# Siemens Corporate PKI

## *Certification Practice Statement for Siemens Issuing CAs*

| | |
|---|---|
| Version: | 1.16 |
| Date: | 29.01.2024 |
| 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<br>Chapter 2.2 Link to https://catestsite.siemens.com/ added<br>Chapter 4.9.1 Revocation reasons added<br>Chapter 4.9.2 Who can request a revocation added<br>Chapter 5 Moved to CP |
| 1.6 | January 31, 2018 | Rufus Buschart | Chapter 3.2.2 Restructured<br>Chapter 6.3.2 Server certificates clarified<br>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<br>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<br>Chapter 3.2.2.3 Stop Issuance of TLS documented<br>Minor changes |
| 1.12 | February 17, 2020 | Rufus Buschart | Chapter 1.1 Added 2020 hierarchy<br>Chapter 3.2.2.1 Removal of TLS domain validation<br>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 adaptions |
| 1.16 | January 24, 2024 | Ilias Cotoulas<br>Marco Fechter | Adaptions over all chapters for SBR101<br>Minor format changes |

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 1.16 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<br>Florian Grotz | Siemens LS<br>Siemens GS IT HR 7 4 | June 10, 2016<br>February 20, 2019 |
| **Authorization** | Mauricio Fernandez | Siemens CYS INF NG | January 29, 2024 |

# 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 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 | | Requirements for issued certificates | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ETSI quality level | | | Secure device | | | |
| | Expiry date | NCP+ | OVCP | DVCP | Smart Card | Smart-Phone | HSM | NSC/ VSC |
| ZZZZZZB2 Siemens Issuing CA EE Auth 2020 | 29/6/2026 | X | | | X | | | |
| ZZZZZZB3 Siemens Issuing CA EE Enc 2020 | 29/6/2026 | X | | | X | X | | X |
| ZZZZZZBD Siemens Issuing CA EE Network Smartcard Auth 2020 | 29/6/2026 | X | | | | | | X |
| ZZZZZZB6 Siemens Issuing CA Medium Strength Authentication 2020 | 29/6/2026 | | | | | | | |
| ZZZZZZD3_Siemens_Issuing_CA_EE_Enc_2021 | 28/7/2025 | X | | | X | X | | X |
| ZZZZZZD2_Siemens_Issuing_CA_EE_Auth_2021 | 28/7/2025 | X | | | X | | | |
| ZZZZZZDD_Siemens_Issuing_CA_EE_Network_Smartcard_Auth_2021 | 28/7/2025 | X | | | | | | X |
| ZZZZZZD6_Siemens_Issuing_CA_Medium_Strength_Authentication_2021 | 28/7/2025 | | | | | | | |
| ZZZZZZE3_Siemens_Issuing_CA_EE_Enc_2023 | 04/06/2028 | X | | | X | X | | X |
| ZZZZZZE2_Siemens_Issuing_CA_EE_Auth_2023 | 04/06/2028 | X | | | X | | | |
| ZZZZZZED_Siemens_Issuing_CA_EE_Network_Smartcard_Auth_2023 | 04/06/2028 | X | | | | | | X |
| ZZZZZZE6_Siemens_Issuing_CA_Medium_Strength_Authentication_2023 | 04/06/2028 | | | | | | | |

