Addendum zu den Zertifikatsrichtlinien (CP/CPS)

Profile der Zertifikate, CRLs und OCSP

Für die Zertifikate der

- Root CAs
- Issuing CAs (Diamant, Saphir, Rubin)
- Benutzer (Diamant, Saphir, Rubin)
- Time-Stamping Services

Version: 3.7

Datum: 27. Januar 2022

Swisscom (Schweiz) AG
Digital Certificate Services
Postfach
8021 Zürich

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
2.0	15.06.2011	H.P. Waldegger	Neue CA 2 Hierarchie und Details für Root eingefügt.
2.1	01.12.2011	Markus Limacher	Update CA 2 Hierarchie; update CA 2 Profile Consolidate Addendums
2.2	16.10.2012	Projekt Team	Anpassungen für Mozilla Root Programm
2.3	25.06.2013	Kerstin Wagner	Anpassung des Intervalls der CRL Generierung
2.4	02.07.2013	Hans Augstburger	Ersatz von „Fixnet"
2.5	29.01.2014	Patrick Graber	Ergänzung Zertifikatsprofil Saphir für All-in Signing Service, Typo Korrekturen
2.6	16.06.2014	Patrick Graber	Anpassungen Extended Key Usage in „Swisscom Smaragd CA 2" Add OCSP Responder in „Swisscom Quarz CA 2"-Profil Elimination Zertifikatsprofile für SuisseID & Customer CA
2.6	10.07.2014	Kerstin Wagner	Auslagerung der Profile in eigenständiges Dokument und Überarbeitung
2.7	02.10.2014	Patrick Graber	Ergänzung Zertifikatsprofil Diamant und Saphir für All-in Signing Service; Ergänzung Zertifikatsprofil Rubin CA3 für Mobile ID.
2.8	27.11.2015	Kerstin Wagner	Ergänzung der OIDs für OV und EV Validation sowie Code-Signing; Auslagerung der Angaben zu den CA 1 Zertifikaten in ein eigenständiges Dokument.
3.0	02.08.2017	H-P Waldegger	Anpassungen neue TAV 2017 und Ergänzung CA basierend auf den neuen ETSI standards.
3.1	06.02.2018	H-P Waldegger	Anpassungen CA 2 EE-Zertifikate an neue TAV 2017 und ETSI standards für die Übergangszeit bis CA 4.
3.2	15.08.2018	H-P Waldegger	Review Feedback CA 4 eingepflegt und für Freigabe vorbereitet.
3.3	07.11.2018	H-P Waldegger	Anpassung: CA4 wird nur als eigenständiger Baum aufgesetzt, d.h. Root CA2 wird keine CA4 signieren. Smaragd CA4 entfernt. Gültigkeitsbeschränkung bei CA 2 EE-Zertifikaten aufgrund Algorithmen und CA Ablauf ergänzt.
3.4	01.02.2019	H-P Waldegger	TSA3 Zertifikat den Anforderungen der TAV 2017 angepasst.
3.4	08.03.2019	Governance Board	Freigabe
3.5	14.08.2019	Kerstin Wagner	OCSP Request und Response ergänzt
3.5	20.01.2020	QTSP Board	Freigabe durch QTSP Board (neu für Governance Board)
3.6	15.06.2020	H-P Waldegger	Haftungsbeschränkungen ergänzt (Diamant)
3.6	01.07.2020	QTSP Board	Freigabe durch QTSP Board
3.7	03.06.2021	K. Wagner	Korrektur der keyUsage bei OCSP-Signer Zertifikaten, Einträge zu 'Smaragd', 'Rubin Gen2' und Timestamping Gen 2 und 3 gelöscht, unnötige Referenzen und Versionsangaben gelöscht
3.7	27.01.2022	QTSP Board	Freigabe durch QTSP Board

Referenzierte Dokumente:

[CAB-BR]	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Version 1.5.3, September 2017
[CPSqcp]	Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klassen „Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten), Version 3.7
[CPSncp+]	Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klassen „Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten), Version 3.7
[CPSlcp]	Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klasse„ "Rubin"
[ElDI-Valt]	SR 641.201.1: „Verordnung des EFD über elektronisch übermittelte Daten und Informationen”, ElDI-V vom 11. Dezember 2009 (Stand am 1. Januar 2010)
[ETSI TS 119 312]	ETSI TS 119 312 V1.3.1 (2019-02): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319 401]	ETSI EN 319 401: General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	ETSI EN 391 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319 411-2]	ETSI EN 391 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319 421]	ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
[ETSI EN 319 412-1]	ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[ETSI EN 319 412-2]	ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[ETSI EN 319 412-3]	ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[ETSI EN 319 412-5]	ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[ETSI EN 319 422]	ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[MozPol]	Mozilla Root Store Policy, Version 2.5
[RFC 3279]	IETF RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC 5280]	IETF RFC 5280:Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
[RFC 6960]	IETF RFC 6960: „Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP”

[TAV]	SR 943.032.1 TAV: Technische und administrative Vorschriften vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur
[TAValt]	SR 943.032.1 TAV: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur, Ausgabe 4 vom 1. August 2011
[VZertES]	SR 943.032, VZertES: Verordnung vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur
[VZertESalt]	SR 943.032, VZertES: Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur, VZertES)
[ZertES]	SR 943.03, ZertES: Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur
[ZertESalt]	SR 943.03, ZertES: Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES)
[Zertifikatsprofile EU]	Addendum zur CP/CPS Diamant & Saphir EU: Profile der Zertifikate, Sperrlisten (CRL) und Online Statusabfragen

swisscom

Inhaltsverzeichnis

Einleitung

Dieses Dokument ist ein Addendum zu den CP/CPS Dokumenten [CPSncp+] und [CPSqcp] von Swisscom Digital Certificate Services, einer Dienstleistung der Swisscom (Schweiz) AG.

Es beschreibt detailliert die Profile der verschiedenen Zertifikatstypen, die von Swisscom Digital Certificate Services oder ihren RA Partnern ausgegeben werden, sowie die Profile der Widerrufslisten und Online Statusabfragen.

1 Profile der Zertifikate

Die Profile der Zertifikate und Widerrufslisten sind entsprechend den Vorgaben aus [RFC 5280]: "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile" aufgebaut. Sie entsprechen ausserdem, den Vorgaben des[ZertES], den [TAV], sowie den referenzierten ETSI Standards.

