



Siemens Trust Center PKI

CA Hierarchy 2023 - EE Policies

Document History

Version	Date	Author	Change Comment
1.0	September 13, 2023	M. Fechter / IT IPS SIP ET	First initial version
1.1	June 02, 2025	F. Meister / IT IPS SIP CT	Switch from Legacy to Multipurpose policy OID

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

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

Scope and Applicability

This document constitutes the Certificate Authority Hierarchy (CA Hierarchy) for the Siemens CA Certificates (Issuing & Root). The purpose of this document is to publicly disclose to subscribers and relying parties the business policies and practices under which Root- and Issuing CA are operated.

Document Status

This document with version 1.1 and status Released has been classified as "Unrestricted".

	Name	Department	Date
Author	Various authors, detailed information in document history		
Checked by	Thorsten Bergmann	IT IPS SIP ET	02.06.2025
Authorization	Vinay Tiwari	CYS INF SH	02.06.2025

This document has been approved by the responsible service owner at Siemens CYS INF NG on June 2, 2025.

Table of Content

SCOPE AND APPLICABILITY2

DOCUMENT STATUS2

1 INTRODUCTION.....4

1.1 OVERVIEW4

1.2 LIST OF ABBREVIATIONS4

2 SIEMENS ISSUING CA EE AUTH 2023 - POLICIES.....5

3 SIEMENS ISSUING CA EE ENC 2023 – POLICIES.....6

4 SIEMENS ISSUING CA INTRANET CODE SIGNING 2023 – POLICIES7

5 SIEMENS ISSUING CA MEDIUM STRENGTH AUTHENTICATION 2023 – POLICIES8

6 SIEMENS ISSUING CA MSA IMPERSONALIZED ENTITIES 2023 – POLICIES.....9

7 SIEMENS ISSUING CA EE NETWORK SMARTCARD AUTH 2023 – POLICIES.....10

1 Introduction

This document explains the Siemens EE Certificate Policies.

1.1 Overview

The following picture shows the architecture of Siemens Root CA together with the respective Issuing CA's:

