Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT

Platform Services – Trust Backend
Swiss Government PKI

Swiss Government PKI

CA Layout and Policies

Version	2.19		
Status	in_Arbeit	in_Pruefung	genehmigt
	[ ]	[ ]	[x]

Personenkreis	
Autoren	Marcel Suter Jürgen Weber
Pruefung	SG Security
Genehmigung	SG PKI Leiter
Verteiler	SG PKI intern

Kontrolle			
Wann	**Version**	**Wer**	**Beschreibung**
14.04.2010	0.1	SuMa	Document created
10.05.2010	0.2	SuMa	Updates
13.07.2010	0.3	SuMa	Updates HSM & Slots & Backup/Restore
24.08.2010	0.4	SuMa	Updates following meeting 23.08.2010
25.08.2010	0.5	SuMa	DN qualifier updates
28.10.2010	0.6	SuMa	Merge suisseID & BP
17.11.2010	0.7	SuMa	Fixed typo added slot list
18.01.2011	0.8	SuMa	Removed old CA ref removed appendices fix pol.
19.01.2011	0.9	SuMa	Renamed KPMG alt name.
20.01.2011	0.10	SuMa	Renamed A CPS user notice.
27.01.2011	0.11	SuMa	Shortened CDP/AIA namings.
28.01.2011	0.12	SuMa	Updated table of content distribution list.
01.02.2011	0.13	SuMa	Updated names.
01.02.2011	0.14	SuMa	Updated names.
08.02.2011	0.15	SuMa	QC alt name update.
11.02.2011	1.0	SuMa	Visible string + validity update. Finalized version
19.04.2012	1.1	SuMa	Enhanced CA 02 (FUB)

Kontrolle			
16.09.2013	1.2	SuMa	End User Policies Enhanced CA 01 & Regular CA 01
17.09.2013	1.3	SuMa	Updated Governikus Policies
08.10.2013	1.4	SuMa	Added SPOC Policy
09.10.2013	1.5	SuMa	Added LRA System
11.10.2013	1.6	JoPa	New Policy ID for LRA Windows 7 System
25.10.2013	1.7	SuMa	Added FUB Class B Policies
03.12.2013	1.8	WeJ	Added TSA Qualified Policy Kap. 2.2.14
09.01.2014	1.9	SuMa	Fixed TSA Qualified Policy Kap. 2.2.14
24.02.2014	1.10	WeJ	Added End User Class A (Qualified)
20.03.2014	1.11	SuMa	Updated OID for ZKV to 2.16.756.1.17.3.22.25
14.04.2014	1.12	SuMa	Sedex policy for RaaS
28.04.2014	1.13	SuMa	Update SSL OID CP text
30.04.2014	1.14	SuMa	Added eDOC
01.05.2014	1.15	SuMa	Added SSL and EV SSL Sub CAs
06.06.2014	1.15	WeJ	Added SSL Server Authentication Policy
19.08.2014	1.16	WeJ	Added SSL Client Authentication Policy Added SSL Server / Client Authentication Policy
06.11.2014	1.17	WeJ	Added OCSP Policy
08.12.2014	1.18	WeJ	Added Regular Client Auth Policy
22.01.2015	1.19	WeJ	Added Regular Group Mailboxes Policy
23.03.2015	1.20	WeJ	Updated Time Stamping Policy
24.03.2015	1.21	WeJ	Added Process Authentication SSO-Portal Policy
26.03.2015	1.22	WeJ	Updated Root CA I policy for FUB Updated Enhanced CA 02 policy
01.04.2015	1.23	JoP	Migration of AdminCA-CD-T01 Policies to Regular
23.04.2015	1.27	DR	Added DFS/FKR Policy
06.05.2015	1.28	SuMa	Updated AKI in Enhanced CA 02
11.05.2015	1.29	SuMa	Updated Enhanced CA 02 end user CP OIDs
13.05.2015	1.30	SuMa	Updated Enhanced CA 02 end user DN according to reported FUB info #0000251 (Bug Mantis http://svn-blackhole.bfi.admin.ch:8080/mantis/view.php?id=251)
18.05.2015	1.31	SuMa	Renamed o=FUB with o=VBS in end user Enhanced CA 02 template
09.06.2015	1.32	KH	Added Klasse RegularCA01 certificate policies: Person Auth. Person Auth/Sign Person Auth/Sign/Encrypt Person Sign/Encrypt
12.06.2015	1.33	KH	Removed data encipherment key sage in policies OID 2.16.756.1.17.3.22.41 and 2.16.756.1.17.3.22.42 because it was not in line with RFC 5280 “4.2.1.3. Key Usage”
15.06.2015	1.34	KH	Added Klasse RegularCA01 certificate policies: Organization Auth/Sign Organization Auth/Sign/Encrypt Organization Sign/Encrypt
17.06.2015	1.35	KH	Added warnings: The usage of certain policies is not recommended due to inappropriate combination of key usages. This is based on an answer from FUB/IS Krypt dated 16.6.2015.
19.06.2015	1.36	KH	Added Klasse RegularCA01 certificate policies: System Auth System Auth/Sign System Auth/Sign/Encrypt System Sign/Encrypt
22.06.2015	1.37	WeJ	Extended FUB Policies with behavior attributes
23.06.2015	1.38	KH	In RegularCA01-Organization-Policies changed order of O/OU in the subject.

Kontrolle			
15.07.2015	1.39	KH	In RegularCA01-policies Person Organization System issuer changed 2.5.4.10 from „Admin“ to “Swiss Government PKI”
23.07.2015	1.40	SuMa	Updated FUB CDP
21.08.2015	1.41	WeJ	Corrected FUB End-Entity CDP
08.12.2015	1.42	WeJ	Added Class C – System Encryption Added SSL CA 01 – Domain Controller
22.12.2015	1.43	Ale	Added Class D – Organization Signature eSchKG BJ
02.02.2016	1.44	Ale	Added Class D – ElCom
07.02.2016	1.45	Ale	Updated Class D – Elcom
12.02.2016	1.46	WeJ	Updated Class D – ElCom
18.02.2016	1.47	Ale	Updatet Governikus Timestamp (Core Timestamp Certificate) Added Governikus Core Signature Certificate Added Governikus OSCI Transport Encryption Certificate Added Governikus OSCI Transport Signature Certificate
23.02.2016	1.48	WeJ	SSL Policy angepasst (Subject)
04.03.2016	1.49	WeJ	Updated eDoc Policy – o=Admin → o=admin in the subject attribute
29.03.2016	1.50	WeJ	Added Swiss Government Root CA III policy Added Swiss Government Public Trust Standard CA 02 policy Added EE CP issued by SG PT ST CA 02 policy
29.03.2016	1.51	MetB	Added CITES policy
04.04.2016	1.52	WeJ	Added Swiss Government Public Trust EV CA 02 policy Added EE CP issued by SG PT EV CA 02 policy Added Standard OCSP Responder policy Added EV OCSP Responder policy
06.04.2016	1.53	MetB	Updated subject for Organization certificates Auth/Enc/Sign policy
29.04.2016	1.54	Pascal Joye	Added 2 x code signing (standard & EV)
04.05.2016	1.55	Pascal Joye	Korrekturen von SecOffs
10.05.2016	1.56	Jürgen Weber	* Kap. 2 Swiss Government PKI CA Layout - Abb. 1 Grafik um Root CA III und SubCAs erweitert * Kap. 2.1 Naming Conventions - O=Admin auf O=Swiss Government PKI geändert - Tabelle 1 CN Particles um Root CA III und SubCAs erweitert * Kap. 2.4.6 Swiss Government Public Trust Standard CA 02 - Policy korrigiert * 2.4.6.4 Public Trust Standard OCSP Responder (2.16.756.1.17.3.62.7) - keyUsage korrigiert * bei allen End User Policies - certificatePolicies korrigiert * 2.4.8.2 Public Trust Standard Code Signing OCSP Responder (2.16.756.1.17.3.62.11) - neu erstellt * 2.4.9.2 Public Trust EV Code Signing OCSP Responder (2.16.756.1.17.3.62.12) - neu erstellt

Kontrolle			
11.05.2016	1.57	Jürgen Weber	Added subjectAltName to all ocsp policies
26.07.2016	1.58	Beatrice Metaj	• Added: *Kap. 2.4.3.2.4. Class B pre-staged – BV: Authentication Only (for A-Accounts or 2nd Token) (2.16.756.1.17.3.2.36) – neu erstellt • Added:*Kap. 2.4.3.2.5. Swiss Government Enhanced CA 02 OCSP Responder (2.16.756.1.17.3.2.39) – neu erstellt • Added: *Kap. 2.4.1.1.4. Swiss Government Enhanced CA 01 OCSP Responder (2.16.756.1.17.3.2.38) – neu erstellt • Added: *Kap. 2.4.2.1.6. Swiss Government Qualified CA 01 OCSP Responder (2.16.756.1.17.3.2.37) – neu erstellt • Added: *Kap. 2.4.4.3 Swiss Government Regular CA 01 OCSP Responder (2.16.756.1.17.3.22.62) – neu erstellt • Added: *Kap. 2.4.5.5. Swiss Government SSL CA 01 OCSP Responder (2.16.756.1.17.3.22.63) – neu erstellt
28.09.2016	1.59	Beatrice Metaj	• Added: *Kap. 2.4.4.1.16 Swiss Government Regular CA 01 Group Mailbox policy for Signature and Encryption only (2.16.756.1.17.3.22.64)– neu erstellt
02.11.2016	1.60	Jürgen Weber	• Added: OCSP Responder Certificate issued by SG Root CA III
09.12.2016	1.61	Jürgen Weber	• Changed: Set validity of EV certificates to 2 years
09.01.2017	1.62	Beatrice Metaj	• Added: *Kap. 2.4.2.1.5 Class B (BV): Authentication Only (for A-Accounts or 2nd Token) (OID: 2.16.756.1.17.3.2.40)
18.01.2017	1.63	Beatrice Metaj	Added: *Kap. 2.4.2.2. ff Class B: Enhanced Ca01 prestaged: • 2.16.756.1.17.3.2.41 Authentication Enhanced CA 01 prestaged • 2.16.756.1.17.3.2.42 Dsig Enhanced CA 01 prestaged • 2.16.756.1.17.3.2.43 Cipher Enhanced CA 01 pre-staged • 2.16.756.1.17.3.2.44 Authentication only Enhanced CA 01 Prestaged
20.01.2016	1.64	Jürgen Weber	Modified: • Kap. 2.4.1.1 SG Root CA III Responder • Kap. 2.4.6.5 Swiss Government SSL CA 01 OCSP Responder
02.02.2017	1.65	Jürgen Weber	Added: “Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL” in the subject remarks of each root/issuing CA
29.05.2017	1.66	Jürgen Weber	Updated: • 2.4.9.1 Public Trust Standard Code Signing (2.16.756.1.17.1.3.62.9)
17.07.2017	1.67	Beatrice Metaj	Added: *Kap 2.4.7.5 Policy for Public Trust standard CA 02 Browser Compatible Server/Client Auth (2.16.756.1.17.1.3.62.14)
16.08.2017	1.68	Michael von Niederhäusern	Updated: 2.4.7.5 according to the requirements of QuoVadis for Root Signing
18.08.2017	1.69	Antonio Alessio	Updated: 2.4.7.5 according the Baseline Requirements (Certificate valitity) and new AIA URL

Kontrolle			
29.08.2017	1.70	Beatrice Metaj	Added: *Kap 2.4.7.6 Policy for Public Trust standard CA 02 Browser Compatible Server/Client Auth SAN Keylenght 4096bit or higher (2.16.756.1.17.1.3.62.16)
03.10.2017	1.71	KH	Added Swiss Government Public Trust standard CA 03 policy
10.10.2017	1.72	KH	Added Public Trust Standard Server Authentication (2.16.756.1.17.3.62.17)
10.10.2017	1.73	KH	Added Public Trust Standard CA03 OCSP Responder (2.16.756.1.17.3.62.18)
12.10.2017	1.74	Jürgen Weber	Added: • 2.5.3.1.2 Geregeltes Behördenzertifikat (provisorisch) Reviewed: • Swiss Government Public Trust Standard CA 03 (2.16.756.1.17.3.61.6) • 2.5.8.1 Public Trust Standard CA03 Server Authentication (2.16.756.1.17.3.62.17) • 2.5.8.2 Public Trust Standard CA03 OCSP Responder (2.16.756.1.17.3.62.18)
25.10.2017	1.75	KH	Fixed 2.5.8.2 Public Trust Standard CA03 OCSP Responder: id-pkix-ocsp-nocheck only Dsig.
31.10.2017	1.76	Jürgen Weber	Policy für geregeltes Behördenzertifikat korrigiert. Updated: • 2.5.3.1.2 Geregeltes Behördenzertifikat
1.11.2017	1.77	KH	Fixed subject (L=Bern S=BE) in 2.5.8.2 Public Trust Standard CA03 OCSP Responder.
14.12.2017	1.78	MetB	Korrekturen in Kap. 2.5.3.1.2 geregelte Behördenzertifikate für falshe Auflösung des CDP Pfades und Note Textes (“” weggelassen)
20.12.2017	1.79	KH	“Löschen” von 1.3.6.1.5.5.7.2.2 - id-qt-unotice in “Public Trust Standard Browser Compatible Server”/”Client Authentication/Public Trust Standard Browser Compatible Server/Client Authentication SAN”
10.10.2018	1.80	StiD/EnkC	Added: • CP Swiss Government Root CA IV 2.16.756.1.17.3.5.0 • CP Swiss Government Regulated CA01 2.16.756.1.17.3.5.2.1 • CP Reguliertes Behördenzertifikat 2.16.756.1.17.3.5.2.2 • qualifiziertes EndUserzertifikat für Signatur 2.16.756.1.17.3.5.2.3 • Anpassung Gliederung – OCSP Responderzertifikat ist immer der erste Eintrag zu der jeweiligen Issuing CA

Kontrolle			
22.11.2018	1.81	EnkC	Modified: Korrektur in den Profilen von SG Qualified CA 01 – Seriennummer hinzugefügt SG Regulated CA 01 – LDAP CRL Pfad entfernt Anpassung der OCSP Responder Zertifikate jeder Sub CA Added: Kommentar zu basicConstraints ergänzt Moved: 4 Issuing CAs nach 2.6 Obsolte inklusive EU CPs • SG SuisseID Authetication CA 01 • SG EV SSL CA01 • SG PT EV SSL CA02 Added Object Identifier for OVCP and EVCP according CAB and ETSI in SSL OV certificates
21.02.2019	1.82	EnkC	Anpassung Policy OID für die Zertifikate der Regulated CA01
12.03.2019	1.83	EnkC	Aufnahme Regulated CA 02 Dekommissionierung Regulated CA01 Anpassung der EU Zertifikate de durch die Regulated CA02
13.03.2019	1.84	Ale	Aufnahme Authentication Enhanced CA 02 prestaged LRAO {id-adminpki}.2.49
16.04.2019	1.85	EnkC	Entfernung monetäres Limit in qcp-n-qccd Zertifikaten Aufnahme der Angabe von CertSerial und DN im Attribut IssuerKeyID im Root CAVI Zertifikat
03.05.2019	1.86	EnkC	Aufnahme id-qcs-pkixQCSyntax-v2 in die QC Statements der Leaf Zertifikate aus der RegulatedCA02
31.07.2019	1.87	EnC	Dekommissionierung Issuing CA: • SG EV SSL CA01 • SG PT EV CA02 • SG PT CS EV CA02 Ausserbetriebnahme EU Policies der dekommissionierten Issuing CAs
15.08.2019	1.88	EnC	BasicConstraints in EU Zertifikaten eingefügt
2.09.2019	1.89	KH	Added: 2.5.7.2.4 Class B (FUB): Authentication Only (for A-Accounts or 2nd Token) (OID: 2.16.756.1.17.3.2.50) (pre-staged)
18.12.2019	1.90	EnC	Added Policy for ClassC PersonSign (OID: 2.16.756.1.17.3.22.67) und PersonEnc (OID: 2.16.756.1.17.3.22.68)
22.01.2020	1.91	WeJ	Added Policy: SCMS Auth (OID: 2.16.756.1.17.3.2.51) SCMS Enc (OID: 2.16.756.1.17.3.2.52) SCMS DSig (OID: 2.16.756.1.17.3.2.53) SCMS Auth only (OID: 2.16.756.1.17.3.2.54) SCMS Auth 90 Days onl (OID: 2.16.756.1.17.3.2.55)
27.03.2020	1.92	EnC	FUB Authentication Only umbenannt in FUB LRAO Authentication Only (OID=2.16.756.1.17.3.2.50)
23.06.2020	1.93	EnC	Dekommissionierung Qualified CA01 / Ausserbetriebnahme EndUser Policies Qualified CA01

Kontrolle			
28.10.2020	1.94	EnC	Neuausstellung von issuing CAs im Rahmen Lifecycle • Enhanced CA03 • Enhanced CA04 • Enhanced CA05 • Regular CA02 • Regulated CA03
03.11.2020	1.95	EnC	Neues geregeltes Behördenzertifikat unter der Regulated CA02 hinzugefügt
20.02.2021	1.96	EnC	Hinzugefügt: • OCSP-Responder-Enhanced-CA03 • OCSP-Responder-Enhanced-CA04 • OCSP-Responder-Enhanced-CA05 • OCSP-Responder-Regular-CA02 • OCSP-Responder-Regulated-CA03
10.05.2021	1.97	EnC	Added policy for Geregeltes Behördenzertifikat für GGG (legal Person) (2.16.756.1.17.3.5.2.14)
26.10.2021	1.98	KH	Review-Versionen der End-Entity-Policies für die Regular CA02 erstellt.
3.12.2021	1.99	KH	Anpassung «subject» bei der End-Entity-Policies für die Regular CA02 erstellt (Organization/System).
03.03.2022	2.0	EnC	Finalisiserung der Endentity Zertifikate der Regulated CA03
11.05.2022	2.01	KH	Den LDAP-Pfad beim Feld «crlDistributionPoints» der End-Entity-Policies für die Regular CA02 entfernt.
15.06.2022	2.02	JoP	Update Document Header (Platform Services – Trust)
30.06.2022	2.03	LvMa	Add a policy for ZKV (Zollkundenverwaltung) OID 2.16.756.1.17.3.62.29
06.07.2022	2.04	GoSt WeJ	Korrektur OCSP-Responder Root CA II Policy 22.64 nach 22.65 (gemäss OID Dokument)
19.08.2022	2.1	Jop	Replace SG-Root-CAIII-OCSP-Responder by SG-Root-CAIV-OCSP-Responder in subject attribute of 2.5.4.1 (OID 2.16.756.1.17.3.5.2.5) Replace "Qualified CA01" by "Regulated CA02" in ***Verwendungszweck*** of 2.5.10.3 (OID 2.16.756.1.17.3.5.2.2) Add new Chapt 2.5.11.5 for Class A Qualified Digtital Signature (natural Person for TW4S)
17.11.2022	2.11	LvMA, GoSt	Add a policy for eDoc (Systemplattform eDokumente) 2.16.756.1.17.3.62.30
17.11.2022	2.12	LvMA, GoSt	Add a policy for Sedex 2.16.756.1.17.3.62.31
17.11.2022	2.13	LvMA, GoSt	Remove Space from CRL Distribution Point at new Sedex Policy
15.12.2022	2.14	KH	Corrected EnhancedCA02 OID from 2.16.756.1.17.3.1.0 to 2.16.756.1.17.3.1.5 to match "Object Identifiers (OID)" and issued certificate
23.1.2023	2.15	KH	Moved Policy OID 2.16.756.1.17.3.5.2.6 from RegulatedCA03 to RegulatedCA02 and set parameters. i.e from chap. 2.5.11.5 to chap.. 2.5.10.7 Class A Qualified Digital Signature (Signaturdienst) (natural Person) (2.16.756.1.17.3.5.2.6) to match issed certificates

Kontrolle			
23.1.2023	2.16	KH	Added alternative policy OIDs to match issued certificates: chap. 2.5.6.3.1 Authentication (2.16.756.1.17.3.2.33 or 2.16.756.1.17.3.2.15) chap. 2.5.6.3.2 Digital Signature (2.16.756.1.17.3.2.34 or 2.16.7 56.1.17.3.2.11) chap. 2.5.6.3.3 Encryption (2.16.756.1.17.3.2.35 or 2.16.756.1.17.3.2.10)
30.1.2023	2.17	KH	Fixed obvious typos in 2.5.14.3 SSL Client Authentication (2.16.756.1.17.3.22.27) (old) 2.16.756.1.17.3.2.27 to (new) 2.16.756.1.17.3.22.27 2.5.14.4 SSL Server / Client Authentication (2.16.756.1.17.3.22.10) (old) 2.16.756.1.17.3.2.10 to (new) 2.16.756.1.17.3.22.10
31.1.2023	2.18	KH	Moved Policy OID 2.16.756.1.17.3.5.2.13 from RegulatedCA03 to RegulatedCA02 and set parameters i.e. 2.5.11.4 to chap.. 2.5.10.8 Class A Qualified Digital Signature (Signaturdienst) (Natural Person) (2.16.756.1.17.3.5.2.13)) to match issued certificates.
9.2.2023	2.19	KH	Updated PKI Layout figures.

Content

1 Purpose

The purpose of this document is to define the new Root and SubCA certificate policies and chaining layout. It is assumed that the reader is familiar with the Swiss Government PKI environment.

2 Swiss Government PKI CA Layout

The renewal of the new Root and Sub CAs gets rid of the obsolete hashing and signing algorithm in addition to:.

