SwissSign CPR Sign

Certificate, CRL and OCSP Profiles for Signing certificates

Document Type:	Certificate, CRL and OCSP Profiles
OID:	n/a
Author:	Information Security and Compliance
Classification:	Attribution-NoDerivs (CC-BY-ND) 4.0
Applicability:	Global
Owner:	CEO
Issue Date:	08 November 2021
Version:	3.0
Obsoletes:	2.0; 11.10.2021
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Disclaimer: The electronic version of this document and all its stipulations are considered binding if saved in Adobe PDF Format and signed by two legal representatives of SwissSign. All other copies and media are null and void.

Version Control

Date	Version	Comment	Author
14.07.2021	1.0	Initial version	Michael Günther
11.10.2021	2.0	Adding new Products / Issuing CAs	Michael Günther
08.11.2021	3.0	Format correction of OID and CPS-URI in policy extension fields	Michael Günther

© SwissSign AG, 08.11.2021

Authorization

Date	Approved by	Approved by	Version
12.07.2021	Michael Günther	Markus Naef	1.0
07.10.2021	Michael Günther	Markus Naef	2.0
08.11.2021	Michael Günther	Markus Naef	3.0

Michael Frank Günther
5. November 2021

Qualified Electronic Signature by SwissID

digital signature

digital signature

Table of Contents

© SwissSign AG, 08.11.2021

1. Introduction

This document describes profiles of the Signing and Sealing certificates issued by the SwissSign Issuing CAs as described in the CPS [3] as well as OCSP responses and CRL profiles related to these certificates.

This document complements Certificate Policy [1] and Certification Practice Statement [3].

SwissSign PKI hierarchy description can be found from chapter 1.1 from CPS [3].

1.1 Terms and abbreviations

Refer to the TSPS [4].

2. General profiles

2.1 Root CA

The Root CA profile **after** effective date of this CPR and the corresponding CP and CPS is the following:

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number			Unique serial number of the certificate
SignatureAlgorithm			
Issuer Distinguished name			Unique issuer distinguished name of the certificate, for the Root CA this field shall be identical with the Subject Distinguished Name
Subject Distinguished name			Unique subject distinguished name of the certificate
	Common Name (CN)	Name of the Root CA	(mandatory)
	OrganizationName (O)	Subject (organization) name as stated in certificate application.	(mandatory)
	OrganizationIdentifier (2.5.4.97)	Unique Identification Number of the Organization, e.g. NTR, VAT, etc.	(optional)
	Country (C)	Country code in accordance with ISO 3166	(mandatory)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Basic Constraints	CA: TRUE		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier			(mandatory)
Authority Key Identifier			(optional)
Extended Key Usage			Not allowed in the Root CA
Name Constraints			Not allowed in the Root CA
Certificate Policies			Not allowed in the Root CA
CRL Distribution Points			Not allowed in the Root CA
Authority Information Access			Not allowed in the Root CA

© SwissSign AG, 08.11.2021

2.2 Issuing CA

The Issuing CA profile **after** effective date of this CPR and the corresponding CP and CPS is the following:

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number			Unique serial number of the certificate
SignatureAlgorithm			
Issuer Distinguished name			Unique issuer (i.e. Root CA) distinguished name of the certificate
Subject Distinguished name			Unique subject distinguished name of the certificate
	Common Name (CN)	Name of the Issuing CA	(mandatory)
	OrganizationName (O)	Subject (organization) name as stated in certificate application.	(mandatory)
	OrganizationIdentifier (2.5.4.97)	Subject's (organization) Unique Identification Number of the Organization, e.g. NTR, VAT, etc.	(mandatory)
	Country (C)	Country code in accordance with ISO 3166	(mandatory)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Basic Constraints	CA: TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier			(mandatory)
Authority Key Identifier			(mandatory)
Extended Key Usage			(optional)
Name Constraints			(optional)
Certificate Policies	Policy OID: <OID referencing SwissSign specific policy> CPSURI: <URI pointing to CPS> User Notice: "regulated certificate" Policy OID: < OID according to ETSI EN 319 411 NCP+, QCP-n-qscd or QCP-l-qscd >		(mandatory) User Notice: "regulated certificate" is only mandatory in CA certificates according to Swiss digital signature law (ZertES).
CRL Distribution Points			(mandatory)
Authority Information Access			(optional)

2.3 Algorithm object identifiers

The algorithms with OIDs supported by this CA and its subsidiaries are:

Algorithm	Object Identifier
SHA256withRSAEncryption	1.2.840.113549.1.1.11
RSASSA-PSS	1.2.840.113549.1.1.10
rsaEncryption	1.2.840.113549.1.1.1

2.4 Key sizes

All leaf certificates contain an RSA public key whose modulus has a length of 2048 bit or higher and is divisible by 8.

