∴ SwissSign

SwissSign CPR S/MIME

Certificate, CRL and OCSP Profiles for S/MIME 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:	07 November 2022
Version:	5.0
Obsoletes:	4.0, 01 July 2022
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Disclaimer: The electronic version of this document and all its stipulations are considered binding if saved in Adobe PDF Format and signed by two legal representatives of SwissSign. All other copies and media are null and void.

Version Control

Date	Version	Comment	Author
14.06.2021	1.0	Initial version	Michael Günther
11.10.2021	2.0	Adding SMIME Root	Michael Günther
25.04.2022	3.0	Restructuring of chapter 3.3, adding new certificate profile in 3.3.1.2	Adrian Mueller, Michael Günther
01.07.2022	4.0	Adding new CAs (Selfsigned Root, Cross & ICAs)	Adrian Müller, Michael Günther
07.11.2022	5.0	Adjustment/amendment of allowed exceptions in Common Name; specifying revocation reason codes	Adrian Müller, Michael Günther

Authorization

Date	Approved by	Approved by	Version
11.06.2021	Michael Günther	Markus Naef	1.0
07.10.2021	Michael Günther	Markus Naef	2.0
25.04.2022	Michael Günther	Michael Widmer	3.0
01.07.2022	Michael Günther	Michael Widmer	4.0
07.11.2022	Michael Günther	Michael Widmer	5.0

digital signature   digital signature

Table of Contents

1. Introduction

This document describes profiles of the S/MIME 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-emailProtection, id-kp-clientAuth **or** id-kp-emailProtection, id-kp-clientAuth msEFS msSCL DocumentSigning Authentic Documents Trust	(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

Algorithm	Object Identifier
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	00BB401C43F55E4FB0	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

3.1.2 SwissSign RSA SMIME Root CA 2021 – 1 (Self-signed)

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	746cd5d1943c167daebe03ede56e07	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	CN = SwissSign RSA SMIME Root CA 2021 - 1 O = SwissSign AG C = CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	CN = SwissSign RSA SMIME Root CA 2021 - 1 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	2 Aug 2021 11:20:08 UTC	Start of certificate validity.
Valid to	27 Jul 2046 11:20:08 UTC	End of certificate validity.
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	090CBF2AA21D04240CB2F9400A41C2CF5A72AA80	
Authority Key Identifier	090CBF2AA21D04240CB2F9400A41C2CF5A72AA80	
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	078385ff7dd89742c365e2d008172dcc27350afa
SHA256 Fingerprint	B6D56F3DD26AC844E57C8BFE9054F57061350A90894B99CD9811E9A545FC84C5

3.1.3 SwissSign RSA SMIME Root CA 2021 – 1 (Cross)

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	00de4c5520f6dcf4021b0f1154f78d10	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 SMIME Root CA 2021 – 1 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	3 Aug 2021 13:14:55 UTC	Start of certificate validity.
Valid to	23 Oct 2036 13:14:55 UTC	End of certificate validity.
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	090CBF2AA21D04240CB2F9400A41C2CF5A72AA80	
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE	
Extended Key Usage	not included in this Cross certificate	
Name Constraints	not included in this Cross certificate	
Certificate Policies	not included in this Cross certificate	
CRL Distribution Points	http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0E ldap://directory.swisssign.net/CN=5B257B96A465517EB839F3C078665EE83AE7F0EE%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	
Authority Information Access	not included in this Root CA certificate	

The Cross certificate is identified via the following fingerprints:

SHA1 Fingerprint	C7724C41CE8F9BAAD3553BCBC0CD0BFCD93E36E2
SHA256 Fingerprint	BC8BBD7D279D2E5F070BCEF6FAF3AAB1BEF30DA3EB2875424295AD147F2AEF07

3.1.4 SwissSign RSA SMIME Root CA 2022 - 1 (Self-signed)

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	460ED4017190A01A832C4A42102815D2611BAD32	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	CN = SwissSign RSA SMIME Root CA 2022 - 1 O = SwissSign AG C = CH	Unique issuer distinguished name of the certificate
Subject Distinguished name	CN = SwissSign RSA SMIME Root CA 2022 - 1 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	08 Jun 2022 10:53:13 UTC	Start of certificate validity.
Valid to	08 Jun 2047 10:53:13 UTC	End of certificate validity.
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	CC2EAD898C83E340A32569A5EA927DD2373AC7C6	
Authority Key Identifier	CC2EAD898C83E340A32569A5EA927DD2373AC7C6	
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	14D76562741050479F8B32C6868A18FAE11999B0
SHA256 Fingerprint	9A12C392BFE57891A0C545309D4D9FD567E480CB613D6342278B195C79A7931F

3.1.5 SwissSign RSA SMIME Root CA 2022 - 1 (Cross)

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	00B30511B116B4A056511D7C681F877D	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 SMIME Root CA 2022 - 1 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	28 Jun 2022 11:26:01 UTC	Start of certificate validity.
Valid to	22 Sep 2036 11:26:01 UTC	End of certificate validity.
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	CC2EAD898C83E340A32569A5EA927DD2373AC7C6	
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE	
Extended Key Usage	not included in this Cross certificate	
Name Constraints	not included in this Cross certificate	
Certificate Policies	Policy OID: 2.5.29.32.0	OID 2.5.29.32.0 stands for *anyPolicy*, see RFC5280, chapter 4.2.1.4.
CRL Distribution Points	http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE	http-URL for CRL-download
Authority Information Access	not included in this Cross certificate	

The Cross certificate is identified via the following fingerprints:

SHA1 Fingerprint	D5374C8C93CEC79335B9C66F4A22BE33A07D0AEA
SHA256 Fingerprint	5A84C94054D340D650A29985EF97BB396352E215AED6C0B33CA7FFDD3BD5D2A2

