



Zertifikatsprofil Qualified.ID

Deutsche Telekom Security GmbH
Telekom Security

öffentlich

Version: 4.0

Gültig ab: 30.03.2025

Status: freigegeben

Letztes Review Datum: 27.03.2025

Mit Veröffentlichung dieses Dokumentes verlieren alle bisherigen Versionen ihre Gültigkeit!

IMPRESSUM

Tabelle 1 Impressum

| | |
|--------------------|--------------------------------|
| Herausgeber | Deutsche Telekom Security GmbH |
|--------------------|--------------------------------|

| Version | Letztes Review | Status |
|----------------|-----------------------|---------------|
| 4.0 | 27.03.2025 | freigegeben |

Copyright © 2025 by Deutsche Telekom Security GmbH,

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Einleitung | 4 |
| 2 | Zertifikats Infrastruktur | 5 |
| 3 | Zertifikats- und Sperrlistenprofile der Zertifikatsinfrastruktur | 6 |
| 3.1 | Wurzel-Zertifikat..... | 6 |
| 3.2 | CA Zertifikate..... | 7 |
| 3.3 | Root OCSP Signer Zertifikat | 8 |
| 3.4 | Sperrliste | 9 |
| 3.5 | EE OCSP Signaturzertifikate | 9 |
| 4 | Profil der Benutzerzertifikate | 11 |
| 4.1 | Qualifizierte Signaturzertifikate | 11 |
| 4.2 | Qualifizierte Siegelzertifikate..... | 12 |
| 4.3 | Beschreibung der Felder..... | 14 |
| 4.3.1 | Das Feld SerialNumber..... | 14 |
| 4.3.2 | Das Feld Signaturalgorithmus..... | 14 |
| 4.3.3 | Das Feld Aussteller..... | 15 |
| 4.3.4 | Das Feld Gültigkeitszeitraum | 15 |
| 4.3.5 | Das Feld Inhaber | 15 |
| 4.3.6 | Das Feld Öffentlicher Schlüssel | 16 |
| 4.3.7 | Das Feld Signatur | 17 |
| 4.3.8 | Das Feld Zertifikatserweiterungen..... | 17 |
| 4.3.9 | Die Extension SubjectAltNames (optional)..... | 17 |
| 4.3.10 | Die Extension Procuration (optional)..... | 17 |
| 4.3.11 | Die Extension Admission (optional)..... | 18 |
| 4.3.12 | Die Extension Restriction (optional) | 19 |
| 4.3.13 | Die Extension AdditionalInformation (optional)..... | 19 |
| A | Verwendete Attributtypen | 20 |
| B | Abkürzungsverzeichnis..... | 21 |
| C | Literaturverzeichnis..... | 22 |

1 EINLEITUNG

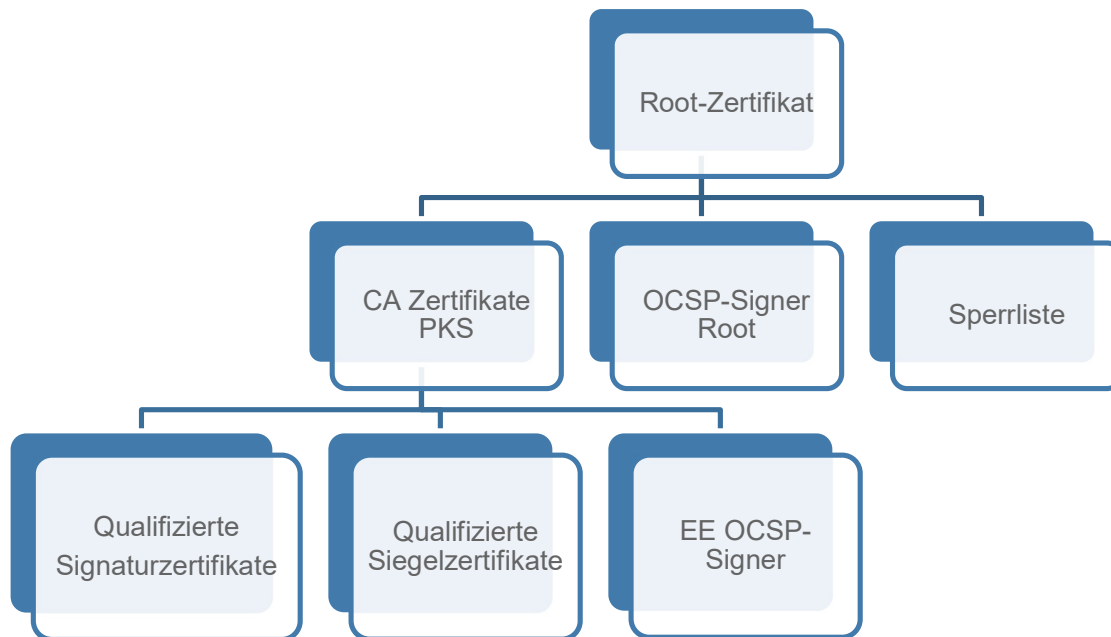
Die qualifizierten Signaturzertifikate des Dienstes Public Key Service / Qualified.ID gemäß eIDAS Verordnung sind konform zur Spezifikation ETSI EN 319 412-2 [ETSI2]. Qualifizierte Siegelzertifikate entsprechen den Anforderungen von ETSI EN 319 412-3 [ETSI3]. Dadurch ist eine Interoperabilität und gegenseitige Anerkennung der Zertifikate innerhalb der Europäischen Union gegeben.

