BAKOM
OFCOM
UFCOM
UFCOM

SR xxx.xxx.xxx / x.xx

Technische und administrative Vorschriften über

Zertifizierungsdienste im Bereich der elektronischen Signatur

Ausgabe 1: xx.xx.xxxx *[Entwurf vom 1.6.04]*

Inkrafttreten: xx.xx.xxxx

BAKOM Bundesamt für Kommunikation
OFCOM Office fédéral de la communication
UFCOM Ufficio federale delle communicazioni
UFCOM Uffizi federal da communicaziuns

Zukunftstrasse 44 / Rue de l'Avenir 44
Postfach / Case postale
CH-2501 Biel/Bienne
www.bakom.ch / www.ofcom.ch

Inhaltsverzeichnis

1 Allgemeines

1.1 Geltungsbereich

Diese technischen und administrativen Vorschriften stützen sich auf:

- das Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) [1],
- die Verordnung vom xxxxxxxx über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES) [2].

Soweit als nötig und zulässig präzisieren sie die in Gesetz und Verordnung definierten Voraussetzungen und grundlegenden Anforderungen, die eine Anbieterin von Zertifizierungsdiensten (CSP), die qualifizierte elektronische Zertifikate ausstellt oder andere Dienste im Bereich der elektronischen Signaturen bereitstellt, erfüllen muss, um anerkannt zu werden.

Das Prinzip der Anerkennung ist in Kapitel 2 beschrieben.

Ein grosser Teil dieses Dokumentes stützt sich auf die Grundsätze und Verfahren, die in den in Kapitel 1.2 referenzierten internationalen Normen beschrieben sind.

1.2 Referenzen

[1] SR XXXXXX, ZertES
Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur

[2] xxx.xxx, VZertES
Verordnung vom xxxxxxxx über Zertifizierungsdienste im Bereich der elektronischen Signatur

[3] SR 946.51, THG
Bundesgesetz vom 6. Oktober 1995 über die technischen Handelshemmnisse

[4] SR 946.512, AkkBV:
Verordnung vom 17. Juni 1996 über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen (Akkreditierungs- und Bezeichnungsverordnung, AkkBV)

[5] Richtlinie 1999/93/EG des europäischen Parlamentes und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

[[6] ETSI TS 101 456 v1.2.1 (2002-04)
Policy requirements for certification authorities issuing qualified certificates

[7] TTP.NL Guidance on ETSI TS 101 456 (30. Mai 2002)

[8] CWA 14167-1 (November 2001)
Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part1: System Security Requirements

[9] ITU-T Recommendation X.509 (2000)– ISO 9594-8:2001 (4. Ausgabe)
Information technology – Open systems interconnection – The Directory : Public key and attribute certificate frameworks

[10] RFC 3280 (April 2002)
Internet X.509 Public Key Infrastructure - Certificate and CRL Profile

[11] RFC 3739 (März 2004)
Internet X.509 Public Key Infrastructure - Qualified Certificates Profile

[[12] ETSI 102 023 v1.1.1 (2002-04)
Policy requirements for time-stamping authorities

[13] ISO/IEC 15408 :1999
Information technology – Security techniques. Evaluation criteria for IT security

[14] ETSI TS 101 862, v1.3.1 (2004-03)
Qualified Certificate Profile

Die Empfehlungen der ITU-T können bei der Internationalen Fernmeldeunion, Place des Nations, 1211 Genf 20 bezogen werden (www.itu.int).

Die ISO-Normen sind beim Zentralsekretariat der Internationalen Organisation für Normung, 1, rue de Varembé, 1211 Genf erhältlich (www.iso.ch).

Die ETSI-Normen sind beim Europäischen Institut für Telekommunikationsnormen, 650 route des Lucioles, 06921 Sophia Antipolis, Frankreich erhältlich (www.etsi.org).

Die CEN-Dokumente sind beim Europäischen Komitee für Normung, 36 rue de Stassart, B - 1050 Brüssel, Belgien erhältlich (http://www.cenorm.be).

