

Siemens Corporate PKI

Certification Practice Statement for Siemens Issuing CAs

Version: 1.18
Date: 27.01.2026
Classification: Public / Unrestricted

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)
1.4	December 1, 2017	Florian Grotz	Revised Certificate Authority Authorization (CAA)
1.5	January 12, 2018	Rufus Buschart	Chapter „Document History“ Added changed after ballots Chapter 2.2 Link to https://catestsite.siemens.com/ added Chapter 4.9.1 Revocation reasons added Chapter 4.9.2 Who can request a revocation added Chapter 5 Moved to CP
1.6	January 31, 2018	Rufus Buschart	Chapter 3.2.2 Restructured Chapter 6.3.2 Server certificates clarified Chapter 6.5.1 2FA added
1.7	February 23, 2018	Rufus Buschart	License changed to CC BY-SA4.0 as required by Mozilla
1.8	March 16, 2018	Rufus Buschart	Chapter 1.1 Clarification of Issuing CA list Chapter 3.2.2.3 Additional validation methods
1.9	December 21, 2018	Rufus Buschart	Chapter 4.9.1 Updated to new requirements from BRGs
1.10	February 22, 2019	Rufus Buschart	All chapter No stipulations removed
1.11	February 10, 2020	Rufus Buschart	Chapter 1.1 Expired ICAs removed Chapter 3.2.2.3 Stop Issuance of TLS documented Minor changes
1.12	February 17, 2020	Rufus Buschart	Chapter 1.1 Added 2020 hierarchy Chapter 3.2.2.1 Removal of TLS domain validation Minor changes
1.13	July 29 , 2021	Mauricio Fernandez	Minor changes Chapter 7
1.14	February 17, 2022	Rufus Buschart	Minor corrections
1.15	February 21, 2023	Rufus Buschart	Minor adaptations
1.16	January 24, 2024	Ilias Cotoulas Marco Fechter	Adaptions over all chapters for SBR101 Minor format changes
1.17	January 24, 2025	Khaled Taleb Fabian Meister Marco Fechter	Added references to Adobe Cloud signing CA throughout the document Minor corrections
1.18	January 27, 2026	Fabian Meister Marco Fechter	Review and minor adjustments on format and wording in chapters 3 -7

This document will be reviewed every year or in the event of an important ad-hoc change according to the Information Security update process for documents. Changes to the CA/B Baseline Requirements will be reflected after passing of the respective ballot into this document. Each new version will be approved by the respective management level before being released.

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

Scope and Applicability

This document constitutes the 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 1.18 and status Released has been classified as “Unrestricted” and is licensed as CC BY-SA4.0.

	Name	Department	Date
Author	Various authors, detailed information in document history		
Checked by	Tobias Lange Florian Grotz	Siemens LS Siemens GS IT HR 7 4	June 10, 2016 February 20, 2019
Authorization	Vinay Kumar Tiwari	Siemens CYS INF SH	January 27, 2026

Table of Content

Scope and Applicability	2
Document Status	3
1 Introduction	8
1.1 Overview.....	8
1.2 Document Name and Identification.....	9
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.....	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
2 Publication and Repository Responsibilities	12
2.1 Repositories.....	12
2.2 Publication of Certification Information.....	12
2.3 Time or Frequency of Publication.....	12
2.4 Access Controls on Repositories.....	12
3 Identification and Authentication	13
3.1 Naming.....	13
3.1.1 Types of Names.....	13
3.1.2 Need of Names to be Meaningful.....	13
3.1.3 Anonymity or Pseudonymity of Subscribers.....	13
3.1.4 Rules for Interpreting Various Name Forms.....	13
3.1.5 Uniqueness of Names.....	13
3.1.6 Recognition, Authentication, and Roles of Trademarks.....	13
3.2 Initial Identity Validation.....	13
3.2.1 Method to Prove Possession of Private Key.....	14
3.2.2 Identification and Authentication of Organization Identity.....	14
3.2.2.1 Identity and Country.....	14
3.2.2.2 Identification and authentication of Organizations.....	14
3.2.2.3 DBA / Tradename.....	14
3.2.2.4 Validation of Domain Authorization or Control.....	14
3.2.2.5 Wildcard Domain Validation.....	15
3.2.2.6 Validation of mailbox authorization or control.....	15
3.2.2.7 Validating authority over mailbox via domain.....	15
3.2.2.8 Validating control over mailbox via email.....	15
3.2.2.9 Validating applicant as operator of associated mail server(s).....	15
3.2.2.10 CAA records.....	15
3.2.3 Identification and Authentication of Individual Identity.....	16
EE Certificates contain commonly understood names permitting the determination of the identity of the individual. The following attributes are directly.....	16
3.2.4 Non-verified Subscriber Information.....	16
3.2.5 Validation of Authority.....	16
3.2.6 Criteria for interoperation.....	16
3.2.7 Reliability of verification sources.....	16
3.3 Identification and Authentication for Re-key Requests.....	16
3.4 Identification and Authentication for Revocation Requests.....	16
4 Certificate Lifecycle Operational Requirements	17
4.1 Certificate Application.....	17
4.1.1 Who can submit a certificate application?.....	17
4.1.2 Enrollment Process and Responsibilities.....	17

4.2	Certificate Application Processing	18
4.2.1	Performing identification and authentication functions	18
4.2.2	Approval or Rejection of Certificate Applications	18
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	CA actions during Certificate issuance	18
4.3.2	Notification to Subscriber by the CA of Certificate issuance	18
4.4	Certificate Acceptance	18
4.4.1	Conduct constituting Certificate acceptance	18
4.4.2	Publication of the Certificate by the CA.....	18
4.4.3	Notification of Certificate issuance by the CA to other entities	18
4.5	Key Pair and Certificate Usage	19
4.5.1	Subject Private Key and Certificate Usage.....	19
4.5.2	Relying Party Public Key and Certificate Usage.....	19
4.6	Certificate Renewal.....	20
4.6.1	Circumstance for Certificate Renewal	20
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
4.7.3	Processing Certificate Re-keying Requests	20
4.7.4	Notification of new Certificate Issuance to Subscriber	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	20
4.8	Certificate Modification.....	21
4.9	Certificate Revocation and Suspension	21
4.9.1	Circumstances for Revocation	21
4.9.1.1	Reasons for Revoking a Subscriber Certificate	21
4.9.1.2	Reasons for Revoking a subordinate CA Certificate	22
4.9.2	Who can request revocation?	23
4.9.3	Procedure for Revocation Request	23
4.9.4	Revocation Request Grace Period	23
4.9.5	Time within which CA must Process the Revocation Request	23
4.9.6	Revocation Checking Requirement for Relying Parties	23
4.9.7	CRL Issuance Frequency.....	23
4.9.8	Maximum Latency for CRLs	23
4.9.9	On-line Revocation Checking Requirements	23
4.9.10	Other Forms of Revocation Advertisements Available	23
4.9.11	Special Requirements for Private Key Compromise	23
4.9.12	Circumstances for Suspension.....	23
4.10	Certificate Status Services	24
4.10.1	Operational Characteristics	24
4.10.2	Service Availability	24
4.10.3	Optional Features	24
4.11	End of Subscription	24
4.12	Key Escrow and Recovery	24
5	Management, Operational, and Physical Controls	25
5.1	Physical Security Controls.....	25
5.1.1	Site Location and Construction	25
5.1.2	Physical Access	25
5.1.3	Power and Air Conditioning	25
5.1.4	Water Exposure.....	25
5.1.5	Fire Prevention and Protection	25
5.1.6	Media Storage	25
5.1.7	Waste Disposal.....	25

