Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Kommunikation BAKOM

Technischeund administrative Vorschriften über

Zertifizierungsdienste im Bereich der elektronischen Signatur

SR 943.032.1

Ausgabe 3: 2006
Inkrafttreten: 2006

Inhaltsverzeichnis

1 Allgemeines

1.1 Geltungsbereich

Diese Technischen und administrativen Vorschriften (TAV) stützen sich auf:

- das Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) [1],
- die Verordnung vom 3. Dezember 2004 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 anbietet, erfüllen muss, um anerkannt zu werden.

Das System für die 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 angegebenen internationalen Normen umschrieben sind.

1.2 Referenzen

[1] SR 943.03, ZertES
Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur

[2] SR 943.032, VZertES
Verordnung vom 3. Dezember 2004 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
(ABl. L 13 vom 19.1.2000, S. 12)

[6] ETSI TS 101 456, v1.4.1 (2006-01)
Policy requirements for certification authorities issuing qualified certificates

[7] 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

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

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

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

[11] ISO/IEC 15408:2005
Information technology – Security techniques. Evaluation criteria for IT security

[12] ETSI TS 101 862, v1.3.2 (2004-06)
Qualified Certificate Profile

[13] FIPS 140-2 (25.5.01)
Security Requirements for Cryptographic Modules

[14] ITSEC Version 1.2 (28. Juni 1991)
Information Technology Security Evaluation Criteria

[15] CWA 14169 (2004)
Secure Signature-Creation Devices "EAL 4+"

[16] ETSI TS 101 861, v1.3.1 (2006-01)
Time Stamping Profile

[17] CWA 14167-3 (2004)
Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)

[18] RFC 3279 (April 2002)
Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[19] FIPS 140-1 (11.1.94)
Security Requirements for Cryptographic Modules

[20] EN 45012:1998
Allgemeine Anforderungen an Stellen, die Qualitätsmanagementsysteme begutachten und zertifizieren (ISO/IEC Guide 62:1996)

[21] ISO/IEC 27001:2005
Information technology – Security techniques – Information security management systems - Requirements

Die oben genannten Dokumente können bei folgenden Organisationen bezogen werden:

ITU-T Empfehlungen	Internationale Fernmeldeunion (ITU) Place des Nations 1211 Genève 20 http://www.itu.int
ISO-Normen	Zentralsekretariat der Internationalen Organisation für Normung (ISO) 1, rue de Varembé 1211 Genève http://www.iso.ch
ETSI-Spezifikationen	ETSI, Europäischen Institut für Telekommunikationsnormen 650 route des Lucioles 06921 Sophia Antipolis, France http://www.etsi.org
CEN-CWA	Europäischen Komitee für Normung (CEN) 36, rue de Stassart B - 1050 Bruxelles, Belgique http://www.cenorm.be
FIPS-Dokumente	National Institute of Standards and Technology (NIST) http://csrc.nist.gov/publications
Gesetzestexte mit einer SR-Referenz	Bundesamt für Bauten und Logistik (BBL) Vertriebsstelle für Bundespublikationen CH-3003 Bern http://www.bundespublikationen.ch
Technische und administrative Vorschriften	BAKOM Zukunftstrasse 44

	Postfach 2501 Biel http://www.bakom.ch/
Richtlinie 1999/93/EG des europäischen Parlamentes	Europäische Union http://www.europa.eu.int/eur-lex/de/search/search_lif.html
ITSEC-Dokument	Bundesamt für Sicherheit in der Informationstechnik (BSI) http://www.bsi.de/zertifiz/itkrit/itsec.htm
RFC-Dokumente	Internet Engineering Task Force (IETF) http://www.ietf.org/
EN-Norm	Deutsches Institut für Normung (DIN) http://www.din.de

1.3 Abkürzungen

AkkBV	Akkreditierungs- und Bezeichnungsverordnung [4]
BAKOM	Bundesamt für Kommunikation
CA	*Certification Authority* - Zertifizierungsbehörde
CB	*Certification Body* – Zertifizierungsstelle oder Anerkennungsstelle in diesen TAV
CEN	*Comité européen de normalisation* – Europäisches Komitee für Normung
CP	*Certification policy* – Zertifizierungspolitik
CPS	*Certification pratice statement* – Aussage über die Zertifizierungspraktiken
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
TAV	Technische und administrative Vorschriften
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 TAV bedeuten:

