SwissSign

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
Owner:	CEO
Applicability:	Global
Copyright:	Attribution-NoDerivs (CC-BY-ND) 4.0
Version:	13
Issue date:	18.09.2025
Obsoletes:	v12.0, 07.08.2025

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

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].

1.2 Document name and identification

This document is named “SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates” as indicated on the cover page of this document.

1.2.1 Revisions

Version	Date	Author	Comment
1.0	14.06.2021	Michael Günther	Initial version
2.0	11.10.2021	Michael Günther	Adding TLS Root
3.0	08.11.2021	Michael Günther	Including auditor feedback
4.0	01.07.2022	Adrian Mueller, Michael Günther	Adding new CA (self-signed Root, Cross & ICAs) and end-user profiles
5.0	30.09.2022	Adrian Mueller, Roman Fischer	Updating OCSP certificate profile. Specifying revocation reason codes & SCTs in OCSP response.
6.0	24.07.2023	Adrian Mueller	Removing old CA certificates; adding chapters 2.5 and 2.6; detailing SCT list
7.0	24.10.2023	Adrian Mueller	Correct JurisdictionStateOrProvinceName
8.0	03.04.2024	Raffaela Achermann, Adrian Mueller	Deletion of CA (SwissSign EV Gold CA 2014-G22 and SwissSign Sever Gold CA 2014 -G22)
9.0	23.08.2024	Roman Fischer, Adrian Mueller	Changed disclaimer, Deletion of CA (SwissSign Server Silver CA 2014 - G22)
10.0	15.10.2024	Adrian Mueller	Delete end-entity profiles issued by 2021 ICAs, Delete Issuing and Root CAs from 2021
11.0	29.01.2025	Raffaela Achermann, Roman Fischer	Deletion of root: SwissSign Silver CA - G2, Conversion to Markdown
12.0	07.08.2025	Roman Fischer	Added SubjectPublicKeyInfo, using automation for CA and end-entity certificates
13.0	18.09.2025	Adrian Mueller	Adding optional OCSPmustStaple extension to TLS certificate profiles, clarify OCSP responder certificate details

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

- Extended Key Usage
- Name Constraints
- CRL Distribution 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
SubjectPublicKeyInfo	rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit or higher)	
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 the initial version 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

Field/Extension	Value(s)	Comment
SubjectPublicKeyInfo	rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit or higher)	
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.

2.5 Distinguished Name structure and encoding

Every Distinguished Name (DN) described in this document is a sequence of Relative DNs (RDNs) where every RDN contains exactly one naming attribute. All attributes are encoded according to the requirements set forth in

- X.509,
- RFC5280 and
- the TLS BR, chapter 7

2.6 Pre-certificate and final profiles

For every TLS certificate a pre-certificate is issued, sent to several CT-logs and upon receipt of the Signed Certificate Timestamps (SCTs) the corresponding final certificate is issued. A pre-certificate is issued by the same CA that issues the final certificate. A pre-certificate differs as follows from the final certificate:

- It contains a critical extension “Precertificate Poison” (OID 1.3.6.1.4.1.11129.2.4.3).
- It does not contain the SCT list extension (OID 1.3.6.1.4.1.11129.2.4.2) while the SCT list extension is included in every final end-entity certificate

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

This list has the format “Field/Extension”: “Values” (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)
- 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: 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:
  - 2.16.756.1.89.1.2.1.1 (SwissSign CP/CPS document OID), 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

3.1.2 SwissSign RSA TLS Root CA 2022 - 1 (Self-signed)

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

- Version: Version 3 (Certificate format version)
- Serial Number: 43FA0C5F4E1B801844EFD1B44F351F44F480EDCB (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 08 Jun 2022 11:08:22 UTC (Start of certificate validity)
- Valid to: 08 Jun 2047 11:08:22 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: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- 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: 81340ABE4CCDCECCE77DCC8AD457E245A0775DCE
- SHA256 Fingerprint: 193144F431E0FDDB740717D4DE926A571133884B4360D30E272913CBE660CE41

3.1.3 SwissSign RSA TLS Root CA 2022 - 1 (Cross)

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

- Version: Version 3 (Certificate format version)
- Serial Number: 686F43B4DC404C067E230E3FAFC32B (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 RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 28 Jun 2022 11:27:11 UTC (Start of certificate validity)
- Valid to: 22 Sep 2036 11:27:11 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: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Authority Key Identifier: 5B257B96A465517EB839F3C078665EE83AE7F0EE
- Extended Key Usage: (not included in this Cross certificate)
- Name Constraints: (not included in this Cross certificate)
- Certificate Policies:
    - 2.5.29.32.0 (anyPolicy)
- CRL Distribution Points:
    - http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE
- Authority Information Access:
    - (not included in this Cross certificate)