- The obsolete hashing and signing algorithm SHA1 with RSAEncryption get replaced with the sha256WithRSAWithEncryption Signature for all new Root and sub CAs
- The keys sizes of the CA and SubCAs get all pumped up to 4096 bit
- All the SWKP HSM get phased out and replaced with SafeNet HW
- All encoding rules for naming conventions (issuer and subject) implement the ASN.1 UTF8String as defined in X509:2005
- Renaming of the CA instances to reflect new naming convention.
- Obsolete X500 names in CDP get dropped. LDAP/URL/OCSP URIs get used in place.
- AIA extension get introduced for SubCAs

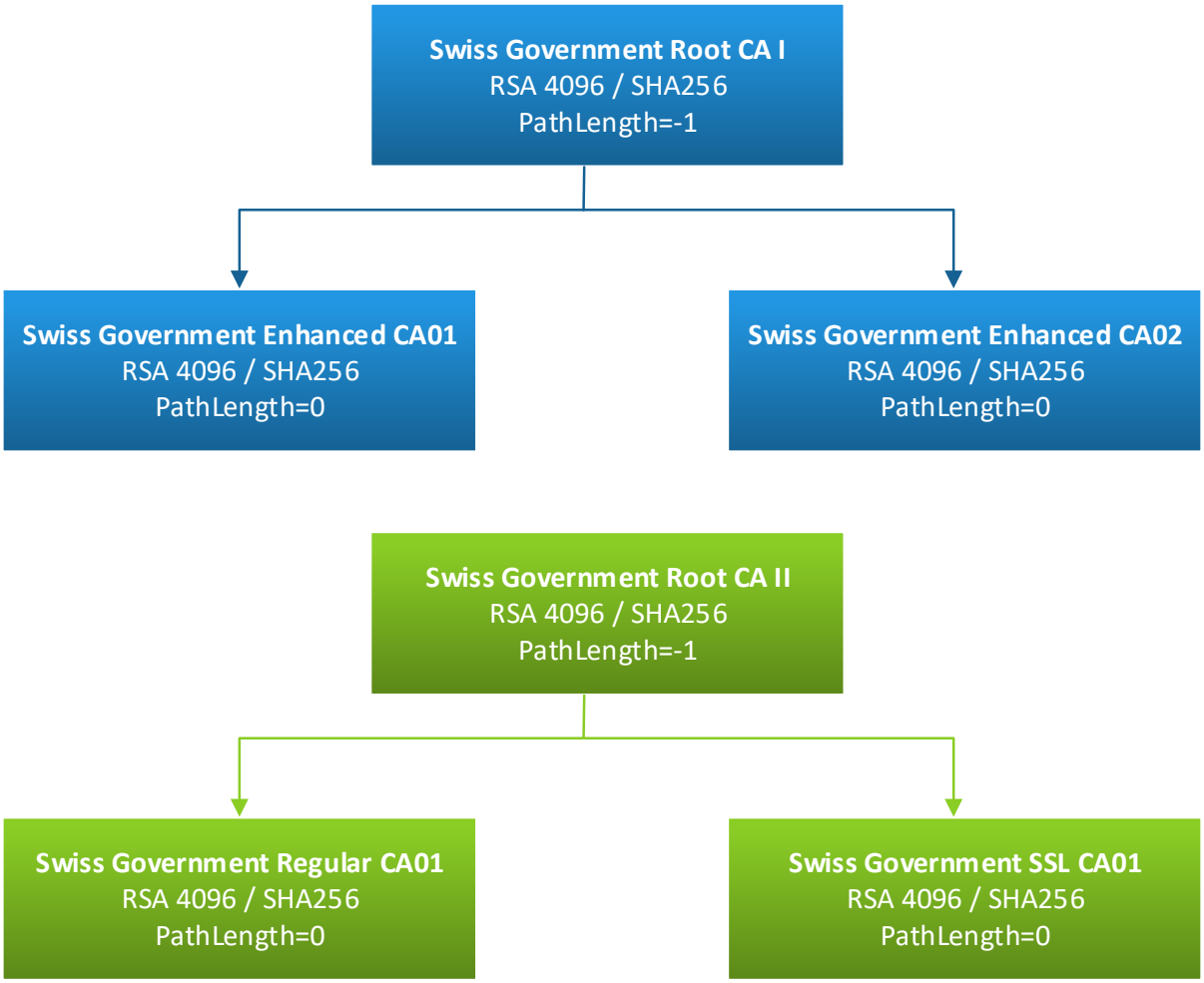

Figure 1: Renewed PKI Layout Root CA I/II

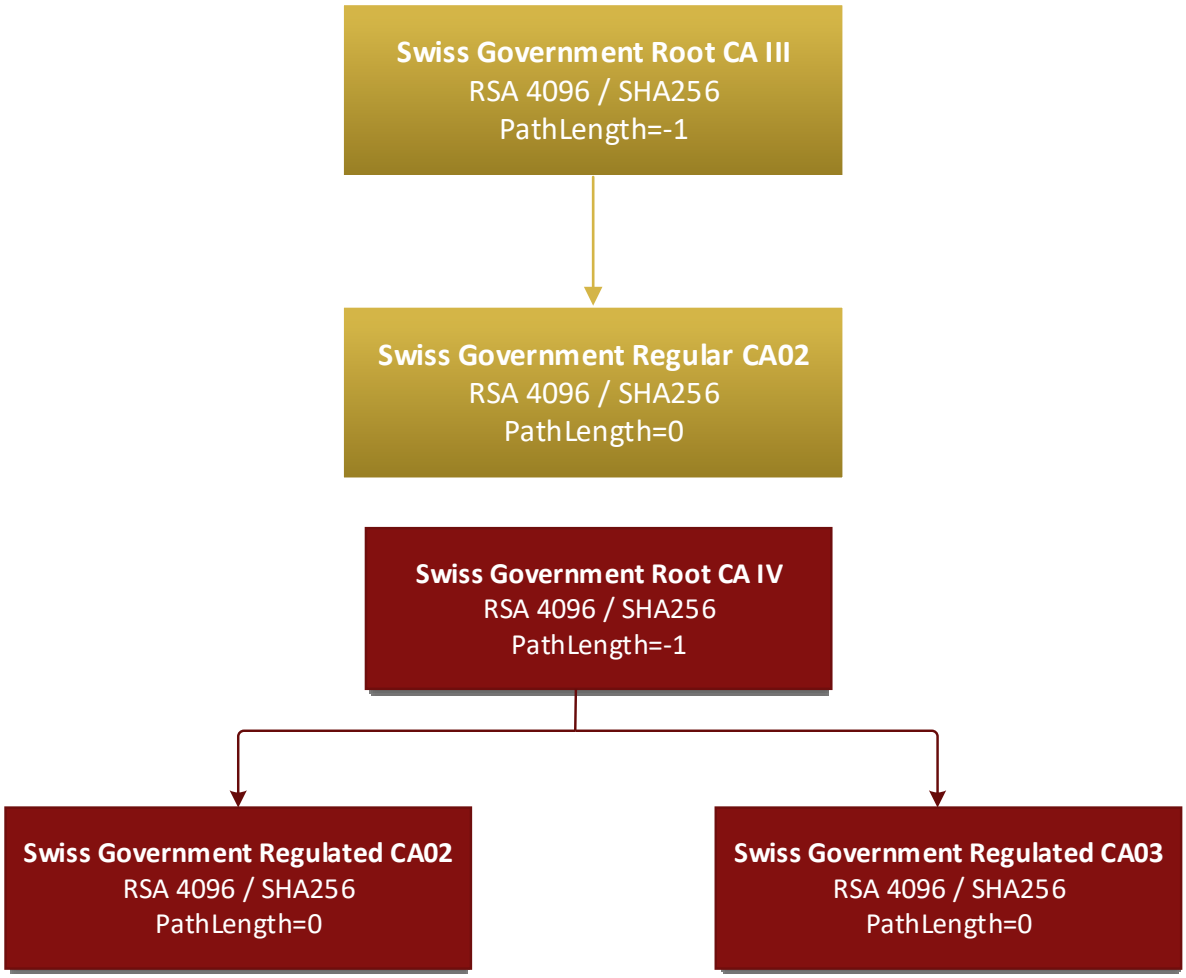

Figure 2: Renewed PKI Layout Root CA III/IV

2.1 Naming Conventions

The CA and sub CA Subject Distinguished Names are defined as in:

Root I II III:

C = CH
O = Swiss Government PKI
OU = Services
OU = Certification Authorities
CN = Swiss Government <<Specifics>> where <<Specifics>> is replaced with

Root IV:

C = CH
O = Bundesamt für Informatik und Telekommunikation (BIT)
OU = Swiss Government PKI
CN = Swiss Government <<Specifics>> where <<Specifics>> is replaced with

Tabelle 1 CN Particles

CN particle in <<TBD>>	Class	Obsoletes
Root CA I	New Root CA Classes A & B	AdminRootCA
Root CA II	New Root CA Classes C & D	New
Root CA III	New Root CA Class C (Public Trust)	New
Root CA IV	New Root CA Class A	Root CA I Class A
Qualified CA 01	New Issuing CA Class A	AdminCA-A-T01
Regulated CA 02	New Issuing CA Class A	Qualified CA 01
Enhanced CA 01	New Issuing CA Class B	Admin-CA3
Enhanced CA 02	New Issuing FUB CA	New
Regular CA 01	New Issuing Class C & D	AdminCA-CD-T01
SSL CA01	Issuing CA Class C	
Public Trust Standard CA 02	New Issuing CA Class C (Public Trust)	New
Public Trust Code Signing Standard CA 02	New Issuing CA Class C (Public Trust)	New
Public Trust Standard CA 03	New Issuing CA Class C (Public Trust)	New

CN particle in <<TBD>>	Class	decommissioned
EV SSL CA01	Issuing CA Class C (Public Trust)	29.07.2019
Public Trust EV CA 02	New Issuing CA Class C (Public Trust)	29.07.2019
Public Trust Code Signing EV CA 02	New Issuing CA Class C (Public Trust)	29.07.2019

2.2 Common Object Identifiers (OID)

OID	Short	Description
1.2.840.113549.1.1.11	sha256WithRSASignature	
0.4.0.194112.1.0	QCP-n	certificate policy for EU qualified certificates issued to natural persons
0.4.0.194112.1.1	QCP-l	certificate policy for EU qualified certificates issued to legal persons
0.4.0.194112.1.2	QCP-n-qscd	certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD
0.4.0.194112.1.3	QCP-l-qscd	certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD
0.4.0.194112.1.4	QCP-w	certificate policy for EU qualified website authentication certificates
0.4.0.2042.1.1	NCP	Normalized Certificate Policy
0.4.0.2042.1.2	NCP+	Normalized Certificate Policy requiring a secure cryptographic device
0.4.0.2042.1.3	LCP	Lightweight Certificate Policy
0.4.0.2042.1.4	EVCP	Extended Validation Certificate Policy auch CAB-EVCP 2.23.140.1.1
0.4.0.2042.1.6	DVCP	Domain Validation Certificate Policy auch CAB-DVCP 2.23.140.1.2.1
0.4.0.2042.1.7	OVCP	Organizational Validation Certificate Policy auch CAB-OVCP 2.23.140.1.2.2
0.4.0.2042.1.2	IVCP	Individual Validation Certificate Policy auch CAB-IVCP 2.23.140.1.2.3
2.23.140.1.3	CAB-CodeSigning EV	
2.23.140.1.31	CAB-.onion EVCP	
2.23.140.2.1	CAB-TestCertificates	
2.23.140.1.2.1	CAB-DVCP	Domain Validation Certificate Policy
2.23.140.1.2.2	CAB-OVCP	Organization Validation Certificate Policy
2.23.140.1.1	CAB-EVCP	Extended Validation Certificate Policy

2.3 Root CA Policies

2.3.1 Swiss Government Root CA I (2.16.756.1.17.3.1.0)

Verwendungszweck:

Wurzel Instanz zur Ausgabe von Issuing CAs zur Herausgabe der Klasse A und Klasse B Endbenutzer Zertifikate.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	Version MUST be 3 (value is 2)
serialNumber	00fd75048d7a608693694caa003c65d33d	Random
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	PrintableString directoryName CAs MUST use either the PrintableString or UTF8String encoding of DirectoryString
validity		
notBefore	“110215090000Z”	UTC TIME ETSI TS 102 280
notAfter	“350215085959Z”	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the ARL When the subject of the certificate is a CA the subject field MUST be encoded in the same way as it is encoded in the issuer field
subjectPublicKeyInfo		

X.509 Field	OIDs/Values	Comments
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	4096 bit	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN + Cert Serial
extnValue	160 bit	OCTET STRING 160 bit SHA1 of root subjectPublicKey BIT STRING + authority DN
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	160 bit	OCTET STRING 160 bit SHA1 BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'B (0x06)	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	1.3.6.1.5.5.7.2.1: http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	PKIX CPS Pointer Qualifier IA5String id-qt-cps RFC 5280
	1.3.6.1.5.5.7.2.2: This is the Swiss Government Root CA I CPS	PKIX policy qualifier unotice VisibleString id-qt-unotice RFC 5280
crlDistributionPoints		
extnId	2.5.29.31	

X.509 Field	OIDs/Values	Comments
extnValue	ldap://admindir.admin.ch:389/cn=Swiss Government Root CA Iou=Certification Authori-tiesou=Serviceso=Adminc=CH	ldap uri IA5String for CA Swiss GovernmentRoot CA I CDPs
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	-1	INTEGER indefinite child CA

2.3.2 Swiss Government Root CA II (2.16.756.1.17.3.21.1)

Verwendungszweck:

Wurzel Instanz zur Ausgabe von Issuing CAs zur Herausgabe der Klasse C und Klasse D Endbenutzer Zertifikate.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	Version MUST be 3 (value is 2)
serialNumber	0e9f1799a5b13d9ccbec06eba3f00e69	Unique random positive integer
issuer	2.5.4.6:CH 2.5.4.10:The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA II	PrintableString directoryName
validity		
notBefore	“110216090000Z”	UTC TIME ETSI TS 102 280
notAfter	“350216085959Z”	UTC TIME ETSI TS 102 280

X.509 Field	OIDs/Values	Comments
subject	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA II	PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the ARL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	4096 bit	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN + Cert Serial
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	‘000001100’B (0x06)	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.32	
extnValue	1.3.6.1.5.5.7.2.1: http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	PKIX CPS Pointer Qualifier IA5String id-qt-cps RFC 5280
	1.3.6.1.5.5.7.2.2: This is the Swiss Government Root CA II CPS	PKIX policy qualifier unotice VisibleString id-qt-unotice RFC 5280
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	ldap://admindir.admin.ch:389/cn=Swiss Government Root CA II ou=Certification Authoritiesou=Serviceso=Adminc=CH	ldap uri IA5String CA Swiss Government Root CA II CDPs
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	-1	INTEGER indefinite child CA

2.3.3 Swiss Government Root CA III (2.16.756.1.17.3.61.0)

Verwendungszweck:

Public Trusted Wurzel Instanz zur Ausgabe von Issuing CAs zur Herausgabe der Klasse C Zertifikate.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	Version MUST be 3 (value is 2)
serialNumber	00fb1f0b422ba8413e57d1ee2a6e5a4fbb	Unique random positive integer with 20-bit entropy according to Base-line Requirements
issuer	2.5.4.6:CH 2.5.4.10:Swiss Government PKI	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.11:www.pki.admin.ch 2.5.4.3:Swiss Government Root CA III	
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"350216085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:www.pki.admin.ch 2.5.4.3:Swiss Government Root CA III	PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the ARL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	4096 bit	BIT STRING 4096 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN + Cert Serial
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'B (0x06)	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	

X.509 Field	OIDs/Values	Comments
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies	NOT SET	
extnId		
extnValue		
crlDistributionPoints	NOT SET	
extnId		
extnValue		
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	-1	INTEGER indefinite child CA

2.3.4 Swiss Government Root CA IV (2.16.756.1.17.3.5.0)

Verwendungszweck:

Ausstellung regulierter und qualifizierter Zertifikate nach ZertES für natürliche und juristische Personen

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	Version MUST be 3 (value is 2)

X.509 Field	OIDs/Values	Comments
serialNumber	….	Unique random positive integer with 20-bit entropy according to Base-line Requirements
issuer	2.5.4.3:Swiss Government Root CA IV 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	PrintableString directoryName When the subject of the certificate is a CA the subject field MUST be encoded in the same way as it is encoded in the issuer field
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"350216085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11: Swiss Government PKI 2.5.4.3:Swiss Government Root CA IV	PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the ARL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	4096 bit	BIT STRING 4096 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	Issuer KeyID + DN + Cert Serial
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'B (0x06)	RFC 5280
digitalSignature	0	
nonRepudiation	0	

X.509 Field	OIDs/Values	Comments
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	
encipherOnly	0	
decipherOnly	0	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN

2.4 Issuing CA Policies

2.4.1 Swiss Government Enhanced CA 01 (2.16.756.1.17.3.1.0)

Verwendungszweck:

Ausstellung von Klasse B Zertifikaten.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	Version MUST be 3 (value is 2)
serialNumber	4e7d310e85118a04638d703e6f9bd458	Unique random positive integer

X.509 Field	OIDs/Values	Comments
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	UTF8String directoryName
validity		
notBefore	"110215090000Z"	UTC TIME ETSI TS 102 280
notAfter	"250215085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	4096 bit	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue	160 bit	OCTET STRING 160 bit0 SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'B (0x06)	keyCertSign (bit 5) cRLSign (bit 6)
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.1.0	
extnId	1.3.6.1.5.5.7.2.2	PKIX policy qualifier unotice
extnValue	This is the Swiss Government Root CA I CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	PKIX CPS Pointer Qualifier
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAI.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA I ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Root CA I CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	Certificate Authority Information Access OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAI.crt	uri IA5String

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.4.2 Swiss Government Enhanced CA 02 (2.16.756.1.17.3.1.5)

Verwendungszweck:

Ausstellung von Klasse B Zertifikaten.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
Signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	Version MUST be 3 (value is 2)
serialNumber	540cd9627e1b2261eb103014b2d08a5a	Unique random positive integer
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	PrintableString directoryName
validity		
notBefore	"1505281402200Z" (28. Mai 2015 14:22:21)	UTC TIME ETSI TS 102 280
notAfter	"30052814222200Z" (28. Mai 2030 14:22:21)	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities	UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL

X.509 Field	OIDs/Values	Comments
	2.5.4.3:Swiss Government Enhanced CA 02	
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	4096 bit	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue		OCTET STRING 160 bit0 SHA1 of BIT STRING (not including S/N and GN)
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue		OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	‘000001100	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.1.5	
extnId	1.3.6.1.5.5.7.2.2	

X.509 Field	OIDs/Values	Comments
extnValue	This is the Swiss Government Root CA I CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAI.crl http://www.technical-pki.admin.ch/crl/RootCAI.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA I ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Root CA I CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAI.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.4.3 Swiss Government Enhanced CA 03 (2.16.756.1.17.3.1.6)

Verwendungszweck:

Ausstellung von Klasse B Zertifikaten für die Kantone.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	Version MUST be 3 (value is 2)
serialNumber		Unique random positive integer
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	UTF8String directoryName
validity		
notBefore	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280
notAfter	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280
subject	2.5.4.3: Swiss Government Enhanced CA 03 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	4096 bit	BIT STRING 4096 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
extnId	2.5.29.35	Cert Serial
extnValue	160 bit	OCTET STRING 160 bit0 SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'B (0x06)	keyCertSign (bit 5) cRLSign (bit 6)
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.1.6	
extnId	1.3.6.1.5.5.7.2.2	PKIX policy qualifier unotice
extnValue	This is the Swiss Government Root CA I CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	PKIX CPS Pointer Qualifier
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAI.crl	uri IA5String CA Swiss Government Root CA I CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	Certificate Authority Information Access OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAI.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.4.4 Swiss Government Enhanced CA 04 (2.16.756.1.17.3.1.7)

Verwendungszweck:

Ausstellung von Klasse B Zertifikaten für die Bundesverwaltung.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	Version MUST be 3 (value is 2)

X.509 Field	OIDs/Values	Comments
serialNumber		Unique random positive integer
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	UTF8String directoryName
validity		
notBefore	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280
notAfter	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280
subject	2.5.4.3:Swiss Government Enhanced CA 04 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	4096 bit	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue	160 bit	OCTET STRING 160 bit0 SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'B (0x06)	keyCertSign (bit 5) cRLSign (bit 6)
digitalSignature	0	

X.509 Field	OIDs/Values	Comments
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.1.7	
extnId	1.3.6.1.5.5.7.2.2	PKIX policy qualifier unotice
extnValue	This is the Swiss Government Root CA I CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	PKIX CPS Pointer Qualifier
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAI.crl	uri IA5String ldap uri IA5String CA Swiss Government Root CA I CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	Certificate Authority Information Access OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	

X.509 Field	OIDs/Values	Comments
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAI.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.4.5 Swiss Government Enhanced CA 05 (2.16.756.1.17.3.1.8)

Verwendungszweck:

Ausstellung von Klasse B Zertifikaten für das FUB.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	Version MUST be 3 (value is 2)
serialNumber	4e7d310e85118a04638d703e6f9bd458	Unique random positive integer
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	UTF8String directoryName
validity		
notBefore	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280
notAfter	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280

X.509 Field	OIDs/Values	Comments
subject	2.5.4.3:Swiss Government Enhanced CA 05 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	4096 bit	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue	160 bit	OCTET STRING 160 bit0 SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	160 bit	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'B (0x06)	keyCertSign (bit 5) cRLSign (bit 6)
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.1.8	
extnId	1.3.6.1.5.5.7.2.2	PKIX policy qualifier unotice
extnValue	This is the Swiss Government Root CA I CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	PKIX CPS Pointer Qualifier
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAI.crl	uri IA5String CA Swiss Government Root CA I CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	Certificate Authority Information Access OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAI.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.4.6 Swiss Government Regular CA 01 (2.16.756.1.17.3.21.1)

Verwendungszweck:

Ausstellung von Klasse C Zertifikaten.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA II	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"250216085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey		BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue		OCTET STRING 160 bit SHA1 ofBIT STRING

X.509 Field	OIDs/Values	Comments
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue		OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRU	BOOLEAN
extnValue	‘000001100	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.21.1	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Root CA II CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA IIou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Root CA II CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.4.7 Swiss Government Regular CA 02 (2.16.756.1.17.3.61.7)

Verwendungszweck:

Ausstellung von Klasse C Zertifikaten.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10:Swiss Government PKI	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.11:www.pki.admin.ch 2.5.4.3:Swiss Government Root CA III	
validity		
notBefore	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280
notAfter	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280
subject	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey		BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue		OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue		OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRU	BOOLEAN
extnValue	'000001100	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	

X.509 Field	OIDs/Values	Comments
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.61.7	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Root CA III CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	https://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	https://www.pki.admin.ch/crl/RootCAIII.crl	uri IA5String Swiss Government Root CA III CDP
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	https://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.4.8 Swiss Government SSL CA 01 (2.16.756.1.17.3.21.2)

Verwendungszweck:

CRL issuing only

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bitYYYYYYY	4096 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	Random	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer.
signature		
algorithm	1.2.840.113549.1.1.11: sha256WithRSASignature	This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate. This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence Certificate. The contents of the optional parameters field will vary according to the algorithm identified.
parameters	NUL	
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA II	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName

X.509 Field	OIDs/Values	Comments
validity		
notBefore	"140515090000Z"	UTC TIME ETSI TS 102 280
notAfter	"280515085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government SSL CA 01	The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name MAY be carried in the subject field and/or the subjectAltName extension. If the subject is a CA then the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject CA. UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey		BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue		OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue		OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'	certSign crlSign
digitalSignature	0	
nonRepudiation	0	

X.509 Field	OIDs/Values	Comments
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.21.2	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this subordinate CA is for SSL server issuance only.	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/SSLCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government SSL CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Root CA II CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers

X.509 Field	OIDs/Values	Comments
accessLocation	http://www.pki.admin.ch/aia/SSLCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.4.9 Swiss Government Regulated CA 02 (2.16.756.1.17.3.5.1.2)

Verwendungszweck:

Issuing CA: Swiss Government Regulated CA 01

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxxxxx	Random
issuer	2.5.4.3:Swiss Government Root CA IV 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"110215090000Z"	UTC TIME ETSI TS 102 280
notAfter	"250215085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.3:Swiss Government Regulated CA 02 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:VATCH-CHE-221.032.573	UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b)

X.509 Field	OIDs/Values	Comments
	2.5.4.6:CH	2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name) 2.5.4.97: organisationIdentifier (ETSI EN 319 412-2 V2.1.1 4.2.3.1 Legal person issuers TAV 2.3.2 b))
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	Issuier KeyID
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	

X.509 Field	OIDs/Values	Comments
extnValue	2.16.756.1.17.3.5.1.2	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is an issuing CA regulated certificate as defined by the Swiss federal law SR 943.03 ZertES	UTF8String encoding id-qt-unotice RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d). Dies liegt zwar in einem Widerspruch zur Definition in rfc5280: „To prevent such duplication this qualifier SHOULD only be present in end entity certificates and CA certificates issued to other organizations.") Der ausführlichere Text wäre für relying Parties aussagekräftiger
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	uri IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAIV.crl	uri IA5String ldap uri IA5String CA inherits CDPs LDAP Eintrag entfernen Grund – Redesign AdminDir
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIV.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.4.10 Swiss Government Regulated CA 03 (2.16.756.1.17.3.5.1.3)

Verwendungszweck:

Issuing CA: Swiss Government Regulated CA 01

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxxxxx	Random
issuer	2.5.4.3:Swiss Government Root CA IV 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"xxxxxxxxx090000Z"	UTC TIME ETSI TS 102 280
notAfter	"250215085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.3:Swiss Government Regulated CA 03 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name) 2.5.4.97: organisationIdentifier (ETSI EN 319 412-2 V2.1.1 4.2.3.1 Legal person issuers TAV 2.3.2 b))
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	.....	BIT STRING 4096 bit

X.509 Field	OIDs/Values	Comments
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	Issuier KeyID
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.1.3	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is an issuing CA regulated certificate as defined by the Swiss federal law SR 943.03 ZertES	UTF8String encoding id-qt-unotice RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d). Dies liegt zwar in einem Widerspruch zur Definition in rfc5280: „To prevent such duplication this qualifier SHOULD only be present in end entity certificates and CA certificates issued to other organizations.") Der ausführlichere Text wäre für relying Parties aussagekräftiger

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.1	
extnValue	https://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	uri IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	https://www.pki.admin.ch/crl/RootCAIV.crl	uri IA5String ldap uri IA5String CA inherits CDPs LDAP Eintrag entfernen Grund – Redesign AdminDir
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	https://www.pki.admin.ch/aia/RootCAIV.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.5 End Entity Policies

2.5.1 Swiss Government Root CA I

2.5.1.1 SG Root CA I OCSP Responder (2.16.756.1.17.3.2.48)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
Signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
Version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	05d63b76f2ec8fd474c62aea141b1cbf	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"yymmddhhmmssZ" (Montag 5. November 2018 13:23:47)	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhmmssZ" (Dienstag 5. November 2019 13:23:47)	UTC TIME ETSI TS 102 280 (3 years)

X.509 Field	OIDs/Values	Comments
subject	2.5.4.6:CH 2.5.4.10: Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11: Swiss Government PKI 2.5.4.3: OCSP-Responder SG-Root-CAI	Printable String
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0x80	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	

X.509 Field	OIDs/Values	Comments
extnValue	2.16.756.1.17.3.2.48	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.2 Swiss Government Root CA II

2.5.2.1 SG Root CA II OCSP Responder (2.16.756.1.17.3.22.65)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	

X.509 Field	OIDs/Values	Comments
Signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
Version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CAII	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280 (1 year)
subject	2.5.4.6:CH 2.5.4.10: Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11: Swiss Government PKI 2.5.4.3: OCSP-Responder-RootCAII	Printble String
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	

X.509 Field	OIDs/Values	Comments
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0x80	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.65	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.3 Swiss Government Root CA III

2.5.3.1 SG Root CA III OCSP Responder (2.16.756.1.17.3.62.13)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
Signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
Version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN).