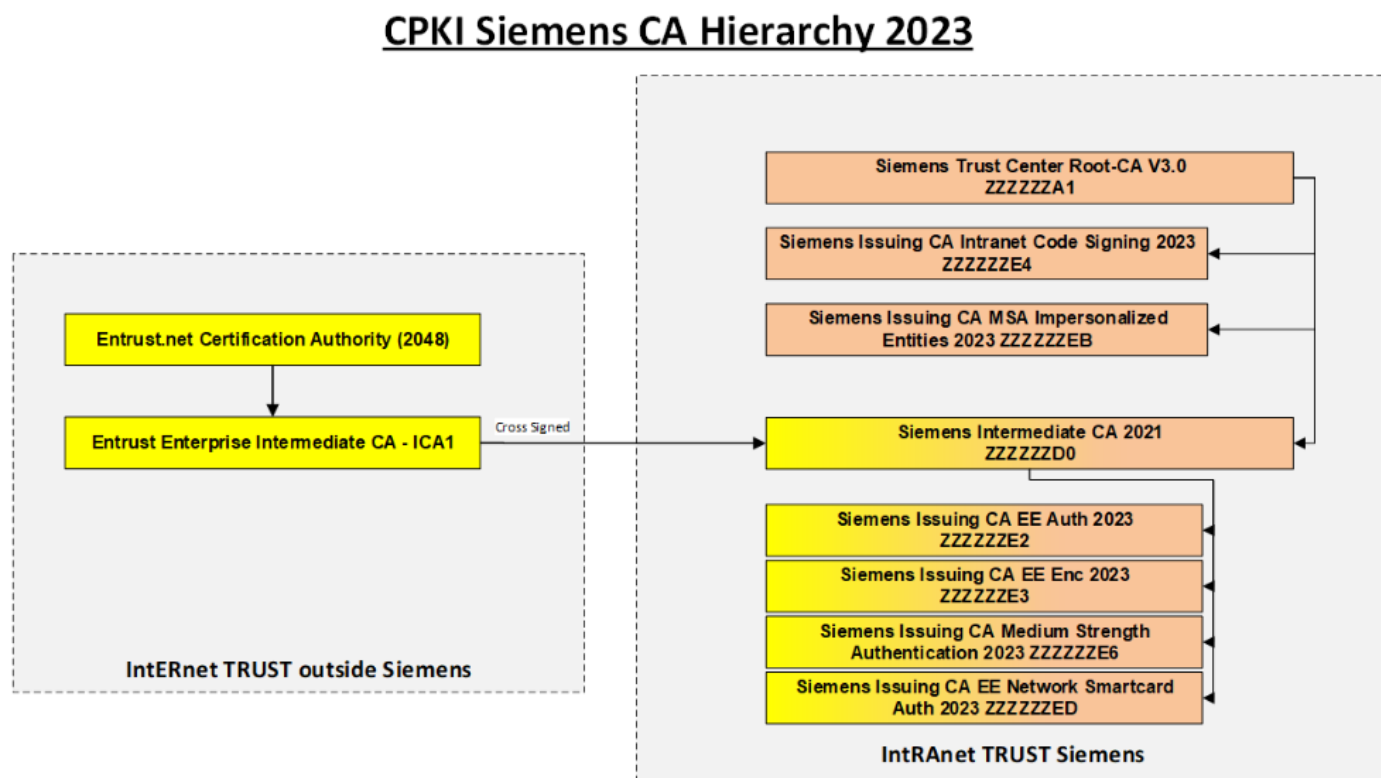


Figure 1: Siemens PKI Hierarchy 2023

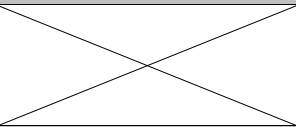
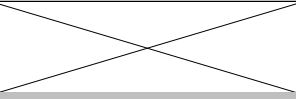
1.2 List of Abbreviations

Abbreviation	Meaning
AIA	Authority Information Access
AKI	Authority Key Identifier
B-Constr.	Basic Constraints
C	Country
CA	Certificate Authority
CDP	CRL Distribution Point
CN	Common Name
CP	Certificate Policies
DN	Distinguished Name
EKU	Extended Key Usage
KU	Key Usage
O	Organisation
OU	Organisation Unit
SAN	Subject Alternative Name
SKI	Subject Key Identifier
SN	Serial Number
SP	State of Province

