

SwissSign eIDAS certificate profiles

Certificate, CRL and OCSP Profiles for eIDAS Signing certificates

Document Type: Certificate, CRL and OCSP Profiles
OID: n/a
Author: Information Security and Compliance
Owner: CEO
Applicability: Global
Copyright: Attribution-NoDerivs (CC-BY-ND) 4.0
Version: 4
Issue date: 02.10.2025
Obsoletes: v3.0, 28.02.2025

Disclaimer: The electronic version of this document and all its stipulations are considered binding if saved in Adobe PDF Format. Additionally, a version in Markdown may be provided for convenience. In case of discrepancies, the PDF version prevails.

Table of Contents

1. INTRODUCTION	2
1.1 Terms and abbreviations	2
1.2 Document name and identification	2
1.2.1 Revisions	2
2. General profiles	2
2.1 Root CA	2
2.2 Issuing CA	3
2.3 Algorithm object identifiers	4
2.4 Key sizes and signature parameters	4
3. Certificate Profiles of the SwissSign Signature Services Root 2023 - 2 PKI	5
3.1 Root CA	5
3.1.1 SwissSign RSA eIDAS Qualified Services Root 2023 - 2	5
3.1.2 SwissSign ECC eIDAS Qualified Services Root 2023 – 2	5
3.2 Issuing CAs	6
3.2.1 SwissSign RSA eIDAS Qualified Services ICA 2023 - 1	6
3.2.2 SwissSign ECC eIDAS Qualified Services ICA 2023 - 1	7
3.3 End-entity certificates	7
3.3.1 QCP-n-qscd eIDAS: eIDAS Qualified Certificate for Electronic Signature issued by SwissSign RSA eIDAS Qualified Services ICA 2023 - 1	7
3.3.2 QCP-n-qscd eIDAS: eIDAS Qualified Certificate for Electronic Signature issued by SwissSign ECC eIDAS Qualified Services ICA 2023 - 1	8
3.3.3 QCP-n eIDAS: eIDAS Qualified Certificate for Electronic Signature issued by SwissSign RSA eIDAS Qualified Services ICA 2023 - 1	9
3.3.4 QCP-n eIDAS: eIDAS Qualified Certificate for Electronic Signature issued by SwissSign ECC eIDAS Qualified Services ICA 2023 - 1	10
4. OCSP Profile	11
4.1 OCSP Response Profile	11
4.2 OCSP Responder Certificate	12
4.2.1 OCSP Responder Certificate for eIDAS Qualified Certificates for Electronic Signature issued by SwissSign RSA eIDAS Qualified Services ICA 2023 - 1	12
4.2.2 OCSP Responder Certificate for eIDAS Qualified Certificates for Electronic Signature issued by SwissSign ECC eIDAS Qualified Services ICA 2023 - 1	12
5. CRL Profile	13
6. References	13

1. INTRODUCTION

This document describes profiles of the eIDAS Signing certificates issued by the SwissSign Issuing CAs as described in the eIDAS CPS [4] as well as OCSP responses and CRL profiles related to these certificates.

This document complements eIDAS Certificate Policies [1] and [2] and eIDAS Certification Practice Statement [4].

SwissSign PKI hierarchy description can be found from chapter 1.1 from eIDAS CPS [4].

1.1 Terms and abbreviations

Refer to the TSPS [5].

1.2 Document name and identification

This document is named "SwissSign eIDAS certificate profiles - Certificate, CRL and OCSP Profiles for eIDAS Signing certificates" as indicated on the cover page of this document.

1.2.1 Revisions

Version	Date	Author	Comment
1.0	16.03.2024	Adrian Mueller & Luis Peñalosa	Initial version
2.0	21.06.2024	Luis Peñalosa	Nationality changes
3.0	28.02.2025	Luis Peñalosa & Adrian Mueller	Update revocationReason for leaf certificates at OCSP Response Profile, add value(s) in Subject Key Identifier at OCSP Responder Certificate, update Value of Serial Number at End-entity certificates
4.0	02.10.2025	Roman Fischer	Conversion to markdown, use automation for certificates and profiles

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	1 Root with RSASSA-PSS, 1 Root with sha512ECDSA based on NIST curve secp512r1	
Issuer Distinguished name		Unique issuer distinguished name of the certificate, for the Root CA this field shall be identical with the Subject Distinguished Name