**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
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 subjet:organizationName (an associated Legal Entity) attribute.<br>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 | 244817A9C7D60184651D8041D8F34F9C6D26926689DA33233892FE915E40D065 |
| Siemens Issuing CA EE Enc 2020 | 4724CFB9 | 167407C794A5BF5D3A4CE6B56FE81228300006A5FE55F01C07E8AA791762FA46 |
| Siemens Issuing CA EE Network Smartcard Auth 2020 | 19393306 | 68C752B1981F111510A8E678775406597696B6B752B89BE04C6BEDDFEF294419 |
| Siemens Issuing CA Medium Strength Authentication 2020 | 7C682BB5 | 8905AD1617C55305648EAB9533886155F8D4CE5B456F1783FB47887BF928821A |
| Siemens Issuing CA EE Enc 2021 | 50094F56B2286DAACE7C6AED623F9968 | A1C5D7B6D0DA22115F3A3841DA90528C9635903423EAFFD4416C2712476A040F |
| Siemens Issuing CA EE Auth 2021 | 435B94F668F3112B56B1F226882FFD29 | 477868C56C81FCC0ECE3B8AFFBB54B1C3DF69E5D7AA54B4A2C65EA67BE83AD3A |
| Siemens Issuing CA EE Network Smartcard Auth 2021 | 5503DF4A70A19BFAC6FFA305FF79AB97 | A72298F93C48EF59E4328B7AE7B50F8CD48EC180BBD83D3B5D4DD734D87464C0 |
| Siemens Issuing CA Medium Strength Authentication 2021 | 474B9852D859806390A3006DC7B57E17 | 5AE5409197A3E77D37695D4BA795845C7A04F7BD7769E9608044CAB9F74733C6 |
| Siemens Issuing CA EE Enc 2023 | 71e6323fb63184f49715d2330d086aa8 | 05E7AB4F1795F4E76E9EF5D49B5AE1E46CB22DA833B1758D031B8AAA7E2FDF84 |
| Siemens Issuing CA EE Auth 2023 | 7468ba9573e8c5f00ff3b79cbd624764 | CEC450B3354FCAC90219D71FAC4DC1CFF4A67B6102F87B00A0301207FC2A4EFA |
| Siemens Issuing CA EE Network Smartcard Auth 2023 | 48017cf4b6848d1723c3ee6faf9d1bc3 | 1D4E9F45681E59D88853B38CA704F3738EE6E2B0BA2DFADEB3ACACF4A0555739 |
| Siemens Issuing CA Medium Strength Authentication 2023 | 7c052b64498efa09670951654986e099 | 6DC59E8EF20AE4304A53A0BDC15E0244897BEB6C75DEF5F6999AD5BB882EC3F6 |

**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 2020 Hierarchy and before:

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

For the Siemens 2021 Hierarchy

- 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”.

For Siemens 2020 and 2016 Hierarchy the Locality attribute is permitted “L”=”Muenchen”.

#### 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

#### 3.2.3.1 End Entity Names

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 between Communities of Trusts

Specified in the Certificate Policy.

### 3.2.7 Criteria for interoperation

The CA SHALL disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e., the Cross Certificate at issue).

### 3.2.8 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<br>• *A/D Certificate*<br>• E Certificate<br>• 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<br>• *A/D Certificate*<br>• *E Certificate*<br>• *Code Signing* | AP via RA | Not performed | AP or SS via RA | Not performed | AP or SS via RA |
| Business Partner Community | Business Partner<br>• *A/D Certificate*<br>• *E Certificate*<br>• *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

Siemens CA shall revoke a Certificate within 24 hours if one or more of the following occurs:

I. The Subscriber requests in writing that Siemens CA revokes 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.

### 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

Specified in the Certificate Policy.

### 4.9.8 Maximum Latency for CRLs

Specified in the Certificate Policy.

### 4.9.9 On-line Revocation Checking Requirements

Specified in the Certificate Policy.

### 4.9.10 Other Forms of Revocation Advertisements Available

Specified in the Certificate Policy.

### 4.9.11 Special Requirements for Private Key Compromise

Specified in the Certificate Policy.

### 4.9.12 Circumstances for Suspension

Specified in the Certificate Policy.

## 4.10 Certificate Status Services

### 4.10.1 Operational Characteristics

Specified in the Certificate Policy.

### 4.10.2 Service Availability

Specified in the Certificate Policy.

### 4.10.3 Optional Features

Specified in the Certificate Policy.

## 4.11 End of Subscription

Specified in the Certificate Policy.

## 4.12 Key Escrow and Recovery

Specified in the Certificate Policy.

# 5 Management, Operational, and Physical Controls

Specified in the 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

For CA Key Pairs that are either

1. used as a CA Key Pair for a Root CA Certificate; or

2. used as a CA Key Pair for a Subordinate CA Certificate, where the Subordinate CA is not the operator of the Root CA or an Affiliate of the Root CA,

the CA SHALL:

1. prepare and follow a Key Generation Script;

2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the

entire CA Key Pair generation process; and

3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during

its Key and Certificate generation process and the controls used to ensure the integrity and

confidentiality of the Key Pair.