2 Siemens Issuing CA EE Auth 2023 - Policies

	Name	ZZZZZZE2_AUTH_FCT_SC	ZZZZZZE2_AUTH_SMA_SC	ZZZZZZE2_AUTH_KBP_SC	ZZZZZZE2_OCSP_SIGNER_P10
General	Description	Strong Authentication for Functional Identity on SmartCard	Strong Authentication for Siemens Employee on SmartCard	Strong Authentication for Known Business Partner on SmartCard	Policy (P10) Class OCSP Signer Certificate on HSM
	Certificate Type	Authentication	Authentication	Authentication	OCSP Signing
	Version	V3	V3	V3	V3
	Algorithm	sha256RSA	sha256RSA	sha256RSA	sha256RSA
	Public Key	RSA 2048 bits generated on SmartCard	RSA 2048 bits generated on SmartCard	RSA 2048 bits generated on SmartCard	RSA 2048 bits generated on HSM
	Validity Period	12 months	825 days	12 months	12 months
Issuer DN		CN=Siemens Issuing CA EE Auth 2023 SN=ZZZZZZE2 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Auth 2023 SN=ZZZZZZE2 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Auth 2023 SN=ZZZZZZE2 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Auth 2023 SN=ZZZZZZE2 O=Siemens SP=Bayern C=DE
Subject DN		Common Name (CN)	Common Name (CN)	Common Name (CN)	CN
		Serial Number (SN)	Surname (SURNAME)	Surname (SURNAME)	Organization Name (O)
		Email (E)	Given Name (GN)	Given Name (GN)	State Name (ST)
		organizationIdentifier (ORG_ID)	Serial Number (SN)	Serial Number (SN)	Country (C)
		Organization Name (O)	Email (E)	Email (E)	
		State Name (ST)	organizationIdentifier (ORG_ID)	organizationIdentifier (ORG_ID)	
		Country (C)	Organization Name (O)	Organization Name (O)	
			State Name (ST)	State Name (ST)	
			Country (C)	Country (C)	
AIA	[1]	http://ah.siemens.com/pki?ZZZZZZE2.crt	http://ah.siemens.com/pki?ZZZZZZE2.crt	http://ah.siemens.com/pki?ZZZZZZE2.crt	
	[2]	ldap://al.siemens.net/CN=ZZZZZZE2,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZE2,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZE2,L=PKI?cACertificate	
	[3]	ldap://al.siemens.com/CN=ZZZZZZE2,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZE2,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZE2,o=Trustcenter?cACertificate	
	[4]	http://ocsp.siemens.com	http://ocsp.siemens.com	http://ocsp.siemens.com	
AKI		Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier
SKI		Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier
SAN	Other Name	User Principal Name	User Principal Name	User Principal Name	
	RFC822-Name	User Mail Address	User Mail Address	User Mail Address	
Key Usage Critical		Digital Signature	Digital Signature	Digital Signature	Digital Signature
EKU Non-Critical		kp-ClientAuth	kp-ClientAuth	kp-ClientAuth	OCSPSigning
		kp-emailProtection	kp-emailProtection	kp-emailProtection	
		SmartCard Logon	SmartCard Logon	SmartCard Logon	
CDP	[1]	http://ch.siemens.com/pki?ZZZZZZE2.crl	http://ch.siemens.com/pki?ZZZZZZE2.crl	http://ch.siemens.com/pki?ZZZZZZE2.crl	
	[2]	ldap://cl.siemens.net/CN=ZZZZZZE2,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZE2,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZE2,L=PKI?certificateRevocationList	
	[3]	ldap://cl.siemens.com/CN=ZZZZZZE2,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZE2,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZE2,o=Trustcenter?certificateRevocationList	
Basic Constr Critical	Type	End Entity	End Entity	End Entity	End Entity
	Path length	Nothing	Nothing	Nothing	Nothing
Certificate Policies	Siemens OID	1.3.6.1.4.1.4329.7.2.2.3.2.1	1.3.6.1.4.1.4329.7.2.2.3.1.1	1.3.6.1.4.1.4329.7.2.2.4.1.1	1.3.6.1.4.1.4329.7.2.5
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/
	SMIME BR OID	2.23.140.1.5.2.2	2.23.140.1.5.3.2	2.23.140.1.5.3.2	
OCSP NoCheck					YES

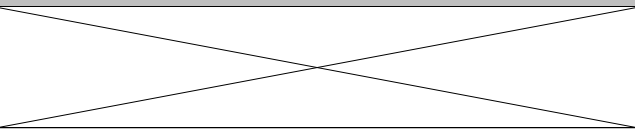
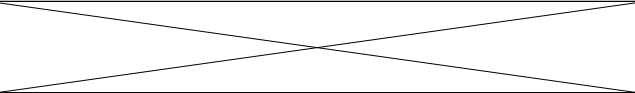
3 Siemens Issuing CA EE Enc 2023 – Policies