Zur Sicherstellung der Kompatibiliäte im internationalen Umfeld und der Rückwärtskomatibilität mit älteren Systemen und Datenbanken können in allen Zertifikaten die Namen des Zertifikats–inhabers (Subject DN) generell entsprechend den Vorgaben aus [RFC 5280] Kapitel 4.1.2.6 Absatz 4 Variante c vereinfacht werden.

1.1 Root CA

1.1.1 Swisscom Root CA 2

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature		
algorithm	{1 2 840 113549 1 1 11}	SHA256withRSAEncryption
issuer	CN=Swisscom Root CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH	DirectoryString, UTF8String
validity		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280, valid for 20 years
subject	CN=Swisscom Root CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH	DirectoryString, UTF8String
subjectPublicKeyInfo		
Algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
subjectPublicKey	'.....'B },	4096 Bit, BIT STRING

Extensions		
authorityKeyIdentifier		
subjectKeyIdentifier		
keyUsage	keyCertSign, cRLSign, DigitalSignature	
Critical	TRUE,	BOOLEAN
basicConstraints {		
extnValue	{ cA TRUE }	BOOLEAN
PathLenConstrains	7	
PolicyMappings		
certificatePolicies {		
extnId	{ 2 5 29 33 },	
extnValue	{ 2 16 756 1 83 2 1} },	In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate.

1.1.2 Swisscom Root CA 4

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Nichtsequentielle positive Zahl [Integer]
signature		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	CN=Swisscom Root CA 4, organizationIdentifier=VATCH-CHE-101.654.423 O=Swisscom, OU=Digital Certificate Services, C=CH	DirectoryString, UTF8String
validity		
notBefore	" YYMMDDHHMMSSZ ",	Zeitpunkt der Ausstellung
notAfter	" YYMMDDHHMMSSZ ",	20 Jahre ab Ausstellung
subject	CN=Swisscom Root CA 4, organizationIdentifier=VATCH-CHE-101.654.423 O=Swisscom, OU=Digital Certificate Services, C=CH	gleich wie "issuer"
subjectPublicKeyInfo		
Algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
subjectPublicKey	'.....'B },	8192 Bit, BIT STRING

Extensions		
subjectKeyIdentifier		
extnId	{ 2 5 29 14 },	
Critical	FALSE	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-1 hash of subjectPublicKey-BitString of the Root CA certificate
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000110000`B },	keyCertSign, cRLSign
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
PolicyMappings		
certificatePolicies {		
extnId	{ 2 5 29 33 },	
extnValue	{ 2 16 756 1 83 30 4 0} },	

1.2 Diamant Issuing CA (geregelt)

1.2.1 Generation 2

1.2.1.1 Swisscom Diamant CA 2 – abgelaufen am 12. Jan 2022

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	
issuer	{ "CN=Swisscom Root CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ " ,	UTC, ETSI TS 102 280, valid for 10 years
subject	{ "CN=Swisscom Diamant CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH },	directoryName, UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublic-Key-BitString of "Root CA 2"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of "Diamant CA 2"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000110001`B },	keyCertSign, cRLSign,DigitalSignature
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 11 0 } },	In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate.
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
issuerAltName {		
extnId	{ 2 5 29 18 },	
extnValue	{ "O=ZertES Recognition Body: KPMG AG" } },	directoryName, UTF8String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, keine weitere CA darunter
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	http://crl.swissdigicert.ch/sdcs-root2.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-calssuers
accessLocation	http://aia.swissdigicert.ch/sdcs-root2.crt ,	[uRI], IA5String
qcStatements {		

Feld X.509	Werte, OID's	Bemerkungen
extnId	{ 1 3 6 1 5 5 7 1 3 },	
critical	FALSE,	BOOLEAN
extnValue	SEQUENCE OF {	OCTET STRING
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 1 }}}}}	qcs-QcCompliance
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11},	sha256WithRSAEncryption
parameters	NULL },	
signature	`..... `B }	2048 Bit, BIT STRING

1.2.1.2 Benutzerzertifikat Diamant CA 2 (qualifiziert)

Dieses Profil war von 2018 bis Dez 2021 im Einsatz.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	[RFC 3279]
issuer	{ "CN=Swisscom Diamant CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH},	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, not more than 3 years, not after 31.12.2021
subject	Name of the certificate holder containing• countryName, choice of (givenName and surname) or pseudonym, commonName and possibly optional name items according to [CPSqcp]	directoryName, UTF8String, ETSI TS 102 280
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of "Diamant CA 2"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of this subject/end entity
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000010`B },	nonRepudiation
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 11 0 },	New OID according to consolidated CP/CPS
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 194112 1 2 }	QCP-n-qscd
extnId	{ 1 3 6 1 5 5 7 2 2},	id-qt-unotice
extnValue	"qualified certificate"	UTF8String
subjectAltName {		
extnId	{ 2 5 29 17 },	*Extension for "All-in Signing Service"*

Feld X.509	Werte, OID's	Bemerkungen
extnValue	{ if present name="MSISDN" serialNumber="MID/SAS transaction number" description="MID/SAS message to user" pseudonym="MID/SAS specific number" OID 2.16.756.1.83.200.0.0="RAS evidenceID", else "N/A"},	*Extension values as used by "All-in Signing Service"* UTF8String OID 2.16.756.1.83.0.0.1 was used until January 2020.
issuerAltName {		
extnId	{ 2 5 29 18 },	*Extension for "All-in Signing Service"*
extnValue	{serialNumber="Response ID" description="Identifying Registration Authority"},	*Extension values as used by "All-in Signing Service"* UTF8String
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	ldap://ldap.swissdigicert.ch/CN=Swisscom Diamant CA 2, dc=diamant2,dc=swissdigicert, dc=ch?certificateRevocationList?, http://crl.swissdigicert.ch/sdcs-diamant2.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://aia.swissdigicert.ch/sdcs-diamant2.crt ,	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/diamant2 ,	[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 6 1 }},	qcs-QcType: qualified electronic signatures
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 4 }}}}}	qcs-QcSSCD
QCStatement	SEQUENCE(	
statementId	{ 0 4 0 1862 1 5 },	
PdsLocations	SEQENCE OF {	
PdsLocation	SEQUENCE {	
url	https://www.swissdigicert.ch/diamant2-n.pdf	
Language	en	
signatureAlgorithm {		
Algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
Parameters	NULL },	[RFC 3279]
Signature	`..... `B }	2048 Bit, BIT STRING

1.2.2 Generation 4

1.2.2.1 Swisscom Diamant CA 4 von Root CA 2 signiert

Die CA 4 wird als vollständig eigenständiger Baum aufgesetzt und nicht von CA 2 signiert.

