Addendum zu den Zertifikatsrichtlinien (CP/CPS)

Profile der Zertifikate, CRLs und OCSP

Für die:

- EU Issuing CA's (Diamant EU, Saphir EU, Time-Stamping)
- Zertifikate (Diamant EU, Saphir EU)
- Time-Stamping Services

Version: 1.6

Datum: 22. Dezember 2021

Swisscom IT Services Finance S.E. ("Swisscom ITSF")

Änderungskontrolle

Version	Datum	Ausführende Stelle	Bemerkungen/Art der Änderung
0.9	31.01.2017	H-P Waldegger	Initiale Version
1.0	19.02.2017	H-P Waldegger	Feedback Reto De Luca, Kerstin Wagner eingepflegt
1.1	20.06.2017	K. Wagner	Ergänzung von ETSI Standards und Angaben zu Timestamping, Update auf RFC 6960
1.2	31.07.2017	H-P Waldegger	Finale Version, ohne Time-stamping
1.3	25.10.2018	K. Wagner H-P Waldegger	RFC 5280 gilt für den gesamten Inhalt des Dokuments; Ergänzung Inhalt des Attributes "subject" bei den Benutzerzertifikaten; Anpassung Intervall der CRL-Erstellung. Anpassung Schlüssel/Algorithmen CA4.
1.3	08.03.2019	Governance Board	Freigabe
1.4		K. Wagner H-P Waldegger	Korrektur der OID von Saphir, Umbenennung TSA → TSU und Anpassungen subjectAltName/issuerAltName an AIS 3.0
1.4	22.01.2020	QTSP Board	Freigabe durch QTSP Board (neu für Governance Board)
1.5	18.02.2020	K. Wagner	Ergänzen der QC-Statements bei Time-stamping
1.5	01.07.2020	QTSP Board	Freigabe durch QTSP Board
1.6	03.06.2021	K. Wagner	Korrektur der keyusage bei OCSP-Signer Zertifikaten
1.6	22.12.2021	QTSP Board	Freigabe

Referenzierte Dokumente:

[eIDAS-VO]	Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
[DVO-2015/1502]	Durchführungsverordnung (EU) 2015/1502 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel
[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 V2.2.1 (2018-04): General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	ETSI EN 391 411-1 V1.2.2 (2018-04): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI EN 319 411-2]	ETSI EN 391 411-2 V2.2.2 (2018-04): 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 V1.1.1 (2016-03): Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
[ETSI EN 319 412-1]	ETSI EN 319 412-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[ETSI EN 319 412-2]	ETSI EN 319 412-2 V2.1.1 (2016-02) 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 V1.1.1 (2016-02) 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 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[ETSI EN 319 422]	ETSI EN 319 422, V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[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 (Mai 2008) 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"
[CP/CPS]	Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klassen „Diamant" (qualifiziert) und „Saphir" (fortgeschritten) AT, Version 3.3
[Addendum]	Addendum zum CP/CPS: Profile der Zertifikate, Sperrlisten (CRL) und Online Statusabfragen, Version 3.6

swisscom

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument ist ein Addendum zum CP/CPS von Swisscom Digital Certificate Services, einer Dienstleistung der Swisscom IT Services Finance S.E..

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.

2 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 der eIDAS Verordnung [eIDAS-VO], der entsprechenden Durchführungsverordnung [DVO-2015/1502], sowie den referenzierten ETSI Standards.
Zur Sicherstellung der Kompatibiliäte im internationalen Umfeld und der Rückwärtskomatibilität mit älteren Systemen und Datenbanken können in alle n Zertifikaten die Namen des Zertifikatsinhabers (Subject DN) generell entsprechend den Vorgaben aus RFC 5280 Kapitel 4.1.2.6 Absatz 4 Variante c vereinfacht werden.

2.1 Root CA 2 (Swisscom Root CA 2)

Das Zertifikatsprofil der Root CA 2 ist im Dokument CPS_SDCS_2_16_756_1_83_Zertifikatsprofile [Addendum] beschrieben.

2.1.1 Diamant EU CA 4 Issuing CA (qualifiziert) (Swisscom Diamant EU CA 4)

Diese Issuing CA ist maximal bis zum 31.12.2022 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 },	
issuer	{ "CN=Swisscom Root CA 2, O=Swisscom, OU=Digital Certificate Services, C=CH" },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	
notAfter	" YYMMDDHHMMSSZ " ,	valid for 10 years
subject	{ "CN=Swisscom Diamant EU CA 4, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	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 EU CA 4"
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 83 100 4 1 },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
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 {		
extnId	{ 1 3 6 1 5 5 7 1 3 },	
critical	FALSE,	BOOLEAN
extnValue	SEQUENCE {	OCTET STRING
QCStatement	SEQUENCE {	

Feld X.509	Werte, OID's	Bemerkungen
statementId	{ 0 4 0 1862 1 1 }	qcs-QcCompliance
statementId	{ 0 4 0 1862 1 4 }}}}}	QcSSCD
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11},	sha256WithRSAEncryption
parameters	NULL },	
signature	`..... `B }	2048 Bit, BIT STRING

