SwissSign CPR TLS

Certificate, CRL and OCSP Profiles for TLS 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:	14 June 2021
Version:	1.0
Obsoletes:	n/a
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Version Control

Date	Version	Comment	Author
14.06.2021	1.0	Initial version	Michael Günther

Authorization

Date	Approved by	Approved by	Version
11.06.2021	Michael Günther	Markus Naef	1.0

Michael Günther (Qualified Signature)
Digital unterschrieben von Michael Günther (Qualified Signature)
Datum: 2021.06.11 12:07:45 +02'00'
digital signature

Markus Naef (Qualified Signature)
Digital unterschrieben von Markus Naef (Qualified Signature)
Datum: 2021.06.11 18:28:16 +02'00'
digital signature

Table of Contents

1. Introduction

This document describes profiles of the TLS certificates issued by the SwissSign Issuing CAs as described in the CPS [5] as well as OCSP responses and CRL profiles related to these certificates.

This document complements Certificate Policy [1], [2] and [3] and Certification Practice Statement [5].

SwissSign PKI hierarchy description can be found in chapter 1.1 of CPS [5].

1.1 Terms and abbreviations

Refer to the TSPS [6].

2. General profiles

2.1 Root CA

The Root CA issued **after** the effective date of this CPR and the corresponding CP and CPS **does not** include the following certificate extensions:

- Certificate Policies
- Extendend Key Usage
- Name Constraints
- CRL Distrubution Points
- Authority Information Access

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
Subject Distinguished name		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 issued **before** the effective date of this CPR and the corresponding CP and CPS **does not** include the following certificate extensions:

- Extended Key Usage,
- Name Constraints.

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

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number		Unique serial number of the certificate
SignatureAlgorithm		
Issuer Distinguished name		Unique issuer distinguished name of the certificate
Subject Distinguished name		Unique subject distinguished name of the certificate
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	id-kp-serverAuth, id-kp-clientAuth	(mandatory)
Name Constraints		(optional)
Certificate Policies		(mandatory)
CRL Distribution Points		(mandatory)
Authority Information Access		(mandatory)

2.3 Algorithm object identifiers

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

Algorithm	Object Identifier
SHA1withRSAEncryption	1.2.840.113549.1.1.5 (phase out)
SHA256withRSAEncryption	1.2.840.113549.1.1.11
RSASSA-PSS	1.2.840.113549.1.1.10
rsaEncryption	1.2.840.113549.1.1.4

2.4 Key sizes

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

3. Certificate Profiles of the SwissSign Gold CA - G2 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 [7], clause 7 of BRG [8] and clause 9 of EVCG [9].

3.1 Root CA

3.1.1 SwissSign Gold CA - G2

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	BB401C43F55E4FB0	Unique serial number of the certificate
SignatureAlgorithm	sha1WithRSAEncryption	
Issuer Distinguished name	CN = SwissSign Gold CA - G2 O = SwissSign AG C = CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	CN = SwissSign Gold CA - G2 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	25 Oct 2006 08:30:35 UTC	Start of certificate validity.
Valid to	25 Oct 2036 08:30:35 UTC	End of certificate validity.
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE	
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE	
Extended Key Usage	not included in this Root CA certificate	
Name Constraints	not included in this Root CA certificate	
Certificate Policies	Policy OID: 2.16.756.1.89.1.2.1.1 CPSURI: http://repository.swisssign.com/	
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	D8C5388AB7301B1B6ED47AE645253A6F9F1A2761
SHA256 Fingerprint	62DD0BE9B9F50A163EA0F8E75C053B1ECA57EA55C8688F647C6881F2C8357B95

3.2 Issuing CAs

3.2.1 SwissSign EV Gold CA 2014 – G22

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	008108383CC00775C40C6D736BE3308B		Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name	CN = SwissSign Gold CA - G2 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name	CN = SwissSign EV Gold CA 2014 - G22 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	15 Sep 2014 16:16:37 UTC		Start of certificate validity.
Valid to	04 Mar 2035 16:16:37 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642		
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE		
Extended Key Usage	not included in this Issuing CA certificate		
Name Constraints	not included in this Issuing CA certificate		
Certificate Policies	Policy OID: X509v3 Any Policy CPSURI: http://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf		
CRL Distribution Points	http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE ldap://directory.swisssign.net/CN=5B257B96A465517EB839F3C078665EE83AE7F0EE%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/5B257B96A465517EB839F3C078665EE83AE7F0EE	
	OCSP	http://gold-ev-g2.ocsp.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	67F7E98639ABC6700E04B4D913B759CF5A63C781
SHA256 Fingerprint	A434AAE4E15A5519E9B111FD08EC190FD2ADF13BBE30815C6E1606555CB31450