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 972B0E2FDBAA76A21DF4F4390B714F64F1D78686
- SHA256 Fingerprint: 288B4A9F605B09B999B215850825C81F9B537DBAF23664ACA98BF6BA98EDC379

3.2 Issuing CAs

3.2.1 SwissSign RSA TLS DV ICA 2022 - 1

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

- Version: Version 3 (Certificate format version)
- Serial Number: 75F85DDB06B0FA815891EA83C5CCFCE5578C190F (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS DV ICA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)

- Valid from: 29 Jun 2022 09:27:46 UTC (Start of certificate validity)
- Valid to: 29 Jun 2036 09:27:46 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: EBBD7F49938CC9EEECA2BAF71CD267F083B1EADE
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: id-kp-serverAuth, id-kp-clientAuth
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
  - 2.23.140.1.2.1 (CABF DV)
  - 0.4.0.2042.1.6 (ETSI DVCP)
  - 2.16.756.1.89.2.1.1 (SwissSign DVCP)
- CRL Distribution Points:
  - http://crl.swisssign.ch/cdp-9661c29f-9121-4f46-acd8-ead4a22f7160
- Authority Information Access:
  - caIssuers: http://aia.swisssign.ch/air-aeff374d-0f7a-4c55-a034-1440290cfa32

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 333150010FA78F700BC061323C679938CFC64BCB
- SHA256 Fingerprint: B400250EF2B09B30E9AAA3E2C20017B8911BD039DF8AF54949C60AED5BF697D4

3.2.2 SwissSign RSA TLS OV ICA 2022 - 1

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

- Version: Version 3 (Certificate format version)
- Serial Number: 6AEC7C44417B9B441FB97634CBC6A780B0041E01 (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS OV ICA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 29 Jun 2022 09:34:30 UTC (Start of certificate validity)
- Valid to: 29 Jun 2036 09:34:30 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: 7C6F0A6F130FD98C246F2634F35C6B436DB723B6
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: id-kp-serverAuth, id-kp-clientAuth
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
  - 2.23.140.1.2.2 (CABF OV)
  - 0.4.0.2042.1.7 (ETSI OVCP)
  - 2.16.756.1.89.2.1.2 (SwissSign OVCP)
- CRL Distribution Points:
  - http://crl.swisssign.ch/cdp-9661c29f-9121-4f46-acd8-ead4a22f7160
- Authority Information Access:
  - caIssuers: http://aia.swisssign.ch/air-aeff374d-0f7a-4c55-a034-1440290cfa32

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 37271FFBC6EECF840CEB32B8A7AEED6DCBD6A7F0

- SHA256 Fingerprint: 332F9EAE3650C77454AF14FE1A621A2498FD128773662890A0D12835B3436E23

3.2.3 SwissSign RSA TLS EV ICA 2022 - 1

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

- Version: Version 3 (Certificate format version)
- Serial Number: 2DAE0FA23A0C385FFBF395C0D903642D14184D2E (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS EV ICA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 29 Jun 2022 09:30:47 UTC (Start of certificate validity)
- Valid to: 29 Jun 2036 09:30:47 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: 4952DF308692595F349C254824ABC0EBD106F2D6
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: id-kp-serverAuth, id-kp-clientAuth
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
  - 2.23.140.1.1 (CABF EV)
  - 0.4.0.2042.1.4 (ETSI EVCP)
  - 2.16.756.1.89.2.1.3 (SwissSign EVCP)
- CRL Distribution Points:
  - http://crl.swisssign.ch/cdp-9661c29f-9121-4f46-acd8-ead4a22f7160
- Authority Information Access:
  - caIssuers: http://aia.swisssign.ch/air-aeff374d-0f7a-4c55-a034-1440290cfa32

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: CD3D43200F279CC95EA6BD955ACB06ED28090B77
- SHA256 Fingerprint: 6AE61943BF4B4FCC8F08ED5044D1C97AA0AD40E1BCFE1BF1B530BD3B151B364D