All CA certificates contain an RSA public key whose modulus has a length of 4096 bit.

3. Certificate Profiles of the SwissSign Signature Services Root 2020 – 2 PKI

The following certificate profiles are compiled in accordance with ITU-T X.509 version 3, IETF RFC 5280 [10], clause 6.6 of ETSI EN 319 411-1/2 [5]/[6].

3.1 Root CA

3.1.1 SwissSign Signature Services Root 2020 – 2

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	2FDBA9B88D001EBCE7B99C2D23EF4A	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Signature Services Root 2020 - 2 O=SwissSign AG C=CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Signature Services Root 2020 - 2 O=SwissSign AG C=CH	Unique subject distinguished name of the certificate
Valid from	2020-10-07 10:19:32 UTC	Start of certificate validity.
Valid to	2050-09-30 10:19:32 UTC	End of certificate validity.
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	C99B6176377D397796F4A1E97BCDEB2070F2E084	
Authority Key Identifier	C99B6176377D397796F4A1E97BCDEB2070F2E084	
Extended Key Usage	not included in this Root CA certificate	
Name Constraints	not included in this Root CA certificate	
Certificate Policies	not included in this Root CA certificate	
CRL Distribution Points	not included in this Root CA certificate	
Authority Information Access	not included in this Root CA certificate	

The Root CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	425419CD83663AE8815437BBEEF09B15E3723E39
SHA256 Fingerprint	B87F292A4D9FEACE2D669159EB26F56D85EC77C19E01098CD754E8ABB310CDE5

3.2 Issuing CAs

3.2.1 SwissSign Qualified Electronic Signature ICA 2021 - 2

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	00CE3774E62AA97F1F3D6D8801DB4AC4	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Signature Services Root 2020 - 2 O=SwissSign AG C=CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Qualified Electronic Signature ICA 2021 - 2 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	2021-03-31 12:28:00 UTC	Start of certificate validity.
Valid to	2036-03-31 12:28:00 UTC	End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	069B3BD514ECA62EFB76573C9923EA1D2DDE2C00	
Authority Key Identifier	C99B6176377D397796F4A1E97BCDEB2070F2E084	
Extended Key Usage	not included in this Issuing CA certificate	
Name Constraints	not included in this Issuing CA certificate	
Certificate Policies	Policy OID: 2.16.756.1.89.1.4.2.1 CPSURI: https://repository.swisssign.com/SwissSign-Signing-Services-CP-CPS.pdf User Notice: “regulated certificate”	
CRL Distribution Points	http://crl.swisssign.net/C99B6176377D397796F4A1E97BCDEB2070F2E084 ldap://directory.swisssign.net/CN=C99B6176377D397796F4A1E97BCDEB2070F2E084%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	

Authority Information Access	Not included in this Issuing CA	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	42393eb31652bd262450a59f828cfa84a233be08
SHA256 Fingerprint	511d6a337b3c310724a21170d360371feaa181e849288efc19b4c7e51028c17b

3.2.2 SwissSign Qualified TSA ICA 2021 - 1

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	35f5d427c383316ccb565bab131029	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Signature Services Root 2020 - 2 O=SwissSign AG C=CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN= SwissSign Qualified TSA ICA 2021 - 1 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	2021-09-27 14:25:51 UTC	Start of certificate validity.
Valid to	2036-09-23 14:25:51 UTC	End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	38995732EEEB8ECFF77504172EE72987224326A6	
Authority Key Identifier	C99B6176377D397796F4A1E97BCDEB2070F2E084	
Extended Key Usage	not included in this Issuing CA certificate	
Name Constraints	not included in this Issuing CA certificate	
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.24 CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf User Notice: “regulated certificate”	
CRL Distribution Points	http://crl.swisssign.net/C99B6176377D397796F4A1E97BCDEB2070F2E084 ldap://directory.swisssign.net/CN=C99B6176377D397796F4A1E97BCDEB2070F2E084%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	

