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:	30.10.2023
Version:	5.0
Obsoletes:	4.0; 12.12.2022
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

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
12.12.2022	4.0	Update of OCSP response (remarks) and TSU profile, removal of UBS profile, Minor redactional changes	Roman Fischer, Adrian Müller
30.10.2023	5.0	Adding qcStatement-1, adding new certificate profiles, updating CP references	Adrian Müller

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
12.12.2022	Michael Günther	Michael Widmer	4.0
30.10.2023	Michael Günther	Johannes Termin	5.0

Michael Günther

October 30, 2023

Qualified Electronic Signature by SwissID

digital signature

Johannes Termin
30. Oktober 2023

Qualified Electronic Signature by SwissID

digital signature

Table of Contents

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

2.2 Issuing CA

The Issuing CA profile **after** effective date of the initial version 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	Comment
ecPublicKey (ANSI X9.62 public key type)	1.2.840.10045.2.1	Not used (Public Key of type elliptic curve)
rsaEncryption	**1.2.840.113549.1.1.1**	**Public Key is of type RSA.**
RSASSA-PSS / RSA-PSS	**1.2.840.113549.1.1.10**	**Signature algorithm with Probabilistic Signature Scheme using an RSA key pair**
SHA256withRSAEncryption	*1.2.840.113549.1.1.11*	*Phasing out (used in certificates under old hierarchy and in cross certificate)*
SHA512withRSAEncryption	*1.2.840.113549.1.1.13*	*Phasing out (used in certificates under old hierarchy and in cross certificate)*
ANSI x9.62 ECDSA with SHA256	1.2.840.10045.4.3.2	Not used (signature algorithm using an elliptic curve)
ANSI x9.62 ECDSA with SHA384	1.2.840.10045.4.3.3	Not used (signature algorithm using an elliptic curve)
ANSI x9.62 ECDSA with SHA512	1.2.840.10045.4.3.4	Not used (signature algorithm using an elliptic curve)
SHA256	2.16.840.1.101.3.4.2.1	Hash-algorithm used with Mask Generation Function
SHA384	2.16.840.1.101.3.4.2.2	Hash-algorithm used with Mask Generation Function
SHA512	**2.16.840.1.101.3.4.2.3**	**Hash-algorithm used with Mask Generation Function**
SHA3-256	2.16.840.1.101.3.4.2.8	Not used
SHA3-384	2.16.840.1.101.3.4.2.9	Not used
SHA3-512	2.16.840.1.101.3.4.2.10	Not used
MGF1	**1.2.840.113549.1.1.8**	**Mask Generation Function used with RSASSA-PSS**
secp256r1/NIST P-256/prime256v1	1.2.840.10045.3.1.7	Not used (curve used with ecDSA)
secp384r1/NIST P-384/prime384v1	1.3.132.0.34	Not used (curve used with ecDSA)
secp521r1/NIST P-521//prime512v1	1.3.132.0.35	Not used (curve used with ecDSA)

2.4 Key sizes

RSA:

All leaf certificates contain an RSA public key whose modulus has a size of **3072 bit** or larger and is divisible by 8.

The CA certificates contain an RSA public key whose modulus has a size of **4096 bit** or larger if not stated otherwise.

All *RSA-PSS signatures* are applied using the Mask Generation Function **MGF1**.

The end-user and Issuing CA applied *RSA-PSS signatures* are created using **SHA-512**.

The *RSA-PSS* signed CA certificates are signed using an **SHA-512** hash algorithm.

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 (CRL & OCSP only)

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	0.4.0.1862.1.1 (qcs-QcCompliance, optional) 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: • Qualified Certificate Compliance (will be mandatory in future versions) • Secure Signature Creation Device Qualified Certificate • Certificate type for electronic signatures • Under which legislation the qualified certificates was issued.