5.1.8	Off-site Backup	25
5.2	Procedural Controls	25
5.2.1	Trusted Roles	25
5.2.2	Numbers of Persons Required per Task.....	25
5.2.3	Identification and Authentication for each Role	25
5.2.4	Roles Requiring Separation of Duties	25
5.3	Personnel Security Controls	26
5.3.1	Qualifications, Experience and Clearance Requirements.....	26
5.3.2	Background Check Procedures.....	26
5.3.3	Training Requirements	26
5.3.4	Retraining Frequency and Requirements	26
5.3.5	Job Rotation Frequency and Sequence.....	26
5.3.6	Sanctions for Unauthorized Actions	26
5.3.7	Independent Contractor Requirements	26
5.3.8	Documents Supplied to Personnel	26
5.4	Audit Logging Procedures.....	26
5.4.1	Types of Events Recorded	26
5.4.2	Frequency of Processing Audit Logging Information	26
5.4.3	Retention Period for Audit Logging Information.....	26
5.4.4	Protection of Audit Logs	26
5.4.5	Backup Procedures for Audit Logging Information	26
5.4.6	Collection System for Monitoring Information (internal or external)	26
5.4.7	Notification to Event-causing Subject	26
5.4.8	Vulnerability Assessments	27
5.5	Records Archival	27
5.5.1	Types of Records Archived	27
5.5.2	Retention Period for Archived Audit Logging Information	27
5.5.3	Protection of Archived Audit Logging Information	27
5.5.4	Archive Backup Procedures	27
5.5.5	Requirements for Time-Stamping of Record	27
5.5.6	Archive Collection System (internal or external)	27
5.5.7	Procedures to Obtain and Verify Archived Information	27
5.6	Key Changeover	27
5.7	Compromise and Disaster Recovery.....	28
5.7.1	Incident and Compromise Handling Procedures.....	28
5.7.2	Corruption of Computing Resources, Software, and/or Data	28
5.7.3	Entity Private Key Compromise Procedures.....	28
5.7.4	Business Continuity Capabilities After a Disaster	28
5.8	CA Termination	28
6	Technical Security Controls.....	29
6.1	Key Pair Generation and Installation.....	29
6.1.1	Key Pair Generation.....	29
6.1.2	Private Key Delivery to subscriber	29
6.1.3	Public Key Delivery to Certificate Issuer.....	30
6.1.4	CA Public Key delivery Relying Parties	30
6.1.5	Key Sizes	30
6.1.6	Public Key Parameters Generation and Quality Checking	30
6.1.7	Key Usage Purposes	30
6.2	Private Key Protection and Cryptographic Module Engineering Controls	30
6.2.1	Cryptographic Module Standards and Controls	31
6.2.2	Private Key (n out of m) Multi-person Control.....	31
6.2.3	Private Key Escrow	31
6.2.4	Private Key Backup	31
6.2.5	Private Key Archival.....	31
6.2.6	Private Key Transfer into or from a Cryptographic Module	31
6.2.7	Storage of Private Keys on the Cryptographic Module	31
6.2.8	Method of Activating Private Key.....	31
6.2.9	Method of Deactivating Private Key	32
6.2.10	Method of Destroying Private Key.....	32
6.2.11	Cryptographic Module Rating.....	32
6.3	Other Aspects of Key Pair Management.....	32

6.3.1	Public Key Archival	32
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	32
6.4	Activation Data	32
6.4.1	Activation Data Generation and Installation	33
6.4.2	Activation Data Protection	33
6.4.3	Other Aspects of Activation Data	33
6.5	Computer Security Controls	33
6.5.1	Specific computer security technical requirements	33
6.5.2	Computer security rating	33
6.6	Life Cycle Security Controls	33
6.6.1	System Development Controls	33
6.6.2	Security Management Controls	33
6.6.3	Life Cycle of Security Controls	33
6.7	Network Security Controls	33
6.8	Time Stamp Process	34
7	Certificate, CRL, and OCSP Profiles	35
7.1	Certificate Profile	35
7.1.1	Version Number	35
7.1.2	Certificate Extensions	35
7.1.2.1	Root CA Certificates	35
7.1.2.2	Subordinate CA Certificate	35
7.1.2.3	Subscriber Certificate	36
7.1.2.4	All Certificates	37
7.1.2.5	Application of RFC 5280	37
7.1.3	Algorithm Object Identifiers	37
7.1.3.1	SubjectPublicKeyInfo	37
7.1.3.2	SignatureAlgorithmIdentifier	38
7.1.4	Name Forms	39
7.1.4.1	Name Encoding	39
7.1.4.2	Subject Information – Subscriber Certificates	39
	Subject Information – Root Certificates and Subordinate CA Certificates	41
7.1.4.3	41
7.1.5	Name Constraints	42
7.1.6	Certificate Policy Object Identifier	42
7.1.6.1	Reserved Certificate Policy Identifiers for S/MIME Baseline Requirements	42
7.1.6.2	Reserved Certificate Policy Identifiers for Siemens CA	42
7.1.6.3	Root CA Certificates	43
7.1.6.4	Subordinate CA Certificates	43
7.1.6.5	Subscriber Certificates	43
7.1.7	Usage of Policy Constraints Extension	43
7.1.8	Policy Qualifiers Syntax and Semantics	43
7.1.9	Processing Semantics for the Critical Certificate Policies Extension	43
7.2	CRL Profile	43
7.2.1	Version Number	43
7.2.2	CRL and CRL Entry Extensions	43
7.3	OCSP Profile	44
7.3.1	Version Number	44
7.3.2	OCSP Extensions	44
8	Compliance Audit and Other Assessment	45
9	Other Business and Legal Matters	46
10	References	47
Annex A:	Acronyms and Definitions	48
A.1	Definitions	48
A.2	Abbreviations	48

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 EN TS 319 411-1] including the respective secure devices. Minimum requirement is NCP.

Issuing CA	Expiry date	Requirements for issued certificates						
		ETSI quality level			Secure device			
		NCP+	OVCP	DVCP	Smart Card	Smart-Phone	HSM	NSC/VSC
ZZZZZB2 Siemens Issuing CA EE Auth 2020	29/6/2026	X			X			
ZZZZZB3 Siemens Issuing CA EE Enc 2020	29/6/2026	X			X	X		X
ZZZZZBD Siemens Issuing CA EE Network Smartcard Auth 2020	29/6/2026	X						X
ZZZZZB6 Siemens Issuing CA Medium Strength Authentication 2020	29/6/2026							
ZZZZZD3 Siemens Issuing CA EE Enc 2021	28/7/2025	X			X	X		X
ZZZZZD2 Siemens Issuing CA EE Auth 2021	28/7/2025	X			X			
ZZZZZDD Siemens Issuing CA EE Network Smartcard Auth 2021	28/7/2025	X						X
ZZZZZD6 Siemens Issuing CA Medium Strength Authentication 2021	28/7/2025							
ZZZZZE3 Siemens Issuing CA EE Enc 2023	04/06/2028	X			X	X		X
ZZZZZE2 Siemens Issuing CA EE Auth 2023	04/06/2028	X			X			
ZZZZZE6 Siemens Issuing CA EE Network Smartcard Auth 2023	04/06/2028	X						X
ZZZZZE6 Siemens Issuing CA Medium Strength Authentication 2023	04/06/2028							
ZZZZZE5 Siemens Issuing CA Adobe short lived certificates 2023	05/06/2028							

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)

An S/MIME Certificate for the purposes of this document can be identified by the existence of an Extended Key Usage (EKU) for id-kp-emailProtection (OID: 1.3.6.1.5.5.7.3.4) and the inclusion of a rfc822Name or an otherName of type id-on-SmtpUTF8Mailbox in the subjectAltName extension.

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: 1.3.6.1.4.1.4329.99.2.2.1.17
 Expiration: This version of the document is the most current one until a subsequent release is published.

This CPS contains the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, as adopted by the CA/Browser Forum.

These Requirements describe four Certificate profiles differentiated by the type of Subject:

Certificate Type	Description
Mailbox-validated	Subject is limited to (optional) subject:emailAddress and/or subject:serialNumber attributes.
Organization-validated	Includes only Organizational (Legal Entity) attributes in the Subject.
Sponsor-validated	Combines Individual (Natural Person) attributes in conjunction with an subject:organizationName (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA.
Individual-validated	Includes only Individual (Natural Person) attributes in the Subject.

