Siemens Corporate PKI

Certification Practice Statement for Siemens Root CAs

Version:	1.14
Date:	28.01.2025
Classification:	Public / Unrestricted

Document History

Version	Date	Author	Change Comment
1.0	June 10, 2016	Alexander Winnen, Michael Munzert	First final version
1.1	December 1, 2016	Rufus Buschart	Minor updated version
1.2	May 29, 2017	Rufus Buschart	Update new CA hierarchy
1.3	January 12, 2018	Rufus Buschart	Chapter „Document History“ Added changed after ballots Chapter 4.9.1 Revocation reasons added Chapter 4.9.2 Who can request a revocation added Chapter 5 Moved to CP
1.4	February 7, 2018	Rufus Buschart	Chapter 4.9.7 Issuing of CARL added Chapter 6.1.5 Reference to ETSI TS 119 312 added Chapter 6.2.7 Details about backup devices Chapter 7.2 / 7.3 Technical specification added
1.5	February 23, 2018	Rufus Buschart	Licensing changed to CC-BY SA 4.0 as required by Mozilla
1.6	March 5, 2018	Rufus Buschart	Chapter 6.6 difference between lifecycle of certificate and key pair clarified
1.7	February 18, 2019	Rufus Buschart	All chapters: No stipulations removed
1.8	January 31, 2020	Rufus Buschart	Minor typographic changes
1.9	February 18, 2021	Rufus Buschart	Chapter 1.1 Added 2020 hierarchy
1.10	July 25, 2021	Mauricio Fernandez	Chapter 1.1 Added 2021 hierarchy minor changes in Chapter 7
1.11	February 17, 2022	Rufus Buschart	Minor changes
1.12	February 21, 2022	Rufus Buschart	Minor adaption
1.13	January 24, 2024	Ilias Cotoulas Marco Fechter	Changes on chapter 1.1: update list of active RootCA’s Changes on chapter 7: update and reformat according to S/MIME Baseline Requirements Minor format changes
1.14	January 24, 2025	Khaled Taleb Fabian Meister Marco Fechter	Review and minor updates

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

Document Status

This document with version 1.14 and status Released has been classified as “Unrestricted“ and is licensed as CC BY-SA 4.0.

	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 28, 2025

Table of Content

1 Introduction

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

1.1 Overview

This Certification Practice Statement (CPS) defines

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

The CPS details the procedures and controls in place to meet the CP requirements. For identical topics the respective chapter in the CP is referenced. The Siemens Root CAs together with the respective Issuing CAsare shown in the CP.

The following table lists the currently operated Root CAs as well as their implemented requirements according to [ETSI EN 319 411-1]:

CA	Secure Device
ZZZZZZA1 Siemens Trust Center Root-CA V3.0	HSM FIPS 140 Level 3

Table 1: Root CA Implementation of ETSI requirements

1.2 Document Name and Identification

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

Title: Certification Practice Statement of Siemens Root CAs

OID: 1.3.6.1.4.1.4329.99.2.1.1.14

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

1.3 PKI Participants

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

1.3.1 Certification Authorities

Refer to Annex B B_1_RootCA

1.3.2 Registration Authorities

Specified in the Certificate Policy.

1.3.3 Subscribers

Specified in the Certificate Policy.

1.3.4 Relying Parties

Specified in the Certificate Policy.

1.3.5 Other participants

Specified in the Certificate Policy.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

Specified in the Certificate Policy.

1.4.2 Prohibited Certificate Usage

Specified in the Certificate Policy.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Specified in the Certificate Policy.

1.5.2 Contact Person

Specified in the Certificate Policy.

2 Publication and Repository Responsibilities

2.1 Repositories

Specified in the Certificate Policy.

2.2 Publication of Certification Information

Specified in the Certificate Policy.

2.3 Time or Frequency of Publication

Specified in the Certificate Policy.

2.4 Access Controls on Repositories

Specified in the Certificate Policy.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Specified in the Certificate Policy.

3.1.2 Need of Names to be Meaningful

Specified in the Certificate Policy.