3.3.2 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)
	OrganizationNa	Subject’s (organization) name as stated in	(mandatory)

	me (O)	certificate application.	
	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)

3.3.3 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	0.4.0.1862.1.1 (qcs-QcCompliance, optional) 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: • ETSI “Qualified Certificate Compliance”, i.e. ZertES Regulated Certificate Compliance (will be mandatory in future versions) • Secure Signature Creation Device Qualified Certificate • Certificate type for electronic signatures • Under which legislation the qualified certificates was issued.
Private Key Usage Period	notBefore: Same as in certificate validity (Valid from) notAfter: notBefore + 14 months	(optional) Please note: This extension indicates for how long the private key belonging to the certificate may be used. As the keypair and certificate of the timestamping unit are updated on an annual basis, the time is set to 1 year plus 2 months buffer time. The inclusion of this extension is recommended within ETSI EN 319 422. However, as the support of this extension is not widespread amongst client- and CA-software it is (or may be) omitted.

4. Certificate Profiles of the SwissSign Signature Services Root CA 2023 – 1 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].

4.1 Root CA

4.1.1 SwissSign RSA SIGN Signature Services Root 2023 – 1

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	3533c200275041af81a4db9a56b9db3dfee562f6	Unique serial number of the certificate
SignatureAlgorithm	• RSA-PSS • SHA512 • MGF1	SHA512 with RSA-PSS and MGF1
Issuer Distinguished Name (IDN)	CN= SwissSign RSA SIGN Signature Services Root CA 2023 – 1 O = SwissSign AG organizationIdentifier = NTRCH-CHE-109.357.012 C = CH	Unique distinguished name of the root certificate Format: • PrintableString (MUST for Country attribute, SHOULD for all other attributes) • Alternative: UTF-8 organizationIdentifier with prefix NTRCH contains the Swiss Enterprise Identification Number, see ETSI EN 319 412-1, chapter 4.1.4 “Legal person semantics identifier”.
Subject Distinguished Name (SDN)	*{byte-for-byte identical to IDN}*	Unique Subject Distinguished Name of the certificate; same as in Issuer DN
Valid from	*2023-06-21 10:36:07 UTC*	Start of certificate validity (Creation date)
Valid to	*2048-06-21 10:36:07 UTC*	End of certificate validity (Creation date +25 years)
Public Key	Type: rsaEncryption (OID: 1.2.840.113549.1.1.1)	
	Modulus, length: 4096bit	
	Public exponent: 65537	
Basic Constraints	CA: TRUE	Critical ()
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier (SKI)	*{SHA1 hash of public key}*	
Authority Key Identifier (AKI)	*{SHA1 hash of public key, identical to SKI}*	
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	

The Root CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	cfbf7502b1e855d50478f2d1dea96120004877c1
SHA256 Fingerprint	37c3be5c2555178a6ecb473ec6fbee4d849d67661afbc10f1f46db95aff57ac6

4.2 Cross certificates

4.2.1 SwissSign RSA SIGN Signature Services Root 2023 – 1 issued by SwissSign Signature Services Root 2020 – 2

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	009a409412c4ffb2b2bdb9ef557ec0e5	Unique serial number of the certificate
SignatureAlgorithm	sha512WithRSAEncryption	Use sha512WithRSAEncryption if possible, otherwise the usual sha256WithRSAEncryption
Issuer Distinguished Name (IDN)	organizationIdentifier = NTRCH-CHE-109.357.012 CN = SwissSign Signature Services Root 2020 – 2 O = SwissSign AG C = CH	
Subject Distinguished Name (SDN)	CN= SwissSign RSA SIGN Signature Services Root CA 2023 – 1 O = SwissSign AG organizationIdentifier = NTRCH-CHE-109.357.012 C = CH	Needs to be byte-for-byte identical to DN in selfsigned root
Valid from	2023-08-08 11:56:23 UTC	Start of certificate validity
Valid to	2039-08-07 11:56:23 UTC	End of certificate
Public Key	Type: rsaEncryption (OID: 1.2.840.113549.1.1.1)	(with/followed by a NULL value)
	Modulus, length: 4096bit	
	Public exponent	
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier (SKI)	0790FD676E871AA143FDFD5F46780A1BF71C5E39	*SHA1 hash of public key}*
Authority Key Identifier (AKI)	C99B6176377D397796F4A1E97BCDEB2070F2E084	*SKI of the Root CA that issued this cross certificate*
Extended Key Usage	not included in this Cross certificate	
Name Constraints	not included in this Cross certificate	
Certificate Policies	not included in this Cross certificate	
CRL Distribution Points	http://crl.swisssign.net/C99B6176377D397796F4A1E97BCDEB2070F2E084	
Authority Information Access	not included	