Authority Information Access	Not included in this Issuing CA	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	8ABB6C89320199C63136320632ED197219B5EBD3
SHA256 Fingerprint	715DBAF62F04EA1EC8C04FB7CFDC3526B86DAF8635EEFF4376E49984C1971A7A

3.2.3 SwissSign Qualified Electronic Signature ICA 2021 - 3

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	10da5f04d354a9a5bb76ab73bc8831	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Signature Services Root 2020 - 2 O=SwissSign AG C=CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Qualified Electronic Signature ICA 2021 - 3 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	2021-09-27 14:33:44 UTC	Start of certificate validity.
Valid to	2036-09-23 14:33:44 UTC	End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	852612B8ED62322B32855C326199C6C07EF8C876	
Authority Key Identifier	C99B6176377D397796F4A1E97BCDEB2070F2E084	
Extended Key Usage	not included in this Issuing CA certificate	
Name Constraints	not included in this Issuing CA certificate	
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.22 CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf User Notice: “regulated certificate”	
CRL Distribution Points	http://crl.swisssign.net/C99B6176377D397796F4A1E97BCDEB2070F2E084 ldap://directory.swisssign.net/CN=C99B6176377D397796F4A1E97BCDEB2070F2E084%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	

Authority Information Access	Not included in this Issuing CA	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	CB5DA3DBF00518BD69FBE5374420052BBB483336
SHA256 Fingerprint	C3907D39F17AE01B29F62B7FA89F35AE3F2756B9052DBDA8F7A0A7A76DA06395

3.2.4 SwissSign Advanced Seal ICA 2021 - 1

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	5f42fce2992fbf0063abc945da76c7	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Signature Services Root 2020 - 2 O=SwissSign AG C=CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN= SwissSign Advanced Seal ICA 2021 - 1 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	2021-09-27 13:10:41 UTC	Start of certificate validity.
Valid to	2036-09-23 13:10:41 UTC	End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	52762051DD92597F53D073195D9F134808E91B85	
Authority Key Identifier	C99B6176377D397796F4A1E97BCDEB2070F2E084	
Extended Key Usage	not included in this Issuing CA certificate	
Name Constraints	not included in this Issuing CA certificate	
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.23 CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf	
CRL Distribution Points	http://crl.swisssign.net/C99B6176377D397796F4A1E97BCDEB2070F2E084 ldap://directory.swisssign.net/CN=C99B6176377D397796F4A1E97BCDEB2070F2E084%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	

Authority Information Access	Not included in this Issuing CA	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	6EF78409DE89D27A8CD0D63D96E3B69F6F35C5CC
SHA256 Fingerprint	9DE4880EFA9A19A9EE767169A85140D1057054985CC9EFF8E0D7D4C8A4DF4E84

3.3 End-entity certificates

3.3.1 QCP-n-qscd RSS: Qualified Electronic Signature Certificates issued by SwissSign Qualified Electronic Signature ICA 2021 - 2

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
Serial Number	Unique serial number of the certificate		The certificate serial number is unique within the range of the Issuing CA and contains randomness.
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Qualified Electronic Signature ICA 2021 - 2 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name			Unique subject distinguished name of the certificate
	Common Name (CN)	GivenName Surname or pseudo: Pseudonym	(mandatory)
	GivenName	Subject's Given Name as stated in certificate application.	(mandatory if CN without Pseudonym)
	Surname	Subject's Surname Name as stated in certificate application.	(mandatory if CN without Pseudonym)
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional)
	SerialNumber	Unique number generated by the TSP.	(mandatory)
	Country (C)	Country code in accordance with ISO 3166	(mandatory)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	069B3BD514ECA62EFB76573C9923EA1D2DDE2C00		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	nonRepudiation		(mandatory) Critical