1.2.2.2 Swisscom Diamant CA 4 von Root CA 4 signiert

Wichtige Änderungen zur Generation 2 sind in der Tabelle farblich markiert.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	{CN=Swisscom Root CA 4, organizationIdentifier=VATCH-CHE-101.654.423 O=Swisscom, OU=Digital Certificate Services, C=CH},	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	Zeitpunkt der Ausstellung
notAfter	" YYMMDDHHMMSSZ " ,	10 Jahre ab Ausstellung
subject	{ "CN=Swisscom Diamant CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH"},	UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	
subjectPublicKey	'.....'B },	4096 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublic-Key-BitString of "Root CA 4"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Issuing CA.
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000110000`B },	keyCertSign, cRLSign
certificatePolicies {		set of supported certificate policies according to [RFC 5280]
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 30 4 1 },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnId	{ 1 3 6 1 5 5 7 2 2},	id-qt-unotice
extnValue	"regulated certificate"	UTF8String
basicConstraints {		
extnId	{ 2 5 29 19 },	

Feld X.509	Werte, OID's	Bemerkungen
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, keine weitere CA darunter
extendedKeyUsage {		
extnId	{ 2 5 29 37 },	
critical	FALSE,	BOOLEAN
extnValue	{1 2 840 113583 1 1 5},	Adobe PDF Signing, used to mark CA as technical constraint for [MozPol]
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	http://crl.swissdigicert.ch/sdcs-root4.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://aia.swissdigicert.ch/sdcs-root4.crt ,	[uRI], IA5String
qcStatements {		
extnId	{ 1 3 6 1 5 5 7 1 3 },	
critical	FALSE,	BOOLEAN
extnValue	SEQUENCE {	OCTET STRING
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 4 }}}}	QcSSCD
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
signature	`..... `B }	8192 Bit, BIT STRING

1.2.2.3 Benutzerzertifikat Diamant CA 4 (qualifiziert)

Wichtige Änderungen zur Generation 2 bis 2018 sind in der Tabelle farblich markiert.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	{ "CN=Swisscom Diamant CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH"},	UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, not more than 3 years

Feld X.509	Werte, OID's	Bemerkungen
subject	Name of the certificate holder containing• countryName, choice of (givenName and surname) or pseudonym, commonName and possibly optional name items according to [CPSqcp]	UTF8String, [ETSI EN 319 412-2], chapter 4.2.4
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	[RFC 3279] / [ETSI TS 119 312]
subjectPublicKey	'……..'B },	3072 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`…..`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of "Diamant CA 4"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`…..`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of this subject/end entity
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000010`B },	contentCommitment (note: has been renamed from nonRepudiation by X.509)
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 30 4 1 },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 194112 1 2 }	QCP-n-qscd
extnId	{ 1 3 6 1 5 5 7 2 2},	id-qt-unotice
extnValue	"qualified certificate"	UTF8String
subjectAltName {		
extnId	{ 2 5 29 17 },	*Optional Extension*
extnValue	{ if present name="MSISDN" serialNumber="MID/SAS transaction number" description="MID/SAS message to user" pseudonym="MID/SAS specific number" OID 2.16.756.1.83.200.0.0="RAS evidenceID", else "N/A"},	*Extension values as used by AIS 2.x:* • *name, serialNumber, description, pseudonym* *Extension values used by AIS 3.x:* • *serialNumber* UTF8String OID 2.16.756.1.83.0.0.1, was used until January 2020.
issuerAltName {		
extnId	{ 2 5 29 18 },	*Optional Extension*
extnValue	{serialNumber="Response ID" description="Identifying Registration Authority"},	*Extension values used by AIS 2.x:* • *serialNumber, description (RA)* *Extension values used by AIS 3.x:* • *serialNumber (Idp), description (Scheme)* UTF8String
extendedKeyUsage {		
extnId	{ 2 5 29 37 },	
critical	FALSE,	BOOLEAN
extnValue	{1 2 840 113583 1 1 5},	Adobe PDF Signing, used to mark certificate technical constraint for [MozPol]
AuthorityInfoAccess{		SEQUENCE
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	

Feld X.509	Werte, OID's	Bemerkungen
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	http://aia.swissdigicert.ch/sdcs-diamant4.crt	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-diamant4	[uRI], IA5String
qcStatements {		
extnId	{ 1 3 6 1 5 5 7 1 3 },	
extnValue	SEQUENCE {	OCTET STRING
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 1 }},	qcs-Compliance
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 6 1 }},	qcs-QcType: qualified electronic signatures
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 4 }}}}}	qcs-QcSSCD: private key resides on a QSCD
QCStatement	SEQUENCE {	Optional extension defining liability limit
statementId	{ 0 4 0 1862 1 2 },	qcs-QcLimitValue
MonetaryValue	SEQUENCE {	value = amount * 10^exponent
currency	CHF	Iso4217CurrencyCode
amount	1	INTEGER
exponent	[1-6]	INTEGER
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 5 },	qcs-QcEuPDS: PKI Disclosure Statements
PdsLocations	SEQUENCE OF {	
PdsLocation	SEQUENCE {	
url	https://www.swissdigicert.ch/diamant4-n.pdf	Info according to annex A of [ETSI EN 319 411-2] [uRI], IA5String
language	en	PrintableString (SIZE(2))
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
Signature	`..... `B }	4096 Bit, BIT STRING, [ETSI TS 119 312]

1.2.2.4 Organisationszertifikat Diamant CA 4 (geregelt)

Diese Zertifikatsklasse wurde 2017 nach der Totalrevision des ZertES ermöglicht und eingeführt.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC

Feld X.509	Werte, OID's	Bemerkungen
issuer	{ "CN=Swisscom Diamant CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH"},	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, not more than 3 years
subject	Name of the certificate holder containing• countryName, organizationName, organization Identifier, commonName and possibly optional name items as per [CPSqcp]	directoryName, UTF8String, [ETSI EN 319 412-3], chapter 4.2.1
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	[RFC 3279]/ [ETSI TS 119 312]
subjectPublicKey	'.....'B },	3072 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Issuing CA
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of this subject/end entity
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000001`B },	digitalSignature
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 30 4 1 } },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 194112 1 3 }	QCP-l-qscd
extnId	{ 1 3 6 1 5 5 7 2 2},	id-qt-unotice
extnValue	"regulated certificate"	UTF8String
subjectAltName		*Optional Extension*
issuerAltName		*Optional Extension*
extendedKeyUsage {		
extnId	{ 2 5 29 37 },	
critical	FALSE,	BOOLEAN
extnValue	{1 2 840 113583 1 1 5},	Adobe PDF Signing, used to mark certificate technical constraint for [MozPol]
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://aia.swissdigicert.ch/sdcs-diamant4.crt	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-diamant4	[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-Compliance
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 6 2 }},	qcs-QcType: qualified electronic seal
QCStatement	SEQUENCE {	

Feld X.509	Werte, OID's	Bemerkungen
statementId	{ 0 4 0 1862 1 4 }}}}}	qcs-QcSSCD: private key resides on a QSCD
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 5 },	qcs-QcEuPDS: PKI Disclosure Statement
PdsLocations	SEQUENCE OF {	
PdsLocation	SEQUENCE {	
url	https://www.swissdigicert.ch/diamant4-l.pdf	Info according to annex A of [ETSI EN 319 411-2] [uRI], IA5String
language	en	PrintableString (SIZE(2))
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
Signature	`..... `B }	4096 Bit, BIT STRING, [ETSI TS 119 312]

1.3 Saphir Issuing CA (NCP+)

1.3.1 Generation 2

1.3.1.1 Swisscom Saphir CA 2 – abgelaufen am 12. Jan 2022

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	
issuer	{ "CN=Swisscom Root CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280, Valid for 10 years
subject	{ "CN=Swisscom Saphir CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH },	directoryName, UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublic-Key-BitString of "Root CA 2"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of "Saphir CA 2"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000110001`B },	keyCertSign, cRLSign,DigitalSignature
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 23 0 } },	In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate.
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, 0=keine weitere CA darunter
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	http://crl.swissdigicert.ch/sdcs-root2.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-calssuers
accessLocation	http://aia.swissdigicert.ch/sdcs-root2.crt ,	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	
signature	`..... `B }	2048 Bit, BIT STRING

1.3.1.2 Benutzerzertifikat Saphir CA 2

Dieses Profil war von 2018 bis Dez 2021 im Einsatz.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	[RFC 3279]
issuer	CN=Swisscom Saphir CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not longer than 3 years Not after 31.12.2021
subject	Name of the certificate holder containing• countryName, choice of (givenName and surname) or pseudonym, commonName and possibly optional name items according to [CPSqcp]	UTF8String [ETSI EN 319 412-2], chapter 4.2.4
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Issuing CA
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of this subject/end entity
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000011`B },	digitalSignature contentCommitment (note: has been renamed from nonrepudiation by X.509)
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 23 0},	OID listed in consolidated CP/CPS
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 2042 1 2 }	NCP+
subjectAltName {		
extnId	{ 2 5 29 17 },	
extnValue	{ if present name="MSISDN" serialNumber="MID/SAS transaction number" description="MID/SAS message to user" pseudonym="MID/SAS specific number" OID 2.16.756.1.83.200.0.0="RAS evidenceID", else "N/A"},	*Extension values as used by "All-in Signing Service"* directoryName, UTF8String OID 2.16.756.1.83.0.0.1, was used until January 2020.
issuerAltName {		
extnId	{ 2 5 29 18 },	
extnValue	{serialNumber="Response ID" description="Identifying Registration Authority"},	*Extension values as used by "All-in Signing Service"* directoryName, UTF8String
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	

Feld X.509	Werte, OID's	Bemerkungen
extnValue	"ldap://ldap.swissdigicert.ch/CN=Swisscom Saphir CA 2, dc=saphir,dc=swissdigicert,dc=ch? certificateRevocationList?, http://crl.swissdigicert.ch/sdcs-saphir2.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-calssuers
accessLocation	http://aia.swissdigicert.ch/sdcs-saphir2.crt ,	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/saphir2 ,	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	[RFC 3279]
signature	`..... `B }	2048 Bit, BIT STRING

1.3.1.3 Organisationszertifikat Saphir CA 2

Dieses Profil war von 2018 bis Dez 2021 im Einsatz.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 11}	SHA256withRSAEncryption
parameters	NULL },	[RFC 3279]
issuer	CN=Swisscom Saphir CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280, Valid for 3 years Not after 31.12.2021
subject	Name of the certificate holder containing• countryName, organizationName, organization Identifier, commonName and possibly optional name items per [CPSqcp]	UTF8String [ETSI EN 319 412-3], chapter 4.2.1
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Issuing CA
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of this subject/end entity
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000011`B },	digitalSignature contentCommitment (note: has been renamed from nonrepudiation by X.509)
certificatePolicies {		

Feld X.509	Werte, OID's	Bemerkungen
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 23 0 },	OID as defined in consolidated CP/CPS
extnValue	http://www.swissdigicert.ch/cps	[uRI], IA5String
extnValue	{ 0 4 0 2042 1 2 }	NCP+ as per [ETSI EN 319 411-1]
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	ldap://ldap.swissdigicert.ch/CN=Swisscom Saphir CA 2, dc=saphir,dc=swissdigicert,dc=ch? certificateRevocationList?, http://crl.swissdigicert.ch/sdcs-saphir2.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://aia.swissdigicert.ch/sdcs-saphir2.crt ,	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/saphir2 ,	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11}	SHA256withRSAEncryption
parameters	NULL },	[RFC 3279]
signature	`..... `B }	2048 Bit, BIT STRING

1.3.2 Generation 4

1.3.2.1 Swisscom Saphir CA 4 von Root CA 2 signiert

Die CA 4 wird als vollständig eigenständiger Baum aufgesetzt und nicht von CA 2 signiert.