Table 2: SBR profiles for validation requirements

In addition, Generations (known as Legacy, Multipurpose, and Strict) are specified for each of these Certificate Types, acknowledging both the current diversity of practice in issuing S/MIME Certificates as well as the desire to move towards more closely-defined practices over time. The following Certificate Policy identifiers are reserved for use by CAs as a means of asserting compliance with this document (OID arc 2.23.140.1.5)¹ as follows:

Mailbox-validated

[SBR-OID] mailbox-validated (1) legacy (1) } (2.23.140.1.5.1.1); and
 [SBR-OID] mailbox-validated (1) multipurpose (2) } (2.23.140.1.5.1.2); and
 [SBR-OID] mailbox-validated (1) strict (3) } (2.23.140.1.5.1.3); and

Organization-validated

[SBR-OID] organization-validated (2) legacy (1) } (2.23.140.1.5.2.1); and
 [SBR-OID] organization-validated (2) multipurpose (2) } (2.23.140.1.5.2.2); and
 [SBR-OID] organization-validated (2) strict (3) } (2.23.140.1.5.2.3); and

Sponsor-validated

[SBR-OID] sponsor-validated (3) legacy (1) } (2.23.140.1.5.3.1); and
 [SBR-OID] sponsor-validated (3) multipurpose (2) } (2.23.140.1.5.3.2); and
 [SBR-OID] sponsor-validated (3) strict (3) } (2.23.140.1.5.3.3); and

Individual-validated

[SBR-OID] individual-validated (4) legacy pg. 9(1) } (2.23.140.1.5.4.1); and
 [SBR-OID] individual-validated (4) multipurpose (2) } (2.23.140.1.5.4.2); and
 [SBR-OID] individual-validated (4) strict (3) } (2.23.140.1.5.4.3).

¹ OIDs for CAB Forum's S/MIME baseline certificate-policies start with: {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) abbreviated as [SBR-OID]

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.

CN Issuing CA	Requirements for issued certificates	
	Serial Number (hex)	Fingerprint (SHA-256)
Siemens Issuing CA EE Auth 2020	601C83B3	244817A9C7D60184651D8041D8F34F9C6D26926689DA3 3233892FE915E40D065
Siemens Issuing CA EE Enc 2020	4724CFB9	167407C794A5BF5D3A4CE6B56FE81228300006A5FE55F0 1C07E8AA791762FA46
Siemens Issuing CA EE Network Smartcard Auth 2020	19393306	68C752B1981F111510A8E678775406597696B6B752B89B E04C6BEDDFEF294419
Siemens Issuing CA Medium Strength Authentication 2020	7C682BB5	8905AD1617C55305648EAB9533886155F8D4CE5B456F17 83FB47887BF928821A
Siemens Issuing CA EE Enc 2021	50094F56B2286DAACE7C6AED623F9968	A1C5D7B6D0DA22115F3A3841DA90528C9635903423EAF FD4416C2712476A040F
Siemens Issuing CA EE Auth 2021	435B94F668F3112B56B1F226882FFD29	477868C56C81FCC0ECE3B8AFFB54B1C3DF69E5D7AA54B 4A2C65EA67BE83AD3A
Siemens Issuing CA EE Network Smartcard Auth 2021	5503DF4A70A19BFAC6FFA305FF79AB97	A72298F93C48EF59E4328B7AE7B50F8CD48EC180BBD83D 3B5D4DD734D87464C0
Siemens Issuing CA Medium Strength Authentication 2021	474B9852D859806390A3006DC7B57E17	5AE5409197A3E77D37695D4BA795845C7A04F7BD7769E 9608044CAB9F74733C6
Siemens Issuing CA EE Enc 2023	71e6323fb63184f49715d2330d086aa8	05E7AB4F1795F4E76E9EF5D49B5AE1E46CB22DA833B175 8D031B8AAA7E2FDF84
Siemens Issuing CA EE Auth 2023	7468ba9573e8c5f00ff3b79cbd624764	CEC450B3354FCAC90219D71FAC4DC1CFF4A67B6102F87B 00A0301207FC2A4EFA
Siemens Issuing CA EE Network Smartcard Auth 2023	48017cf4b6848d1723c3ee6faf9d1bc3	1D4E9F45681E59D88853B38CA704F3738EE6E2B0BA2DFA DEB3ACAC4A0555739
Siemens Issuing CA Medium Strength Authentication 2023	7c052b64498efa09670951654986e099	6DC59E8EF20AE4304A53A0BDC15E0244897BEB6C75DEF5 F6999AD5BB882EC3F6
Siemens Issuing CA Adobe short lived certificates 2023	6f0e7929f2ebb12ce5c725fb75c4f30e	E78AAAD993803D1F7CEE4D0F0C2F3A36711E53357EE7E0 58AC0E62C5085BC79E

Table 3: Siemens Issuing CA CN, Serial Numbers and Fingerprints

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

The Certificates signed by the Siemens Issuing CAs are approved for the following usages:Certificate	Use
S/MIME certificates	Senders and recipients of email messages will have 'reasonable assurance' that the Subject identified in an S/MIME Certificate has control of the domain or Mailbox Address being asserted. A variation of this use case is where an Individual or organization digitally signs email to establish its authenticity and source of origin.
Client authentication certificates	Systems and service will have 'reasonable assurance' to authenticate clients (Individual, functions and organizations, based on the assurance level given by the respective CA.
Code Signing certificates	Certificates only intended to sign code and not to be used for S/MIME.

Table 4: Issuing CA Use Cases

Certificates may be issued to serve one or more use cases as described above (combined usage) and be used for any purpose as outlined in the 'key usage' and 'extended key usage' extension of the related certificate.

1.4.2 Prohibited Certificate Usage

All certificate usages not listed in chapter 1.4.1 are prohibited.

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

The CA SHALL authenticate all identity attributes of the Subject.

In case of S/MIME-certificates the CA SHALL authenticate all identity attributes of the Subject and their control over the Mailbox Addresses to be included in the S/MIME Certificate according to the requirements of the following sections:

Certificate Type	Mailbox Control	Organization Identity	Individual Identity
Mailbox-validated	Section 3.2.2.6	NA	NA
Organization-validated	Section 3.2.2.6	Section 3.2.2.7	NA
Sponsor-validated	Section 3.2.2.6	Section 3.2.2.7	Section 3.2.2.8
Individual-validated	Section 3.2.2.6	NA	Section 3.2.2.8

Table 5: Issuing CA Identity authentication requirements

3.2.1 Method to Prove Possession of Private Key

Specified in the Certificate Policy.

3.2.2 Identification and Authentication of Organization Identity

3.2.2.1 Identity and Country

All certificates are issued with the following information as part of the Subject Distinguished Name:

For the Siemens 2021 CA Hierarchy and newer

- O = Siemens
- S = Bayern
- C = DE

3.2.2.2 Identification and authentication of Organizations

All certificates are issued with the subject organization Siemens as stated in 3.2.2.1. The information is verified according to business registration München, HRB 6684; WEEE-Reg.-Nr. DE 23691322 and is authorized by Siemens management.

Certificates are not issued for legal entities. Siemens AG acts as the RA and authenticates the organizations that are named in the certificate. This means that the only organization entries permitted in the DN field "O" is "Siemens" for the CAs of the Siemens AG. Since the registered office of the organization ("Siemens") is relevant for the DN fields "C" and "S", the only value permitted for these entries are "C"="DE" and "S"="Bayern".

3.2.2.3 DBA / Tradename

No DBA / Tradename except of "Siemens" is to be included in a server certificate.

3.2.2.4 Validation of Domain Authorization or Control

Siemens CA only issues certificates for domains that are controlled by Siemens Community.

Siemens CA performs the validation of domain authorization. Siemens CA sends emails with a 64-character long string ("Random Value") consisting of upper and lower characters and digits to the Domain Contacts according the WHOIS-record (3.2.2.4.2) and the constructed email addresses (3.2.2.4.4) of every FQDN to validate. The Random Value is different for every receiver.

If one of the Domain Contacts approves the domain validation request by transmitting the Random Value back to the Siemens CA by the use of a web site, the domain is validated.