3.2 Issuing CAs

3.2.1 SwissSign Personal Gold CA 2008 – G2 (CRL & OCSP only)

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	392B241D6144C35A		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 Personal Gold CA 2008 – G2 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	07 Jul 2008 17:24:18 UTC		Start of certificate validity.
Valid to	07 Jul 2023 17:24:18 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	AE7A8B15F8253EF41AEF436B25C0A6E11A3CA6AB		
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	calssuers	http://swisssign.net/cgi-bin/authority/download/5B257B96A465517EB839F3C078665EE83AE7F0EE	
	OCSP	not included in this Issuing CA certificate	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	EFE1F5361B03107D284810D8FC3DCC879207F661
SHA256 Fingerprint	2B65E45EA181C1CC21B1CC9E9FB1E10F54129432BB78973F608C66A4151FBF0E

3.2.2 SwissSign Personal Gold CA 2014 – G22 (CRL & OCSP only)

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	191795DC22741B121DDB544C5CCBDC	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 Personal Gold CA 2014 – G22 O = SwissSign AG C = CH	Unique subject distinguished name of the certificate
Valid from	19 Sep 2014 14:10:25 UTC	Start of certificate validity.
Valid to	15 Sep 2029 14:10:25 UTC	End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	DA32F949F851CC9871660CD9CEB6DB923F094BEF	
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 Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	184B85D90DB4F4BCB53AC8F3DCDF42B4A4527889
SHA256 Fingerprint	77D6C2AF5A7B86F63D9918C87533779F2AF08D35CFA14DA4938C803F53DE18A1

3.2.3 SwissSign RSA SMIME LCP ICA 2021 – 2

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	2C5AA9D954FDB2AB96AD17B65F8CF4		Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name	CN=SwissSign RSA SMIME Root CA 2021 – 1 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name	CN=SwissSign RSA SMIME LCP ICA 2021 – 2 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	04 Aug 2021 12:12:59 UTC		Start of certificate validity.
Valid to	31. Jul 2036 12:12:59 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	FA54C082A6FE96BD04C75F9F5F820C3DC3954F47		
Authority Key Identifier	090CBF2AA21D04240CB2F9400A41C2CF5A72AA80		
Extended Key Usage	id-kp-emailProtection		
Name Constraints	not included in this Issuing CA certificate		
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.11 (SwissSign LCP CP) Policy OID: 0.4.0.2042.1.3 (ETSI LCP)		
CRL Distribution Points	http://crl.swisssign.net/090CBF2AA21D04240CB2F9400A41C2CF5A72AA80, ldap://directory.swisssign.net/CN=090CBF2AA21D04240CB2F9400A41C2CF5A72AA80%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/090CBF2AA21D04240CB2F9400A41C2CF5A72AA80	
	OCSP	not included in this Issuing CA certificate	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	5342BB246ABFD5B0E8AE2F8DB561B8CB790A896E
SHA256 Fingerprint	5CFFA8DB135F913363ACEB7CE362D098F3C1EBD26C63C560C095381E896504FA

3.2.5 SwissSign RSA SMIME LCP ICA 2022-1

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	5530D33DD130D46B1E9D76E8DA0C0A128C6E7F76		Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name	CN=SwissSign RSA SMIME Root CA 2022 – 1 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name	CN=SwissSign RSA SMIME LCP ICA 2022 – 1 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	29 June 2022 09:10:52 UTC		Start of certificate validity.
Valid to	29 June 2036 09:10:52 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	0B83D4722086CCE13AEF99B677CD51A6A3728F5C		
Authority Key Identifier	CC2EAD898C83E340A32569A5EA927DD2373AC7C6		
Extended Key Usage	id-kp-emailProtection		
Name Constraints	not included in this Issuing CA certificate		
Certificate Policies	0.4.0.2042.1.3 (ETSI LCP) 2.16.756.1.89.2.1.11 (SwissSign LCP CP)		
CRL Distribution Points	http://crl.swisssign.ch/cdp-3ee55fd4-5938-41ee-82db-3223acef5c23		
Authority Information Access	caIssuers	http://aia.swisssign.ch/air-4a7f1788-26b5-48ec-a547-c1cd0bf17c3d	
	OCSP	not included in this Issuing CA certificate	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	C35C18E7AF0069B2830B423BB7CF30D9F0E3900B
SHA256 Fingerprint	D7F41FABE5A459BAC6882465C75CCFF2BAA52487AABC34706CAF2A18AC53A5C2

3.2.6 SwissSign RSA SMIME NCP ICA 2021 -1

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	68D130DD08874B1E60622EA5E26304		Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name	CN=SwissSign RSA SMIME Root CA 2021 – 1 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name	CN=SwissSign RSA SMIME NCP ICA 2021 – 1 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	03 Aug 2021 19:09:30 UTC		Start of certificate validity.
Valid to	30 Jul 2036 19:09:30 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	E1644D6ECA9EC75DC97ECD4FDC3B53F45D0F18D3		
Authority Key Identifier	090CBF2AA21D04240CB2F9400A41C2CF5A72AA80		
Extended Key Usage	id-kp-clientAuth id-kp-emailProtection		
Name Constraints	not included in this Issuing CA certificate		
Certificate Policies	2.16.756.1.89.2.1.12 (SwissSign NCP CP) 0.4.0.2042.1.1 (ETSI NCP)		
CRL Distribution Points	http://crl.swisssign.net/090CBF2AA21D04240CB2F9400A41C2CF5A72AA80, ldap://directory.swisssign.net/CN=090CBF2AA21D04240CB2F9400A41C2CF5A72AA80%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/090CBF2AA21D04240CB2F9400A41C2CF5A72AA80	
	OCSP	not included in this Issuing CA certificate	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	E8A744F44591DD7539FB20CE3F8CF988EA915346
SHA256 Fingerprint	1935AA544A73D755E913357FCE0E44AFC90E0809AC97A89964F0A90A59C376B6