Die Gesetzestexte mit einer SR-Referenz sind in der Systematischen Rechtssammlung der Bundesgesetze publiziert, die auf der Website www.bk.admin.ch konsultiert werden kann, und können bei der Eidg. Drucksachen- und Materialzentrale (EDMZ), CH-3003 Bern bezogen werden.

Die Technischen und administrativen Vorschriften sind beim BAKOM, Zukunftstrasse 44, Postfach, 2501 Biel erhältlich (www.bakom.ch).

1.3 Abkürzungen

AkkBV	Akkreditierungs- und Bezeichnungsverordnung [4]
BAKOM	Bundesamt für Kommunikation
CB	*Certification Body* – Anerkennungsstelle
CEN	*Comité européen de normalisation* – Europäisches Komitee für Normung
CP	*Certification policy* – Zertifizierungspolitik
CPS	*Certification pratice statement* – Aussage der Zertifizierungspraxis
CRL	*Certificate Revocation List* – Liste der für ungültig erklärten Zertifikate
CSP	*Certification Service Provider* – Anbieterin von Zertifizierungsdiensten
CWA	*CEN Workshop Agreement* – CEN-Workshop-Vereinbarung
EA	Europäische Akkreditierung
EESSI	*European Electronic Signature Standardisation Initiative* – Europäische Initiative für die Standardisierung der elektronischen Signatur
ETSI	*European Telecommunications Standards Institute* – Europäisches Institut für Telekommunikationsnormen
IETF	*Internet Engineering Task Force*

ISO	*International Standardization Organization* – Internationale Organisation für Normung
ITU-T	*International Telecommunication Union. Telecommunication Standardization Sector* - Internationale Fernmeldeunion. Sektor für Telekommunikationsstandardisierung.
metas	Bundesamt für Metrologie und Akkreditierung
OID	*Object identifier* – Objektbezeichner
QC	*Qualified Certificate* – qualifiziertes Zertifikat
RFC	*Request for Comments*
SAS	Schweizerische Akkreditierungsstelle
SR	Systematische Rechtssammlung
SSCD	*Secure-signature-creation device* – sichere Signaturerstellungseinheit
THG	Bundesgesetz über die technischen Handelshemmnisse [3]
TS	*Technical specification* – technische Spezifikation
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur [2]
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur [1]

1.4 Definitionen

In diesen technischen und administrativen Vorschriften bedeuten:

Anbieterin von Zertifizierungsdiensten (CSP): Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt;

Anerkennungsstelle: Stelle, die nach dem Akkreditierungsrecht für die Anerkennung und die Überwachung der Anbieterinnen von Zertifizierungsdiensten akkreditiert ist;

Aussage der Zertifizierungspraxis (CPS): Aussage über die Zertifizierungspraxis, die von der CSP für die Ausstellung von Zertifikaten effektiv umgesetzt wird. Die CSP definiert die Ausrüstungen, die Politik und die Verfahren, die von der CSP in Übereinstimmung mit der von ihr gewählten Zertifizierungspolitik verwendet werden;

Benutzer des Zertifikats : Person, die in ihrem Handeln den überprüften elektronischen Signaturen vertraut, indem sie dieses Zertifikats verwendet.

Digitales Zertifikat: elektronische Bescheinigung, die einen Signaturprüfschlüssel mit dem Namen einer Person verknüpft. Im vorliegenden Dokument ist der Terminus „Zertifikat“ als „qualifiziertes Zertifikat“ zu verstehen.