X.509 Field	OIDs/Values	Comments
	2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA III	PrintableString directoryName
validity		
notBefore	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10: Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11: Swiss Government PKI 2.5.4.3: OCSP-Responder-RootCAIII-	Printable String
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '10'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	

X.509 Field	OIDs/Values	Comments
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.13	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.4 Swiss Government Root CA IV

2.5.4.1 SG Root CA IV OCSP Responder (2.16.756.1.17.3.5.2.5)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
Signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
Version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.3:Swiss Government Root CA IV 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3:SG-Root-CAIV-OCSP-Responder 2.5.4.11: Swiss Government PKI 2.5.4.10: Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	Printable String UTF 8
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0x80	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.5	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	

X.509 Field	OIDs/Values	Comments
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.5 Swiss Government Enhanced CA01

2.5.5.1 Swiss Government Enhanced CA 01 OCSP Responder (2.16.756.1.17.3.2.38)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
Signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
Version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative

X.509 Field	OIDs/Values	Comments
		integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.3:EnhancedCA01-OCSP-Responder	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '10'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	

X.509 Field	OIDs/Values	Comments
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.38	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
extnValue	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.5.2 Class B (BV): Authentication Only (for A-Accounts or 2nd Token) (OID: 2.16.756.1.17.3.2.40) (standard)

Verwendungszweck:

Authentication certificate for special access rights – issuing with wizard.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.40	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Authentication only of the Swiss Government Enhanced CA 01	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.5.3 Class B – Standard

2.5.5.3.1 Authentication (2.16.756.1.17.3.2.15)

Verwendungszweck:

Standard Class B certificate for Authentication

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit

X.509 Field	OIDs/Values	Comments
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	Digital Signature
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.15	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Enhanced CA 01 CPS for end users	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	

X.509 Field	OIDs/Values	Comments
Critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.5.3.2 Digital Signature (2.16.756.1.17.3.2.11)

Verwendungszweck:

Das Class B digital signature certificate.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	.....	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId

X.509 Field	OIDs/Values	Comments
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'010000000'B	Digital Signature Non Repudiation
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.11	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Enhanced CA 01 CPS for end users	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

X.509 Field	OIDs/Values	Comments
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.5.3.3 Encryption (2.16.756.1.17.3.2.10)

Verwendungszweck:

Class B encryption certificate.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		

X.509 Field	OIDs/Values	Comments
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	4 unused bits '1100'B	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.10	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Enhanced CA 01 CPS for end users	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 01 CDPs

X.509 Field	OIDs/Values	Comments
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
	Encrypting File System (1.3.6.1.4.1.311.10.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.5.3.4 Class B (BV): Authentication Only (for A-Accounts or 2nd Token) (OID: 2.16.756.1.17.3.2.40) (standard)

Verwendungszweck:

Class B authentication certificate - Only (for A-Accounts or 2nd Token*)* issuing with wizard.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	

X.509 Field	OIDs/Values	Comments
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.40	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Authentication only of the Swiss Government Enhanced CA 01	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING

X.509 Field	OIDs/Values	Comments
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.5.4 Swiss Government Enhanced CA01 Prestaged Policies

2.5.5.4.1 Authentication (SG Enhanced CA01 – prestaged) (2.16.756.1.17.3.2.41)

Verwendungszweck:

Class B Authentication Certificate with prestaged key

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING

X.509 Field	OIDs/Values	Comments
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280

X.509 Field	OIDs/Values	Comments
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.41	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the prestaged Certificate Policy for Authentication of the Swiss Government Enhanced CA 01	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.5.4.2 Digital Signature (SG Enhanced CA01 – prestaged) (2.16.756.1.17.3.2.42)

Verwendungszweck:

Class B certificate for digital signature with prestaged key

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random

X.509 Field	OIDs/Values	Comments
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '11'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.42	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the prestaged Certificate Policy for Digital Signature of the Swiss Government Enhanced CA 01	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA01.crt	uri IA5String

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.5.4.3 Encryption (SG Enhanced CA01 – prestaged) (2.16.756.1.17.3.2.43)

Verwendungszweck:

Class B certificate for Encryption with prestaged key

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName
validity		

X.509 Field	OIDs/Values	Comments
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '100'B	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	

X.509 Field	OIDs/Values	Comments
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.43	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the prestaged Certificate Policy for Encipherment of the Swiss Government Enhanced CA 01	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates

X.509 Field	OIDs/Values	Comments
	Secure Email (1.3.6.1.5.5.7.3.4)	
	Encrypting File System (1.3.6.1.4.1.311.10.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.5.4.4 Authentication Only (for A-Accounts or 2nd Token) (SG Enhanced CA01 – prestaged) (2.16.756.1.17.3.2.44)

Verwendungszweck:

Class B authentication certificate with prestaged key for A-Accounts

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.44	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the prestaged Certificate Policy for Authentication only of the Swiss Government Enhanced CA 01	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates

X.509 Field	OIDs/Values	Comments
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.6 Swiss Government Enhanced CA02

2.5.6.1 Swiss Government Enhanced CA 02 OCSP Responder (2.16.756.1.17.3.2.39)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName

X.509 Field	OIDs/Values	Comments
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.3:EnhancedCA02-OCSP-Responder	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '10'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	

X.509 Field	OIDs/Values	Comments
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.39	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.6.2 Class B – Pre-staged (FUB)

2.5.6.2.1 Authentication (2.16.756.1.17.3.2.30)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
Signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6: CH 2.5.4.10: Admin 2.5.4.11: VBS 2.5.4.11: <AIS Entry OU> 2.16.840.1.113730.3.1.3: <Employee Number> 2.5.4.3: <First Last>	UTF8String directoryName First Last maps to LDAP DisplayName in AIS imported fields Employee Number maps to SSN in uid LDAP filed imported from AIS OU is AIS mapped OU (first in chain)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	

X.509 Field	OIDs/Values	Comments
visible	FALSE	
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING include Authority Key Identifier: TRUE
subjectKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		

X.509 Field	OIDs/Values	Comments
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.32	id-ce-certificatePolicies
extnValue	2.16.756.1.17.3.2.30	
extnId	1.3.6.1.5.5.7.2.2	VisibleString id-qt-unotice RFC 3280
extnValue	This is the Swiss Government Enhanced CA 02 CPS for end users	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String id-qt-cps
basicConstraints		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.19	
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl http://www.technical-pki.admin.ch/crl/EnhancedCA02.crl ldap:///CN=Swiss%20Government%20Enhanced%20CA%2002CN=SG-CA02CN=CDPCN=Public%20Key%20ServicesCN=ServicesCN=ConfigurationDC=ifrDC=intra2DC=adminDC=ch?certificateRevocationList?base?objectClass=cRLDistributionPoint	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE

X.509 Field	OIDs/Values	Comments
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication
	1.3.6.1.4.1.311.20.2.2	Smart Card Logon
subjectAltName		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.6.2.2 Digital Signature (2.16.756.1.17.3.2.31)

Verwendungszweck:

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6: CH 2.5.4.10: Admin 2.5.4.11: VBS 2.5.4.11: AIS Entry OU 2.16.840.1.113730.3.1.3: Employee Number 2.5.4.3: First Last	UTF8String directoryName First Last maps to LDAP DisplayName in AIS imported fields Employee Number maps to SSN in uid LDAP filed imported from AIS OU is AIS mapped OU (first in chain)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING Include Authority Key Identifier
subjectKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits ‘11’B	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	

X.509 Field	OIDs/Values	Comments
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.31	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Enhanced CA 02 CPS for end users	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	
extnId	2.5.29.19	
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl	uri IA5String

X.509 Field	OIDs/Values	Comments
	http://www.technical-pki.admin.ch/crl/EnhancedCA02.crl ldap:///CN=Swiss%20Government%20Enhanced%20CA%2002CN=SG-CA02CN=CDPCN=Public%20Key%20ServicesCN=ServicesCN=ConfigurationDC=ifrDC=intra2DC=adminDC=ch?certificateRevocationList?base?objectClass=cRLDistributionPoint	ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
subjectAltName		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.6.2.3 Encryption (2.16.756.1.17.3.2.32)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6: CH 2.5.4.10: Admin 2.5.4.11: VBS 2.5.4.11: AIS Entry OU 2.16.840.1.113730.3.1.3: Employee Number 2.5.4.3: First Last	UTF8String directoryName First Last maps to LDAP DisplayName in AIS imported fields Employee Number maps to SSN in uid LDAP filed imported from AIS OU is AIS mapped OU (first in chain)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING Include Authority Key Identifier
subjectKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits ‘100’B	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	

X.509 Field	OIDs/Values	Comments
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.32	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Enhanced CA 02 CPS for end users	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.31	

X.509 Field	OIDs/Values	Comments
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl http://www.technical-pki.admin.ch/crl/EnhancedCA02.crl ldap:///CN=Swiss%20Government%20Enhanced%20CA%2002CN=SG-CA02CN=CDPCN=Public%20Key%20ServicesCN=ServicesCN=ConfigurationDC=ifrDC=intra2DC=adminDC=ch?certificateRevocationList?base?objectClass=cRLDistributionPoint	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4	Email Protection (Secure Email)
	1.3.6.1.4.1.311.10.3.4	Microsoft EFS
subjectAltName		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.6.2.4 Class B (FUB): FUB LRAO Authentication Only (for A-Accounts or 2nd Token) (OID: 2.16.756.1.17.3.2.50) (pre-staged) (umbenannt – "LRAO" ergänzt)

Verwendungszweck:

Authentication certificate for special access rights – issuing with wizard.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6: CH 2.5.4.10: Admin 2.5.4.11: VBS 2.5.4.11: <AIS Entry OU> 2.16.840.1.113730.3.1.3: <Employee Number> 2.5.4.3: <First Last>	UTF8String directoryName First Last maps to LDAP DisplayName in AIS imported fields Employee Number maps to SSN in uid LDAP filed imported from AIS OU is AIS mapped OU (first in chain)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING include Authority Key Identifier: TRUE
subjectKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	

X.509 Field	OIDs/Values	Comments
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.50	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Authentication only of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl http://www.technical-pki.admin.ch/crl/EnhancedCA02.crl ldap:///CN=Swiss%20Government%20Enhanced%20CA%2002CN=SG-CA02CN=CDPCN=Public%20Key%20ServicesCN=ServicesCN=ConfigurationDC=ifrDC=intra2DC=adminDC=ch?certificateRevocationList?base?objectClass=cRLDistributionPoint	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication
	1.3.6.1.4.1.311.20.2.2	Smart Card Logon
subjectAltName		
critical	FALSE	
mandatory	TRUE	

X.509 Field	OIDs/Values	Comments
editable	FALSE	
visible	TRUE	
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.6.3 Class B pre-staged (BV)

2.5.6.3.1 Authentication (2.16.756.1.17.3.2.33 or 2.16.756.1.17.3.2.15)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		

X.509 Field	OIDs/Values	Comments
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.33 or 2.16.756.1.17.3.2.15	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Authentication of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 02ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs

X.509 Field	OIDs/Values	Comments
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.6.3.2 Digital Signature (2.16.756.1.17.3.2.34 or 2.16.756.1.17.3.2.11)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING

X.509 Field	OIDs/Values	Comments
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '11'B	RFC 5280

X.509 Field	OIDs/Values	Comments
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.34 or 2.16.756.1.17.3.2.11	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Digital Signature of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 02ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.6.3.3 Encryption (2.16.756.1.17.3.2.35 or 2.16.756.1.17.3.2.10)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '100'B	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	

X.509 Field	OIDs/Values	Comments
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.35 or 2.16.756.1.17.3.2.10	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Encipherment of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 02ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp

X.509 Field	OIDs/Values	Comments
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
	Encrypting File System (1.3.6.1.4.1.311.10.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.6.3.4 Class B pre-staged (BV): Authentication Only (for A-Accounts or 2nd Token) (2.16.756.1.17.3.2.36)

Verwendungszweck:

Authentifikationszertifikat für zusätzliches Token oder Spezial Accounts (A-Accounts)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280

X.509 Field	OIDs/Values	Comments
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	

X.509 Field	OIDs/Values	Comments
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.36	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Authentication only of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Enhanced CA 02ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 02 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication

X.509 Field	OIDs/Values	Comments
	1.3.6.1.4.1.311.20.2.2	Smart Card Logon
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.6.3.5 Class B pre-staged (BV): Authentication Only (for LRAO) (2.16.756.1.17.3.2.49)

Verwendungszweck:

Authentifikationszertifikat für zusätzliches Token oder Spezial Accounts (LRAO) -> Befristet bis zum Wegfall der LRA-Stationen

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.11:LRA 2.5.4.3:Last First Hash	
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	bits '001100000'B (bit 0)	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.49	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Authentication only of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication
	1.3.6.1.4.1.311.20.2.2	Smart Card Logon
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

X.509 Field	OIDs/Values	Comments
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.6.4 Class B SCMS Bund pre-staged

2.5.6.4.1 Authentication (2.16.756.1.17.3.2.51)

Verwendungszweck:
Dient der zertifikat-basierte Authentifizierung, um einen Benutzer zu identifizieren, bevor diesem Zugang zu einer Ressource, einem Netzwerk, einer Anwendung usw. gewährt wird.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.51	
extnId	1.3.6.1.5.5.7.2.2	

X.509 Field	OIDs/Values	Comments
extnValue	This is the Certificate Policy for Authentication of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.6.4.2 Digital Signature (2.16.756.1.17.3.2.53)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits ‘11’B	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.53	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Digital Signature of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.6.4.3 Encryption (2.16.756.1.17.3.2.52)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		

X.509 Field	OIDs/Values	Comments
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '100'B	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.52	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Encipherment of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING

X.509 Field	OIDs/Values	Comments
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
	Encrypting File System (1.3.6.1.4.1.311.10.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.6.4.4 Authentication Only (2.16.756.1.17.3.2.54)

Verwendungszweck:

Authentifikationszertifikat

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random

X.509 Field	OIDs/Values	Comments
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.54	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Authentication only of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	

X.509 Field	OIDs/Values	Comments
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication
	1.3.6.1.4.1.311.20.2.2	Smart Card Logon
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.6.4.5 Authentication Only (90-Days) (2.16.756.1.17.3.2.55)

Verwendungszweck:

Authentifikationszertifikat befristet auf 90 Tage

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Enhanced CA 02	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
validity		
notBefore	"200123090000Z"	UTC TIME ETSI TS 102 280
notAfter	"200422090000Z"	UTC TIME ETSI TS 102 280 (90 days)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:LRA 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	bits '001100000'B (bit 0)	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	

X.509 Field	OIDs/Values	Comments
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.55	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Certificate Policy for Authentication only 90 Days of the Swiss Government Enhanced CA 02	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/EnhancedCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EnhancedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates

X.509 Field	OIDs/Values	Comments
	1.3.6.1.5.5.7.3.2	Client Authentication
	1.3.6.1.4.1.311.20.2.2	Smart Card Logon
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.7 Swiss Government Enhanced CA03

2.5.7.1 Swiss Government Enhanced CA 03 OCSP Responder (2.16.756.1.17.3.2.68)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.

X.509 Field	OIDs/Values	Comments
issuer	2.5.4.3: Swiss Government Enhanced CA 03 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3:EnhancedCA03-OCSP-Responder 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '10'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.68	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.8 Swiss Government Enhanced CA04

2.5.8.1 Swiss Government Enhanced CA 04 OCSP Responder (2.16.756.1.17.3.2.69)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.3: Swiss Government Enhanced CA 04 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3:EnhancedCA04-OCSP-Responder 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit

X.509 Field	OIDs/Values	Comments
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘10’B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.69	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.9 Swiss Government Enhanced CA05

2.5.9.1 Swiss Government Enhanced CA 05 OCSP Responder (2.16.756.1.17.3.2.70)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative

X.509 Field	OIDs/Values	Comments
		integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.3: Swiss Government Enhanced CA 05 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3:EnhancedCA05-OCSP-Responder 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '10'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	

X.509 Field	OIDs/Values	Comments
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.70	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.10 Swiss Government Regulated CA02

2.5.10.1 Swiss Government Regulated CA 02 OCSP Responder (2.16.756.1.17.3.5.2.1)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
Version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.3:Swiss Government Regulated CA 02 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:VATCH-CHE-221.032.573 2.5.4.6:CH	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"yymmddhhMMssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhMMssZ"	UTC TIME ETSI TS 102 280 (1 years)
subject	2.5.4.3:RegulatedCA02-OCSP-Responder 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0x80	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
certificatePolicies		
extnId	2.5.29.32	

X.509 Field	OIDs/Values	Comments
extnValue	2.16.756.1.17.3.5.2.1	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
ocsp-nocheck		4.2.2.2.1 Revocation Checking of an Authorized Responder (RFC 2560) A CA may specify that an OCSP client can trust a responder for the lifetime of the responder's certificate. The CA does so by including the extension id-pkix-ocsp-nocheck. This SHOULD be a non-critical extension. The value of the extension should be NULL
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.10.2 Class A Qualified Digital Signature (Natural Person) (2.16.756.1.17.3.5.2.3)

Verwendungszweck:

Qualifizierte persönliche Signaturzertifikate gemäss ZertES

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert

X.509 Field	OIDs/Values	Comments
serialNumber	xxxxx	Random
Issuer	2.5.4.3:Swiss Government Regulated CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:VATCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name) 2.5.4.67: organisationalIdentifier (ETSI EN 319 412-2 V2.1.1 4.2.3.1 Legal person issuers TAV 2.3.2 b))
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.3:Givenname Surname Hash 2.5.4.4:Surname 2.5.4. 42:Givenname 2.5.4.6:CH	UTF8String directoryName Alternativ zu Surname/Givenname: Pseudonym Es werden vom Standard keine O und OU Attribute verlangt also kann man sie weglassen. Falls man sie beigbehalten will empfehle ich The commonName attribute has a usage purpose that is different from the required choice of pseudonym or givenName/surname. commonName is used for user friendly representation of the person's name whereas givenName/surname is used where more formal representation or verification of specific identity of the user is required. To maximize interoperability both are considered necessary.
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	`. . . . . .`B	BIT STRING 2048 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	

X.509 Field	OIDs/Values	Comments
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '01'B	RFC 5280
digitalSignature	0	Gemäss ETSI EN 319 412-2 Kapitel 4.3.2 kann Typ A oderB verwendet werden. Ich würde hier TYP B empfehlen – wir müssen testen ob die Funktionalität mit "nur" ContentCommitment» (Typ A) gegeben ist?
contentCommitment	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.3	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a qualifed certificate for natural persons as defined by the Swiss federal law SR 943.03 ZertES	IA5String id-qt-unotice RFC 5280 oder UTF8 RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d) Der ausführlichere Text wäre für relying Parties aussagekräftiger
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
subjectAltName		SEQUENCE

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	rfc822 Email
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegulatedCA02.crl	uri IA5String ldap uri IA5String CA Swiss Government Regulated CA 01 CDPs LDAP URI → weglassen wegen Redesign AdminDir
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegulatedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical. In accordance to https://tools.ietf.org/html/rfc3739.html

X.509 Field	OIDs/Values	Comments
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	qcs-QcSSCD
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.5	id-etsi-qcs-QcPDS
statementInfo	SEQUENCE	
url	http://www.pki.admin.ch/cps/PDS-SGPKI_Regulated_CA_02.pdf	PKI Disclosure Statements a) It shall provide at least one URL to a PDS in English. Other PDS documents in other languages may be referenced using this QCStatement provided that they provide information that corresponds to the information given in the referenced English PDS; and b) it shall not reference more than one PDS per language.
language	EN	ISO 639-1 language code
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	1	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 }

X.509 Field	OIDs/Values	Comments
		-- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.5.10.3 Class A - Geregeltes Behördenzertifikat (legal Person) (2.16.756.1.17.3.5.2.2)

Verwendungszweck:

Verwaltungsstellen (Behörden) sollen mit einem solchen Zertifikat zusammen mit einem qualifizierten Zeitstempel Dokumente digital signieren können.

Provisorische Konfiguration: Abgeleitet aus der bestehenden Policy für qualifizierte Signaturzertifikate unter der Issuing CA Swiss Government Regulated CA02

Zukünftige Konfiguration: Der Vergleich der Bestimmungen des neuen ZertES VZertES und den TAV mit der provisorischen Konfiguration zeigt dass folgende Anpassungen durchgeführt werden müssen:

- Neue Policy für das geregelte Behördenzertifikat
- Neue Policy für bestehende Klasse A Zertifikate
- Neue Issuing CA mit angepassten Attributen als Issuer der beiden oben erwähnten Zertifikatstypen.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signatureValue	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Unique Random

X.509 Field	OIDs/Values	Comments
Issuer	2.5.4.3:Swiss Government Regulated CA 02 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:VATCH-CHE-221.032.573 2.5.4.6:CH	***PrintableString*** directoryName 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name)
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.3:CommonName (CN) 2.5.4.11:organizationalUnitName (OU). 2.5.4.11:organizationalUnitName (OU) 2.5.4.10:OrganizationName (O) 2.5.4.97:organizationIdentifier (OI - different from OrganisationName) 2.5.4.7:localityName (L) 2.5.4.8:stateOrProvinceName (ST) 2.5.4.6:CH (C)	***PrintableString*** directoryName: Attribute die nicht gemäss TAV/ETSI definert werden müssen entsprechen dem Vorschlag des ISB für Amtssiegel: 2.5.4.6: C=CH oder LI 2.5.4.10: O=Name exakt wie im UID-Register 2.5.4.97: OI=„NTRCH"-UID der Behörde bzw. „VATCH"-UID bzw. „CH:"-UID der Behörde 2.5.4.3: CN=Allgemein gebräuchlicher Name der Behörde 2.5.4.11: $OU_{1..n}$:Nähere Bezeichnung 2.5.4.7: L=Bezeichnung der Gemeinde in der die Behörde ihren Sitz hat 2.5.4.8:ST= Bezeichnung des Kantons in der die Behörde ihren Sitz hat
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	`. . . . . .`B	BIT STRING 2048 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING

X.509 Field	OIDs/Values	Comments
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0X80	RFC 5280
digitalSignature	**1**	
contentCommitment	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.2	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a regulated certificate for legal persons as defined by the Swiss federal law SR 943.03 ZertES	VisibleString id-qt-unotice RFC 5280 RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d) Der ausführlichere Text wäre für relying Parties aussagekräftiger
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegulatedCA02.crl	uri IA5String ldap uri IA5String CA Swiss Government Qualified CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegulatedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		SEQUENCE
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	rfc822 Email (E-Mail Adresse die im Validator benützt wird um die Auskunftstelle für den signierten Dokumententyp anzuzeigen) gemäss RFC 5280 otherName [0] OtherName, rfc822Name [1] IA5String, dNSName [2] IA5String, x400Address [3] ORAddress, directoryName [4] Name, ediPartyName [5] EDIPartyName, uniformResourceIdentifier [6] IA5String, iPAddress [7] OCTET STRING, registeredID [8] OBJECT IDENTIFIER
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	

X.509 Field	OIDs/Values	Comments
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical. In accordance to https://tools.ietf.org/html/rfc3739.html
qCStatement	SEQUENCE	
statementId	0.4.0.194121.1.2	id-etsi-qcs-SemanticsId-Legal -> Legal person semantics (for legal person certificates – electronic seal)
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	id-etsi-qcs-QcSSCD: ETSI EN 319 412-5 Kap. 4.2.2 TAV Kap. 2.3.2 Abschn. g) When the certificate is issued as a certificate where the private key related to the certified public key resides in a qualified signature/seal creation device in accordance with Regulation (EU) No 910/2014 [i.8] or in a secure signature creation device as defined in Directive 1999/93/EC [i.3] this statement shall be present.
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.5	id-etsi-qcs-QcPDS Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Das PKI Disclosure Statement PDS ist ein Dokument das die Transparenz gegenüber den Kunden stark erhöht. Zudem ist es nicht direkt an die EU Rechtssprechung gebunden
statementInfo	SEQUENCE	
url	http://www.pki.admin.ch/cps/PDS-SGPKI_Regulated_CA_02.pdf	PKI Disclosure Statements a) It shall provide at least one URL to a PDS in English. Other PDS documents in other languages may be referenced using this QCStatement provided that they

X.509 Field	OIDs/Values	Comments
		provide information that corresponds to the information given in the referenced English PDS; and b) it shall not reference more than one PDS per language.
language	EN	ISO 639-1 language code
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	2	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.5.10.4 Time Stamp Signer (Legal Person) (2.16.756.1.17.3.5.2.4)

Verwendungszweck:

Ausstellung von Zeitstempeln gemäss ZertES

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
Algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
Parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regulated CA 02 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:VATCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"YYMMDDHHMMSSZ"	UTC TIME ETSI TS 102 280
notAfter	"YYMMDDHHMMSSZ"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3: Swiss Government TSA 2.5.4.11:Time Stamp Services 2.5.4.11:Swiss Government PKI 2.5.4.10: Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:VATCH-CHE-221.032.573 2.5.4.7:Bern 2.5.4.6:CH	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	RFC 3279
subjectPublicKey	`……..`B	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.35	KeyId
extnValue	`.....`O	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`.....`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0x80	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.4	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a regulated certificate of the Swiss Government Regulated CA 02 CPS for timestamping purposes	VisibleString id-qt-unotice RFC 3280 regulated certificate
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
extendedKeyUsage		
extnId	2.5.29.37	
Critical	TRUE	
	1.3.6.1.5.5.7.3.8	timeStamping
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegulatedCA02.crl	uri IA5String ldap uri IA5String CA Swiss Government Regulated CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegulatedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 “The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical.” In accordance to https://tools.ietf.org/html/rfc3739.html

X.509 Field	OIDs/Values	Comments
qCStatement	SEQUENCE	
statementId	0.4.0.194121.1.2	id-etsi-qcs-SemanticsId-Legal -> Legal person semantics (for legal person certificates – electronic seal)
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	id-etsi-qcs-QcSSCD: ETSI EN 319 412-5 Kap. 4.2.2 TAV Kap. 2.3.2 Abschn. g) When the certificate is issued as a certificate where the private key related to the certified public key resides in a qualified signature/seal creation device in accordance with Regulation (EU) No 910/2014 [i.8] or in a secure signature creation device as defined in Directive 1999/93/EC [i.3] this statement shall be present.
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.5	id-etsi-qcs-QcPDS Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Das PKI Disclosure Statement PDS ist ein Dokument das die Transparenz gegenüber den Kunden stark erhöht. Zudem ist es nicht direkt an die EU Rechtssprechung gebunden
statementInfo	SEQUENCE	
url	http://www.pki.admin.ch/cps/PDS-SGPKI_Regulated_CA_02.pdf	PKI Disclosure Statements a) It shall provide at least one URL to a PDS in English. Other PDS documents in other languages may be referenced using this QCStatement provided that they provide information that corresponds to the information given in the referenced English PDS; and b) it shall not reference more than one PDS per language.