3.2.7 SwissSign RSA SMIME NCP ICA 2022 - 1

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	796C0FD9724F3291C0083A1A6DEEC2670EB6DCA0		Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name	CN=SwissSign RSA SMIME Root CA 2022 - 1 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name	CN=SwissSign RSA SMIME NCP ICA 2022 - 1 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	29 June 2022 09:17:39 UTC		Start of certificate validity.
Valid to	29 June 2036 09:17:39 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	E4BEC760A782A318E864FCE216530587D46AE98E		
Authority Key Identifier	CC2EAD898C83E340A32569A5EA927DD2373AC7C6		
Extended Key Usage	id-kp-clientAuth id-kp-emailProtection		
Name Constraints	not included in this Issuing CA certificate		
Certificate Policies	0.4.0.2042.1.1 (ETSI NCP) 2.16.756.1.89.2.1.12 (SwissSign NCP CP)		
CRL Distribution Points	http://crl.swisssign.ch/cdp-3ee55fd4-5938-41ee-82db-3223acef5c23		
Authority Information Access	caIssuers	http://aia.swisssign.ch/air-4a7f1788-26b5-48ec-a547-c1cd0bf17c3d	
	OCSP	not included in this Issuing CA certificate	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	1CE92DDA2FEB1DD9CFE39A4E51BEF7C2D311F607
SHA256 Fingerprint	99A56DD8DACA399FCA2E3834ED75760E96C133564062F8B530B355BED99A409D

3.2.8 SwissSign RSA SMIME NCP extended ICA 2021 - 1

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	45738B321942F875317A4806EB0A95		Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name	CN=SwissSign RSA SMIME Root CA 2021 - 1 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name	CN=SwissSign RSA SMIME NCP extended ICA 2021 - 1 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	03 Aug 2021 19:16:28 UTC		Start of certificate validity.
Valid to	30 Jul 2036 19:16:28 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	2B661A63041903A719FC35E7C3B8D1368F4E9A41		
Authority Key Identifier	090CBF2AA21D04240CB2F9400A41C2CF5A72AA80		
Extended Key Usage	id-kp-clientAuth id-kp-emailProtection msEFS msSCL		
Name Constraints	not included in this Issuing CA certificate		
Certificate Policies	2.16.756.1.89.2.1.13 (SwissSign NCP extended) 0.4.0.2042.1.1 (ETSI NCP)		
CRL Distribution Points	http://crl.swisssign.net/090CBF2AA21D04240CB2F9400A41C2CF5A72AA80, ldap://directory.swisssign.net/CN=090CBF2AA21D04240CB2F9400A41C2CF5A72AA80%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint		
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/090CBF2AA21D04240CB2F9400A41C2CF5A72AA80	
	OCSP	not included in this Issuing CA certificate	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	D0FE06298701709267D1F105692552C01E394C33
SHA256 Fingerprint	0A6EEB87C2B4AC4A0DF4A68CA7E5244408E06A0CF3BE973156A52AAD835D7466

3.2.9 SwissSign RSA SMIME NCP extended ICA 2022 - 1

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	4653D903D9AE555F0BB20F3EC8B2B50D83D7CA34		Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name	CN=SwissSign RSA SMIME Root CA 2022 - 1 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject Distinguished name	CN=SwissSign RSA SMIME NCP extended ICA 2022 - 1 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	29 June 2022 09:21:13 UTC		Start of certificate validity.
Valid to	29 June 2036 09:21:13 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	56A2DFF3E1841D1BA0FF7F3FF071188528F83DCD		
Authority Key Identifier	CC2EAD898C83E340A32569A5EA927DD2373AC7C6		
Extended Key Usage	id-kp-emailProtection id-kp-clientAuth msEFS msSCL		
Name Constraints	not included in this Issuing CA certificate		
Certificate Policies	0.4.0.2042.1.1 (ETSI NCP) 2.16.756.1.89.2.1.13 (SwissSign NCP extended)		
CRL Distribution Points	http://crl.swisssign.ch/cdp-3ee55fd4-5938-41ee-82db-3223acef5c23		
Authority Information Access	caIssuers	http://aia.swisssign.ch/air-4a7f1788-26b5-48ec-a547-c1cd0bf17c3d	
	OCSP	not included in this Issuing CA certificate	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	F4C4C1703ABA2EAC24EE315F40E1A8B6CB3E76FD
SHA256 Fingerprint	7196E86DCFDB92B0509213D806DCA2465FC41415A0B4069D35F946DE6813CF79

3.3 End-entity certificates

3.3.1 Lightweight Certificate Policy (LCP)

3.3.1.1 SwissSign Personal S/MIME E-Mail ID Silver Certificate (LCP) issued by SwissSign RSA SMIME LCP ICA 2021 - 2 - Default profile (E-Mail only)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	CN = SwissSign RSA SMIME LCP ICA 2021 – 2 O = SwissSign AG C = CH		Unique issuer distinguished name of the certificate
Subject DN			Unique subject distinguished name of the certificate
	Common Name (CN)	E-Mail address of Subject as stated in certificate application.	(mandatory)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	FA54C082A6FE96BD04C75F9F5F820C3DC3954F47		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature, keyEncipherment, dataEncipherment		(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection		(mandatory)
Subject Alternative Name	E-mail address of the subject		(mandatory)
Certificate Policies	Policy OID: 0.4.0.2042.1.3 (ETSI LCP) Policy OID: 2.16.756.1.89.2.1.11 (SwissSign LCP) CPSURI: https://repository.swissign.com/SwissSign_CPS_SMIME.pdf		(mandatory)
CRL Distribution Points	http://crl.swisssign.net/FA54C082A6FE96BD04C75F9F5F820C3DC3954F47 ldap://directory.swisssign.net/CN=FA54C082A6FE96BD04C75F9F5F820C3DC3954F47,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/FA54C082A6FE96BD04C75F9F5F820C3DC3954F47	(mandatory)
	OCSP	http://ocsp.swisssign.net/FA54C082A6FE96BD04C75F9F5F820C3DC3954F47	(mandatory)
Microsoft Certificate	OID to designate the specific MS-Template		(optional)