The Cross CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	43828c0b0fc93b08bb60131b4c8105a9e9e073cc
SHA256 Fingerprint	03db18f3752142c93c68b63d754380e0e1085dbaae8069721799213f272713ee

4.3 Issuing CAs

4.3.1 SwissSign RSA SIGN ZertES QES ICA 2023 - 1

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	1c6f52df84f6c11e981c4bb0f8a572e5da043133	Unique serial number of the certificate
SignatureAlgorithm	• RSA-PSS • SHA512 • MGF1	SHA512 with RSA-PSS and MGF1
Issuer Distinguished Name (IDN)	*<SDN of Root CA>*	Unique Issuer Distinguished Name of the certificate
Subject Distinguished Name (SDN)	CN= SwissSign RSA SIGN ZertES QES ICA 2023 - 1 O = SwissSign AG organizationIdentifier = NTRCH-CHE-109.357.012 C = CH	Unique Subject Distinguished Name (SDN) of the certificate Format (for all elements): PrintableString or UTF-8
Valid from	2023-08-10 09:26:33 UTC	Start of certificate validity
Valid to	*2038-08-10 09:26:33 UTC*	End of certificate validity
Public Key	Type: rsaEncryption (OID: 1.2.840.113549.1.1.1)	
	Modulus, length: 4096bit	
	Public exponent	
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier (SKI)	DC41077C0A527E38428D549A6C4E28AAD692D636	SHA1 hash of public key
Authority Key Identifier (AKI)	0790FD676E871AA143FDFD5F46780A1BF71C5E39	SKI of Root CA
Extended Key Usage	not included in this Issuing CA certificate	
Name Constraints	not included in this Issuing CA certificate	
Certificate Policies	Policy OID: 2.16.756.1.89.1.4.2.1.21 (SwissSign ZertES QES) CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf User Notice: “regulated certificate”	
CRL Distribution Points	http://crl.swisssign.ch/cdp-68ac2a5f-d2b9-49c5-8a53-2c3a9c64db6a	

Authority Information Access	Certification Authority Issuer = http://aia.swisssign.ch/air-74d777fc-c971-42d2-bd21-8d256bda9fd1	The CA download URL points to a cross certificate (if available) issued to the Root CA From ETSI EN 319 412-2 id-ad-caIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA. At least one accessLocation shall use the http or https RFC 2818 scheme
	OCSP: {empty}	*Please note: OCSP-URL is not set for CA certificates.*

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	349a2aedccd0d0f16a2cc6a1effd2ab1bc762970
SHA256 Fingerprint	0fcf8f0c05b25b3e7ba02b0b5300015a82b06d6dc38c875ccbb9cb258ac14a96

4.3.2 SwissSign RSA SIGN ZertES Qualified TSA ICA 2023 – 1 (timestamping CA)

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	164b78623f32bc16ce746cb6a159e80668e088fb	Unique serial number of the certificate
SignatureAlgorithm	• RSA-PSS • SHA512 • MGF1	SHA512 with RSA-PSS and MGF1
Issuer Distinguished Name (IDN)	*<SDN of Root CA>*	Unique Issuer Distinguished Name (IDN) of the certificate
Subject Distinguished Name (SDN)	CN = SwissSign RSA SIGN ZertES Qualified TSA ICA 2023 - 1 O = SwissSign AG organizationIdentifier = NTRCH-CHE-109.357.012 C = CH	Unique Subject Distinguished Name (SDN) of the certificate
Valid from	2023-08-10 09:18:17 UTC	Start of certificate validity
Valid to	2038-08-10 09:18:17 UTC	End of certificate validity
Public Key	Type: rsaEncryption (OID: 1.2.840.113549.1.1.1)	
	Modulus, length: 4096bit	
	Public exponent	
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier (SKI)	EF0C5A87D36EF58F9E278A7CCE5931F6273E3E0E	SHA1 hash of public key
Authority Key Identifier (AKI)	0790FD676E871AA143FDFD5F46780A1BF71C5E39	SKI of Root CA
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 (SwissSign CP QCP-l-qscd for timestamping) CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf User Notice: “regulated certificate”	
CRL Distribution Points	http://crl.swisssign.ch/cdp-68ac2a5f-d2b9-49c5-8a53-2c3a9c64db6a	