X.509 Field	OIDs/Values	Comments
language	EN	ISO 639-1 language code
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	2	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.5.10.5 Class A - Geregeltes Behördenzertifikat ab 01.01.2021 (legal Person) (2.16.756.1.17.3.5.2.7)

Verwendungszweck:

Verwaltungsstellen (Behörden) sollen mit einem solchen Zertifikat zusammen mit einem qualifizierten Zeitstempel Dokumente digital signieren können.

Provisorische Konfiguration: Abgeleitet aus der bestehenden Policy für qualifizierte Signaturzertifikate unter der Issuing CA Swiss Government Qualified CA 01

Zukünftige Konfiguration: Der Vergleich der Bestimmungen des neuen ZertES VZertES und den TAV mit der provisorischen Konfiguration zeigt dass folgende Anpassungen durchgeführt werden müssen:

- Neue Policy für das geregelte Behördenzertifikat
- Neue Policy für bestehende Klasse A Zertifikate
- Neue Issuing CA mit angepassten Attributen als Issuer der beiden oben erwähnten Zertifikatstypen.

X.509 Field	**OIDs/Values**	**Comments**
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signatureValue	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Unique Random
Issuer	2.5.4.3:Swiss Government Regulated CA 02 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	***PrintableString*** directoryName 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name)
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.3:CommonName (CN) 2.5.4.11:organizationalUnitName (OU). 2.5.4.11:organizationalUnitName (OU) 2.5.4.11:organizationalUnitName (OU) 2.5.4.10:OrganizationName (O) 2.5.4.97:organizationIdentifier (OI - different from OrganisationName) 2.5.4.15:BusinessCategory 2.5.4.7:localityName (L)	***PrintableString*** directoryName: Attribute die nicht gemäss TAV/ETSI definert werden müssen entsprechen dem Vorschlag des ISB für Amtssiegel: 2.5.4.10: O=Name exakt wie im UID-Register Der O muss mit dem Namen im UID-Register übereinstimmen. 2.5.4.97: OI=„NTRCH"-UID der Behörde bzw.„CH:"-UID der Behörde UID Nummer der ausstellenden Behörde (gemäss UID-G) im von ZertES verlangten Format.

X.509 Field	OIDs/Values	Comments
	2.5.4.8:stateOrProvinceName (ST) 2.5.4.6:CH (C) 2.5.29.17:SubjectAltName	2.5.4.3: CN= Allgemein gebräuchlicher Name der Verwaltungsstelle. Der Name muss für den Empfänger des elektronisch gesiegelten Dokumentes sprechend sein und wird bei einer automatisierten Prüfung eines elektronisch gesiegelten Dokumentes ggf. in einem Prüfberichtbericht aufgeführt. 2.5.4.11: OU1/2: Nähere Bezeichnung der Organisationseinheit (Departement, Abteilung, etc.), die dem Zertifikat zugeordnet ist. Es können bis zu 2 OU Felder angegeben werden. 2.5.4.11: OUn+1: Behörden-Identifikation: • GE - 0220 – Amtskürzel oder -bezeichnung Bundesbehörde (Bundesamt) • GE - 0221 - Kantonskürzel - Amtskürzel oder -bezeichnung kantonale Behörde • GE - 0222 - Kantonskürzel - Hist. BFSNR - Amtskürzel oder -bezeichnung Behörde eines Bezirks • GE - 0223 - Hist. BFSNR - Amtskürzel oder -bezeichnung kommunale Behörde ntonskürzel - Hist. BFSNR - Amtskürzel oder -bezeichnung Behörde eines Bezirks 2.5.4.15:BusinessCategory = «governmental Instituion» 2.5.4.7: L=Bezeichnung der Gemeinde in der die Behörde ihren Sitz hat 2.5.4.8:ST= Bezeichnung des Kantons in der die Behörde ihren Sitz hat 2.5.4.6: C=CH oder LI 2.5.29.17:SubjectAltName E-Mail-Adresse, die bei einer automatisierten Prüfung eines elektronisch gesiegelten Do-kumentes ggf. in einem Prüfbericht aufgeführt wird, um die Auskunftstelle für den signierten Dokumententyp anzuzeigen
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	`.....`B	BIT STRING 2048 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId

X.509 Field	OIDs/Values	Comments
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0X80	RFC 5280
digitalSignature	**1**	
contentCommitment	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.7	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a regulated certificate for legal persons as defined by the Swiss federal law SR 943.03 ZertES	VisibleString id-qt-unotice RFC 5280 RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d) Der ausführlichere Text wäre für relying Parties aussagekräftiger
basicConstraints		
extnId	2.5.29.19	

X.509 Field	OIDs/Values	Comments
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegulatedCA02.crl	uri IA5String ldap uri IA5String CA Swiss Government Qualified CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegulatedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		SEQUENCE
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	rfc822 Email (E-Mail Adresse die im Validator benützt wird um die Auskunftstelle für den signierten Dokumententyp anzuzeigen) gemäss RFC 5280 otherName [0] OtherName, rfc822Name [1] IA5String, dNSName [2] IA5String, x400Address [3] ORAddress, directoryName [4] Name, ediPartyName [5] EDIPartyName, uniformResourceIdentifier [6] IA5String, iPAddress [7] OCTET STRING,

X.509 Field	OIDs/Values	Comments
		registeredID [8] OBJECT IDENTIFIER
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical. In accordance to https://tools.ietf.org/html/rfc3739.html
qCStatement	SEQUENCE	
statementId	0.4.0.194121.1.2	id-etsi-qcs-SemanticsId-Legal -> Legal person semantics (for legal person certificates – electronic seal)
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	id-etsi-qcs-QcSSCD: ETSI EN 319 412-5 Kap. 4.2.2 TAV Kap. 2.3.2 Abschn. g) When the certificate is issued as a certificate where the private key related to the certified public key resides in a qualified signature/seal creation device in accordance with Regulation (EU) No 910/2014 [i.8] or in a secure signature creation device as defined in Directive 1999/93/EC [i.3] this statement shall be present.
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.5	id-etsi-qcs-QcPDS Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Das PKI Disclosure Statement PDS ist ein Dokument das die Transparenz gegenüber den Kunden stark erhöht. Zudem ist es nicht direkt an die EU Rechtssprechung gebunden
statementInfo	SEQUENCE	

X.509 Field	OIDs/Values	Comments
url	http://www.pki.admin.ch/cps/PDS-SGPKI_Regulated_CA_02.pdf	PKI Disclosure Statements a) It shall provide at least one URL to a PDS in English. Other PDS documents in other languages may be referenced using this QCStatement provided that they provide information that corresponds to the information given in the referenced English PDS; and b) it shall not reference more than one PDS per language.
language	EN	ISO 639-1 language code
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	2	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.5.10.6 Class A - Geregeltes Behördenzertifikat für GGG (legal Person) (2.16.756.1.17.3.5.2.14)

Verwendungszweck:

Verwaltungsstellen (Behörden) sollen mit einem solchen Zertifikat zusammen mit einem qualifizierten Zeitstempel Dokumente digital signieren können.

Provisorische Konfiguration: Abgeleitet aus der bestehenden Policy für qualifizierte Signaturzertifikate unter der Issuing CA Swiss Government Qualified CA 01

Zukünftige Konfiguration: Der Vergleich der Bestimmungen des neuen ZertES VZertES und den TAV mit der provisorischen Konfiguration zeigt dass folgende Anpassungen durchgeführt werden müssen:

- Neue Policy für das geregelte Behördenzertifikat
- Neue Policy für bestehende Klasse A Zertifikate
- Neue Issuing CA mit angepassten Attributen als Issuer der beiden oben erwähnten Zertifikatstypen.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signatureValue	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Unique Random
Issuer	2.5.4.3:Swiss Government Regulated CA 02 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	***PrintableString*** directoryName 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name)
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.3:CommonName (CN)(COVID-certificate-CH-dd-mm) 2.5.4.11:organizationalUnitName (OU)(Taskforce BAG Covid-19) 2.5.4.11:organizationalUnitName (OU)(GE-0220-BAG)	***PrintableString*** directoryName: Attribute die nicht gemäss TAV/ETSI definert werden müssen entsprechen dem Vorschlag des ISB für Amtssiegel:

X.509 Field	OIDs/Values	Comments
	2.5.4.10:OrganizationName (O)(Bundesamt für Gesundheit (BAG) 2.5.4.97:organizationIdentifier (OI) (NTRCH-CHE-467.023.568) 2.5.4.15:BusinessCategory (Government Entity) 2.5.4.7:localityName (L)(Könitz) 2.5.4.8:stateOrProvinceName (ST) (Bern) 2.5.4.6:C (CH) 2.5.29.17:SubjectAltName (covid-zertifikat@bag.admin.ch)	2.5.4.10: O=Name exakt wie im UID-Register Der O muss mit dem Namen im UID-Register übereinstimmen. 2.5.4.97: OI=„NTRCH“-UID der Behörde bzw.„CH:“-UID der Behörde UID Nummer der ausstellenden Behörde (gemäss UID-G) im von ZertES verlangten Format. 2.5.4.3: CN= Allgemein gebräuchlicher Name der Verwaltungsstelle. Der Name muss für den Empfänger des elektronisch gesiegelten Dokumentes sprechend sein und wird bei einer automatisierten Prüfung eines elektronisch gesiegelten Dokumentes ggf. in einem Prüfberichtbericht aufgeführt. 2.5.4.11: OU1/2: Nähere Bezeichnung der Organisationseinheit (Departement, Abteilung, etc.), die dem Zertifikat zugeordnet ist. Es können bis zu 2 OU Felder angegeben werden. 2.5.4.11: OUn+1: Behörden-Identifikation: • GE - 0220 – Amtskürzel oder -bezeichnung Bundesbehörde (Bundesamt) • GE - 0221 - Kantonskürzel - Amtskürzel oder -bezeichnung kantonale Behörde • GE - 0222 - Kantonskürzel - Hist. BFSNR - Amtskürzel oder -bezeichnung Behörde eines Bezirks • GE - 0223 - Hist. BFSNR - Amtskürzel oder -bezeichnung kommunale Behörde ntonskürzel - Hist. BFSNR - Amtskürzel oder -bezeichnung Behörde eines Bezirks 2.5.4.15:BusinessCategory = «governmental Instituion» 2.5.4.7: L=Bezeichnung der Gemeinde in der die Behörde ihren Sitz hat 2.5.4.8:ST= Bezeichnung des Kantons in der die Behörde ihren Sitz hat 2.5.4.6: C=CH oder LI 2.5.29.17:SubjectAltName E-Mail-Adresse, die bei einer automatisierten Prüfung eines elektronisch gesiegelten Do-kumentes ggf. in einem Prüfbericht aufgeführt wird, um die Auskunftstelle für den signierten Dokumententyp anzuzeigen
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	

X.509 Field	OIDs/Values	Comments
subjectPublicKey	`. . . . . .`B	BIT STRING 2048 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0X80	RFC 5280
digitalSignature	**1**	
contentCommitment	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.14	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
extnId	1.3.6.1.5.5.7.2.2	

X.509 Field	OIDs/Values	Comments
extnValue	This is a regulated certificate for legal persons as defined by the Swiss federal law SR 943.03 ZertES	VisibleString id-qt-unotice RFC 5280 RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d) Der ausführlichere Text wäre für relying Parties aussagekräftiger
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegulatedCA02.crl	uri IA5String ldap uri IA5String CA Swiss Government Qualified CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegulatedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		SEQUENCE
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	rfc822 Email (E-Mail Adresse die im Validator benützt wird um die Auskunftstelle für den signierten Dokumententyp anzuzeigen) gemäss RFC 5280 otherName [0] OtherName, rfc822Name [1] IA5String, dNSName [2] IA5String,

X.509 Field	OIDs/Values	Comments
		x400Address [3] ORAddress, directoryName [4] Name, ediPartyName [5] EDIPartyName, uniformResourceIdentifier [6] IA5String, iPAddress [7] OCTET STRING, registeredID [8] OBJECT IDENTIFIER
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical. In accordance to https://tools.ietf.org/html/rfc3739.html
qCStatement	SEQUENCE	
statementId	0.4.0.194121.1.2	id-etsi-qcs-SemanticsId-Legal -> Legal person semantics (for legal person certificates – electronic seal)
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	id-etsi-qcs-QcSSCD: ETSI EN 319 412-5 Kap. 4.2.2 TAV Kap. 2.3.2 Abschn. g) When the certificate is issued as a certificate where the private key related to the certified public key resides in a qualified signature/seal creation device in accordance with Regulation (EU) No 910/2014 [i.8] or in a secure signature creation device as defined in Directive 1999/93/EC [i.3] this statement shall be present.
qCStatement	SEQUENCE	

X.509 Field	OIDs/Values	Comments
statementId	0.4.0.1862.1.5	id-etsi-qcs-QcPDS Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Das PKI Disclosure Statement PDS ist ein Dokument das die Transparenz gegenüber den Kunden stark erhöht. Zudem ist es nicht direkt an die EU Rechtssprechung gebunden
statementInfo	SEQUENCE	
url	http://www.pki.admin.ch/cps/PDS-SGPKI_Regulated_CA_02.pdf	PKI Disclosure Statements a) It shall provide at least one URL to a PDS in English. Other PDS documents in other languages may be referenced using this QCStatement provided that they provide information that corresponds to the information given in the referenced English PDS; and b) it shall not reference more than one PDS per language.
language	EN	ISO 639-1 language code
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	2	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 }

X.509 Field	OIDs/Values	Comments
		-- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.5.10.7 Class A Qualified Digital Signature (Signaturdienst) (natural Person) (2.16.756.1.17.3.5.2.6)

Verwendungszweck:

Qualifizierte persönliche Signaturzertifikate gemäss ZertES zur Nutzung mit dem Signaturdienst

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
Issuer	2.5.4.3:Swiss Government Regulated CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:VATCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name) 2.5.4.67: organisationalIdentifier (ETSI EN 319 412-2 V2.1.1 4.2.3.1 Legal person issuers TAV 2.3.2 b))
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.3:Givenname Surname Hash	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.4:Surname 2.5.4. 42:Givenname 2.5.4.6:CH	Alternativ zu Surname/Givenname: Pseudonym Es werden vom Standard keine O und OU Attribute verlangt also kann man sie weglassen. Falls man sie beigbehalten will empfehle ich The commonName attribute has a usage purpose that is different from the required choice of pseudonym or givenName/surname. commonName is used for user friendly representation of the person's name whereas givenName/surname is used where more formal representation or verification of specific identity of the user is required. To maximize interoperability both are considered necessary.
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	`. . . . . .`B	BIT STRING 2048 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits ‘01’B	RFC 5280
digitalSignature	0	Gemäss ETSI EN 319 412-2 Kapitel 4.3.2 kann Typ A oderB verwendet werden. Ich würde hier TYP B empfehlen – wir müssen testen ob die Funktionalität mit “nur” ContentCommitment» (Typ A) gegeben ist?
contentCommitment	1	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.6	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a qualifed certificate for natural persons as defined by the Swiss federal law SR 943.03 ZertES	IA5String id-qt-unotice RFC 5280 oder UTF8 RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d) Der ausführlichere Text wäre für relying Parties aussagekräftiger
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
subjectAltName		SEQUENCE
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	rfc822 Email
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegulatedCA02.crl	uri IA5String ldap uri IA5String CA Swiss Government Regulated CA 01 CDPs LDAP URI → weglassen wegen Redesign AdminDir

X.509 Field	OIDs/Values	Comments
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegulatedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical. In accordance to https://tools.ietf.org/html/rfc3739.html
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	qcs-QcSSCD
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.5	id-etsi-qcs-QcPDS
statementInfo	SEQUENCE	
url	http://www.pki.admin.ch/cps/PDS-SGPKI_Regulated_CA_02.pdf	PKI Disclosure Statements a) It shall provide at least one URL to a PDS in English. Other PDS documents in other languages may be referenced using this QCStatement provided that they provide information that corresponds to the information given in the referenced English PDS; and

X.509 Field	OIDs/Values	Comments
		b) it shall not reference more than one PDS per language.
language	EN	ISO 639-1 language code
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	1	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.5.10.8 Class A Qualified Digital Signature (Signaturdienst) (Natural Person) (2.16.756.1.17.3.5.2.13)

Verwendungszweck:

Qualifizierte persönliche Signaturzertifikate gemäss ZertES zur Nutzung mit dem Signaturdienst

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
Issuer	2.5.4.3:Swiss Government Regulated CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97: VATCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name) 2.5.4.67: organisationalIdentifier (ETSI EN 319 412-2 V2.1.1 4.2.3.1 Legal person issuers TAV 2.3.2 b))
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.3:Givenname Surname Hash 2.5.4.4:Surname 2.5.4. 42:Givenname 2.5.4.6:CH	UTF8String directoryName Alternativ zu Surname/Givenname: Pseudonym Es werden vom Standard keine O und OU Attribute verlangt also kann man sie weglassen. Falls man sie beigbehalten will empfehle ich The commonName attribute has a usage purpose that is different from the required choice of pseudonym or givenName/surname. commonName is used for user friendly representation of the person's name whereas givenName/surname is used where more formal representation or verification of specific identity of the user is required. To maximize interoperability both are considered necessary.
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	

X.509 Field	OIDs/Values	Comments
subjectPublicKey	`. . . . . .`B	BIT STRING 2048 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '01'B	RFC 5280
digitalSignature	0	Gemäss ETSI EN 319 412-2 Kapitel 4.3.2 kann Typ A oderB verwendet werden. Ich würde hier TYP B empfehlen – wir müssen testen ob die Funktionalität mit "nur" ContentCommitment» (Typ A) gegeben ist?
contentCommitment	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.13	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a qualifed certificate for natural persons as defined by the Swiss federal law SR 943.03 ZertES	IA5String id-qt-unotice RFC 5280 oder UTF8 RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d) Der ausführlichere Text wäre für relying Parties aussagekräftiger
extnId	1.3.6.1.5.5.7.2.1	
extnValue	https://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
subjectAltName		SEQUENCE
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	rfc822 Email
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	https://www.pki.admin.ch/crl/RegulatedCA02.crl	uri IA5String ldap uri IA5String CA Swiss Government Regulated CA 01 CDPs LDAP URI → weglassen wegen Redesign AdminDir
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	https://www.pki.admin.ch/aia/RegulatedCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
qcStatements		

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical. In accordance to https://tools.ietf.org/html/rfc3739.html
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	qcs-QcSSCD
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	1	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

~~Class A - Geregeltes~~

2.5.11 Swiss Government Regulated CA03

2.5.11.1 Time Stamp Signer (Legal Person) (2.16.756.1.17.3.5.2.10)

Verwendungszweck:

Ausstellung von Zeitstempeln gemäss ZertES

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
Algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
Parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regulated CA 03 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:VATCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"YYMMDDHHMMSSZ"	UTC TIME ETSI TS 102 280
notAfter	"YYMMDDHHMMSSZ"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3: Swiss Government TSA 2.5.4.11:Time Stamp Services 2.5.4.11:Swiss Government PKI 2.5.4.10: Bundesamt fuer Informatik und Telekommunikation (BIT)	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.97:VATCH-CHE-221.032.573 2.5.4.7:Bern 2.5.4.6:CH	
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	RFC 3279
subjectPublicKey	`……..`B	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`…..`O	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`…..`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0x80	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.10	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a regulated certificate of the Swiss Government Regulated CA 03 CPS for timestamping purposes	VisibleString id-qt-unotice RFC 3280 regulated certificate
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
extendedKeyUsage		
extnId	2.5.29.37	
Critical	TRUE	
	1.3.6.1.5.5.7.3.8	timeStamping
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegulatedCA03.crl	uri IA5String ldap uri IA5String CA Swiss Government Regulated CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegulatedCA03.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

X.509 Field	OIDs/Values	Comments
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 "The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical." In accordance to https://tools.ietf.org/html/rfc3739.html
qCStatement	SEQUENCE	
statementId	0.4.0.194121.1.2	id-etsi-qcs-SemanticsId-Legal -> Legal person semantics (for legal person certificates – electronic seal)
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	id-etsi-qcs-QcSSCD: ETSI EN 319 412-5 Kap. 4.2.2 TAV Kap. 2.3.2 Abschn. g) When the certificate is issued as a certificate where the private key related to the certified public key resides in a qualified signature/seal creation device in accordance with Regulation (EU) No 910/2014 [i.8] or in a secure signature creation device as defined in Directive 1999/93/EC [i.3] this statement shall be present.
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.5	id-etsi-qcs-QcPDS Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Das PKI Disclosure Statement PDS ist ein Dokument das die Transparenz gegenüber den Kunden stark erhöht. Zudem ist es nicht direkt an die EU Rechtssprechung gebunden
statementInfo	SEQUENCE	

X.509 Field	OIDs/Values	Comments
url	http://www.pki.admin.ch/cps/PDS-SGPKI_Regulated_CA_03.pdf	PKI Disclosure Statements a) It shall provide at least one URL to a PDS in English. Other PDS documents in other languages may be referenced using this QCStatement provided that they provide information that corresponds to the information given in the referenced English PDS; and b) it shall not reference more than one PDS per language.
language	EN	ISO 639-1 language code
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	2	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }

X.509 Field	OIDs/Values	Comments
		-- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.5.11.2 Swiss Government Regulated CA 03 OCSP Responder (2.16.756.1.17.3.5.2.11)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
Version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.3:Swiss Government Regulated CA 03 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"yymmddhhMMssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhMMssZ"	UTC TIME ETSI TS 102 280 (1 years)

X.509 Field	OIDs/Values	Comments
subject	2.5.4.3:Regulated-CA03-OCSP-Responder 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	PrintableString directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0x80	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
extendedKeyUsage		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.11	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
ocsp-nocheck		4.2.2.2.1 Revocation Checking of an Authorized Responder (RFC 2560) A CA may specify that an OCSP client can trust a responder for the lifetime of the responder's certificate. The CA does so by including the extension id-pkix-ocsp-nocheck. This SHOULD be a non-critical extension. The value of the extension should be NULL
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.11.3 Class A Qualified Digital Signature (Natural Person) (2.16.756.1.17.3.5.2.9)

Verwendungszweck:

Qualifizierte persönliche Signaturzertifikate gemäss ZertES mit FreeDN auf SmartCard

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		

X.509 Field	OIDs/Values	Comments
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
Issuer	2.5.4.3:Swiss Government Regulated CA 03 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name) 2.5.4.67: organisationalIdentifier (ETSI EN 319 412-2 V2.1.1 4.2.3.1 Legal person issuers TAV 2.3.2 b))
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.3:Givenname Surname Hash 2.5.4.4:Surname 2.5.4. 42:Givenname 2.5.4.6:CH	UTF8String directoryName Alternativ zu Surname/Givenname: Pseudonym Es werden vom Standard keine O und OU Attribute verlangt also kann man sie weglassen. Falls man sie beigbehalten will empfehle ich The commonName attribute has a usage purpose that is different from the required choice of pseudonym or givenName/surname. commonName is used for user friendly representation of the person's name whereas givenName/surname is used where more formal representation or verification of specific identity of the user is required. To maximize interoperability both are considered necessary.
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	`. . . . . .`B	BIT STRING 2048 Bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '01'B	RFC 5280
digitalSignature	0	Gemäss ETSI EN 319 412-2 Kapitel 4.3.2 kann Typ A oderB verwendet werden. Ich würde hier TYP B empfehlen – wir müssen testen ob die Funktionalität mit "nur" ContentCommitment» (Typ A) gegeben ist?
contentCommitment	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.9	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
extnId	1.3.6.1.5.5.7.2.2	

X.509 Field	OIDs/Values	Comments
extnValue	This is a qualifed certificate for natural persons as defined by the Swiss federal law SR 943.03 ZertES	IA5String id-qt-unotice RFC 5280 oder UTF8 RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d) Der ausführlichere Text wäre für relying Parties aussagekräftiger
extnId	1.3.6.1.5.5.7.2.1	
extnValue	https://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
subjectAltName		SEQUENCE
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	rfc822 Email
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	https://www.pki.admin.ch/crl/RegulatedCA03.crl	uri IA5String ldap uri IA5String CA Swiss Government Regulated CA 01 CDPs LDAP URI → weglassen wegen Redesign AdminDir
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	https://www.pki.admin.ch/aia/RegulatedCA03.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	

X.509 Field	OIDs/Values	Comments
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical. In accordance to https://tools.ietf.org/html/rfc3739.html
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	qcs-QcSSCD
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	1	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.5.11.4 Behördenzertifikat (Signaturdienst) (legal Person) (2.16.756.1.17.3.5.2.8)

Verwendungszweck:

- Geregeltes Behördensigel zur Nutzung mit dem Signaturdienst

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signatureValue	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Unique Random
Issuer	2.5.4.3:Swiss Government Regulated CA 03 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	***PrintableString*** directoryName 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name)
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.3:CommonName (CN) 2.5.4.11:organizationalUnitName (OU). 2.5.4.11:organizationalUnitName (OU) 2.5.4.11:organizationalUnitName (OU) 2.5.4.10:OrganizationName (O) 2.5.4.97:organizationIdentifier (OI - different from OrganisationName) 2.5.4.15:BusinessCategory 2.5.4.7:localityName (L) 2.5.4.8:stateOrProvinceName (ST)	***PrintableString*** directoryName: Attribute die nicht gemäss TAV/ETSI definert werden müssen entsprechen dem Vorschlag des ISB für Amtssiegel: 2.5.4.10: O=Name exakt wie im UID-Register Der O muss mit dem Namen im UID-Register übereinstimmen. 2.5.4.97: OI=„NTRCH"-UID der Behörde bzw.„CH:"-UID der Behörde UID Nummer der ausstellenden Behörde (gemäss UID-G) im von ZertES verlangten Format. 2.5.4.3: CN= Allgemein gebräuchlicher Name der Verwaltungsstelle. Der Name muss für den Empfänger des elektronisch gesiegelten

X.509 Field	OIDs/Values	Comments
	2.5.4.6:CH (C) 2.5.29.17:SubjectAltName	Dokumentes sprechend sein und wird bei einer automatisierten Prüfung eines elektronisch gesiegelten Dokumentes ggf. in einem Prüfberichtbericht aufgeführt. 2.5.4.11: OU1/2: Nähere Bezeichnung der Organisationseinheit (Departement, Abteilung, etc.), die dem Zertifikat zugeordnet ist. Es können bis zu 2 OU Felder angegeben werden. 2.5.4.11: OUn+1: Behörden-Identifikation: • GE - 0220 – Amtskürzel oder -bezeichnung Bundesbehörde (Bundesamt) • GE - 0221 - Kantonskürzel - Amtskürzel oder -bezeichnung kantonale Behörde • GE - 0222 - Kantonskürzel - Hist. BFSNR - Amtskürzel oder -bezeichnung Behörde eines Bezirks • GE - 0223 - Hist. BFSNR - Amtskürzel oder -bezeichnung kommunale Behörde ntonskürzel - Hist. BFSNR - Amtskürzel oder -bezeichnung Behörde eines Bezirks 2.5.4.15:BusinessCategory = «governmental Instituion» 2.5.4.7: L=Bezeichnung der Gemeinde in der die Behörde ihren Sitz hat 2.5.4.8:ST= Bezeichnung des Kantons in der die Behörde ihren Sitz hat 2.5.4.6: C=CH oder LI 2.5.29.17:SubjectAltName E-Mail-Adresse, die bei einer automatisierten Prüfung eines elektronisch gesiegelten Do-kumentes ggf. in einem Prüfbericht aufgeführt wird, um die Auskunftstelle für den signierten Dokumententyp anzuzeigen
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	`. . . . . .`B	BIT STRING 2048 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.14	
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	0X80	RFC 5280
digitalSignature	**1**	
contentCommitment	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.2.8	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
extnId	1.3.6.1.5.5.7.2.1	
extnValue	https://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	IA5String cps
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a regulated certificate for legal persons as defined by the Swiss federal law SR 943.03 ZertES	VisibleString id-qt-unotice RFC 5280 RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d) Der ausführlichere Text wäre für relying Parties aussagekräftiger
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN

X.509 Field	OIDs/Values	Comments
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	https://www.pki.admin.ch/crl/RegulatedCA03.crl	uri IA5String ldap uri IA5String CA Swiss Government Qualified CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	https://www.pki.admin.ch/aia/RegulatedCA03.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		SEQUENCE
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	rfc822 Email (E-Mail Adresse die im Validator benützt wird um die Auskunftstelle für den signierten Dokumententyp anzuzeigen) gemäss RFC 5280 otherName [0] OtherName, rfc822Name [1] IA5String, dNSName [2] IA5String, x400Address [3] ORAddress, directoryName [4] Name, ediPartyName [5] EDIPartyName, uniformResourceIdentifier [6] IA5String, iPAddress [7] OCTET STRING, registeredID [8] OBJECT IDENTIFIER

X.509 Field	OIDs/Values	Comments
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2 ETSI EN 319 412-5 Chapter 4.1 The qcStatements extension shall be as specified in clause 3.2.6 of IETF RFC 3739. The qcStatements extension shall not be marked as critical. In accordance to https://tools.ietf.org/html/rfc3739.html
qCStatement	SEQUENCE	
statementId	0.4.0.194121.1.2	id-etsi-qcs-SemanticsId-Legal -> Legal person semantics (for legal person certificates – electronic seal)
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	id-etsi-qcs-QcSSCD: ETSI EN 319 412-5 Kap. 4.2.2 TAV Kap. 2.3.2 Abschn. g) When the certificate is issued as a certificate where the private key related to the certified public key resides in a qualified signature/seal creation device in accordance with Regulation (EU) No 910/2014 [i.8] or in a secure signature creation device as defined in Directive 1999/93/EC [i.3] this statement shall be present.
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER

X.509 Field	OIDs/Values	Comments
id-etsi-qcs-QcType	2	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.5.12 Swiss Government Regular CA01

2.5.12.1 Swiss Government Regular CA 01 OCSP Responder (2.16.756.1.17.3.22.62)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3

X.509 Field	OIDs/Values	Comments
		(value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.3:RegularCA01-OCSP-Responder	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	….	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	7 unused bits '11'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.62	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocsp-nocheck		4.2.2.2.1 Revocation Checking of an Authorized Responder (RFC 2560) A CA may specify that an OCSP client can trust a responder for the lifetime of the responder's certificate. The CA does so by including the extension id-pkix-ocsp-nocheck. This SHOULD be a non-critical extension. The value of the extension should be NULL
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN

X.509 Field	OIDs/Values	Comments
pathLenConstraint	None	INTEGER End Entity

2.5.12.2 Class C : Standard Products

2.5.12.2.1 Group Mailbox Authentication/Signature/Encryption (2.16.756.1.17.3.22.22)

Verwendungszweck:

Tbd

Warning: The usage of this policy is not recommended due to inappropriate combination of key usages. It is nevertheless listed here to match the official product catalogue.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.7:<Locality z.B. Bern> 2.5.4.10:<Organizationname z.B. Kanton Bern> 2.5.4.11:eGov-Services 2.5.4.11:Group Mailboxes 2.5.4.3:<Displayname Groupmailbox z.B. _BIT-PKI-Info>	
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	‘00010111’B	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	

X.509 Field	OIDs/Values	Comments
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.22	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 Policy for Group Mail Box	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	clientAuthentication

X.509 Field	OIDs/Values	Comments
	1.3.6.1.5.5.7.3.4	emailProtection
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.12.2.2 Group Mailbox Signature/Encryption (2.16.756.1.17.3.22.64)

Verwendungszweck: Tbd

History: New policy for Group Mailboxes without Authentication Ext. Key Usage the 28th sept. 2016 - MetB

Warning: The usage of this policy is not recommended due to inappropriate combination of key usages. It is nevertheless listed here to match the official product catalogue.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	Unique integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location z.B. Bern>	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.10:<Organizationname z.B. Kanton Bern> 2.5.4.11:eGov-Services 2.5.4.11:Group Mailboxes 2.5.4.3:<Displayname Groupmailbox z.B. _BIT-PKI-Info>	
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits ‘111’B	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.64	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 Policy for Group Mailbox signature and encryption purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Secure Email Encrypting File System

X.509 Field	OIDs/Values	Comments
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <<rfc822 Email>>	RFC 822 Email

2.5.12.2.3 Person Authentication (2.16.756.1.17.3.22.36)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Organisation Name> 2.5.4.11: <Organisation Unit> 2.5.4.3:<Common Name>	UTF8String directoryName L = City O = City or Administration Unit or Swiss Government PKI etc. OU = Organisation Unit CN = Lastname Firstname

X.509 Field	OIDs/Values	Comments
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.36	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for person authentication	VisibleString id-qt-unotice RFC 3280

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.4 Person Signature (2.16.756.1.17.3.22.67)

Verwendungszweck:

ClassC Certiticate for signature purpose only. (SECURE MAIL ENABLED)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Organisation Name> 2.5.4.11: <Organisation Unit> 2.5.4.3:<Common Name>	UTF8String directoryName L = City O = City or Administration Unit or Swiss Government PKI etc. OU = Organisation Unit CN = Lastname Firstname
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.67	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for person authentication	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN

X.509 Field	OIDs/Values	Comments
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4	Secure Email
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.5 Person Encryption (2.16.756.1.17.3.22.68)

Verwendungszweck:

ClassC Certificate for encryption purpose only. (SECURE MAIL ENABLED)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Organisation Name> 2.5.4.11: <Organisation Unit> 2.5.4.3:<Common Name>	UTF8String directoryName L = City O = City or Administration Unit or Swiss Government PKI etc. OU = Organisation Unit CN = Lastname Firstname
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING

X.509 Field	OIDs/Values	Comments
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.36	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for person authentication	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs

X.509 Field	OIDs/Values	Comments
	ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.6 Person Authentication/Signature (2.16.756.1.17.3.22.40)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	

X.509 Field	OIDs/Values	Comments
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Organisation Name> 2.5.4.11: <Organisation Unit> 2.5.4.3:<Common Name>	UTF8String directoryName L = City O = City or Administration Unit or Swiss Government PKI etc. OU = Organisation Unit CN = Lastname Firstname
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	6 unused bits '11'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.40	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for persons authentication and signature purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING

X.509 Field	OIDs/Values	Comments
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4	Client Authentication Secure Email
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.7 Person Authentication/Signature/Encryption (2.16.756.1.17.3.22.41)

Verwendungszweck:

Tbd

Warning: The usage of this policy is not recommended due to inappropriate combination of key usages. It is nevertheless listed here to match the official product catalogue.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert

X.509 Field	OIDs/Values	Comments
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Organisation Name> 2.5.4.11: <Organisation Unit> 2.5.4.3:<Common Name>	UTF8String directoryName L = City O = City or Administration Unit or Swiss Government PKI etc. OU = Organisation Unit CN = Lastname Firstname
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '111'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	

X.509 Field	OIDs/Values	Comments
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.41	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for persons authentication signature and encryption purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers

X.509 Field	OIDs/Values	Comments
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Client Authentication Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1]< rfc822 Email>	RFC 822 Email

2.5.12.2.8 Person Signature/Encryption (2.16.756.1.17.3.22.42)

Verwendungszweck:

Tbd

Warning: The usage of this policy is not recommended due to inappropriate combination of key usages. It is nevertheless listed here to match the official product catalogue.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]

X.509 Field	OIDs/Values	Comments
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Organisation Name> 2.5.4.11: <Organisation Unit> 2.5.4.3:<Common Name>	UTF8String directoryName L = City O = City or Administration Unit or Swiss Government PKI etc. OU = Organisation Unit CN = Lastname Firstname
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '111'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	1	

X.509 Field	OIDs/Values	Comments
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.42	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for persons signature and encryption purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1]<<rfc822 Email>	RFC 822 Email

2.5.12.2.9 Organization Authentication (2.16.756.1.17.3.22.37)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Organisation Name> 2.5.4.11: <Organisation Unit> 2.5.4.3: <UID>	UTF8String directoryName L = Ort O = *Name Firma oder Bezeichnung* OU = *Zusätzlicher Name* CN = UID (see https://www.uid.admin.ch)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	

X.509 Field	OIDs/Values	Comments
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.37	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for organization authentication	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.10 Organization Authentication/Signature (2.16.756.1.17.3.22.43)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	“110216090000Z”	UTC TIME ETSI TS 102 280
notAfter	“140216085959Z”	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location>	UTF8String directoryName L = Ort

X.509 Field	OIDs/Values	Comments
	2.5.4.10: <Organisation Name> 2.5.4.11: <Organisation Unit> 2.5.4.3: <UID>	O = *Name Firma oder Bezeichnung* OU = *Zusätzlicher Name* CN = UID (see https://www.uid.admin.ch)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits ‘11’B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	

X.509 Field	OIDs/Values	Comments
extnValue	2.16.756.1.17.3.22.43	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for organization authentication and signature purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4	Client Authentication Secure Email
subjectAltName		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.11 Organization Authentication/Signature/Encryption (2.16.756.1.17.3.22.44)

Verwendungszweck:

Tbd

Warning: The usage of this policy is not recommended due to inappropriate combination of key usages. It is nevertheless listed here to match the official product catalogue.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:<CH> 2.5.4.7:<Location> 2.5.4.10: <Organisation Name>	UTF8String directoryName L = Ort O = *Name Firma Bezeichnung oder UID* (see https://www.uid.admin.ch)

X.509 Field	OIDs/Values	Comments
	2.5.4.11: <Organisation Unit> 2.5.4.3: <Common Name>	OU = *Zusätzlicher Name oder UID* (see https://www.uid.admin.ch) CN = *Name Firma oder Bezeichnung*
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '111'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.44	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for organization authentication signature and encryption purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Client Authentication Secure Email Encrypting File System
subjectAltName		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.12 Organization Signature/Encryption (2.16.756.1.17.3.22.45)

Verwendungszweck:

Tbd

Warning: The usage of this policy is not recommended due to inappropriate combination of key usages. It is nevertheless listed here to match the official product catalogue.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Organisation Name>	UTF8String directoryName L = Ort O = *Name Firma oder Bezeichnung*

X.509 Field	OIDs/Values	Comments
	2.5.4.11: <Organisation Unit> 2.5.4.3: <UID>	OU = *Zusätzlicher Name* CN = UID (see https://www.uid.admin.ch)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '111'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.45	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for organization signature and encryption purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates

X.509 Field	OIDs/Values	Comments
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.13 System Authentication (2.16.756.1.17.3.22.46)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11: <Systemplattform-Name> 2.5.4.3: <System-Name>	UTF8String directoryName z.B. O = *Systemplattform eDokumente* z.B. CN = TUSER-SYSP-SCU1119B
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption

X.509 Field	OIDs/Values	Comments
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.46	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for system authentication	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps

X.509 Field	OIDs/Values	Comments
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.14 System Authentication/Signature (2.16.756.1.17.3.22.47)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11: <Systemplattform-Name> 2.5.4.3: <System-Name>	UTF8String directoryName z.B. O = *Systemplattform eDokumente* z.B. CN = TUSER-SYSP-SCU1119B
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '11'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.47	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for system authentication and signature purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4	Client Authentication Secure Email
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.15 System Authentication/Signature/Encryption (2.16.756.1.17.3.22.48)

Verwendungszweck:

Tbd

Warning: The usage of this policy is not recommended due to inappropriate combination of key usages. It is nevertheless listed here to match the official product catalogue.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		

X.509 Field	OIDs/Values	Comments
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11: <Systemplattform-Name> 2.5.4.3: <System-Name>	UTF8String directoryName z.B. OU = *Systemplattform eDokumente* z.B. CN = TUSER-SYSP-SCU1119B
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '111'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.48	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for system authentication signature and encryption purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs

X.509 Field	OIDs/Values	Comments
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Client Authentication Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.16 System Signature/Encryption (2.16.756.1.17.3.22.49)

Verwendungszweck:

Tbd

Warning: The usage of this policy is not recommended due to inappropriate combination of key usages. It is nevertheless listed here to match the official product catalogue.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	

X.509 Field	OIDs/Values	Comments
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11: <Systemplattform-Name> 2.5.4.3: <System-Name>	UTF8String directoryName z.B. O = *Systemplattform eDokumente* z.B. CN = TUSER-SYSP-SCU1119B
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	6 unused bits '11'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.49	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for system signature and encryption purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING

X.509 Field	OIDs/Values	Comments
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.17 System Signature (2.16.756.1.17.3.22.53)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]

X.509 Field	OIDs/Values	Comments
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11: <Systemplattform-Name> 2.5.4.3: <System-Name>	UTF8String directoryName z.B. O = *Systemplattform eDokumente* z.B. CN = TUSER-SYSP-SCU1119B
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '11'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.53	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for System Signature purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.2.18 System Encryption (2.16.756.1.17.3.22.55)

Verwendungszweck:

Tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
Algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
Parameters	NULL	
Signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
Version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		

X.509 Field	OIDs/Values	Comments
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11: <Systemplattform-Name> 2.5.4.3: <System-Name>	UTF8String directoryName z.B. O = *Systemplattform eDokumente* z.B. CN = TUSER-SYSP-SCU1119B
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
Parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
Critical	TRUE	BOOLEAN
extnValue	6 unused bits '001'B	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	

X.509 Field	OIDs/Values	Comments
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.55	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for System Encryption purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates

X.509 Field	OIDs/Values	Comments
	Secure Email (1.3.6.1.5.5.7.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.3 Class D : Customer specific Policies

2.5.12.3.1 Client Authentication (2.16.756.1.17.3.22.31)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280

X.509 Field	OIDs/Values	Comments
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Anwendungen 2.5.4.3:<Anwendungsname z.B. SEDEX>	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.31	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for client authentication purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
subjectAltName		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.12.3.2 Process Authentication EJPD SSO-Portal (2.16.756.1.17.3.22.35)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique random integer	Unique random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"YYMMDDHHMMSSZ"	UTC TIME ETSI TS 102 280
notAfter	"YYMMDDHHMMSSZ"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Name Verwaltung>	UTF8String directoryName L = Stadt oder Gemeinde O = Stadt- Gemeindeverwaltung etc.