Zertifikatserweiterungen zur Definition zusätzlicher Attribute werden gemäß der COMMON-PKI Spezifikation [COMMON-PKI] in die Zertifikate eingetragen. COMMON-PKI wurde spezifiziert durch den TeleTrust Verein, um eine Interoperabilität von Zertifikatserweiterungen sicher zu stellen.

Dieses Dokument beschreibt den Aufbau der Zertifikatsinfrastruktur und der qualifizierten Signaturzertifikate. Die in dem jeweiligen Zertifikattyp enthaltenen Daten werden ausgehend von der jeweils grundlegenden Struktur gemäß X.509 [X509] erläutert. Dabei werden die Felder und mögliche Inhalte, sowie die zu verwendenden Datentypen festgelegt.

2 ZERTIFIKATS INFRASTRUKTUR

Die Zertifikats Infrastruktur besteht aus einem Wurzel-Zertifikat, ggf. mehreren Zwischenzertifikaten und den Endbenutzer Zertifikaten sowie Sperrliste und OCSP Responder. Das Nachfolgende Schaubild zeigt die für den Qualified.ID verwendete Infrastruktur.



3 ZERTIFIKATS- UND SPERRLISTENPROFILE DER ZERTIFIKATSINFRASTRUKTUR

3.1 Wurzel-Zertifikat

Das Root Zertifikat, oder Wurzel-Zertifikat, ist das oberste Zertifikat in der Zertifikats Infrastruktur. Auf dieses Zertifikat lassen sich alle anderen Zertifikate zurückführen.

| Feld | Wert | |
|--------------------------|---|---|
| Version | 3 | |
| Seriennummer | 11 79 a2 c4 70 e1 21 c3 | |
| Signaturalgorithmus | ecdsa-with-SHA512 (1.2.840.10045.4.3.4) | |
| Aussteller | CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE | |
| Gültigkeitszeitraum | notBefore | 5. April 2017 09:30:31 |
| | notAfter | 5. April 2047 23:59:59 |
| Inhaber | CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE | |
| Öffentlicher Schlüssel | AlgorithmIdentifier | ecPublicKey (1.2.840.10045.2.1) |
| | Parameter | Secp521r1 (1.3.132.0.35) |
| | Wert | 04 00 15 aa 45 8a 35 b7 55 9f 01 09 76 a9 8a 13 f5 7c 15 22 56 15 ff e9 13 bd b0 a3 35 a6 7c e1 b3 fd 70 e0 eb e8 73 fa 50 92 6e 60 cb c8 6a 1f ab f3 5a 7a 83 59 b5 29 90 4c a0 67 11 5b ef a2 7a 44 16 00 9d 10 35 95 d9 09 87 1b c6 c1 68 94 fc a2 fd 64 0a c6 a9 7f d5 0a 0a 53 6e 2c 22 0d 00 3e 28 cf 45 42 9e 12 a4 c0 1a 94 e6 78 70 bc f5 6c 00 52 62 71 f3 73 92 90 c4 e4 ae cd cb 86 a5 6a ea c3 e3 |
| Zertifikatserweiterungen | SubjectKeyIdentifier | 25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f |
| | KeyUsage | kritisch crlSign + keyCertSign |
| | BasicConstraints | Kritisch Ist eine Zertifizierungsstelle Maximale Anzahl an Zwischen-Zertifizierungsstellen: uneingeschränkt |
| | AuthorityKeyIdentifier | 25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f |
| Signatur | AlgorithmIdentifier | ecdsa-with-SHA512 (1.2.840.10045.4.3.4) |

| | | |
|----------------------|--|--------------------------|
| | Signature | <Bitstring der Signatur> |
| Fingerprint (SHA256) | 2f 82 33 68 9c 6e 9a 75 e2 db 3b 5c 0d 04 ab 12 4d c6 54 9f e9 ce 4c d4 8a 7c a9 ca dc 84 a5 f7 | |

3.2 CA Zertifikate

Die CA Zertifikate, oder Zwischenzertifikate, stellen die Benutzerzertifikate aus. Diese Zertifikate sind in der Trusted List der EU als vertrauenswürdige Zertifikate eingetragen.