Template	Integer to designate the «templateMajorVersion»	(optional)
	Integer to designate the «templateMinorVersion»	(optional)

3.3.1.2 SwissSign E-Mail ID Silver (LCP) Certificate issued by SwissSign RSA SMIME LCP ICA 2021 - 2 - E-Mail & organization

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	Please see the general profile in clause 3.3.1.1		
Subject DN			Unique subject distinguished name of the certificate
	Common Name (CN)	E-Mail address of Subject as stated in certificate application	(mandatory)
	Email	E-mail address of Subject as stated in certificate application	(optional)
	OrganizationalUnit (OU)	Organizational unit as stated in certificate application.	(optional)
	OrganisationName (O)	Subject (organisation) name as stated in certificate application	(mandatory)
	LocalityName (L)	Name of the locality as described in the certificate application	(optional)
	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)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	Please see the general profile in clause 3.3.1.1		
Subject Key Identifier	Please see the general profile in clause 3.3.1.1		
Key Usage	Please see the general profile in clause 3.3.1.1		
Extended Key Usage	Please see the general profile in clause 3.3.1.1		
Subject Alternative Name	Please see the general profile in clause 3.3.1.1		
Certificate Policies	Please see the general profile in clause 3.3.1.1		
CRL Distribution Points	Please see the general profile in clause 3.3.1.1		
Authority Information Access	Please see the general profile in clause 3.3.1.1		

3.3.1.3   SwissSign Personal S/MIME E-Mail ID Silver Certificate (LCP) issued by SwissSign RSA SMIME LCP ICA 2022 – 1 - Default Profile (E-Mail only)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	CN = SwissSign RSA SMIME LCP 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)	E-Mail address of Subject as stated in certificate application.	(mandatory)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	0B83D4722086CCE13AEF99B677CD51A6A3728F5C		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature, keyEncipherment, dataEncipherment		(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection		(mandatory)
Subject Alternative Name	E-mail address of the subject		(mandatory)
Certificate Policies	Policy OID: 0.4.0.2042.1.3 (ETSI LCP) Policy OID: 2.16.756.1.89.2.1.11 (SwissSign LCP) CPSURI: https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf		(mandatory)
CRL Distribution Points	http://crl.swisssign.ch/cdp-d5057ba0-ce09-4d1d-8cc9-0a60fa4c49c0		(mandatory) HTTP-URL of the CRL Distribution point
Authority Information Access	caIssuers	http://aia.swisssign.ch/air-79b46fac-4cd2-4d42-9fe0-9cd078d13d8c	(mandatory)
	OCSP	http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec	(mandatory)
Microsoft Certificate Template	OID to designate the specific MS-Template		(optional)
	Integer to designate the «templateMajorVersion»		(optional)
	Integer to designate the «templateMinorVersion»		(optional)

3.3.1.4   Allowed exceptions for Common Name

Name Allowed exceptions with a fixed string in the common name in LCP certificates, with a then mandatory entry for /E-Mail are:

-    "Secure Mail: Gateway Certificate"

- "Secure Mail: SEPPmail Certificate"
- "XnetSolutions Mailgateway"
- "Secure Mail: SX-Mail Crypt Certificate"
- "Secure E-Mail: SX-Mail Crypt Certificate"
- "Zertificon Mailgateway"
- "Z1 SecureMail Gateway Certificate"

3.3.2 Normalized Certificate Policy (NCP)

3.3.2.1 Pro S/MIME E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 - G22 - Default profile (no authentication)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	CN = SwissSign Personal 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)	GivenName Surname or pseudo: Pseudonym	(mandatory)
	GivenName	Subject's Given Name as stated in certificate application.	(optional)
	Surname	Subject's Surname Name as stated in certificate application.	(optional)
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
	SerialNumber	Unique number generated by the TSP.	(optional, only mandatory if Email missing)
	OrganizationalUnit (OU)	Organizational unit as stated in certificate application.	(optional)
	OrganizationName (O)	Subject (organisation) name as stated in certificate application.	(optional)
	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	(optional)
	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)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	DA32F949F851CC9871660CD9CEB6DB923F094BEF		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)

Key Usage	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment	(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection	(mandatory)
Subject Alternative Name	E-mail address of the subject	(mandatory)
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.12 CPSURI: https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf Policy OID: 0.4.0.2042.1.1 (NCP)	(mandatory)
CRL Distribution Points	http://crl.swisssign.net/DA32F949F851CC9871660CD9CEB6DB923F094BEF ldap://directory.swisssign.net/CN=DA32F949F851CC9871660CD9CEB6DB923F094BEF%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers http://swisssign.net/cgi-bin/authority/download/DA32F949F851CC9871660CD9CEB6DB923F094BEF	(mandatory)
	OCSP http://ocsp.swisssign.net/DA32F949F851CC9871660CD9CEB6DB923F094BEF	(mandatory)

3.3.2.2   Pro S/MIME E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 - G22 - no authentication, MS-template

Field/Extension	Values	Comment
Version	Version 3	Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption	
Issuer Name	Please see the general profile in clause 3.3.2.1	
Subject DN	Please see the general profile in clause 3.3.2.1	
Valid from		Start of certificate validity.
Valid to		End of certificate validity.
Authority Key Identifier	Please see the general profile in clause 3.3.2.1	(mandatory)
Subject Key Identifier	Please see the general profile in clause 3.3.2.1	(mandatory)
Key Usage	Please see the general profile in clause 3.3.2.1	
Extended Key Usage	Please see the general profile in clause 3.3.2.1	
Subject Alternative Name	Please see the general profile in clause 3.3.2.1	
Certificate Policies	Please see the general profile in clause 3.3.2.1	
CRL Distribution Points	Please see the general profile in clause 3.3.2.1	
Authority Information Access	Please see the general profile in clause 3.3.2.1	
Microsoft Certificate Template	OID to designate the specific MS-Template	(mandatory)
	Integer to designate the «templateMajorVersion»	(mandatory)