For other CA Key Pairs that are for the operator of the Root CA or an Affiliate of the Root CA, the CA SHOULD:

1. prepare and follow a Key Generation Script; and

2. either (i) have a Qualified Auditor witness the CA Key Pair generation process, or (ii)

video-record the entire CA Key Pair generation process for review by its Qualified Auditor.

In all cases, the CA SHALL:

1. generate the CA Key Pair in a physically secured environment as described in the CA's CP and/or CPS;

2. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;

3. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CP and/or CPS;

4. log its CA Key Pair generation activities; and

5. maintain effective controls to provide reasonable assurance that the Private Key was

generated and protected in conformance with the procedures described in its CP and/or CPS

and (if applicable) its Key Generation Script.

#### 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, complying to the minimum requirements as documented here and in 'PKI3_EE_Policies'.

The CA will reject a Certificate request if one or more of the following conditions are met:

(i) The Key Pair does not meet the requirements set forth in §6.1.5 and/or §6.1.6;

(ii) There is clear evidence that the specific method used to have generate the Private Key was flawed;

(iii) The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;

(iv) The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;

(v) The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

Client Certificates:

I. In order to support key backup, the CA may optionally provide a service to generate the Key Pair on behalf of the Applicant or Subscriber, in this case the related certificate signing request MUST NOT request the attribute extended key-usage set to 'non-repudiation'.

### 6.1.2 Private Key Delivery to Subject

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

For an Authentication/Digital Signatures Certificate, there is no delivery of Private Key to Subscribers because each Subscriber will generate his own Private Key with the Secure Signature Creation Device ("SSCD").

For 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 Subject in person after Validation of Subject's identity or by securely mailing or delivering via courier the Private Key with procedure for Validation of Subject's identity or through PKISS/MyPKI.

**For S/MIME certificates the following stipulations apply:** Parties other than the Subscriber SHALL NOT archive the EE-Subscriber Private Key without authorization by the EE-Subscriber.

If the CA or any of its designated RAs become aware that a EE Subscriber's Private Key has been communicated to a person or organization not authorized by the EE-Subscriber, then the CA SHALL revoke all Certificates that include the Public Key corresponding to the communicated Private Key.

If the CA or a Delegated Third Party generates the Private Key on behalf of the EE-Subscriber where the Private Keys will be transported to the EE-Subscriber, then the entity generating the Private Key SHALL either transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption or encrypt the Private Key with at least 128 bits of encryption strength.

Example methods include using a 128-bit AES key to wrap the Private Key or storing the key in a PKCS 12 file encrypted with a randomly generated password of more than 16 characters containing uppercase letters, lowercase letters, numbers, and symbols for transport. The CA or Delegated Third Party SHALL NOT store EE-Subscriber Private Keys in clear text.

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.

For Server Certificates the Certificate Applicant is responsible for the security of the private key. The Siemens Issuing CA does not store or generate this key. No private keys for SSL/TLS certificate are delivered to the subscriber.

### 6.1.3 Public Key Delivery to Certificate Issuer

Public Key is sent encrypted by standard protocols.

### 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.

For S/MIME certificates the following stipulations apply:

For RSA key pairs the CA SHALL:

- Ensure that the modulus size, when encoded, is at least 2048 bits; and
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, the CA SHALL:

- Ensure that the key represents a valid point on the NIST P-256, NIST P-384, or NIST P-521 elliptic curve.

For EdDSA key pairs, the CA SHALL:

- Ensure that the key represents a valid point on the curve25519 or curve 448 elliptic curve.

No other algorithms or key sizes are permitted.

### 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.

**For S/MIME certificates the following stipulations apply:**

For RSA key pairs: the CA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16 + 1 and 2^256 - 1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. (See NIST SP 800-89, Section 5.3.3.)

For ECDSA key pairs: the CA SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. (See NIST SP 800-56A: Revision 2, Sections 5.6.2.3.2 and 5.6.2.3.3.)