1.3.2.2 Swisscom Saphir CA 4 von Root CA 4 signiert

Wichtige Änderungen zur Generation 2 sind in der Tabelle farblich markiert.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	{CN=Swisscom Root CA 4, organizationIdentifier=VATCH-CHE-101.654.423 O=Swisscom, OU=Digital Certificate Services, C=CH},	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid for 10 years
subject	{ "CN=Swisscom Saphir CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH" },	UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	
subjectPublicKey	'.....'B },	4096 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublic-Key-BitString of "Root CA 4"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of "Saphir CA 4"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000110000`B },	keyCertSign, cRLSign
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 30 4 2 } },	OID as defined in consolidated CP/CPS
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, 0=keine weitere CA darunter
extendedKeyUsage {		

Feld X.509	Werte, OID's	Bemerkungen
extnId	{ 2 5 29 37 },	
critical	FALSE,	BOOLEAN
extnValue	{1 2 840 113583 1 1 5},	Adobe PDF Signing, used to mark CA as technical constraint for [MozPol]
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	http://crl.swissdigicert.ch/sdcs-root4.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-calssuers
accessLocation	http://aia.swissdigicert.ch/sdcs-root4.crt ,	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
signature	`..... `B }	8192 Bit, BIT STRING

1.3.2.3 Benutzerzertifikat Saphir CA 4

Wichtige Änderungen zur Generation 2 sind in der Tabelle farblich markiert.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	{ "CN=Swisscom Saphir CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH" },	UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not longer than 3 years
subject	Name of the certificate holder containing• countryName, choice of (givenName and surname) or pseudonym, commonName and possibly optional name items according to [CPCqcp]	UTF8String [ETSI EN 319 412-2], chapter 4.2.4
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	3072 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	

Feld X.509	Werte, OID's	Bemerkungen
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Issuing CA
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of this subject/end entity
.....keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000011`B },	digitalSignature contentCommitment (note: has been renamed from nonrepudiation by X.509)
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 30 4 2},	OID as defined in the CP/CPS
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 2042 1 2 }	NCP+
subjectAltName {		*Optional Extension*
extnId	{ 2 5 29 17 },	
extnValue	{ if present name="MSISDN" serialNumber="MID/SAS transaction number" description="MID/SAS message to user" pseudonym="MID/SAS specific number" OID 2.16.756.1.83.200.0.0="RAS evidenceID", else "N/A"},	*Extension values as used by AIS 2.x:* • *name, serialNumber, description, pseudonym* *Extension values used by AIS 3.x:* • *serialNumber* directoryName, UTF8String OID 2.16.756.1.83.0.0.1 was used until January 2020.
issuerAltName {		*Optional Extension*
extnId	{ 2 5 29 18 },	
extnValue	{serialNumber="Response ID" description="Identifying Registration Authority"},	*Extension values used by AIS 2.x:* • *serialNumber, description (RA)* *Extension values used by AIS 3.x:* *serialNumber (Idp), description (Scheme)* directoryName, UTF8String
extendedKeyUsage {		
extnId	{ 2 5 29 37 },	
critical	FALSE,	BOOLEAN
extnValue	{1 2 840 113583 1 1 5},	Adobe PDF Signing, used to mark certificate technical constraint for [MozPol]
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://aia.swissdigicert.ch/sdcs-saphir4.crt	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-saphir4	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
signature	`..... `B }	4096 Bit, BIT STRING

1.3.2.4 Organisationszertifikat Saphir CA 4

Wichtige Änderungen zur Generation 2 sind in der Tabelle farblich markiert.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	{ "CN=Swisscom Saphir CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH" },	UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid for 3 years
subject	Name of the certificate holder containing• countryName, organizationName, organization Identifier, commonName and possibly optional name items per [CPSqcp]	UTF8String [ETSI EN 319 412-3], chapter 4.2.1
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	3072 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Issuing CA
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of this subject/end entity
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000011`B },	digitalSignature contentCommitment (note: has been renamed from nonrepudiation by X.509)
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 30 4 2},	OID as defined in the CP/CPS
extnValue	http://www.swissdigicert.ch/cps	[uRI], IA5String
extnValue	{ 0 4 0 2042 1 2 }	NCP+ as per [ETSI EN 319 411-1]
extendedKeyUsage {		
extnId	{ 2 5 29 37 },	
critical	FALSE,	BOOLEAN
extnValue	{1 2 840 113583 1 1 5},	Adobe PDF Signing, used to mark certificate technical constraint for [MozPol]
AuthorityInfoAccess{	SEQUENCE{	
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING

Feld X.509	Werte, OID's	Bemerkungen
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	http://aia.swissdigicert.ch/sdcs-saphir4.crt	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-saphir4	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
signature	`..... `B }	4096 Bit, BIT STRING

1.4 Rubin Issuing CA (LCP)

1.4.1 Generation 3

1.4.1.1 Swisscom Rubin CA 3

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	
issuer	{ "CN=Swisscom Root CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280, valid for 10 years
subject	{ "CN=Swisscom Rubin CA 3, O=Swisscom, OU=Digital Certificate Services, C=CH },	directoryName, UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublic-Key-BitString of "Root CA 2"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Issuing CA
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000110000`B },	keyCertSign, cRLSign
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 22 0 },	In a CA certificate, these policy information terms limit the set of policies for certification paths which in-clude this certificate.
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, 0=keine weitere CA darunter
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	http://crl.swissdigicert.ch/sdcs-root2.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-calssuers
accessLocation	http://aia.swissdigicert.ch/sdcs-root2.crt ,	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11},	sha256WithRSAEncryption
parameters	NULL },	
signature	`..... `B }	2048 Bit, BIT STRING

1.4.1.2 Benutzerzertifikat Rubin CA 3

Dieses Profil ist seit 2018 im Einsatz.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 11}	SHA256withRSAEncryption
parameters	NULL },	[RFC 3279]
issuer	CN=Swisscom Rubin CA 3, O=Swisscom, OU=Digital Certificate Services, C=CH	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not longer than 3 years, expiration not later than 31.12.2024
subject	Name of the certificate holder containing• countryName, choice of (givenName and surname) or pseudonym, commonName and possibly optional name items according to [CPSIcp]	UTF8String [ETSI EN 319 412-2], chapter 4.2.4
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Issuing CA
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of this subject/end entity
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000101`B },	keyEncipherment, digitalSignature
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 22 0},	OID as defined in consolidated CP/CPS.
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	ldap://ldap.swissdigicert.ch/CN=Swisscom Rubin CA 3, dc= rubin, dc=swissdigicert,dc=ch? certificateRevocationList?	[uRI], IA5String
extnValue	http://crl.swissdigicert.ch/sdcs-rubin2.crl	[uRI], IA5String
extKeyUsage {		
extnId	{ 2 5 29 37 },	
extnValue	{ 1 3 6 1 5 5 7 3 2 }, { 1 3 6 1 5 5 7 3 4} },	clientAuthentication, email protection
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://aia.swissdigicert.ch/sdcs-rubin2.crt ,	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp

Feld X.509	Werte, OID's	Bemerkungen
accessLocation	http://ocsp.swissdigicert.ch/rubin2 ,	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11}	SHA256withRSAEncryption
parameters	NULL },	[RFC 3279]
signature	`..... `B }	2048 Bit, BIT STRING

1.4.2 Generation 4

1.4.2.1 Swisscom Rubin CA 4 von Root CA 2 signiert

Die CA 4 wird als vollständig eigenständiger Baum aufgesetzt und nicht von CA 2 signiert.

