Siemens Trust Center PKI

CA Hierarchy 2017 - EE Policies

Document History

Version	Date	Author	Change Comment
1.0	January 31, 2019	M. Fechter / GS IT HR 7 4	First initial version
1.1	March 08, 2019	M. Fechter / GS IT HR 7 4	Department GS IT ISEC changed to CT CYS
1.2	April 01, 2019	M. Fechter / SOP IT IN COR TSQ	GS IT HR 7 4 is reorganized to SOP IT IN COR TSQ CT CYS is reorganized to CT CYS CCS IT

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 1.2 and status Released has been classified as “Unrestricted”.

	Name	Department	Date
Author	Various authors, detailed information in document history		
Checked by	Rufus Buschart Florian Grotz	Siemens SOP IT IN COR Siemens SOP IT IN COL	02.04.2019
Authorization	Markus Wichmann	Siemens CT CYS CCS IT	02.04.2019

This document has been approved by the responsible service owner at Siemens CT CYS CCS IT on April 02, 2019.

Table of Content

SCOPE AND APPLICABILITY 2
DOCUMENT STATUS 2
1 INTRODUCTION 4
1.1 OVERVIEW 4
1.2 LIST OF ABBREVIATIONS 4
2 SIEMENS ISSUING CA INTRANET SERVER 2017 – POLICIES 5
3 SIEMENS ISSUING CA INTERNET SERVER 2017 – POLICIES 6

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:

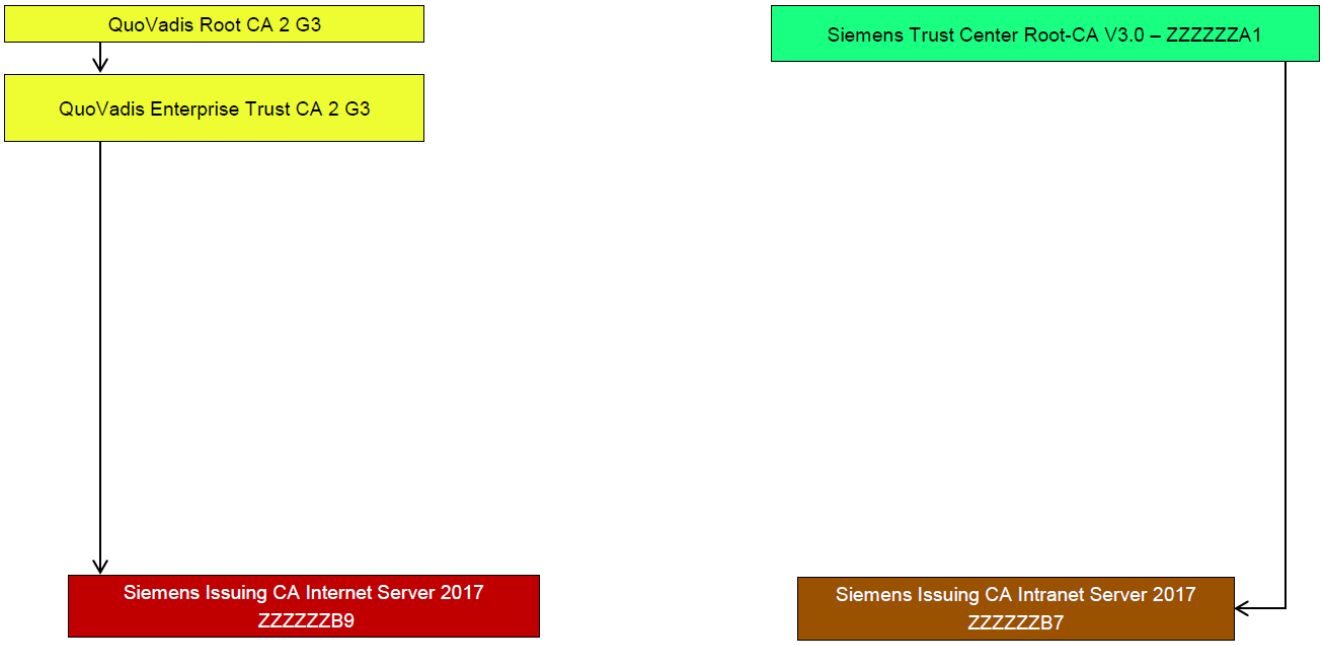

Figure 1: Siemens PKI Hierarchy 2017

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 Intranet Server 2017 – Policies