Extended Key Usage			not allowed
Subject Alternative Name			not allowed
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.21 CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf Policy OID: 0.4.0.194112.1.2 (QCP-n-qscd) User Notice: “qualified certificate”		(mandatory)
CRL Distribution Points	http://crl.swisssign.net/069B3BD514ECA62EFB76573C9923EA1D2DDE2C00 ldap://directory.swisssign.net/CN=069B3BD514ECA62EFB76573C9923EA1D2DDE2C00%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/069B3BD514ECA62EFB76573C9923EA1D2DDE2C00	(mandatory)
	OCSP	http://ocsp.swisssign.net/069B3BD514ECA62EFB76573C9923EA1D2DDE2C00	(mandatory)
QC Statement	0.4.0.1862.1.4 (Secure Signature Creation Device Qualified Certificate) 0.4.0.1862.1.5 PDS=https://repository.swisssign.com/SwissSign-PDS.pdf 0.4.0.1862.1.6 QC Type=0.4.0.1862.1.6.1 0.4.0.1862.1.7 QC CC Legislation=CH		The following QC statements shall be set: • Secure Signature Creation Device Qualified Certificate • Certificate type for electronic signatures • Under which legislation the qualified certificates was issued.

3.3.2 QCP-n-qscd UBS: Qualified Electronic Signature Certificates issued by SwissSign Qualified Electronic Signature ICA 2021 - 3

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
Serial Number	Unique serial number of the certificate		The certificate serial number is unique within the range of the Issuing CA and contains randomness.
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Distinguished name	organizationIdentifier=NTRCH-CHE-109.357.012 CN=SwissSign Qualified Electronic Signature ICA 2021 - 3 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name			Unique subject distinguished name of the certificate
	Common Name	GivenName Surname or	(mandatory)

	(CN)	pseudo: Pseudonym	
	GivenName	Subject's Given Name as stated in certificate application.	(mandatory)
	Surname	Subject's Surname Name as stated in certificate application.	(mandatory)
	SerialNumber	Unique number generated by the TSP / Registration Authority (RA) uniquely identifying the subject	(mandatory)
	Country (C)	Country code in accordance with ISO 3166	(mandatory)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	852612b8ed62322b32855c326199c6c07ef8c876		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	nonRepudiation		(mandatory) Critical
Extended Key Usage	1.3.6.1.4.1.311.10.3.12 (MS Document Signing) 1.2.840.113583.1.1.5 (Adobe Authentic Documents Trust)		
Subject Alternative Name			not allowed
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.22 CPSURI: _ https://repository.swisssign.com/SwissSign_CPS_Signing.pdf Policy OID: 0.4.0.194112.1.2 User Notice: "This is a qualified certificate according to Swiss digital signature law. This is a qualified certificate for electronic signatures and must only be used for UBS documents and contracts with UBS."		(mandatory)
CRL Distribution Points	http://crl.swisssign.net/852612B8ED62322B32855C326199C6C07EF8C876 ldap://directory.swisssign.net/CN=852612b8ed62322b32855c326199c6c07ef8c876%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/852612B8ED62322B32855C326199C6C07EF8C876	(mandatory)
	OCSP	http://ocsp.swisssign.net/852612b8ed62322b32855c326199c6c07ef8c876	(mandatory)
QC Statement	0.4.0.1862.1.4 0.4.0.1862.1.5 PDS=https://repository.swisssign.com/SwissSign-PDS.pdf 0.4.0.1862.1.6 QC Type=0.4.0.1862.1.6.1 0.4.0.1862.1.7 QC CC Legislation=CH		The following QC statements shall be set: • Secure Signature Creation Device Qualified Certificate • Certificate type for electronic signatures • Under which legislation the qualified certificates was issued.