Authority Information Access	Certification Authority Issuer = http://aia.swisssign.ch/air-74d777fc-c971-42d2-bd21-8d256bda9fd1	The CA download URL points to a cross certificate (if available) issued to the Root CA From ETSI EN 319 412-2 id-ad-caIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA. At least one accessLocation shall use the http or https RFC 2818 scheme
	OCSP: {empty}	*Please note: OCSP-URL is not set for CA certificates.*

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	d0c1af79e7ad09db50bd4b9f3e4f57207d54bcaf
SHA256 Fingerprint	00dd968c10fbc69973ba88221fd72e49aba8f9076a7e7511ec5c139b12cb3034

4.3.3 SwissSign RSA SIGN NCPplus Advanced Seal ICA 2023 - 1

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	70b3b014800c45d447b40eaddec6eee7c77f0890	Unique serial number of the certificate
SignatureAlgorithm	• RSA-PSS • SHA512 • MGF1	SHA512 with RSA-PSS and MGF1
Issuer Distinguished Name (IDN)	*<SDN of Root>*	Unique Issuer Distinguished Name of the certificate
Subject Distinguished Name (SDN)	CN = SwissSign RSA SIGN NCPplus Advanced Seal ICA 2023 - 1 O = SwissSign AG organizationIdentifier = NTRCH-CHE-109.357.012 C = CH	Unique Subject Distinguished Name of the certificate
Valid from	2023-08-29 11:03:36 UTC	Start of certificate validity
Valid to	2038-08-29 11:03:36 UTC	End of certificate validity
Public Key	Type: rsaEncryption (OID: 1.2.840.113549.1.1.1)	
	Modulus, length: 4096bit	
	Public exponent	
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier (SKI)	58C8B8EFA8C3BB78BA3C10C4495242CDC43B5BAD	
Authority Key Identifier (AKI)	0790FD676E871AA143FDFD5F46780A1BF71C5E39	
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 (SwissSign CP NCP+) CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf	
CRL Distribution Points	http://crl.swisssign.ch/cdp-68ac2a5f-d2b9-49c5-8a53-2c3a9c64db6a	

Authority Information Access	Certification Authority Issuer = http://aia.swisssign.ch/air-74d777fc-c971-42d2-bd21-8d256bda9fd1	The CA download URL points to a cross certificate (if available) issued to the Root CA From ETSI EN 319 412-2 id-ad-caIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA. At least one accessLocation shall use the http or https RFC 2818 scheme
	OCSP: {empty}	*Please note: OCSP-URL is not set for CA certificates.*

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	9539e0e486e960111e9e19adef639a03b9afc718
SHA256 Fingerprint	1d46c97101f60ab4d17c6b378aae6f85605533767caac96e63115525df481901

4.4 End-entity certificates

4.4.1 QCP-n-qscd ZertES: ZertES Qualified Certificate for Electronic Signature issued by SwissSign RSA SIGN ZertES QES ICA 2023 - 1