General	Name	GSIT_SERVER_INTRANET_24M_SHA2_ZZZZZZB7	GSIT_SERVER_Auth_P12_SHA2_ZZZZZZB7	GSIT_SERVER_INTRANET_24M_SHA2_ZZZZZZB7_SAP	GSIT_OCSP_SIGNER_P10_SHA2_ZZZZZZB7
	Description	Class Server Intranet certificates - 24 month	Class Server Intranet certificates - P12 files	Class Server Intranet certificates - SAP systems	Class OCSP Signer certificates - 12 month
	Certificate Type	Server	Server	Server	Server
	Signing CA (DN)	CN=Siemens Issuing CA Intranet Server 2017;OU=Siemens Trust Center;SN=ZZZZZZB7;O=Siemens;L=Muenchen;SP=Bayern;C=DE	CN=Siemens Issuing CA Intranet Server 2017;OU=Siemens Trust Center;SN=ZZZZZZB7;O=Siemens;L=Muenchen;SP=Bayern;C=DE	CN=Siemens Issuing CA Intranet Server 2017;OU=Siemens Trust Center;SN=ZZZZZZB7;O=Siemens;L=Muenchen;SP=Bayern;C=DE	CN=Siemens Issuing CA Intranet Server 2017;OU=Siemens Trust Center;SN=ZZZZZZB7;O=Siemens;L=Muenchen;SP=Bayern;C=DE
Subject DN	DN	CN	CN	CN	CN
		OU	OU	C	OU
		O	O	O	O
		C	C	OU	C
Options	Algorhytm used	RSA/SHA256	RSA/SHA256	RSA/SHA256	RSA/SHA256
	Key Lenth	2048	2048	2048	2048
	Validity Period	24	12	24	12
	Key Type	User or system generated Keys	Centrally Generated Keys	User or system generated Keys	User or system generated Keys
	Delivery by Email (PKCS12)	no	no	no	no
		PKCS11	PKCS12	PKCS11	PKCS11
AIA	Method:	CA Issuers	CA Issuers	CA Issuers	
	Type:	Uniform Resource Identifier	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	http://ah.siemens.com/pki?ZZZZZZB7.crt	http://ah.siemens.com/pki?ZZZZZZB7.crt	http://ah.siemens.com/pki?ZZZZZZB7.crt	
AIA	Method:	CA Issuers	CA Issuers	CA Issuers	
	Type:	Uniform Resource Identifier	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	ldap://al.siemens.net/CN=ZZZZZZB7,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZB7,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZB7,L=PKI?cACertificate	
AIA	Method:	CA Issuers	CA Issuers	CA Issuers	
	Type:	Uniform Resource Identifier	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	ldap://al.siemens.com/CN=ZZZZZZB7,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZB7,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZB7,o=Trustcenter?cACertificate	
AIA	Method:	OCSP	OCSP	OCSP	
	Type:	Uniform Resource Identifier	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	http://ocsp1.pki-services.siemens.com	http://ocsp1.pki-services.siemens.com	http://ocsp1.pki-services.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 Authority Key Identifier	Include Subject Key Identifier
SAN	Type	DNS Name	DNS Name	DNS Name	
	Value	empty	empty	empty	
KU		Digital Signature	Digital Signature	Digital Signature	Digital Signature
		Key encipherment	Key encipherment	Key encipherment	
		critical	**critical**	**critical**	**critical**
EKU		kp-ServerAuth	kp-ServerAuth	kp-ServerAuth	OCSPSigning
		kp-ClientAuth	kp-ClientAuth	kp-ClientAuth	
		Non-Critical	**Non-Critical**	**Non-Critical**	**Non-Critical**
CDP	Type:	Uniform Resource Identifier	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	http://ch.siemens.com/pki?ZZZZZZB7.crl	http://ch.siemens.com/pki?ZZZZZZB7.crl	http://ch.siemens.com/pki?ZZZZZZB7.crl	
CDP	Type:	Uniform Resource Identifier	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	ldap://cl.siemens.net/CN=ZZZZZZB7,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZB7,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZB7,L=PKI?certificateRevocationList	
CDP	Type:	Uniform Resource Identifier	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	ldap://cl.siemens.com/CN=ZZZZZZB7,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZB7,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZB7,o=Trustcenter?certificateRevocationList	
B-Constr.		End Entity	End Entity	End Entity	End Entity
		critical	**critical**	**critical**	**critical**
CP	Siemens Public Key Infrastructure	1.3.6.1.4.1.4329.7.2.4	1.3.6.1.4.1.4329.7.2.4	1.3.6.1.4.1.4329.7.2.4	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/
		Non-Critical	**Non-Critical**	**Non-Critical**	**Non-Critical**
CP	CPS	1.3.6.1.4.1.4329.99.1.1.1.1.0	1.3.6.1.4.1.4329.99.1.1.1.1.0	1.3.6.1.4.1.4329.99.1.1.1.1.0	
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/	
CP	CPS	1.3.6.1.4.1.4329.99.2.2.1.1.0	1.3.6.1.4.1.4329.99.2.2.1.1.0	1.3.6.1.4.1.4329.99.2.2.1.1.0	
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/	
OCSP NoCheck					YES

