Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Kommunikation BAKOM

Anhang der Verordnung des BAKOM vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.032.1)

Technische und administrative Vorschriften

über

Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate

Ausgabe 1: 23.11.2016
Inkrafttreten: 1.1.2017

Inhaltsverzeichnis

1 Allgemeines

1.1 Geltungsbereich

Diese technischen und administrativen Vorschriften (TAV) bilden den Anhang der Verordnung des BAKOM vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.032.1). Sie stützen sich auf:

- Artikel 21 Absatz 2 des Gesetzes vom 18. März 2016 über die elektronische Signatur (ZertES) [1],
- die Artikel 3 Absatz 2, 4 Absatz 1, 10 und 15 der Verordnung vom 23. November 2016 über die elektronische Signatur (VZertES) [2].

Sie präzisieren sie die in Gesetz und Verordnung definierten Voraussetzungen und grundlegenden Anforderungen, die eine Anbieterin von Zertifizierungsdiensten (CSP), die qualifizierte Zertifikate ausstellt und andere Dienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate anbieten kann, erfüllen muss, um anerkannt zu werden.

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
Gesetz vom 18. März 2016 über die elektronische Signatur

[2] SR 943.032, VZertES
Verordnung vom 23. November 2016 über die elektronische Signatur

[3] ETSI EN 319 411-2 V2.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[4] FIPS 140-2 (2001)
Security Requirements for Cryptographic Modules

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

[6] EN 419211-2:2013
Protection profiles for secure signature creation device. Part 2: Device with key generation

[7] EN 419211-3:2013
Protection profiles for secure signature creation device. Part 3: Device with key import

[8] EN 419211-4:2014
Protection profiles for secure signature creation device. Part 4: Extension for device with key generation and trusted channel to certificate generation application

[9] EN 419211-5:2014
Protection profiles for secure signature creation device. Part 5: Extension for device with key generation and trusted channel to signature creation application

[10] EN 419211-6:2014
Protection profiles for secure signature creation device. Part 6: Extension for device with key import and trusted channel to signature creation application

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

[12] ISO/IEC 15408-3:2008
Information technology – Security techniques. Evaluation criteria for IT security – Part 3: Security assurance components

[13] CEN/TS 419241:2014
Security Requirements for Trustworthy Systems Supporting Server Signing

[14] ETSI EN 319 412-1 V1.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

[15] 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

[16] 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

[17] ETSI EN 319 412-4 V1.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

[18] ETSI EN 319 412-5 V2.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[19] RFC 5280 (Mai 2008)
Internet X.509 Public Key Infrastructure - Certificate and CRL Profile

[20] Common PKI Specifications for Interoperable Applications. Version 2.0 – 20 January 2009

[21] ETSI EN 319 421 V1.1.1 (2016-03)
Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[22] ETSI EN 319 422, V1.1.1 (2016-03)
Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

Die oben genannten Dokumente können bei folgenden Organisationen bezogen werden:

Gesetzestexte mit einer SR-Referenz	Bundesamt für Bauten und Logistik (BBL) Vertriebsstelle für Bundespublikationen CH-3003 Bern www.bundespublikationen.ch
ETSI-Dokumente	ETSI, Europäisches Institut für Telekommunikationsnormen 650 Route des Lucioles 06921 Sophia Antipolis, Frankreich www.etsi.org
FIPS-Dokumente	National Institute of Standards and Technology (NIST) csrc.nist.gov/publications
CEN-Dokumente	Europäisches Komitee für Normung (CEN) 36, Rue de Stassart B - 1050 Brüssel, Belgien www.cenorm.be
EN-Normen	Schweizerische Normen-Vereinigung (SNV) Bürglistr. 29 CH-8400 Winterthur www.snv.ch
ISO-Normen	Zentralsekretariat der Internationalen Organisation für Normung (ISO)