	Integer to designate the «templateMinorVersion»	(mandatory)

3.3.2.3 Pro S/MIME E-Mail ID Gold Certificate issued by SwissSign RSA SMIME NCP ICA 2021 - 1 - Default profile (no authentication)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	CN=SwissSign RSA SMIME NCP ICA 2021 - 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)	GivenName Surname or pseudo: Pseudonym	(mandatory)
	GivenName	Subject's Given Name as stated in certificate application.	(optional)
	Surname	Subject's Surname Name as stated in certificate application.	(optional)
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
	SerialNumber	Unique number generated by the TSP.	(optional, only mandatory if Email missing)
	OrganizationalUnit (OU)	Organizational unit as stated in certificate application.	(optional)
	OrganizationName (O)	Subject (organisation) name as stated in certificate application.	(optional)
	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	(optional)
	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)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	E1644D6ECA9EC75DC97ECD4FDC3B53F45D0F18D3		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter		(mandatory)

	4.2.1.2	
Key Usage	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment	(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection	(mandatory)
Subject Alternative Name	E-mail address of the subject	(mandatory)
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.12 CPSURI: https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf Policy OID: 0.4.0.2042.1.1 (NCP)	(mandatory)
CRL Distribution Points	http://crl.swisssign.net/E1644D6ECA9EC75DC97ECD4FDC3B53F45D0F18D3 ldap://directory.swisssign.net/CN=E1644D6ECA9EC75DC97ECD4FDC3B53F45D0F18D3%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/E1644D6ECA9EC75DC97ECD4FDC3B53F45D0F18D3	(mandatory)
	OCSP	http://ocsp.swisssign.net/E1644D6ECA9EC75DC97ECD4FDC3B53F45D0F18D3	(mandatory)
Microsoft Certificate Template	OID to designate the specific MS-Template	(optional)
	Integer to designate the «templateMajorVersion»	(optional)
	Integer to designate the «templateMinorVersion»	(optional)

3.3.2.4 Pro S/MIME E-Mail ID Gold Certificate issued by SwissSign RSA SMIME NCP ICA 2022 - 1 - Default profile (no authentication)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	CN=SwissSign RSA SMIME NCP 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)	GivenName Surname or pseudo: Pseudonym	(mandatory)
	GivenName	Subject's Given Name as stated in certificate application.	(optional)
	Surname	Subject's Surname Name as stated in certificate application.	(optional)
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
	SerialNumber	Unique number generated by the TSP.	(optional, only mandatory if Email missing)
	OrganizationalUnit (OU)	Organizational unit as stated in certificate application.	(optional)
	OrganizationName (O)	Subject (organisation) name as stated in certificate application.	(optional)
	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	(optional)
	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)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	E4BEC760A782A318E864FCE216530587D46AE98E		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature, nonRepudiation, keyEncipherment,		(mandatory)

	dataEncipherment	Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection	(mandatory)
Subject Alternative Name	E-mail address of the subject	(mandatory)
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.12 CPSURI: https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf Policy OID: 0.4.0.2042.1.1 (NCP)	(mandatory)
CRL Distribution Points	http://crl.swisssign.ch/cdp-5639ce88-5da9-408f-b25d-685d1e3e020a	URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://aia.swisssign.ch/air-9c868187-6fca-4313-aa5b-ce5fec83132f	(mandatory)
	OCSP	http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec	(mandatory)
Microsoft Certificate Template	OID to designate the specific MS-Template	(optional)
	Integer to designate the «templateMajorVersion»	(optional)
	Integer to designate the «templateMinorVersion»	(optional)

3.3.2.5   Allowed exceptions for Common Name

Allowed exceptions with a fixed string in the common name in NCP certificates, with a then mandatory entry for /E-Mail are:

- "Secure Mail: Gateway Certificate"
- "Secure Mail: SEPPmail Certificate"
- "XnetSolutions Mailgateway"
- "Secure Mail: SX-Mail Crypt Certificate"
- "Secure E-Mail: SX-Mail Crypt Certificate"
- "Zertificon Mailgateway"
- "Z1 SecureMail Gateway Certificate"

3.3.3 Normalized Certificate Policy extended

3.3.3.1 Pro S/MIME E-Mail ID Gold Certificate issued by SwissSign RSA SMIME NCP extended ICA 2021 - 1 (NCP) – Default Profile (authentication)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption or RSASSA-PSS with SHA-256		
Issuer Name	CN = SwissSign RSA SMIME NCP extended ICA 2021 - 1 O = SwissSign AG C = CH		
Subject DN			Unique subject distinguished name of the certificate
	Common Name (CN)	GivenName Surname or pseudo: Pseudonym	(mandatory)
	GivenName	Subject's Given Name as stated in certificate application.	(optional)
	Surname	Subject's Surname Name as stated in certificate application.	(optional)
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
	SerialNumber	Unique number generated by the TSP.	(optional, only mandatory if Email missing)
	OrganizationalUnit (OU)	Organizational unit as stated in certificate application.	(optional)
	OrganizationName (O)	Subject (organisation) name as stated in certificate application.	(optional)
	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	(optional)
	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)
	User ID (UID)	Login ID of user	(optional)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	2B661A63041903A719FC35E7C3B8D1368F4E9A41		

Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2	(mandatory)
Key Usage	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement	(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection, id-kp-clientAuth, msEFS, msSCL	(mandatory) The values msEFS, msSCL are optional.
Subject Alternative Name	E-mail address of the subject	(mandatory)
	universalPrincipalName/Microsoft UPN (OID 1.3.6.1.4.1.311.20.2.3)	(optional)
Certificate Policies	Policy OID: 0.4.0.2042.1.1 (ETSI NCP) Policy OID: 2.16.756.1.89.2.1.13 (SwissSign NCP extended) CPSURI: https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf	
CRL Distribution Points	http://crl.swisssign.net/2B661A63041903A719FC35E7C3B8D1368F4E9A41 ldap://directory.swisssign.net/CN=2B661A63041903A719FC35E7C3B8D1368F4E9A41%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/2B661A63041903A719FC35E7C3B8D1368F4E9A41	(mandatory)
	OCSP	http://ocsp.swisssign.net/2B661A63041903A719FC35E7C3B8D1368F4E9A41	(mandatory)
Microsoft Certificate Template	OID to designate the specific MS-Template	(optional)
	Integer to designate the «templateMajorVersion»	(optional)
	Integer to designate the «templateMinorVersion»	(optional)

3.3.3.2 Pro S/MIME E-Mail ID Gold Certificate issued by SwissSign RSA SMIME NCP extended ICA 2021 - 1 – Document Signing (only for certificates issued before 1 April 2022)

Field/Extension	Values	Comment
Version	Version 3	Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption	
Issuer Name	Please see the general profile in clause 3.3.3.1	
Subject DN	Please see the general profile in clause 3.3.3.1	
Valid from		Start of certificate validity.
Valid to		End of certificate validity.
Authority Key Identifier	Please see the general profile in clause 3.3.3.1	
Subject Key Identifier	Please see the general profile in clause 3.3.3.1	(mandatory)
Key Usage	Please see the general profile in clause 3.3.3.1	

Extended Key Usage	id-kp-emailProtection	(mandatory)
Subject Alternative Name	Please see the general profile in clause 3.3.3.1	optional
Certificate Policies	Please see the general profile in clause 3.3.3.1	
CRL Distribution Points	Please see the general profile in clause 3.3.3.1	
Authority Information Access	Please see the general profile in clause 3.3.3.1	

3.3.3.3 Pro S/MIME E-Mail ID Gold Certificate issued by SwissSign RSA SMIME NCP extended ICA 2022 - 1 (NCP) – Default Profile (authentication)

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption or RSASSA-PSS with SHA-256		
Issuer Name	CN = SwissSign RSA SMIME NCP extended ICA 2022 - 1 O = SwissSign AG C = CH		
Subject DN			Unique subject distinguished name of the certificate
	Common Name (CN)	GivenName Surname or pseudo: Pseudonym	(mandatory)
	GivenName	Subject's Given Name as stated in certificate application.	(optional)
	Surname	Subject's Surname Name as stated in certificate application.	(optional)
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
	SerialNumber	Unique number generated by the TSP.	(optional, only mandatory if Email missing)
	OrganizationalUnit (OU)	Organizational unit as stated in certificate application.	(optional)
	OrganizationName (O)	Subject (organisation) name as stated in certificate application.	(optional)
	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	(optional)
	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)
	User ID (UID)	Login ID of user	(optional)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	56A2DFF3E1841D1BA0FF7F3FF071188528F83DCD		
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement		(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection, id-kp-clientAuth, msEFS, msSCL		(mandatory) The values msEFS, msSCL are optional.
Subject Alternative Name	E-mail address of the subject		(mandatory)
	universalPrincipalName/Microsoft UPN (OID 1.3.6.1.4.1.311.20.2.3)		(optional)
Certificate Policies	Policy OID: 0.4.0.2042.1.1 (ETSI NCP) Policy OID: 2.16.756.1.89.2.1.13 (SwissSign NCP extended) CPSURI: https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf		
CRL Distribution Points	http://crl.swisssign.ch/cdp-26ab0cd6-f539-4f93-be04-39250cd56682		URLs of the CRL Distribution points (LDAP and/or HTTP)
Authority Information Access	caIssuers	http://aia.swisssign.ch/air-d8cd150b-23a8-4989-a18e-b683fdb5bb85	(mandatory)
	OCSP	http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec	(mandatory)
Microsoft Certificate Template	OID to designate the specific MS-Template		(optional)
	Integer to designate the «templateMajorVersion»		(optional)
	Integer to designate the «templateMinorVersion»		(optional)

3.3.3.4 Pro S/MIME E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 -- G22 –Default Profile, authentication

Field/Extension	Values	Comment
Version	Version 3	Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption or RSASSA-PSS with SHA-256	
Issuer Name	CN = SwissSign Personal 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)	GivenName Surname or pseudo: Pseudonym	(mandatory)
	GivenName	Subject's Given Name as stated in certificate application.	(optional)
	Surname	Subject's Surname Name as stated in certificate application.	(optional)
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
	SerialNumber	Unique number generated by the TSP.	(optional, only mandatory if Email missing)
	OrganizationalUnit (OU)	Organizational unit as stated in certificate application.	(optional)
	OrganizationName (O)	Subject (organisation) name as stated in certificate application.	(optional)
	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	(optional)
	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)
	User ID (UID)	Login ID of user	(optional) Used for smartcard-login
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	DA32F949F851CC9871660CD9CEB6DB923F094BEF		
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement		(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection, id-kp-clientAuth, msEFS, msSCL		(mandatory) The values msEFS, msSCLare optional.
Subject Alternative Name	E-mail address of the subject,		(mandatory)
	universalPrincipalName/Microsoft UPN (OID 1.3.6.1.4.1.311.20.2.3)		(optional)

Certificate Policies	Policy OID: 2.16.756.1.89.2.1.13 CPSURI: https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf Policy OID: 0.4.0.2042.1.1 (NCP)	
CRL Distribution Points	http://crl.swisssign.net/DA32F949F851CC9871660CD9CEB6DB923F094BEF ldap://directory.swisssign.net/CN=DA32F949F851CC9871660CD9CEB6DB923F094BEF%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	
Authority Information Access	caIssuers	http://swisssign.net/cgi-bin/authority/download/DA32F949F851CC9871660CD9CEB6DB923F094BEF	(mandatory)
	OCSP	http://ocsp.swisssign.net/DA32F949F851CC9871660CD9CEB6DB923F094BEF	(mandatory)