Anbieterin von Zertifizierungsdiensten (CSP) oder **Zertifizierungsstelle (CA)**: 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 über die Zertifizierungspraktiken (CPS): Aussage über die Regeln und Richtlinien , die von der Anbieterin von Zertifizierungsdiensten für die Ausstellung von Zertifikaten effektiv umgesetzt werden. Die CPS definiert die Ausrüstungen, die Politik und die Verfahren, die von der Anbieterin von Zertifizierungsdiensten in Übereinstimmung mit der von ihr gewählten Zertifizierungspolitik verwendet werden;

Benutzer/-in des Zertifikats: Person oder Prozess, die oder der sich bei der Verwendung dieses Zertifikats auf die überprüften elektronischen Signaturen verlässt;

Digitales Zertifikat: elektronische Bescheinigung, die einen Signaturprüfschlüssel mit dem Namen einer Person verknüpft. In diesem 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 Anbieterin von Zertifizierungsdiensten; Erzeugung eines digitalen Zertifikats auf der Grundlage des Namens der Antragstellerin oder des Antragstellers eines Zertifikats und ihrer/seiner allfälliger Attribute, die bei der Registrierung überprüft werden;

Inhaber/-in des Zertifikats: Natürliche Person, die Inhaberin des Signaturschlüssels ist, der dem im Zertifikat aufgeführten Signaturprüfschlüssel zugeordnet ist;

Liste der für ungültig erklärten Zertifikate (CRL): von der Anbieterin von Zertifizierungsdiensten signierte Liste, die alle Seriennummern der Zertifikate enthält, welche vor Ablauf ihrer Gültigkeit für ungültig erklärt wurden;

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

1. Sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet;
2. Sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers;
3. Sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer/seiner alleinigen Kontrolle halten kann;
4. Sie wird durch eine sichere Signaturerstellungseinheit nach Artikel 6 Absatz 1 und 2 ZertES [1] 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 [1] erfüllt;

Registrierung: Dienst der Anbieterin von Zertifizierungsdiensten, der darin besteht, die Identität und wenn nötig die Attribute jeder Antragstellerin und jedes Antragstellers eines Zertifikats zu überprüfen, bevor ihr/sein Zertifikat erzeugt oder die Aktivierungsdaten (oder das Passwort) zur Aktivierung der Nutzung des Signaturschlüssels zugewiesen werden;

Schlüsselpaar: Signaturschlüssel und dazugehörender Signaturprüfschlüssel, die mathematisch durch einen asymmetrischen Signaturalgorithmus miteinander verknüpft sind;

Sichere Signaturerstellungseinheit: Einheit nach Artikel 6 Absatz 2 ZertES [1], die für die Implementierung des Signaturschlüssels konfiguriert ist, den die Inhaberin oder 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. Mit der Sicherheitsstrategie und -politik kann die gesamthaft zu erreichende Sicherheitsstufe für ein Informationssystem und besonders für jedes Element der Sicherheitsarchitektur eindeutig definiert werden;

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 von der Inhaberin oder 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 darin besteht, das Zertifikat nach seiner Generierung der Inhaberin oder dem Inhaber und – bei Einwilligung der Inhaberin oder des Inhabers – den Benutzerinnen und Benutzern des Zertifikats zur Verfügung zu stellen;

Verwaltung des Zertifikatstatus: Dienst der Anbieterin von Zertifizierungsdiensten, anhand dessen die Benutzerinnen und Benutzer eines Zertifikats 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 Anbieterin von Zertifizierungsdiensten versehene Bescheinigung abgibt, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt existiert haben;