Siemens CA stopped the issuance of publicly trusted TLS certificates on October 15th 2019.

3.2.2.5 Wildcard Domain Validation

Siemens CA stopped the issuance of publicly trusted TLS certificates on October 15th 2019.

3.2.2.6 Validation of mailbox authorization or control

This section defines the permitted processes and procedures for confirming the Applicant's control of Mailbox Addresses to be included in issued Certificates.

The CA SHALL verify that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the email account holder to act on the account holder's behalf.

The CA SHALL NOT delegate the verification of mailbox authorization or control.

The CA's CP and/or CPS SHALL specify the procedures that the CA employs to perform this verification. CAs SHALL maintain a record of which validation method, including the relevant version number from the TLS Baseline Requirements or S/MIME Baseline Requirements, was used to validate every domain or email address in issued Certificates.

Completed validations of Applicant authority MAY be valid for the issuance of multiple Certificates over time. In all cases, the validation SHALL have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1) prior to Certificate issuance.

Note: Mailbox Fields MAY be listed in Subscriber Certificates using rfc822Name or otherNames of type id-on-SmtpUTF8Mailbox in the subjectAltName extension. Mailbox Fields MAY be listed in Subordinate CA Certificates via rfc822Name in permittedSubtrees within the nameConstraints extension.

3.2.2.7 Validating authority over mailbox via domain

The CA MAY confirm the Applicant, such as an Enterprise RA, has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the Mailbox Address to be used in the Certificate.

The CA SHALL use only the approved methods in Section 3.2.2.4 of the TLS Baseline Requirements to perform this verification.

For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

3.2.2.8 Validating control over mailbox via email

The CA MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

Control over each Mailbox Address SHALL be confirmed using a unique Random Value. The Random Value SHALL be sent only to the email address being validated and SHALL not be shared in any other way.

The Random Value SHALL be unique in each email. The Random Value SHALL remain valid for use in a confirming response for no more than 24 hours from its creation. The CA MAY specify a shorter validity period for Random Values in its CP and/or CPS.

The Random Value SHALL be reset upon each instance of the email sent by the CA to a Mailbox Address, however all relevant Random Values sent to that Mailbox Address MAY remain valid for use in a confirming response within the validity period described in this Section. In addition, the Random Value SHALL be reset upon first use by the user if intended for additional use as an authentication factor following the Mailbox Address verification.

3.2.2.9 Validating applicant as operator of associated mail server(s)

The CA MAY confirm the Applicant's control over each Mailbox Field to be included in the Certificate by confirming control of the SMTP FQDN to which a message delivered to the Mailbox Address should be directed. The SMTP FQDN SHALL be identified using the address resolution algorithm defined in RFC 5321 Section 5.1 which determines which SMTP FQDNs are authoritative for a given Mailbox Address. If more than one SMTP FQDN has been discovered, the CA SHALL verify control of an SMTP FQDN following the selection process at RFC 5321 Section 5.1. Aliases in MX record RDATA SHALL NOT be used for this validation method.

To confirm the Applicant's control of the SMTP FQDN, the CA SHALL use only the currently-approved methods in Section 3.2.2.4 of the TLS Baseline Requirements.

3.2.2.10 CAA records

The recent version of the S/MIME Baseline Requirements does not require the CA to check for CAA records. The CAA property tags for issue, issuewild, and iodef as specified in RFC 8659 are not recognized for the issuance of S/MIME Certificates.

3.2.3 Identification and Authentication of Individual Identity

EE Certificates contain commonly understood names permitting the determination of the identity of the individual. The following attributes are directly.

Natural persons must provide unambiguous proof of their identity Natural persons are identified and authenticated in the control sphere of the subscriber as the RA.

Basis for First Name, Last Name, GID and E-Mail address is an entry in the Corporate Directory based on HR processes or sponsorship by an employee of Siemens or a subsidiary or an affiliate.

“E-Mail” is based on the assigned e-mail address in the Corporate Directory which is in the control sphere of the subscriber as the RA. Only mail domains under the control of Siemens, its subsidiaries and affiliates and divested entities as reflected by the name constraints of the Issuing CA. SmartCards are only handed over after unambiguous proof of the holder’s identity by the RA or its representatives.

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

Siemens CA is member of the European Bridge CA and exchanges PKI related information with its partners. Cross Certificates that identify Siemens CA as the Subject are listed in the Repository where Siemens CA has arranged or accepted the establishment of the trust relationship.

3.2.7 Reliability of verification sources

Before relying on a source of verification data to validate Certificate Requests, the CA SHALL verify its suitability as a Reliable Data Source. Enterprise RA records are a Reliable Data Source for Individual Subject attributes included in Sponsor-validated Certificates issued to the Enterprise RA’s Organisation.

The CA or RA MAY rely upon a letter attesting that Subject Information or other fact is correct. The CA or RA SHALL verify that the letter was written by an accountant, lawyer, government official, or other reliable third party in the Applicant’s jurisdiction customarily relied upon for such information.

An Attestation SHALL include a copy of documentation supporting the fact to be attested. The CA or RA SHALL use a Reliable Method of Communication to contact the sender and to confirm the Attestation is authentic.

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	Not performed	EE or AP via RA or MyPKI	Not performed	EE or AP via RA or MyPKI (only for E Cert)
	Siemens Functional Group <ul style="list-style-type: none"> • A/D Certificate • E Certificate • Code Signing 	AP via RA	Not performed	AP or SS via RA	Not performed	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	Not performed	EE, or AP via RA or MyPKI	Not performed	AP or SS via RA and EE via MyPKI

Table 6: 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 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 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	Directory Broker (certbox)
Repository Classification	internal	Internal	Internal/External
Authentication Certificates	Yes	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 7: 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

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Prior to performing a revocation Siemens CA will verify the authenticity of the revocation request. Siemens CA revokes a Certificate within twenty-four (24) hours if one or more of the following occurs:

- I. The Subscriber requests in writing that Siemens CA shall revoke the Certificate;
- II. The Subscriber notifies Siemens CA that the original certificate request was not authorized and does not retroactively grant authorization;
- III. Siemens CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
- IV. Siemens CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see <https://wiki.debian.org/SSLkeys>);
- V. Siemens CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name, e-mail address or IP address in the Certificate should not be relied upon.

Siemens CA should revoke a certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following occurs:

- I. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
- II. Siemens CA obtains evidence that the Certificate was misused;
- III. Siemens CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
- IV. Siemens CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- V. Siemens CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- VI. Siemens CA is made aware of a material change in the information contained in the Certificate;
- VII. Siemens CA is made aware that the Certificate was not issued in accordance with these Requirements or Siemens CA's Certificate Policy or Certification Practice Statement;
- VIII. Siemens CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
- IX. Siemens CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless Siemens CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- X. Revocation is required by Siemens CA's Certificate Policy and/or Certification Practice Statement; or
- XI. Siemens CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Other Revocation Considerations

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

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

4.9.1.2 Reasons for Revoking a subordinate CA Certificate

Revocation of a Subordinate CA Certificate is performed within seven (7) days under the following Circumstances:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies Siemens CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
4. The Issuer CA obtains evidence that the CA Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable CP and/or CPS;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the Issuing CA's CP and/or CPS.

Other Revocation Considerations

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

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

4.9.2 Who can request revocation?

The following entities may request revocation of an End Entity Certificate.

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

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

Each CRL contains a sequentially increasing number assigned to every issued CRL

Issuing CA's that issue CRL's for subscriber certificates will re-issue and update at least once every seven days, and the value of the nextUpdate field will not be more than ten (10) days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates the CRL's will be re-issued and updated at least once every 6 month and within 24 hours after revoking a Subordinate CA Certificate. The value of the nextUpdate field will not be more than twelve (12) months beyond the value of the thisUpdate field.

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 Certificate Policy.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

Specified in the Certificate Policy.

5.1.2 Physical Access

Specified in the Certificate Policy.

5.1.3 Power and Air Conditioning

Specified in the Certificate Policy.