Elektronische Signatur oder **Signatur**: Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dieser Daten dienen;

Generierung der Zertifikate: Dienst der CSP; Erzeugung eines digitalen Zertifikats auf der Grundlage des Namens der Antragstellerin des Zertifikats und ihrer allfälligen Attribute, die bei der Registrierung überprüft werden;

Inhaber des Zertifikats: Inhaber des Signaturschlüssels, welcher dem im Zertifikat aufgeführten Signaturprüfschlüssel zugeordnet ist;

Liste der für ungültig erklärten Zertifikate (CRL): Liste, die alle Seriennummern der Zertifikate enthält, die vor Ablauf des Gültigkeitsdatums für ungültig erklärt wurden;

Qualifizierte elektronische Signatur: elektronische Signatur, die folgende Anforderungen erfüllt:

1. Sie ist ausschliesslich dem Inhaber zugeordnet.
2. Sie ermöglicht die Identifizierung des Inhabers.
3. Sie wird mit Mitteln erzeugt, welche der Inhaber unter seiner alleinigen Kontrolle halten kann.
4. Sie wird durch eine sichere Signaturerstellungseinheit nach Artikel 6 Absatz 1 und 2 ZertES erzeugt.
5. Sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.
6. Sie beruht auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat.

Qualifiziertes Zertifikat: digitales Zertifikat, das die Anforderungen von Artikel 7 ZertES erfüllt;

Registrierung: Dienst der CSP, der darin besteht, die Identität und wenn nötig die Attribute jeder Antragstellerin eines Zertifikats zu überprüfen, bevor ihr Zertifikat erzeugt oder der Aktivierungscode (oder das Passwort) zur Aktivierung der Nutzung des Signaturschlüssels zugewiesen wird;

Schlüsselpaar: Signaturschlüssel und dazugehörender Signaturprüfschlüssel, die mathematisch auf Grund eines Signaturalgorithmus miteinander verknüpft sind;

Sichere Signaturerstellungseinheit: Einheit nach Artikel 6 Absatz 2 ZertES, die für die Implementierung des Signaturschlüssels konfiguriert ist, den der Inhaber des Zertifikats zur Erstellung einer elektronischen Signatur verwendet;

Sicherheitspolitik (SP): Gesamtheit von Regeln und Richtlinien, die auf Grund einer Risikoanalyse zur Reduzierung der Wahrscheinlichkeit von möglichen Zwischenfällen (vorbeugende Massnahmen) und zur Behebung der Auswirkungen solcher Zwischenfälle (Korrekturmassnahmen) ausgearbeitet wurden, um die für die Anbieterin von Diensten der elektronischen Zertifizierung als schützenswert identifizierten Ressourcen zu schützen. Die Spezifikationen einer Sicherheitsstrategie und -politik erlauben, die gesamthaft zu erreichende Sicherheitsstufe für ein Informationssystem und besonders für jedes Element der Sicherheitsarchitektur eindeutig zu definieren;

Signaturprüfschlüssel: Daten wie Codes oder öffentliche kryptografische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;

Signaturschlüssel: einmalige Daten wie Codes oder private kryptografische Schlüssel, die vom Inhaber zur Erstellung einer elektronischen Signatur verwendet werden;

Ungültigerklärung des Zertifikats: Dienst der Anbieterin von Zertifizierungsdiensten, der die Gültigkeit eines Zertifikats vor dessen Ablauf aufhebt;

Verteilung der Zertifikate: Dienst der Anbieterin von Zertifizierungsdiensten, der das Zertifikat, nachdem es generiert wurde, seinem Inhaber und bei Einwilligung des Zertifikatinhabers den Benutzern des Zertifikats zur Verfügung stellt;

Verwaltung des Zertifikatstatus: Dienst der Anbieterin von Zertifizierungsdiensten, anhand dessen die Benutzer von einem Zertifikat überprüfen können, ob dieses für ungültig erklärt worden ist.

Zeitstempel: Dienst der Anbieterin von Zertifizierungsdiensten, der eine mit dem Datum, der Uhrzeit und der qualifizierten Signatur der CSP versehene Bescheinigung abgibt, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorliegen;

Zertifizierungspolitik (CP): Regeln, welche die Anwendbarkeit eines Zertifikats für eine Gesamtheit von Personen und/oder eine Klasse spezieller Anwendungen mit gemeinsamen Sicherheitsanforderungen vorschreiben;

2 Prinzip der Anerkennung der CSP

Die Anerkennung der CSP erfolgt durch eine im Rahmen des Schweizerischen Akkreditierungssystems akkreditierten Anerkennungsstelle (CB). Dieses System basiert auf dem THG [3] und der AkkBV [4] (Art. 2 Bst. g und Art. 3 Abs. 2).