2.1.1.1 Benutzerzertifikat EU Diamant CA 4 (qualifiziert) für natürliche Personen

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 EU CA 4, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not more than 3 years, not after 31.12.2022
subject	Name of the certificate holder containing countryName, choice of (givenName and surname) or pseudonym, commonName and possibly optional name items according to CP/CPS Diamant EU CA 4 [CP/CPS]	directoryName, 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 },	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 EU 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 83 100 4 1 },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 194112 1 2 }	QCP-n-qscd
subjectAltName {		
extnId	{ 2 5 29 17 },	*Optional Extension*

Feld X.509	Werte, OID's	Bemerkungen
extnValue	{ if present name="MSISDN" serialNumber=" transaction number" description="MID/SAS message to user" pseudonym="MID/SAS specific number", else "N/A"},	*Extension values used by AIS 2.x:* • *name, serialNumber, description, pseudonym* *Extension values used by AIS 3.x:* • *serialNumber* directoryName, UTF8String
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)* directoryName, UTF8String
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	ldap://ldap.swissdigicert.ch/CN=Swisscom%20Diamant%20EU%20CA%204,dc=diamant4-eu,dc=swissdigicert,dc=ch?certificateRevocationList?, http://crl.swissdigicert.ch/sdcs-diamant4-eu.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-diamant4-eu.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-eu	[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 SSCD
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 5 },	qcs-QcEuPDS: PKI Disclosure Statements
PdsLocations	SEQUENCE OF {	
PdsLocation	SEQUENCE {	
url	https://www.swissdigicert.ch/diamant4eu-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 11}	sha256WithRSAEncryption
Parameters	NULL },	[RFC 3279]
Signature	`..... `B }	2048 Bit, BIT STRING, [ETSI TS 119 312]

2.1.1.2 Organisationszertifikat Diamant EU CA 4 (qualifiziert) für juristische Personen

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 EU CA 4, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not more than 3 years, not after 31.12.2022
subject	Gemäss den Anforderungen der CP/CPS Diamant EU CA 4 [CP/CPS], mindestens: - countryName - organizationName - organizationIdentifier und - commonName	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 },	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 EU 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 83 100 4 1 },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 194112 1 3 }	QCP-l-qscd
subjectAltName		*Optional Extension*
issuerAltName		*Optional Extension*
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	ldap://ldap.swissdigicert.ch/CN=Swisscom%20Diamant%20EU%20CA%204,dc=diamant4-eu,dc=swissdigicert,dc=ch?certificateRevocationList?, http://crl.swissdigicert.ch/sdcs-diamant4-eu.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-diamant4-eu.crt	[uRI], IA5String

Feld X.509	Werte, OID's	Bemerkungen
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-diamant4-eu	[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: electronic seals
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 4 }}}}	qcs-QcSSCD
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 5 },	qcs-QcEuPDS: PKI Disclosure Statements
PdsLocations	SEQUENCE {	
PdsLocation	SEQUENCE {	
url	https://www.swissdigicert.ch/diamant4eu-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 11}	sha256WithRSAEncryption
Parameters	NULL },	[RFC 3279]
Signature	`..... `B }	2048 Bit, BIT STRING, [ETSI TS 119 312]

2.1.2 Saphir EU CA 4 Issuing CA (fortgeschritten) (Swisscom Saphir EU CA 4)

Diese Issuing CA ist maximal bis zum 31.12.2022 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 },	
issuer	{ "CN=Swisscom Root CA 2, 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 EU CA 4, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E. OU=Digital Certificate Services, C=AT },	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 EU 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 83 100 4 2 },	
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

2.1.2.1 Benutzerzertifikat Saphir EU CA 4 (fortgeschritten) für natürliche Personen

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 EU CA 4, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E. OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not more than 3 years, not after 31.12.2022
subject	Name of the certificate holder containing countryName, choice of (givenName and surname) or pseudonym, commonName and possibly optional name items according toCP/CPS Saphir EU CA 4 [CP/CPS]	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 "Saphir EU 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	`000000011`B },	digitalSignature contentCommitment (note: has been renamed from nonrepudiation by X.509)
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 100 4 2},	
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=" transaction number" description="MID/SAS message to user" pseudonym="MID/SAS specific number", else "N/A"},	*Extension values used by AIS 2.x:* • *name, serialNumber, description, pseudonym* *Extension values used by AIS 3.x:* • *serialNumber* directoryName, UTF8String
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)*

Feld X.509	Werte, OID's	Bemerkungen
		directoryName, UTF8String
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	ldap://ldap.swissdigicert.ch/CN=Swisscom%20Saphir%20EU%20CA%204,dc=saphir4-eu,dc=swissdigicert,dc=ch?certificateRevocationList?, http://crl.swissdigicert.ch/sdcs-saphir4-eu.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-saphir4-eu.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-eu	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	[RFC 3279]
signature	`..... `B }	2048 Bit, BIT STRING