Field/Extension	Value(s)	Comment
Subject Distinguished name	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)	Unique subject distinguished name of the certificate
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	1 ICA with RSASSA-PSS, 1 ICA with sha512ECDSA based on NIST curve secp512r1	
Issuer Distinguished name		Unique issuer (i.e. Root CA) distinguished name of the certificate
Subject Distinguished name	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) = Unique Identification Number of the Organization, e.g. NTR, VAT, etc. (optional), Country (C) = Country code in accordance with ISO 3166 (mandatory)	Unique subject distinguished name of the certificate
Valid from		Start of certificate validity
Valid to		End of certificate validity

Field/Extension	Value(s)	Comment
Basic Constraints	CA: TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier		(mandatory)
Authority Key Identifier		(optional)
Extended Key Usage		(optional)
Name Constraints		(optional)
Certificate Policies	Policy OID: <OID referencing SwissSign specific policy>, CPSURI: <URI pointing to CPS>, Policy OID: <OID according to ETSI EN 319 411-2 QCP-n-qscd and QCP-n >	(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
RSASSA-PSS / RSA-PSS	1.2.840.113549.1.1.10	Signature algorithm with Probabilistic Signature Scheme using an RSA key pair
MGF1	1.2.840.113549.1.1.8	Mask Generation Function used with RSASSA-PSS
rsaEncryption	1.2.840.113549.1.1.1	Public Key is of type RSA.
ANSI x9.62 ECDSA with SHA512	1.2.840.10045.4.3.4	Signature algorithm using an elliptic curve
secp521r1 / NIST P-521 / prime521v1	1.3.132.0.35	curve used with ecDSA
ecPublicKey (ANSI X9.62 public key type)	1.2.840.10045.2.1	Public Key is of type elliptic curve.
SHA512	2.16.840.1.101.3.4.2.3	Hash-algorithm used with Mask Generation Function
SHA384	2.16.840.1.101.3.4.2.2	Hash-algorithm used with Mask Generation Function

2.4 Key sizes and signature parameters

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 contains an RSA public key whose modulus has a size of 4096 bit or larger.
- All signatures are applied using the Mask Generation Function MGF1.
- The end-user and Issuing CA applied signatures are applied using SHA-384 or a stronger SHA2 hash algorithm.
- The CAs use a SHA-512 hash algorithm.

Elliptic curves:

- All leaf and Issuing CA certificates contain an ECC public key with a size of 521 bit. The applied signatures are ECDSA with SHA512.

- The CA certificates contain an ECC public key with a size of 521 bit and applies signatures according to ECDSA with SHA512. Please note: The elliptic curves used are the NIST curves.

3. Certificate Profiles of the SwissSign Signature Services Root 2023 - 2 PKI

The following certificate profiles are compiled in accordance with ITU-T X.509 version 3, IETF RFC 5280 [11], clause 6.6 of ETSI EN 319 411-1/2 [6]/[7].

Please note: Two hierarchies are set up:

- RSASSA-PSS based
- ECC based (with NIST curves) in particular P-512 (secp512r1)

Therefore, two Root CA certificates and two Issuing CA certificates are implemented.

3.1 Root CA

3.1.1 SwissSign RSA eIDAS Qualified Services Root 2023 - 2

This list has the format "Field/Extension": "Values" (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 258DC3784F3E3C720D7E73756DAE0F54B81E05B8 (Unique serial number of the certificate)
- SignatureAlgorithm: RSASSA-PSS (Hash: SHA512, MGF: MGF1 with SHA512)
- Issuer Distinguished name: CN = SwissSign RSA eIDAS Qualified Services Root 2023 - 2, O = SwissSign GmbH, organizationIdentifier = VATAT-U79130637, C = AT (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA eIDAS Qualified Services Root 2023 - 2, O = SwissSign GmbH, organizationIdentifier = VATAT-U79130637, C = AT (Unique subject distinguished name of the certificate)
- Valid from: 15 Mar 2023 09:27:29 UTC (Start of certificate validity)
- Valid to: 15 Mar 2048 09:27:29 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 94C54B8F87B50D855C51BF65EEA0D65ADB1E6620
- Authority Key Identifier: 94C54B8F87B50D855C51BF65EEA0D65ADB1E6620
- 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: 7ED5334E9034ABC483FE17B8C57B2F2E5977556C
- SHA256 Fingerprint: 7236D23857AD8990617816FB3D0227165F73849C4F134D7D324E8C87B49DE23B