	Name	ZZZZZE3_ENC_FCT_SC	ZZZZZE3_ENC_FCT_P12	ZZZZZE3_ENC_SMA_SC	ZZZZZE3_ENC_KBP_SC	ZZZZZE3_OCSP_SIGNER_P10
General	Description	Encryption for Functional Identity on SmartCard	Encryption for Functional Identity on soft token p12	Encryption for Siemens Employee on SmartCard	Encryption for Known Business Partner on SmartCard	Policy (P10) Class OCSP Signer
	Certificate Type	Encryption	Encryption	Encryption	Encryption	OCSP Signing
	Version	V3	V3	V3	V3	V3
	Algorithm	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA
	Public Key	RSA 2048 bits generated and archived centrally	RSA 2048 bits generated and archived centrally	RSA 2048 bits generated and archived centrally	RSA 2048 bits generated and archived centrally	RSA 2048 bits generated on HSM
	Validity Period	12 months	12 months	825 days	12 months	12 months
Issuer DN		CN=Siemens Issuing CA EE Enc 2023 SN=ZZZZZE3 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Enc 2023 SN=ZZZZZE3 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Enc 2023 SN=ZZZZZE3 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Enc 2023 SN=ZZZZZE3 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Enc 2023 SN=ZZZZZE3 O=Siemens SP=Bayern C=DE
Subject DN		Common Name (CN)	Common Name (CN)	Common Name (CN)	Common Name (CN)	CN
		Serial Number (SN)	Serial Number (SN)	Surname (SURNAME)	Surname (SURNAME)	Organization Name (O)
		Email (E)	Email (E)	Given Name (GN)	Given Name (GN)	State Name (ST)
		organizationIdentifier (ORG_ID)	organizationIdentifier (ORG_ID)	Serial Number (SN)	Serial Number (SN)	Country (C)
		Organization Name (O)	Organization Name (O)	Email (E)	Email (E)	
		State Name (ST)	State Name (ST)	organizationIdentifier (ORG_ID)	organizationIdentifier (ORG_ID)	
		Country (C)	Country (C)	Organization Name (O)	Organization Name (O)	
				State Name (ST)	State Name (ST)	
AIA	[1]	http://ah.siemens.com/pki?ZZZZZE3.crt	http://ah.siemens.com/pki?ZZZZZE3.crt	http://ah.siemens.com/pki?ZZZZZE3.crt	http://ah.siemens.com/pki?ZZZZZE3.crt	
	[2]	ldap://al.siemens.net/CN=ZZZZZE3,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZE3,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZE3,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZE3,L=PKI?cACertificate	
	[3]	ldap://al.siemens.com/CN=ZZZZZE3,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZE3,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZE3,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZE3,o=Trustcenter?cACertificate	
	[4]	http://ocsp.siemens.com	http://ocsp.siemens.com	http://ocsp.siemens.com	http://ocsp.siemens.com	
AKI		Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier	
SKI		Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier	Include Authority Key Identifier
SAN	RFC822-Name	User Mail Address	User Mail Address	User Mail Address	User Mail Address	Include Subject Key Identifier
Key Usage Critical		Key Encipherment	Key Encipherment			Digital Signature
		Data Encipherment	Data Encipherment			
EKU Non-Critical		kp-emailProtection	kp-emailProtection	kp-emailProtection	kp-emailProtection	OCSPSigning
		Encrypting File System	Encrypting File System	Encrypting File System	Encrypting File System	
		File Recovery	File Recovery	File Recovery	File Recovery	
				driveEncryption (bitlocker)	driveEncryption (bitlocker)	
CDP	[1]	http://ch.siemens.com/pki?ZZZZZE3.crl	http://ch.siemens.com/pki?ZZZZZE3.crl	http://ch.siemens.com/pki?ZZZZZE3.crl	http://ch.siemens.com/pki?ZZZZZE3.crl	
	[2]	ldap://cl.siemens.net/CN=ZZZZZE3,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZE3,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZE3,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZE3,L=PKI?certificateRevocationList	
	[3]	ldap://cl.siemens.com/CN=ZZZZZE3,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZE3,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZE3,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZE3,o=Trustcenter?certificateRevocationList	
Basic Constr Critical	Type	End Entity	End Entity	End Entity	End Entity	End Entity
	Path length	Nothing	Nothing	Nothing	Nothing	Nothing
Certificate Policies	Siemens OID	1.3.6.1.4.1.4329.7.2.2.3.2.3	1.3.6.1.4.1.4329.7.2.2.3.2.3	1.3.6.1.4.1.4329.7.2.2.3.1.3	1.3.6.1.4.1.4329.7.2.2.4.1.3	1.3.6.1.4.1.4329.7.2.5
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/
	SMIME BR OID	2.23.140.1.5.2.2	2.23.140.1.5.2.2	2.23.140.1.5.3.2	2.23.140.1.5.3.2	
OCSP NoCheck						YES