3.2.2 SwissSign Server Gold CA 2014 - G22

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	00FA1DAAEAC9B3A5FA57980B9974DA31		Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name	CN = SwissSign Gold CA - G2 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name	CN = SwissSign Server Gold CA 2014 - G22 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	19 Sep 2014 14:09:12 UTC		Start of certificate validity.
Valid to	15 Sep 2029 14:09:12 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE		
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE		
Extended Key Usage	not included in this Issuing CA certificate		
Name Constraints	not included in this Issuing CA certificate		
Certificate Policies	Policy OID: 2.16.756.1.89.1.2.1.6 CPSURI: http://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf		
CRL Distribution Points	http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE ldap://directory.swisssign.net/CN=5B257B96A465517EB839F3C078665EE83AE7F0EE%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/5B257B96A465517EB839F3C078665EE83AE7F0EE	
	OCSP	http://ocsp.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE	

The Root CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	ADF2897316718B4525CE370082D9F123D4938F98
SHA256 Fingerprint	561DC78351F5E7EE5A464AC6E58A0D164EF2768F98F02E6EE65501120FCD9C5E

3.2.3 SwissSign Server Gold CA 2008 - G2 (used for CRL & OCSP only)

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	5ECCFA69C03327EF		Unique serial number of the certificate
SignatureAlgorithm	sha1WithRSAEncryption		
Issuer Distinguished name	CN = SwissSign Gold CA - G2 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name	CN = SwissSign Server Gold CA 2008 - G2 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	07 Jul 2008 17:06:03 UTC		Start of certificate validity.
Valid to	07 Jul 2023 17:06:03 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	9776DE0A34E5109A40C4EBD89D5A537B21CC473E		
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE		
Extended Key Usage	not included in this Issuing CA certificate		
Name Constraints	not included in this Issuing CA certificate		
Certificate Policies	Policy OID: 2.16.756.1.89.1.2.1.3 CPSURI: http://repository.swisssign.com/SwissSign-Gold-CP-CPS-R3.pdf		
CRL Distribution Points	http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE ldap://directory.swisssign.net/CN=5B257B96A465517EB839F3C078665EE83AE7F0EE%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/5B257B96A465517EB839F3C078665EE83AE7F0EE	
	OCSP	not included in this Issuing CA certificate	

The Root CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	5C29FEBF626C5DF04A0DCAC8A03DDCE87B161153
SHA256 Fingerprint	FD2991B134CE57BF9CD686878854A5EED5EA64433002452BA40398DA78845CA7

3.3 End-entity certificates

3.3.1 TLS Extended Validation Certificate (EVCP)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	CN = SwissSign EV Gold CA 2014 - G22 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject DN			Unique subject distinguished name of the certificate
	Common Name (CN)	FQDN	(mandatory)
	SerialNumber	Unique Registration Number as stated in certificate application OR “Government Entity”	(mandatory)
	Organisational Unit (OU)	The name of organisational unit as described in subscriber application.	(optional)
	OrganisationName (O)	Subject (organisation) name as stated in certificate application.	(mandatory)
	Street	Name of street as described in the certificate application.	(optional)
	PostalCode	Postal code as described in the certificate application.	(optional)
	LocalityName (L)	Name of the locality as described in the certificate application	(mandatory)
	State (ST)	State or province name or code as described in certificate application and in accordance with ISO 3166-2	(optional)
	Country (C)	Country code in accordance with ISO 3166-1	(mandatory)
	Business Category (BC)	One of the following options: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" as described in certificate application.	(mandatory)
	Jurisdiction-LocalityName (joiL)	Name of the locality as described in the certificate application	(optional)
	Jurisdiction-StateOr-ProvinceName (joiST)	State or province name or code as described in certificate application and in accordance with ISO 3166-2.	(optional)
	Jurisdiction-CountryName (joiC)	Country code in accordance with ISO 3166-1.	(mandatory)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.

Authority Key Identifier	EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature, keyEncipherment		(mandatory)
Extended Key Usage	serverAuth, clientAuth		(mandatory)
Subject Alternative Name	At least subject FQDN		(mandatory) 1 to 200 Alternative DNS names. Wildcard are not allowed
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.3 CPSURI: https://repository.swisssign.com/SwissSign_CPS_TLS.pdf Policy OID: 0.4.0.2042.1.4 (EVCP) Policy OID: 2.23.140.1.1 (CAB-EV)		(mandatory)
CRL Distribution Points	http://crl.swisssign.net/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642 ldap://directory.swisssign.net/CN=EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642,O=SwissSign,C=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		(mandatory) URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642	(mandatory)
	OCSP	http://ocsp.swisssign.net/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642	(mandatory)