### 6.1.7 Key Usage Purposes

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

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA SHALL implement physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system or device specified above SHALL consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

### 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.

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

### 6.2.4 Private Key Backup

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

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

§6.2.3 addresses the backup of Subscriber Private Keys.

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

Issuing CA Private Key archival: Compare 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

Private Keys of the Issuing CAs are securely stored exclusively on hardware cryptographic modules.

If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA. If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

### 6.2.7 Storage of Private Keys on the Cryptographic Module

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

### 6.2.8 Method of Activating Private Key

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

  

employees and is documented for audit logging purposes.

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

### 6.2.9 Method of Deactivating Private Key

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

### 6.2.10 Method of Destroying Private Key

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

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

### 6.2.11 Cryptographic Module Rating

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. This Validity Period is based on the Validity Period of the Root CA Certificate set forth in the table below."

See table 4 below.

| | CA Certificate | Authentication/ Digital Signature Certificate | Encryption Certificate | EFS Certificate | Server Certificate | Multi-purpose Certificate | Code Signing Certificate |
|---|---|---|---|---|---|---|---|
| Siemens Issuing CAs | 2190 (6 years) | N/A | N/A | N/A | N/A | N/A | N/A |
| Siemens employee | N/A | 825 | 825 | 825 | N/A | N/A | N/A |
| Functional Group | N/A | 365 | 365 | N/A | N/A | N/A | 1095 |
| Business Partner | N/A | 365 | 365 | N/A | N/A | 365 | N/A |
| Servers | N/A | N/A | N/A | N/A | 457 | N/A | N/A |

**Table 9 Validity Period of Certificates (in days from date of issuance)**

Summarizing:

- Special purpose certificates like Code signing certificates may be valid up to 3 years
- Server certificates are valid up to 1year plus 92 days.
- Siemens employee certificates may be valid up to 825 days, S/MIME Certificates up to 825 days or 1185 days for Legacy S/MIME certificates.
- Business partner certificates may be valid up to 1 year

## 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

The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

### 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

No stipulation.

#### 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-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[2].

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[3]

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

Certificate extensions are as set as stipulated in IETF RFC 5280 and in accordance with “Siemens-PKI_EE_Policy_2023.pdf” which is published under www.siemens.com/pki

All fields and extensions are documented in Siemens-PKI_EE_Policy_2023.pdf

[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 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).

The following requirements apply to the subjectPublicKeyInfo field within a Certificate. No other encodings are permitted.

##### 7.1.3.1.1 RSA

The CA SHALL indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters SHALL be present, and SHALL be an explicit NULL.

The CA SHALL NOT use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key.

When encoded, the AlgorithmIdentifier for RSA keys SHALL be byte-for-byte identical with

the following hex-encoded bytes: 300d06092a864886f70d0101010500

##### 7.1.3.1.2 ECDSA

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

• For P-256 keys, the namedCurve SHALL be secp256r1 (OID: 1.2.840.10045.3.1.7).

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

• For P-521 keys, the namedCurve SHALL be secp521r1 (OID: 1.3.132.0.35).

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

• For P-256 keys, 301306072a8648ce3d020106082a8648ce3d030107.

• For P-384 keys, 301006072a8648ce3d020106052b81040022.

• For P-521 keys, 301006072a8648ce3d020106052b81040023.

#### 7.1.3.1.3 EdDSA

The CA SHALL indicate an EdDSA key using one of the following algorithm identifiers below:

• For curve25519 keys, the algorithm SHALL be id-Ed25519 (OID: 1.3.101.112).

• For curve448 keys, the algorithm SHALL be id-Ed448 (OID: 1.3.101.113).

The parameters for EdDSA keys SHALL be absent. When encoded, the AlgorithmIdentifier for EdDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

• For Curve25519 keys, 300506032b6570.

• For Curve448 keys, 300506032b6571.