Es kommen mehrere Zertifikate parallel zum Einsatz.

| Feld | Wert | |
|--------------------------|---|--|
| Version | 3 | |
| Seriennummer | Zertifikatsseriennummer | |
| Signaturalgorithmus | ecdsa-with-SHA512 (1.2.840.10045.4.3.4) | |
| Aussteller | CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE | |
| Gültigkeitszeitraum | notBefore | Beginndatum |
| | notAfter | Ablaufdatum |
| Inhaber | CN = <Name des CA Zertifikats> organizationIdentifier OID (2.5.4.97) = <ID des VDA> O = Deutsche Telekom AG C = DE | |
| Öffentlicher Schlüssel | AlgorithmIdentifier | ecPublicKey (1.2.840.10045.2.1) oder rsaEncryption (1.2.840.113549.1.1.1) |
| | Parameter | brainpoolP256r1 (1.3.36.3.3.2.8.1.1.7) oder prime256v1 (1.2.840.10045.3.1.7) oder NULL |
| | Wert | <Schlüsseldaten> |
| Zertifikatserweiterungen | SubjectKeyIdentifier | SHA1 Hashwert des öffentlichen Schlüssels |
| | AuthorityKeyIdentifier | 25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f |
| | KeyUsage | kritisch crlSign + keyCertSign |

| | | |
|----------|----------------------|---|
| | BasicConstraints | Kritisch Ist eine Zertifizierungsstelle Maximale Anzahl an Zwischen-Zertifizierungsstellen: uneingeschränkt |
| | Policy | OID zu QCP-n-qscd oder QCP-l-qscd Optional: CPS URI: http://pks.telesec.de/cps |
| | CRLDistributionPoint | http://tqrc1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl |
| | AuthorityInfoAccess | (1) OCSP: URI: http://tqrc1.ocsp.telesec.de/ocsp (2) CA-Aussteller: URI: http://tqrc1.pki.telesec.de/crt/TeleSec_qualified_Root_CA_1.crt |
| Signatur | AlgorithmIdentifier | ecdsa-with-SHA512 (1.2.840.10045.4.3.4) |
| | Signature | <Bitstring der Signatur> |

3.3 Root OCSP Signer Zertifikat

Dieses OCSP Signaturzertifikat signiert Statusanfragen zu Zertifikaten welche vom Wurzel-Zertifikat ausgestellt wurden. Dieses Zertifikat wird regelmäßig getauscht und ist deswegen hier ohne konkreten Zertifikatsinhalt in den Feldern Seriennummer, Gültigkeitszeitraum und öffentlicher Schlüssel angegeben.

| Feld | Wert | |
|--------------------------|---|---|
| Version | 3 | |
| Seriennummer | < 126 Bit langer Zufallswert > | |
| Signaturalgorithmus | ecdsa-with-SHA256 (1.2.840.10045.4.3.2) | |
| Aussteller | CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE | |
| Gültigkeitszeitraum | notBefore | < Produktionszeitpunkt > |
| | notAfter | < notBefore + 3 Monate > |
| Inhaber | CN = <Name des OCSP Zertifikats> organizationIdentifier OID (2.5.4.97) = <ID des VDA> O = Deutsche Telekom AG C = DE | |
| Öffentlicher Schlüssel | AlgorithmIdentifier | ecPublicKey (1.2.840.10045.2.1) |
| | Parameter | prime256v1 (1.2.840.10045.3.1.7) |
| | Wert | <Schlüsseldaten> |
| Zertifikatserweiterungen | SubjectKeyIdentifier | SHA1 Hashwert des öffentlichen Schlüssels |

| | | |
|----------|------------------------|--|
| | AuthorityKeyIdentifier | 25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f |
| | KeyUsage | kritisch digitalSignature |
| | ExtendedKeyUsage | ocspSigning |
| | OCSPNoCheck | NULL |
| Signatur | AlgorithmIdentifier | ecdsa-with-SHA256 (1.2.840.10045.4.3.2) |
| | Signature | <Bitstring der Signatur> |

3.4 Sperrliste

Die Sperrliste enthält Sperrinformationen zu Zertifikaten, welche vom Wurzel-Zertifikat ausgestellt wurden. Die Sperrliste enthält die folgenden Inhalte:

| Feld | Wert | |
|-----------------------|---|--|
| Version | 2 | |
| Signaturalgorithmus | ecdsa-with-SHA256 (1.2.840.10045.4.3.2) | |
| Aussteller | CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE | |
| Ausstelldatum | <Generierungsdatum der Sperrliste> | |
| Nächstes Update | <Ausstelldatum plus 6 Monate> | |
| Gesperrte Zertifikate | Dieses Feld enthält die Liste der gesperrten Zertifikate. Wenn keine gesperrten Zertifikate vorhanden sind, ist das Feld nicht vorhanden. | |
| Erweiterungen | Laufende Nummer | <laufende Nummer der Sperrliste> |
| | authorityKeyIdentifier | 25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f |
| Signatur | <BitString der Signatur> | |