Um sich zum Zweck der Anerkennung der Anbieterinnen von Zertifizierungsdiensten zu akkreditieren, müssen die Anerkennungsstellen die Kriterien der europäischen Norm EN 45012 erfüllen. Die Anerkennung der Anbieterinnen von Zertifizierungsdiensten setzt mindestens eine akkreditierte Anerkennungsstelle voraus. Falls keine solche Stelle besteht, anerkennt die Schweizerische Akkreditierungsstelle (SAS) die Anbieterinnen von Zertifizierungsdiensten selbst.

Die Liste der akkreditierten Anerkennungsstellen und die Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten sind auf der SAS-Website einsehbar (www.sas.ch/).

3 Grundlegende Anforderungen

3.1 Grundsatz

Zur Förderung der Interoperabilität und der internationalen Harmonisierung gemäss Artikel 20 Absatz 1 ZertES [1] basieren die vorliegenden technischen und administrativen Vorschriften auf den Spezifikationen und Normen der EESSI (European European Electronic Signature Standardization Initiative), die ihre Grundlage in der europäischen Richtlinie 1999/93/EG [5] haben.

Die Technischen und administrativen Vorschriften beziehen sich insbesondere auf die Spezifikation ETSI TS 101 456 [6], *Policy requirements for certification authorities issuing qualified certificate,* für welche eine Anleitung, die für die Beurteilung der Konformität nützlich ist, unter der Bezeichnung *TTP.NL Guidance on ETSI TS 101 456* [7] existiert.

3.2 Umgebung und Verwaltung des Betriebs

3.2.1 Organisation

a) Die Organisation der CSP muss der Spezifikation ETSI TS 101 456 [6], Kapitel 7.5, *Organizational,* entsprechen*.*

b) Die CSP muss jedes Jahr interne Audits durchführen, um die Konformität mit folgenden Dokumenten zu überprüfen:

- ZertES [1], VZertES [2] sowie diese technischen und administrativen Vorschriften
- Zertifizierungspolitik (CP)
- Aussage der Zertifizierungspraxis (CPS)

3.2.2 Verwaltung der Politik

Die CSP muss ihre Politik in Übereinstimmung mit folgenden Referenzen verwalten:

Zertifizierungspolitik (CP)	ETSI TS 101 456 [6], Kapitel 6.1, *Certification authority obligations*; 8.1, *Qualified certificate policy management*
Aussage der Zertifizierungspraxis (CPS)	ETSI TS 101 456 [6], Kapitel 6.1, *Certification authority obligations*; 7.1, *Certification pratice statement*
Sicherheitspolitik	ETSI TS 101 456 [6], 7.4.1, *Security Management*

3.2.3 Verwaltung der Sicherheit

Die Politik und die Praxis der CSP in Bezug auf die Verwaltung der Sicherheit müssen mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.1, *Security management,* konform sein.

3.2.4 Klassifizierung und Verwaltung der Aktiven

Die Politik und die Praxis der CSP in Bezug auf die Klassifizierung und die Verwaltung von Aktiven müssen mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.2, *Asset classification and management,* konform sein.

3.2.5 Sicherheit des Personals

Die Umsetzung der Politik und der Praxis in Bezug auf die Sicherheit des Personals muss mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.3, *Personnel security,* konform sein.

3.2.6 Physische Sicherheit

Die Politik und die Praxis der CSP in Bezug auf die physische Sicherheit müssen mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.4, *Physical and environmental security,* konform sein.

3.2.7 Verwaltung des Betriebs

Die CSP muss eine Praxis pflegen, die mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.5, *Operations management,* konform ist, um einen korrekten und sicheren Betrieb ihrer Systeme sicherzustellen.