### 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.

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

• RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes:
Encoding:

304106092a864886f70d01010a3034a00f300d06096086480165030402010500a11c301a06092a864886f70d010108300d06096086480165030402010500a203020120

• RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:
Encoding:
304106092a864886f70d01010a3034a00f300d06096086480165030402020500a11c301a06092a864886f70d010108300d06096086480165030402020500a203020130

• RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:
Encoding:
304106092a864886f70d01010a3034a00f300d06096086480165030402030500a11c301a06092a864886f70d010108300d06096086480165030402030The CA SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

• If the signing key is P-256, the signature SHALL use ECDSA with SHA-256. When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040302.

• If the signing key is P-384, the signature SHALL use ECDSA with SHA-384. When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040303.

• If the signing key is P-521, the signature SHALL use ECDSA with SHA-512. When encoded, the AlgorithmIdentifier SHALL be byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040304.

### 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 10: Issuing CA Name Encoding**

#### 7.1.4.2 Subject Information – Subscriber Certificates

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

Name forms for Subscriber Certificates are as stipulated in §3.1.1. 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.

Entries in the dNSName are in the "preferred name syntax" as specified in IETF RFC 5280 and thus do not contain underscore characters.

##### 7.1.4.2.1 Subject alternative name extension

**Certificate Field:** extensions:subjectAltName

**Required/Optional:** SHALL be present

**Contents:** This extension SHALL contain at least one GeneralName entry of the following types:

- Rfc822Name and/or
- otherName of type id-on-SmtpUTF8Mailbox, encoded in accordance with RFC 8398

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.

The CA MAY include GeneralName entries of type dirName provided that the information contained in the Name complies with the requirements set forth in the appropriate subsection of Section 7.1.4.2.2 according to the Certificate Type. Additionally, information contained in the Name SHALL be validated according to Section 3.1, Section 3.2.3, and/or Section 3.2.4, as appropriate for the Certificate Type.

For Legacy and Multipurpose Generation profiles, then the CA MAY include otherName entries of any type, provided that the CA has validated the field value according to its CP and/or CPS.

The CA SHALL NOT include GeneralName entries that do not conform to the requirements of this section.

#### 7.1.4.2.2 Subject distinguished name fields

a.) **Certificate Field:** subject:commonName (OID 2.5.4.3)

**Contents:** If present, this attribute SHALL contain one of the following values verified in accordance with Section 3.2.

| Certificate | Type Contents |
|---|---|
| **Mailbox-validated** | Mailbox Address |
| **Organization-validated** | subject:organizationName or Mailbox Address |
| **Sponsor-validated** | Personal Name, Pseudonym, or Mailbox Address |
| **Individual-validated** | Personal Name, Pseudonym, or Mailbox Address |

**Table 11: Issuing CA EE Attribute Requirements**

If present, the Personal Name SHALL contain a name of the Subject. The Personal Name SHOULD be presented as subject:givenName and/or subject:surname. 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.

If present, the Mailbox Address SHALL contain a rfc822Name or otherName value of type id-on-SmtpUTF8Mailbox from extensions:subjectAltName.

If present, the Pseudonym SHALL contain the subject:pseudonym if that Subject attribute is also present.

**Note:** Like all other Certificate attributes, subject:commonName and subject:emailAddress SHALL comply with the attribute upper bounds defined in RFC 5280.

Additional specifications for naming are provided in Section 3.1.

b.) **Certificate Field:** subject:organizationName (OID 2.5.4.10)

**Contents:** If present, the subject:organizationName field SHALL contain the Subject's full legal organization name and/or an Assumed Name as verified under Section 3.2.3. If both are included, the Assumed Name SHALL appear first, followed by the full legal organization name in parentheses. 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:organizationalUnitName (OID: 2.5.4.11)

**Contents:** If present, the CA SHALL confirm that the subject:organizationalUnitName is the full legal organization name of an Affiliate of the subject:organizationName in the Certificate and has been verified in accordance with the requirements of Section 3.2.3. 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.

d. **Certificate Field:** subject:organizationIdentifier (2.5.4.97)

**Contents:** If present, the subject:organizationIdentifier field SHALL contain a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme.
The subject:organizationIdentifier SHALL be encoded as a PrintableString or UTF8String.

