Specified in the Root CA CPS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Specified in the Root CA CPS.

5.2.2 Numbers of Persons Required per Task

Specified in the Root CA CPS.

5.2.3 Identification and Authentication for each Role

Specified in the Root CA CPS.

5.2.4 Roles Requiring Separation of Duties

Specified in the Root CA CPS.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Specified in the Root CA CPS.

5.3.2 Background Check Procedures

Specified in the Root CA CPS.

5.3.3 Training Requirements

Specified in the Root CA CPS.

5.3.4 Retraining Frequency and Requirements

Specified in the Root CA CPS.

5.3.5 Job Rotation Frequency and Sequence

Specified in the Root CA CPS.

5.3.6 Sanctions for Unauthorized Actions

Specified in the Root CA CPS.

5.3.7 Independent Contractor Requirements

Specified in the Root CA CPS.

5.3.8 Documents Supplied to Personnel

Specified in the Root CA CPS.

5.4 Audit Logging Procedures

Specified in the Root CA CPS.

5.4.1 Types of Events Recorded

Specified in the Root CA CPS.

5.4.2 Frequency of Processing Audit Logging Information

Specified in the Root CA CPS.

5.4.3 Retention Period for Audit Logging Information

Specified in the Root CA CPS.

5.4.4 Protection of Audit Logs

Specified in the Root CA CPS.

5.4.5 Backup Procedures for Audit Logging Information

No stipulation.

5.4.6 Collection System for Monitoring Information (internal or external)

Specified in the Root CA CPS.

5.4.7 Notification to Event-causing Subject

Specified in the Root CA CPS.

5.4.8 Vulnerability Assessments

Specified in the Root CA CPS.

5.5 Records Archival

5.5.1 Types of Records Archived

Specified in the Root CA CPS.

5.5.2 Retention Period for Archived Audit Logging Information

Specified in the Root CA CPS.

5.5.3 Protection of Archived Audit Logging Information

Specified in the Root CA CPS.

5.5.4 Archive Backup Procedures

Specified in the Root CA CPS.

5.5.5 Requirements for Time-Stamping of Record

Specified in the Root CA CPS.

5.5.6 Archive Collection System (internal or external)

Specified in the Root CA CPS.

5.5.7 Procedures to Obtain and Verify Archived Information

Specified in the Root CA CPS.

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 Issuing CA	6 years	3 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

Specified in the Root CA CPS.

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

Specified in the Root CA CPS.

5.7.3 Entity Private Key Compromise Procedures

Specified in the Root CA CPS.

5.7.4 Business Continuity Capabilities After a Disaster

Specified in the Root CA CPS.

5.8 CA Termination

Specified in the Root CA CPS.

6 Technical Security Controls

Specified in the Root CA CPS.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Specified in the Root CA CPS.

6.1.2 Private Key Delivery to Subject

During the operation of the Siemens Issuing CAs, the trusted operator ensures that the CAs' Private Key do not leave its secure facility.

For an Authentication/Digital Signatures Certificate, there is no delivery of Private Key to Subscribers because each Subscriber will generate his own Private Key with the Secure Signature Creation Device ("SSCD"). For a Encryption Certificate, the Private Key will be securely delivered to the Subject through the respective RA, either by physically handing the Private Key to the Subject in person after Validation of Subject's identity or by securely mailing or delivering via courier the Private Key with procedure for Validation of Subject's identity or through PKISS.

For Server Certificates requested by PKCS#10 the Certificate Applicant is responsible for the security of the private key. The Siemens Issuing CA does not store or generate this key.

6.1.3 Public Key Delivery to Certificate Issuer

No stipulation.

6.1.4 CA Public Key delivery Relying Parties

Specified in the Root CA CPS.

6.1.5 Key Sizes

Specified in the Root CA CPS.

6.1.6 Public Key Parameters Generation and Quality Checking

Specified in the Root CA CPS.

6.1.7 Key Usage Purposes

Specified in the Root CA CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Specified in the Root CA CPS.

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

Specified in the Root CA CPS.

6.2.3 Private Key Escrow

For End Entity Subscribers having an Encryption Certificate, the Private Key will be escrowed by Siemens CA's trusted operator. For End Entity Subscribers having the *Authentication/Digital Certificate/Server Certificates*, there is no stipulation.

6.2.4 Private Key Backup

For Private Keys of Issuing CAs, separate backup hardware cryptographic modules are used and kept secure at separate sites in the trusted operator's backup locations during operation of the Issuing CA. The following requirements apply to Issuing CA Private Keys.

1. Hardware cryptographic modules used for Issuing CA Private Key storage are to meet the requirements of §6.2.1.
2. Issuing CA Private Keys are copied to backup hardware cryptographic modules in accordance with §6.2.6.
3. Modules containing onsite backup copies and disaster recovery copies of Issuing CA Private Keys are subject to the requirements of §5.1 and §6.2.1.

§6.2.3 addresses the backup of Subscriber Private Keys.

6.2.5 Private Key Archival

Issuing CA Private Key archival: No stipulation.