X.509 Field	OIDs/Values	Comments
	2.5.4.11: SSO Portal EJPD 2.5.4.3:<Common Name>	OU = Konstante „SSO Portal EJPD“ CN = Maschinenname oder Benutzername
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	`. . . . . ` B	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . . ` O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`. . . . . ` O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	` 00001101 ` B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.35	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for Authentication/Encryption the EJPD SSO portal	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	clientAuthentication
	1.3.6.1.5.5.7.3.4	emailProtection
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates

X.509 Field	OIDs/Values	Comments
	[1] rfc822 Email	RFC 822 Email
	[0] OID 1.3.6.1.4.1.311.20.2.3 UTF8 String	Microsoft UPN

2.5.12.3.3 Governikus Core Signature Certificate (2.16.756.1.17.3.22.57)

Verwendungszweck:

This is the Swiss Government Regular CA 01 CP for Governikus Core Signature only purposes.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	Xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:Bern 2.5.4.10:BIT	UTF8String directoryName C= Landesabkürzung nach ISO 3166 L = Standort O = Organisation OU = Market Operations

X.509 Field	OIDs/Values	Comments
	2.5.4.11:Governikus 2.5.4.3:Governikus Core Signature Certificate	CN = Governikus <Funktion>
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	‘010000000’B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.57	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for Governikus Core Signature purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37	OCTECT STING encapsulates
critical	TRUE SEQUENCE OF OIDs	BOOLEAN
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates

X.509 Field	OIDs/Values	Comments
	[1] rfc822 Email	RFC 822 Email (OPTIONAL)

2.5.12.3.4 Governikus OSCI Transport Encryption Certificate (2.16.756.1.17.3.22.58)

Verwendungszweck:

This is the Swiss Government Regular CA 01 CP for Governikus OSCI Transport Encryption purposes

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature		2048 bit
TBSCertificate		
version	2	v3 cert
serialNumber	Xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:Bern 2.5.4.10:BIT 2.5.4.11:Governikus 2.5.4.3: Governikus OSCI Transport Encryption Certificate	UTF8String directoryName C= Landesabkürzung nach ISO 3166 L = Standort O = Organisation OU = Market Operations CN = Governikus <Funktion>
subjectPublicKeyInfo		

X.509 Field	OIDs/Values	Comments
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	1	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.58	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for Governikus OSCI Transport Encryption purposes	VisibleString id-qt-unotice RFC 3280

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl	uri IA5String ldap uri IA5String CA Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37	OCTECT STING encapsulates
critical	TRUE SEQUENCE OF OIDs	BOOLEAN
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email (OPTIONAL)

2.5.12.3.5 Governikus OSCI Transport Signature Certificate (2.16.756.1.17.3.22.59)

Verwendungszweck:

This is the Swiss Government Regular CA 01 CP for Governikus OSCI Transport Signature only purposes

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	Xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:Bern 2.5.4.10:BIT 2.5.4.11:Governikus 2.5.4.3: Governikus OSCI Transport Signature Certificate	UTF8String directoryName C= Landesabkürzung nach ISO 3166 L = Standort O = Organisation OU = Market Operations CN = Governikus <Funktion>
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.59	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for Governikus OSCI Transport Signature purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	

X.509 Field	OIDs/Values	Comments
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37	OCTECT STING encapsulates
critical	TRUE SEQUENCE OF OIDs	BOOLEAN
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email (OPTIONAL)

2.5.12.3.6 Governikus Core Timestamp Certificate (2.16.756.1.17.3.22.60)

Verwendungszweck:

This is the Swiss Government Regular CA 01 CPS for Governikus Core Timestamp only purpose

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	Xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:Bern 2.5.4.10:BIT 2.5.4.11:Governikus 2.5.4.3: Governikus Core Timestamp Certificate	UTF8String directoryName C= Landesabkürzung nach ISO 3166 L = Standort O = Organisation OU = Market Operations CN = Governikus <Funktion>
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (0x80)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.60	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for Governikus Core Timestamp purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	

X.509 Field	OIDs/Values	Comments
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37	OCTECT STING encapsulates
critical	TRUE SEQUENCE OF OIDs	BOOLEAN
	Time Stamp (1.3.6.1.5.5.7.3.8)	id-kp-timeStamping
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email (OPTIONAL)

2.5.12.3.7 ZKV (2.16.756.1.17.3. 22.25)

Verwendungszweck:

Authentifizierung Verschlüsselung

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature

X.509 Field	OIDs/Values	Comments
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:The Federal Authorities of the Swiss Confederation 2.5.4.11:Anwendungen 2.5.4.11:ZKV 2.5.4.3:Common Name SUFFIX	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	4 unused bits '1101'B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.25	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for ZKV authentication purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/ RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs

X.509 Field	OIDs/Values	Comments
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4	Email Protection
	1.3.6.1.5.5.7.3.2	Client Auth

2.5.12.3.8 SEDEX (2.16.756.1.17.3. 22.20)

Verwendungszweck:

Authentifizierung Verschlüsselung

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		

X.509 Field	OIDs/Values	Comments
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:The Federal Authorities of the Swiss Confederation 2.5.4.11:Anwendungen 2.5.4.11:SEDEX 2.5.4.3:SEDEX Adapter Name/Identifier	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	4 unused bits '1110'B	RFC 5280

X.509 Field	OIDs/Values	Comments
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.20	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for SEDEX authentication purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/ RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Email Protection (1.3.6.1.5.5.7.3.4)	
	Client Auth (1.3.6.1.5.5.7.3.2)	
sedexInternalUsage		
extnId	2.16.756.1.17.3. 23.8	OCTECT STING encapsulates
critical	FALSE	BOOLEAN
	DER encoded ASN.1 internal structure to SEDEX	OCTECT STING

2.5.12.3.9 eDOC (2.16.756.1.17.3. 22.23)

Verwendungszweck:

Authentisierung Verschlüsselung

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING

X.509 Field	OIDs/Values	Comments
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:admin 2.5.4.11: Systemplattform eDokumente 2.5.4.3: Adapter Name/Identifier	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	4 unused bits '1110'B	RFC 5280

X.509 Field	OIDs/Values	Comments
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.23	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this certificate is solely intended for system platform eDokumente application usages. The subject is a technical user referenced in the database of ISC-EJPD.	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING

X.509 Field	OIDs/Values	Comments
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4	Secure Email
	1.3.6.1.5.5.7.3.2	Client Authentication
	1.3.6.1.4.1.311.20.2.2	Smart Card Logon
	1.3.6.1.4.1.311.10.3.4	Encrypting File System

2.5.12.3.10 SPOC Server 2.16.756.1.17.3.2.19

Verwendungszweck:

Tbd

--- muss neu von SG SSL CA 01 ausgestellt werden ---

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING

X.509 Field	OIDs/Values	Comments
TBSCertificate		
version	2	v3 cert
serialNumber	Xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:BIT 2.5.4.3:SPOC TLS Server	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B	RFC 5280

X.509 Field	OIDs/Values	Comments
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.19	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for SPOC authentication purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_11_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/ RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[x] DNS Name spoc-mrtd-ws.pki.admin.ch	DNS
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	Server Authentication
	1.2.203.7064.1.1.369791.2	SPOC specific OID

2.5.12.3.11 SPOC Client (2.16.756.1.17.3.2.19)

Verwendungszweck:

Tbd

--- muss neu von SG SSL CA 01 ausgestellt werden ---

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	Xxxxx	Random

X.509 Field	OIDs/Values	Comments
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:BIT 2.5.4.3:SPOC TLS Client	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.19	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for SPOC authentication purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/ RegularCA01.crt	uri IA5String

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[x] DNS Name spoc-mrtd-ws.pki.admin.ch	DNS
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	
	SPOC specific OID (1.2.203.7064.1.1.369791.1)	

2.5.12.3.12 LRA Station System (2.16.756.1.17.3.22.24)

Verwendungszweck:

Tbd

--- muss neu von SG SSL CA 01 ausgestellt werden ---

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	Xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.3:Swiss Government Regular CA 01	
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"160216085959Z"	UTC TIME ETSI TS 102 280 (5 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Services 2.5.4.3: lra.host.name	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	

X.509 Field	OIDs/Values	Comments
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.24	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for LRA Station authentication purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[x] DNS Name lra.host.name	DNS
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Client Authentication (1.3.6.1.5.5.7.3.2)	

2.5.12.3.13 DFS / FKR - Digitaler Fahrtschreiber - DFS-CA Operator (2.16.756.1.17.3. 22.12)

Verwendungszweck:

Authentifizierung an der CA Operator Console der DFS-CA

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	“110216090000Z”	UTC TIME ETSI TS 102 280
notAfter	“140216085959Z”	UTC TIME ETSI TS 102 280 (3 years)

X.509 Field	OIDs/Values	Comments
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:DFS-Services 2.5.4.3: <Common Name>	UTF8String directoryName CN editierbar
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	`00000001` B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	

X.509 Field	OIDs/Values	Comments
extnValue	2.16.756.1.17.3. 22.12	DFS-CA Operator
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this certificate is solely intended for Digital Tachograph CA Operator Authentification purpose	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	SSLClient2.16.840.1.113730.1.1	NetscapeExtension mandatory='True' editable='False'
	GenericIA5StringExtension2.16.756.1.17.3.23.4.1	Editierbar: FL CH

2.5.12.3.14 DFS / FKR - Digitaler Fahrtschreiber - DFS-CA Service Administrator (2.16.756.1.17.3. 22.13)

Verwendungszweck:

tbd

Diese Zertifikate (Klasse D) werden zur Authentifizierung an der CA Service Console der DFS-CA verwendet.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:DFS-Services 2.5.4.3: <Common Name>	UTF8String directoryName CN editierbar
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	`00000001` B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.13	DFS-CA Service Admin
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this certificate is solely intended for Digital Tachograph CA Service Administrator Authentification purpose	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	

X.509 Field	OIDs/Values	Comments
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	SSLClient2.16.840.1.113730.1.1	NetscapeExtension mandatory='True' editable='False'
	GenericIA5StringExtension2.16.756.1.17.3.23.4.2	Editierbar FL CH

2.5.12.3.15 DFS / FKR - Digitaler Fahrtschreiber - DFS-CA (2.16.756.1.17.3. 22.14)

Verwendungszweck:

Diese Policy definiert die Eigenschaften der DFS-CA DocumentSigner Zertifikate.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11: DFS-Services 2.5.4.3: <Common Name>	UTF8String directoryName CN editierbar
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING

X.509 Field	OIDs/Values	Comments
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	`00000111` B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.14	DFS-CA Entity
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a Class D Document Signer Certificate for Digital Tachograph Certification Authority Entities	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl	uri IA5String

X.509 Field	OIDs/Values	Comments
	ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	GenericIA5StringExtension2.16.756.1.17.3.23.4.3	Editierbar FL CH

2.5.12.3.16 DFS / FKR - Digitaler Fahrtschreiber - DFS-CIA (2.16.756.1.17.3. 22.15)

Verwendungszweck:

Diese Policy definiert die Eigenschaften der DFS-CIA DocumentSigner Zertifikate.
CIA : Card Issuing Authority

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert

X.509 Field	OIDs/Values	Comments
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:DFS-Services 2.5.4.3: <Common Name>	UTF8String directoryName CN editierbar
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	`00000111` B	RFC 5280
digitalSignature	1	
nonRepudiation	1	

X.509 Field	OIDs/Values	Comments
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.15	DFS-CIA Entity
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a Class D Document Signer Certificate for Digital Tachograph Card Issuing Authority Entities	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers

X.509 Field	OIDs/Values	Comments
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	GenericIA5StringExtension2.16.756.1.17.3.23.4.4	Editierbar FL CH

2.5.12.3.17 DFS / FKR - Digitaler Fahrtschreiber - DFS-CP (2.16.756.1.17.3. 22.16)

Verwendungszweck:

Diese Policy definiert die Eigenschaften der DFS-CP DocumentSigner Zertifikate.
CP : Card Production

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		

X.509 Field	OIDs/Values	Comments
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:DFS-Services 2.5.4.3: <Common Name>	UTF8String directoryName CN editierbar
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	`00000111` B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	

X.509 Field	OIDs/Values	Comments
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.16	DFS-CP Entity
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a Class D Document Signer Certificate for Digital Tachograph Card Production Authority Entities	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	GenericIA5StringExtension2.16.756.1.17.3.23.4.5	Editierbar FL CH

2.5.12.3.18 Organization Signature eSchKG BJ (2.16.756.1.17.3. 22.54)

Verwendungszweck:

Authentisierung Digital Signature

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:<Location> 2.5.4.10: <Organisation Name> 2.5.4.11: eSchKG / e-LP / e-LEF 2.5.4.3: <Sedex-ID>	UTF8String directoryName L = Ort O = *Name Firma oder Bezeichnung* OU = *Fixer Wert* CN = Sedex-ID (evtl. Mit Abkürzung Amt)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits ‘11’B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.54	EJPD – eSchKG Verbund
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for organization signature purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN

X.509 Field	OIDs/Values	Comments
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Secure Email (1.3.6.1.5.5.7.3.4)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.3.19 ElCom (2.16.756.1.17.3.22.50)

Verwendungszweck:

Authentisierung Digital Signature

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:<Country> 2.5.4.7:<Location> 2.5.4.10: <Organisation> 2.5.4.11: <Organisation Name> 2.5.4.3: <Commen Name>	UTF8String directoryName C= Landesabkürzung nach ISO 3166 L = Land O = EXAA AG OU = Market Operations CN = ElCom-RRM-EXAA
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	

X.509 Field	OIDs/Values	Comments
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	4 unused bits ‘1110’B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.50	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for ElCom RRM Client Authentication/Signature purposes.	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	

X.509 Field	OIDs/Values	Comments
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	clientAuthentication

2.5.12.3.20 CITES System Authentication/Signature/Encryption (2.16.756.1.17.3.22.61)

Verwendungszweck:

Tbd

Warning: The usage of this policy is not recommended due to inappropriate combination of key usages. It is nevertheless listed here to match the official product catalogue.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature

X.509 Field	OIDs/Values	Comments
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:<CH> 2.5.4.7:<Location> 2.5.4.10: <Organisation Name> 2.5.4.11: <Organisation Unit> 2.5.4.3: <UID>	UTF8String directoryName C = Country L = Ort O = *Name Firma oder Bezeichnung* OU = *Zusätzlicher Name* CN = UID (see https://www.uid.admin.ch)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING

X.509 Field	OIDs/Values	Comments
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '111'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.61	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for CITES system authentication signature and encryption purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl	uri IA5String

X.509 Field	OIDs/Values	Comments
	ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2 1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Client Authentication Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.12.3.21 EESSI Signature (2.16.756.1.17.3.22.66)

Verwendungszweck:

Electronic Exchange of Social Security Information (EESSI)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH (C) 2.5.4.10:OrganizationName (O) 2.5.4.3:CommonName (CN) 2.5.4.97:organizationIdentifier (OI - different from OrganisationName) 2.5.4.11:organizationalUnitName (OU). 2.5.4.11:organizationalUnitName (OU) 2.5.4.7:localityName (L) 2.5.4.8:stateOrProvinceName (ST)	***PrintableString*** directoryName: Attribute die nicht gemäss TAV/ETSI definert werden müssen entsprechen dem Vorschlag des ISB für Amtssiegel: 2.5.4.6: C=CH oder LI 2.5.4.10: O=Name exakt wie im UID-Register 2.5.4.97: OI=„NTRCH"-UID der Behörde bzw. „VATCH"-UID bzw. „CH:"-UID der Behörde 2.5.4.3: CN=Allgemein gebräuchlicher Name der Behörde 2.5.4.11: $OU_{1..n}$:Nähere Bezeichnung 2.5.4.7: L=Bezeichnung der Gemeinde in der die Behörde ihren Sitz hat 2.5.4.8:ST= Bezeichnung des Kantons in der die Behörde ihren Sitz hat
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit

X.509 Field	OIDs/Values	Comments
Extensions		
authorityKeyIdentifier	non-critical	(a) "Authority KeyIdentifier" MUST be included as an extension in the certificate. (b) The "SubjectKeyIdentifier" of the issuing CA MUST be used. (c) AuthorityCertIssuer and AuthorityCertSerialNumber SHOULD NOT be used as AuthorityKeyIdentifier.
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier	non-critical	(a) "SubjectKeyIdentifier" MUST be included as an extension in the certificate (b) One of the methods described in clause 4.2.1.2 of [RFC 5280] MUST be used.
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage	critical	(a) "KeyUsage" MUST be included as an extension in the certificate. (b) The extension MUST be designated as critical. (c) [Seal - ebMS] [Seal – Business Signature]: The Non-Repudiation bits MUST be set to true to the exclusion of all other Key Usage bits that MUST be set to false.
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	8 unused bits '01'B	RFC 5280
digitalSignature	0	
nonRepudiation	1	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.66	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CP for EESSI signature	VisibleString id-qt-unotice RFC 5280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints	critical	
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints	non-critical	(a) "CRLDistributionPoints" MUST be included as an extension in the certificate. (b) The certificate MUST include a CRL distribution point extension. (c) When present, the CRL distribution point extension MUST include at least one reference to a publicly available CRL. (d) At least one of the present references MUST use http (http://) [RFC 7230-7235] (e) The extension shall not be marked critical.
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess	non-critical	(a) "AuthorityInfoAccess" MUST be included as an extension in the certificate. (b) When OCSP is supported by the issuing CA, the Authority Information Access extension MUST include an accessMethod OID, id-ad-ocsp, with an accessLocation value specifying at least one access

X.509 Field	OIDs/Values	Comments
		location of an OCSP [RFC 6960] responder authoritative to provide certificate status information for the present certificate. (c) When present, at least one access location MUST specify either the http (http://) [RFC 7230-7235] or https (https://) [RFC 2818] scheme to reference a publicly available OCSP responder, which accepts unsigned and unauthenticated status requests. (d) When the issuing CA is not represented by a self-signed root certificate, the Authority Information Access extension MUST include an accessMethod OID, id-ad-caIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA. At least one access location shall use the http (http://) IETF RFC 7230-7235 scheme or https (https://) IETF RFC 2818 scheme. This requirement MAY be ignored altogether when the issuing CA is represented by a self-signed root certificate.
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
~~extendedKeyUsage~~	~~non-critical~~	
~~extnId~~	~~2.5.29.37 SEQUENCE OF OIDs~~	~~OCTECT STING encapsulates~~
	~~1.3.6.1.5.5.7.3.2~~ ~~1.3.6.1.5.5.7.3.4~~ ~~1.3.6.1.4.1.311.10.3.4~~	~~Client Authentication~~ ~~Secure Email~~ ~~Encrypting File System~~
~~subjectAltName~~		
~~extnId~~	~~2.5.29.17 SEQUENCE~~	~~OCTECT STING encapsulates~~
	~~[1] <rfc822 Email>~~	~~RFC 822 Email~~

2.5.13 Swiss Government Regular CA02

2.5.13.1 Swiss Government Regular CA202 OCSP Responder (2.16.756.1.17.3.62.19)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3:RegularCA02-OCSP-Responder 2.5.4.11:Swiss Government PKI	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	….	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘11’B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.19	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocsp-nocheck		4.2.2.2.1 Revocation Checking of an Authorized Responder (RFC 2560) A CA may specify that an OCSP client can trust a responder for the lifetime of the responder's certificate. The CA does so by including the extension id-pkix-ocsp-nocheck. This SHOULD be a non-critical extension. The value of the extension should be NULL
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.13.2 Class C : Standard Products

2.5.13.2.1 Person Authentication (2.16.756.1.17.3.62.20)

Verwendungszweck:

(Entwurf zur Durchsicht)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"210907090000Z"	UTC TIME ETSI TS 102 280
notAfter	"240907859592"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3:Givenname Surname Hash 2.5.4.4:Surname 2.5.4.42:Givenname 2.5.4.11: Organizationunitname 2.5.4.10: Organizationname 2.5.4.97: OrganizationIdentifier 2.5.4.6:CH	PrintableString directoryName 2.5.4.97:NTRCH-CHE-xxxxx (OrganizationIdentifier)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING

X.509 Field	OIDs/Values	Comments
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.20 , 0.4.0.2042.1.3 ,	LCP
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for person authentication	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.13.2.2 Person Signature (2.16.756.1.17.3.62.21)

Verwendungszweck:

(Entwurf zur Durchsicht)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	

X.509 Field	OIDs/Values	Comments
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"210907090000Z"	UTC TIME ETSI TS 102 280
notAfter	"240907859592"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3:Givenname Surname Hash 2.5.4.4:Surname 2.5.4.42:Givenname 2.5.4.11: Organizationunitname 2.5.4.10: Organizationname 2.5.4.97: OrganizationIdentifier 2.5.4.6:CH	PrintableString directoryName 2.5.4.97:NTRCH-CHE-xxxxx (OrganizationIdentifier)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING

X.509 Field	OIDs/Values	Comments
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.21 , 0.4.0.2042.1.3 ,	LCP
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for person signature	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4	Secure Email
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.13.2.3 Person Encryption (2.16.756.1.17.3.62.22)

Verwendungszweck:

(Entwurf zur Durchsicht)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert

X.509 Field	OIDs/Values	Comments
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"210907090000Z"	UTC TIME ETSI TS 102 280
notAfter	"240907859592"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3:Givenname Surname Hash 2.5.4.4:Surname 2.5.4.42:Givenname 2.5.4.11: Organizationunitname 2.5.4.10: Organizationname 2.5.4.97: OrganizationIdentifier 2.5.4.6:CH	PrintableString directoryName 2.5.4.97:NTRCH-CHE-xxxxx (OrganizationIdentifier)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.22 , 0.4.0.2042.1.3 ,	LCP
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for person encryption	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	

X.509 Field	OIDs/Values	Comments
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.13.2.4 Organization Authentication (2.16.756.1.17.3.62.23)

Verwendungszweck:

(Entwurf zur Durchsicht)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regular CA 02	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	
validity		
notBefore	"210907090000Z"	UTC TIME ETSI TS 102 280
notAfter	"240907859592"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3: <UID> 2.5.4.11: Organizationunitname 2.5.4.10: Organizationname 2.5.4.97: OrganizationIdentifier 2.5.4.6:CH	PrintableString directoryName 2.5.4.97:NTRCH-CHE-xxxxx (OrganizationIdentifier)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.23 , 0.4.0.2042.1.3 ,	LCP
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for organization authentication	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp

X.509 Field	OIDs/Values	Comments
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.13.2.5 Organization Signature (2.16.756.1.17.3.62.24)

Verwendungszweck:

(Entwurf zur Durchsicht)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		

X.509 Field	OIDs/Values	Comments
notBefore	"210907090000Z"	UTC TIME ETSI TS 102 280
notAfter	"240907859592"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3: <UID> 2.5.4.11: Organizationunitname 2.5.4.10: Organizationname 2.5.4.97: OrganizationIdentifier 2.5.4.6:CH	PrintableString directoryName 2.5.4.97:NTRCH-CHE-xxxxx (OrganizationIdentifier)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	

X.509 Field	OIDs/Values	Comments
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.24 , 0.4.0.2042.1.3 ,	LCP
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for organization signature	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4	Secure Email

X.509 Field	OIDs/Values	Comments
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.13.2.6 Organization Encryption (2.16.756.1.17.3.62.25)

Verwendungszweck:

(Entwurf zur Durchsicht)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	“210907090000Z”	UTC TIME ETSI TS 102 280
notAfter	“240907859592”	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3: <UID> 2.5.4.11: Organizationunitname 2.5.4.10: Organizationname	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.97: OrganizationIdentifier 2.5.4.6:CH	2.5.4.97:NTRCH-CHE-xxxxx (OrganizationIdentifier)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.25 , 0.4.0.2042.1.3 ,	LCP

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for organization encryption	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.13.2.7 System Authentication (2.16.756.1.17.3.62.26)

Verwendungszweck:

(Entwurf zur Durchsicht)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"210907090000Z"	UTC TIME ETSI TS 102 280
notAfter	"240907859592"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3: <System-Name> 2.5.4.11: <Systemplattform-Name> 2.5.4.10: Organizationname 2.5.4.97: OrganizationIdentifier 2.5.4.6:CH	PrintableString directoryName 2.5.4.97:NTRCH-CHE-xxxxx (OrganizationIdentifier)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.26 , 0.4.0.2042.1.3 ,	LCP
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for system authentication	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	Client Authentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.13.2.8 System Signature (2.16.756.1.17.3.62.27)

Verwendungszweck:

(Entwurf zur Durchsicht)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"210907090000Z"	UTC TIME ETSI TS 102 280
notAfter	"240907859592"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3: <System-Name> 2.5.4.11: <Systemplattform-Name> 2.5.4.10: Organizationname 2.5.4.97: OrganizationIdentifier 2.5.4.6:CH	PrintableString directoryName 2.5.4.97:NTRCH-CHE-xxxxx (OrganizationIdentifier)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	**1**	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.27 , 0.4.0.2042.1.3 ,	LCP
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for system signature	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	

X.509 Field	OIDs/Values	Comments
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4	Secure Email
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.13.2.9 System Encryption (2.16.756.1.17.3.62.28)

Verwendungszweck:

(Entwurf zur Durchsicht)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING

X.509 Field	OIDs/Values	Comments
TBSCertificate		
version	2	v3 cert
serialNumber	unique Integer	Random [integer]
issuer	2.5.4.3:Swiss Government Regular CA 02 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.11:Swiss Government PKI 2.5.4.97:NTRCH-CHE-221.032.573 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"210907090000Z"	UTC TIME ETSI TS 102 280
notAfter	"240907859592"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.3: <System-Name> 2.5.4.11: <Systemplattform-Name> 2.5.4.10: Organizationname 2.5.4.97: OrganizationIdentifier 2.5.4.6:CH	PrintableString directoryName 2.5.4.97:NTRCH-CHE-xxxxx (OrganizationIdentifier)
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	

X.509 Field	OIDs/Values	Comments
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	**1**	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.28 , 0.4.0.2042.1.3 ,	LCP
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for system encryption	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4 1.3.6.1.4.1.311.10.3.4	Secure Email Encrypting File System
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] <rfc822 Email>	RFC 822 Email

2.5.13.2.10 ZKV (2.16.756.1.17.3.62.29)

Verwendungszweck:

Authentifizierung Verschlüsselung

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random

X.509 Field	OIDs/Values	Comments
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 02	PrintableString directoryName
validity		
notBefore	"220630090000Z"	UTC TIME ETSI TS 102 280
notAfter	"250630085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:The Federal Authorities of the Swiss Confederation 2.5.4.11:Anwendungen 2.5.4.11:ZKV 2.5.4.3:Common Name SUFFIX	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	4 unused bits '1101'B	RFC 5280
digitalSignature	1	
nonRepudiation	0	

X.509 Field	OIDs/Values	Comments
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.29	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for ZKV authentication purposes	VisibleString id-qt-unotice RFC 5280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	https://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_7.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	https://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	

X.509 Field	OIDs/Values	Comments
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4	Email Protection
	1.3.6.1.5.5.7.3.2	Client Auth

2.5.13.2.11 eDOC (2.16.756.1.17.3.62.30)

Verwendungszweck:

Authentisierung Verschlüsselung

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 02	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:admin 2.5.4.11: Systemplattform eDokumente 2.5.4.3: Adapter Name/Identifier	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	4 unused bits '1110'B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	

X.509 Field	OIDs/Values	Comments
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.23	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this certificate is solely intended for system platform eDokumente application usages. The subject is a technical user referenced in the database of ISC-EJPD.	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

X.509 Field	OIDs/Values	Comments
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.4	Secure Email
	1.3.6.1.5.5.7.3.2	Client Authentication

2.5.13.2.12 SEDEX (2.16.756.1.17.3.62.31)

Verwendungszweck:

Authentifizierung Verschlüsselung

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 02	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)

X.509 Field	OIDs/Values	Comments
subject	2.5.4.6:CH 2.5.4.10:The Federal Authorities of the Swiss Confederation 2.5.4.11:Anwendungen 2.5.4.11:SEDEX 2.5.4.3:SEDEX Adapter Name/Identifier	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	4 unused bits ‘1110’B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	1	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3. 22.20	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 02 CPS for SEDEX authentication purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA02.crl	uri IA5String
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RegularCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Email Protection (1.3.6.1.5.5.7.3.4)	

X.509 Field	OIDs/Values	Comments
	Client Auth (1.3.6.1.5.5.7.3.2)	
sedexInternalUsage		
extnId	2.16.756.1.17.3. 23.8	OCTECT STING encapsulates
critical	FALSE	BOOLEAN
	DER encoded ASN.1 internal structure to SEDEX	OCTECT STING

2.5.14 Swiss Government SSL CA 01

2.5.14.1 Swiss Government SSL CA 01 OCSP Responder (2.16.756.1.17.3.22.63)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
Signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
Version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	6566605112202185b3c1da23bcd9cc2e	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.