5.1.4 Water Exposure

Specified in the Certificate Policy.

5.1.5 Fire Prevention and Protection

Specified in the Certificate Policy.

5.1.6 Media Storage

Specified in the Certificate Policy.

5.1.7 Waste Disposal

Specified in the Certificate Policy.

5.1.8 Off-site Backup

Specified in the Certificate Policy.

5.2 Procedural Controls

5.2.1 Trusted Roles

Specified in the Certificate Policy.

5.2.2 Numbers of Persons Required per Task

Specified in the Certificate Policy.

5.2.3 Identification and Authentication for each Role

Specified in the Certificate Policy.

5.2.4 Roles Requiring Separation of Duties

Specified in the Certificate Policy.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Specified in the Certificate Policy.

5.3.2 Background Check Procedures

Specified in the Certificate Policy.

5.3.3 Training Requirements

Specified in the Certificate Policy.

5.3.4 Retraining Frequency and Requirements

Specified in the Certificate Policy.

5.3.5 Job Rotation Frequency and Sequence

Specified in the Certificate Policy.

5.3.6 Sanctions for Unauthorized Actions

Specified in the Certificate Policy.

5.3.7 Independent Contractor Requirements

Specified in the Certificate Policy.

5.3.8 Documents Supplied to Personnel

Specified in the Certificate Policy.

5.4 Audit Logging Procedures

Specified in the Certificate Policy.

5.4.1 Types of Events Recorded

Specified in the Certificate Policy.

5.4.2 Frequency of Processing Audit Logging Information

Specified in the Certificate Policy.

5.4.3 Retention Period for Audit Logging Information

Specified in the Certificate Policy.

5.4.4 Protection of Audit Logs

Specified in the Certificate Policy.

5.4.5 Backup Procedures for Audit Logging Information

Specified in the Certificate Policy.

5.4.6 Collection System for Monitoring Information (internal or external)

Specified in the Certificate Policy.

5.4.7 Notification to Event-causing Subject

Specified in the Certificate Policy.

5.4.8 Vulnerability Assessments

Specified in the Certificate Policy.

5.5 Records Archival

5.5.1 Types of Records Archived

Specified in the Certificate Policy.

5.5.2 Retention Period for Archived Audit Logging Information

Specified in the Certificate Policy.

5.5.3 Protection of Archived Audit Logging Information

Specified in the Certificate Policy.

5.5.4 Archive Backup Procedures

Specified in the Certificate Policy.

5.5.5 Requirements for Time-Stamping of Record

Specified in the Certificate Policy.

5.5.6 Archive Collection System (internal or external)

Specified in the Certificate Policy.

5.5.7 Procedures to Obtain and Verify Archived Information

Specified in the Certificate Policy.

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	5-6 years	2-3 years

Table 8: Issuing CA Operational Period

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 Certificate Policy.

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

Specified in the Certificate Policy.

5.7.3 Entity Private Key Compromise Procedures

Specified in the Certificate Policy.

5.7.4 Business Continuity Capabilities After a Disaster

Specified in the Certificate Policy.

5.8 CA Termination

Specified in the Certificate Policy.

6 Technical Security Controls

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

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

6.1.1.1 CA key pair generation

Siemens CA generates and stores all key pairs used for Root CA or Subordinated CA within a Hardware-Security-Module (HSM) which is at least certified to FIPS 140-2 level 3 or FIPS 140-3 level 3 standard.

All activities to generate key pairs for Root- or Subordinate CA's are performed within a so called "CA Event". The CA Event will be conducted by specialized trusted staff (PKI & HSM Administrators) inside a low-radiation room on a HSM device. All steps and needed actions are planned and written down in advance into a CA Event Script. During the CA Event all activities will be documented and signed at least by two PKI Administrators and in addition all Events will be video recorded.

Key pairs for Root CA certificates are generated within an offline environment consisting of CA system with connected Hardware-Security-Module.

For all CA key generation Events a qualified auditor participates the CA Event. If participation of an Auditor is not possible regarding special and exceptional situations the entire video recording of the whole key generation Event will be reviewed by a qualified and independent Auditor.

6.1.1.2 RA key pair generation

No stipulation.

6.1.1.3 Subscriber key pair generation

The Applicant or Subscriber is required to generate or initiate the generation of a new key-pair to be used in association with the subscriber's certificate request or applicant's certificate application.

Key pairs issued for end-entity authentication and signature certificates on corporate ID card are generated on the token itself (PKCS#11) by the manufacturer of the smart card which is currently CardOS 5.3 from Eviden formerly ATOS.

Key pairs issued for end-entity authentication and signature certificates for a Virtual-Smart-Card are generated centrally within the Siemens CA Trust Center in a special protected environment using a Hardware-Security-Module (HSM) and stored securely inside the vendors system which is currently Safenet IDPrime Virtual from Thales.

Key pairs for end-entity encryption certificates are generated centrally within the Siemens CA Trust Center in a special protected environment using a Hardware-Security-Module (HSM) and stored securely on the corporate ID card during personalization. These keys will be also securely archived for key recovery.

Other end-entity keys based on Soft-PSE token are generated centrally within the Siemens CA Trust Center in a special protected environment using a Hardware-Security-Module (HSM).

6.1.2 Private Key Delivery to subscriber

For an Authentication/Digital Signatures Certificate based on corporate ID card or Virtual Smart Card token, there is no delivery of Private Key to Subscribers because each Subscriber will generate the Private Key on his personal token like physically smart card or virtual smart card.

For an 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 subscriber 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 through PKISS/MyPKI.

Example methods include using a 128-bit AES key to wrap the Private Key or storing the key in a PKCS 12 file encrypted using a password and algorithm whose combination provides at least 112 bits of encryption strength. The password for PKCS 12 file is a random generated password with more than 16 characters containing uppercase letters, lowercase letters, numbers, and symbols for transport.

The material used to activate/protect the Private Key (e.g., a password used to secure a PKCS 12 file) must be delivered to the EE-Subscriber securely and separately from the container holding the Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

No stipulation.

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, parameters and key lengths allowed by Siemens CA are defined in the Certificate Profile document available on www.siemens.com/pki based on the recommendations of ETSI TS 119 312.

Siemens CA is using RSA keys within Corporate PKI with following key sizes:

- 4096 bit for Root- and Subordinate CA certificates
- 3072 bit for end-entity certificates after 26. August 2025
- 2048 bit for end-entity certificates before 27. August 2025

6.1.6 Public Key Parameters Generation and Quality Checking

While issuing a certificate the Public Key is checked against known weaknesses like ROCA or Debian Weak Key.

For RSA keys the most common public exponent 0x10001 (65537) is used.

6.1.7 Key Usage Purposes

Private keys corresponding to Root CA Certificates are just used to sign

- Certificates for Subordinate CAs (Intermediate CA, Issuing CA)
- Certificates for OCSP Response verification

"KeyUsage" extension fields of Siemens CA Certificates are specified in accordance RFC 5280 and defined in the Certificate Profile document on www.siemens.com/pki

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Siemens CA has implemented physical, organizational and technical mechanisms to ensure the security of all kind of CA keys like Root-CA, Subordinate- or Issuing CA.

All private keys for certification authorities are stored securely on an HSM inside Trust Center and protected against unauthorized use.

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

Private Key Escrow is not being performed for Root-, Subordinate and Issuing CA keys.

Only for End Entity Subscribers having an Encryption Certificate, the Private Key will be escrowed by Siemens CA in encrypted form and protected against unauthorized access and disclosure.

6.2.4 Private Key Backup

For all private Keys of Root-, Subordinate and Issuing CA's separate backup hardware cryptographic modules are used and kept secure at separate sites inside special Trust Center rooms with safes and physical authorization access control. The following requirements apply to all kind of CA Private Keys.

1. Hardware cryptographic modules used for CA Private Key storage are to meet the requirements of §6.2.1.
2. CA Private Keys are copied to backup hardware cryptographic modules (backup HSM) 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.

The CA Private Key SHALL be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

6.2.5 Private Key Archival

CA Private Key archival is described on chapter 6.2.4.