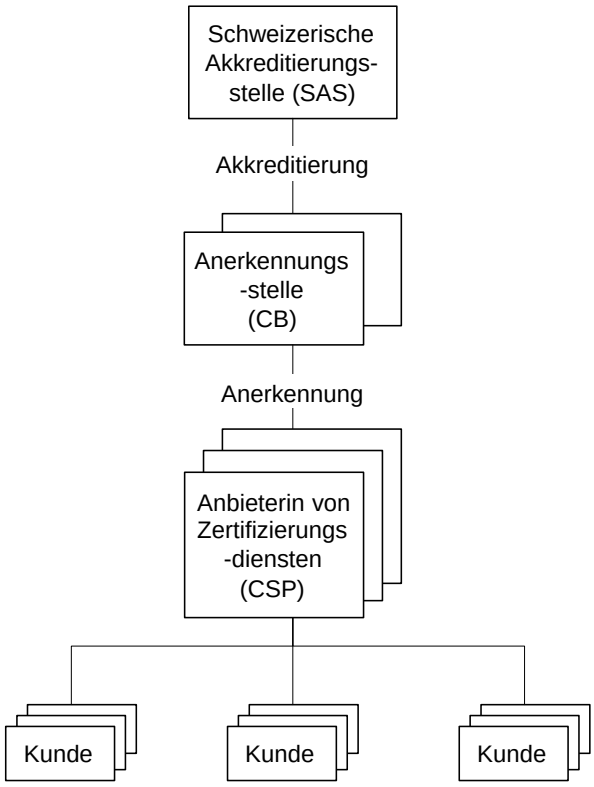
Zertifizierungsstelle (CA): siehe „Anbieterin von Zertifizierungsdiensten“;

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

2 System für die Anerkennung der CSP

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

Um sich für die Anerkennung von Anbieterinnen von Zertifizierungsdiensten akkreditieren zu lassen, müssen die Anerkennungsstellen die Kriterien der europäischen Norm EN 45012 [20] erfüllen. Die Anerkennung der Anbieterinnen von Zertifizierungsdiensten setzt mindestens eine akkreditierte Anerkennungsstelle voraus. Falls keine solche Stelle besteht, anerkennt das Bundesamt für Kommunikation (BAKOM) die Anbieterinnen von Zertifizierungsdiensten.



Die Liste der akkreditierten Anerkennungsstellen und die Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten werden auf der SAS-Website veröffentlicht (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 TAV auf den Spezifikationen und Normen der EESSI (Europäische Initiative für die Standardisierung der elektronischen Signatur), die ihre Grundlage in der europäischen Richtlinie 1999/93/EG [5] haben.

Diese TAV beziehen sich insbesondere auf die Spezifikation ETSI TS 101 456 [6], *Policy requirements for certification authorities issuing qualified certificate*.

3.2 Organisation und operative Grundsätze

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

b) Die CSP muss ihre operativen Grundsätze gemäss den folgenden Referenzen ausgestalten:

Zertifizierungspolitik (CP)	ETSI TS 101 456 [6], Kapitel 6.1, *Certification authority obligations*; 8.1, *Qualified certificate policy management*
Datierungspolitik	ETSI TS 102 023 [10], Kapitel 6.1.1, *TSA obligations - General*
Aussage über die Zertifizierungspraktiken (CPS)	ETSI TS 101 456 [6], Kapitel 6.1, *Certification authority obligations*; 7.1, *Certification pratice statement*
Aussage über die Datierungspraktiken	ETSI TS 102 023 [10], Kapitel 6.1.1, *TSA obligations – General;* 7.1.1 *TSA Practice Statement*
Sicherheitspolitik	ETSI TS 101 456 [6], Kapitel 7.4.1, *Security Management* ETSI TS 102 023 [10], Kapitel 7.4.1, *Security Management*

c) Die CSP muss jedes Jahr interne Audits gemäss Kapitel 6 der Norm ISO/IEC 27001 [21] durchführen, um die Konformität ihrer Aktivitäten mit folgenden Dokumenten zu überprüfen:

- ZertES [1], VZertES [2] sowie diese TAV ;
- Zertifizierungspolitik (CP) ;
- Datierungspolitik ;
- Aussage über die Zertifizierungspraktiken (CPS);
- Aussage über die Datierungspraktiken.

d) Die internen Audits müssen insbesondere jegliche Änderungen gegenüber den erwähnten Dokumenten zum Ausdruck bringen und aufbewahrt werden.

e) Die Politik und die Praktiken der CSP müssen der Spezifikation ETSI TS 101 456 [6], Kapitel 7.4, *CA Management and Operation,* entsprechen.

f) Jegliche reparierte, gemäss Risikoanalyse sicherheitskritische Ausrüstung muss durch zwei Vertrauensangestellte und gemäss einem dokumentierten Verfahren geprüft, konfiguriert und wieder in Betrieb genommen werden.

g) Die CSP muss einen Plan für die Kontinuität der Tätigkeiten im Schadensfall erstellen, der folgenden Aspekten Rechnung trägt:

- Bestimmung der möglichen Schäden und der Massnahmen zu deren Bekämpfung;
- Dokumentation der bei einem Schadensfall auszulösenden Verfahren (Notfallplan);
- Dokumentation der Verfahren zur Fortführung der normalen Tätigkeit an einem Ausweichstandort (Wiederherstellungsplan);
- Dokumentation der Verfahren zur Wiederaufnahme der Tätigkeit am Ursprungsstandort;
- Identifizierung der Aufgaben und der verantwortlichen Personen für jedes Verfahren;
- Voraussetzungen, die für die Aktivierung eines der Verfahren nötig sind;
- Ausbildung und Sensibilisierung der betroffenen Angestellten;
- Massnahmen, um diese Verfahren regelmässig zu testen;
- Anpassung der Verfahren an die Ergebnissen der Tests oder die gemachten Erfahrungen bei einem Schadensfall.

h) Die CSP muss die Aktualität und die Wirksamkeit ihres Kontinuitätsplans in regelmässigen Abständen beurteilen und ihren Kontinuitätsplan entsprechend dem Ergebnis dieser Beurteilung nachführen.

i) Die CSP muss alle Informationen, die für die Wiederaufnahme ihrer Tätigkeiten nach einem Schadensfall benötigt werden, aktuell halten und regelmässig speichern. Zudem muss die CSP diese Informationen so wiederherstellen können, wie sie zuletzt gespeichert wurden.

3.3 Verwaltung der Schlüssel

3.3.1 Verwaltung der Schlüssel der CSP

a) Die CSP muss ihre eigenen Schlüssel entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2, *Public key infrastructure – Key management life cycle*, verwalten und verwenden.

b) Die CSP muss darauf achten, dass die Handhabung der kryptografischen Ausrüstungen der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2, *Public key infrastructure – Key management life cycle,* entspricht.

3.3.2 Generierung des Schlüssels der Antragstellerin oder des Antragstellers durch die CSP

a) In den Fällen, in denen die CSP selber das Schlüsselpaar der Antragstellerin oder des Antragstellers 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 CSP selber das Schlüsselpaar der Antragstellerin oder des Antragstellers generiert, muss diese Generierung in einem System erfolgen,:

- das die Anforderungen erfüllt, die in Dokument FIPS 140-1 [19] oder FIPS 140-2 [13] Stufe 3 oder höher festgelegt sind, oder
- das die in Dokument CWA 14167-3 [17] festgelegten Anforderungen erfüllt, oder
- welches die Prüfung der Prüfstufe EAL 4 der Norm ISO/IEC 15408:1999 [11] umfassen muss, erhöht um die Versicherungselemente ADV_IMP.2 (implementation of the TSF), AVA_CCA.1 (vulnerability assessment, covert channel analysis) und AVA_VLA.4 (vulnerability assessment, highly resistant), oder
- welches die Prüfung der Prüfstufe E3 hoch des Dokuments ITSEC [14] umfassen muss.

In den beiden letzten Fällen muss ein Prüfungsgegenstand geliefert werden, der die in Dokument CWA 14167-3 [17] festgelegten Anforderungen erfüllt.

3.3.3 Sichere Signaturerstellungseinheiten

a) Die CSP muss den Antragstellerinnen und Antragstellern eines Zertifikats sichere Signaturerstellungseinheiten liefern, die den Mindestanforderungen von Artikel 6 Absatz 2 ZertES [1] entsprechen, oder sicherstellen, dass diese solche verwenden. Mit dem Dokument CWA 14169 [15] wird die Konformität mit den Anforderungen von Artikel 6 Absatz 2 ZertES [1] sichergestellt.

Die sicheren Signaturerstellungseinheiten müssen zudem folgende zusätzliche Anforderungen erfüllen:

- Sie dürfen weder den zu signierenden Inhalt ändern, noch die signierende Person daran hindern, diesen Inhalt vor dem Signieren genau zur Kenntnis zu nehmen;
- Das qualifizierte Zertifikat (oder der eindeutige Verweis auf dieses Zertifikat) muss im System vorhanden sein;
- Der dem qualifizierten Zertifikat entsprechende Signaturschlüssel darf nicht verwendet werden, bevor er durch Aktivierungsdaten aktiviert worden ist;
- Inkorrekte und aufeinander folgende Aktivierungsversuche müssen festgestellt werden können;
- Wenn eine im Voraus festgelegte Anzahl aufeinander folgender und inkorrekter Aktivierungsversuche erreicht wurde, muss der Gebrauch der Signaturschlüssel gesperrt werden. Die im Voraus festgelegte Anzahl darf nicht höher als vier sein;
- Die erneute Freigabe eines gesperrten Schlüssels setzt ein Verfahren voraus, bei dem sowohl die Beteiligung der CSP als auch die Eingabe von korrekten Aktivierungsdaten erforderlich sind.