X.509 Field	OIDs/Values	Comments
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government SSL CA 01	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z" (Montag 5. November 2018 15:58:57)	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z" (Dienstag 5. November 2019 15:58:57)	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.3: OCSP-Responder-SSLCA01	Holder information e.g. "CH" Holder information e.g. "Bern" Holder information e.g. "Swiss Government PKI" Holder information e.g. "Services" Holder information
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.1	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '10'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.63	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocsp-nocheck		4.2.2.2.1 Revocation Checking of an Authorized Responder (RFC 2560) A CA may specify that an OCSP client can trust a responder for the lifetime of the responder's certificate. The CA does so by including the extension id-pkix-ocsp-nocheck. This SHOULD be a non-critical extension. The value of the extension should be NULL
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.5.14.2 SSL Server Authentication (2.16.756.1.17.3.22.26)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government SSL CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:Bern 2.5.4.10:Swiss Government PKI 2.5.4.11:Servers 2.5.4.11:SSL 2.5.4.3:FQDN	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	.....	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '101'B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.26	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this certificate is solely intended for SSL web server authentication.	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	

X.509 Field	OIDs/Values	Comments
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/ SSLCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Gvernment SSL CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government SSL CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/ SSLCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	serverAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc1034 dNSName	IA5String or
	[2] rfc791 iPAdress	OCTECT STING in “network byte order”

2.5.14.3 SSL Client Authentication (2.16.756.1.17.3.22.27)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government SSL CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Clients 2.5.4.11:SSL 2.5.4.3:FQDN	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '1'B (bit 0)	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.27	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this certificate is solely intended for SSL web client authentication.	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	

X.509 Field	OIDs/Values	Comments
extnValue	http://www.pki.admin.ch/crl/ SSLCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government SSL CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government SSL CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/ SSLCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	clientAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc1034 dNSName	IA5String or
	[2] rfc791 iPAdress	OCTECT STING in “network byte order”

2.5.14.4 SSL Server / Client Authentication (2.16.756.1.17.3.22.10)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature

X.509 Field	OIDs/Values	Comments
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government SSL CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Servers 2.5.4.11:SSL 2.5.4.3:FQDN	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '101'B	Digital Signature Key Encipherment
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.10	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this certificate is solely intended for SSL web server and client authentication.	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/ SSLCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government SSL CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government SSL CA 01 CDPs

X.509 Field	OIDs/Values	Comments
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/ SSLCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	serverAuthentication
	1.3.6.1.5.5.7.3.2	clientAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc1034 dNSName	IA5String or
	[2] rfc791 iPAdress	OCTECT STING in “network byte order”

2.5.14.5 CodeSigning (2.16.756.1.17.3.22.5)

Verwendungszweck:

Vertrauenswürdige Signierung von Software die öffentlich verteilt wird. Im gleichen Zug werden die Endanwender der signierten Software über den Ursprung und die Integrität der Software und über die Identität des Herausgebers informiert.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	

X.509 Field	OIDs/Values	Comments
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government SSL CA 01	PrintableString directoryName
validity		
editable	FALSE	1 or 2 years
notBefore	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280 (1 year or 2 years)
subject	2.5.4.6: CH 2.5.4.7: <Locality> 2.5.4.10: <Organisation> 2.5.4.11: <Organisational Unit> 2.5.4.11: <Organisational Unit> 2.5.4.3: <CN>	UTF8String directoryName O = Description according to UID-Register z.B "Bundesamt für Zukunftsforschung (BFZ)" OU = UID according to UID-Register z.B. "CHE-123.456.789" OU = Organisational Unit z.B „Büroautomation" CN = Description according to UID-Register z.B "Bundesamt für Zukunftsforschung (BFZ)"
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING Include Authority Key Identifier
subjectKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
critical	FALSE	

X.509 Field	OIDs/Values	Comments
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.5	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government SSL CA 01 CP for code signing	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	
extnId	2.5.29.19	
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/SSLCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government SSL CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government SSL CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/SSLCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.3	id_kp_codeSigning
subjectAltName		
critical	FALSE	
mandatory	TRUE	
editable	TRUE	
visible	TRUE	
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.5.14.6 Domain Controller (2.16.756.1.17.3.22.56)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government SSL CA 01	PrintableString directoryName
validity		
editable	FALSE	1 or 2 years
notBefore	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280 (1 year or 2 years)
subject	2.5.4.6: CH 2.5.4.7: <Locality> 2.5.4.10: <Organisation> 2.5.4.11: <Organisational Unit> 2.5.4.3: <CN>	UTF8String directoryName L = Locality zB. „Bern" O = Description Organization z.B "Bundesamt für Zukunftsforschung (BFZ)" OU = Organisational Unit z.B „Büroautomation" CN = FQDN z.B. „DC1.irgendetwas.bit.admin.ch"
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
critical	FALSE	
mandatory	TRUE	

X.509 Field	OIDs/Values	Comments
editable	FALSE	
visible	FALSE	
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING Include Authority Key Identifier
subjectKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	‘101000000’B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	

X.509 Field	OIDs/Values	Comments
certificatePolicies		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.56	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government SSL CA 01 CP for domain controller	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	
extnId	2.5.29.19	
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/SSLCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government SSL CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government SSL CA 01 CDPs
authorityInfoAccess		SEQUENCE

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/SSLCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	Server Authentication
	1.3.6.1.5.5.7.3.2	Client Authentication
subjectAltName		
critical	FALSE	
mandatory	TRUE	
editable	TRUE	
visible	TRUE	
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] Other Name:1.3.6.1.4.1.311.25.1=<GUID> [2] DNS Name=<FQDN>	
certificateTemplateName		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.4.1.311.20.2 SEQUENCE	
	DomainController	

2.6 OBSOLETE

2.6.1 Issuing CA Policies

2.6.1.1 Swiss Government SuisseID Authentication CA 01

Verwendungszweck:

obsolete

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	PrintableString directoryName
validity		
notBefore	"110215090000Z"	UTC TIME ETSI TS 102 280

X.509 Field	OIDs/Values	Comments
notAfter	"250215085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government SuisseID Authentication CA 01	UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	

X.509 Field	OIDs/Values	Comments
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.1.0	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Root CA I CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER 0 child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAI.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA I ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Root CA I CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAI.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.6.1.2 Swiss Government EV SSL CA 01

Verwendungszweck:

obsolete

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
signature		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA II	PrintableString directoryName
validity		
notBefore	"140515090000Z"	UTC TIME ETSI TS 102 280
notAfter	"280515085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government EV SSL CA 01	UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	

X.509 Field	OIDs/Values	Comments
subjectPublicKey	…..	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	‘000001100	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	anyPolicy
extnValue	2.16.756.1.17.3.21.3	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this subordinate CA is for EV SSL server issuance only.	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAII.crl ldap://admindir.admin.ch:389/cn=Swiss Government EV SSL CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Root CA II CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/EVSSLCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.6.1.3 Swiss Government Public Trust EV CA 02

Verwendungszweck:

Issuing CA: Swiss Government Public Trust EV CA 02

Obsolete

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
algorithm	1.2.840.113549.1.1.11: sha256WithRSASignature	This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate. This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence Certificate. The contents of the optional parameters field will vary according to the algorithm identified.
parameters	NULL	
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements
issuer	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:www.pki.admin.ch 2.5.4.3:Swiss Government Root CA III	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	“140515090000Z”	UTC TIME ETSI TS 102 280
notAfter	“280515085959Z”	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services	The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name MAY be carried in the subject field and/or the subjectAltName extension. If the subject is a CA then the subject field MUST be populated with a non-empty

X.509 Field	OIDs/Values	Comments
	2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust EV CA 02	distinguished name matching the contents of the issuer field in all certificates issued by the subject CA. PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	‘000001100	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	
encipherOnly	0	

X.509 Field	OIDs/Values	Comments
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	anyPolicy
extnValue	2.16.756.1.17.3.61.2	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAIII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA IIIou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.6.1.4 Swiss Government Regulated CA 01

Verwendungszweck:

Issuing CA: Swiss Government Regulated CA 01 (2.16.756.1.17.3.5.1.1)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxxxxx	Random
issuer	2.5.4.3:Swiss Government Root CA IV 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.6:CH	PrintableString directoryName
validity		
notBefore	"110215090000Z"	UTC TIME ETSI TS 102 280
notAfter	"250215085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.3:Swiss Government Regulated CA 01 2.5.4.11:Swiss Government PKI 2.5.4.10:Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97:VATCH-CHE-221.032.573 2.5.4.6:CH	UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name) 2.5.4.97: organisationIdentifier (ETSI EN 319 412-2 V2.1.1 4.2.3.1 Legal person issuers TAV 2.3.2 b))
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	.....	BIT STRING 4096 bit

X.509 Field	OIDs/Values	Comments
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	Issuier KeyID
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.5.1.1	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is an issuing CA regulated certificate as defined by the Swiss federal law SR 943.03 ZertES	UTF8String encoding id-qt-unotice RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d). Dies liegt zwar in einem Widerspruch zur Definition in rfc5280: „To prevent such duplication this qualifier SHOULD only be present in end entity certificates and CA certificates issued to other organizations.") Der ausführlichere Text wäre für relying Parties aussagekräftiger

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf	uri IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAIV.crl	uri IA5String ldap uri IA5String CA inherits CDPs LDAP Eintrag entfernen Grund – Redesign AdminDir
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIV.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.6.1.5 Swiss Government Public Trust Code Signing EV CA 02 (2.16.756.1.17.3.61.4)

Verwendungszweck:

Issuing CA: Swiss Government Public Trust Code Signing EV CA 02

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
algorithm	1.2.840.113549.1.1.11: sha256WithRSASignature	This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate. This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence Certificate. The contents of the optional parameters field will vary according to the algorithm identified.
parameters	NULL	
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements
issuer	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:www.pki.admin.ch 2.5.4.3:Swiss Government Root CA III	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	“yymmddhhmmssZ”	UTC TIME ETSI TS 102 280
notAfter	“yymmddhhmmssZ”	UTC TIME ETSI TS 102 280 (14 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI	The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name MAY be carried in the subject field and/or the subjectAltName extension. If the subject

X.509 Field	OIDs/Values	Comments
	2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Code Signing EV CA 02	is a CA then the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject CA. PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	

X.509 Field	OIDs/Values	Comments
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	anyPolicy
extnValue	2.16.756.1.17.3.61.4	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAIII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA IIIou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.6.1.6 Swiss Government Qualified CA 01 (2.16.756.1.17.3.1.0)

Verwendungszweck:

Ausstellung von Klasse A Zertifikaten.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	00ae915652b451cdbba2d9e3d97ddfec78	Random
issuer	2.5.4.6:CH 2.5.4.10: The Federal Authorities of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Root CA I	PrintableString directoryName
validity		
notBefore	"110215090000Z"	UTC TIME ETSI TS 102 280
notAfter	"250215085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:C 2.5.4.10:Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Qualified CA 01	UTF8String directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey		BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.35	DN + Cert Serial
extnValue		OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue		OCTET STRING 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.1.0	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	O=ZertES Recognition Body: KPMG AG	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
issuerAltName		
extnId	2.5.29.18	UTF8String directoryName
extnValue	O=ZertES Recognition Body: KPMG AG	
basicConstraints		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAI.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA Iou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA inherits CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAI.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
qcStatments		
etxnId	1.3.6.1.5.5.7.1.3	
critical	FLASE	BOOLEAN
extnValue	SEQUENCE OF	OCTET STRING
QCStatment	SEQUENCE	
statmentId	0.4.0.1862.1.1	qcs-Qccompliance
issuerAltName		
etxnId	2.5.29.18	UTF8String directoryName
extnValue	O=ZertES Recognition Body: KPMG AG	

2.6.1.7 Swiss Government Public Trust Standard CA 02 (2.16.756.1.17.3.61.1)

Dekommissioniert: 21.01.2021

Verwendungszweck:

Issuing CA: Swiss Government Public Trust Standard CA 02

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
algorithm	1.2.840.113549.1.1.11: sha256WithRSASignature	This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate. This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence Certificate. The contents of the optional parameters field will vary according to the algorithm identified.
parameters	NULL	
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	20-Bit entropy	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:www.pki.admin.ch 2.5.4.3:Swiss Government Root CA III	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName

X.509 Field	OIDs/Values	Comments
validity		
notBefore	"140515090000Z"	UTC TIME ETSI TS 102 280
notAfter	"280515085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 02	The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name MAY be carried in the subject field and/or the subjectAltName extension. If the subject is a CA then the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject CA. PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey		BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue		OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue		OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'	certSign crlSign
digitalSignature	0	
nonRepudiation	0	

X.509 Field	OIDs/Values	Comments
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
critical	TRUE	BR 1.3.3 Chap. 7.1.2.2 a.
extnValue	2.16.756.1.17.3.61.1	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 5280
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAIII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA IIIou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	

X.509 Field	OIDs/Values	Comments
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.6.1.8 Swiss Government Public Trust Standard CA 03 (2.16.756.1.17.3.61.6)

Dekommissioniert: 21.01.2021

Verwendungszweck:

Issuing CA: Swiss Government Public Trust Standard CA 03

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
algorithm	1.2.840.113549.1.1.11: sha256WithRSASignature	This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate. This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence Certificate. The contents of the optional parameters field will vary according to the algorithm identified.
parameters	NULL	
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When

X.509 Field	OIDs/Values	Comments
		extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	20-Bit entropy	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:www.pki.admin.ch 2.5.4.3:Swiss Government Root CA III	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"140515090000Z"	UTC TIME ETSI TS 102 280
notAfter	"280515085959Z"	UTC TIME ETSI TS 102 280
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 03	The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name MAY be carried in the subject field and/or the subjectAltName extension. If the subject is a CA then the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject CA. PrintableString directoryName. Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING

X.509 Field	OIDs/Values	Comments
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
critical	FALSE	BR 1.5.1 Chap. 7.1.2.2 a
extnValue	2.16.756.1.17.3.61.6	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	

X.509 Field	OIDs/Values	Comments
extnValue	http://www.pki.admin.ch/crl/RootCAIII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA IIIou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.6.1.9 Swiss Government Public Trust Code Signing Standard CA 02 (2.16.756.1.17.3.61.3)

Verwendungszweck:

Issuing CA: Swiss Government Public Trust Code Signing Standard CA 02

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING
algorithm	1.2.840.113549.1.1.11: sha256WithRSASignature	This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate. This field MUST contain the same algorithm identifier as the

X.509 Field	OIDs/Values	Comments
		signatureAlgorithm field in the sequence Certificate. The contents of the optional parameters field will vary according to the algorithm identified.
parameters	NULL	
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	Random	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements
issuer	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:www.pki.admin.ch 2.5.4.3:Swiss Government Root CA III	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280 (14 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Code Signing Standard CA 02	The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name MAY be carried in the subject field and/or the subjectAltName extension. If the subject is a CA then the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject CA. PrintableString directoryName Should be byte-for-byte equivalent to the encoding of the Issuer field in the CRL
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption

X.509 Field	OIDs/Values	Comments
parameters	NULL	
subjectPublicKey	…..	BIT STRING 4096 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN +Cert Serial
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'	certSign crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
critical	TRUE	BR 1.3.3 Chap. 7.1.2.2 a.
extnValue	2.16.756.1.17.3.61.3	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
extnId	1.3.6.1.5.5.7.2.2	

X.509 Field	OIDs/Values	Comments
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 5280
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN
pathLenConstraint	0	INTEGER no child CA
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RootCAIII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA III ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.6.2 End Entity Policies

2.6.2.1 Swiss Government Regular CA 01

2.6.2.1.1 System - Swiss Government Regular CA 01

Verwendungszweck:

Tbd

--- OBSOLETE ---

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Servers 2.5.4.3:server/system name	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '101'B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.10	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Regular CA 01 CPS for authentication purposes	VisibleString id-qt-unotice RFC 3280

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/ RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/ RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Server Auth (1.3.6.1.5.5.7.3.1)	
	Client Auth (1.3.6.1.5.5.7.3.2)	
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email (OPTIONAL)

Note: applies also for Governikus transport signature transport encryption core signature

2.6.2.1.2 SSL Web Server - Swiss Government Regular CA 01

Verwendungszweck:

Tbd

--- OBSOLETE ---

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
issuer	2.5.4.6:CH 2.5.4.10: Admin 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Regular CA 01	PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:The Federal Authorities of the Swiss Confederation 2.5.4.11:Servers 2.5.4.11: SSL 2.5.4.3: server/system name	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	.....	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '101'B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.22.26	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	The purpose of this certificate is solely intended for SSL web server authentication.	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_21_1.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/RegularCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Regular CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Regular CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/ RegularCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	Server Auth (1.3.6.1.5.5.7.3.1)	

2.6.2.2 Swiss Government Public Trust EV CA 02

2.6.2.2.1 Public Trust EV Server Authentication

Verwendungszweck:

End Entity Certificate Policy

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust EV CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"130216085959Z"	UTC TIME ETSI TS 102 280 (2 years)
subject	2.5.4.6:<countryName> 2.5.4.8:<stateOrProvinceName> 2.5.4.7:<localityName> 2.5.4.10:<organizationName> 2.5.4.11:[ ]<organizationalUnitName> 2.5.4.3:FQDN 2.5.4.15:<businessCategory> 2.5.4.5:<serialNumber> 1.3.6.1.4.1.311.60.2.1.2:<jurisdictionOfIncorporationStateOrProvince 1.3.6.1.4.1.311.60.2.1.3:<jurisdictionOfIncorporationCountryName	Holder information e.g. "CH" Holder information e.g. "BE" (canton short) Holder information e.g. "Bern" Holder information e.g. "Swiss Government PKI" Holder information e.g. "BIT" Holder information e.g. "your.server.domain.com" Holder information e.g. "Government Entity"[1] Holder information e.g. "CHE-xxx.xxx.xxx" "Bern" "CH"

[1] Valid values are "Private Organization" "Government Entity" "Business Entity" or "Non-Commercial Entity"

X.509 Field	OIDs/Values	Comments
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits ‘101’B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.4	
extnId	1.3.6.1.5.5.7.2.2	

X.509 Field	OIDs/Values	Comments
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 5280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTEVCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust EV CA 02 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/PTEVCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	serverAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	<your.server.address.com>	[1] rfc1034 dNSName IA5String

2.6.2.2.2 Public Trust EV Client Authentication

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust EV CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"130216085959Z"	UTC TIME ETSI TS 102 280 (2 years)
subject	2.5.4.6:<countryName> 2.5.4.8:<stateOrProvinceName> 2.5.4.7:<localityName> 2.5.4.10:<organizationName> 2.5.4.11:[ ]<organizationalUnitName> 2.5.4.3:FQDN	Holder information e.g. "CH" Holder information e.g. "BE" (canton short) Holder information e.g. "Bern" Holder information e.g. "Swiss Government PKI" Holder information e.g. "BIT" Holder information e.g. "your.client.domain.com"

X.509 Field	OIDs/Values	Comments
	2.5.4.15:<businessCategory> 2.5.4.5:<serialNumber> 1.3.6.1.4.1.311.60.2.1.2:<jurisdictionOfIncorporationStateOrProvince 1.3.6.1.4.1.311.60.2.1.3:<jurisdictionOfIncorporationCountryName	Holder information e.g. “Government Entity”[2] Holder information e.g. “CHE-xxx.xxx.xxx” “Bern” “CH”
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	

[2] Valid values are “Private Organization” “Government Entity” “Business Entity” or “Non-Commercial Entity”

X.509 Field	OIDs/Values	Comments
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.5	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 5280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTEVCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust EV CA 02 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/PTEVCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	clientAuthentication

X.509 Field	OIDs/Values	Comments
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	<your.client.address.com>	[1] rfc1034 dNSName IA5String

2.6.2.2.3 Public Trust EV Server/Client Authentication

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust EV CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280

X.509 Field	OIDs/Values	Comments
notAfter	"130216085959Z"	UTC TIME ETSI TS 102 280 (2 years)
subject	2.5.4.6:<countryName> 2.5.4.8:<stateOrProvinceName> 2.5.4.7:<localityName> 2.5.4.10:<organizationName> 2.5.4.11:[ ]<organizationalUnitName> 2.5.4.3:FQDN 2.5.4.15:<businessCategory> 2.5.4.5:<serialNumber> 1.3.6.1.4.1.311.60.2.1.2:<jurisdictionOfIncorporationStateOrProvince 1.3.6.1.4.1.311.60.2.1.3:<jurisdictionOfIncorporationCountryName	Holder information e.g. "CH" Holder information e.g. "BE" (canton short) Holder information e.g. "Bern" Holder information e.g. "Swiss Government PKI" Holder information e.g. "BIT" Holder information e.g. "your.client.domain.com" Holder information e.g. "Government Entity"[3] Holder information e.g. "CHE-xxx.xxx.xxx" "Bern" "CH"
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '101'B	Digital Signature Key Encipherment
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	

[3] Valid values are "Private Organization" "Government Entity" "Business Entity" or "Non-Commercial Entity"

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.6	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTEVCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust EV CA 02 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/PTEVCA02.crt	uri IA5String

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	serverAuthentication
	1.3.6.1.5.5.7.3.2	clientAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	<your.{server/client}.address.com	[1] rfc1034 dNSName IA5String

2.6.2.2.4 Public Trust EV OCSP Responder

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative

X.509 Field	OIDs/Values	Comments
		integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust EV CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.3:ev-ocsp-responder.pki.admin.ch	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '11'B	RFC 5280
digitalSignature	1	
nonRepudiation	1	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.8	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 5280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTEVCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust EV CA 02 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/PTEVCA02.crt	uri IA5String

X.509 Field	OIDs/Values	Comments
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	<your.ocsp.address.com>	[1] rfc1034 dNSName IA5String

2.6.2.3 Swiss Government Public Trust Codesigning EV CA 02

2.6.2.3.1 Public Trust EV Code Signing OCSP Responder (2.16.756.1.17.3.62.12)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	Xxxxx	The serial number MUST be a positive integer assigned by the CA to

X.509 Field	OIDs/Values	Comments
		each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Code Signing EV CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.3:public-trust-ev-code-signing-OCSP-Responder	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '10'B	RFC 5280
digitalSignature	**1**	

X.509 Field	OIDs/Values	Comments
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.12	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
ocsp-nocheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	

2.6.2.3.2 Public Trust EV Code Signing (2.16.756.1.17.3.62.10)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

die Identität des Herausgebers informiert.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Codesigning EV CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
editable	FALSE	1 or 2 years
notBefore	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280 (1 year or 2 years)
subject	2.5.4.6: CH 2.5.4.7: <Locality> 2.5.4.10: <Organisation> 2.5.4.11: <Organisational Unit> 2.5.4.11: <Organisational Unit> 2.5.4.3: <CN>	UTF8String directoryName L = Locality z.B. „Bern" O = Description according to UID-Register z.B "Bundesamt für Zukunftsforschung (BFZ)" OU = UID according to UID-Register z.B. "CHE-123.456.789" OU = Organisational Unit z.B „Büroautomation" CN = Description according to UID-Register z.B "Bundesamt für Zukunftsforschung (BFZ)"
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption

X.509 Field	OIDs/Values	Comments
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING Include Authority Key Identifier
subjectKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	