2.1.2.2 Organisationszertifikat Saphir EU CA 4 (fortgeschritten) für juristische Personen

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 EU CA 4, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E. OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not more than 3 years, not after 31.12.2021
subject	Gemäss den Anforderungen der CP/CPS Saphir EU CA 4, mindestens - countryName - organizationName - organizationIdentifier - commonName	directoryName, UTF8String
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 "Saphir EU 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

Feld X.509	Werte, OID's	Bemerkungen
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 83 100 4 2},	
extnValue	http://www.swissdigicert.ch/cps	[uRI], IA5String
extnValue	{ 0 4 0 2042 1 2 }	NCP+
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	ldap://ldap.swissdigicert.ch/CN=Swisscom%20Saphir%20EU%20CA%204,dc=saphir4-eu,dc=swissdigicert,dc=ch?certificateRevocationList?, http://crl.swissdigicert.ch/sdcs-saphir4-eu.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-saphir4-eu.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-eu	[uRI], IA5String
signatureAlgorithm {		
algorithm	{1 2 840 113549 1 1 11}	SHA256withRSAEncryption
parameters	NULL },	[RFC 3279]
signature	`..... `B }	2048 Bit, BIT STRING

2.2 Root CA 4 (Swisscom Root CA 4)

Das Zertifikatsprofil der Root CA 4 ist im Dokument CPS_SDCS_2_16_756_1_83_Zertifikatsprofile [Addendum] beschrieben.

2.2.1 Diamant EU CA 4.1 Issuing CA (qualifiziert) (Swisscom Diamant EU CA 4.1)

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 ",	
notAfter	" YYMMDDHHMMSSZ " ,	valid for 10 years
subject	{ "CN=Swisscom Diamant EU CA 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	directoryName, 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 "Diamant EU CA 4.1"
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 83 100 4 1 },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, keine weitere CA darunter
cRLDistributionPoints {		

Feld X.509	Werte, OID's	Bemerkungen
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
qcStatements {		
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
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

2.2.1.1 Benutzerzertifikat EU Diamant CA 4.1 (qualifiziert) für natürliche Personen

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 EU CA 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not more 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 CP/CPS Diamant EU CA 4 [CP/CPS]	directoryName, 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 {		

Feld X.509	Werte, OID's	Bemerkungen
extnId	{ 2 5 29 35 },	
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of "Diamant EU CA 4.1"
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 83 100 4 1 },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 194112 1 2 }	QCP-n-qscd
subjectAltName {		
extnId	{ 2 5 29 17 },	*Optional Extension*
extnValue	{ if present name="MSISDN" serialNumber=" transaction number" description="MID/SAS message to user" pseudonym="MID/SAS specific number", else "N/A"},	*Extension values used by AIS 2.x:* • *name, serialNumber, description, pseudonym* *Extension values used by AIS 3.x:* • *serialNumber* directoryName, UTF8String
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)* directoryName, UTF8String
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-diamant4.1-eu.crt	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-diamant4.1-eu	[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 {	Optional extension defining liability limit
statementId	{ 0 4 0 1862 1 2 },	qcs-QcLimitValue
MonetaryValue	SEQUENCE {	value = amount * 10^exponent
currency	EUR	Iso4217CurrencyCode
amount	1	INTEGER
exponent	[1-6]	INTEGER
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 SSCD
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 5 },	qcs-QcEuPDS: PKI Disclosure Statements
PdsLocations	SEQUENCE OF {	

Feld X.509	Werte, OID's	Bemerkungen
PdsLocation	SEQUENCE {	
url	https://www.swissdigicert.ch/diamant4eu-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]

2.2.1.2 Organisationszertifikat Diamant EU CA 4.1 (qualifiziert) für juristische Personen

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 EU CA 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not more than 3 years
subject	Gemäss den Anforderungen der CP/CPS Diamant EU CA 4 [CP/CPS], mindestens: - countryName - organizationName - organizationIdentifier - commonName	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 "Diamant EU CA 4.1"
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 {		

Feld X.509	Werte, OID's	Bemerkungen
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 83 100 4 1 },	
extnValue	http://www.swissdigicert.ch/cps/	[uRI], IA5String
extnValue	{ 0 4 0 194112 1 3 }	QCP-l-qscd
subjectAltName		*Optional Extension*
issuerAltName		*Optional Extension*
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-diamant4.1-eu.crt	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-diamant4.1-eu	[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 {	
QCStatement	SEQUENCE {	Optional extension defining liability limit
statementId	{ 0 4 0 1862 1 2 },	qcs-QcLimitValue
MonetaryValue	SEQUENCE {	value = amount * 10^exponent
currency	EUR	Iso4217CurrencyCode
amount	1	INTEGER
exponent	[1-6]	INTEGER
statementId	{ 0 4 0 1862 1 6 2 },	qcs-QcType: electronic seals
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 4 },	qcs-QcSSCD
QCStatement	SEQUENCE {	
statementId	{ 0 4 0 1862 1 5 },	qcs-QcEuPDS: PKI Disclosure Statements
PdsLocations	SEQUENCE {	
PdsLocation	SEQUENCE {	
url	https://www.swissdigicert.ch/diamant4eu-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]