3.1.3 Anonymity or Pseudonymity of Subscribers

Specified in the Certificate Policy.

3.1.4 Rules for Interpreting Various Name Forms

Specified in the Certificate Policy.

3.1.5 Uniqueness of Names

Specified in the Certificate Policy.

3.1.6 Recognition, Authentication, and Roles of Trademarks

Specified in the Certificate Policy.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Specified in the Certificate Policy.

3.2.2 Identification and Authentication of Organization Identity

Specified in the Certificate Policy.

3.2.3 Identification and Authentication of Individual Identity

Specified in the Certificate Policy.

3.2.4 Non-verified Subscriber Information

Specified in the Certificate Policy.

3.2.5 Validation of Authority

Specified in the Certificate Policy.

3.2.6 Criteria for Interoperation between Communities of Trusts

Specified in the Certificate Policy.

3.3 Identification and Authentication for Re-key Requests

Specified in the Certificate Policy.

3.4 Identification and Authentication for Revocation Requests

Specified in the Certificate Policy.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Specified in the Certificate Policy.

4.1.2 Enrollment Process and Responsibilities

Specified in the Certificate Policy.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

Specified in the Certificate Policy.

4.2.2 Approval or Rejection of Certificate Applications

Specified in the Certificate Policy.

4.2.3 Time to Process Certificate Applications

Specified in the Certificate Policy.

4.3 Certificate Issuance

4.3.1 Root CA actions during Certificate issuance

Specified in the Certificate Policy.

4.3.2 Notification to Subscriber by the CA of Certificate issuance

Specified in the Certificate Policy.

4.4 Certificate Acceptance

4.4.1 Conduct constituting Certificate acceptance

Specified in the Certificate Policy.

4.4.2 Publication of the Certificate by the CA

Specified in the Certificate Policy.

4.4.3 Notification of Certificate issuance by the CA to other entities

Specified in the Certificate Policy.

4.5 Key Pair and Certificate Usage

4.5.1 Subject Private Key and Certificate Usage

Specified in the Certificate Policy.

4.5.2 Relying Party Public Key and Certificate Usage

Specified in the Certificate Policy.

4.6 Certificate Renewal

Specified in the Certificate Policy.

4.6.1 Circumstance for Certificate Renewal

Specified in the Certificate Policy.

4.6.2 Who may request renewal?

Specified in the Certificate Policy.

4.6.3 Processing Certificate Renewal Request

Specified in the Certificate Policy.

4.6.4 Notification of new Certificate Issuance to Subject

Specified in the Certificate Policy.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Specified in the Certificate Policy.

4.6.6 Publication of the Renewal Certificate by the CA

Specified in the Certificate Policy.

4.6.7 Notification of Certificate Issuance by the CA to the Entities

Specified in the Certificate Policy.

4.7 Certificate Re-key

Specified in the Certificate Policy.

4.7.1 Circumstances for Certificate Re-key

Specified in the Certificate Policy.

4.7.2 Who may request certification of a new Public Key?

Specified in the Certificate Policy.

4.7.3 Processing Certificate Re-keying Requests

Specified in the Certificate Policy.

4.7.4 Notification of new Certificate Issuance to Subscriber

Specified in the Certificate Policy.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Specified in the Certificate Policy.

4.7.6 Publication of the Re-keyed Certificate by the CA

Specified in the Certificate Policy.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

Specified in the Certificate Policy.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Specified in the Certificate Policy.

4.8.2 Who may request Certificate modification?

Specified in the Certificate Policy.

4.8.3 Processing Certificate Modification Requests

Specified in the Certificate Policy.

4.8.4 Notification of new Certificate Issuance to Subject

Specified in the Certificate Policy.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Specified in the Certificate Policy.

4.8.6 Publication of the Modified Certificate by the CA

Specified in the Certificate Policy.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Specified in the Certificate Policy.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

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

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

4.9.2 Who can request revocation?

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

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

After an issuing CA certificate has been revoked a new CARL shall be generated.