3.1.2 SwissSign ECC eIDAS Qualified Services Root 2023 – 2

This list has the format "Field/Extension": "Values" (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 118D7150F2B563E3B363074C43BFA6C03C2C604 (Unique serial number of the certificate)
- SignatureAlgorithm: sha512ECDSA using secp521r1

- Issuer Distinguished name: CN = SwissSign ECC eIDAS Qualified Services Root 2023 - 2, O = SwissSign GmbH, organizationIdentifier = VATAT-U79130637, C = AT (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign ECC eIDAS Qualified Services Root 2023 - 2, O = SwissSign GmbH, organizationIdentifier = VATAT-U79130637, C = AT (Unique subject distinguished name of the certificate)
- Valid from: 15 Mar 2023 09:01:46 UTC (Start of certificate validity)
- Valid to: 15 Mar 2048 09:01:46 UTC (End of certificate validity)
- SubjectPublicKeyInfo: id-ecPublicKey (OID: 1.2.840.10045.2.1), ID-ECPUBLICKEY key (length 521 bit)
- Basic Constraints: CA:True (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 1B543F30D8E9407B09346F3657B00F1493D0C375
- Authority Key Identifier: 1B543F30D8E9407B09346F3657B00F1493D0C375
- 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: 1079FB49339F7E33CED53162F549FDB9A67E2EED
- SHA256 Fingerprint: 43B7DB57AE5189E63146A9B1193D9CB5A9336C419580D411CD01903C9A805FCA

3.2 Issuing CAs

3.2.1 SwissSign RSA eIDAS Qualified Services ICA 2023 - 1

This list has the format "Field/Extension": "Values" (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: D267A02A606856B43248EA87ECCFC2AE486A9E6 (Unique serial number of the certificate)
- SignatureAlgorithm: RSASSA-PSS (Hash: SHA512, MGF: MGF1 with SHA512)
- Issuer Distinguished name: CN = SwissSign RSA eIDAS Qualified Services Root 2023 - 2, O = SwissSign GmbH, organizationIdentifier = VATAT-U79130637, C = AT (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA eIDAS Qualified Services ICA 2023 - 1, O = SwissSign GmbH, organizationIdentifier = VATAT-U79130637, C = AT (Unique subject distinguished name of the certificate)
- Valid from: 29 Aug 2023 10:55:15 UTC (Start of certificate validity)
- Valid to: 29 Aug 2038 10:55:15 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True, pathlen:0 (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 91482615CC936DA27EFAA7F697AFA8C3BFD1EA3F
- Authority Key Identifier: 94C54B8F87B50D855C51BF65EEA0D65ADB1E6620
- Extended Key Usage: (not included in this Issuing CA certificate)
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
 - 2.16.756.1.89.3.1.1 (SwissSign CP QCP-n-qscd QES eIDAS)
 - 2.16.756.1.89.3.1.2 (SwissSign CP QCP-n AES eIDAS), CPSURI: https://repository.swissign.com/SwissSign_CPS_
- CRL Distribution Points:
 - <http://crl.swissign.ch/cdp-ff3b4d05-4a55-4db2-a8fa-234f50779af3>
- Authority Information Access:
 - caIssuers: <http://aia.swissign.ch/air-1518d2c9-5d91-40f1-943d-95d39b44adc5>

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 2DF79ABDEF76F38A13954E0D025AF591B7C5B2E4
- SHA256 Fingerprint: 088A590DD650596FDB99770550835AB5C2763283688BC9FB61380C4C77E01BDE

3.2.2 SwissSign ECC eIDAS Qualified Services ICA 2023 - 1

(Currently ECC certificates are not part of SwissSign's eIDAS signing service offering and are therefore no end-user certificates are issued.)