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. This is only applicable for Encryption Certificates.

Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All CA private keys must be generated exclusively on a secured cryptographic hardware module (HSM) which can be online for Subordinate- or Issuing CA's. In case of Root CA's the needed equipment including HSM for key generation is offline without any network connection. A transfer of CA private keys is just performed in case of key backup or key restore operation if necessary. CA private key backups will be performed and stored by a so called "cloning process" on special designed and secured backup HSM's. The Backup HSMs are also role based protected with PED keys and PIN's.

6.2.7 Storage of Private Keys on the Cryptographic Module

All CA Private Keys are stored on hardware cryptographic modules (HSM) certified to FIPS 140-2 level 3 and Common Criteria (CC) Evaluation Assurance Level (EAL) 4+ and, which is generally equivalent to Information Technology Security Evaluation Criteria (ITSEC) assurance level E3. Where CA Key Pairs are backed up to an equivalent hardware cryptographic module (Backup HSM), such Key Pairs are transported between modules in encrypted form inside the high security cell of the secure facility.

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

All 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

All 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

The HSMS are operated with firmware levels compliant to at least FIPS 140-2 Level 3 certification standards.

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 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.

1:“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 ”

2:“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. The following validity periods are

Type of Certificate	Period of validity
Siemens Root CA	12 years
Siemens Intermediate CA	up to 10 years
Siemens Issuing CA	up to 6 years
EE Certificates for Siemens Employee	825 days
EE Certificates for Business Partners	365 days
EE Certificates for Functions (Siemens Employee only)	365 days
Siemens internal Code Signing (Siemens Employee only)	up to 3 years
Siemens internal Adobe Short lived Certificates	60 minutes

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

Procedures and regulations are documented in inter CA and HSM management manual [InterCaMan].

6.4.2 Activation Data Protection

As above.

6.4.3 Other Aspects of Activation Data

As above.

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 by operators who have identified with two-factor-authentication.

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.

6.5.1 Specific computer security technical requirements

See chapter 6.5 above.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Security Controls

Life Cycle Security Controls for the CA key pairs are maintained from the keys pair's generation until its destruction and are not limited to the expiry dates of the corresponding certificates.

6.6.1 System Development Controls

System development controls are provided in accordance with systems development and change management standards of Siemens 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

Siemens is certified based on the requirements version ETSI EN 319 411-1 V2.2.1, ETSI EN 319 401 V.2.2.2 as well as on Network and Certificate System Security Requirements [NSSSR].

The CA/Browser Forum's *Network and Certificate System Security Requirements* [NSSSR] are incorporated by reference as if fully set forth herein.

6.8 Time Stamp Process

Logfiles contain an embedded time stamp. CA event protocols are being signed and time stamped.

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

Certificate profiles for Root CA Certificate, Subordinate CA Certificates and Subscriber Certificates are described in 'Siemens Trust Center PKI- CA Hierarchy Policy 2023' and the sections below.

The CA SHALL meet the technical requirements set forth in Section 2.2, Section 6.1.5, and Section 6.1.6.

CAs SHALL generate non-sequential Certificate serial numbers greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.

7.1.1 Version Number

All Certificates issued by the CAs are [X.509 version 3] certificates.

7.1.2 Certificate Extensions

This section specifies the additional requirements for Certificate content and extensions for Certificates.

7.1.2.1 Root CA Certificates

Defined inside Siemens CPS RootCA.

7.1.2.2 Subordinate CA Certificate

Certificate extensions are as set as stipulated in IETF RFC 5280 and in accordance with 'Siemens Trust Center PKI- CA Hierarchy Policy 2023' [CertProfile].

Effective January 1, 2019, the extension requirements for extended key usage are:

- (i) Must contain an EKU extension,
- (ii) Must not include the anyExtendedKeyUsage EKU, and
- (iii) Must not include either id-kp-serverAuth, id-kp-emailProtection, id-kp-codeSigning or id-kp-timeStamping EKUs in the same certificate.

Additional requirements for Certificate content and extensions for Subordinate- and Issuing-CA-Certificates.

- a. certificatePolicies (SHALL be present) This extension SHOULD NOT be marked critical.

All policyIdentifiers included in this extension SHALL be included in accordance with 7.1.6.3.

If the value of this extension includes a PolicyInformation which contains a qualifier of type id-qt-cps (OID: 1.3.6.1.5.5.7.2.1), then the value of the qualifier SHALL be a HTTP or HTTPS URL for the Issuing CA's CP and/or CPS, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA. If a qualifier of type id-qt-notice (OID: 1.3.6.1.5.5.7.2.2) is included, then it SHALL contain explicitText and SHALL NOT contain noticeRef.

- b. cRLDistributionPoints (SHALL be present)

This extension SHALL NOT be marked critical. It SHALL contain the HTTP URL of the CA's CRL service.

- c. authorityInformationAccess (SHOULD be present)

This extension SHALL NOT be marked critical.

It SHOULD contain the HTTP URL of the Issuing CA Certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

It MAY contain the HTTP URL of the Issuing CA OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

d. d. basicConstraints (SHALL be present)

This extension SHALL be marked critical. The cA field SHALL be set true. The pathLenConstraint field MAY be present.

e. e. keyUsage (SHALL be present)

This extension SHALL be marked critical. Bit positions for keyCertSign and cRLSign SHALL be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit SHALL be set.

f. f. nameConstraints (MAY be present)

This extension SHOULD be marked critical².

g. g. extKeyUsage (MAY be present for Cross Certificates; SHALL be present otherwise)

For Cross Certificates that share a Subject Distinguished Name and Subject Public Key with a Root CA Certificate operated in accordance with these Requirements, this extension MAY be present. If present, this extension SHOULD NOT be marked critical. This extension SHALL only contain usages for which the Issuing CA has verified the Cross Certificate is authorized to assert. This extension SHALL NOT contain the anyExtendedKeyUsage usage. For all other Subordinate CA Certificates, including Technically Constrained Subordinate CA Certificates, this extension SHALL be present and SHOULD NOT be marked critical³

For Subordinate CA Certificates that will be used to issue S/MIME Certificates, the value id-kp-emailProtection SHALL be present. The values id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage SHALL NOT be present. Other values MAY be present.

The issuance of end entity S/MIME Certificates by Extant S/MIME CAs and transition:

Following the Effective Date for v 1.0.0 of these Requirements (September 1, 2023) an Extant S/MIME CA MAY continue to issue end entity S/MIME Certificates that are compliant with these Requirements.

On or after September 15, 2024, all newly-issued Publicly-Trusted end entity S/MIME Certificates SHALL be issued from S/MIME Subordinate CAs that are compliant with these Requirements.

For backwards compatibility, Extant S/MIME CA Certificates that share the same Public Keys with S/MIME Subordinate CAs that are compliant with these Requirements, or are no longer used for signing end entity S/MIME Certificates, are not required to be revoked.

7.1.2.3 Subscriber Certificate

All certificate fields and extensions follow RFC5280, ETSI, S/MIME BR and comply with the Applicable Requirements and documented within:

- Siemens CA Hierarchy Policy 2023.pdf
- Siemens EE Policy 2023.pdf

Published under www.siemens.com/pki

² Non-critical Name Constraints are an exception to RFC 5280 (4.2.1.10), however, they MAY be used until the name-Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

³ While RFC 5280, Section 4.2.1.12, notes that this extension will generally only appear within end-entity Certificates, these Requirements make use of this extension to further protect relying parties by limiting the scope of Subordinate Certificates, as implemented by a number of Application Software Suppliers.

7.1.2.4 All Certificates

All certificate fields and extensions follow RFC5280, ETSI, S/MIME BR and comply with the Applicable Requirements and documented within:

- Siemens CA Hierarchy Policy 2023.pdf
- Siemens EE Policy 2023.pdf

Published under www.siemens.com/pki

7.1.2.5 Application of RFC 5280

For purposes of clarification, a precertificate, as described in RFC 6962 (Certificate Transparency), shall not be considered to be a "certificate" subject to the requirements of RFC 5280.

