



Siemens Trust Center PKI

CA Hierarchy Policy 2017

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 STATUS2**
- 1 INTRODUCTION4**
 - 1.1 OVERVIEW4
- 2 SIEMENS ROOT CA.....5**
 - 2.1 SIEMENS TRUST CENTER ROOT CA V3.0 20165
- 3 SIEMENS ISSUING CA`S.....6**
 - 3.1 SIEMENS ISSUING CA INTRANET SERVER 20176
 - 3.2 SIEMENS ISSUING CA INTERNET SERVER 2017.....7

1 Introduction

This document explains the Siemens CA Hierarchy 2016 (Root & Issuing).

1.1 Overview

The following picture shows the Siemens Root CAs together with the respective Issuing CAs:

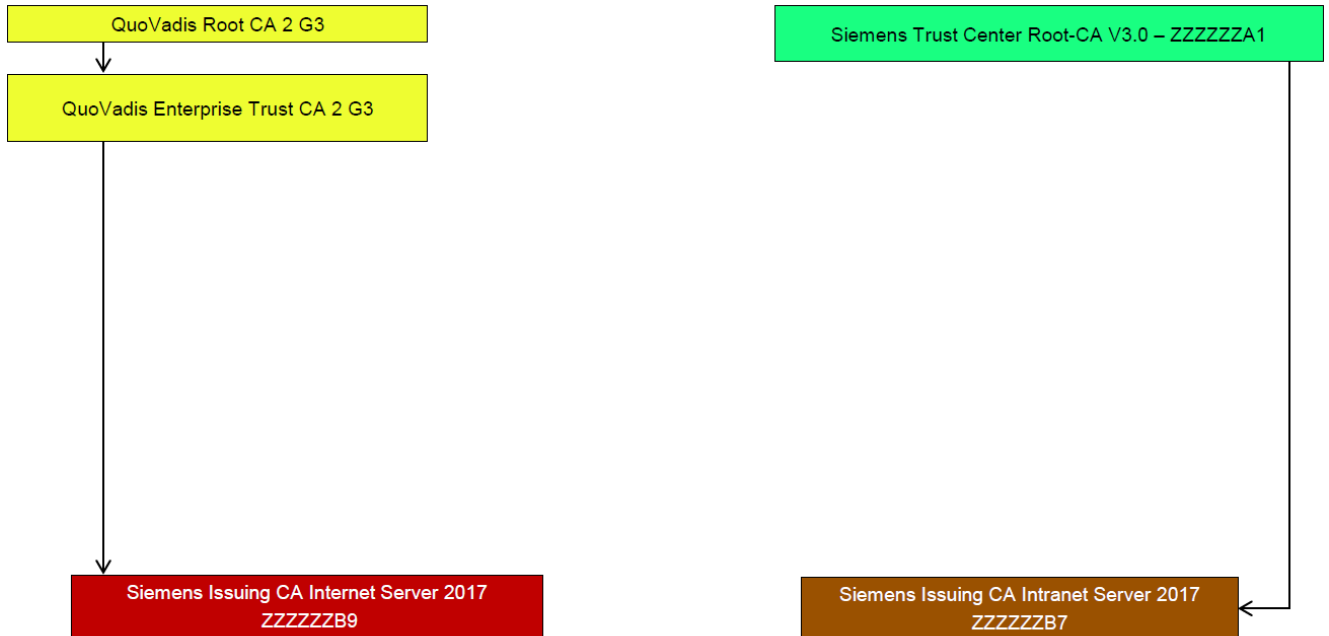


Figure 1: Siemens PKI Hierarchy 2017

2 Siemens Root CA

2.1 Siemens Trust Center Root CA V3.0 2016

Contents	Definition	Value
Subject Distinguished Name (DN)		CN=Siemens Root CA V3.0 2016;OU=Siemens Trust Center;SN=ZZZZZA1;O=Siemens;L=Muenchen;SP=Bayern;C=DE
Key Length		4096
Signature Algorithm		sha256withRSA
Reference	New Cross Certificate	Siemens Trust Center Root CA V3.0 2016
Crypto Token		Safenet, Inc. - rootca
Issuer Distinguished Name (DN)		CN=Siemens Root CA V3.0 2016;OU=Siemens Trust Center;SN=ZZZZZA1;O=Siemens;L=Muenchen;SP=Bayern;C=DE
Not Valid After:		12 years
Authority Key Identifier		Include Authority Key Identifier
Subject Key Identifier		Include Subject Key Identifier
Key Usage		Key Cert Sign
		CRL Sign
		critical
Basic Constraints		CA
	Path Length	-1
		critical
Certificate Policies	Any Policy	2.5.29.32.0
	CPS URI	http://www.siemens.com/pki/
		Non-Critical