This list has the format "Field/Extension": "Values" (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 34E1FDA5C900B84616CE3EC850DA9AF6A996F022 (Unique serial number of the certificate)
- SignatureAlgorithm: sha512ECDSA using secp521r1
- Issuer Distinguished name: CN = SwissSign ECC eIDAS Qualified Services Root 2023 - 2, O = SwissSign GmbH, organizationIdentifier = VATAT-U79130637, C = AT (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign ECC eIDAS Qualified Services ICA 2023 - 1, O = SwissSign GmbH, organizationIdentifier = VATAT-U79130637, C = AT (Unique subject distinguished name of the certificate)
- Valid from: 29 Aug 2023 11:58:42 UTC (Start of certificate validity)
- Valid to: 29 Aug 2038 11:58:42 UTC (End of certificate validity)
- SubjectPublicKeyInfo: id-ecPublicKey (OID: 1.2.840.10045.2.1), ID-ECPUBLICKEY key (length 521 bit)
- Basic Constraints: CA:True, pathlen:0 (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 52BD7CC7C35EB1DF979104BAD60486EBDB9CE80B
- Authority Key Identifier: 1B543F30D8E9407B09346F3657B00F1493D0C375
- Extended Key Usage: (not included in this Issuing CA certificate)
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
 - 2.16.756.1.89.3.1.1 (SwissSign CP QCP-n-qscd QES eIDAS)
 - 2.16.756.1.89.3.1.2 (SwissSign CP QCP-n AES eIDAS), CPSURI: https://repository.swissign.com/SwissSign_CPS_
- CRL Distribution Points:
 - <http://crl.swissign.ch/cdp-50b0537e-871c-4200-8b3e-85e9df52133f>
- Authority Information Access:
 - caIssuers: <http://aia.swissign.ch/air-41f3a48c-9496-4d92-a22d-cfe10afe4a9f>

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: C69B9F5FBC7DBF382FC57B4B51B4326B2BFAB3EE
- SHA256 Fingerprint: 6C19512DAF67F7FBA669C6590702CCA4BBC95927D442B007F83E43FCF26E4A55

3.3 End-entity certificates

3.3.1 QCP-n-qscd eIDAS: eIDAS Qualified Certificate for Electronic Signature issued by SwissSign RSA eIDAS Qualified Services ICA 2023 - 1

This list has the format "Field/Extension": "Values" (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: (The certificate serial number is unique within the range of the Issuing CA and contains randomness.)
- SignatureAlgorithm: RSASSA-PSS (Hash: SHA384, MGF: MGF1)
- Issuer Distinguished name: CN= SwissSign RSA eIDAS Qualified Services ICA 2023 - 1, O= SwissSign GmbH, organizationIdentifier= VATAT-U79130637, C= AT (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: (Unique subject distinguished name of the certificate)
 - Common Name (CN): GivenName Surname (mandatory, Format: UTF-8)

- GivenName: Subject's Given Name as stated in certificate application. (mandatory, Format: UTF-8)
- Surname: Subject's Surname Name as stated in certificate application. (mandatory, Format: UTF-8)
- SerialNumber: Unique value assigned by the TSP to assure that the Subject DN is unique for each subject/certificate holder. (mandatory, Format: PrintableString)
- Country (C): Country code in accordance with ISO 3166, Country contains the nationality of the subject indicated in the identification document used for registration. (mandatory, Format: PrintableString)
- Valid from: Creation date (Start of certificate validity.)
- Valid to: Creation date + 10 minutes, (End of certificate validity.)
- Authority Key Identifier: 91482615cc936da27efaa7f697afa8c3bfd1ea3f (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 included)
- Subject Alternative Name: (not allowed)
- Certificate Policies: Policy OID: 0.4.0.194112.1.2 (QCP-n-qscd), Policy OID: 2.16.756.1.89.3.1.1, CPSURI: https://repository.swisssign.com/SwissSign_CPS_eIDAS_Signing.pdf (mandatory, The policy OID QCP-n-qscd is defined and described in ETSI EN 319 411-2.)
- CRL Distribution Points: <http://crl.swisssign.ch/cdp-5450dcc8-a133-4e80-8dc9-28443562cee3> (URLs of the CRL Distribution points, LDAP and/or HTTP)
- Authority Information Access:
 - caIssuers: <http://aia.swisssign.ch/air-8c9d6baa-1e66-43f9-a962-8153c92d58ca> (mandatory)
 - OCSP: <http://ocsp.swisssign.ch/sign/ocs-b6767b25-6f3c-46e2-bbaa-d154efa419e4> (mandatory)
- QC Statement: (The following QC statements shall be set: Secure Signature Creation Device Qualified Certificate, Certificate type for electronic signatures (QES), Under which legislation the qualified certificates was issued (i.e. valid in the EU/EEA area).)
 - 0.4.0.1862.1.1 (EU qualified certificate)
 - 0.4.0.1862.1.4 (Secure Signature Creation Device Qualified Certificate)
 - 0.4.0.1862.1.5 (PKI Disclosure Statements, PDS=<https://repository.swisssign.com/SwissSign-PDS.pdf>, language: en)
 - 0.4.0.1862.1.6 (Certificate Type, QC Type=0.4.0.1862.1.6.1 (electronic signature))
- Extension for short-term certificate "id-etsi-ext-valassured-ST-certs" (OID: 0.4.0.194121.2.1): NULL value (Optional, Syntax according to ETSI EN 319 412-1, section 5.2.3)