4 Siemens Issuing CA Intranet Code Signing 2023 – Policies

	Name	ZZZZZZE4_CS_FCT_SC	ZZZZZZE4_CS_FCT_P12	ZZZZZZE4_OCSP_SIGNER_P10
General	Description	Internal Code Signing for Functional Identity on SmartCard	Internal Code Signing for Functional Identity on soft token	Policy (P10) Class OCSP Signer Certificate on HSM
	Certificate Type	Authentication	Authentication	OCSP Signing
	Version	V3	V3	V3
	Algorithm	sha256RSA	sha256RSA	sha256RSA
	Public Key	RSA 2048 bits generated on SmartCard	RSA 2048 bits generated centrally	RSA 2048 bits generated on HSM
	Validity Period	36 months	36 days	12 months
Issuer DN		CN=Siemens Issuing CA Intranet Code Signing 2023 OU = Siemens Trust Center SN=ZZZZZZE4 O=Siemens L=Muenchen SP=Bayern C=DE	CN=Siemens Issuing CA Intranet Code Signing 2023 OU = Siemens Trust Center SN=ZZZZZZE4 O=Siemens L=Muenchen SP=Bayern C=DE	CN=Siemens Issuing CA Intranet Code Signing 2023 OU = Siemens Trust Center SN=ZZZZZZE4 O=Siemens L=Muenchen SP=Bayern C=DE
Subject DN		Common Name (CN)	Common Name (CN)	CN
		Serial Number (SN)	Serial Number (SN)	Organization Name (O)
		Organization Name (O)	Organization Name (O)	State Name (ST)
				Country (C)
AIA	[1]	http://ah.siemens.com/pki?ZZZZZZE4.crt	http://ah.siemens.com/pki?ZZZZZZE4.crt	
	[2]	ldap://al.siemens.net/CN=ZZZZZZE4,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZE4,L=PKI?cACertificate	
	[3]	ldap://al.siemens.com/CN=ZZZZZZE4,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZE4,o=Trustcenter?cACertificate	
	[4]	http://ocsp.siemens.com	http://ocsp.siemens.com	
AKI		Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier
SKI		Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier
Key Usage Critical		Digital Signature	Digital Signature	Digital Signature
EKU		kp-codeSigning	kp-codeSigning	OCSPSigning
CDP	[1]	http://ch.siemens.com/pki?ZZZZZZE4.crl	http://ch.siemens.com/pki?ZZZZZZE4.crl	
	[2]	ldap://cl.siemens.net/CN=ZZZZZZE4,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZE4,L=PKI?certificateRevocationList	
	[3]	ldap://cl.siemens.com/CN=ZZZZZZE4,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZE4,o=Trustcenter?certificateRevocationList	
Basic Constr Critical	Type	End Entity	End Entity	End Entity
	Path length	Nothing	Nothing	Nothing
Certificate Policies	Siemens OID	1.3.6.1.4.1.4329.7.2.2.3.2.3	1.3.6.1.4.1.4329.7.2.2.3.2.3	1.3.6.1.4.1.4329.7.2.5
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/
OCSP NoCheck				YES