1.4.2.2 Swisscom Rubin CA 4 von Root CA 4 signiert

Wichtige Änderungen zur Generation 2 sind in der Tabelle farblich markiert.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	{ "CN=Swisscom Saphir CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid for 10 years
subject	{ "CN=Swisscom Rubin CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH" },	UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	
subjectPublicKey	'.....'B },	4096 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublic-Key-BitString of "Root CA 4"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of "Rubin CA 4"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000110000`B },	keyCertSign, cRLSign
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 30 4 4 },	OID as defined in the CP/CPS
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, 0=keine weitere CA darunter
extendedKeyUsage {		

Feld X.509	Werte, OID's	Bemerkungen
extnId	{ 2 5 29 37 },	
critical	FALSE,	BOOLEAN
extnValue	{1 3 6 1 5 5 7 3 2 },	id-kp-clientAuth Required as technical restriction for [MozPol]
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	http://crl.swissdigicert.ch/sdcs-root4.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://aia.swissdigicert.ch/sdcs-root4.crt ,	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
signature	`..... `B }	8192 Bit, BIT STRING

1.4.2.3 Benutzerzertifikat Rubin CA 4

1.4.2.3.1 Benutzerzertifikat Rubin CA 4 - RSA

Wichtige Änderungen zur Generation 3 sind in der Tabelle farblich markiert.

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	{ "CN=Swisscom Rubin CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not longer than 3 years, expiration not later than 31.12.2024
subject	Name of the certificate holder containing• countryName, choice of (givenName and surname) or pseudonym, commonName and optional name items according to [CPClcp]	UTF8String [ETSI EN 319 412-2], chapter 4.2.4
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	2048 Bit, BIT STRING
extensions {		
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of "Rubin CA 4"
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of this subject/end entity
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000001`B },	digitalSignature
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 30 4 4 },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 2042 1 3 }	LCP as per [ETSI EN 319 411-1]
extKeyUsage {		
extnId	{ 2 5 29 37 },	
extnValue	{ 1 3 6 1 5 5 7 3 2 }},	clientAuthentication, Required for [CAB-BR] compliance
AuthorityInfoAccess {	SEQUENCE {	
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING

Feld X.509	Werte, OID's	Bemerkungen
AccessDescription	SEQUENCE {	
accessMethod	{ 1 3 6 1 5 5 7 48 2 },	id-ad-caIssuers
accessLocation	http://aia.swissdigicert.ch/sdcs-rubin4.crt ,	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/rubin4	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
signature	`..... `B }	4096 Bit, BIT STRING

1.4.2.3.2 Benutzerzertifikat Rubin CA 4 - ECC

Abweichungen zum RSA-Profil.

Feld X.509	Werte, OID's	Bemerkungen
subjectPublicKeyInfo {		
algorithm {		
algorithm	{1 2 840 10045 2 1},	id-ecPublicKey
parameters	{1 2 840 100453 1 7}}	prime256v1 [ETSI TS 119 312] also known as secp256r1 [RFC 5280] or P-256 in [FIPS186-3]
subjectPublicKey	'.....'B },	256 bit, BIT STRING

1.4.2.4 DV SSL Zertfikate der Rubin CA 4

Platzhalter: Werden unter der Generation 4 aktuell nicht ausgestellt.

1.5 Time-Stamping

1.5.1 Time Stamping CA 4.1

Seit 2020 werden die TSU Zertifikate von der TSA CA 4.1 EU signiert, deren Profile entsprechen aber gleichfalls den Anforderungen des Schweizer Rechts.

Die Details sind in Kapitel 2.3 des Dokumentes [Zertifikatsprofile EU] beschrieben.

2 Profile der Widerrufslisten

Die Widerrufslisten (CRLs) der Root CAs werden von diesen mit den eigenen privaten Schlüsseln signiert. Alle von einer Root CA widerrufenen Zertifikate erscheinen in der Widerrufsliste dieser Root CA. Die Widerrufslisten der Swisscom Digital Certificate Services sind im Format CRL v2 aufgebaut.

Die Ausstellung der Widerrufslisten erfolgt nach einer Änderung, aber mindestens 1 mal im Jahr.

Der LDAP-Baumknoten ist:

dc = ch

dc = swissdigicert

cn = [CA-Name]

Attribut: certificateRevocationList

Das CRL Profil enthält gemäss [RFC 5280], Kapitel 5.1, die Sequenz *tbsCertList* mit folgenden Feldern:

- Version, (Wert =1 gibt an, dass es sich um eine CRL Version 2 handelt)
- signature;
- issuer;
- lastUpdate;
- nextUpdate;
- revokedCertificates, inklusive Seriennummer des Zertifikats und Datum/Zeit der Ungültigerklärung.

Entsprechend [RFC 5280], Kapitel 5.2, sind der Sequenz *tbsCertList* folgende nichtkritische Erweiterungen angefügt:

- authorityKeyIdentifier
- cRLNumber

Die jeweils letzte CRL jeder CA wird durch einen speziellen Code im `nextUpdate` Feld gekennzeichnet.

Die nachfolgend referenzierten «Reason Codes» haben folgende Bedeutung:

Code	Bezeichnung	Bedeutung
0	Unspezifiziert	Keine genauere Beschreibung des Grundes für die Revokation.
1	Key Compromise	Der private Schlüssel ist oder könnte kompromittiert worden sein, nur bei Endzertifikaten.
2	CA Compromise	Der private Schlüssel einer CA ist oder könnte kompromittiert worden sein.
3	Affiliation Changed	Die "Zugehörigkeit" d.h. der Name oder andere Informationen über den Inhaber haben sich geändert.
4	Superseeded	Das Zertifikat wurde durch ein neueres abgelöst.
5	Cessation of Operation	Das Zertifikat wird nicht mehr länger für den ausgestellten Zweck benötigt.
6	Certificate Hold	Das Zertifikat ist (vorübergehend) gesperrt. **Hinweis**: Wird von Swisscom nicht verwendet.
7		Nicht verwendet.