4.9.8 Maximum Latency for CRLs

Specified in the Certificate Policy.

4.9.9 On-line Revocation/Status Checking Availability

Specified in the Certificate Policy.

4.9.10 Other Forms of Revocation Advertisements Available

Specified in the Certificate Policy.

4.9.11 Special Requirements for Private Key Compromise

Specified in the Certificate Policy.

4.9.12 Circumstances for Suspension

Specified in the Certificate Policy.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Specified in the Certificate Policy.

4.10.2 Service Availability

Specified in the Certificate Policy.

4.10.3 Optional Features

Specified in the Certificate Policy.

4.11 End of Subscription

Specified in the Certificate Policy.

4.12 Key Escrow and Recovery

Specified in the Certificate Policy.

5 Management, Operational, and Physical Controls

Specified in the Root CA CPS.

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 Root CAs	12 years	6-7 years

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Specified in the 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

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

6.1.2 Private Key Delivery to Subject

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

Not applicable.

6.1.4 CA Public Key delivery Relying Parties

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

6.1.5 Key Sizes

The algorithms, 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.

6.1.6 Public Key Parameters Generation and Quality Checking

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

6.1.7 Key Usage Purposes

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

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

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

6.2.3 Private Key Escrow

Private Key Escrow is not being performed for Root and Issuing CAs.

6.2.4 Private Key Backup

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

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

6.2.5 Private Key Archival

No archival is performed exceeding chapter 6.2.5.

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

6.2.7 Storage of Private Keys on the Cryptographic Module

Siemens Root CA´s Private Key is held in HSM backup modules in encrypted form. Where Root CA Key Pairs are backed up to an equivalent hardware cryptographic module, such Key Pairs are transported between modules in encrypted form inside the high security cell of the secure facility.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

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

6.2.10 Method of Destroying Private Key

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

When performed, the destruction process is logged.

6.2.11 Cryptographic Module Rating

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

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

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

6.4 Activation Data

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

6.4.1 Activation Data Generation and Installation

Further information are documented in the inter CA and HSM management manual.

6.4.2 Activation Data Protection

Further information are documented in the inter CA and HSM management manual.

6.4.3 Other Aspects of Activation Data

Further information are documented in the inter CA and HSM management manual.

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.

6.6 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 ISMS. Systems development is performed by trusted software supplier(s) in accordance with specifications for secure programming.

6.6.2 Security Management Controls

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

6.6.3 Life Cycle of Security Controls

All Security Controls are audited annually by an external auditor.

6.7 Network Security Controls

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

6.8 Time Stamp Process

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 root CAs comply with digital Certificate and CRL profiles as described in [RFC 5280]. The profile for the Certificates and Certificate Revocation List (CRL) issued by a CA conform to the specifications contained in the IETF RFC 5280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.

7.1 Certificate Profile

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

The profile for the Certificates and Certificate Revocation List (CRL) issued by a CA conform to the specifications contained in the IETF RFC 5280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile

7.1.1 Version Number

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

Certificate serial numbers are not generated in sequence and length is 128 bit. Output is from a JAVA CSRNG. Certificates have a serial number greater than zero (0) that contains at least 64 unpredictable bits.

7.1.2 Certificate Extensions

7.1.2.1 Root CA Certificate

Certificate extensions are as set as stipulated in IETF RFC 5280.

a. basicConstraints (SHALL be present)
This extension SHALL be marked critical. The cA field SHALL be set true.
The pathLenConstraint field SHOULD NOT be present.

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

c. certificatePolicies (SHOULD NOT be present)
This extension SHOULD NOT be present.
Future revisions of the Siemens Root CA certificate will omit this extension.

d. extKeyUsage (SHALL NOT be present)
This extension SHALL NOT be present.

e. subjectKeyIdentifier (SHALL be present)
This extension SHALL NOT be marked critical. It SHALL contain a value that is included in the keyIdentifier field of the authorityKeyIdentifier extension in Certificates issued by the Root CA.

f. authorityKeyIdentifier (SHALL be present)
This extension SHALL NOT be marked critical.