2.2.2 Saphir EU CA 4.1 Issuing CA (fortgeschritten) (Swisscom Saphir EU CA 4.1)

Diese Issuing CA ist frühestens ab 2020 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 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 EU CA 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E. OU=Digital Certificate Services, C=AT },	directoryName, 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 EU CA 4.1"
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 83 100 4 2 },	
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-root4.crl",	[uRI], IA5String
AuthorityInfoAccess{		SEQUENCE
extnId	{ 1 3 6 1 5 5 7 1 1 },	OCTET STRING

Feld X.509	Werte, OID's	Bemerkungen
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

2.2.2.1 Benutzerzertifikat Saphir EU CA 4.1 (fortgeschritten) für natürliche Personen

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 EU CA 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E. OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not more 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 CP/CPS Saphir EU CA 4 [CP/CPS]	directoryName, UTF8String, ETSI TS 102 280
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 "Saphir EU CA 4.1"
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 },	

Feld X.509	Werte, OID's	Bemerkungen
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 83 100 4 2},	
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=" transaction number" description="MID/SAS message to user" pseudonym="MID/SAS specific number", else "N/A"},	*Extension values used by AIS 2.x:* • *name, serialNumber, description, pseudonym* *Extension values used by AIS 3.x:* • *serialNumber* directoryName, UTF8String
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
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-saphir4.1-eu.crt	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-saphir4.1-eu	[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

2.2.2.2 Organisationszertifikat Saphir EU CA 4.1 (fortgeschritten) für juristische Personen

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 Saphir EU CA 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E. OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, valid not more than 3 years
subject	Gemäss den Anforderungen der CP/CPS Saphir EU CA 4, mindestens - countryName - organizationName - organizationIdentifier - commonName	directoryName, UTF8String
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 "Saphir EU CA 4.1"
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 83 100 4 2},	
extnValue	http://www.swissdigicert.ch/cps	[uRI], IA5String
extnValue	{ 0 4 0 2042 1 2 }	NCP+
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-saphir4.1-eu.crt	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-saphir4.1-eu	[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

2.3 Time Stamping

2.3.1 Generation 3

Die Zertifikatsprofile und weitere Details der TSS CA 2 und der TSA 3 sind im Dokument CPS_SDCS_2_16_756_1_83_Zertifikatsprofile [Addendum] beschrieben.

2.3.2 Generation 4.1

2.3.2.1 Time Stamping Service CA 4.1 Issuing CA (Swisscom TSS CA 4.1)

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 Root CA 4, organizationIdentifier=VATCH-CHE-101.654.423 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 TSS CA 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	directoryName, 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 "TSS CA 4.1"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`001100000`B },	CertSign, cRLSign
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 100 4 5 },	OID of the related CP/CPS
extnValue	http://www.swissdigicert.ch/cps	[uRI], IA5String
basicConstraints {		
extnId	{ 2 5 29 19 },	

Feld X.509	Werte, OID's	Bemerkungen
critical	TRUE,	BOOLEAN
extnValue	{ cA TRUE },	BOOLEAN
pathLenConstraint	0 },	INTEGER, 0=keine weitere CA unterhalb
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
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 {	
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 Statements
PdsLocations	SEQUENCE OF {	
PdsLocation	SEQUENCE {	
url	https://www.swissdigicert.ch/timestamping4.1.pdf	According to [ETSI EN 319 421] [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 }	8192 Bit, BIT STRING

2.3.2.2 TSU Time Stamping Unit Zertifikat CA 4.1 (Swisscom TSU CA 4.1)

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

Feld X.509	Werte, OID's	Bemerkungen
tsaCertificate Certificate ::={		
tbsCertificate }		
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 TSS CA 4.1, organizationIdentifier=VATAT-U64741248,	directoryName, UTF8String

Feld X.509	Werte, OID's	Bemerkungen
	O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280, valid for 3 years
subject	{ "CN= Swisscom TSU 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
subjectPublicKeyInfo {		
algorithm {		
algorithm	{ 1 2 840 113549 1 1 1 },	hashAlgorithmIdentifier
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 the subjectPublicKey-BitString of "TSU 4.1"
keyUsage {		
extnId	{ 2 5 29 15 },	
critical	TRUE,	BOOLEAN
extnValue	`000000010`B },	nonRepudation
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{ 2 16 756 1 83 100 4 5 },	ETSI TS 101 861 V1.2.1
extnValue	http://www.swissdigicert.ch/cps ,	[uRI], IA5String
basicConstraints {		
extnId	{ 2 5 29 19 },	
critical	TRUE,	BOOLEAN
extnValue	{ cA FALSE },	BOOLEAN
pathLenConstraint	0 },	INTEGER
extendedKeyUsage {		
extnId	{ 2 5 29 37 },	
critical	TRUE,	BOOLEAN
extnValue	{1 3 6 1 5 5 7 3 8 },	timeStamping
cRLDistributionPoints {		
extnId	{ 2 5 29 31 },	
extnValue	http://crl.swissdigicert.ch/sdcs-tss4.1.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-tss4.1.crt ,	[uRI], IA5String
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 1 },	id-ad-ocsp
accessLocation	http://ocsp.swissdigicert.ch/sdcs-tss4.1	[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 {	

Feld X.509	Werte, OID's	Bemerkungen
statementId	{ 0 4 0 1862 1 6 2 },	qcs-QcType: qualified electronic seal
QCStatement	SEQUENCE {	
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 Statements
PdsLocations	SEQUENCE OF {	
PdsLocation	SEQUENCE {	
url	https://www.swissdigicert.ch/timestamping4.1.pdf	According to [ETSI EN 319 421] [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

3 Profile der Widerrufslisten

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

Die Ausstellung der Widerrufslisten erfolgt periodisch im Intervall von 60 Minuten, die Gültigkeit beträgt 7 Tage.