3.3.3.5 Pro S/MIME E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 – G22 – authentication, MS-Template

Field/Extension	Values	Comment
Version	Version 3	Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption	
Issuer Name	Please see the general profile in clause 3.3.3.3	
Subject DN	Please see the general profile in clause 3.3.3.3	
	User ID (UID)	(optional)
Valid from		Start of certificate validity.
Valid to		End of certificate validity.
Authority Key Identifier	Please see the general profile in clause 3.3.3.3	
Subject Key Identifier	Please see the general profile in clause 3.3.3.3	
Key Usage	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement	(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection, id-kp-clientAuth, msEFS, msSCL	(mandatory) The values msEFS, msSCL are optional.
Subject Alternative Name	E-mail address of the subject	(mandatory)
	universalPrincipalName/Microsoft UPN (OID 1.3.6.1.4.1.311.20.2.3)	(optional)
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.13 CPSURI: https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf Policy OID: 0.4.0.2042.1.1 (NCP)	
CRL Distribution Points	Please see the general profile in clause 3.3.3.3	
Authority Information Access	Please see the general profile in clause 3.3.3.3	

Microsoft Certificate Template	OID to designate the specific MS-Template	(mandatory)
	Integer to designate the «templateMajorVersion»	(mandatory)
	Integer to designate the «templateMinorVersion»	(mandatory)

3.3.3.6 E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 – G22 (NCP) – Document Signing only

Field/Extension	Values	Comment
Version	Version 3	Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption	
Issuer Name	Please see the general profile in clause 3.3.3.3	
Subject DN	Please see the general profile in clause 3.3.3.3	
Valid from		Start of certificate validity.
Valid to		End of certificate validity.
Authority Key Identifier	Please see the general profile in clause 3.3.3.3	
Subject Key Identifier	Please see the general profile in clause 3.3.3.3	(mandatory)
Key Usage	Please see the general profile in clause 3.3.3.3	
Extended Key Usage	id-kp-emailProtection, DocumentSigning, Authentic Documents Trust	(mandatory) Any combination of the EKU values is permissible.
Subject Alternative Name	Please see the general profile in clause 3.3.3.3	optional
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.13 CPSURI: https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf Policy OID: 0.4.0.2042.1.1 (NCP)	
CRL Distribution Points	Please see the general profile in clause 3.3.3.3	
Authority Information Access	Please see the general profile in clause 3.3.3.3	

3.3.3.7 Allowed exceptions for Common Name

Name Allowed exceptions with a fixed string in the common name in NCP certificates, with a then mandatory entry for /E-Mail are:

- "Secure Mail: Gateway Certificate"
- "Secure Mail: SEPPmail Certificate"
- "XnetSolutions Mailgateway"
- "Secure Mail: SX-Mail Crypt Certificate"
- "Secure E-Mail: SX-Mail Crypt Certificate"
- "Zertificon Mailgateway"
- "Z1 SecureMail Gateway Certificate"

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

4.2.1 SwissSign Personal Silver CA 2014 - G22 (CRL & OCSP only)

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number	544D64EAD1ED336D532405D00B936		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 Personal Silver CA 2014 - G22 O = SwissSign AG C = CH		Unique subject distinguished name of the certificate
Valid from	19 Sep 2014 20:36:49 UTC		Start of certificate validity.
Valid to	15 Sep 2029 20:36:49 UTC		End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0		Critical
Key Usage	Certificate Sign, CRL Sign		Critical
Subject Key Identifier	F0C7A33291B5EBCAB5587715A74EBE1A5D614325		
Authority Key Identifier	17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658		
Certificate Policies	Policy OID: 2.16.756.1.89.1.3.1.6 CPSURI: http://repository.swisssign.com/SwissSign-Gold-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	caIssuers	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	ABF481D8A1991E8CACDBB9BAA0969A710C596D8A
SHA256 Fingerprint	C9E40F4E83396F34A7C861817B4EDAB3DC1F8BAC699FD50CB261FA9123D55EF4

4.2.2 SwissSign Personal Silver CA 2008 - G2 (CRL & OCSP only)

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	E256B753976B7658	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 Personal Silver CA 2008 - G2, O = SwissSign AG, C = CH	Unique subject distinguished name of the certificate
Valid from	09 Jul 2008 11:11:09 UTC	Start of certificate validity.
Valid to	09 Jul 2023 11:11:09 UTC	End of certificate validity.
Basic Constraints	CA:TRUE, pathlen:0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	EB35B1566D156058F4E122CD1C461CAED0040065	
Authority Key Identifier	17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658	
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	caIssuers · http://swisssign.net/cgi-bin/authority/download/17A0CDC1E441B63A5B3BCB459DBD1CC298FA8658	
	OCSP · not included in this Issuing CA certificate	

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	2D28475232F981CDB73FE24250F76862CF236F5B
SHA256 Fingerprint	FA397DE8DB6F110A7FA34D101BAC8A914750F53B0223A8BD2FB812E757155C20

4.3 End-entity certificates

4.3.1 SwissSign E-Mail ID Silver Certificate issued by SwissSign Personal Silver CA 2014 – G22 (LCP), E-Mail only

Field/Extension	Values	Comment
Version	Version 3	Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption	

Issuer Name	CN = SwissSign Personal 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)	E-Mail address of Subject as stated in certificate application.	(mandatory)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	F0C7A33291B5EBCAB5587715A74EBE1A5D614325		(mandatory)
Subject Key Identifier	SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2		(mandatory)
Key Usage	digitalSignature, keyEncipherment, dataEncipherment		(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection		(mandatory)
Subject Alternative Name	E-mail address of the subject		(mandatory)
Certificate Policies	Policy OID: 2.16.756.1.89.2.1.11 CPSURI: https://repository.swissign.com/SwissSign_CPS_SMIME.pdf Policy OID: 0.4.0.2042.1.3 (LCP)		(mandatory)
CRL Distribution Points	http://crl.swissign.net/F0C7A33291B5EBCAB5587715A74EBE1A5D614325 ldap://directory.swissign.net/CN=F0C7A33291B5EBCAB5587715A74EBE1A5D614325,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/F0C7A33291B5EBCAB5587715A74EBE1A5D614325	(mandatory)
	OCSP	http://ocsp.swissign.net/F0C7A33291B5EBCAB5587715A74EBE1A5D614325	(mandatory)