7.1.3 Algorithm Object Identifiers

7.1.3.1 SubjectPublicKeyInfo

7.1.3.1.1 RSA

According to the Requirements, for RSA the CA will indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters must be present and must be explicit NULL.

The encoding of the `AlgorithmIdentifier` for RSA keys is byte-for-byte identical with the following hex-encoded bytes: `300d06092a864886f70d0101010500`

No other OID is used to indicate RSA Encryption as algorithm identifier.

7.1.3.1.2 ECDSA

Siemens CA does not issue certificates with ECDSA at the moment.

7.1.3.1.3 EdDSA

Siemens CA does not issue certificates with EdDSA at the moment.

7.1.3.1.4 ML-DSA

Siemens CA does not issue certificates with ML-DSA at the moment but according to S/MIME Requirements and for future use to be PQC ready the CA SHALL indicate an ML-DSA key using one of the following algorithm identifiers below:

- ML-DSA-44 (OID: 2.16.840.1.101.3.4.3.17), or
- ML-DSA-65 (OID: 2.16.840.1.101.3.4.3.18), or
- ML-DSA-87 (OID: 2.16.840.1.101.3.4.3.19)

The parameters for ML-DSA keys SHALL be absent. The CA MUST NOT use HashML-DSA; only "pure" ML-DSA is permitted.

When encoded, the AlgorithmIdentifier for ML-DSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For ML-DSA-44, 300b0609608648016503040311.
- For ML-DSA-65, 300b0609608648016503040312.
- For ML-DSA-87, 300b0609608648016503040313

7.1.3.1.5 ML-KEM

Siemens CA does not issue certificates with ML-KEM at the moment but according to S/MIME Requirements and for future use to be PQC ready the CA SHALL indicate an ML-KEM key using one of the following algorithm identifiers below:

- ML-KEM-512 (OID: 2.16.840.1.101.3.4.4.1), or

- ML-KEM-768 (OID: 2.16.840.1.101.3.4.4.2), or
- ML-KEM-1024 (OID: 2.16.840.1.101.3.4.4.3)

The parameters for ML-KEM keys SHALL be absent.

When encoded, the AlgorithmIdentifier for ML-KEM keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For ML-KEM-512, 300b0609608648016503040401
- For ML-KEM-768, 300b0609608648016503040402
- For ML-KEM-1024, 300b0609608648016503040403

7.1.3.2 SignatureAlgorithmIdentifier

All objects signed by a CA Private Key must conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate.
- The signature field of a TBSCertificate (for example, as used by a Certificate).
- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

The CA SHALL use one of the following signature algorithms and encodings. When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256: Encoding: 300d06092a864886f70d01010b0500
- RSASSA-PKCS1-v1_5 with SHA-384: Encoding: 300d06092a864886f70d01010c0500
- RSASSA-PKCS1-v1_5 with SHA-512: Encoding: 300d06092a864886f70d01010d0500
- No RSASSA-PSS signature algorithms are used by Siemens CA.

7.1.3.2.2 ECDSA

No ECDSA signature algorithms are used by Siemens CA.

7.1.3.2.3 EdDSA

No EdDSA signature algorithms are used by Siemens CA.

7.1.3.2.4 ML-DSA

No ML-DSA signature algorithms is used by Siemens CA at the moment but according to S/MIME Requirements and for future use to be PQC ready the CA SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is ML-DSA-44, the signature algorithm SHALL be id-ml-dsa-44 (OID: 2.16.840.1.101.3.4.3.17). When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300b0609608648016503040311.

If the signing key is ML-DSA-65, the signature algorithm SHALL be id-ml-dsa-65 (OID: 2.16.840.1.101.3.4.3.18). When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300b0609608648016503040312.

If the signing key is ML-DSA-87, the signature algorithm SHALL be id-ml-dsa-87 (OID: 2.16.840.1.101.3.4.3.19). When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300b0609608648016503040313.

7.1.4 Name Forms

Attribute values SHALL be encoded according to RFC 5280.

7.1.4.1 Name Encoding

For every valid Certification Path (as defined by RFC 5280, Section 6) for all Certificate and Subordinate CA Certificate, the following must be met:

- (i) For each Certificate in the Certification Path, the encoded content of the issuer distinguished name field of a Certificate shall be byte-for-byte identical with the encoded form of the Subject distinguished name field of the issuing CA certificate.
- (ii) For each CA Certificate in the Certification Path, the encoded content of the Subject distinguished name field of a Certificate shall be byte-for-byte identical among all Certificates whose Subject distinguished names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates

Siemens Issuing CAs use the following encoding:

Country - C	Organization Name - O	Common Name - CN	SerialNumber
PRINTABLESTRING	UTF8STRING	UTF8STRING	PRINTABLESTRING

Table 9: Issuing CA Name Encoding

7.1.4.2 Subject Information – Subscriber Certificates

All subscriber certificates (End-Entity) contain a unique issuer name (Issuer-DN) of the respective certification authority according to ‘Siemens CA Hierarchy Policy 2023’ which is published under www.siemens.com/pki

All attributes and it’s values of the subjectDN depends on the certificate type. Siemens CA issues following types of certificate profiles:

- Organization validated Multipurpose Profile according to S/MIME BR Group, robot or function accounts and function mailboxes
- Sponsor validated Multipurpose Profile according to S/MIME BR Natural persons which are internal and external employees of Siemens AG and its subsidiaries and affiliates – named as “Known Business Partner”
- Internal Certificate Profiles issued by internal CA’s For internal Code Signing, impersonalized entities for internal mobile APPs, internal Server TLS, Adobe Cloud Signature for internal employees

Name forms for Subscriber Certificates and contents are defined inside Siemens EE Policy 2023’ under www.siemens.com/pki. All other optional attributes must contain information that has been verified by the CA or RA. Optional attributes will not contain only metadata such as ‘,’ and ‘ ’ (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.1 Subject alternative name extension

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
subjectAltName	SHALL	SHALL	MAY

All issued certificates from Siemens CA have always Rfc822Name encoded at least. Additionally, if the certificate is used for Authentication according to its purpose this extension will also contain otherName of type id-on-SmtpUTF8Mailbox.

All Mailbox Addresses in the subject field or entries of type dirName of this extension SHALL be repeated as rfc822Name or otherName values of type id-on-SmtpUTF8Mailbox in this extension.

7.1.4.2.2 Subject distinguished name fields

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
commonName OID 2.5.4.3	MAY	MAY	MAY
	organizationName	Personal Name	Personal Name / organizationName

The Personal Name SHALL contain a name of the Subject and consists of subject:surname and subject:givenName. The Personal Name MAY be in the Subject's preferred presentation format or a format preferred by the CA or Enterprise RA, but SHALL be a meaningful representation of the Subject's name as verified under Section 3.2.4.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
organizationName OID 2.5.4.10	SHALL	SHALL	MAY
	Siemens	Siemens	Siemens

If present, the content of subject:organizationName is always "Siemens".

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
organizationalUnitName OID 2.5.4.11	MAY	MAY	MAY
	--	--	--

Certificate field subject:organizationalUnitName is not used.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
organizationIdentifier OID 2.5.4.97	SHALL	SHALL	MAY
	NTRDE-HRB 6684	NTRDE-HRB 6684	--

The Certificate field organisationIdentifier is a mandatory field for organisation-validated and sponsor-validated multipurpose profiles and contain a registration reference for a legal entity assigned according to the identified registration scheme. Siemens CA is using NTR (National Trade Register) as registration scheme according to S/MIME BR.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
givenName OID 2.5.4.42	SHALL NOT	MAY	MAY
	--	givenName	--
surname OID 2.5.4.4	SHALL NOT	MAY	MAY
	--	surname	--

If present, the subject:givenName field and subject:surname field SHALL contain a Natural Person Subject's name as verified under Section 3.2.4.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
Pseudonym OID 2.5.4.65	SHALL NOT	MAY	MAY
	--	--	--

Certificate field subject:pseudonym is not used.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
serialNumber OID 2.5.4.5	MAY	MAY	MAY
	Internal Identifier	Internal Identifier	Internal Identifier

Certificate field subject:serialNumber is used and content an internal Siemens Global Identifier which is unique and bind to a natural person or functional identity.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
emailAddress 1.2.840.113549.1.9.1	MAY	MAY	MAY
	Mailbox address	Mailbox address	Mailbox address

If present, certificate field subject:emailAddress contents a single mailbox address as verified under chapter 3.2.2.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
title OID 2.5.4.12	SHALL NOT	MAY	MAY
	--	--	--

Certificate field subject:title is not used.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
streetAddress OID 2.5.4.9	SHALL NOT	SHALL NOT	MAY
	--	--	--

Certificate field subject:streetAddress is not used.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
localityName OID 2.5.4.7	MAY	MAY	MAY
	--	--	--

Certificate field subject:localityName is not used anymore in subscriber certificates.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
stateOrProvinceName OID 2.5.4.8	MAY	MAY	MAY
	Bayern	Bayern	Bayern

Certificate field subject:stateOrProvinceName is used and content is always "Bayern".