The Registration Scheme identified in the Certificate SHALL be the result of the verification performed in accordance with Section 3.2.3. The Registration Scheme SHALL be identified using the following structure in the presented order:

- 3 character Registration Scheme identifier;
- 2 character ISO 3166 country code for the nation in which the Registration Scheme is operated, or if the scheme is operated globally ISO 3166 code "XG" SHALL be used;
- For the NTR Registration Scheme identifier, where registrations are administrated at the subdivision (state or province) level, a plus "+" (0x2B (ASCII), U+002B (UTF-8)) followed by an up-to-three alphanumeric character ISO 3166-2 identifier for the subdivision of the nation in which the Registration Scheme is operated;
- a hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));
- Registration Reference allocated in accordance with the identified Registration Scheme.

**Note 1:** Registration References MAY contain hyphens but Registration Schemes, ISO 3166 country codes, and ISO 3166-2 identifiers do not. Therefore if more than one hyphen appears in the structure, the leftmost hyphen is a separator, and the remaining hyphens are part of the Registration Reference. For example:

- NTRGB-12345678 (NTR scheme, Great Britain, Unique Identifier at Country level is 12345678).
- NTRUS+CA-12345678 (NTR Scheme, United States - California, Unique identifier at State level is 12345678).
- VATDE-123456789 (VAT Scheme, Germany, Unique Identifier at Country Level is 12345678).
- PSDBE-NBB-1234.567.890 (PSD Scheme, Belgium, NCA's identifier is NBB, Unique Identifier assigned by the NCA is 1234.567.890).

Registration Schemes listed in Appendix A are recognized as valid under these Requirements. The CA SHALL:

1. Confirm that the organization represented by the Registration Reference is the same as the organization named in the organizationName field as specified in Section 7.1.4.2.2; and

2. Further verify the Registration Reference matches other information verified in accordance with Section 3.2.3.

**Note 2:** For the following types of entities that do not have an identifier from the Registration Schemes listed in Appendix A:

- For Government Entities, the CA SHALL enter the Registration Scheme identifier 'GOV' followed by the 2 character ISO 3166 country code for the nation in which the Government Entity is located. If the Government Entity is verified at a subdivision (state or province) level, then a plus "+" (0x2B (ASCII), U+002B (UTF-8)) followed by an ISO 3166-2 identifier for the subdivision (up to three alphanumeric characters) is added.
- For International Organization Entities, the CA SHALL enter the Registration Scheme identifier 'INT' followed by the ISO 3166 code "XG". An International Organization Entity is founded by a

constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.

For example:

- GOVUS (Government Entity, United States)
- GOVUS+CA (Government Entity, United States - California)
- INTXG (International Organization)

e. **Certificate Field:** subject:givenName (2.5.4.42) and/or subject:surname (2.5.4.4)

**Contents:** 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. Subjects with a single legal name SHALL provide the name in the subject:surname attribute. The subject:givenName and/or subject:surname SHALL NOT be present if the subject:pseudonym is present.

f. **Certificate Field:** subject:pseudonym (2.5.4.65)

**Contents:** The subject:pseudonym SHALL NOT be present if the subject:givenName and/or subject:surname are present. If present, the subject:pseudonym field SHALL be verified according to Section 3.1.3.

g. **Certificate Field:** subject:serialNumber (2.5.4.5)

**Contents:** If present, the subject:serialNumber MAY be used to contain an identifier assigned by the CA or RA to identify and/or to disambiguate the Subscriber.

In addition, the subject:serialNumber MAY be used in the Sponsor-validated and Individual-validated profiles to contain a Natural Person Identifier as described in ETSI EN 319 412-1 Section 5.1.3. Registration Schemes listed in Appendix A are recognized as valid under these Requirements. The CA SHALL confirm that the Individual represented by the Natural Person Identifier is the same as the Certificate Subject in accordance with Section 3.2.4.

h. **Certificate Field:** subject:emailAddress (1.2.840.113549.1.9.1)

**Contents:** If present, the subject:emailAddress SHALL contain a single Mailbox Address as verified under Section 3.2.2.

i. **Certificate Field:** subject:title (2.5.4.12)

**Contents:** If present, the subject:title field SHALL contain only a organizational role/title or a regulated professional designation verified according to Section 3.2.4.