b) Die Zertifizierung der sicheren Signaturerstellungseinheiten muss für alle oben stehenden Anforderungen erhältlich sein und

- entweder die Prüfstufe EAL 4 der Norm ISO/IEC 15408:1999 [11] umfassen, erhöht um die Versicherungselemente AVA_MSU.3 (vulnerability assessment, analysis and testing of insecure states) und AVA_VLA.4 (vulnerability assessment, highly resistant),
- oder die Prüfstufe E3 hoch des Dokuments ITSEC [14] umfassen.

c) Wenn die CSP die sicheren Signaturerstellungseinheiten liefert, muss sie diese entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.2.9, *Secure-signature-creation device preparation,* handhaben.

d) Wenn eine Signaturerstellungseinheit in einer physisch gesicherten Umgebung betrieben wird, dann gilt sie als sichere Signaturerstellungseinheit, um qualifizierte elektronische Signaturen gemäss ZertES zu erstellen, sofern folgende Anforderungen erfüllt sind:

- Die CSP muss sicherstellen, dass die Signaturerstellungseinheit gemäss FIPS 140-2 Level 3 (oder höher) zertifiziert ist;
- Die CSP muss sicherstellen, dass die Signaturerstellungseinheit und der Server, auf dem sich die Signierapplikation befindet, von anderen, nicht mit der Signaturerstellung zusammenhängenden Komponenten logisch getrennt sind;
- Die CSP muss sicherstellen, dass die Signaturerstellungseinheit von der Inhaberin oder vom Inhaber des qualifizierten Zertifikats oder von einer bevollmächtigten Person betrieben wird;
- Die CSP muss sicherstellen, dass der Betrieb der Signaturerstellungseinheit unter Umsetzung der Kontrollen erfolgt, die in Anhang A der Norm ISO/IEC 27001 [21] genannt und auf Grund der Risikoanalyse als notwendig betrachtet werden;
- Die CSP muss sicherstellen, dass der Zutritt zur physisch gesicherten Umgebung sowie der Zugriff zur Signaturerstellungseinheit und zur Signierapplikation kontrolliert und nachvollziehbar protokolliert werden.

3.4 Verwaltung der Zertifikate

3.4.1 Registrierung, Verwaltung und Ungültigerklärung von Zertifikaten für Dritte

a) Die CSP muss die Antragstellerinnen und Antragsteller eines Zertifikats registrieren und die Zertifikate entsprechend der Spezifikation ETSI TS 101 456 [6], Kapitel 7.3, *Public Key Infrastructure - Certificate Management Life Cycle,* verwalten.

b) Die CSP, die ein Zertifikat für ungültig erklärt, muss relevante Informationen, die den Status dieses Zertifikats betreffen und über die sie verfügt, aktualisieren.

c) Bevor die CSP die Gründe für die Ungültigerklärung eines Zertifikats publiziert, muss sie die Einwilligung der Inhaberin oder des Inhabers dieses Zertifikats einholen.

d) Entsprechend dem Dokument RFC 3280 [8], Kapitel 5.1, muss die CSP Listen der für ungültig erklärten Zertifikate (CRL) erstellen, welche die Felder tbsCertList, signatureAlgorithm und signatureValue enthalten.

e) Für die CRL muss die CSP sicherstellen, dass entsprechend dem Dokument RFC 3280 [8], Kapitel 5.1, folgende Felder der Sequenz tbsCertList hinzugefügt wurden:

- version, deren Wert 1 ist, um anzugeben, dass es sich um eine CRL Version 2 handelt;
- signature;
- issuer;
- thisUpdate;
- nextUpdate;
- revokedCertificates, inklusive Seriennummer des Zertifikats und Datum der Ungültigerklärung;

f) Für die CRL muss die CSP sicherstellen, dass entsprechend dem Dokument RFC 3280 [8], Kapitel 5.2, die nicht kritischen Erweiterungen authorityKeyIdentifier und cRLNumber der Sequenz tbsCertList hinzugefügt wurden.

g) Die Ungültigerklärung ist endgültig. Die Suspendierung von Zertifikaten ist nicht erlaubt.