Code	Bezeichnung	Bedeutung
8	Remove from CRL	Mit diesem Code wird innerhalb von delta CRLs angezeigt, dass dieses widerrufene Zertifikat abgelaufen ist, und von der Liste zu streichen ist. Ansonsten wird dieser Code genutzt, um eine Sperre wieder aufzuheben.
9	Privilege Withdrawn	Ein im Zertifikat dokumentiertes Recht wurde zurückgezogen.
10	AA Compromise	Der private Schlüssel einer Attribute Authority ist oder könnte kompromittiert worden sein.

2.1 Generation 2

Die Wiederrufslisten sind folgendermassen aufgebaut:

Feld X.509	Werte, OID's	Bemerkungen
CertificateList{		
tbsCertList	SEQUENCE {	
version	1,	Version 2
signature {		
algorithm	{1 2 840 113549 1 1 11} ,	sha256WithRSAEncryption
parameters	NULL ,	Für alle RSA Algorithmen ausser id-RSASSA-PSS
issuer	{ "CN=Swisscom [CA Name] , O=Swisscom, OU=Digital Certificate Services, C=ch},	distinguishedName, UTF8String
lastUpdate	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
nextUpdate	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
revokedCertificates {	SEQUENCE of SEQUENCE{	
userCertificate	<serial number>	Seriennummer des revozierten Zertifikats
revocationDate	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
CRLEntryExtensions{	SEQUENCE {	
CRLReason {	Reason Code gemäss Tabelle,	BITSTRING, optional
invalidityDate	" YYMMDDHHMMSSZ ",}	optional, wenn ungleich revocationDate
cRLExtensions	SEQUENCE{	CRL Erweiterungen
ExpiredCertsOnCRL	" YYMMDDHHMMSSZ ",	date on which the CRL starts to keep revocation status information for expired certificates
cRLNumber	< Laufnummer der CRL >	monoton steigende Laufnummer
authorityKeyIdentifier	`..... `O }	OCTET STRING, composed of the SHA-256-hash of subjectPublicKey-BitString of the associated CA
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11} ,	sha256WithRSAEncryption
parameters	NULL },	[RFC 3279]
signature	`..... `B }	2048 Bit, BIT STRING

2.2 Generation 4

Die Wiederrufslisten sind folgendermassen aufgebaut:

Feld X.509	Werte, OID's	Bemerkungen
CertificateList{		
tbsCertList	SEQUENCE {	
version	1,	Version 2
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	{ "CN=Swisscom Root CA 4, organizationIdentifier=VATCH-CHE-101.654.423,O=Swisscom, OU=Digital Certificate Services, C=CH"},	distinguishedName, UTF8String
lastUpdate	" YYMMDDHHMMSSZ ",	UTC

Feld X.509	Werte, OID's	Bemerkungen
nextUpdate	" YYMMDDHHMMSSZ ",	UTC 99991231235959Z bei Terminierung der CA im issuer DN
revokedCertificates {	SEQUENCE of SEQUENCE{	
userCertificate	<serial number>	Seriennummer des revozierten Zertifikats
revocationDate	" YYMMDDHHMMSSZ ",	UTC
CRLEntryExtensions{	SEQUENCE {	
CRLReason {	Reason Code gemäss Tabelle,	BITSTRING, optional
invalidityDate	" YYMMDDHHMMSSZ ",}	optional, wenn ungleich revocationDate
cRLExtensions	SEQUENCE{	CRL Erweiterungen
ExpiredCertsOnCRL	" YYMMDDHHMMSSZ ",	date on which the CRL starts to keep revocation status information for expired certificates
	{ 2 5 29 60 }	id-ce-expiredCertsOnCRL
cRLNumber	< Laufnummer der CRL >	monoton steigende Laufnummer
authorityKeyIdentifier	`..... `O }	OCTET STRING, composed of the SHA-256-hash of subjectPublicKey-BitString of the associated CA
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
signature	`..... `B }	4096 Bit, BIT STRING

3 Profile der Online-Statusabfragen

Die Profile für Online-Statusabfragen sind entsprechend den Vorgaben aus [RFC 6960] "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP" aufgebaut.

Die Instanzen, die Antworten auf OCSP Requests signieren, haben folgende Zertifikatsdefinitionen:

3.1 OCSP Signer Profil Generation 2

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	RFC 3279
issuer	CN=Swisscom <CAname>[1] CA [2-3], O=Swisscom, OU=Digital Certificate Services, C=CH	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280, valid for 2 years
subject	CN= OCSP Signer Swisscom <CAname> CA [2-4], O=Swisscom, OU=Digital Certificate Services, C=CH ,	directoryName, UTF8String, ETSI TS 102 280
subjectPublicKeyInfo {		
Algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
Parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	4096 Bit, BIT STRING
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Isssuing CA
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the associated CA
keyUsage {		
extnId	{ 2 5 29 15 },	
Critical	TRUE,	BOOLEAN
extnValue	`000100010`B },	nonRepudiation, cRLSign
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{2 16 756 1 83 11 0 = Diamant CA 2}; {2 16 756 1 83 16 0 = TSS CA2}; {2 16 756 1 83 17 0 = Smaragd CA 2}; {2 16 756 1 83 18 0 = Rubin CA 3}; {2 16 756 1 83 23 0 = Saphir CA 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.
extnValue	http://www.swissdigicert.ch/cps/ ,	[uRI], IA5String
PolicyQualifierId	(1 3 6 1 5 5 7 2 1),	
Qualifier	http://www.swissdigicert.ch/documents ,	[uRI], IA5String
basicConstraints {		
extnId	{ 2 5 29 19 },	
Critical	TRUE,	BOOLEAN
extnValue	{ cA FALSE },	BOOLEAN
pathLenConstraint	none },	INTEGER
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	