3 Siemens Issuing CA's

3.1 Siemens Issuing CA Intranet Server 2017

Contents	Definition	Value
Subject Distinguished Name (DN)		CN=Siemens Issuing CA Intranet Server 2017;OU=Siemens Trust Center;SN=ZZZZZB7;O=Siemens;L=Muenchen;SP=Bayern;C=DE
Key Length		4096
Signature Algorithm		sha256withRSA
Reference	New Cross Certificate	Siemens Issuing CA Intranet Server 2017
Issuer Distinguished Name (DN)		CN=Siemens Root CA V3.0 2016;OU=Siemens Trust Center;SN=ZZZZZA1;O=Siemens;L=Muenchen;SP=Bayern;C=DE
Not Valid After:		6 years
Authority Information Access	Method:	CA Issuers
	Type:	Uniform Resource Identifier
	Value:	ldap://al.siemens.net/CN=ZZZZZA1,L=PKI?cACertificate
Authority Information Access	Method:	CA Issuers
	Type:	Uniform Resource Identifier
	Value:	http://ah.siemens.com/pki?ZZZZZA1.crt
Authority Information Access	Method:	CA Issuers
	Type:	Uniform Resource Identifier
	Value:	ldap://al.siemens.com/uid=ZZZZZA1,o=Trustcenter?cACertificate
Authority Information Access	Method:	OCSP
	Type:	Uniform Resource Identifier
	Value:	http://ocsp1.pki-services.siemens.com
Authority Key Identifier		Include Authority Key Identifier
Subject Key Identifier		Include Subject Key Identifier
Key Usage		Key Cert Sign
		CRL Sign
		critical
Extended Key Usage		kp-serverAuth
		kp-clientAuth
		OCSPSigning
		Non-Critical
CRL Distribution Point	Type:	Uniform Resource Identifier
	Value:	ldap://cl.siemens.net/CN=ZZZZZA1,L=PKI?authorityRevocationList
CRL Distribution Point	Type:	Uniform Resource Identifier
	Value:	http://ch.siemens.com/pki?ZZZZZA1.crl
CRL Distribution Point	Type:	Uniform Resource Identifier
	Value:	ldap://cl.siemens.com/uid=ZZZZZA1,o=Trustcenter?authorityRevocationList
Basic Constraints		CA
	Path Length	0
		critical
Certificate Policies	Siemens Public Key Infrastructure	1.3.6.1.4.1.4329.7
	CPS URI	http://www.siemens.com/pki/
		Non-Critical
	Siemens Public Key Infrastructure	1.3.6.1.4.1.4329.99.1.1.1.1.0
	CPS URI	http://www.siemens.com/pki/
		Non-Critical
	Siemens Public Key Infrastructure	1.3.6.1.4.1.4329.99.2.2.1.1.0
	CPS URI	http://www.siemens.com/pki/
		Non-Critical

3.2 Siemens Issuing CA Internet Server 2017

Contents	Definition	Value
Subject Distinguished Name (DN)		CN=Siemens Issuing CA Internet Server 2017;OU=Siemens Trust Center;SN=ZZZZZB9;O=Siemens;L=Muenchen;SP=Bayern;C=DE
Key Length		4096
Signature Algorithm		sha256withRSA
Reference	New Cross Certificate	Siemens Issuing CA Internet Server 2017
Issuer Distinguished Name (DN)		CN=QuoVadis Enterprise Trust CA 2 G3;O=QuoVadis Limited;C=BM
Not Valid After:		6 years
Authority Information Access	Method:	CA Issuers
	Type:	Uniform Resource Identifier
	Value:	http://trust.quovadisglobal.com/qventca2g3.crt
Authority Information Access	Method:	OCSP
	Type:	Uniform Resource Identifier
	Value:	http://rs.ocsp.quovadisglobal.com
Authority Key Identifier		Include Authority Key Identifier
Subject Key Identifier		Include Subject Key Identifier
Key Usage		Key Cert Sign
		CRL Sign
		critical
Extended Key Usage		kp-clientAuth
		OCSPSigning
		kp-serverAuth
		Non-Critical
CRL Distribution Point	Type:	Uniform Resource Identifier
	Value:	http://crl.quovadisglobal.com/qventca2g3.crl
Basic Constraints		CA
	Path Length	0
		critical
Certificate Policies	QV OID which identifies Siemens	1.3.6.1.4.1.8024.0.2.1800.0
	CPS URI	http://www.quovadisglobal.com/repository
		Non-Critical
Certificate Policies	Siemens Public Key Infrastructure	1.3.6.1.4.1.4329.7
	CPS URI	http://www.siemens.com/pki/
		Non-Critical
Certificate Policies	QV OID	2.23.140.1.2.2
		Non-Critical
Certificate Policies	CPS	1.3.6.1.4.1.4329.99.1.1.1.0
	CPS URI	http://www.siemens.com/pki/
		Non-Critical
Certificate Policies	CPS	1.3.6.1.4.1.4329.99.2.2.1.1.0
	CPS URI	http://www.siemens.com/pki/
		Non-Critical