3.3.2 QCP-n-qscd eIDAS: eIDAS Qualified Certificate for Electronic Signature issued by SwissSign ECC eIDAS Qualified Services ICA 2023 - 1

(Currently ECC certificates are not part of SwissSign's eIDAS signing service offering and are therefore not issued.)

This list has the format "Field/Extension": "Values" (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: (The certificate serial number is unique within the range of the Issuing CA and contains randomness.)
- SignatureAlgorithm: sha256ECDSA using secp512r1
- Issuer Distinguished name: CN= SwissSign ECC eIDAS Qualified Services ICA 2023 - 1, O= SwissSign GmbH, organizationIdentifier= VATAT-U79130637, C= AT (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: (Unique subject distinguished name of the certificate)
 - Common Name (CN): GivenName Surname (mandatory, Format: UTF-8)
 - GivenName: Subject's Given Name as stated in certificate application. (mandatory, Format: UTF-8)
 - Surname: Subject's Surname Name as stated in certificate application. (mandatory, Format: UTF-8)
 - SerialNumber: Unique value assigned by the TSP to assure that the Subject DN is unique for each subject/certificate holder. (mandatory, Format: PrintableString)
 - Country (C): Country code in accordance with ISO 3166, Country contains the nationality of the subject indicated in the identification document used for registration.(mandatory, Format: PrintableString)

- Valid from: Creation date (Start of certificate validity.)
- Valid to: Creation date + 10 minutes, (End of certificate validity.)
- Authority Key Identifier: 52bd7cc7c35eb1df979104bad60486ebdb9ce80b (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 included)
- Subject Alternative Name: (not allowed)
- Certificate Policies: Policy OID: 0.4.0.194112.1.2 (QCP-n-qscd), Policy OID: 2.16.756.1.89.3.1.1, CPSURI: https://repository.swisssign.com/SwissSign_CPS_eIDAS_Signing.pdf (mandatory, The policy OID QCP-n-qscd is defined and described in ETSI EN 319 411-2.)
- CRL Distribution Points: <http://crl.swisssign.ch/cdp-411b2d10-80d2-47f7-bf58-d54d72600f82> (URLs of the CRL Distribution points, LDAP and/or HTTP)
- Authority Information Access:
 - calssuers: <http://aia.swisssign.ch/air-46ead75e-dfe6-41bf-83c6-076d00d70c42> (mandatory)
 - OCSP: <http://ocsp.swisssign.ch/sign/ocs-b6767b25-6f3c-46e2-bbaa-d154efa419e4> (mandatory)
- QC Statement: (The following QC statements shall be set: Secure Signature Creation Device Qualified Certificate, Certificate type for electronic signatures (QES), Under which legislation the qualified certificates was issued (i.e. valid in the EU/EEA area).)
 - 0.4.0.1862.1.1 (EU qualified certificate)
 - 0.4.0.1862.1.4 (Secure Signature Creation Device Qualified Certificate)
 - 0.4.0.1862.1.5 (PKI Disclosure Statements, PDS=<https://repository.swisssign.com/SwissSign-PDS.pdf>, language: en)
 - 0.4.0.1862.1.6 (Certificate Type, QC Type=0.4.0.1862.1.6.1 (electronic signature)
- Extension for short-term certificate “id- etsi-ext-valassured-ST-certs” (OID: 0.4.0.194121.2.1): NULL value (Optional, Syntax according to ETSI EN 319 412-1, section 5.2.3)