[1] Wobei CAName einer der folgenden Werte ist: Diamant, Saphir, Rubin oder TSS

Feld X.509	Werte, OID's	Bemerkungen
extnValue	ldap://ldap.swissdigicert.ch: cn=Swisscom <CAname> CA [2-4], dc=<CAname>,dc=swissdigicert, dc=ch?certificateRevocationList?	[uRI], IA5String
extnValue	http://crl.swissdigicert.ch/sdcs-<CAname>[2-4].crl ,	[uRI], IA5String
extKeyUsage {		
extnId	{ 2 5 29 37 },	
Critical	TRUE,	BOOLEAN
extnValue	{1 3 6 1 5 5 7 3 9}},	ocspSigning
ocspNoCheck {		
extnId	{ 1 3 6 1 5 5 7 48 1 5 },	
extnValue	{NULL}},	
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://aia.swissdigicert.ch/sdcs-<CAname>[2-4]2.crt ,	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11},	sha256WithRSAEncryption
parameters	NULL },	[RFC 3279]
signature	`..... `B }	2048 Bit, BIT STRING

3.2 OCSP Signer Profil Generation 4

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Positive Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
issuer	CN=Swisscom <CAname>[2] CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid for 1 year
subject	CN= OCSP Signer Swisscom <CAname> CA 4, organizationIdentifier=VATCH-CHE-101.654.423, O=Swisscom (Schweiz) AG, OU=Digital Certificate Services, C=CH ,	directoryName, UTF8String, ETSI TS 102 280
subjectPublicKeyInfo {		
Algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
Parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	4096 Bit, BIT STRING
authorityKeyIdentifier {		
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the Isssuing CA
subjectKeyIdentifier {		

[2] Wobei CAName einer der folgenden Werte ist: Diamant, Saphir oder Rubin

Feld X.509	Werte, OID's	Bemerkungen
extnId	{ 2 5 29 14 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the associated CA
keyUsage {		
extnId	{ 2 5 29 15 },	
Critical	TRUE,	BOOLEAN
extnValue	`000000010`B },	ContentCommitment
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{2 16 756 1 83 30 4 1 = Diamant CA 4}; {2 16 756 1 83 30 4 2 = Saphir CA 4}; {2 16 756 1 83 30 4 4 = Rubin CA 4};	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.
extnValue	http://www.swissdigicert.ch/cps/ ,	[uRI], IA5String
PolicyQualifierId	(1 3 6 1 5 5 7 2 1),	
Qualifier	http://www.swissdigicert.ch/documents ,	[uRI], IA5String
basicConstraints {		
extnId	{ 2 5 29 19 },	
Critical	TRUE,	BOOLEAN
extnValue	{ cA FALSE },	BOOLEAN
pathLenConstraint	none },	INTEGER
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	ldap://ldap.swissdigicert.ch: cn=Swisscom <CAname> CA [2-4], dc=<CAname>,dc=swissdigicert, dc=ch?certificateRevocationList?	[uRI], IA5String
extnValue	http://crl.swissdigicert.ch/sdcs-<CAname>4.crl ,	[uRI], IA5String
extKeyUsage {		
extnId	{ 2 5 29 37 },	
Critical	TRUE,	BOOLEAN
extnValue	{1 3 6 1 5 5 7 3 9}},	ocspSigning
ocspNoCheck {		
extnId	{ 1 3 6 1 5 5 7 48 1 5 },	
extnValue	{NULL}},	
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://aia.swissdigicert.ch/sdcs-<CAname>4.crt ,	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 10	id-RSASSA-PSS with mgf1 SHA256 (also known as SHA256WithRSAandMGF1)
parameters	{	SEQUENCE RSASSA-PSS-params
hashAlgorithm	2 16 840 1 101 3 4 2 1	id-sha256
maskGenAlgorithm	{	[1] MaskGenAlgorithm
	1 2 840 113549 1 1 8	id-mgf1
	2 16 840 1 101 3 4 2 1}	id-sha256
saltLength	32	INTEGER
trailerField	1}}	trailerFieldBC
signature	`..... `B }	BIT STRING

3.3 OCSP-Requests und -Responses

3.3.1 OCSP-Requests

Das Format der OCSP-Requests ist im [RFC 6960] beschrieben.

Feld X.509	Werte, OID's	Bemerkungen
OCSPRequest	Sequence	
tbsRequest		TBSRequest
optionalSignature		Optional: Signatur des Clients
TBSRequest {		
version	1	Version 2
requestorName	GeneralName	Optional, nur nötig, wenn der Request com Client signiert wird
requestList {		
Request {		
CertID {		
hashAlgorithm ,		AlgorithmIdentifier
issuerNameHash		Hash of Issuer's DN
issuerKeyHash		Hash of Issuers public key
serialNumber	}	SerialNumber of the Certificate
singleRequestExtensions {		Optional:
OCSNonce	}}}	
extensions	IMPLICIT Extensions	optional

Der OCSP-Request muss vom Client nicht signiert werden. Eine allfällige im OCSP-Request enthaltene Signatur wird vom OCSP-Responder nicht geprüft.

3.3.2 OCSP-Response

Das Format der OCSP-Responses ist im [RFC 6960] beschrieben.

Sofern der OCSP-Responder den Request erfolgreich validieren konnte, ist der Status "successful" und es wird ein OCSP-Response erstellt.

Feld X.509	Werte, OID's	Bemerkungen
version	1,	Version 2
serialNumber	[Integer]	positive Zahl
issuer		directoryName, UTF8String
OCSPResponse		
status	PKIStatusInfo	
status		PKIStatus
statusString		optional
failInfo	PKIFailureInfo	optional: [BIT STRING]
MessageImprint		
signature		sha256WithRSAEncryption.

3.3.2.1 Statusmeldungen

Mögliche Statusmeldungen und deren Bedeutung:

Statusmeldung	Zertifikat Status	Bedeutung
Good	Active	Der Zustand "Good" zeigt eine positive Antwort auf die Statusabfrage an.
Revoked	Revoked, suspended	Das Zertifikat sollte abgelehnt werden.
Unknown	Unknown	Der Status des Zertifikats konnte nicht eruiert werden.

3.3.2.2 Fehlerfälle

Im Fehlerfall gibt der OCSP-Responder eine entsprechende Meldung zurück. Fehler können von folgenden Typen sein:

- internalError: der OCSP-Responder hat einen inkonsistenten internen Zustand erreicht. Der Request sollte erneut gesendet werden, möglicherweise an einen anderen Responder.
- malformedRequest: der empfangene Request entspricht nicht der OCSP-Syntax.
- sigRequired: der Server verlangt, dass der Client den Request signiert.
- tryLater: der Service existiert zwar, kann aber vorübergehend nicht antworten.
- unauthorized: der Client ist nicht berechtigt, diese Anfrage an diesen Server zu richten oder der Server ist nicht in der Lage, autoritativ zu antworten.

Fehlermeldungen werden nicht signiert.