Der LDAP-Baumknoten ist:

dc = ch
dc = swissdigicert
cn = [CAname][1]
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;
- thisUpdate;
- 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. **Anmerkung**: wird von Swisscom nicht verwendet.
7		Nicht verwendet.
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.

[1] Wobei CAname einer der folgenden Werte ist: Diamant, Saphir

3.1 Generation 4

Die Wiederrufslisten sind folgendermassen aufgebaut:

Feld X.509	Werte, OID's	Bemerkungen
CertificateList{		
tbsCertList		
version	1,	Version 2
signature {		
algorithm	{1 2 840 113549 1 1 11} ,	sha256WithRSAEncryption
Parameters	NULL },	[RFC 3279]
issuer	{ "CN=Swisscom [CAname] EU CA 4, O=Swisscom IT Services Finance S.E., organizationIdentifier=VATAT-U64741248, OU=Digital Certificate Services, C=AT},	distinguishedName, UTF8String
thisUpdate	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
nextUpdate	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280 99991231235959Z bei Terminierung der CA im issuer DN
RevokedCertificates {	SEQUENCE{	
userCertificate	<serial number>	Seriennummer des revozierten Zertifikats
RevocationDate	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
CRLEntryExtension{		
CRLReason {	SEQUENCE{	
extnId	{ 2 5 29 21 },	
extnValue	Reason Code *) },	BITSTRING, optional
InvalidityDate	SEQUENCE{	
extnId	{ 2 5 29 24 },	
extnValue	" YYMMDDHHMMSSZ " },	UTC, ETSI TS 102 280
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

3.2 Generation 4.1

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 [CA Name] EU CA 4.1 , O=Swisscom IT Services Finance S.E., organizationIdentifier=VATAT-U64741248, OU=Digital Certificate Services, C=AT "},	distinguishedName, UTF8String

Feld X.509	Werte, OID's	Bemerkungen
lastUpdate	" YYMMDDHHMMSSZ ",	UTC
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

4 Profile der Online-Statusabfragen

Die Profile für Online-Statusabfragen sind entsprechend den Vorgaben der CP/CPS, sowie den referenzierten Dokumenten, insbesondere dem [RFC 6960], aufgebaut.

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

4.1 OCSP Signer Profil EU CA 4

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	Zahl [Integer]
signature {		
algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
parameters	NULL },	[RFC 3279]
issuer	CN=Swisscom <CAname>[2] EU CA 4, O=Swisscom IT Services Finance S.E. OU=Digital Certificate Services, C=AT	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280, valid for 1 year
subject	CN= OCSP Signer Swisscom <CAname> EU CA 4, O=Swisscom IT Services Finance S.E. OU=Digital Certificate Services, C=AT	directoryName, UTF8String, ETSI TS 102 280
subjectPublicKeyInfo {		
Algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
Parameters	NULL },	[RFC 3279]
subjectPublicKey	'……..'B },	2048 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 issuer
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	
extnValue	`…..`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the subject
keyUsage {		
extnId	{ 2 5 29 15 },	
Critical	TRUE,	BOOLEAN
extnValue	`000000010`B },	contentCommitment
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{2 16 756 1 83 100 4 1} or {2 16 756 1 83 100 4 2}	OID of the related CA
PolicyQualifierId	(1 3 6 1 5 5 7 2 1),	
Qualifier	http://www.swissdigicert.ch/cps	[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	http://crl.swissdigicert.ch/sdcs-<CAname>4-eu.crl ,	[uRI], IA5String

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

Feld X.509	Werte, OID's	Bemerkungen
	ldap://ldap.swissdigicert.ch: cn=Swisscom <CAname> EU CA 4, dc=<CAname>4-eu,dc=swissdigicert, dc=ch?certificateRevocationList?	
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-eu.crt ,	[uRI], IA5String
signatureAlgorithm {		
Algorithm	{1 2 840 113549 1 1 11}	sha256WithRSAEncryption
Parameters	NULL },	[RFC 3279]
Signature	`..... `B }	2048 Bit, BIT STRING, [ETSI TS 119 312]