	1, Rue de Varembé 1211 Genf www.iso.ch
RFC-Dokumente	Internet Engineering Task Force (IETF) www.ietf.org
Common PKI Specifications for Interoperable Applications	T7 (Arbeitsgemeinschaft von deutschen Trustcenterbetreibern und Zertifizierungsdiensteanbietern) www.t7ev.org
Technische und administrative Vorschriften	BAKOM Zukunftstrasse 44 Postfach 2501 Biel www.bakom.admin.ch

1.3 Abkürzungen

CEN	*Comité européen de normalisation* – Europäisches Komitee für Normung
CP	*Certification policy* – Zertifizierungspolitik
CPS	*Certification pratice statement* – Aussage über die Zertifizierungspraxen
CRL	*Certificate Revocation List* – Liste der für ungültig erklärten Zertifikate
CSP	*Certification Service Provider* – Anbieterin von Zertifizierungsdiensten
CWA	*CEN Workshop Agreement* – CEN-Workshop-Vereinbarung
EAL	*Evaluation Assurance Level* – Vertrauenswürdigkeitsstufe
EN	*European Normative* – europäische Norm
ETSI	*European Telecommunications Standards Institute* – Europäisches Institut für Telekommunikationsnormen
FIPS	*Federal Information Processing Standards*
IEC	*International Electrotechnical Commission* – Internationale Elektrotechnische Kommission
IETF	*Internet Engineering Task Force*
ISO	*International Standardization Organization* – Internationale Organisation für Normung
OID	*Object identifier* – Objektbezeichner
PIN	*Personal Identification Number* – Persönliche Identifikations-Nummer
PKI	*Public Key Infrastruktur* – Public-Key-Infrastruktur
RFC	*Request for Comments*
SR	Systematische Rechtssammlung
UID	Unternehmens-Identifikationsnummer
UIDG	Bundesgesetz über die Unternehmens-Identifikationsnummer
VZertES	Verordnung über die elektronische Signatur [2]
ZertES	Gesetz über die elektronische Signatur [1]

2 Grundlegende Anforderungen

2.1 Organisation und operative Grundsätze

2.1.1 Zertifizierungspolitik und Aussage über die Zertifizierungspraxen

Die CSP erarbeitet und verwaltet eine Zertifizierungspolitik (CP) sowie eine Aussage über die Zertifizierungspraxen (CPS) gemäss den Anforderungen der Norm ETSI EN 319 411-2 [3], Kapitel 5 *General provisions on Certificate Pratice Statement and Certificate Policies* und 7 *Framework for the definition of other certificate policies.*

2.1.2 Sicherheitsmanagement

Die CSP implementiert ein Sicherheitsmanagementsystem gemäss den Anforderungen der Norm ETSI EN 319 411-2 [3], Kapitel 6.4 Facility, Management, and Operational Controls, 6.5.5 Computer Security Controls, 6.5.6 Life Cycle Security Controls und 6.5.7 Network Security Controls.

2.1.3 Finanzielle und rechtliche Aspekte

Die Praxis der CSP entspricht den Anforderungen der Norm ETSI EN 319 411-2 [3], Kapitel 6.8 Other Business and Legal Matters.

2.1.4 Weitere organisatorische und operative Aspekte

Die Praxis der CSP entspricht den Anforderungen der Norm ETSI EN 319 411-2 [3], Kapitel 6.9 Other Provisions.

2.2 Verwaltung der Schlüssel

2.2.1 Verwaltung und Verwendung der Schlüssel der CSP

Die CSP muss ihre eigenen Schlüssel entsprechend der Spezifikation ETSI EN 319 411-2 [3], Kapitel 6.5.1 *Key Pair Generation and Installation*, 6.5.2 *Private Key Protection and Cryptographic Module Engineering Controls*, 6.5.3 *Other Aspects of Key Pair Management*, 6.5.4 *Activation Data,* verwalten und verwenden.

2.2.2 Generierung der Schlüssel 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 EN 319 411-2 [3], Kapitel 6.5.1 *Key Pair Generation and Installation,* 6.5.2 *Private Key Protection and Cryptographic Module Engineering Controls,* 6.5.4 *Activation Data,* konform sein.