5 Siemens Issuing CA Medium Strength Authentication 2023 – Policies

	Name	ZZZZZZE6_AUTH_FCT_P12	ZZZZZZE6_AUTH_SMA_P12	ZZZZZZE6_AUTH_KBP_P12	ZZZZZZE6_OCSP_SIGNER_P10
General	Description	Authentication for Functional Identity on soft token P12	Strong Authentication for Siemens Employee on SmartCard	Strong Authentication for Known Business Partner on SmartCard	Policy (P10) Class OCSP Signer Certificate on HSM
	Certificate Type	Authentication	Authentication	Authentication	OCSP Signing
	Version	V3	V3	V3	V3
	Algorithm	sha256RSA	sha256RSA	sha256RSA	sha256RSA
	Public Key	RSA 2048 bits generated centrally	RSA 2048 bits generated centrally	RSA 2048 bits generated centrally	RSA 2048 bits generated on HSM
	Validity Period	12 months	825 days	12 months	12 months
Issuer DN		CN=Siemens Issuing CA Medium Strength Authentication 2023 SN=ZZZZZZE6 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA Medium Strength Authentication 2023 SN=ZZZZZZE6 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA Medium Strength Authentication 2023 SN=ZZZZZZE6 O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA Medium Strength Authentication 2023 SN=ZZZZZZE6 O=Siemens SP=Bayern C=DE
Subject DN		Common Name (CN)	Common Name (CN)	Common Name (CN)	CN
		Serial Number (SN)	Surname (SURNAME)	Surname (SURNAME)	Organization Name (O)
		Email (E)	Given Name (GN)	Given Name (GN)	State Name (ST)
		organizationIdentifier (ORG_ID)	Serial Number (SN)	Serial Number (SN)	Country (C)
		Organization Name (O)	Email (E)	Email (E)	
		State Name (ST)	organizationIdentifier (ORG_ID)	organizationIdentifier (ORG_ID)	
		Country (C)	Organization Name (O)	Organization Name (O)	
			State Name (ST)	State Name (ST)	
			Country (C)	Country (C)	
AIA	[1]	http://ah.siemens.com/pki?ZZZZZZE6.crt	http://ah.siemens.com/pki?ZZZZZZE6.crt	http://ah.siemens.com/pki?ZZZZZZE6.crt	
	[2]	ldap://al.siemens.net/CN=ZZZZZZE6,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZE6,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZE6,L=PKI?cACertificate	
	[3]	ldap://al.siemens.com/CN=ZZZZZZE6,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZE6,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZE6,o=Trustcenter?cACertificate	
	[4]	http://ocsp.siemens.com	http://ocsp.siemens.com	http://ocsp.siemens.com	
AKI		Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier
SKI		Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier
SAN	Other Name	User Principal Name	User Principal Name	User Principal Name	
	RFC822-Name	User Mail Address	User Mail Address	User Mail Address	
Key Usage Critical		Digital Signature	Digital Signature	Digital Signature	Digital Signature
EKU Non-Critical		kp-ClientAuth	kp-ClientAuth	kp-ClientAuth	OCSPSigning
		kp-emailProtection	kp-emailProtection	kp-emailProtection	
CDP	[1]	http://ch.siemens.com/pki?ZZZZZZE6.crl	http://ch.siemens.com/pki?ZZZZZZE6.crl	http://ch.siemens.com/pki?ZZZZZZE6.crl	
	[2]	ldap://cl.siemens.net/CN=ZZZZZZE6,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZE6,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZE6,L=PKI?certificateRevocationList	
	[3]	ldap://cl.siemens.com/CN=ZZZZZZE6,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZE6,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZE6,o=Trustcenter?certificateRevocationList	
Basic Constr Critical	Type	End Entity	End Entity	End Entity	End Entity
	Path length	Nothing	Nothing	Nothing	Nothing
Certificate Policies	Siemens OID	1.3.6.1.4.1.4329.7.2.2.3.2.3	1.3.6.1.4.1.4329.7.2.2.3.1.3	1.3.6.1.4.1.4329.7.2.2.4.1.3	1.3.6.1.4.1.4329.7.2.5
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/
	SMIME BR OID	2.23.140.1.5.2.2	2.23.140.1.5.3.2	2.23.140.1.5.3.2	
OCSP NoCheck					YES