4.2 OCSP Signer Profil EU CA 4.1

Feld X.509	Werte, OID's	Bemerkungen
version	2,	Version 3
serialNumber	eineindeutiger Integer	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> EU CA 4.1, organizationIdentifier=VATAT-U64741248, O=Swisscom IT Services Finance S.E., OU=Digital Certificate Services, C=AT },	directoryName, UTF8String
validity {		
notBefore	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280
notAfter	" YYMMDDHHMMSSZ ",	UTC, ETSI TS 102 280, valid for 1 year
subject	CN= OCSP Signer Swisscom <CAname> EU CA 4.1, organizationIdentifier= VATAT-U64741248, O=Swisscom IT Services Finance S.E. OU=Digital Certificate Services, C=AT	directoryName, UTF8String, ETSI TS 102 280
subjectPublicKeyInfo {		
Algorithm	{ 1 2 840 113549 1 1 1 },	rsaEncryption
Parameters	NULL },	[RFC 3279]
subjectPublicKey	'.....'B },	2048 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 issuer
subjectKeyIdentifier {		
extnId	{ 2 5 29 14 },	

Feld X.509	Werte, OID's	Bemerkungen
extnValue	`.....`O },	OCTET STRING, composed of the 160-bit SHA-256 hash of subjectPublicKey-BitString of the subject
keyUsage {		
extnId	{ 2 5 29 15 },	
Critical	TRUE,	BOOLEAN
extnValue	`000000010`B },	contentCommitment
certificatePolicies {		
extnId	{ 2 5 29 32 },	
extnValue	{2 16 756 1 83 100 4 1} or {2 16 756 1 83 100 4 2}	OID of the related CA
PolicyQualifierId	(1 3 6 1 5 5 7 2 1),	
Qualifier	http://www.swissdigicert.ch/cps	[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	http://crl.swissdigicert.ch/sdcs-<CAname>4.1-eu.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>4.1-eu.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 }	4096 Bit, BIT STRING

4.3 OCSP Responses

Der OCSP Responder beantwortet OCSP Anfragen auf Port 80 gemäss [RFC 6960].

4.3.1 Statusmeldungen

Folgende Statusmeldungen werden unterstützt:

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

4.3.2 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.