j. **Certificate Field:** Number and street: subject:streetAddress (OID: 2.5.4.9)

**Contents:** If present, the subject:streetAddress field SHALL contain the Subject's street address information as verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types.

k. **Certificate Field:** subject:localityName (OID: 2.5.4.7)

**Contents:** If present, the subject:localityName field SHALL contain the Subject's locality information as verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types.
If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2 (n), the localityName field MAY contain the Subject's locality and/or state or province information.

l. **Certificate Field:** subject:stateOrProvinceName (OID: 2.5.4.8)

**Contents:** If present, the subject:stateOrProvinceName field SHALL contain the Subject's state or province information as verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX

in accordance with Section 7.1.4.2.2 (n), the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information.

m. **Certificate Field:** subject:postalCode (OID: 2.5.4.17)

**Contents:** If present, the subject:postalCode field SHALL contain the Subject's zip or postal information as verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types.

n. **Certificate Field:** subject:countryName (OID: 2.5.4.6)

**Contents:** If present, the subject:countryName SHALL contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.3 for Organization-validated and Sponsor-validated Certificate Types or Section 3.2.4 for Individual-validated Certificate Types. If a Country is not represented by an official ISO 3166-1 country code, the CA MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

#### 7.1.4.2.3 Subject DN attributes for mailbox-validated profile

| Attribute | Legacy | Multipurpose | Strict |
|---|---|---|---|
| **commonName** | MAY | MAY | MAY |
| **organizationName** | SHALL NOT | SHALL NOT | SHALL NOT |
| **organizationalUnitName** | SHALL NOT | SHALL NOT | SHALL NOT |
| **organizationIdentifier** | SHALL NOT | SHALL NOT | SHALL NOT |
| **givenName** | SHALL NOT | SHALL NOT | SHALL NOT |
| **surname** | SHALL NOT | SHALL NOT | SHALL NOT |
| **pseudonym** | SHALL NOT | SHALL NOT | SHALL NOT |
| **serialNumber** | MAY | MAY | MAY |
| **emailAddress** | MAY | MAY | MAY |
| **title** | SHALL NOT | SHALL NOT | SHALL NOT |
| **streetAddress** | SHALL NOT | SHALL NOT | SHALL NOT |
| **localityName** | SHALL NOT | SHALL NOT | SHALL NOT |
| **stateOrProvinceName** | SHALL NOT | SHALL NOT | SHALL NOT |
| **postalCode** | SHALL NOT | SHALL NOT | SHALL NOT |
| **countryName** | SHALL NOT | SHALL NOT | SHALL NOT |
| **Other** | SHALL NOT | SHALL NOT | SHALL NOT |

**Table 12: Issuing CA DN requirements mailbox validated**

#### 7.1.4.2.4 Subject DN attributes for organization-validated profile

| Attribute | Legacy | Multipurpose | Strict |
|---|---|---|---|
| commonName | MAY | MAY | MAY |
| organizationName | SHALL | SHALL | SHALL |
| organizationalUnitName | MAY | MAY | MAY |
| organizationIdentifier | SHALL | SHALL | SHALL |
| givenName | SHALL NOT | SHALL NOT | SHALL NOT |
| surname | SHALL NOT | SHALL NOT | SHALL NOT |
| pseudonym | SHALL NOT | SHALL NOT | SHALL NOT |
| serialNumber | MAY | MAY | MAY |
| emailAddress | MAY | MAY | MAY |
| title | SHALL NOT | SHALL NOT | SHALL NOT |
| streetAddress | MAY | MAY | SHALL NOT |
| localityName | MAY | MAY | MAY |
| stateOrProvinceName | MAY | MAY | MAY |
| postalCode | MAY | MAY | SHALL NOT |
| countryName | MAY | MAY | MAY |
| Other | MAY | SHALL NOT | SHALL NOT |