7.1.2.2 Subordinate CA Certificate

Certificate extensions are as set as stipulated in IETF RFC 5280.

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.

The issuance of end entity S/MIME Certificates by Extant S/MIME CAs is described in SBR101 Appendix B.

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

All policyIdentifiers included in this extension SHALL be included in accordance with SBR101 Section 7.1.6.3. pg. 53

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-unotice (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. nameConstraints (MAY be present)

   This extension SHOULD be marked critical[1].

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 critical[2]

   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.

7.1.2.3 Subscriber Certificate

Certificate extensions are as set as stipulated in IETF RFC 5280, and defined in the Issuing CA CPS.

[1] 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.

[2] 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 fields and extensions SHALL be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a keyUsage flag, extKeyUsage value, Certificate extension, or other data not specified in Section 7.1.2.1, Section 7.1.2.2, or Section 7.1.2.3 unless the CA is aware of a reason for including the data in the Certificate. If the CA includes fields or extensions in a Certificate that are not specified but are otherwise permitted by these Requirements, then the CA SHALL document the processes and procedures that the CA employs for the validation of information contained in such fields and extensions in its CP and/or CPS.

CAs SHALL NOT issue a Certificate with:

1. Extensions that do not apply in the context of the public Internet (such as an extKeyUsage value for a service that is only valid in the context of a privately managed network), unless:

i. such value falls within an OID arc for which the Applicant demonstrates ownership, or

ii. the Applicant can otherwise demonstrate the right to assert the data in a public context;

or

2. Field or extension values which have not been validated according to the processes and procedures described in these Requirements or the CA's CP and/or CPS.

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

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.

For ECDSA, the CA must indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters must use the namedCurve encoding:

(i) For P-256 keys, the namedCurve must be secp256r1 (OID: 1.2.840.10045.3.1.7), or

(ii) For P-384 keys, the namedCurve must be secp384r1 (OID: 1.3.132.0.34).

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.

For RSA, the CA must use one of the following signature algorithms and encodings.

(i) RSASSA-PKCS1-v1_5 with SHA-256

(ii) RSASSA-PKCS1-v1_5 with SHA-384

(iii) RSASSA-PKCS1-v1_5 with SHA-512

For ECDSA, the CA must use the appropriate signature algorithm and encoding based upon the signing key used.

(iv) If the signing key is P-256, the signature MUST use ECDSA with SHA-256.

(v) If the signing key is P-384, the signature MUST use ECDSA with SHA-384.

(vi) If the signing key is P-521, the signature MUST use ECDSA with SHA-512.

7.1.4 Name Forms

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

7.1.4.2 Subject Information – Subscriber Certificates

Subject information for subscriber certificates are regulated in the respective CPS and must meet the requirements stated in 'Siemens Trust Center PKI- CA Hierarchy Policy 2023'.

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

Subject information must meet the requirements stated in 'Siemens Trust Center PKI- CA Hierarchy Policy 2023'.

7.1.4.3.1 Subject distinguished name fields

a. **Certificate Field:** subject:commonName (OID 2.5.4.3)
Required/Optional: SHALL be present
Contents: This field SHOULD contain an identifier for the Certificate such that the Certificate's Name is unique across all Certificates issued by the Issuing CA.

b. **Certificate Field:** subject:organizationName (OID 2.5.4.10)
Required/Optional: SHALL be present
Contents: This field SHALL contain either the Subject CA's name or DBA as verified under Section 3.2.3.2.2 The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name".

c. **Certificate Field:** subject:countryName (OID: 2.5.4.6)
Required/Optional: SHALL be present
Contents: This field SHALL contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.

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

7.1.5 Name Constraints

CAs do not support the issuance of technically constrained Subordinate CA Certificates.

7.1.6 Certificate Policy Object Identifier

This section describes the content requirements for the Root CA, Subordinate CA, and Subscriber Certificates as they relate to the identification of Certificate Policy.