3.3.2 TLS Organization Validated Certificates (OVCP)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	CN = SwissSign Server Gold CA 2014 - G22 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject DN			Unique subject distinguished name of the certificate
	Common Name (CN)	FQDN	(mandatory)
	Organisational Unit (OU)	The name of organisational unit as described in subscriber application.	(optional)
	Organisation-Name (O)	Subject (organisation) name as stated in certificate application.	(mandatory)
	LocalityName (L)	Name of the locality of the subject as described in the certificate application	(optional)
	State (ST)	State or province name or code of the subject as described in certificate application and in accordance with ISO 3166-2 [15]	(optional)
	Country (C)	Country code of the Subscriber in accordance with ISO 3166-1 [15]	(mandatory)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature, keyEncipherment		(mandatory)
Extended Key Usage	serverAuth, clientAuth		(mandatory)
Subject Alternative Name	At least subject FQDN		(mandatory) 1 to 200 Alternative DNS names. Wildcard defined as *.FQDN
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.2 CPSUri: https://repository.swisssign.com/SwissSign_CPS_TLS.pdf Policy OID: 0.4.0.2042.1.7 (OVCP) Policy OID: 2.23.140.1.2.2 (CAB-OV)		(mandatory)
CRL Distribution Points	http://crl.swisssign.net/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE ldap://directory.swisssign.net/CN=E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		(mandatory) URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information	calssuers	http://swisssign.net/cgi-bin/authority/download/E7F1E7FD2E53AD11	(mandatory)

Access		E5811A57A4738F127D98C8AE	
	OCSP	http://ocsp.swisssign.net/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE	(mandatory)

4. Certificate Profiles of the SwissSign Silver CA - G2 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 [7], clause 7 of BRG [8] and clause 9 of EVCG [9].

4.1 Root CA

4.1.1 SwissSign Silver CA - G2

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	4F1BD42F54BB2F4B	Unique serial number of the certificate
SignatureAlgorithm	sha1WithRSAEncryption	
Issuer Distinguished name	CN = SwissSign Silver CA - G2 O = SwissSign AG C = CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	CN = SwissSign Silver CA - G2 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	25 Oct 2006 08:32:46 UTC	Start of certificate validity.
Valid to	25 Oct 2036 08:32:46 UTC	End of certificate validity.
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658	
Authority Key Identifier	17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658	
Extended Key Usage	not included in this Root CA certificate	
Name Constraints	not included in this Root CA certificate	
Certificate Policies	Policy OID: 2.16.756.1.89.1.3.1.1 CPSURI: http://repository.swisssign.com/	
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	9BAAE59F56EE21CB435ABE2593DFA7F040D11DCB
SHA256 Fingerprint	BE6C4DA2BBB9BA59B6F3939768374246C3C005993FA98F020D1DEDBED48A81D5

4.2 Issuing CAs

The Issuing CA issued before the effective date of this CPR and the corresponding CP and CPS does not include the certificate extensions Extended Key Usage and Name Constraints.

The Issuing CA issued after the effective date of this CPR and the corresponding CP and CPS includes mandatory the certificate extension Extended Key Usage with id-kp-serverAuth and id-kp-serverAuth. The extension Name Constraints may be included optional.

4.2.1 SwissSign Server Silver CA 2014 - G22

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	006BC318C92ACD1763EB41C86FAF47F7	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	CN = SwissSign Silver CA - G2 O = SwissSign AG C = CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	CN = SwissSign Server Silver CA 2014 - G22 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	19 Sep 2014 20:36:43 UTC	Start of certificate validity.
Valid to	15 Sep 2029 20:36:43 UTC	End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	DBBCBF821859DC69FAF8ABAA834D771D0BB08BD8	
Authority Key Identifier	17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658	
Extended Key Usage	not included in this Issuing CA certificate	
Name Constraints	not included in this Issuing CA certificate	
Certificate Policies	Policy OID: 2.16.756.1.89.1.3.1.6 CPSURI: http://repository.swisssign.com/SwissSign-Silver-CP-CPS.pdf	
CRL Distribution Points	http://crl.swisssign.net/17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658 ldap://directory.swisssign.net/CN=17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	

Authority Information Access	calssuers	http://swisssign.net/cgi-bin/authority/download/17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658	
	OCSP	http://ocsp.swisssign.net/17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	55BE467AA44BF0C15D4BCBD06BDCA24BBA941E13
SHA256 Fingerprint	67F91F26F5BFBFA48738BE0678DD2F8F75F7B80761D5656783CA8B920AAA5659