6 Siemens Issuing CA MSA Impersonalized Entities 2023 – Policies

	Name	ZZZZZZEB_APP_FCT_P12	ZZZZZZEB_OCSP_SIGNER_P10
General	Description	Internal APP authentication for Functional Identity on soft token	Policy (P10) Class OCSP Signer Certificate on HSM
	Certificate Type	Authentication	OCSP Signing
	Version	V3	V3
	Algorithm	sha256RSA	sha256RSA
	Public Key	RSA 2048 bits generated on SmartCard	RSA 2048 bits generated on HSM
	Validity Period	36 months	12 months
Issuer DN		CN=Siemens Issuing CA MSA Impersonalized Entities 2023 OU = Siemens Trust Center SN=ZZZZZZEB O=Siemens L=Muenchen SP=Bayern C=DE	CN=Siemens Issuing CA MSA Impersonalized Entities 2023 OU = Siemens Trust Center SN=ZZZZZZEB O=Siemens L=Muenchen SP=Bayern C=DE
Subject DN		Common Name (CN)	CN
		Serial Number (SN)	Organization Name (O)
		Organization Name (O)	State Name (ST)
			Country (C)
AIA	[1]	http://ah.siemens.com/pki?ZZZZZZEB.crt	
	[2]	ldap://al.siemens.net/CN=ZZZZZZEB,L=PKI?cACertificate	
	[3]	ldap://al.siemens.com/CN=ZZZZZZEB,o=Trustcenter?cACertificate	
	[4]	http://ocsp.siemens.com	
AKI		Include Authority Key Identifier	Include Authority Key Identifier
SKI		Include Subject Key Identifier	Include Subject Key Identifier
Key Usage Critical		Digital Signature	Digital Signature
EKU		kp-ClientAuth	OCSPSigning
CDP	[1]	http://ch.siemens.com/pki?ZZZZZZEB.crl	
	[2]	ldap://cl.siemens.net/CN=ZZZZZZEB,L=PKI?certificateRevocationList	
	[3]	ldap://cl.siemens.com/CN=ZZZZZZEB,o=Trustcenter?certificateRevocationList	
Basic Constr Critical	Type	End Entity	End Entity
	Path length	Nothing	Nothing
Certificate Policies	Siemens OID	1.3.6.1.4.1.4329.7.2.2.3.2.3	1.3.6.1.4.1.4329.7.2.5
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/
OCSP NoCheck			YES