5 Beispiele (Informativ)

5.1 Benutzerzertifikat EU Diamant CA 4 für natürliche Personen

```
SEQUENCE (3 elem)
 SEQUENCE (8 elem)
  [0] (1 elem)
   INTEGER 2
  INTEGER (123 bit) 8246832020543727620036271797347158053
  SEQUENCE (2 elem)
   OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
   NULL
  SEQUENCE (5 elem)
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
     PrintableString VATAT-U64741248
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
     PrintableString AT
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
     PrintableString Swisscom IT Services Finance S.E.
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
     PrintableString Digital Certificate Services
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
     PrintableString Swisscom Diamant EU CA 4
  SEQUENCE (2 elem)
   UTCTime 2017-06-26 09:38:22 UTC
   UTCTime 2017-06-26 09:48:22 UTC
  SEQUENCE (7 elem)
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
     PrintableString Reto De Luca QC-N 2017-06-26
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
     PrintableString MIDCHEHF4F4CF4O8
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
     PrintableString De Luca
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
     PrintableString Reto
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
     PrintableString AIS PROD - Test purposes only
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
     PrintableString Swisscom (Schweiz) AG
   SET (1 elem)
    SEQUENCE (2 elem)
     OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
     PrintableString ch
  SEQUENCE (2 elem)
   SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
    NULL
   BIT STRING (1 elem)
    SEQUENCE (2 elem)
     INTEGER (2048 bit) 29429633850353621520672307645318636622682297230635193909620289220…
```

```
69          INTEGER 65537
70        [3] (1 elem)
71        SEQUENCE (9 elem)
72          SEQUENCE (2 elem)
73            OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
74            OCTET STRING (1 elem)
75              SEQUENCE (2 elem)
76                SEQUENCE (2 elem)
77                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
78                  [6] http://ocsp.swissdigicert.ch/sdcs-diamant4-eu
79                SEQUENCE (2 elem)
80                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/AIA descriptor)
81                  [6] http://aia.swissdigicert.ch/sdcs-diamant4-eu.crt
82          SEQUENCE (2 elem)
83            OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
84            OCTET STRING (1 elem)
85              SEQUENCE (1 elem)
86                [0] (20 byte) 8B01D7DEC792B2E45B249EB68F493AAFA9C672DD
87          SEQUENCE (2 elem)
88            OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
89            OCTET STRING (1 elem)
90              SEQUENCE (2 elem)
91                SEQUENCE (2 elem)
92                  OBJECT IDENTIFIER 2.16.756.1.83.100.4.1 cps (Swisscom Diamant/Saphir CP/CPS)
93                  SEQUENCE (1 elem)
94                    SEQUENCE (2 elem)
95                      OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
96                      IA5String http://www.swissdigicert.ch/cps/
97                SEQUENCE (1 elem)
98                  OBJECT IDENTIFIER 0.4.0.194112.1.2 etsiPolicyIdentifier (QCP-n-qscd)
99          SEQUENCE (2 elem)
100           OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
101           OCTET STRING (1 elem)
102             SEQUENCE (2 elem)
103               SEQUENCE (1 elem)
104                 [0] (1 elem)
105                   [0](1 elem)
106                     [6] http://crl.swissdigicert.ch/sdcs-diamant4-eu.crl
107               SEQUENCE (1 elem)
108                 [0] (1 elem)
109                   [0] (1 elem)
110                     [6] ldap://ldap.swissdigicert.ch/CN=Swisscom%20Diamant%20EU%20CA%204,dc=diam…
111         SEQUENCE (3 elem)
112           OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
113           BOOLEAN true
114           OCTET STRING (1 elem)
115             BIT STRING (2 bit) 01
116         SEQUENCE (2 elem)
117           OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
118             OCTET STRING (1 elem)
119               SEQUENCE (1 elem)
120                 [4] (1 elem)
121                   SEQUENCE (4 elem)
122                     SET (1 elem)
123                       SEQUENCE (2 elem)
124                         OBJECT IDENTIFIER 2.5.4.13 description (X.520 DN component)
125                         UTF8String S3-Monitor AIS PROD eIDAS QC-N - please confirm
126                     SET (1 elem)
127                       SEQUENCE (2 elem)
128                         OBJECT IDENTIFIER 2.5.4.41 name (X.520 DN component)
129                         UTF8String N/A
130                     SET (1 elem)
131                       SEQUENCE (2 elem)
132                         OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
133                         PrintableString ID-0f2ddaf2-4413-4ab5-b7b5-312bd21e3717
134                     SET (1 elem)
135                       SEQUENCE (2 elem)
136                         OBJECT IDENTIFIER 2.5.4.65 pseudonym (X.520 DN component)
137                         UTF8String MIDCHEHF4F4CF4O8
138         SEQUENCE (2 elem)
139           OBJECT IDENTIFIER 2.5.29.18 issuerAltName (X.509 extension)
140           OCTET STRING (1 elem)
141             SEQUENCE (1 elem)
142               [4] (1 elem)
```

```
143             SEQUENCE (2 elem)
144               SET (1 elem)
145                 SEQUENCE (2 elem)
146                   OBJECT IDENTIFIER 2.5.4.13 description (X.520 DN component)
147                   UTF8String s3-monitor
148               SET (1 elem)
149                 SEQUENCE (2 elem)
150                   OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
151                   PrintableString WVDWAgoKeB8AARZE1v0AAABZ
152       SEQUENCE (2 elem)
153         OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
154         OCTET STRING (1 elem)
155           SEQUENCE (4 elem)
156             SEQUENCE (1 elem)
157               OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (EU qualified certificate)
158             SEQUENCE (1 elem)
159               OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (Private Key resides in QSCD)
160             SEQUENCE (1 elem)
161               OBJECT IDENTIFIER 0.4.0.1862.1.6.1 etsiQcSQcType (Electronic signatures)
162             SEQUENCE (2 elem)
163               OBJECT IDENTIFIER 0.4.0.1862.1.5 etsiQcEuPDS (PKI Disclosure Statements)
164               SEQUENCE (1 elem)
165                 SEQUENCE (2 elem)
166                   IA5String https://www.swissdigicert.ch/diamant4eu-n.pdf
167                   PrintableString en
168     SEQUENCE (2 elem)
169       OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
170         OCTET STRING (1 elem)
171           OCTET STRING (20 byte) BA7D9503D634E9384EE05D72741C5541FB543599
172   SEQUENCE (2 elem)
173     OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
174     NULL
175   BIT STRING (2048 bit) 0101000000110110000010011100110111101011001101001000100011010000010…
```