3.3.3 QCP-n eIDAS: eIDAS Qualified Certificate for Electronic Signature issued by SwissSign RSA eIDAS Qualified Services ICA 2023 - 1

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: (The certificate serial number is unique within the range of the Issuing CA and contains randomness.)
- SignatureAlgorithm: RSASSA-PSS (Hash: SHA384, MGF: MGF1)
- Issuer Distinguished name: CN= SwissSign RSA eIDAS Qualified Services ICA 2023 - 1, O= SwissSign GmbH, organizationIdentifier= VATAT-U79130637, C= AT (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: (Unique subject distinguished name of the certificate)
 - Common Name (CN): GivenName Surname (mandatory, Format: UTF-8)
 - GivenName: Subject’s Given Name as stated in certificate application. (mandatory, Format: UTF-8)
 - Surname: Subject’s Surname Name as stated in certificate application. (mandatory, Format: UTF-8)
 - SerialNumber: Unique value assigned by the TSP to assure that the Subject DN is unique for each subject/certificate holder. (mandatory, Format: PrintableString)
 - Country (C): Country code in accordance with ISO 3166, Country contains the nationality of the subject indicated in the identification document for registration. (mandatory, Format: PrintableString)
- Valid from: Creation date (Start of certificate validity.)
- Valid to: Creation date + 10 minutes, (End of certificate validity.)
- Authority Key Identifier: 91482615cc936da27efaa7f697afa8c3bfd1ea3f (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 included)
- Subject Alternative Name: (not allowed)
- Certificate Policies: (mandatory, The policy OID QCP-n is defined and described in ETSI EN 319 411-2.)

- Policy OID: 0.4.0.194112.1.0 (ETSI EN 319 411, QCP-n)
- Policy OID: 0.4.0.2042.1.2 (NCP+)
- Policy OID: 2.16.756.1.89.3.1.2
- CPSURI: https://repository.swisssign.com/SwissSign_CPS_eIDAS_Signing.pdf
- CRL Distribution Points: <http://crl.swisssign.ch/cdp-5450dcc8-a133-4e80-8dc9-28443562cee3> (URLs of the CRL Distribution points, LDAP and/or HTTP)
- Authority Information Access:
 - calssuers: <http://aia.swisssign.ch/air-8c9d6baa-1e66-43f9-a962-8153c92d58ca> (mandatory)
 - OCSP: <http://ocsp.swisssign.ch/sign/ocs-b6767b25-6f3c-46e2-bbaa-d154efa419e4> (mandatory)
- QC Statement: (The following QC statements are set: Certificate type for electronic signatures, Under which legislation the qualified certificates was issued (i.e. valid in the EU/EEA area).)
 - 0.4.0.1862.1.1 (EU qualified certificate)
 - 0.4.0.1862.1.5 (PKI Disclosure Statements, PDS=<https://repository.swisssign.com/SwissSign-PDS.pdf>, language: en)
 - 0.4.0.1862.1.6 (Certificate Type, QC Type=0.4.0.1862.1.6.1, electronic signature)
- Extension for short-term certificate “id- etsi-ext-valassured-ST-certs” (OID: 0.4.0.194121.2.1): NULL value (Optional, Syntax according to ETSI EN 319 412-1, section 5.2.3)

3.3.4 QCP-n eIDAS: eIDAS Qualified Certificate for Electronic Signature issued by SwissSign ECC eIDAS Qualified Services ICA 2023 - 1

(Currently ECC certificates are not part of SwissSign’s signing service offering and are therefore not issued.)