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
Serial Number	*Unique serial number assigned by CA platform*		The certificate serial number is unique within the range of the Issuing CA and contains randomness.
SignatureAlgorithm	• RSA-PSS • SHA512 • MGF1		(SHA384 with RSA-PSS and MGF1 /) Preferred: SHA512 with RSA-PSS and MGF1
Issuer Distinguished Name (IDN)	CN = SwissSign RSA SIGN ZertES Qualified Signature ICA 2023 - 1 O = SwissSign AG organizationIdentifier = NTRCH-CHE-109.357.012 C = CH		Unique Issuer Distinguished Name of the certificate
Subject Distinguished Name (SDN)	(composed of the elements below)		Unique Subject Distinguished Name of the certificate
	Common Name (CN)	GivenName Surname or pseudo: Pseudonym	(mandatory) Format: UTF-8
	GivenName	Subject's Given Name as stated in certificate application.	(mandatory if CN without Pseudonym) Format: UTF-8 shall not be present if Pseudonym is present
	Surname	Subject's Surname Name as stated in certificate application.	(mandatory if CN without Pseudonym) Format: UTF-8 shall not be present if Pseudonym is present
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional) Format: UTF-8 shall not be present if GivenName and Surname are present
	SerialNumber	Unique number assigned by the TSP.	(mandatory) Format: PrintableString
	Country (C)	Country code in accordance with ISO 3166	(mandatory) Format: PrintableString
Valid from	*Creation date*		Start of certificate validity.
Valid to	*Creation date + 10 minutes*		End of certificate validity.
Public Key	Type: rsaEncryption (OID: 1.2.840.113549.1.1.1)		
	Modulus, length: 3072 bit or higher		
	Public exponent		

<table>
<tr><td>Authority Key Identifier (AKI)</td><td colspan="3">DC41077C0A527E38428D549A6C4E28AAD692D636</td><td>(mandatory)
equal to SKI in ICA profile</td></tr>
<tr><td>Subject Key Identifier (SKI)</td><td colspan="3">SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2</td><td>(mandatory)</td></tr>
<tr><td>Key Usage</td><td colspan="3">nonrepudiation (1)</td><td>(mandatory)
Critical</td></tr>
<tr><td>Extended Key Usage</td><td colspan="3"></td><td>Not included</td></tr>
<tr><td>Subject Alternative Name</td><td colspan="3"></td><td>not allowed</td></tr>
<tr><td>Certificate Policies</td><td colspan="3">Policy OID: 0.4.0.194112.1.2 (QCP-n-qscd)
Policy OID: 2.16.756.1.89.2.1.21 (SwissSign RSS ZertES QES)
CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf
User Notice: “qualified certificate”</td><td>(mandatory)
The policy OID QCP-n-qscd is defined and described in ETSI EN 319 411-2.</td></tr>
<tr><td>CRL Distribution Points</td><td colspan="3">http://crl.swisssign.ch/cdp-5f22416a-3a10-4e70-b0f7-b6fa5656f534</td><td>URLs of the CRL Distribution points (LDAP and/or HTTP)</td></tr>
<tr><td rowspan="2">Authority Information Access</td><td>caIssuers</td><td colspan="2">http://aia.swisssign.ch/air-cdcdd56e-41c1-4e49-909e-db758284333b</td><td>(mandatory)</td></tr>
<tr><td>OCSP</td><td colspan="2">http://ocsp.swisssign.ch/sign/ocs-cbd4cafa-e50a-4c88-a0ec-06cdc4e76fb1</td><td>(mandatory)</td></tr>
<tr><td>QC Statement</td><td>Include</td><td>OID /Key</td><td>Value</td><td rowspan="8">The following QC statements shall be set:
• Qualified Certificate Compliance
• Secure Signature Creation Device Qualified Certificate
• Pointer to PKI Disclosure Statement (PDS)
• Certificate type for electronic signatures
• Under which legislation the qualified certificates was issued, i.e. “CH” for Switzerland.

NOT set are the types
• qct-eseal (0.4.0.1862.1.6.2)
• qct-web (0.4.0.1862.1.6.3)</td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.1 (qcs-QcCompliance)</td><td></td></tr>
<tr><td>no</td><td>0.4.0.1862.1.2 (qcs-QcLimitValue)</td><td></td></tr>
<tr><td>no</td><td>0.4.0.1862.1.3 (qcs-QcRetentionPeriod)</td><td></td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.4 (qcs-QcSSCD)</td><td></td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.5 (qcs-QcPDS; pointer to PKI Disclosure Statement)</td><td>https://repository.swisssign.com/SwissSign-PDS.pdf language=en</td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.6 (qcs-QcType)</td><td>0.4.0.1862.1.6.1 (qct-esign)</td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.7 (QC CC legislation)</td><td>CH</td></tr>
<tr><td>Extension for short-term certificate “id-etsi-ext-valassured-ST-certs”
(OID: 0.4.0.194121.2.1)</td><td colspan="3">NULL value</td><td>Optional
(Syntax according to ETSI EN 319 412-1, section 5.2.3)</td></tr>
</table>