Die Sperrliste ist abrufbar von der URL

http://tqrc1.pki.telesec.de/ri/TeleSec_qualified_Root_CA_1.crl

3.5 EE OCSP Signaturzertifikate

Diese Zertifikate signieren Statusanfragen zu Benutzerzertifikaten. Zur Lastverteilung sind immer mehrere OCSP-Signaturzertifikate in Betrieb. Diese Zertifikate werden regelmäßig ausgetauscht.

| Feld | Wert |
|--------------|------------------------------|
| Version | 3 |
| Seriennummer | <126 Bit langer Zufallswert> |

| | | |
|--------------------------|---|---|
| Signaturalgorithmus | ecdsa-with-SHA256 (1.2.840.10045.4.3.2) | |
| Aussteller | CN = <Name des CA Zertifikats> organizationIdentifier OID (2.5.4.97) = <ID des VDA> O = Deutsche Telekom AG C = DE | |
| Gültigkeitszeitraum | notBefore | < Produktionszeitpunkt > |
| | notAfter | < notBefore + 6 Monate> |
| Inhaber | CN = <Name des OCSP Zertifikats> organizationIdentifier OID (2.5.4.97) = <ID des VDA> O = Deutsche Telekom AG C = DE | |
| Öffentlicher Schlüssel | AlgorithmIdentifier | ecPublicKey (1.2.840.10045.2.1) |
| | Parameter | prime256v1 (1.2.840.10045.3.1.7) |
| | Wert | <Schlüsseldaten> |
| Zertifikatserweiterungen | SubjectKeyIdentifier | SHA1 Hashwert des öffentlichen Schlüssels |
| | AuthorityKeyIdentifier | Keyidentifizier des Ausstellerzertifikats |
| | KeyUsage | kritisch digitalSignatur |
| | ExtendedKeyUsage | ocspSigning |
| | OCSP No Check | NULL |
| Signatur | AlgorithmIdentifier | ecdsa-with-SHA256 (1.2.840.10045.4.3.2) |
| | Signature | <Bitstring der Signatur> |

4 PROFIL DER BENUTZERZERTIFIKATE

Die folgende Tabelle zeigt alle möglichen Felder innerhalb des Zertifikates, die von TeleSec genutzt werden. Felder und Zertifikatserweiterungen (Extensions), die personalisierten Inhalt enthalten, werden in den nachfolgenden Kapiteln erläutert.

4.1 Qualifizierte Signaturzertifikate

Qualifizierte Signaturzertifikate werden für natürliche Personen ausgestellt. Folgende Inhalte werden verwendet.

| Feld | Wert | |
|------------------------|---|--|
| Version | 3 | |
| Seriennummer | <126 Bit langer Zufallswert> | |
| Signaturalgorithmus | ecdsa-with-SHA256 (1.2.840.10045.4.3.2) | |
| Aussteller | CN = <Name des CA Zertifikats> organizationIdentifier OID (2.5.4.97) = <ID des VDA> O = Deutsche Telekom AG C = DE | |
| Gültigkeitszeitraum | notBefore | < Produktionszeitpunkt > |
| | notAfter | < je nach Beauftragung > |
| Inhaber | Pflichtfelder: CN: C: SerialNumber: Optional: SN: GN: O: OU: Pseudonym: | |
| Öffentlicher Schlüssel | Algorithm Identifier | ecPublicKey (1.2.840.10045.2.1) oder rsaEncryption (1.2.840.113549.1.1.1) |
| | Parameter | brainpoolP256r1 (1.3.36.3.3.2.8.1.1.7) oder prime256v1 (1.2.840.10045.3.1.7) oder |

| | | |
|------------------------------|--|--|
| | | NULL |
| | Wert | <Schlüsseldaten> |
| Zertifikatserweiterungen | SubjectKeyIdentifier | SHA1 Hashwert des öffentlichen Schlüssels |
| | AuthorityKeyIdentifier | Keyidentifer des Ausstellerzertifikats |
| | KeyUsage | kritisch contentCommitment |
| | Basic Constraints | Kritisch Ist keine Zertifizierungsstelle |
| | Policy | QCP-n-qscd (0.4.0.194112.1.2) CPS URI: http://pks.telesec.de/cps |
| | QCStatement | <pre>SEQUENCE { OBJECT IDENTIFIER qcStatements (1.3.6.1.5.5.7.1.3) (PKIX private extension) OCTET STRING, encapsulates { SEQUENCE { SEQUENCE { OBJECT IDENTIFIER qcs-QcCompliance(0.4.0.1862.1.1) } SEQUENCE { OBJECT IDENTIFIER qcs-QcSSCD(0.4.0.1862.1.4) } SEQUENCE { OBJECT IDENTIFIER qcs-QcPDS(0.4.0.1862.1.5) SEQUENCE { SEQUENCE { IA5String 'https://www.telesec.de/signaturkarte/agb' PrintableString 'en' } } } } } }</pre> |
| AuthorityInfo Access | (1) OCSP: URI: http://pks.telesec.de/ocspr (2) CA-Aussteller: URI: <a href="http://tqrc1.pki.telesec.de/crt/TeleSec_PKS_eIDAS_QES_CA_<x>.crt">http://tqrc1.pki.telesec.de/crt/TeleSec_PKS_eIDAS_QES_CA_<x>.crt | |
| Weitere optionale Extensions | SubjectAltNames, Restriction, Admission, Procuration, AdditionalInformation | |
| Signatur | Algorithm Identifier | ecdsa-with-SHA256 (1.2.840.10045.4.3.2) |
| | Signature | <Bitstring der Signatur> |