3.2.8 Zugang zu den Systemen und Informationen

Die Politik und die Praxis der CSP in Bezug auf die Verwaltung des Zugangs zu ihren Systemen und Informationen müssen mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.6, *System access management,* konform sein.

3.2.9 Systeme

a) Die CSP muss Systeme und Produkte einsetzen, die mit dem Dokument CWA 14167-1 [8] oder einem gemäss der Norm ISO/IEC 15408:1999 [13] definierten Schutzprofil konform sind.

b) Die Politik und die Praxis in Bezug auf die Einsetzung und die Wartung der Systeme und Produkte muss mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.7, *Trustworthy systems deployment and maintenance,* konform sein.

3.2.10 Betriebskontinuität

Die Politik und die Praxis der CSP in Bezug auf die Verwaltung der Betriebskontinuität müssen mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.8, *Business continuity management,* konform sein.

3.2.11 Einstellung der Geschäftstätigkeit

Die Politik und die Praxis der CSP, die für den Fall einer Einstellung der Geschäftstätigkeit vorgesehen sind, müssen mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.9, *CA termination,* konform sein.

3.2.12 Tätigkeitsjournal

Die Politik und die Praxis der CSP in Bezug auf die Tätigkeitsjournale müssen mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.10, *Compliance with legal requirements*, und 7.4.11, *Recording of information concerning qualified certificates,* konform sein.

3.3 Verwaltung der Schlüssel

3.3.1 Generierung der Schlüssel der CSP

Die CSP muss ihre eigenen Schlüssel entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.1, *Certification authority key generation,* generieren.

3.3.2 Aufbewahrung des Signaturschlüssels der CSP

Die CSP muss ihren Signaturschlüssel entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.2, *Certification authority key storage, backup and recovery,* aufbewahren.

3.3.3 Verteilung des Signaturprüfschlüssels der CSP

Die CSP muss ihren Signaturprüfschlüssel entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.3, *Certification authority public key distribution,* verteilen.

3.3.4 Verwendung des Signaturschlüssels der CSP

a) Die CSP muss ihren Signaturschlüssel entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.5, *Certification authority key usage,* verwenden.

b) Die CSP darf ein Schlüsselpaar nicht mehr verwenden, wenn die Gültigkeitsdauer abgelaufen ist oder wenn der Signaturschlüssel nicht mehr zuverlässig ist oder angenommen werden muss, dass er nicht mehr zuverlässig ist.

3.3.5 Vernichtung des Signaturschlüssels der CSP

Die CSP muss ihren Signaturschlüssel entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.6, *End of CA key live cycle,* vernichten.

3.3.6 Ersetzen des Signaturschlüssels der CSP

Die CSP muss ihren Signaturschlüssel entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4.8, *Business continuity management and incident handling,* ersetzen.

3.3.7 Handhabung von kryptographischen Ausrüstungen

Die CSP muss darauf achten, dass die Handhabung der kryptographischen Ausrüstungen der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.2, *Certification authority key storage, backup and recovery*; 7.2.7, *Life cycle management of cryptographic hardware used to sign certificates*; 7.2.9, *Secure-Signature-Creation device preparation,* konform ist.

3.3.8 Generierung des Schlüssels der Antragstellerin eines Zertifikats

a) In den Fällen, in denen die CSP selber das Schlüsselpaar der Antragstellerin generiert, muss diese Generierung mit der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.8, *CA provided subject key management services*, konform sein.

b) In den Fällen, in denen die Antragstellerin eines Zertifikats ihr Schlüsselpaar selber generiert, muss die CSP sicherstellen, dass Letzteres in einer sicheren Signaturerstellungseinheit generiert wurde, so wie sie in Kapitel 3.3.9 dieses Dokuments definiert ist.