3.3 End-entity certificates

3.3.1 TLS Extended Validation Certificate (EVCP) issued by SwissSign RSA TLS EV ICA 2022 – 1 (EVCP)

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

- Version: Version 3 (Certificate format version)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Name: CN=SwissSign RSA TLS EV ICA 2022 - 1,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, a date of incorporation, formation, or establishment, “Government Entity”, OR language to indicate an International Organization Entity (like “International Organization”) (mandatory)
  - OrganizationName (O): Subject organization name as stated in certificate application. (mandatory)
  - Street: Name of the 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 if ST-attribute is missing, otherwise optional) (optional)
  - State-Or-Province (ST): State or province name or code as described in certificate application and in accordance with ISO 3166-2 (mandatory if L-attribute is missing, otherwise optional) (optional)
  - Country (C): Country code in accordance with ISO 3166-1 (mandatory)
  - Business Category (BC): One of the following: “Private Organization”, “Government Entity”, “Business Entity”, or “Non-Commercial Entity” as described in certificate application. (mandatory)
  - Jurisdiction Locality Name (joiL): Name of the locality as described in the certificate application. (optional)
  - Jurisdiction State or Province Name (joiST): State or province name in accordance with ISO 3166-2. (optional)
  - Jurisdiction Country Name (joiC): Country code in accordance with ISO 3166-1. (mandatory)
- Valid from: Start of certificate validity.
- Valid to: End of certificate validity.
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 2048 bit or higher)
- Authority Key Identifier: 4952DF308692595F349C254824ABC0EBD106F2D6 (mandatory)
- Subject Key Identifier: SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2 (mandatory)
- Key Usage (critical): digitalSignature (mandatory), keyEncipherment (mandatory)
- Extended Key Usage: 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) (mandatory), 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) (mandatory)
- Subject Alternative Name:
  - DNS: Must contain the subject CN and may contain additional DNS names (Wildcard entries are not allowed) (mandatory)
- Certificate Policies:
  - Policy OID: 2.23.140.1.1 (CABF EV) (mandatory)
  - Policy OID: 0.4.0.2042.1.4 (ETSI EN 319 411-1 EVCP) (mandatory)
  - Policy OID: 2.16.756.1.89.2.1.3 (SwissSign EVCP) (mandatory)
  - CPSURI: https://repository.swisssign.com/SwissSign_CPS_TLS.pdf (mandatory)
- OCSPmustStaple: ‘5’ (optional)
- CRL Distribution Point:
  - http://crl.swisssign.ch/cdp-9fdd910e-b9ff-4b2f-be38-2e93708c1b36 (mandatory)
- Authority Information Access:
  - caIssuer: http://aia.swisssign.ch/air-20350159-813d-4532-b988-8519eca57650 (mandatory)
  - ocsp: http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec (mandatory)
- SCT list: List of Signed Certificate Timestamps (SCT) (SCTs are provided by the CT-logs accessed)

3.3.2 TLS Organization Validated Certificates (OVCP) issued by SwissSign RSA TLS OV ICA 2022 - 1

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

- Version: Version 3 (Certificate format version)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Name: CN=SwissSign RSA TLS OV ICA 2022 - 1,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)
  - OrganizationName (O): Subject organization name as stated in certificate application. (mandatory)
  - LocalityName (L): Name of the locality as described in the certificate application (mandatory if ST-attribute is missing, otherwise optional) (optional)
  - State-Or-Province (ST): State or province name or code as described in certificate application and in accordance with ISO 3166-2 (mandatory if L-attribute is missing, otherwise optional) (optional)
  - Country (C): Country code in accordance with ISO 3166-1 (mandatory)
- Valid from: Start of certificate validity.
- Valid to: End of certificate validity.

- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 2048 bit or higher)
- Authority Key Identifier: 7C6F0A6F130FD98C246F2634F35C6B436DB723B6 (mandatory)
- Subject Key Identifier: SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2 (mandatory)
- Key Usage (critical): digitalSignature (mandatory), keyEncipherment (mandatory)
- Extended Key Usage: 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) (mandatory), 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) (mandatory)
- Subject Alternative Name:
  - DNS: Must contain the subject CN and may contain additional DNS names (Wildcard entries are allowed) (mandatory)
- Certificate Policies:
  - Policy OID: 2.23.140.1.2.2 (CABF OV) (mandatory)
  - Policy OID: 0.4.0.2042.1.7 (ETSI EN 319 411-1 OVCP) (mandatory)
  - Policy OID: 2.16.756.1.89.2.1.2 (SwissSign OVCP) (mandatory)
  - CPSURI: https://repository.swisssign.com/SwissSign_CPS_TLS.pdf (mandatory)
- OCSPmustStaple: ‘5’ (optional)
- CRL Distribution Point:
  - http://crl.swisssign.ch/cdp-96b62f5a-6b73-4da4-87f7-ce4002c1cd34 (mandatory)
- Authority Information Access:
  - caIssuer: http://aia.swisssign.ch/air-0f2bf9a5-dd37-48c9-a85b-12acdcb8be45 (mandatory)
  - ocsp: http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec (mandatory)
- SCT list: List of Signed Certificate Timestamps (SCT) (SCTs are provided by the CT-logs accessed)