4.2 Qualifizierte Siegelzertifikate

Qualifizierte Siegelzertifikate werden für juristische Personen ausgestellt. Folgende Inhalte werden verwendet.

| Feld | Wert | |
|--------------------------|---|---|
| Version | 3 | |
| Seriennummer | <126 Bit langer Zufallswert> | |
| Signaturalgorithmus | ecdsa-with-SHA256 (1.2.840.10045.4.3.2) | |
| Aussteller | CN = <Name des CA Zertifikats> organizationIdentifier OID (2.5.4.97) = <ID des VDA> O = Deutsche Telekom AG C = DE | |
| Gültigkeitszeitraum | notBefore | < Produktionszeitpunkt > |
| | notAfter | < je nach Beauftragung > |
| Inhaber | Pflichtfelder: CN: C: O: SerialNumber: OrganizationIdentifier: | |
| Öffentlicher Schlüssel | Algorithm Identifier | ecPublicKey (1.2.840.10045.2.1) oder rsaEncryption (1.2.840.113549.1.1.1) |
| | Parameter | brainpoolP256r1 (1.3.36.3.3.2.8.1.1.7) oder prime256v1 (1.2.840.10045.3.1.7) oder NULL |
| | Wert | <Schlüsseldaten> |
| Zertifikatserweiterungen | SubjectKeyIdentifier | SHA1 Hashwert des öffentlichen Schlüssels |
| | AuthorityKeyIdentifier | Keyidentifer des Ausstellerzertifikats |
| | KeyUsage | kritisch contentCommitment |
| | Basic Constraints | Kritisch Ist keine Zertifizierungsstelle |
| | Policy | QCP-I-qscd (0.4.0.194112.1.3) CPS URI: http://pks.telesec.de/cps |
| | QC Statement | SEQUENCE { OBJECT IDENTIFIER qcStatements (1.3.6.1.5.5.7.1.3) OCTET STRING, encapsulates { SEQUENCE { SEQUENCE { OBJECT IDENTIFIER |

| | | |
|----------|------------------------------|---|
| | | <pre> qcs-QcCompliance (0.4.0.1862.1.1) } SEQUENCE { OBJECT IDENTIFIER qcs-QcSSCD(0.4.0.1862.1.4) } SEQUENCE { OBJECT IDENTIFIER qcs-QcPDS (0.4.0.1862.1.5) SEQUENCE { SEQUENCE { IA5String 'https://www.telesec.de/signaturkarte/agb' PrintableString 'en' } } } SEQUENCE { OBJECT IDENTIFIER qcs-QcType(0.4.0.1862.1.6) SEQUENCE { OBJECT IDENTIFIER qct-eseal(0.4.0.1862.1.6.2) } } } } } </pre> |
| | AuthorityInfo Access | (1) OCSP: URI: http://pks.telesec.de/ocspr (2) CA-Aussteller: URI: <a href="http://tqrca1.pki.telesec.de/crt/TeleSec_PKS_eIDAS_QES_CA_<x>.crt">http://tqrca1.pki.telesec.de/crt/TeleSec_PKS_eIDAS_QES_CA_<x>.crt |
| | Weitere optionale Extensions | SubjectAltNames, Restriction |
| Signatur | Algorithm Identifier | ecdsa-with-SHA256 (1.2.840.10045.4.3.2) |
| | Signature | <Bitstring der Signatur> |

4.3 Beschreibung der Felder

4.3.1 Das Feld SerialNumber

In diesem Feld wird die Zertifikatsnummer abgelegt. Diese ist ein bis zu 126 Bit langer zufallswert.

4.3.2 Das Feld Signaturalgorithmus

Das Feld Signature enthält den Bezeichner des Signaturalgorithmus, der von der CA für die Erstellung des Zertifikates benutzt wird.

Abhängig von der Generation der Benutzerzertifikate werden unterschiedliche Algorithmen benutzt.

- Ecdsa-with-SHA256 {1.2.840.10045.4.3.2}
- RSA-PSS {1.2.840.113549.1.1.10}
- sha256WithRsaEncryption {1.2.840.113549.1.1.11}
- sha1WithRSAEncryption

4.3.3 Das Feld Aussteller

In dem Feld Issuer wird der Name des Herausgebers abgelegt. Der Inhalt dieses Feldes muss exakt mit dem Inhalt des Subject-Feldes des CA-Zertifikates übereinstimmen, von dem das Benutzerzertifikat unterschrieben worden ist.