3.3.9 Sichere Signaturerstellungseinheiten

a) Die CSP muss sichere Signaturerstellungseinheiten, die gemäss einem Schutzprofil entsprechend Artikel 6 Absatz 2 ZertES [1] entwickelt wurden, verwenden und den Antragstellerinnen eines Zertifikats liefern.

b) Die CSP muss die Handhabung der sicheren Signaturerstellungseinheiten entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.9, *Secure-signature-creation device preparation,* sicherstellen.

3.4 Verwaltung der Zertifikate

3.4.1 Registrierung

a) Die CSP muss die Antragstellerin des Zertifikats entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.3.1, *Subject registration,* registrieren.

3.4.2 Generierung der Zertifikate

a) Die CSP muss Zertifikate generieren, deren Format Kapitel 3.4.3.1 entspricht.

b) Die CSP muss Zertifikate generieren, die der Spezifikation ETSI TS 101 456 [6], Kapitel 7.3.3, *Certificate Generation,* entsprechen.

3.4.3 Format der Zertifikate

Die Anforderungen dieses Kapitels stützen sich auf die Spezifikation ETSI 101 862 [14] und erfüllen gleichzeitig die spezifischen Bestimmungen des ZertES [1].

3.4.3.1 Felder des Zertifikats

Die CSP muss Zertifikate entsprechend den Vorschriften in diesem Kapitel generieren.

Beschreibung	Feld/Erweiterung/Attribut	Inhalt
Seriennummer	**serialNumber**	Seriennummer des Zertifikats gemäss den Dokumenten ITU-T X.509, Kapitel 7, und RFC 3280 [10], Kapitel 4.1.2.2.
Name/Pseudonym und spezifische Attribute des Inhabers	**subject** **title** **subjectAltName**	Name oder Pseudonym der natürlichen Person, die Inhaberin des Signaturschlüssels ist, sowie ihre spezifische Attribute, um eine bestimmte juristische Person zu vertreten, gemäss dem Dokument RFC 3739 [11], Kapitel 3.1.2.
Schlüssel und Algorithums zur Prüfung der Signatur	**subjectPublicKeyInfo**	Schlüssel und Bezeichnung des Algorithmus zur Prüfung der Signatur des Zertifikatsinhabers gemäss dem Dokument RFC 3280 [10], Kapitel 4.1.2.7.
Gültigkeitsdauer	**validity**	Gültigkeitsdauer gemäss dem Dokument RFC 3280 [10], Kapitel 4.1.2.5.
Name der CSP und Niederlassungsstaat der CSP	**issuer** **countryName**	Name der CSP und Niederlassungsstaat gemäss dem Dokument RFC 3739 [11], Kapitel 3.1.1.
Qualifizierte elektronische Signatur der CSP	**signatureValue**	Qualifizierte elektronische Signatur der CSP gemäss dem Dokument RFC 3280 [10], Kapitel 4.1.1.3.
Angabe, ob die Anbieterin anerkannt ist oder nicht	**issuerAltName**	Die Erweiterung issuerAltName gemäss dem Dokument RFC 3280 [10], Kapitel 4.2.1.8 muss folgende Informationen beinhalten O = EA O = SAS O = „Name der Anerkennungsstelle“ CN = „Name der Anbieterin“
Nutzungsbereich	**keyUsage**	Nutzungsbereich gemäss den Dokumenten ITU-T X.509 [9] Kapitel 8.2.2.3 und RFC 3280 [10], Kapitel 4.2.1.3. Bit Nr. 1 setzen, um anzuzeigen, dass das Zertifikat ausschliesslich zur Überprüfung der Unterschrift verwendet wird.
Verteilungspunkt der	**cRLDistributionPoints**	Verteilungspunkt der Liste der ungültig erklärten