4.3.2 SwissSign E-Mail ID Silver Certificate issued by SwissSign Personal Silver CA 2014 – G22 (LCP), email only & MS-Template

Field/Extension	Values	Comment
Version	Version 3	Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption	
Issuer Name	Please see the general profile in clause4.3.1	
Subject DN	Please see the general profile in clause 4.3.1	Unique subject distinguished name of the certificate
Valid from		Start of certificate validity.

Valid to		End of certificate validity.
Authority Key Identifier	Please see the general profile in clause 4.3.1	
Subject Key Identifier	Please see the general profile in clause 4.3.1	(mandatory)
Key Usage	digitalSignature, keyEncipherment, dataEncipherment	(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection	(mandatory)
Subject Alternative Name	E-mail address of the subject	(mandatory)
Certificate Policies	Please see the general profile in clause 4.3.1	
CRL Distribution Points	Please see the general profile in clause 4.3.1	
Authority Information Access	Please see the general profile in clause 4.3.1	
Microsoft Certificate Template	OID to designate the specific MS-Template	(mandatory)
	Integer to designate the «templateMajorVersion»	(mandatory)
	Integer to designate the «templateMinorVersion»	(mandatory)

4.3.3 SwissSign E-Mail ID Silver Certificate issued by SwissSign Personal Silver CA 2014 – G22 (LCP), organization entry

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	Please see the general profile in clause 4.3.1		
Subject DN			Unique subject distinguished name of the certificate
	Common Name (CN)	E-Mail address of Subject as stated in certificate application.	(mandatory)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional)
	OrganisationName (O)	Subject (organisation) name as stated in certificate application.	(mandatory)
	OrganizationalUnit (OU)	Organizational unit as stated in certificate application.	(optional)
	LocalityName (L)	Name of the locality as described in the certificate application	(optional)

	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)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	Please see the general profile in clause 4.3.1		
Subject Key Identifier	Please see the general profile in clause 4.3.1		(mandatory)
Key Usage	digitalSignature, keyEncipherment, dataEncipherment		(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection		(mandatory)
Subject Alternative Name	E-mail address of the subject		(mandatory)
Certificate Policies	Please see the general profile in clause 4.3.1		
CRL Distribution Points	Please see the general profile in clause 4.3.1		
Authority Information Access	Please see the general profile in clause 4.3.1		

4.3.4 SwissSign E-Mail ID Silver Certificate issued by SwissSign Personal Silver CA 2014 – G22 (LCP), organization entry & MS-Template

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption		
Issuer Name	Please see the general profile in clause 4.3.1		
Subject DN			Unique subject distinguished name of the certificate
	Common Name (CN)	E-Mail address of Subject as stated in certificate application.	(mandatory)
	Email	E-mail address of Subject as stated in certificate application.	(optional)
	Pseudonym	Subject's Pseudonym as stated in certificate application.	(optional)
	OrganisationName (O)	Subject (organisation) name as stated in certificate application.	(mandatory)
	OrganizationalUnit (OU)	Organizational unit as stated in certificate application.	(optional)
	LocalityName (L)	Name of the locality as described in the certificate application	(optional)

	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)
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Authority Key Identifier	Please see the general profile in clause 4.3.1		
Subject Key Identifier	Please see the general profile in clause 4.3.1		(mandatory)
Key Usage	digitalSignature, keyEncipherment, dataEncipherment		(mandatory) Critical extension, any combination of these key usages is permissible.
Extended Key Usage	id-kp-emailProtection		(mandatory)
Subject Alternative Name	E-mail address of the subject		(mandatory)
Certificate Policies	Please see the general profile in clause 4.3.1		
CRL Distribution Points	Please see the general profile in clause 4.3.1		
Authority Information Access	Please see the general profile in clause 4.3.1		
Microsoft Certificate Template	OID to designate the specific MS-Template		(mandatory)
	Integer to designate the «templateMajorVersion»		(mandatory)
	Integer to designate the «templateMinorVersion»		(mandatory)

4.3.5 Allowed exceptions for Common Name

Allowed exceptions with a fixed string in the common name, with a then mandatory entry for /E-Mail are:

- "Secure Mail: Gateway Certificate"
- "Secure Mail: SEPPmail Certificate"
- "XnetSolutions Mailgateway"
- "Secure Mail: SX-Mail Crypt Certificate"
- "Secure E-Mail: SX-Mail Crypt Certificate"
- "Zertificon Mailgateway"
- "Z1 SecureMail Gateway Certificate"

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 January 1, 1970 for non-issued certificates according to chapter 2.2 of RFC6960 (optional)
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 7.3
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 Definititon		Extended revoked extension according to chapter 2.2 and 4.4.8 of RFC6960 (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" 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. 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 Issing CA

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

7.   References

[1]   SwissSign CP LCP - Certificate Policy according to Lightweight Certificate Policy, published under:
      https://repository.swisssign.com

[2]   SwissSign CP NCP - Certificate Policy for according to Normalized Certificate Policy, published under:
      https://repository.swisssign.com

[3]   SwissSign CP NCP Extended - Certificate Policy for Normalized Certificate Policy with extended EKU, published under:
      https://repository.swisssign.com

[4]   SwissSign CPR S/MIME - Certificate, CRL and OCSP Profiles for S/MIME certificates, published under:
      https://repository.swisssign.com

[5]   SwissSign CPS S/MIME - Certification Practice Statement for for S/MIME 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 (2021-05)   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;