3.3.3 NCP+: Advanced Electronic Seals Certificates issued by SwissSign Advanced Seal ICA 2021 – 1

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
Serial Number	Unique serial number of the certificate		The certificate serial number is unique within the range of the Issuing CA and contains randomness.
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Distinguished name	organizationIdentifier= NTRCH-CHE-109.357.012 CN= SwissSign Advanced Seal ICA 2021 – 1 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name			Unique subject distinguished name of the certificate
	Common Name (CN)	Subject's (organization) name as stated in certificate application.	(mandatory)
	OrganizationName (O)	Subject's (organization) name as stated in certificate application.	(mandatory)
	OrganizationIdentifier (2.5.4.97)	Subject's (organization) Unique Identification Number of the Organization, e.g. NTR, VAT, etc.	(mandatory)
	OrganizationUnit (OU)	Organization unit belonging to the subject's organization	(optional)
	Locality (L)	Subject's locality	(optional)
	StateOrProvince (ST)	Subject's state or province	(optional)
	Country (C)	Country code in accordance with ISO 3166	(mandatory)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	52762051dd92597f53d073195d9f134808e91b85		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature (mandatory), nonRepudiation (optional)		(mandatory) Critical
Extended Key Usage	1.3.6.1.4.1.311.10.3.12 (MS Document Signing) 1.2.840.113583.1.1.5 (Adobe Authentic Documents Trust)		
Subject Alternative Name			not allowed
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.23 CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf Policy OID: 0.4.0.2042.1.2		(mandatory)

CRL Distribution Points	http://crl.swisssign.net/52762051DD92597F53D073195D9F134808E91B85 ldap://directory.swisssign.net/CN=52762051dd92597f53d073195d9f134808e91b85%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/52762051DD92597F53D073195D9F134808E91B85	(mandatory)
	OCSP	http://ocsp.swisssign.net/52762051dd92597f53d073195d9f134808e91b85	(mandatory)

3.3.4 QCP-l-qscd: Regulated Electronic Seal Certificates for Time Stamping issued by SwissSign Qualified TSA ICA 2021 - 1

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
Serial Number	Unique serial number of the certificate		The certificate serial number is unique within the range of the Issuing CA and contains randomness.
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Distinguished name	CN= SwissSign Qualified TSA ICA 2021 - 1 O = SwissSign AG C = CH organizationIdentifier=NTRCH-CHE-109.357.012		Unique issuer distinguished name of the certificate
Subject Distinguished name			Unique subject distinguished name of the certificate
	Common Name (CN)	Subject's (organization) name as stated in certificate application.	(mandatory)
	OrganizationName (O)	Subject's (organization) name as stated in certificate application.	(mandatory)
	OrganizationIdentifier (2.5.4.97)	Subject's (organization) Unique Identification Number of the Organization, e.g. NTR, VAT, etc.	(mandatory)
	Country (C)	Country code in accordance with ISO 3166	(mandatory)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	38995732eeeb8ecff77504172ee72987224326a6		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature		(mandatory) Critical
Extended Key Usage	id-kp-timeStamping		(mandatory) Critical

Subject Alternative Name			not allowed
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.24 CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf Policy OID: 0.4.0.194112.1.3 User Notice: “regulated certificate”		(mandatory)
CRL Distribution Points	http://crl.swisssign.net/38995732EEEB8ECFF77504172EE72987224326A6 ldap://directory.swisssign.net/CN=38995732eeeb8ecff77504172ee72987224326a6%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/38995732EEEB8ECFF77504172EE72987224326A6	(mandatory)
	OCSP	http://ocsp.swisssign.net/38995732eeeb8ecff77504172ee72987224326a6	(mandatory)
QC Statement	0.4.0.1862.1.4 0.4.0.1862.1.5 PDS=https://repository.swisssign.com/SwissSign-PDS.pdf 0.4.0.1862.1.6 QC Type=0.4.0.1862.1.6.2 0.4.0.1862.1.7 QC CC Legislation=CH		The following QC statements shall be set: • Secure Signature Creation Device Qualified Certificate • Certificate type for electronic signatures • Under which legislation the qualified certificates was issued.

4. OCSP Profile

SwissSign OCSP v1 is built according to RFC 6960 [13].

OCSP response Field	Values	Comment
Response Status	0 for successful or error code	Result of the query
Response Type	id-pkix-ocsp-basic	Type of the response (mandatory)
Version	V1	(mandatory)
Responder Id	DN	Distinguished name of the OCSP responder (mandatory)
Produced At	Date	Date when the OCSP response was signed (mandatory)
CertID	Unique ID for requested certificate	The CertID from the OCSP request is included in the response.
Cert Status	Good, revoked, or unknown	Indicates the response for certificate status (mandatory)
Revocation Time		Date of revocation of certificate
revocationReason		For the Issuing CA this exention may be present. For leaf certificates the revocationReason shall not be present
This Update		Date when the status was queried from database (mandatory)
Next Update		The time at or before which newer information will be available about the status of the certificate. The OCSP response is valid for 3 days. The information provided is updated at least 8 hours prior to the nextUpdate. For Root and Issuing CA: The OCSP response is valid for 3 days. The information provided is updated at least 8 hours prior to the nextUpdate.
Nonce		Value is copied from request if it is included. (optional)
Signature Algorithm:	sha256WithRSAEncryption	(mandatory)
Certificate		Details of certificate used to sign the response (mandatory)

The OCSP extensions used are specified below:

- Nonce

The ArchiveCutOff extension is not set in the OCSP responses.