Folgende Attribute werden verwendet:

- countryName (vorgeschrieben)
- organizationName (vorgeschrieben)
- organizationalUnitName (optional)
- commonName (vorgeschrieben)
- pseudonym (bedingt, muss verwendet werden, wenn sich im commonName ein pseudonym befindet)
- organizationIdentifier (bedingt, muss verwendet werden, wenn sich im commonName dieses Feld befindet. Dieses Feld wird durch die eIDAS Verordnung gefordert, wenn das Zertifikat für eine juristische Person ausgestellt wurde. Dies ist bei den eIDAS konformen CA Zertifikaten der Fall)

Anmerkung:

Der Inhalt des Feldes Issuer wird aus dem Subject-Feld des CA-Zertifikates entnommen, von dem das Zertifikat unterschrieben werden soll.

4.3.4 Das Feld Gültigkeitszeitraum

In diesem Feld wird der Gültigkeitszeitraum des Zertifikates eingetragen. Der Inhalt des Feldes hat folgende Syntax:

```
Validity ::= SEQUENCE
{
    notBefore      Time
    notAfter       Time
}

Time ::= CHOICE
{
    utcTime        UTCTime
    generalizedTime GeneralizedTime
}
```

Die Uhrzeit wird bis zum Jahr 2049 als UTCTime kodiert werden. Ab dem Jahr 2050 wird die Kodierung GeneralizedTime verwendet.

4.3.5 Das Feld Inhaber

Der Name des Zertifikatsinhabers wird in dem Feld Subject gespeichert. Der Name für den Zertifikatsinhaber muss innerhalb der Zertifizierungsstelle für die komplette Lebensdauer der CA eindeutig sein.

Folgende Attribute werden verwendet:

| Attributname | Qualifiziertes Signaturzertifikat | Qualifiziertes Siegelzertifikat |
|------------------|-----------------------------------|---------------------------------|
| countryName | ✓ | ✓ |
| organizationName | ○ | ✓ |

| | | |
|------------------------|-----|---|
| organizationalUnitName | O | O |
| organizationIdentifier | X | ✓ |
| commonName | ✓ | ✓ |
| serialNumber | ✓ | ✓ |
| pseudonym | (1) | X |
| surname | (2) | X |
| givenname | (2) | X |

| | |
|---|--|
| ✓ | Pflichtfeld |
| O | Optional |
| X | Nicht verwendet |
| 1 | Wenn der Zertifikatsinhaber ein Pseudonym als Name wünscht, wird zusätzlich das Attribut Pseudonym kodiert. Der Pseudonym-Name befindet sich immer in den Attributen commonName und pseudonym. Hierbei wird ein Pseudonym mit der Endung „:PN“ gekennzeichnet. |
| 2 | Die Attribute surname/givenname und pseudonym schließen sich gegenseitig aus. Wenn im Zertifikat ein Pseudonym eingetragen ist werden surname/givenname nicht verwendet. Wird kein Pseudonym verwendet so sind die Felder surname und givenname erforderlich. |

Das Feld hat die gleiche Datenstruktur wie das Feld Issuer (siehe Kapitel 4.3).

4.3.6 Das Feld Öffentlicher Schlüssel

Der PublicKey des Zertifikatsinhabers wird in diesem Feld zusammen mit dem Algorithmus für den Gebrauch des Schlüssels gespeichert. Der Inhalt des Feldes hat folgende Syntax:

```
SubjectPublicKeyInfo ::= SEQUENCE
{
    algorithm          AlgorithmIdentifier
    subjectPublicKey   BIT STRING
}
AlgorithmIdentifier ::= SEQUENCE
{
    algorithm          OBJECT IDENTIFIER
    parameters        ANY DEFINED BY algorithm OPTIONAL
}
```

Das Feld parameters kann zusätzliche Parameter des Algorithmus enthalten. Für den verwendeten Algorithmus (RSA) werden sie nicht benötigt, deshalb ist dieses Feld Null (explizit NULL). Für Schlüssel basierend auf elliptischen Kurven wird hier die OID der Kurve eingetragen. Für diesen Zertifizierungsbereich wird die Kurve brainpoolP256r1 (OID { 1.3.36.3.3.2.8.1.1.7}) oder prime256v1 (OID {1.2.840.10045.3.1.7}) verwendet. Die Codierung erfolgt immer als benannte Kurve.

4.3.7 Das Feld Signatur

Dieses Feld enthält die Signatur des Zertifikates, die von der Zertifizierungsstelle erzeugt worden ist.

4.3.8 Das Feld Zertifikatserweiterungen

Die Extensions dienen zur Erweiterung der im Zertifikat enthaltenen Daten. Es gibt mehrere verschiedene Extensions, die in den folgenden Unterkapiteln aufgeführt werden.