7.1.6.1 Reserved Certificate Policy Identifiers

Subscriber Certificates must include one of the following reserved Certificate Policy Identifiers, if the CA is asserting the Certificate meets the associated certificate policy:

CertificateType	Generation	Policy Identifier
SSL Certificates		2.23.140.1.2.2
EV SSL Certificates		2.23.140.1.1
Code Signing Certificates		2.23.140.1.4.1
EV Code Signing Certificates		2.23.140.1.3
Verified Mark Certificates		1.3.6.1.4.1.53087.1.1
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
EE certificates Class 1		2.16.840.1.114028.10.1.4.1
EE certificates Class 2		2.16.840.1.114028.10.1.4.2
EE Document Signing Certificates		2.16.840.1.114028.10.1.6

7.1.6.2 Root CA Certificates

Root CA Certificates issued after August 1st 2021 do not contain the certificate policy object identifiers.

7.1.6.3 Subordinate CA Certificates

A Certificate issued to a Subordinate CA that is not an Affiliate of the Issuing CA:

1. SHALL include one or more explicit policy identifiers defined in Section 7.1.6.1 that indicate the Subordinate CA's adherence to and compliance with these Requirements and MAY contain one or more identifiers documented by the Subordinate CA in its CP and/or CPS; and
2. SHALL NOT contain the anyPolicy identifier (2.5.29.32.0).

A Certificate issued to a Subordinate CA that is an Affiliate of the Issuing CA SHALL include a set of policy identifiers from one of the two options below:

1. One or more explicit policy identifiers defined in Section 7.1.6.1 that indicate the Subordinate CA's adherence to and compliance with these Requirements and MAY contain one or more identifiers documented by the Subordinate CA in its CP and/or CPS; or
2. The anyPolicy identifier (2.5.29.32.0).

The Subordinate CA and the Issuing CA SHALL represent, in their CP and/or CPS, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with these Requirements.

7.1.6.4 Subscriber Certificates

See CPS issuing CA

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 'Siemens Trust Center PKI- CA Hierarchy Policy 2023'.

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

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:

(i) keyCompromise (1), if the key to the certificate has been or is suspected to be compromised

(ii) cACompromise (2), if the CA has been or is suspected to be compromised

(iii) affiliationChanged (3), if verified information in the Certificate has changed and as such the Relying Parties should no longer trust the Certificate

(iv) superseded (4), if the Certificate has been reissued, rekeys or renewed by another Certificate

(v) cessationOfOperation (5), if the application or device is no longer in service

7.3 OCSP Profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that Certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus SHALL be present.

The CRLReason indicated SHALL contain a value permitted for CRLs, as specified in Section 7.2.2.

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.

Annex B: Certificate profiles

B.1 Root CA V3.0 2016

Certificate Field	Content	Comment
Issuer Distinguished Name (DN)	CN=Siemens Root CA V3.0 2016 OU=Siemens Trust Center SERIALNUMBER =ZZZZZZA1 O=Siemens L=Muenchen SP=Bayern C=DE	Must match subject
Serial-Number	762907e3	
Key Length	4096	
Signature Algorithm	sha256withRSA	
Subject Distinguished Name (DN)	CN=Siemens Root CA V3.0 2016 OU=Siemens Trust Center SERIALNUMBER =ZZZZZZA1 O=Siemens L=Muenchen SP=Bayern C=DE	Must contain countryName, stateAndProvince, organizationName, Serialnumber and commonName
Authority Key Identifier	Include Authority Key Identifier	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Subject Key Identifier	Include Subject Key Identifier	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Key Usage **critical**	Key Cert Sign CRL Sign	keyCertsign and cRLSign bits are set; digitalSignature if Root signs OCSP responses
Basic Constraints **critical**	Type=CA	CA is TRUE; pathLenConstraint is not present
Certificate Policies	2.5.29.32.0 http://www.siemens.com/pki/	Should not be present for future and new RootCA's
Thumbprint (SHA-1)	a6ff9adaaa1925d18b1d4076c8d86b22d2557b19	
Subject Key Identifier	706da050eca9d02c679d1915fefd047335c3e2d4	