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
postalCode OID 2.5.4.17	MAY	MAY	MAY
	--	--	--

Certificate field subject:postalCode is not used.

Certificate field	Organization validated profile	Sponsor validated profile	Internal profile
countryName OID 2.5.4.6	MAY	MAY	MAY
	DE	DE	DE

Certificate field subject:countryName is used and content is always "DE" for Germany.

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

Certificate field	Root-CA	Subordinate-CA
commonName OID 2.5.4.3	SHALL	SHALL
	Unique name	Unique name

This field contain a uniquely assigned name for the Certificate that reflects the technical purpose together with affiliation to Siemens CA.

Certificate field	Root-CA	Subordinate-CA
organizationName	SHALL	SHALL

OID 2.5.4.10	--	--
--------------	----	----

This field contain always the organization name "Siemens".

Certificate field	Root-CA	Subordinate-CA
countryName	SHALL	SHALL
OID 2.5.4.6	DE	DE

This field contain always the country code "DE" for Germany.

Other attributes MAY be present within the subject field. If present, other attributes SHALL contain information that has been verified by the CA.

Certificate Profile definitions for CA Certificates are documented in 'Siemens PKI CA Hierarchy Policy 2023' under www.siemens.com/pki.

7.1.5 Name Constraints

Siemens CA does not issue technically constrained Subordinate CA Certificates but Certificate issuance is restricted to Siemens domains. For this purpose, a restriction to approved mail domains is implemented in the certificate management system.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers for S/MIME Baseline Requirements

The following CA/Browser Forum Certificate Policy identifiers are reserved for use by CAs to assert that a Certificate complies with S/MIME BR Requirements:

CertificateType	Version/Level	Policy Identifier
S/MIME certificate Mailbox-validated	Legacy	2.23.140.1.5.1.1
S/MIME certificate Mailbox-validated	Multipurpose	2.23.140.1.5.1.2
S/MIME certificate Mailbox-validated	Strict	2.23.140.1.5.1.3
S/MIME certificate Organization-validated	Legacy	2.23.140.1.5.2.1
S/MIME certificate Organization-validated	Multipurpose	2.23.140.1.5.2.2
S/MIME certificate Organization-validated	Strict	2.23.140.1.5.2.3
S/MIME certificate Sponsor-validated	Legacy	2.23.140.1.5.3.1
S/MIME certificate Sponsor-validated	Multipurpose	2.23.140.1.5.3.2
S/MIME certificate Sponsor-validated	Strict	2.23.140.1.5.3.3
S/MIME certificate Individual-validated	Legacy	2.23.140.1.5.4.1
S/MIME certificate Individual-validated	Multipurpose	2.23.140.1.5.4.2
S/MIME certificate Individual validated	Strict	2.23.140.1.5.4.3

Effective July 15, 2025 S/MIME Subscriber Certificates SHALL NOT be issued using the Legacy Generation profiles.

7.1.6.2 Reserved Certificate Policy Identifiers for Siemens CA

CertificateType	Policy Identifier
Siemens Public Key Infrastructure	1.3.6.1.4.1.4329.7
Siemens PKI CP/CPS Document Identifier	1.3.6.1.4.1.4329.99
Siemens OCSP Signer Hardware Token (HSM)	1.3.6.1.4.1.4329.7.2.5
Siemens Employee Authentication to Corporate ID card or VSC/NSC	1.3.6.1.4.1.4329.7.2.2.3.1.1
Function Authentication to corporate ID card	1.3.6.1.4.1.4329.7.2.2.3.2.1
Known Business Partner Authentication to corporate ID card or VSC/NSC	1.3.6.1.4.1.4329.7.2.2.4.1.1
Function Soft PSE	1.3.6.1.4.1.4329.7.2.2.3.2.3
Siemens Employee Soft PSE	1.3.6.1.4.1.4329.7.2.2.3.1.3
Known Business Partner Soft PSE	1.3.6.1.4.1.4329.7.2.2.4.1.3

Siemens Employee Adobe Cloud Signature	1.3.6.1.4.1.4329.7.2.2.3.1.4
--	------------------------------

7.1.6.3

7.1.6.3 Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension. If present, the extension SHALL conform to the requirements set forth for Certificates issued to Subordinate CAs in Section 7.1.6.4.

7.1.6.4 Subordinate CA Certificates

Siemens CA does not issue Subordinate CA Certificates that is not an Affiliate of the Issuing CA.

A Certificate issued to a Subordinate CA that is an Affiliate of the Issuing CA SHALL include either the “any policy” identifier (2.5.29.32.0) or one or more explicit certificate policy object identifiers that indicates compliance with a specific certificate policy. Certificate policy object identifiers are listed in chapter 7.1.6.1 and 7.1.6.2.

7.1.6.5 Subscriber Certificates

A Certificate issued to a Subscriber SHALL contain, within the Certificate’s certificatePolicies extension, a policy identifier that is specified in Section 7.1.6.1 and 7.1.6.2.

The Certificate MAY also contain additional policy identifier(s) documented by the Siemens CA in its CP and/or CPS.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

CAs include policy qualifiers in all Subscriber Certificates as stipulated in chapter 7.1.6.1 and 7.1.6.2.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificate policies extension is marked Not Critical.

7.2 CRL Profile

The following fields of the X.509 version 2 CRL format are used by the CAs:

- version: set to v2
- signature: identifier of the algorithm used to sign the CRL
- issuer: the full Distinguished Name of the CA issuing the CRL
- this update: time of CRL issuance
- next update: time of next expected CRL update
- revoked Certificates: list of revoked Certificate information

7.2.1 Version Number

No stipulation.

7.2.2 CRL and CRL Entry Extensions

Issued CRLs contain the following "extension" entries:

CRL Field	Value
Authority Key Identifier OID 2.5.29.35	Contains the key hash value from related CA
CRL Number OID 2.5.29.20	Unique, ascending number of the revocation list
Reason Code OID 2.5.29.21	Coding of the revocation reason in accordance with RFC 5280

If present, the reasonCode (OID 2.5.29.21) is not marked critical.

The CRLReason code extension is used for all revoked Certificates. The CRLReason indicated must not be unspecified (0) or certificateHold (6). This extension must not be marked critical. The most appropriate reason must be selected by the Subscriber or the CA from one the following:

- keyCompromise (1), if the key to the certificate has been or is suspected to be compromised
- cACompromise (2), if the CA has been or is suspected to be compromised
- affiliationChanged (3), if verified information in the Certificate has changed and as such the Relying Parties should no longer trust the Certificate
- superseded (4), if the Certificate has been reissued, rekeys or renewed by another Certificate
- cessationOfOperation (5), if the application or device is no longer in service

7.3 OCSP Profile

The profile for the Online Certificate Status Protocol (OCSP) messages issued by a CA conform to the specifications contained in the IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP) Profile [RFC 6960].

7.3.1 Version Number

No stipulation.

7.3.2 OCSP Extensions

The singleExtensions of an OCSP response shall not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

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.