Die Extensions haben folgende Syntax:

```
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE
{
    extnId          OBJECT IDENTIFIER
    critical        BOOLEAN DEFAULT FALSE
    extnValue       OCTET STRING
}
```

Der Wert `extnId` gibt mit Hilfe eines Object Identifiers den Typ der in `extnValue` enthaltenen Extension an. Das Flag `critical` zeigt an, ob die Extension als kritisch markiert worden ist. Wenn `critical` auf TRUE gesetzt wird, bedeutet dies, dass der Client das Zertifikat als ungültig betrachten muss, wenn er die Extension nicht auswerten kann.

4.3.8.1 Die Extension SubjectAltNames

Mit Hilfe dieser Extension können alternative Namen für den Zertifikatsinhaber im Zertifikat eingefügt werden.

Diese Extension wird als nicht kritisch markiert.

Die Extension hat folgende Datenstruktur:

```
SubjectAltNames ::= GeneralNames
```

Wenn diese Extension vorhanden ist enthält sie genau eine E-Mail-Adresse des Zertifikatsinhabers als `rfc822Name`.

4.3.8.2 Die Extension Procuration

Diese Extension wird verwendet, wenn der Zertifikatsinhaber für eine andere Person Unterschriften leisten darf.

Diese Extension wird als nicht kritisch markiert.

Die Extension hat den folgenden Aufbau:

```
ProcurationSyntax ::= SEQUENCE
{
    country                [1] EXPLICIT PrintableString OPTIONAL
    typeOfSubstitution     [2] EXPLICIT DirectoryString OPTIONAL
}
```

```

        signingFor          [3] EXPLICIT SigningFor
    }

SigningFor ::= CHOICE
{
    thirdPerson      GeneralName
    certRef          IssuerSerial
}

IssuerSerial ::= SEQUENCE
{
    issuer            GeneralNames
    serial            CertificateSerialNumber
    issuerUID        UniqueIdentifier OPTIONAL
}

```

Es wird das Feld `thirdPerson` in der Sequence `SigningFor` verwendet dieses kann alle Attribute aus Anhang A enthalten.

Die Länge des Feldes `typeOfSubstitution` wird auf eine Länge von 128 Bytes begrenzt.

Diese Extension wird für qualifizierte Siegelzertifikate nicht angeboten.

4.3.8.3 Die Extension Admission

Diese Extension Admission wird verwendet, um Informationen über die Berechtigung bestimmte Aufgaben erledigen zu dürfen in das Zertifikat aufzunehmen.

Diese Extension wird als nicht kritisch markiert.

Die Extension Admission hat die folgende Datenstruktur:

```

AdmissionSyntax ::= SEQUENCE
{
    admissionAuthority      GeneralName OPTIONAL
    contentsOfAdmissions    SEQUENCE OF Admissions
}
Admissions ::= SEQUENCE
{
    admissionAuthority      [0] EXPLICIT GeneralName OPTIONAL
    namingAuthority         [1] EXPLICIT NamingAuthority OPTIONAL
    professionInfos         SEQUENCE OF ProfessionInfos
}

NamingAuthority ::= SEQUENCE
{
    namingAuthorityId       OBJECT IDENTIFIER OPTIONAL
    namingAuthorityUrl      IA5String OPTIONAL
    namingAuthorityText     DirectoryString OPTIONAL
}

ProfessionInfo ::= SEQUENCE
{
    namingAuthority         [0] EXPLICIT NamingAuthority OPTIONAL
    professionItems         SEQUENCE OF DirectoryString
    professionOIDs         SEQUENCE OF OBJECT IDENTIFIER Optional
    registrationNumber     PrintableString OPTIONAL
}

```

```

    addProfessionInfo    OCTET STRING OPTIONAL
}

```

Das Feld `admissionAuthority` wird immer nur an einer Stelle kodiert. Wenn alle vorhandenen Bestätigungen von einer Instanz bestätigt wurden, wird das Feld in der Sequence `AdmissionSyntax` genutzt. Andernfalls muss das Feld in der Sequence `Admissions` verwendet werden. Der Inhalt des Feldes ist ein `DirectoryName`, der sich aus den Attributen aus Anhang A und den zusätzlichen Attributen `OrganizationName` und `OrganizationalUnitName` zusammensetzt.

In dem Feld `namingAuthority` befinden sich Informationen über den Aussteller der Bestätigungen. Wenn alle Bestätigungen von einer Instanz ausgestellt worden sind, wird das entsprechende Feld in der Sequence `Admissions` genutzt. Andernfalls muss das Feld in der Sequence `ProfessionInfos` benutzt werden. Wenn in dem Feld `namingAuthorityText` Informationen vorhanden sind, müssen diese als UTF8-String kodiert werden.

Diese Extension wird für qualifizierte Siegelzertifikate nicht angeboten.

4.3.8.4 Die Extension Restriction

Diese Extension kann für die Aufnahme von Einschränkungen in das Zertifikat aufgenommen werden.

Diese Extension wird als nicht kritisch markiert.