4.4.2 QCP-l-qscd: Regulated Electronic Seal Certificates for Time Stamping issued by SwissSign RSA SIGN ZertES Qualified TSA ICA 2023 – 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	• RSA-PSS • SHA512 • MGF1		SHA512 with RSA-PSS and MGF1
Issuer Distinguished Name (IDN)	CN= SwissSign RSA SIGN Qualified TSA ICA 2023 – 1 O = SwissSign AG organizationIdentifier = NTRCH-CHE-109.357.012 C = CH		Unique Issuer Distinguished Name of the certificate
Subject Distinguished Name (SDN)	(composed of the elements below)		Unique Subject Distinguished Name of the certificate
	Common Name (CN)	SwissSign ZertES TSA UNIT A 2023 – 1	(mandatory)
	OrganizationName (O)	SwissSign AG	(mandatory)
	OrganizationIdentifier (2.5.4.97)	NTRCH-CHE-109.357.012	(mandatory)
	Country (C)	CH	(mandatory)
Valid from	*Creation date*		Start of certificate validity
Valid to	*Creation date + max. 3 years*		End of certificate validity
Public Key	Type: rsaEncryption (OID: 1.2.840.113549.1.1.1)		
	Modulus, length: 3072 bit or higher		
	Public exponent		
Authority Key Identifier	EF0C5A87D36EF58F9E278A7CCE5931F6273E3E0E		(mandatory) equal to SKI in ICA
Subject Key Identifier	*<SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2>*		(mandatory)
Key Usage	digitalSignature (0)		(mandatory) Critical
Extended Key Usage	id-kp-timeStamping		(mandatory) Critical
Subject Alternative Name			not allowed

<table>
<tr><td>Certificate Policies</td><td colspan="3">Policy OID: 0.4.0.194112.1.3 (ETSI qcp-legal-qscd CP)
Policy OID: 2.16.756.1.89.2.1.24 (SwissSign TSA CP)
CPSURI:
https://repository.swisssign.com/SwissSign_CPS_Signing.pdf
User Notice: “regulated certificate”</td><td>(mandatory)</td></tr>
<tr><td>CRL Distribution Points</td><td colspan="3">http://crl.swisssign.ch/cdp-4177662b-421f-4e54-acd6-aec0d1b98f57</td><td>URLs of the CRL Distribution points (LDAP and/or HTTP)</td></tr>
<tr><td rowspan="2">Authority Information Access</td><td>caIssuers</td><td colspan="2">http://aia.swisssign.ch/air-bd959f50-aa2e-4f02-b52f-2f29db40cb67</td><td>(mandatory)</td></tr>
<tr><td>OCSP</td><td colspan="2">http://ocsp.swisssign.ch/sign/ocs-cbd4cafa-e50a-4c88-a0ec-06cdc4e76fb1</td><td>(mandatory)</td></tr>
<tr><td rowspan="8">QC Statement</td><td>Include</td><td>OID /Key</td><td>Value</td><td rowspan="8">The following QC statements shall be set:
• Qualified Certificate Compliance
• Secure Signature Creation Device Qualified Certificate
• Pointer to PKI Disclosure Statement (PDS)
• Certificate type for electronic seals
• Under which legislation the qualified certificates was issued, i.e. “CH” for Switzerland.