Table 13: Issuing CA DN requirements organization validated

#### 7.1.4.2.5 Subject DN attributes for sponsor-validated profile

| Attribute | Legacy (See Note 1) | Multipurpose (See Note 2) | Strict (See Note 2) |
|---|---|---|---|
| commonName | MAY | MAY | MAY |
| organizationName | SHALL | SHALL | SHALL |
| organizationalUnitName | MAY | MAY | MAY |
| organizationIdentifier | SHALL | SHALL | SHALL |
| givenName | MAY | MAY | MAY |
| surname | MAY | MAY | MAY |
| pseudonym | MAY | MAY | MAY |
| serialNumber | MAY | MAY | MAY |

| | | | |
|---|---|---|---|
| **emailAddress** | MAY | MAY | MAY |
| **title** | MAY | MAY | MAY |
| **streetAddress** | MAY | MAY | SHALL NOT |
| **localityName** | MAY | MAY | MAY |
| **stateOrProvinceName** | MAY | MAY | MAY |
| **postalCode** | MAY | MAY | SHALL NOT |
| **countryName** | MAY | MAY | MAY |
| **Other** | MAY | SHALL NOT | SHALL NOT |

**Table 14: Issuing CA DN requirements sponsor validated**

Note:

1. Legacy Generation profiles MAY omit the subject:givenName, subject:surname, and subject:pseudonym attributes and include only the subject:commonName as described in Section 7.1.4.2.2(a).

2. Multipurpose and Strict Generation profiles SHALL include either subject:givenName and/or subject:surname, or the subject:pseudonym.

#### 7.1.4.2.6 Subject DN attributes for individual-validated profile

| Attribute | Legacy (See Note 1) | Multipurpose (See Note 2) | Strict (See Note 2) |
|---|---|---|---|
| **commonName** | MAY | MAY | MAY |
| **organizationName** | SHALL NOT | SHALL NOT | SHALL NOT |
| **organizationalUnitName** | SHALL NOT | SHALL NOT | SHALL NOT |
| **organizationIdentifier** | SHALL NOT | SHALL NOT | SHALL NOT |
| **givenName** | MAY | MAY | MAY |
| **surname** | MAY | MAY | MAY |
| **pseudonym** | MAY | MAY | MAY |
| **serialNumber** | MAY | MAY | MAY |
| **emailAddress** | MAY | MAY | MAY |
| **title** | MAY | MAY | MAY |
| **streetAddress** | MAY | MAY | SHALL NOT |
| **localityName** | MAY | MAY | MAY |
| **stateOrProvinceName** | MAY | MAY | MAY |
| **postalCode** | MAY | MAY | SHALL NOT |
| **countryName** | MAY | MAY | MAY |

| | | | |
|---|---|---|---|
| **Other** | MAY | SHALL NOT | SHALL NOT |

**Table 15: Issuing CA DN requirements sponsor validated**

Note:

1. Legacy Generation profiles MAY omit the subject:givenName, subject:surname, and subject:pseudonym attributes and include only the subject:commonName as described in Section 7.1.4.2.2(a).

2. Strict and Multipurpose Generation profiles SHALL include either subject:givenName and/or subject:surname, or the subject:pseudonym.

#### 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'.

### 7.1.5 Name Constraints

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

### 7.1.6 Certificate Policy Object Identifier

#### 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 |
| **NCP: Normalized Certificate Policy** | | 0.4.0.2042.1.1 |
| **NCP+: Normalized Certificate Policy requiring a secure cryptographic device** | | 0.4.0.2042.1.2 |
| **Siemens Public Key Infrastructure** | | 1.3.6.1.4.1.4329.7 |
| **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 |

**Table 16: Issuing CA reserved certificate policy OIDs**

#### 7.1.6.2 Root CA Certificates

No stipulation.

#### 7.1.6.3 Subordinate CA Certificates

Subordinate CA Certificates must include either the “any policy” certificate policy object identifier or one or more explicit certificate policy object identifiers that indicates compliance with a specific certificate policy.

Certificate policy object identifiers are listed in §7.1.6.1 and §7.1.6.4.

#### 7.1.6.4 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.

The Certificate MAY also contain additional policy identifier(s) defined by the Issuing CA. The Issuing CA SHALL document in its CP and/or CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

Related policy identifiers are documented in ‘Siemens Trust Center PKI- CA Hierarchy Policy 2023’.

### 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

No stipulation.

## 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.