5.2 Benutzerzertifikat EU Saphir CA 4 für natürliche Personen

```
1   SEQUENCE (3 elem)
2     SEQUENCE (8 elem)
3       [0] (1 elem)
4         INTEGER 2
5       INTEGER (128 bit) 301279643701029415739413838114472404765
6       SEQUENCE (2 elem)
7         OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
8         NULL
9       SEQUENCE (5 elem)
10        SET (1 elem)
11          SEQUENCE (2 elem)
12            OBJECT IDENTIFIER 2.5.4.97 organizationIdentifier (X.520 DN component)
13            PrintableString VATAT-U64741248
14        SET (1 elem)
15          SEQUENCE (2 elem)
16            OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
17            PrintableString AT
18        SET (1 elem)
19          SEQUENCE (2 elem)
20            OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
21            PrintableString Swisscom IT Services Finance S.E.
22        SET (1 elem)
23          SEQUENCE (2 elem)
24            OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
25            PrintableString Digital Certificate Services
26        SET (1 elem)
27          SEQUENCE (2 elem)
28            OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
29            PrintableString Swisscom Saphir EU CA 4
30      SEQUENCE (2 elem)
31        UTCTime 2017-06-26 09:36:12 UTC
32        UTCTime 2017-06-26 09:46:12 UTC
33      SEQUENCE (7 elem)
34        SET (1 elem)
35          SEQUENCE (2 elem)
```

```
36          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
37          PrintableString Reto De Luca ADV-N 2017-06-26
38        SET (1 elem)
39          SEQUENCE (2 elem)
40          OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
41          PrintableString MIDCHEHF4F4CF4O8
42        SET (1 elem)
43          SEQUENCE (2 elem)
44          OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
45          PrintableString De Luca
46        SET (1 elem)
47          SEQUENCE (2 elem)
48          OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
49          PrintableString Reto
50        SET (1 elem)
51          SEQUENCE (2 elem)
52          OBJECT IDENTIFIER 2.5.4.11 organizationalUnitName (X.520 DN component)
53          PrintableString AIS PROD - Test purposes only
54        SET (1 elem)
55          SEQUENCE (2 elem)
56          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
57          PrintableString Swisscom (Schweiz) AG
58        SET (1 elem)
59          SEQUENCE (2 elem)
60          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
61          PrintableString ch
62      SEQUENCE (2 elem)
63        SEQUENCE (2 elem)
64          OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
65          NULL
66        BIT STRING (1 elem)
67          SEQUENCE (2 elem)
68          INTEGER (2048 bit) 29584954320887071129583109350651659011056121048936237129248301476…
69          INTEGER 65537
70      [3] (1 elem)
71      SEQUENCE (8 elem)
72        SEQUENCE (2 elem)
73          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
74          OCTET STRING (1 elem)
75            SEQUENCE (2 elem)
76              SEQUENCE (2 elem)
77                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
78                [6] http://ocsp.swissdigicert.ch/sdcs-saphir4-eu
79              SEQUENCE (2 elem)
80                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/AIA descriptor)
81                [6] http://aia.swissdigicert.ch/sdcs-saphir4-eu.crt
82        SEQUENCE (2 elem)
83          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
84          OCTET STRING (1 elem)
85            SEQUENCE (1 elem)
86              [0] (20 byte) BA6E95DAB45C25BD9BA6FEFC14D710AE4B989945
87        SEQUENCE (2 elem)
88          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
89          OCTET STRING (1 elem)
90            SEQUENCE (2 elem)
91              SEQUENCE (2 elem)
92                OBJECT IDENTIFIER 2.16.756.1.83.100.4.1 cps (Swisscom Diamant/Saphir CP/CPS)
93                SEQUENCE (1 elem)
94                  SEQUENCE (2 elem)
95                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
96                  IA5String http://www.swissdigicert.ch/cps/
97              SEQUENCE (1 elem)
98                OBJECT IDENTIFIER 0.4.0.2042.1.2 etsiPolicyIdentifier (NCP+)
99        SEQUENCE (2 elem)
100         OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
101         OCTET STRING (1 elem)
102           SEQUENCE (2 elem)
103             SEQUENCE (1 elem)
104               [0] (1 elem)
105               [0] (1 elem)
106               [6] http://crl.swissdigicert.ch/sdcs-saphir4-eu.crl
107             SEQUENCE (1 elem)
108               [0] (1 elem)
109               [0] (1 elem)
```

```
110           [6] ldap://ldap.swissdigicert.ch/CN=Swisscom%20Saphir%20EU%20CA%204,dc=saphir4-…
111     SEQUENCE (3 elem)
112       OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
113       BOOLEAN true
114       OCTET STRING (1 elem)
115         BIT STRING (2 bit) 11
116     SEQUENCE (2 elem)
117       OBJECT IDENTIFIER 2.5.29.17 subjectAltName (X.509 extension)
118       OCTET STRING (1 elem)
119         SEQUENCE (1 elem)
120         [4] (1 elem)
121           SEQUENCE (4 elem)
122             SET (1 elem)
123               SEQUENCE (2 elem)
124                 OBJECT IDENTIFIER 2.5.4.13 description (X.520 DN component)
125                 UTF8String S3-Monitor AIS PROD eIDAS ADV-N - bitte bestätigen, please confirm
126             SET (1 elem)
127               SEQUENCE (2 elem)
128                 OBJECT IDENTIFIER 2.5.4.65 pseudonym (X.520 DN component)
129                 UTF8String MIDCHEHF4F4CF4O8
130             SET (1 elem)
131               SEQUENCE (2 elem)
132                 OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
133                 PrintableString ID-9acb1a56-dc19-445f-a8bb-f458528d52c3
134             SET (1 elem)
135               SEQUENCE (2 elem)
136                 OBJECT IDENTIFIER 2.5.4.41 name (X.520 DN component)
137                 UTF8String N/A
138     SEQUENCE (2 elem)
139       OBJECT IDENTIFIER 2.5.29.18 issuerAltName (X.509 extension)
140       OCTET STRING (1 elem)
141         SEQUENCE (1 elem)
142         [4] (1 elem)
143           SEQUENCE (2 elem)
144             SET (1 elem)
145               SEQUENCE (2 elem)
146                 OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
147                 PrintableString WVDVgAoKeB8AAB4jW7sAAAD
148             SET (1 elem)
149               SEQUENCE (2 elem)
150                 OBJECT IDENTIFIER 2.5.4.13 description (X.520 DN component)
151                 UTF8String s3-monitor
152     SEQUENCE (2 elem)
153       OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
154       OCTET STRING (1 elem)
155         OCTET STRING (20 byte) F1EEBC296839DB51EB4D23EEDDAF00BCB616A3A4
156   SEQUENCE (2 elem)
157     OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
158     NULL
159   BIT STRING (2048 bit) 10011001010101111010001010100110100110110100101010101010000011100111 0…
```