NOT set are the types
• qct-esign (0.4.0.1862.1.6.1)
• qct-web (0.4.0.1862.1.6.3)</td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.1
(qcs-QcCompliance)</td><td></td></tr>
<tr><td>no</td><td>0.4.0.1862.1.2
(qcs-QcLimitValue)</td><td></td></tr>
<tr><td>no</td><td>0.4.0.1862.1.3
(qcs-QcRetentionPeriod)</td><td></td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.4
(qcs-QcSSCD)</td><td></td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.5
(qcs-QcPDS)</td><td>https://repository.swisssign.com/SwissSign-PDS.pdf
language=en</td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.6
(qcs-QcType)</td><td>0.4.0.1862.1.6.2
(qct-eseal)</td></tr>
<tr><td>yes</td><td>0.4.0.1862.1.7
(QC CC legislation)</td><td>CH</td></tr>
<tr><td>Private Key Usage Period</td><td colspan="3">notBefore: Start of allowed usage period for signing timestamps
notAfter: notBefore + 14 months
(end of allowed usage period for signing timestamps)</td><td>(optional)
Please note:
This extension indicates for how long the private key belonging to the certificate may be used. As the keypair and certificate of the timestamping unit are updated on an annual basis, the time is set to 1 year plus 2 months buffer time.
The inclusion of this extension is recommended within ETSI EN 319 422.
However, as the support of this extension is not widespread amongst client- and CA-software it is (or may be) omitted.</td></tr>
</table>

4.4.3 NCPplus: Advanced Electronic Seal Certificates issued by SwissSign NCPplus Advanced Seal ICA 2023 - 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	• RSA-PSS • SHA512 • MGF1		SHA512 with RSA-PSS and MGF1
Issuer Distinguished Name (IDN)	CN= SwissSign NCPplus Advanced Seal ICA 2023 - 1 O = SwissSign AG organizationIdentifier= NTRCH-CHE-109.357.012 C = CH		Unique Issuer Distinguished Name of the certificate
Subject Distinguished Name (SDN)			Unique Subject Distinguished Name of the certificate
	Common Name (CN)	Subject's (organization) name as stated in certificate application.	(mandatory)
	OrganizationUnit (OU)	Organization unit belonging to the subject's organization	(optional)
	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)
	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
Public Key	Type: rsaEncryption (OID: 1.2.840.113549.1.1.1)		
	Modulus, length: 3072 bit or higher		
	Public exponent		
Authority Key Identifier (AKI)	58C8B8EFA8C3BB78BA3C10C4495242CDC43B5BAD		(mandatory) Equal to SKI of ICA
Subject Key Identifier (SKI)	*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			Not present

Subject Alternative Name			not allowed
Certificate Policies	Policy OID: 0.4.0.2042.1.2 (ETSI NCP+) Policy OID: 2.16.756.1.89.2.1.23 (SwissSign NCP+) CPSURI: https://repository.swisssign.com/SwissSign_CPS_Signing.pdf		(mandatory)
CRL Distribution Points	http://crl.swisssign.ch/cdp-ea52960d-d5d1-445d-b80a-a965e4b3eb9d		URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://aia.swisssign.ch/air-e738bc4e-8d63-4c6a-a157-3f7356259d06	(mandatory)
	OCSP	http://ocsp.swisssign.ch/sign/ocs-cbd4cafa-e50a-4c88-a0ec-06cdc4e76fb1	(mandatory)

5. OCSP

5.1 OCSP Response 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 OR • RSA-PSS • SHA512 • MGF1	(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.

Reasoning: After revocation or expiration of the last leaf certificate issued under a CA a “lastCRL” is issued that contains the serial numbers of all revoked certificates, then the Issuing CA itself is revoked. Therefore, status information is provided via the lastCRL and the continuation of the OCSP service under a revoked CA does not provide an added value.

5.2 OCSP Responder Certificate

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number			Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption OR • RSA-PSS • SHA512 • MGF1		• sha256WithRSAEncryption used within old hierarchy • SHA512 with RSA-PSS and MGF1 used within new hierarchy
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		

6. 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 OR • RSA-PSS • SHA512 • MGF1	Hash method and the signature algorithm used to sign the CRL pursuant to RFC 5280. • sha256WithRSAEncryption used within old hierarchy SHA512 with RSA-PSS and MGF1 used within new hierarchy
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

7. 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 v1.3.1 (2021-05) 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 v2.3.1 (2021-05)): 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-l-qscd – Certificate Policy for Regulated Seal certificates, published under: https://repository.swisssign.com
[16] SwissSign CP NCP+ – Certificate Policy for Advanced Seal certificates, published under: https://repository.swisssign.com