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: (The certificate serial number is unique within the range of the Issuing CA and contains randomness.)
- SignatureAlgorithm: sha256ECDSA using secp512r1
- Issuer Distinguished name: CN= SwissSign ECC eIDAS Qualified Services ICA 2023 - 1, O= SwissSign GmbH, organizationIdentifier= VATAT-U79130637, C= AT (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: (Unique subject distinguished name of the certificate)
 - Common Name (CN): GivenName Surname (mandatory, Format: UTF-8)
 - GivenName: Subject’s Given Name as stated in certificate application. (mandatory, Format: UTF-8)
 - Surname: Subject’s Surname Name as stated in certificate application. (mandatory, Format: UTF-8)
 - SerialNumber: Unique value assigned by the TSP to assure that the Subject DN is unique for each subject/certificate holder. (mandatory, Format: PrintableString)
 - Country (C): Country code in accordance with ISO 3166, Country contains the nationality of the subject indicated in the identification document used for registration. (mandatory, Format: PrintableString)
- Valid from: Creation date (Start of certificate validity.)
- Valid to: Creation date + 10 minutes, (End of certificate validity.)
- Authority Key Identifier: 52bd7cc7c35eb1df979104bad60486ebdb9ce80b (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 included)
- Subject Alternative Name: (not allowed)
- Certificate Policies:
 - Policy OID: 0.4.0.194112.1.0 (ETSI EN 319 411, QCP-n)
 - Policy OID: 0.4.0.2042.1.2 (NCP+)
 - Policy OID: 2.16.756.1.89.3.1.2
 - CPSURI: https://repository.swisssign.com/SwissSign_CPS_eIDAS_Signing.pdf (mandatory, The policy OID QCP-n is defined and described in ETSI EN 319 411-2.)
- CRL Distribution Points: <http://crl.swisssign.ch/cdp-411b2d10-80d2-47f7-bf58-d54d72600f82> (URLs of the CRL

- Distribution points, LDAP and/or HTTP)
- Authority Information Access:
 - calssuers: <http://aia.swisssign.ch/air-46ead75e-dfe6-41bf-83c6-076d00d70c42> (mandatory)
 - OCSP: <http://ocsp.swisssign.ch/sign/ocs-b6767b25-6f3c-46e2-bbaa-d154efa419e4> (mandatory)
- QC Statement: (The following QC statements are set:, Certificate type for electronic signatures, Under which legislation the qualified certificates was issued (i.e. valid in the EU/EEA area).)
 - 0.4.0.1862.1.1 (EU qualified certificate)
 - 0.4.0.1862.1.5 (PKI Disclosure Statements, PDS=<https://repository.swisssign.com/SwissSign-PDS.pdf>, language: en)
 - 0.4.0.1862.1.6 (Certificate Type, QC Type=0.4.0.1862.1.6.1, electronic signature)
- Extension for short-term certificate “id- etsi-ext-valassured-ST-certs” (OID: 0.4.0.194121.2.1): NULL value (Optional, Syntax according to ETSI EN 319 412-1, section 5.2.3)

4. OCSP Profile

4.1 OCSP Response Profile

SwissSign OCSP v1 is built according to RFC 6960 [14].

This list has the format “Field/Extension”: “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 or (optional) January 1, 1970 for non-issued certificates according to chapter 2.2 of RFC6960)
- revocationReason: (For the Issuing CA this extension may be present. For leaf certificates the revocationReason shall be specified as in RFC 5280. For serial numbers of non-issued certificates the the reasonCode is set to certificateHold (6) as defined in chapter 2.2 of RFC6960.)
- 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)
- Extended Revoked Definition: (Extended revoked extension according to chapter 2.2 and 4.4.8 of RFC6960, optional)
- Signature Algorithm: (mandatory)
 - RSASSA-PSS
 - sha512ECDSA using secp512r1
- 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.

4.2 OCSP Responder Certificate

4.2.1 OCSP Responder Certificate for eIDAS Qualified Certificates for Electronic Signature issued by SwissSign RSA eIDAS Qualified Services ICA 2023 - 1

(Currently ECC certificates are not part of SwissSign's signing service offering and are therefore not issued.)