Die Extension Restriction hat die folgende Datenstruktur:

```
RestrictionSyntax ::= DirectoryString
```

Die Länge des Strings ist grundsätzlich auf 1024 Zeichen beschränkt, bedingt durch den verfügbaren Speicherplatz auf der Chipkarte kann die verfügbare Länge aber noch weiter eingeschränkt werden.

4.3.8.5 Die Extension AdditionalInformation

Diese Extension wird für die Integration von Informationen mit nicht einschränkendem Charakter in das Zertifikat verwendet.

Die Extension AdditionalInformation hat die folgende Datenstruktur:

```
AdditionalInformationSyntax ::= DirectoryString
```

Die Länge des Strings ist grundsätzlich auf 2000 Zeichen beschränkt, bedingt durch den verfügbaren Speicherplatz auf der Chipkarte kann die verfügbare Länge aber noch weiter eingeschränkt werden.

Diese Extension wird für qualifizierte Siegelzertifikate nicht angeboten.

A VERWENDETE ATTRIBUTTYPEN

| Name des Attributs | Object Identifier | ASN.1 String Typ | maximale Länge |
|----------------------------|------------------------------|------------------------------|---|
| commonName | {id-at 3} | UTF8 | 64 |
| surName | {id-at 4} | UTF8 | 64 |
| givenName | {id-at 42} | UTF8 | 64 |
| serialNumber | {id-at 5} | PrintableString | 64 |
| organizationIdentifier | {id-at 97} | UTF8 | 64 |
| title | {id-at 12} | UTF8 | 64 |
| organizationName | {id-at 10} | UTF8 | 64 |
| organizationalUnitName | {id-at 11} | UTF8 | 64 |
| BusinessCategory | {id-at 15} | UTF8 | 128 |
| localityName | {id-at 7} | UTF8 | 128 |
| stateOrProvinceName | {id-at 8} | UTF8 | 128 |
| countryName | {id-at 6} | PrintableString | 2 (ISO 3166 Code) |
| distinguishedNameQualifier | {id-at 46} | PrintableString | 64 |
| initials | {id-at 43} | UTF8 | 64 |
| generationQualifier | {id-at 44} | UTF8 | 64 |
| eMailAddress | {pkcs-9 1} | IA5String | 128 |
| domainComponent | {0 9 2342 19200300 100 1 25} | IA5String | definiert in RFC 2247 |
| postalAddress | {id-at 16} | SEQUENCE SIZE (1..6) OF UTF8 | 6 * 30, Verwendung wird in RFC 3039 beschrieben |
| pseudonym | {pkix 9 3} | UTF8 | 64 |
| dateOfBirth | {id-pda 1} | GeneralizedTime | 15 |
| placeOfBirth | {id-pda 2} | UTF8 | 128 |
| gender | {id-pda 3} | PrintableString SIZE (1) | Inhalt: „M“ oder „F“ |
| countryOfCitizenship | {id-pda 4} | PrintableString | 2 (ISO 3166 Code) |
| countryOfResidence | {id-pda 5} | PrintableString | 2 (ISO 3166 Code) |
| nameAtBirth | {id-isismtt-at 14} | UTF8 | 64 |

Für die UTF8-Kodierung wird einen Auszug aus dem UTF8-Zeichensatz verwendet, der nur ANSI / ISO 8859-1 Zeichen (Unicode Latin-1 Seite) enthält. Andere Zeichen, die nicht in diesem Zeichensatz enthalten sind, dürfen nicht benutzt werden.

Besonderheiten für bestimmte Attribute:

- commonName: Ein Pseudonym wird immer mit der Endung „:PN“ als CommonName eingefügt werden. Zusätzlich wird der gleiche Inhalt (einschließlich der Endung) in dem Attribut pseudonym eingefügt.
- postalAddress: Die Adresse wird komplett in diesem Attribut gespeichert. z.B.
 1. Element: Turmstraße 123
 2. Element: 10123 Berlin
 3. Element: Germany.
- DateOfBirth: Das Geburtsdatum wird im GeneralizedTime-Format kodiert. Der Teil mit der Angabe der Uhrzeit wird mit „0“ gefüllt (z.B. 19720508000000Z).

B ABKÜRZUNGSVERZEICHNIS

| | |
|------|---|
| CA | Certification Authority |
| ECC | Elliptic Curve Cryptography ist ein asymmetrisches kryptographisches Verfahren |
| HTTP | Hypertext Transmission Protocol |
| LDAP | Lightweight Directory Access Protocol |
| OCSP | Online Certificate Status Protocol |
| PN | Pseudonym |
| RSA | RSA (Rivest, Shamir und Adleman) ist ein asymmetrisches kryptographisches Verfahren |

C LITERATURVERZEICHNIS

| | |
|--------------|---|
| [ETSI2] | ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons. |
| [ETSI2] | ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons |
| [COMMON-PKI] | Common-PKI COMMON PKI SPECIFICATIONS FOR INTEROPERABLE APPLICATIONS VERSION 2.0 – 20 JANUARY 2009 |
| [X509] | Recommendation X.509: The Directory – Authentication Frame |