3.4.2 Format der Zertifikate für Inhaberinnen und Inhaber

a) Entsprechend Dokument RFC 3280 [8], Kapitel 4.1, muss die CSP Zertifikate generieren, welche die Felder tbsCertificate, signatureAlgorithm und signatureValue enthalten.

b) Entsprechend Artikel 7 ZertES [1] und dem Dokument RFC 3280 [8], Kapitel 4.1, muss die CSP der Sequenz tbsCertificate folgende Felder hinzufügen:

Beschreibung	Feld	Inhalt
Version	**version**	Gemäss Dokument RFC 3280 [8], Kapitel 4.1.2.1. Dieses Feld muss den Wert 2 haben, um anzuzeigen, dass es sich um ein Zertifikat der Version 3 handelt.
Seriennummer des Zertifikats	**serialNumber**	Gemäss den Dokumenten ITU-T X.509 [7], Kapitel 7 und RFC 3280 [8], Kapitel 4.1.2.2.
Objektbezeichner des Signaturalgorithmus, der für das Signieren des Zertifikats benutzt wurde	**signature**	Gemäss den Dokumenten RFC 3280 [8], Kapitel 4.1.2.3 und RFC 3279 [18]..
- Name der CSP, - Niederlassungs-Staat der CSP	**issuer**	Gemäss Dokument RFC 3280 [8], Kapitel 4.1.2.4.
Gültigkeitsdauer des Zertifikats	**validity**	Gemäss Dokument RFC 3280 [8], Kapitel 4.1.2.5.

- Name oder Pseudonym und - wenn nötig, spezifische Attribute der Inhaberin oder des Inhabers	**subject**	Gemäss Dokument RFC 3739 [9], Kapitel 3.1.2.
Schlüssel und Algorithmus zur Prüfung der Signatur der Inhaberin oder des Inhabers des Zertifikats	**subjectPublicKeyInfo**	Gemäss den Dokumenten RFC 3280 [8], Kapitel 4.1.2.7 und RFC 3279 [18]

c) Entsprechend Dokument RFC 3280 [8], Kapitel 4.2, muss die CSP der Sequenz tbsCertificate folgende Erweiterungen hinzufügen:

Beschreibung	Kritische Erweiterung	Name der Erweiterung	Inhalt
Objektbezeichner des Schlüssels der CSP, die das Zertifikat signiert hat	Nein	**authorityKeyIdentifier**	Gemäss dem Dokument RFC 3280 [8], Kapitel 4.2.1.1.
Geltungsbereich des Zertifikats	Ja	**keyUsage**	Gemäss den Dokumenten ITU-T X.509 [7], Kapitel 8.2.2.3 und RFC 3280 [8], Kapitel 4.2.1.3. Nur Bit Nr. 1 setzen, um anzuzeigen, dass das Zertifikat ausschliesslich zur Überprüfung der elektronischen Signaturen, die den Unterzeichner verpflichten, verwendet wird.
- Zertifizierungs-Politik - Geltungsbereich des Zertifikats, wenn nötig	Nein	**certificatePolicies**	Gemäss Dokument RFC 3280 [8], Kapitel 4.2.1.5. Diese Erweiterung muss das Feld policyQualifiers enthalten. Darin müssen CPS Pointer und User Notice erscheinen, die auf die Zertifizierungspraktiken der CSP bzw. den Benutzerhinweis verweisen.
- Hinweis, ob die CSP anerkannt ist oder nicht, - Name der Anerkennungs-Stelle	Nein	**issuerAltName**	Die anerkannten CSP müssen in den Zertifikaten, die sie ausstellen, den Namen der Anerkennungsstelle in folgender Form in der Erweiterung «issuerAltName» (gemäss RFC 3280 [8], Kapitel 4.2.1.8) einfügen: - ZertES-Anerkennungsstelle: «Name der Anerkennungsstelle» Die Übersetzungen «organisme de reconnaissance SCSE», «organismo di riconoscimento FiEle» oder «ZertES Recognition Body» sind zulässig. Die nicht-anerkannten CSP müssen die folgende Anmerkung in der Erweiterung «issuerAltName» (gemäss RFC 3280 [8], Kapitel 4.2.1.8) einfügen: - ZertES-Anerkennungsstelle: (nicht anerkannte CSP) Die Übersetzungen «organisme de