4.2.2 SwissSign Server Silver CA 2008 - G2 (used for CRL & OCSP only)

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	009D154E306A8BA0CE	Unique serial number of the certificate
SignatureAlgorithm	sha1WithRSAEncryption	
Issuer Distinguished name	CN = SwissSign Silver CA - G2 O = SwissSign AG C = CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	CN = SwissSign Server Silver CA 2008 - G2 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	07 Jul 2008 17:07:16 UTC	Start of certificate validity.
Valid to	07 Jul 2023 17:07:16 UTC	End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	D3446FD9FE7AFCDEAC1C7AA2210D64FA65B0D782	
Authority Key Identifier	17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658	
Extended Key Usage	not included in this Issuing CA certificate	
Name Constraints	not included in this Issuing CA certificate	
Certificate Policies	Policy OID: 2.16.756.1.89.1.3.1.3 CPSURI: http://repository.swisssign.com/SwissSign-Silver-CP-CPS-R3.pdf	
CRL Distribution Points	http://crl.swisssign.net/17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658 ldap://directory.swisssign.net/CN=17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	

Authority Information Access	calssuers	http://swisssign.net/cgi-bin/authority/download/17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658	
	OCSP	not included in this Issuing CA certificate	

The Root CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	95EEF9F8BB003D337C47B0F9A947FFAFE02725C3
SHA256 Fingerprint	06E5DEC31C91D7D33435201D2E22116C207193A874E0A426532A2F69530C86B5

4.3 End-entity certificates

4.3.1 TLS Domain Validated Certificates (DVCP)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	CN = SwissSign Server Silver CA 2014 - G22 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject DN			Unique subject distinguished name of the certificate
	Common Name (CN)	FQDN	(mandatory)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	DBBCBF821859DC69FAF8ABAA834D771D0BB08BD8		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature, keyEncipherment		(mandatory)
Extended Key Usage	serverAuth, clientAuth		(mandatory)
Subject Alternative Name	At least subject FQDN		(mandatory) 1 to 200 Alternative DNS names. Wildcard defined as *.FQDN

Field/Extension	Values		Comment
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.1 CPSUri:https://repository.swisssign.com/SwissSign_CPS_TLS.pdf Policy OID: 0.4.0.2042.1.6 (DVCP) Policy OID: 2.23.140.1.2.1 (CAB-DV)		(mandatory)
CRL Distribution Points	http://crl.swisssign.net/DBBCBF821859DC69FAF8ABAA834D771D0BB08BD8 ldap://directory.swisssign.net/CN=DBBCBF821859DC69FAF8ABAA834D771D0BB08BD8%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		(mandatory) URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/DBBCBF821859DC69FAF8ABAA834D771D0BB08BD8	(mandatory)
	OCSP	http://ocsp.swisssign.net/DBBCBF821859DC69FAF8ABAA834D771D0BB08BD8	(mandatory)

5. OCSP Profile

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		Only present if issuing CA is revoked The extension is set as described in BRG clause 7.3
This Update		Date when the status was queried from database (mandatory)
Next Update		The time at or before which newer information will be available about the status of the certificate. The OCSP response is valid for 3 days. The information provided is updated at least 8 hours prior to the nextUpdate. For Root and Issuing CA: The OCSP response is valid for 3 days. The information provided is updated at least 8 hours prior to the nextUpdate.
Nonce		Value is copied from request if it is included. (optional)
Signature Algorithm:	sha256WithRSAEncryption	(mandatory)
Certificate		Details of certificate used to sign the response (mandatory)

The OCSP extensions used are specified below:

- Nonce

The ArchiveCutOff extension is not set in the OCSP responses.

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		
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	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
Revoked Certificates:		List of the serial numbers and revocation dates 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 Issing CA

The ExpiredCertsOnCRL extension is not set as expired ceritifcates are removed from the CRL.

7. References

[1] SwissSign CP EV - Certificate Policy for Extended Validation Certificates , published under: https://repository.swisssign.com
[2] SwissSign CP OV - Certificate Policy for Organization Validated Certificates, published under: https://repository.swisssign.com
[3] SwissSign CP DV - Certificate Policy for Domain Validated Certificates, published under: https://repository.swisssign.com
[4] SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, published under: https://repository.swisssign.com
[5] SwissSign CPS TLS - Certification Practice Statement for TLS certificates, published under: https://repository.swisssign.com
[6] SwissSign TSPS - Trust Services Practice Statement, published under: https://repository.swisssign.com
[7] ETSI EN 319 411-1 v1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
[8] BRG: current version of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates;
[9] EVCG: current version of the Guidelines For The Issuance And Management Of Extended Validation Certificates;
[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] RFC 6962 – Certificate Transparency;
[15] ISO 3166 Codes;