4.1 OCSP Responder Certificate

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number			Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name			Unique issuer distinguished name of the certificate (Root CA for the Issuing CA and the Issuing CA for the end entity certificate)
Subject Distinguished name	CommonName		Unique subject distinguished name of the OCSP Signer certificate. The CN shall include the string “OCSP Responder” and the reference to the Issuer.
	OrganizationName (O)	SwissSign AG	
	Country (C)	CH	
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Key Usage	digitalSignature		(mandatory)
Subject Key Identifier			(mandatory)
Authority Key Identifier			(mandatory)
Extended Key Usage	id-kp-ocspSigning		(mandatory)
Certificate Policies	Policy OID: CPSURI:		(optional)
ocspNoCheck			(mandatory)
CRL Distribution Points	Not included in this certificate		
Authority Information Access	Not included in this certificate		

5. CRL Profile

SwissSign issues CRLs in accordance to the guides of RFC 5280 [10].

The CRL profile is applicable to the Root CA and its subordinated issuing CAs.

Extension Attribute	**Values**	**Comment**
Version Number	V2	CRL format version pursuant to X.509.
Signature Algorithm	sha256WithRSAEncryption	Hash method and the signature algorithm used to sign the CRL pursuant to RFC 5280.
Issuer Distinguished Name		Unique issuer distinguished name of the certificate
Effective Date		Date and time of CRL issuance.
Next Update		Date and time of issuance of the next CRL. Maximum validity for CARL of the Root CA is 1 year after the publication of the CRL. The validity for CRLs provided by the Issuing CAs is 10 days. If it is the last CRL issued for those certificates in the scope of this CRL, the nextUpdate field in the CRL will be set to "99991231235959Z" as required by IETF RFC 5280.
Revocation List Number		CRL sequence number
ExpiredCertsOnCRL		Indication that revoked certificates are kept in the CRL after their expiration.
Revoked Certificates:		List of the serial numbers of the revoked Certificate.
Serial Number		Serial number of the revoked certificate.
Revocation Date		Date and time of revocation of the certificate.
reasonCode		Reason code for certificate revocation. Not applicable for end-entity certificates. For CARL issued by the Root CA - reasonCode extension is present and not marked critical - possible reason codes in CARL: - cACompromise (2), or - cessationOfOperation (5)
Signature		Confirmation signature of the authority issued the CRL.
Authority Key Identifier		The Authority key identifier of the Root or Issuing CA

© SwissSign AG, 08.11.2021

6. References

[1] SwissSign CP QCP-n-qscd RSS – Certificate Policy for Qualified Signature certificates for RSS, published under: https://repository.swisssign.com
[2] SwissSign CPR Sign - Certificate, CRL and OCSP Profiles for Signing certificates, published under: https://repository.swisssign.com
[3] SwissSign CPS Sign - Certification Practice Statement for Signing certificates, published under: https://repository.swisssign.com
[4] SwissSign TSPS - Trust Services Practice Statement, published under: https://repository.swisssign.com
[5] ETSI EN 319 411-1 v1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
[6] ETSI EN 319 411-2 (2018): Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[7] ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)
[8] VZertES: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032)
[9] TAV-BAKOM: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)
[10] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
[11] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;
[12] RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
[13] RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
[14] ISO 3166 Codes;
[15] SwissSign CP QCP-n-qscd UBS – Certificate Policy for Qualified Signature certificates for UBS, published under: https://repository.swisssign.com
[16] SwissSign CP QCP-l-qscd – Certificate Policy for Regulated Seal certificates, published under: https://repository.swisssign.com
[17] SwissSign CP NCP+ – Certificate Policy for Advanced Seal certificates, published under: https://repository.swisssign.com

© SwissSign AG, 08.11.2021