End Entity Subscriber Private Key archival: When Key Pairs reach the end of their Validity Period, the Key Pair will be archived for a period of at least thirty (30) years.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private Keys of the Issuing CAs are securely stored exclusively on hardware cryptographic modules. Where Issuing CA Key Pairs are backed up to an equivalent hardware cryptographic module, such Key Pairs are transported between modules in encrypted form inside the high security cell of the secure facility.

6.2.7 Storage of Private Keys on the Cryptographic Module

Issuing CA Private Keys are stored on hardware cryptographic modules with Common Criteria (CC) Evaluation Assurance Level (EAL) 4+, which is generally equivalent to Information Technology Security Evaluation Criteria (ITSEC) assurance level E3.

6.2.8 Method of Activating Private Key

Upon issuance, Issuing CA Private Keys are activated on the hardware cryptographic module in the trusted operator high security cell, which is witnessed by a representative of Siemens CA and at least two (2) authorized trusted operator employees and is documented for audit logging purposes.

End Entity Subscriber Private Keys are generally activated through Subscriber's use of Activation Data. All Siemens PKI Participants are required to protect the Activation Data for their Private Keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.9 Method of Deactivating Private Key

Issuing CA Private Keys on hardware cryptographic modules can be deactivated (and reactivated, if necessary) through deactivation software in the trusted operator's high security cell, which is witnessed by at least two authorized trusted operator employees and is documented for audit logging purposes.

6.2.10 Method of Destroying Private Key

Issuing CA private keys are solely stored within cryptographic hardware modules (see 6.2.7). Their destruction (in case they are no longer needed) requires the participation of three trusted employees. When performed, the destruction process is logged.

In case subject private keys are no longer needed, the corresponding certificate will be revoked. Due to key-recovery requirements for encryption keys, these keys will be securely archived by the corresponding Issuing CA. E.g. in case an employee leaves the company the corresponding employee card (which includes the private key) will be retracted and securely destroyed. The destruction process is documented accordingly.

6.2.11 Cryptographic Module Rating

Specified in the Root CA CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Specified in the Root CA CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Issuing CA Key Pair usage period is subject to the Validity Period of the Certificates issued by the CA. The Validity Period of the Private Key and Public Key of Issuing CAs, RAs and Subjects ends upon its expiration or revocation. This Validity Period is based on the Validity Period of the Root CA Certificate set forth in the table below.

	CA Certificate	Authentication/ Digital Signature Certificate	Encryption Certificate	EFS Certificate	Server Certificate	Multi-purpose Certificate	Code Signing Certificate
Siemens Issuing CAs	6	N/A	N/A	N/A	N/A	N/A	N/A
Siemens employee	N/A	3	3	3	N/A	N/A	N/A
Functional Group	N/A	1	1	N/A	N/A	N/A	3
Business Partner	N/A	1	1	N/A	N/A	1	N/A
Servers	N/A	N/A	N/A	N/A	1	N/A	N/A

Table 4 Validity Period of Certificates (in years from date of issuance)

6.4 Activation Data

Activation Data refers to data values other than whole Private Keys that are required to operate Private Keys or hardware cryptographic modules containing Private Keys, such as a PIN, password or portions of a Private Key used in a key-splitting scheme. Protection of Activation Data prevents unauthorized use of the Private Key, and potentially needs to be considered for the Siemens Issuing CA, RAs and Subjects.

No Activation Data for Siemens Issuing CA Private Keys are currently provided by its trusted operator to ensure fully automated CA operation with a minimum of manual intervention.

6.4.1 Activation Data Generation and Installation

Specified in the Root CA CPS.

6.4.2 Activation Data Protection

Specified in the Root CA CPS.

6.4.3 Other Aspects of Activation Data

Specified in the Root CA CPS.

6.5 Computer Security Controls

Specified in the Root CA CPS.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

Specified in the Root CA CPS.

6.6.2 Security Management Controls

Specified in the Root CA CPS.

6.6.3 Life Cycle of Security Controls

Specified in the Root CA CPS.

6.7 Network Security Controls

The Issuing CA's network security controls that protect the networks that tie together the single computer platforms and their applications (addressed in §6.5.1) are provided by trusted operator in accordance with its ISMS. They include the use of:

1. firewalls and other controls to protect the integrity of the networks of the PKI Participants from intrusion from external domains;
2. sufficiently strong authentication to ensure that the appropriate entities are communicating (e.g., RA communicating with Issuing CA), integrity mechanisms to ensure that the information being exchanged will not be modified, and confidentiality mechanisms to ensure that selected information is protected from unauthorized examination (e.g., through Digitally Signed or encrypted messages);
3. access controls to protect networks from unauthorized use; and
4. mechanisms to prevent damage from denial-of-service attacks.

All information technology (IT) components in the trusted operator's secure facility are protected by firewalls from different manufacturers, which permit only dedicated access to its innermost systems for Issuing CA operations. The resulting security is constantly checked with the help of targeted attempts to penetrate the Siemens-internal network by independent Siemens departments according to schedules that are not made generally known to the trusted operator.

6.8 Time Stamp Process

Specified in the Root CA CPS.

7 Certificate, CRL, and OCSP Profiles

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

7.1 Certificate Profile

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

7.2 CRL Profile

Detailed description of the CRLs policies 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.