This list has the format "Field/Extension": "Values" (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: (Unique serial number of the certificate)
- SignatureAlgorithm: RSASSA-PSS (Hash: SHA384, MGF: MGF1)
- Issuer Distinguished name: CN= SwissSign RSA eIDAS Qualified Services ICA 2023 - 1, O= SwissSign GmbH, organizationIdentifier= VATAT-U79130637, C= AT (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: (Unique subject distinguished name of the OCSP Signer certificate.)
 - CommonName: (The CN should include the string "OCSP" and the reference to the Issuer. The CN may contain an ID unique to the specific OCSP responder certificate, e.g.: "OCSP" (MANDATORY), + "Responder" (optional) , + <Sequence number> (optional, e.g. "2022-1"), + <reference to CA that issued the OCSP responder certificate> (MANDATORY))
 - OrganizationName (O): SwissSign AG
 - Country (C): CH
- Valid from: (Start of certificate validity.)
- Valid to: (End of certificate validity, maximum "Valid from" date + 2 years)
- Key Usage: digitalSignature (mandatory, critical)
- Subject Key Identifier: SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2 (mandatory, SHA1 hash of the subject's public key as specified in RFC5280 [11].)
- Authority Key Identifier: 91482615cc936da27efaa7f697afa8c3bfd1ea3f (mandatory, SHA1 hash of the issuing CA's public key as specified in RFC5280 [11].)
- Extended Key Usage: id-kp-ocspSigning (mandatory)
- Certificate Policies: Not included in this certificate
- ocspNoCheck: null value (mandatory)
- CRL Distribution Points: (Not included in this certificate)
- Authority Information Access: (Not included in this certificate)

4.2.2 OCSP Responder Certificate for eIDAS Qualified Certificates for Electronic Signature issued by SwissSign ECC eIDAS Qualified Services ICA 2023 - 1

This list has the format "Field/Extension": "Values" (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: (Unique serial number of the certificate)
- SignatureAlgorithm: sha512ECDSA (using secp512r1)
- Issuer Distinguished name: CN= SwissSign RSA eIDAS Qualified Services ICA 2023 - 1, O= SwissSign GmbH, organizationIdentifier= VATAT-U79130637, C= AT (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: (Unique subject distinguished name of the OCSP Signer certificate.)
 - CommonName: (The CN should include the string "OCSP" and the reference to the Issuer. The CN may contain an ID unique to the specific OCSP responder certificate, e.g.: "OCSP" (MANDATORY), + "Responder" (optional), + <Sequence number> (optional, e.g. "2022-1"), + <reference to CA that issued the OCSP responder certificate> (MANDATORY))
 - OrganizationName (O): SwissSign AG
 - Country (C): CH
- Valid from: (Start of certificate validity.)
- Valid to: (End of certificate validity, maximum "Valid from" date + 2 years)

- Key Usage: digitalSignature (mandatory, critical)
- Subject Key Identifier: (mandatory, SHA1 hash of the subject's public key as specified in RFC5280 [11].)
- Authority Key Identifier: 52bd7cc7c35eb1df979104bad60486ebdb9ce80b (mandatory, SHA1 hash of the issuing CA's public key as specified in RFC5280 [11].)
- Extended Key Usage: id-kp-ocspSigning (mandatory)
- Certificate Policies: Not included in this certificate
- ocspNoCheck: null value (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 [11].

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

This list has the format "Field/Extension": "Values" (Comment):

- Version Number: V2 (CRL format version pursuant to X.509.)
- Signature Algorithm: RSASSA-PSS (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)

6. References

[1] SwissSign eIDAS CP QCP-n-qscd RSS - Certificate Policy for eIDAS Qualified Electronic Signature for RSS, published under: <https://repository.swisssign.com>

[2] SwissSign eIDAS CP QCP-n RSS - Certificate Policy for eIDAS Advanced Electronic Signature for RSS, published under: <https://repository.swisssign.com>

[3] SwissSign eIDAS CPR Sign - Certificate, CRL and OCSP Profiles for eIDAS Signing certificates, published under: <https://repository.swisssign.com>

[4] SwissSign CPS eIDAS Sign - Certification Practice Statement for eIDAS Signing certificates, published under: <https://repository.swisssign.com>

[5] SwissSign TSPS - Trust Services Practice Statement, published under: <https://repository.swisssign.com>

- [6] ETSI EN 319 411-1 V1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- [7] ETSI EN 319 411-2 V2.5.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
- [8] eIDAS: Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- [9] SVG: Austrian Federal Law on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Law)
- [10] SVV: Austrian Ordinance on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Ordinance)
- [11] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- [12] RFC 3647 - Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;
- [13] 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;
- [14] RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- [15] ISO 3166 Codes;