			reconnaissance SCSE: (CSP non reconnu)», «organismo di riconoscimento FiEle: (CSP non riconosciuto)» oder «ZertES Recognition Body: (unrecognised CSP)» sind zulässig.
Verteilungspunkt der Liste der ungültig erklärten Zertifikate	Nein	**cRLDistributionPoints**	Gemäss den Dokumenten ITU-T X.509 [7], Kapitel 8.6.2.1 und RFC 3280 [8], Kapitel 4.2.1.14. Das Feld reasons muss fehlen.
Zugangspunkt zum Zertifikat der CSP	Nein	**AuthorityInformation Access**	Gemäss Dokument RFC 3280 [8], Kapitel 4.2.2.1.
Hinweis, dass es sich um ein qualifiziertes Zertifikat handelt	Ja/Nein	**qcStatements**	In Form eines Objektbezeichners (OID) gemäss Definition in Dokument ETSI TS 101 862 [12], Kapitel 5.2.1.
Hinweis, dass der Signaturschlüssel durch eine sichere Signaturerstellungseinheit geschützt ist (SSCD)	Ja/Nein	**qcStatements**	In Form eines Objektbezeichners (OID) gemäss Definition in Dokument ETSI TS 101 862 [12], Kapitel 5.2.4.
Grenzwert der Transaktionen, wenn nötig	Ja/Nein	**qcStatements**	In Form eines Objektbezeichners (OID) gemäss Definition in Dokument ETSI TS 101 862 [12], Kapitel 5.2.2.

Die Anforderungen dieses Kapitels stützen sich auf die Spezifikation ETSI TS 101 862 [12] und erfüllen gleichzeitig die Bestimmungen von Art. 7 ZertES [1].

3.4.3 Verwaltung des Zertifikats der CSP

a) Die CSP muss sicherstellen, dass ihr Zertifikat entsprechend dem Dokument RFC 3280 [8], Kapitel 4.1, die Felder tbsCertificate, signatureAlgorithm und signatureValue enthält.

b) Für ihr eigenes Zertifikat muss die CSP sicherstellen, dass entsprechend dem Dokument RFC 3280 [8], Kapitel 4.1, folgende Felder der Sequenz tbsCertificate hinzugefügt wurden:

- version, deren Wert 2 ist, um anzuzeigen, dass es sich um ein Zertifikat der Version 3 handelt;
- serialNumber;
- signature;
- issuer;
- validity;
- subject;
- subjectPublicKeyInfo;

c) Für ihr eigenes Zertifikat muss die CSP sicherstellen, dass gemäss dem Dokument RFC 3280 [8], Kapitel 4.2, die folgenden kritischen Erweiterungen der Sequenz tbsCertificate vorhanden sind:

- keyUsage, für welche die Bits 5 und 6 erhöht werden müssen;
- basicConstraints, dessen „cA boolean“-Feld dem Wert TRUE entsprechen muss;
- qcStatements, mit dem Hinweis, dass es sich um ein qualifiziertes Zertifikat handelt, gemäss Kapitel 3.4.2, Bst. c von diesem Dokument.

d) Für ihr eigenes Zertifikat muss die CSP sicherstellen, dass entsprechend dem Dokument RFC 3280 [8], Kapitel 4.2, die folgenden nicht kritischen Erweiterungen der Sequenz tbsCertificate vorhanden sind:

- authorityKeyIdentifier ;
- certificatePolicies ;
- issuerAltName gemäss Kapitel 3.4.2, Bst. c von diesem Dokument;

- crlDistributionPoints.

3.5 Datierungssystem

a) 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 TS 102 023 [10] entspricht.

b) Die Datierungssysteme müssen Zeitstempel erzeugen, die dem Dokument ETSI TS 101 861 [16] entsprechen.

c) Die CSP muss jeden Zeitstempel mit einem ausschliesslich dafür vorgesehenen Schlüssel signieren. Das diesem Schlüssel entsprechende Zertifikat muss den Bezeichner «id-kp-timeStamping» in der Erweiterung «Extended Key Usage» gemäss RFC 3280 [8], Kapitel 4.2.1.13 enthalten.

Biel, den

BUNDESAMT FÜR KOMMUNIKATION

Der Direktor:

Martin Dumermuth