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
Classification:	Attribution-NoDerivs (CC-BY-ND) 4.0
Applicability:	Global
Owner:	CEO
Issue Date:	16 February 2024
Version:	1.0
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Version Control

Date	Version	Comment	Author
16.02.2024	1.0	Initial version	Adrian Mueller & Luis Peñalosa

Authorization

Date	Approved by	Approved by	Version
16.02.2024	Michael Günther	Johannes Termin	1.0

Michael Günther
February 16, 2024
Qualified Electronic Signature by SwissID
digital signature

Johannes Termin
Februar 16, 2024
Qualified Electronic Signature by SwissID
digital signature

Table of Contents

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].

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
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	• **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			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> 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 paramaters

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 enduser 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 – 1 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

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	258dc3784f3e3c720d7e73756dae0f54b81e05b8	Unique serial number of the certificate
SignatureAlgorithm	• RSASSA-PSS • SHA512 • MGF1	
Issuer Distinguished name	CN= *SwissSign RSA eIDAS Qualified Services Root 2023 - 2* O= SwissSign GmbH organizationIdentifier= VATAT-U79130637 C= AT	Unique distinguished name of the root certificate Format: PrintableString organizationIdentifier with prefix VATAT contains the Value Added Tax ID, see ETSI EN 319 412-1, chapter 4.1.4 “Legal person semantics identifier”.
Subject Distinguished name	*{Identical to IDN}*	Unique subject distinguished name of the certificate
Valid from	15 March 2023 10:27:29 UTC	Start of certificate validity.
Valid to	15 March 2048 10:27:29 UTC	End of certificate validity.
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 RSA eIDAS Qualified Services Root 2023 – 2 certificate is identified via the following fingerprints:

SHA1 Fingerprint	7ed5334e9034abc483fe17b8c57b2f2e5977556c
SHA256 Fingerprint	7236d23857ad8990617816fb3d0227165f73849c4f134d7d324e8c87b49de23b

3.1.2 SwissSign ECC eIDAS Qualified Services Root 2023 – 2

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

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	0118d7150f2b563e3b363074c43bfa6c03c2c604	Unique serial number of the certificate
SignatureAlgorithm	sha512ECDSA using secp512r1	
Issuer Distinguished name	CN= *SwissSign ECC eIDAS Qualified Services Root 2023 - 2* O= SwissSign GmbH organizationIdentifier= VATAT-U79130637 C= AT	Unique distinguished name of the root certificate Format: PrintableString organizationIdentifier with prefix VATAT contains the Value Added Tax ID, see ETSI EN 319 412-1, chapter 4.1.4 "Legal person semantics identifier".
Subject Distinguished name	*{Identical to IDN}*	Unique subject distinguished name of the certificate
Valid from	15 March 2023 10:01:46	Start of certificate validity.
Valid to	15 March 2048 10:01:46	End of certificate validity.
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 ECC eIDAS Qualified Services Root 2023 – 2 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

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	0d267a02a606856b43248ea87eccfc2ae486a9e6	Unique serial number of the certificate
SignatureAlgorithm	• RSASSA-PSS • SHA512 • MGF1	
Issuer Distinguished name	**SDN of Root CA**	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 Format: PrintableString
Valid from	29 August 2023 11:55:15	Start of certificate validity.
Valid to	29 August 2038 11:55:15	End of certificate validity.
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	Policy OID for QCP-n-qscd (QES): 2.16.756.1.89.3.1.1 Policy OID for QCP-n (AdES): 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-ff3b4d05-4a55-4db2-a8fa-234f50779af3	
Authority Information Access	Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://aia.swisssign.ch/air-1518d2c9-5d91-40f1-943d-95d39b44adc5	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 Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://XXX.crt

The issuing CA RSA eIDAS Qualified Services ICA 2023 – 1 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 enduser certificates are issued.)

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	34e1fda5c900b84616ce3ec850da9af6a996f022	Unique serial number of the certificate
SignatureAlgorithm	sha512ECDSA using secp512r1	
Issuer Distinguished name	**SDN of Root CA**	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 Format: PrintableString
Valid from	29 August 2023 12:58:42	Start of certificate validity.
Valid to	29 August 2038 12:58:42	End of certificate validity.
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	Policy OID for QCP-n-qscd (QES): 2.16.756.1.89.3.1.1 Policy OID for QCP-n (AdES): 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-50b0537e-871c-4200-8b3e-85e9df52133f	

Authority Information Access	Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.swisssign.ch/air-41f3a48c-9496-4d92-a22d-cfe10afe4a9f	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 Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://XXX.crt

The Issuing CA ECC eIDAS Qualified Services ICA 2023 – 1 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*

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 • SHA384 • 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 number assigned by the TSP.	(mandatory) Format: PrintableString
	Country (C)	Country code in accordance with ISO 3166	(mandatory)

		Country is restricted to “CH”, only Swiss passports or IDs are used for registration.	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	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)		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).
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.)

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 number assigned by the TSP.	(mandatory) Format: PrintableString
	Country (C)	Country code in accordance with ISO 3166 Country is restricted to "CH", only Swiss passports or IDs are 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	caIssuers	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	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)	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).
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*

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 • SHA384 • 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 number assigned by the TSP.	(mandatory) Format: PrintableString
	Country (C)	Country code in accordance with ISO 3166 Country is restricted to "CH", only Swiss passports or IDs are 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: 0.4.0.194112.1.0 (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-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	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)		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).
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.)

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	Unique issuer distinguished name of the certificate

	organizationIdentifier= VATAT-U79130637 C = AT		
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 number assigned by the TSP.	(mandatory) Format: PrintableString
	Country (C)	Country code in accordance with ISO 3166 Country is restricted to "CH", only Swiss passports or IDs are 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	caIssuers	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	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)		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).

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].

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 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 not be present. 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 Definititon		Extended revoked extension according to chapter 2.2 and 4.4.8 of RFC6960 (optional)
Signature Algorithm:	**1.** RSASSA-PSS or **2.** sha512ECDSA using secp512r1	(mandatory)
Certificate		Details of certificate used to sign the response (mandatory)

The OCSP extensions used are specified below:

- Nonce

The ArchiveCutOff extension is not set in the OCSP responses.

4.2 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.)

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number			Unique serial number of the certificate
SignatureAlgorithm	• RSASSA-PSS • SHA384 • 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	CommonName		Unique subject distinguished name of the OCSP Signer certificate. 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	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*

Field/Extension	Value(s)		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	CommonName		Unique subject distinguished name of the OCSP Signer certificate. 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.

Extension Attribute	**Values**	**Comment**
Version Number	V2	CRL format version pursuant to X.509.
Signature Algorithm	**1.** 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 v1.3.1 (2021-05) 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 v2.4.1 (2021-11):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;