7 Siemens Issuing CA EE Network Smartcard Auth 2023 – Policies

	Name	ZZZZZZED_AUTH_SMA_NSC	ZZZZZZED_AUTH_KBP_NSC	ZZZZZZED_AUTH_SMA_VSC	ZZZZZZED_AUTH_KBP_NSC	ZZZZZZED_OCSP_SIGNER_P10
General	Description	Network Smartcard for Siemens Employee	Network Smartcard for Known Business Partner	Virtual Smartcard for Siemens Employee	Virtual Smartcard for Known Business Partner	Policy (P10) Class OCSP Signer
	Certificate	Authentication	Authentication	Authentication	Authentication	OCSP Signing
	Version	V3	V3	V3	V3	V3
	Algorithm	sha256RSA	sha256RSA	sha256RSA	sha256RSA	sha256RSA
	Public Key	RSA 2048 bits generated on NSC backend	RSA 2048 bits generated on NSC backend	RSA 2048 bits generated on HSM	RSA 2048 bits generated on HSM	RSA 2048 bits generated on
	Validity Period	825 days	12 months	825 days	12 months	12 months
Issuer DN		CN=Siemens Issuing CA EE Network Smartcard Auth 2023 SN=ZZZZZZED O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Network Smartcard Auth 2023 SN=ZZZZZZED O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Network Smartcard Auth 2023 SN=ZZZZZZED O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Network Smartcard Auth 2023 SN=ZZZZZZED O=Siemens SP=Bayern C=DE	CN=Siemens Issuing CA EE Network Smartcard Auth 2023 SN=ZZZZZZED O=Siemens SP=Bayern
Subject DN		Common Name (CN)	Common Name (CN)	Common Name (CN)	Common Name (CN)	CN
		Serial Number (SN)	Surname (SURNAME)	Surname (SURNAME)	Surname (SURNAME)	Organization Name (O)
		Email (E)	Given Name (GN)	Given Name (GN)	Given Name (GN)	State Name (ST)
		organizationIdentifier (ORG_ID)	Serial Number (SN)	Serial Number (SN)	Serial Number (SN)	Country (C)
		Organization Name (O)	Email (E)	Email (E)	Email (E)	
		State Name (ST)	organizationIdentifier (ORG_ID)	organizationIdentifier (ORG_ID)	organizationIdentifier (ORG_ID)	
		Country (C)	Organization Name (O)	Organization Name (O)	Organization Name (O)	
			State Name (ST)	State Name (ST)	State Name (ST)	
			Country (C)	Country (C)	Country (C)	
AIA	[1]	http://ah.siemens.com/pki?ZZZZZZED.crt	http://ah.siemens.com/pki?ZZZZZZED.crt	http://ah.siemens.com/pki?ZZZZZZED.crt	http://ah.siemens.com/pki?ZZZZZZED.crt	
	[2]	ldap://al.siemens.net/CN=ZZZZZZED,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZED,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZED,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZED,L=PKI?cACertificate	
	[3]	ldap://al.siemens.com/CN=ZZZZZZED,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZED,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZED,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZED,o=Trustcenter?cACertificate	
	[4]	http://ocsp.siemens.com	http://ocsp.siemens.com	http://ocsp.siemens.com	http://ocsp.siemens.com	
AKI		Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier	Include Authority Key Identifier
SKI		Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier	Include Subject Key Identifier
SAN	Other Name	User Principal Name	User Principal Name	User Principal Name	User Principal Name	
	RFC822-Name	User Mail Address	User Mail Address	User Mail Address	User Mail Address	
Key Usage Critical		Digital Signature	Digital Signature	Digital Signature	Digital Signature	Digital Signature
EKU		kp-ClientAuth	kp-ClientAuth	kp-ClientAuth	kp-ClientAuth	OCSPSigning
		kp-emailProtection	kp-emailProtection	kp-emailProtection	kp-emailProtection	
		SmartCard Logon	SmartCard Logon	SmartCard Logon	SmartCard Logon	
CDP	[1]	http://ch.siemens.com/pki?ZZZZZZED.crl	http://ch.siemens.com/pki?ZZZZZZED.crl	http://ch.siemens.com/pki?ZZZZZZED.crl	http://ch.siemens.com/pki?ZZZZZZED.crl	
	[2]	ldap://cl.siemens.net/CN=ZZZZZZED,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZED,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZED,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZED,L=PKI?certificateRevocationList	
	[3]	ldap://cl.siemens.com/CN=ZZZZZZED,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZED,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZED,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZED,o=Trustcenter?certificateRevocationList	
Basic Constr Critical	Type	End Entity	End Entity	End Entity	End Entity	End Entity
	Path length	Nothing	Nothing	Nothing	Nothing	Nothing
Certificate Policies	Siemens OID	1.3.6.1.4.1.4329.7.2.2.3.1.1	1.3.6.1.4.1.4329.7.2.2.4.1.1	1.3.6.1.4.1.4329.7.2.2.3.1.1	1.3.6.1.4.1.4329.7.2.2.4.1.1	1.3.6.1.4.1.4329.7.2.5
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/
	SMIME BR OID	2.23.140.1.5.3.2	2.23.140.1.5.3.2	2.23.140.1.5.3.2	2.23.140.1.5.3.2	
OCSP NoCheck						YES