3 Siemens Issuing CA Internet Server 2017 – Policies

General	Name	GSIT_SERVER_INTERNET_24M_SHA2_ZZZZZZB9	GSIT_SERVER_Auth_P12_SHA2_ZZZZZZB9	GSIT_OCSP_SIGNER_P10_SHA2_ZZZZZZB9
	Description	Class Server Intranet certificates - 24 month	Class Server Intranet certificates - P12 files	Class OCSP Signer certificates - 12 month
	Certificate Type	Server	Server	Authentication
	Signing CA (DN)	CN=Siemens Issuing CA Internet Server 2017;OU=Siemens Trust Center;SN=ZZZZZZB9;O=Siemens;L=Muenchen;SP=Bayern;C=DE	CN=Siemens Issuing CA Internet Server 2017;OU=Siemens Trust Center;SN=ZZZZZZB9;O=Siemens;L=Muenchen;SP=Bayern;C=DE	CN=Siemens Issuing CA Internet Server 2017;OU=Siemens Trust Center;SN=ZZZZZZB9;O=Siemens;L=Muenchen;SP=Bayern;C=DE
Subject DN	DN	CN	CN	CN
		OU	OU	OU
		O	O	O
		L	L	C
		SP	SP	
		C	C	
Options	Algorhytm used	RSA/SHA256	RSA/SHA256	RSA/SHA256
	Key Lenth	2048	2048	2048
	Validity Period	24	12	12
	Key Type	User or system generated Keys	Centrally Generated Keys	User or system generated Keys
	Delivery by Email (PKCS12)	no	no	no
		PKCS11	PKCS12	PKCS11
AIA	Method:	CA Issuers	CA Issuers	
	Type:	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	http://ah.siemens.com/pki?ZZZZZZB9.crt	http://ah.siemens.com/pki?ZZZZZZB9.crt	
AIA	Method:	CA Issuers	CA Issuers	
	Type:	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	ldap://al.siemens.net/CN=ZZZZZZB9,L=PKI?cACertificate	ldap://al.siemens.net/CN=ZZZZZZB9,L=PKI?cACertificate	
AIA	Method:	CA Issuers	CA Issuers	
	Type:	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	ldap://al.siemens.com/CN=ZZZZZZB9,o=Trustcenter?cACertificate	ldap://al.siemens.com/CN=ZZZZZZB9,o=Trustcenter?cACertificate	
AIA	Method:	OCSP	OCSP	
	Type:	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	http://ocsp1.pki-services.siemens.com	http://ocsp1.pki-services.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
SAN	Type	DNS Name	DNS Name	
	Value	empty	empty	
KU		Digital Signature	Digital Signature	Digital Signature
		Key encipherment	Key encipherment	
		critical	**critical**	**critical**
EKU		kp-ServerAuth	kp-ServerAuth	OCSPSigning
		kp-ClientAuth	kp-ClientAuth	
		Non-Critical	**Non-Critical**	**Non-Critical**
CDP	Type:	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	http://ch.siemens.com/pki?ZZZZZZB9.crl	http://ch.siemens.com/pki?ZZZZZZB9.crl	
CDP	Type:	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	ldap://cl.siemens.net/CN=ZZZZZZB9,L=PKI?certificateRevocationList	ldap://cl.siemens.net/CN=ZZZZZZB9,L=PKI?certificateRevocationList	
CDP	Type:	Uniform Resource Identifier	Uniform Resource Identifier	
	Value:	ldap://cl.siemens.com/CN=ZZZZZZB9,o=Trustcenter?certificateRevocationList	ldap://cl.siemens.com/CN=ZZZZZZB9,o=Trustcenter?certificateRevocationList	
B-Constr.		End Entity	End Entity	End Entity
		critical	**critical**	**critical**
CP	Siemens Public Key Infrastructure	1.3.6.1.4.1.4329.7.2.4	1.3.6.1.4.1.4329.7.2.4	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/
		Non-Critical	**Non-Critical**	**Non-Critical**
CP	QuoVadis OID assigned to Siemens	1.3.6.1.4.1.8024.0.2.1800.0	1.3.6.1.4.1.8024.0.2.1800.0	1.3.6.1.4.1.8024.0.2.1800.0
	CPS URI	http://www.quovadisglobal.com/repository	http://www.quovadisglobal.com/repository	http://www.quovadisglobal.com/repository
CP	OV Certificates	2.23.140.1.2.2	2.23.140.1.2.2	
CP	CP	1.3.6.1.4.1.4329.99.1.1.1.1.0	1.3.6.1.4.1.4329.99.1.1.1.1.0	1.3.6.1.4.1.4329.99.1.1.1.1.0
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/
CP	CPS	1.3.6.1.4.1.4329.99.2.2.1.1.0	1.3.6.1.4.1.4329.99.2.2.1.1.0	1.3.6.1.4.1.4329.99.2.2.1.1.0
	CPS URI	http://www.siemens.com/pki/	http://www.siemens.com/pki/	http://www.siemens.com/pki/
OCSP NoCheck				YES
Certificte Transperancy SCT	SCT out of the CT log	1.3.6.1.4.1.11129.2.4.2	1.3.6.1.4.1.11129.2.4.2	