3.3.3 TLS Domain Validated Certificates (DVCP) issued by SwissSign RSA TLS DV ICA 2022 - 1

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

- Version: Version 3 (Certificate format version)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Name: CN=SwissSign RSA TLS DV ICA 2022 - 1,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.
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 2048 bit or higher)
- Authority Key Identifier: EBBD7F49938CC9EEECA2BAF71CD267F083B1EADE (mandatory)
- Subject Key Identifier: SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2 (mandatory)
- Key Usage (critical): digitalSignature (mandatory), keyEncipherment (mandatory)
- Extended Key Usage: 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) (mandatory), 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) (mandatory)
- Subject Alternative Name:
  - DNS: Must contain the subject CN and may contain additional DNS names (Wildcard entries are allowed) (mandatory)
- Certificate Policies:
  - Policy OID: 2.23.140.1.2.1 (CABF DV) (mandatory)
  - Policy OID: 0.4.0.2042.1.6 (ETSI EN 319 411-1 DVCP) (mandatory)
  - Policy OID: 2.16.756.1.89.2.1.1 (SwissSign DVCP) (mandatory)
  - CPSURI: https://repository.swisssign.com/SwissSign_CPS_TLS.pdf (mandatory)
- OCSPmustStaple: ‘5’ (optional)
- CRL Distribution Point:
  - http://crl.swisssign.ch/cdp-679723b2-8641-4642-8500-f6d2ff37e6ba (mandatory)
- Authority Information Access:
  - caIssuer: http://aia.swisssign.ch/air-1b863385-f4a9-47fa-88a5-2a5abfd4a167 (mandatory)

  - ocsp: http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec (mandatory)
- SCT list: List of Signed Certificate Timestamps (SCT) (SCTs are provided by the CT-logs accessed)

4. OCSP Profile

4.1 OCSP Response Profile

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

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 (mandatory, Type of the response)
- Version: V1 (mandatory)
- Responder Id: DN (mandatory, Distinguished name of the OCSP responder)
- Produced At: Date (mandatory, Date when the OCSP response was signed)
- CertID: Unique ID for requested certificate (The CertID from the OCSP request is included in the response)
- Cert Status: Good, revoked, or unknown (mandatory, Indicates the response for certificate status)
- Revocation Time: (optional, Date of revocation of certificate, January 1, 1970 for non-issued certificates according to chapter 2.2 of RFC6960)
- revocationReason: (Optional for end-entity certificates. If present, the possible values are as follows:)
  - unspecified (0)
  - keyCompromise (1)
  - affiliationChanged (3)
  - superseded (4)
  - cessationOfOperation (5) or
  - privilegeWithdrawn (9)
  - For CA certificates: Only present if issuing CA is revoked, The extension is set as described in BRG clause 7.2.2 and 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)
- Extended Revoked Definition: Extended revoked extension according to chapter 2.2 and 4.4.8 of RFC6960 (optional)
- SCT: SCTs for requested certificate (Optional, the Signed Certificate Timestamps (SCTs) for the requested certificate may be included in the response)
- Signature Algorithm: sha256WithRSAEncryption (mandatory)
- Certificate: Details of certificate used to sign the response (mandatory)

The OCSP extensions used are specified below:

- Nonce

The ArchiveCutOff extension is not set in the OCSP responses.

4.2 OCSP Responder Certificate

This list has the format “Field/Extension”: “Values” (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: (Unique subject distinguished name of the OCSP Signer certificate.)
  - CommonName (CN): (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.)
  - OrganizationName (O): SwissSign AG
  - Country (C): CH
- Valid from: Start of certificate validity
- Valid to: End of certificate validity
- subjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 2048 bit or higher)
- Key Usage: digitalSignature (mandatory, critical)
- Subject Key Identifier: SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2 (mandatory)
- Authority Key Identifier: SHA-1 hash value of Issuing CA’s Public Key according to RFC5280 chapter 4.2.1.2 (mandatory)
- 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 [10].

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: 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. Optional for end-entity certificates (please note: reason code 0 for “unspecified” is not set). If present, the possible values are as follows:
  - keyCompromise (1)
  - affiliationChanged (3)
  - superseded (4)
  - cessationOfOperation (5) or
  - privilegeWithdrawn (9)
  - 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 Issuing CA

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

6. 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 319 411-1V1.4.1 (2023-10) 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 TLS Server 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;