Liste der ungültig erklärten Zertifikate		Zertifikate gemäss den Dokumenten ITU-T X.509 [9] Kapitel 8.6.2.1 und RFC 3280 [10], Kapitel 4.2.1.14.
Wert der Transaktionen	**QCStatements**	Der Maximalwert der Transaktionen sind in der Erweiterung QCStatements gemäss dem Dokument RFC 3739 [11], Kapitel 3.2.6, in Form eines Objektbezeichners (OID) der Erklärung angegeben, wie es im Dokument ETSI TS 101 862 [14], kapitel 5.2.2 definiert ist.
Präzisierung, dass es sich um ein qualifiziertes Zertifikat handelt	**QCStatements**	Information, dass es sich um ein qualifiziertes Zertifikat handelt, ist in der Erweiterung QCStatements gemäss dem Dokument RFC 3739 [11], Kapitel 3.2.6, in Form eines Objektbezeichners (OID) der Erklärung enthalten, wie es im Dokument ETSI TS 101 862 [14], Kapitel 5.2.1 definiert ist.
Präzisierung, dass der Signaturschlüssel durch eine sichere Signaturerstellungseinheit (SSCD) geschützt ist	**QCStatements**	Die Präzisierung, dass der Signaturschlüssel durch eine SSCD im Sinne von Anhang III der europäischen Richtlinie [5] geschützt ist. Diese Information ist in der Erweiterung QCStatements gemäss dem Dokument RFC 3739 [11], Kapitel 3.2.6, in Form eines Objektbezeichners (OID) der Erklärung enthalten, wie es im Dokument ETSI TS 101 862 [14], Kapitel 5.2.4 definiert ist.

3.4.4 Erneuerung und Anpassung des Zertifikats

Die CSP muss ein Zertifikat entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.3.2, *Certificate renewal, rekey and update,* erneuern oder anpassen.

3.4.5 Ungültigerklärung des Zertifikats

a) Die CSP muss die Zertifikate entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.3.6*, Certificate revocation and suspension,* ungültig erklären.

b) Die CSP, die ein Zertifikat ungültig erklärt, muss alle Informationen nachführen, über die sie verfügt und die den Status dieses Zertifikats betreffen. Wenn die CSP Listen der ungültig erklärten Zertifikate (CRL) publiziert, muss darin jedes ungültig erklärte Zertifikat aufgeführt sein.

3.4.6 Verteilung der Zertifikate

a) Die CSP muss das Zertifikat, nachdem es generiert wurde, seinem Inhaber zur Verfügung stellen.

b) Wenn die CSP einen Verzeichnisdienst zur Verfügung stellt, muss sie sicherstellen, dass der Inhaber in die Veröffentlichung seines Zertifikats im Verzeichnis einwilligt. Sie muss im Übrigen den Inhaber informieren, dass er seine Einwilligung betreffend die Veröffentlichung des Zertifikats im Verzeichnis jederzeit zurückziehen kann.

c) Stellt die CSP einen Verzeichnisdienst zur Verfügung, muss sie dessen Verfügbarkeit entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.3.5, *Certificate dissemination,* sicherstellen.

3.4.7 Publikation des Zertifikatstatus

Die CSP muss sicherstellen, dass die Information betreffend die Ungültigerklärung des Zertifikats seinem Inhaber und den Benutzern von Zertifikaten entsprechend der Spezifi-

kation ETSI TS 101 456 [6], Kapitel 7.3.6, *Certificate revocation and suspension*, zur Verfügung steht.

3.4.8 Information betreffend die Nutzungsbedingungen von Zertifikaten

Die CSP muss die Inhaber und Benutzer von Zertifikaten über die Nutzungsbedingungen entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.3.4, *Dissemination of terms and conditions,* informieren.

3.5 Zeitstempel

Um eine Bestätigung zur Feststellung der Existenz von digitalen Daten zu einem bestimmten Zeitpunkt auszustellen, muss die CSP auf ein Datierungssystem zurückgreifen, das der Spezifikation ETSI 102 023 [12] entspricht.

Biel, den (*gleiches Datum wie bei „Ausgabe" auf der ersten Seite)*

BUNDESAMT FÜR KOMMUNIKATON

Der Direktor:

Marc Furrer