X.509 Field	OIDs/Values	Comments
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.10, 2.23.140.1.1	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	
extnId	2.5.29.19	
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
critical	FALSE	
mandatory	TRUE	

X.509 Field	OIDs/Values	Comments
editable	FALSE	
visible	FALSE	
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTCSEVCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust Codesigning EV CA 02ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government SSL CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/PTCSEVCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.3	id_kp_codeSigning
subjectAltName		
critical	FALSE	
mandatory	TRUE	
editable	TRUE	
visible	TRUE	
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email

2.6.2.4 Swiss Government Public Trust Standard CA 02

2.6.2.4.1 Public Trust Standard OCSP Responder (2.16.756.1.17.3.62.7)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI	UTF8String directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.11:Services 2.5.4.3:public-trust-standard-OCSP-Responder	
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘10’B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.7	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocsp-nocheck		4.2.2.2.1 Revocation Checking of an Authorized Responder (RFC 2560) A CA may specify that an OCSP client can trust a responder for the lifetime of the responder's certificate. The CA does so by including the extension id-pkix-ocsp-nocheck. This SHOULD be a non-critical extension. The value of the extension should be NULL
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	~~BOOLEAN~~
extnValue	cA FALSE	~~BOOLEAN~~
pathLenConstraint	None	~~INTEGER End Entity~~

2.6.2.4.2 Public Trust Standard Server Authentication (2.16.756.1.17.3.62.1)

Verwendungszweck:

End Entity Certificate Policy

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature

X.509 Field	OIDs/Values	Comments
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). UTF-8 String directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.8:<stateOrProvinceName> 2.5.4.7:<localityName> 2.5.4.10:<organizationName> 2.5.4.11:[ ]<organizationalUnitName> 2.5.4.3:FQDN	Holder information e.g. "CH" Holder information e.g. "BE" (Canton short) Holder information e.g. "Bern" Holder information e.g. "BIT" Holder information e.g. "Swiss Government PKI" Holder information
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
extensions		
authorityKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '101'B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.1	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 5280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN

X.509 Field	OIDs/Values	Comments
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTSTCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust Standard CA 02 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/PTSTCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	serverAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	<your.server.address.com>	[1] rfc1034 dNSName IA5String

2.6.2.4.3 Public Trust Standard Client Authentication (2.16.756.1.17.3.62.2)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). UTF-8 String directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.8:<stateOrProvinceName> 2.5.4.7:<localityName> 2.5.4.10:<organizationName> 2.5.4.11:[ ]<organizationalUnitName> 2.5.4.3:FQDN	Holder information e.g. "CH" Holder information e.g. "BE" (Canton short) Holder information e.g. "Bern" Holder information e.g. "BIT" Holder information e.g. "Swiss Government PKI" Holder information
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B (bit 0)	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.2	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 5280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	

X.509 Field	OIDs/Values	Comments
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTSTCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust Standard CA 02 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/PTSTCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.2	clientAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	<your.client.address.com>	[1] rfc1034 dNSName IA5String

2.6.2.4.4 Public Trust Standard Server/Client Authentication (2.16.756.1.17.3.62.3)

Verwendungszweck:

tbd

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). UTF-8 String directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.8:<stateOrProvinceName> 2.5.4.7:<localityName> 2.5.4.10:<organizationName> 2.5.4.11:[ ]<organizationalUnitName> 2.5.4.3:FQDN	Holder information e.g. "CH" Holder information e.g. "BE" (Canton short) Holder information e.g. "Bern" Holder information e.g. "BIT" Holder information e.g. "Swiss Government PKI" Holder information
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		

X.509 Field	OIDs/Values	Comments
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits ‘101’B	Digital Signature Key Encipherment
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.3	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	

X.509 Field	OIDs/Values	Comments
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTSTCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust Standard CA 02 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/PTSTCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	serverAuthentication
	1.3.6.1.5.5.7.3.2	clientAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	<your.{server/client}.address.com	[1] rfc1034 dNSName IA5String

2.6.2.4.5 Public Trust Standard Browser Compatible Server/Client Authentication (2.16.756.1.17.3.62.14)

Verwendungszweck:

Browser Compatible SSL/TLS certificates for server/client authentication

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	The serialNumber is a non-sequential serial number greater than zero (0) containing at least 64 bits of output from a RNG
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (2 years)
subject	2.5.4.6:CH 2.5.4.7:Bern 2.5.4.8:BE 2.5.4.10Bundesamt fuer Informatik und Telekommunikation 2.5.4.11:[ ]<organizationalUnitName> 2.5.4.3:FQDN	Holder information is static: O = Bundesamt fuer Informatik und Telekommunikation L = Bern S = BE C = CH 2.5.4.11 OU MAY contain the specific OU that is registered as holder. 2.5.4.3:FQDN If present this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension

X.509 Field	OIDs/Values	Comments
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits ‘101’B	Digital Signature Key Encipherment
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.14	
~~extnId~~	~~1.3.6.1.5.5.7.2.2~~	

X.509 Field	OIDs/Values	Comments
~~extnValue~~	~~Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS~~	~~VisibleString id-qt-unotice RFC 3280~~
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTSTCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust Standard CA 02 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/PTSTCA02BC.crt	uri IA5String →BC = Browser Compatible (Adapted AIA for chaining to the QuoVadis Root)
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocspbc	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	serverAuthentication
	1.3.6.1.5.5.7.3.2	clientAuthentication
subjectAltName		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	<your.{server/client}.address.com	[1] rfc1034 dNSName IA5String

2.6.2.4.6 Public Trust Standard Browser Compatible Server/Client Authentication SAN Keylength > 2048 bit (2.16.756.1.17.3.62.16)

Verwendungszweck:

Browser Compatible SSL/TLS certificates for server/client authentication with multiple SAN entries Keylenght >2048KB

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	4096 bit	4096 bit BIT STRING or higher
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	The serialNumber is a non-sequential serial number greater than zero (0) containing at least 64 bits of output from a RNG
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (2 years)
subject	2.5.4.6:CH 2.5.4.7:Bern	Holder information is static: O = Bundesamt fuer Informatik und Telekommunikation

X.509 Field	OIDs/Values	Comments
	2.5.4.8:BE 2.5.4.10Bundesamt fuer Informatik und Telekommunikation 2.5.4.11:[ ]<organizationalUnitName> 2.5.4.3:FQDN	L = Bern S = BE C = CH 2.5.4.11 OU MAY contain the specific OU that is registered as holder. 2.5.4.3:FQDN If present this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 4096 bit or higher
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '101'B	Digital Signature Key Encipherment
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	**1**	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	

X.509 Field	OIDs/Values	Comments
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.16	
~~extnId~~	~~1.3.6.1.5.5.7.2.2~~	
~~extnValue~~	~~Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS~~	~~VisibleString id-qt-unotice RFC 3280~~
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTSTCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust Standard CA 02 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/PTSTCA02BC.crt	uri IA5String →BC = Browser Compatible (Adapted AIA for chaining to the QuoVadis Root)
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp

X.509 Field	OIDs/Values	Comments
accessLocation	http://www.pki.admin.ch/aia/ocspbc	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	serverAuthentication
	1.3.6.1.5.5.7.3.2	clientAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	<your.{server/client}.address.com	[1] rfc1034 dNSName IA5String
	DomainController	

2.6.2.5 Swiss Government Qualified CA 01

2.6.2.5.1 Class A Qualified Digital Signature

Verwendungszweck:

Qualified Certitficate for digital Signature. (2.16.756.1.17.3.2.17)

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Random
Issuer	2.5.4.6:CH 2.5.4.10: Admin	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Qualified CA 01	
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.6:CH 2.5.4.10:Admin 2.5.4.11:Weisse Seiten 2.5.4.3:Last First Hash	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	`. . . . . .`B	BIT STRING 2048 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '10'B	RFC 5280
digitalSignature	0	
nonRepudiation	**1**	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	

X.509 Field	OIDs/Values	Comments
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.17	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Qualified CA 01 CPS for end users	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
issuerAltName		
extnId	2.5.29.18	
extnValue	"O=ZertES Recognition Body: KPMG AG"	directoryName
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/QualifiedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Qualified CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Enhanced CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	

X.509 Field	OIDs/Values	Comments
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/QualifiedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.1	qcs-QcCompliance
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.2	qcs-QcLimitValue
statementInfo	SEQUENCE	
currency	CHF	Iso4217CurrencyCode
amount	2	CHF 0-2 Mio
exponent	6	INTEGER
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	qcs-QcSSCD

2.6.2.5.2 Class A Geregeltes Behördenzertifikat (2.16.756.1.17.3.2.46)

Verwendungszweck:

Verwaltungsstellen (Behörden) sollen mit einem solchen Zertifikat zusammen mit einem qualifizierten Zeitstempel Dokumente digital signieren können.

Provisorische Konfiguration: Abgeleitet aus der bestehenden Policy für qualifizierte Signaturzertifikate unter der Issuing CA Swiss Government Qualified CA 01

Zukünftige Konfiguration: Der Vergleich der Bestimmungen des neuen ZertES VZertES und den TAV mit der provisorischen Konfiguration zeigt dass folgende Anpassungen durchgeführt werden müssen:

- Neue Policy für das geregelte Behördenzertifikat

- Neue Policy für bestehende Klasse A Zertifikate
- Neue Issuing CA mit angepassten Attributen als Issuer der beiden oben erwähnten Zertifikatstypen.

X.509 Field	**OIDs/Values**	**Comments**
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signatureValue	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	xxxxx	Unique Random
Issuer	2.5.4.6:CH 2.5.4.10:The Federal Authority of the Swiss Confederation 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Qualified CA 01	***PrintableString*** directoryName 2.5.4.6: C (Country) 2.5.4.10: O (Organisation) (TAV 2.3.2 b) 2.5.4.11: OU (OrganisationalUnit) 2.5.4.3: CN (Common Name)
validity		
notBefore	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280
notAfter	"ddmmyyHHMMSSZ"	UTC TIME ETSI TS 102 280 (3 years)
Subject	2.5.4.6:CH (C) 2.5.4.10:OrganizationName (O) 2.5.4.3:CommonName (CN) 2.5.4.97:organizationIdentifier (OI - different from OrganisationName) 2.5.4.11:organizationalUnitName (OU). 2.5.4.11:organizationalUnitName (OU) 2.5.4.7:localityName (L) 2.5.4.8:stateOrProvinceName (ST)	***PrintableString*** directoryName: Attribute die nicht gemäss TAV/ETSI definert werden müssen entsprechen dem Vorschlag des ISB für Amtssiegel: 2.5.4.6: C=CH oder LI 2.5.4.10: O=Name exakt wie im UID-Register 2.5.4.97: OI=„NTRCH"-UID der Behörde bzw. „VATCH"-UID bzw. „CH:"-UID der Behörde 2.5.4.3: CN=Allgemein gebräuchlicher Name der Behörde 2.5.4.11: $OU_{1..n}$:Nähere Bezeichnung 2.5.4.7: L=Bezeichnung der Gemeinde in der die Behörde ihren Sitz hat 2.5.4.8:ST= Bezeichnung des Kantons in der die Behörde ihren Sitz hat

X.509 Field	OIDs/Values	Comments
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	`. . . . . .`B	BIT STRING 2048 Bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`. . . . .`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	6 unused bits '10'B	RFC 5280
digitalSignature	**1**	
contentCommitment	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.46	In an end entity certificate these policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used.
extnId	1.3.6.1.5.5.7.2.1	

X.509 Field	OIDs/Values	Comments
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is a regulated certificate for legal persons as defined by the Swiss federal law SR 943.03 ZertES	VisibleString id-qt-unotice RFC 5280 RFC 5280 explicitText. ZertES Art. 7 2b. TAV 2.3.2 d) Der ausführlichere Text wäre für relying Parties aussagekräftiger
issuerAltName		
extnId	2.5.29.18	
extnValue	O=ZertES Recognition Body: KPMG AG	directoryName
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/QualifiedCA01.crl	uri IA5String ldap uri IA5String CA Swiss Government Qualified CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/QualifiedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
subjectAltName		SEQUENCE
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates

X.509 Field	OIDs/Values	Comments
	[1] rfc822 Email	rfc822 Email (E-Mail Adresse die im Validator benützt wird um die Auskunftstelle für den signierten Dokumententyp anzuzeigen)
qcStatements		
extnId	1.3.6.1.5.5.7.1.3	
extnValue	SEQUENCE OF	OCTET STRING
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.4	id-etsi-qcs-QcSSCD: ETSI EN 319 412-5 Kap. 4.2.2 TAV Kap. 2.3.2 Abschn. g) When the certificate is issued as a certificate where the private key related to the certified public key resides in a qualified signature/seal creation device in accordance with Regulation (EU) No 910/2014 [i.8] or in a secure signature creation device as defined in Directive 1999/93/EC [i.3] this statement shall be present.
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.5	id-etsi-qcs-QcPDS Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Das PKI Disclosure Statement PDS ist ein Dokument das die Transparenz gegenüber den Kunden stark erhöht. Zudem ist es nicht direkt an die EU Rechtssprechung gebunden
statementInfo	SEQUENCE	
url	http://www.pki.admin.ch/cps/PDS-SGPKI_Qualified_CA_01.pdf	PKI Disclosure Statements a) It shall provide at least one URL to a PDS in English. Other PDS documents in other languages may be referenced using this QCStatement provided that they provide information that corresponds to the information given in the referenced English PDS; and b) it shall not reference more than one PDS per

X.509 Field	OIDs/Values	Comments
		language.
language	EN	ISO 639-1 language code
qCStatement	SEQUENCE	
statementId	0.4.0.1862.1.6	id-etsi-qcs-QcType Ich würde dieses qCStatement einfügen obwohl es vom ZertES nicht verlangt wird. Es identifiziert zusätzlich eindeutig den Verwendungszweck des Zertifikats. Zudem verweist ETSI EN_319412-05 darauf dass „NOTE: This statement without the one defined in clause 4.2.1 (id-etsi-qcs-QcCompliance) can be potentially used in other regulatory environments which use electronic signature electronic seal or web site with the same meaning" also explizit ausserhalb der EU.
statementInfo	SEQUENCE OF	OBJECT IDENTIFIER
id-etsi-qcs-QcType	2	-- QC type identifiers id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 } -- Certificate for electronic signatures as defined in Regulation (EU) No 910/2014 id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 } -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014 id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 } -- Certificate for website authentication as defined in Regulation (EU) No 910/2014

2.6.2.5.3 FreeDN

Verwendungszweck:

Equals 2.6.2.5.1 – in this case the CN must not be listed in the AdminDir.

2.6.2.5.4 FreeDN pre-assigned

Verwendungszweck:

Equals 2.6.2.5.1 – for this type of certificate the content of the CN will be added with special priveleges in the AdminDir before issuing the certificate.

2.6.2.5.5 SHAB Archive Signer

Verwendungszweck:

Equals 2.6.2.5.1 – in this case the CN must not be listed in the AdminDir.

2.6.2.5.6 Time Stamp Signer (Luna SA) (2.16.756.1.17.3.2.18)

Verwendungszweck:

Certficate to sign Time Stamp.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
Algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
Parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	v3 cert
serialNumber	unique integer	Random [integer]
issuer	2.5.4.6:CH 2.5.4.10: Admin	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Qualified CA 01	
validity		
notBefore	"YYMMDDHHMMSSZ"	UTC TIME ETSI TS 102 280
notAfter	"YYMMDDHHMMSSZ"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.7:Bern 2.5.4.10:Swiss Government PKI 2.5.4.11:Time Stamp Services 2.5.4.3: Swiss Government TSA	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	RFC 3279
subjectPublicKey	`……..`B	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	`…..`O	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	`…..`O	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'00000010'B	RFC 5280
digitalSignature	0	
nonRepudiation	**1**	
keyEncipherment	0	
dataEncipherment	0	

X.509 Field	OIDs/Values	Comments
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.18	
extnId	1.3.6.1.5.5.7.2.2	
extnValue	This is the Swiss Government Qualified CA 01 CPS for timestamping purposes	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
issuerAltName		
extnId	2.5.29.18	
extnValue	"O=ZertES-Certification Body: KPMG AG"	directoryName UTF8String
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
extendedKeyUsage		
extnId	2.5.29.37	
Critical	TRUE	
	1.3.6.1.5.5.7.3.8	timeStamping
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/QualifiedCA01.crl ldap://admindir.admin.ch:389/cn=Swiss Government Qualified CA 01ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government Qualified CA 01 CDPs

X.509 Field	OIDs/Values	Comments
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/QualifiedCA01.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

2.6.2.5.7 Swiss Government Qualified CA 01 OCSP Responder (2.16.756.1.17.3.2.37)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. V extensions are used as expected in this profile version MUST (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by th each certificate. It MUST be unique for each certificate issue given CA. CAs MUST force the serialNumber to be a non-neg

X.509 Field	OIDs/Values	Comments
		integer with 20-bit entropy according to Baseline Requireme
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Qualified CA 01	The issuer field identifies the entity that has signed and issu certificate. The issuer field MUST contain a non-empty disti name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (3 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.3:QualifiedCA01-OCSP-Responder	UTF8String directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STR
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '10'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	

X.509 Field	OIDs/Values	Comments
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.2.37	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocspNoCheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.6.2.6 Swiss Government Public Trust Standard CA 03

2.6.2.6.1 Public Trust Standard CA03 OCSP Responder (2.16.756.1.17.3.62.18)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 03	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (1 years)
subject	2.5.4.6:CH	PrintableString directoryName

X.509 Field	OIDs/Values	Comments
	2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.3:ptstca03-OCSP-Responder	
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘10’B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.18	

X.509 Field	OIDs/Values	Comments
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocsp-nocheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.6.2.6.2 Public Trust Standard CA03 Server Authentication (2.16.756.1.17.3.62.17)

Verwendungszweck:

End Entity Certificate Policy

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3

X.509 Field	OIDs/Values	Comments
		(value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Standard CA 03	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (825 days) BR 1.5.1 from 2018-03-01
subject	2.5.4.6:CH 2.5.4.8:<stateOrProvinceName> 2.5.4.7:<localityName> 2.5.4.10:<organizationName> 2.5.4.11:[ ]<organizationalUnitName> 2.5.4.3:FQDN	Holder information "CH" Holder information e.g. "BE" (Canton short) Holder information e.g. "Bern" Holder information e.g. "BIT" Holder information e.g. "Swiss Government PKI" Holder information PrintableString directoryName
subjectPublicKeyInfo	To check	
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	

X.509 Field	OIDs/Values	Comments
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	5 unused bits '101'B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	1	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.17, 2.23.140.1.2.2, 0.4.0.2042.1.7	OID for CAB and ETSI OVCP
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTSTCA03.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust Standard CA 03 ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA CDPs

X.509 Field	OIDs/Values	Comments
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/PTSTCA03.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.1	serverAuthentication
subjectAltName		
extnId	2.5.29.17 SEQUENCE	OCTECT STRING encapsulates
	<your.server.address.com>	[1] rfc1034 dNSName IA5String

2.6.2.7 Swiss Government Public Trust Codesigning Standard CA 02

2.6.2.7.1 Public Trust Codesigning Standard CA02 OCSP Responder (2.16.756.1.17.3.62.11)

Verwendungszweck:

An OCSP responder is a web service that indicates to the client the status of the certificate. The OCSP responder certificate will be used to sign the OCSP response.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	

X.509 Field	OIDs/Values	Comments
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Codesigning Standard CA 02	The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). PrintableString directoryName
validity		
notBefore	"110216090000Z"	UTC TIME ETSI TS 102 280
notAfter	"140216085959Z"	UTC TIME ETSI TS 102 280 (1 years)
subject	2.5.4.6:CH 2.5.4.10:Swiss Government PKI 2.5.4.11:Services 2.5.4.3:ptstcsca03-OCSP-Responder	PrintableString directoryName
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		

X.509 Field	OIDs/Values	Comments
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits '10'B	RFC 5280
digitalSignature	**1**	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.11	
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
extendedKeyUsage		
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.9	ocspSigning
ocsp-nocheck		
extnId	1.3.6.1.5.5.7.48.1.5	
critical	FALSE	
extnValue	NULL	
basicConstraints		
extnId	2.5.29.19	

X.509 Field	OIDs/Values	Comments
critical	TRUE	BOOLEAN
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity

2.6.2.7.2 Public Trust Standard Code Signing (2.16.756.1.17.1.3.62.9)

Verwendungszweck:

Vertrauenswürdige Signierung von Software die öffentlich verteilt wird. Im gleichen Zug werden die Endanwender der signierten Software über den Ursprung und die Integrität der Software und über die Identität des Herausgebers informiert.

X.509 Field	OIDs/Values	Comments
signatureAlgorithm		
algorithm	1.2.840.113549.1.1.11	sha256WithRSASignature
parameters	NULL	
signature	2048 bit	2048 bit BIT STRING
TBSCertificate		
version	2	This field describes the version of the encoded certificate. When extensions are used as expected in this profile version MUST be 3 (value is 2).
serialNumber	xxxxx	The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA. CAs MUST force the serialNumber to be a non-negative integer with 20-bit entropy according to Baseline Requirements.
issuer	2.5.4.6:CH 2.5.4.10: Swiss Government PKI 2.5.4.11:Services 2.5.4.11:Certification Authorities 2.5.4.3:Swiss Government Public Trust Codesigning Standard CA 02	Specified in BR Section 7.1.4.1 The content of the Certificate Issuer Distinguished Name field MUST match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280 section 4.1.2.4. PrintableString directoryName

X.509 Field	OIDs/Values	Comments
validity		
notBefore	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280
notAfter	"yymmddhhmmssZ"	UTC TIME ETSI TS 102 280 (1 year or 2 years)
subject	2.5.4.6: CH 2.5.4.7: <Locality> 2.5.4.10: <Organisation> 2.5.4.11: <Organisational Unit> 2.5.4.11: <Organisational Unit> 2.5.4.3: <CN>	Required. This field MUST contain the Subject's legal name as verified under BR Section 3.2. L = Locality z.B. „Bern" O = Description according to UID-Register z.B "Bundesamt für Zukunftsforschung (BFZ)" OU = UID according to UID-Register z.B. "CHE-123.456.789" OU = Organisational Unit z.B „Büroautomation" CN = Description according to UID-Register z.B " Code Signing Officer 999x Bundesamt für Zukunftsforschung (BFZ)"
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1	rsaEncryption
parameters	NULL	
subjectPublicKey	…..	BIT STRING 2048 bit
Extensions		
authorityKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.35	KeyId
extnValue	…..	OCTET STRING 160 bit SHA1 ofBIT STRING Include Authority Key Identifier
subjectKeyIdentifier		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	

X.509 Field	OIDs/Values	Comments
visible	FALSE	
extnId	2.5.29.14	
extnValue	…..	OCTET STRING 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	7 unused bits ‘1’B	RFC 5280
digitalSignature	1	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	0	
cRLSign	0	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		A Policy Identifier defined by the Issuer that indicates a Certificate Policy asserting the Issuer's adherence to and compliance with these Requirements.
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.32	
extnValue	2.16.756.1.17.3.62.9, 2.23.140.1.2.2	
extnId	1.3.6.1.5.5.7.2.2	

X.509 Field	OIDs/Values	Comments
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf	IA5String cps
basicConstraints		
critical	TRUE	
mandatory	TRUE	
editable	FALSE	
visible	TRUE	
extnId	2.5.29.19	
extnValue	cA FALSE	BOOLEAN
pathLenConstraint	None	INTEGER End Entity
crlDistributionPoints		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.31	
extnValue	http://www.pki.admin.ch/crl/PTCSSTCA02.crl ldap://admindir.admin.ch:389/cn=Swiss Government Public Trust Codesigning Standard CA 02ou=Certification Authoritiesou=Serviceso=Adminc=CH	uri IA5String ldap uri IA5String CA Swiss Government SSL CA 01 CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/PTCSSTCA02.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp	uri IA5String

X.509 Field	OIDs/Values	Comments
extendedKeyUsage		
critical	FALSE	
mandatory	TRUE	
editable	FALSE	
visible	FALSE	
extnId	2.5.29.37 SEQUENCE OF OIDs	OCTECT STING encapsulates
	1.3.6.1.5.5.7.3.3	id_kp_codeSigning
subjectAltName		
critical	FALSE	
mandatory	TRUE	
editable	TRUE	
visible	TRUE	
extnId	2.5.29.17 SEQUENCE	OCTECT STING encapsulates
	[1] rfc822 Email	RFC 822 Email