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:	14 June 2021
Version:	1.0
Obsoletes:	n/a
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

Authorization

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

Michael Günther (Qualified Signature)

Digital unterschrieben von Michael Günther (Qualified Signature)
Datum: 2021.06.11 12:02:35 +02'00'

digital signature

Markus Naef (Qualified Signature)

Digital unterschrieben von Markus Naef (Qualified Signature)
Datum: 2021.06.11 18:26:39 +02'00'

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 follwoing 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

3.2 Issuing CAs

3.2.1 SwissSign Personal Gold CA 2014 - G22

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	calssuers	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

3.2.2 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	caIssuers 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

3.3 End-entity certificates

3.3.1 E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 – G22 (NCP) – 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. Up to “valid from” plus 3 years

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	calssuers	http://swisssign.net/cgi-bin/authority/download/DA32F949F851CC9871660CD9CEB6DB923F094BEF	(mandatory)
	OCSP	http://ocsp.swisssign.net/DA32F949F851CC9871660CD9CEB6DB923F094BEF	(mandatory)

3.3.2 E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 – G22 (NCP) – with authentication

Field/Extension	Values		Comment
Version	Version 3		Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption or RSASSA-PSS with SHA-256		
Issuer Name	Please see the general profile in clause 3.3.1.		
Subject DN	Please see the general profile in clause 3.3.1. In addition:		
	User ID (UID)	Login ID of user	(optional) Used for smartcard-Logn
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.		
Subject Key Identifier	Please see the general profile in clause 3.3.1.		(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) MS UPN is present in certificates used for smartcard logon
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 3.3.1.	
Authority Information Access	Please see the general profile in clause 3.3.1.	

3.3.3 E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 – G22 (NCP) – 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 3.3.1.	
Subject DN	Please see the general profile in clause 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 3.3.1.	(mandatory)
Subject Key Identifier	Please see the general profile in clause 3.3.1.	(mandatory)
Key Usage	Please see the general profile in clause 3.3.1.	
Extended Key Usage	Please see the general profile in clause 3.3.1.	
Subject Alternative Name	Please see the general profile in clause 3.3.1.	
	universalPrincipalName/Microsoft UPN (OID 1.3.6.1.4.1.311.20.2.3)	(optional)
Certificate Policies	Please see the general profile in clause 3.3.1.	
CRL Distribution Points	Please see the general profile in clause 3.3.1.	
Authority Information Access	Please see the general profile in clause 3.3.1.	
Microsoft Certificate Template	OID to designate the specific MS-Template	(mandatory)
	Integer to designate the «templateMajorVersion»	(mandatory)
	Integer to designate the «templateMinorVersion»	(mandatory)

3.3.4 E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 – G22 (NCP) – Authentication, MS-Template

Field/Extension	Values	Comment
Version	Version 3	Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption	
Issuer Name	Please see the general profile in clause 3.3.1.	
Subject DN	Please see the general profile in clause 3.3.1.	
	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 3.3.1.	
Subject Key Identifier	Please see the general profile in clause 3.3.1.	
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 3.3.1.	
Authority Information Access	Please see the general profile in clause 3.3.1.	
Microsoft Certificate Template	OID to designate the specific MS-Template	(mandatory)
	Integer to designate the «templateMajorVersion»	(mandatory)
	Integer to designate the «templateMinorVersion»	(mandatory)

3.3.5 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 3.3.1.	
Subject DN	Please see the general profile in clause 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 3.3.1.	
Subject Key Identifier	Please see the general profile in clause 3.3.1.	(mandatory)
Key Usage	Please see the general profile in clause 3.3.1.	
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 3.3.1.	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 3.3.1.	
Authority Information Access	Please see the general profile in clause 3.3.1.	

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

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

The Issuing CA certificate is identified via the following fingerprints:

SHA1 Fingerprint	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	calssuers	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. Up to “valid from” plus 3 years
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.swisssign.com/SwissSign_CPS_SMIME.pdf Policy OID: 0.4.0.2042.1.3 (LCP)		(mandatory)
CRL Distribution Points	http://crl.swisssign.net/F0C7A33291B5EBCAB5587715A74EBE1A5D614325 ldap://directory.swisssign.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.swisssign.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	(optional)

		certificate application.	
	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	(optional)

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

The OCSP extensions used are specified below:

- Nonce

The ArchiveCutOff extension is not set in the OCSP responses.

5.2 OCSP Responder Certificate

Field/Extension	Value(s)		Comment
Version	Version 3		Certificate format version
Serial Number			Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption		
Issuer Distinguished name			Unique issuer distinguished name of the certificate (Root CA for the Issuing CA and the Issuing CA for the end entity certificate)
Subject Distinguished name	CommonName		Unique subject distinguished name of the OCSP Signer certificate. The CN shall include the string “OCSP Responder” and the reference to the Issuer.
	OrganizationName (O)	SwissSign AG	
	Country (C)	CH	
Valid from			Start of certificate validity.
Valid to			End of certificate validity.
Key Usage	digitalSignature		(mandatory)
Subject Key Identifier			(mandatory)
Authority Key Identifier			(mandatory)
Extended Key Usage	id-kp-ocspSigning		(mandatory)
Certificate Policies	Policy OID: CPSURI:		(optional)
ocspNoCheck			(mandatory)
CRL Distribution Points	Not included in this certificate		
Authority Information Access	Not included in this certificate		

6. CRL Profile

SwissSign issues CRLs in accordance to the guides of RFC 5280 [10].

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

Extension Attribute	Values	Comment
Version Number	V2	CRL format version pursuant to X.509.
Signature Algorithm	sha256WithRSAEncryption	Hash method and the signature algorithm used to sign the CRL pursuant to RFC 5280.
Issuer Distinguished Name		Unique issuer distinguished name of the certificate
Effective Date		Date and time of CRL issuance.
Next Update		Date and time of issuance of the next CRL. Maximum validity for CARL of the Root CA is 1 year after the publication of the CRL. The validity for CRLs provided by the Issuing CAs is 10 days. If it is the last CRL issued for those certificates in the scope of this CRL, the nextUpdate field in the CRL will be set to "99991231235959Z" as required by IETF RFC 5280.
Revocation List Number		CRL sequence number
Revoked Certificates:		List of the serial numbers and revocation dates of the revoked Certificate.
Serial Number		Serial number of the revoked certificate.
Revocation Date		Date and time of revocation of the certificate.
reasonCode		Reason code for certificate revocation. Not applicable for end-entity certificates.For CARL issued by the Root CA - reasonCode extension is present and not marked critical - possible reason codes in CARL: - cACompromise (2), or - cessationOfOperation (5)
Signature		Confirmation signature of the authority issued the CRL.
Authority Key Identifier		The Authority key identifier of the Issing CA

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

7. References

[1] SwissSign CP 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 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

[8] BRG: current version of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates;

[9] EVCG: current version of the Guidelines For The Issuance And Management Of Extended Validation Certificates;

[10] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

[11] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;

[12] RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

[13] RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;

[14] RFC 6962 – Certificate Transparency;

[15] ISO 3166 Codes;