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

- in einem zertifizierten System gemäss den Anforderungen in Dokument FIPS 140-2 [4] Stufe 3 oder höher ;
- in einem System, das die in Dokument CWA 14169 [5] festgelegten Anforderungen erfüllt, und nach der Prüfstufe EAL 4 der Norm ISO/IEC 15408:2005 [11] geprüft wurde, erweitert um die Versicherungselemente ADV-IMP.2 (*Implementation of the TSF*), AVA-CCA.1 (*vulnerability assessment, covert channel analysis*) und AVA_VLA.1 (*vulnerability assessment, highly resistant*) oder die entsprechenden Versicherungselemente der Norm ISO/IEC 15408-3:2008 [12]
- in einem System, das die in Dokument EN 419211-2 [6], EN 419 211-4 [8] oder EN 419211-5 [9] festgelegten Anforderungen erfüllt, und nach der Prüfstufe EAL 4 der Norm ISO/IEC 15408-3:2008 [12] geprüft wurde, erweitert um die Versicherungselemente AVA_VAN.5 (*Advanced methodical vulnerability analysis*) oder gleichwertige anerkannte Prüfungskriterien im Sicherheitsbereich
- in einem System, das nach der Prüfstufe EAL 4 der Norm ISO/IEC 15408-3:2008 [12] geprüft wurde, erweitert um das Versicherungselement AVA_VAN.5 (*Advanced methodical vulnerability analysis*) oder gleichwertige anerkannte Prüfungskriterien im Sicherheitsbereich; in diesem Fall muss ein Prüfungsgegenstand geliefert werden, der die in den oben genannten Dokumenten festgelegten Anforderungen erfüllt.

2.2.3 Sichere Signatur- und Siegelerstellungseinheiten

a) Die CSP muss den Antragstellerinnen und Antragstellern eines Zertifikats sichere Signatur- und Siegelerstellungseinheiten liefern, die den Mindestanforderungen von Artikel 6 Absatz 2 ZertES [1] entsprechen, oder sicherstellen, dass diese solche verwenden. Mit den folgenden Dokumenten wird die Konformität mit den Anforderungen von Artikel 6 Absatz 2 ZertES [1] sichergestellt:

- CWA 14169 [5]
- EN 419 211-2 [6]
- EN 419 211-3 [7]
- EN 419 211-4 [8]
- EN 419 211-5 [9]
- EN 419 211-6 [10]

Die sicheren Signatur- und Siegelerstellungseinheiten müssen zudem folgende zusätzliche Anforderungen erfüllen:

- Wenn eine im Voraus festgelegte Anzahl aufeinander folgender und inkorrekter Aktivierungsversuche erreicht wurde, muss der Gebrauch des privaten kryptografischen Schlüssels gesperrt werden. Diese Anzahl darf nicht grösser als 4 Versuche für eine PIN-Länge von 6 Zeichen sein. Bei einer längeren PIN kann sie grösser als 4 sein, sofern die vom Entwickler der zertifizierten sicheren Signatur- und Siegelerstellungseinheiten bereitgestellte Dokumentation das vorsieht.
- Die CSP kann einen gesperrten privaten kryptografischen Schlüssel erst freigeben, nachdem sie verifiziert hat, dass der Antrag auf Freigabe von der Schlüsselinhaberin oder vom Schlüsselinhaber stammt.

b) Die Zertifizierung der sicheren Signatur- und Siegelerstellungseinheiten muss für alle unter a) aufgeführten Anforderungen erfolgen:

- gemäss Prüfstufe EAL 4 der Norm ISO/IEC 15408-3:2005 [11], erweitert um die Versicherungselemente ADV-IMP.2 (Implementation of the TSF), AVA-CCA.1 (vulnerability assessment, covert channel analysis) und AVA_VLA.1 (vulnerability assessment, highly resistant), oder
- gemäss Prüfstufe EAL 4 der Norm ISO/IEC 15408-3:2008 [12], erweitert um das Versicherungselement AVA_VAN.5 (Advanced methodical vulnerability analysis).

c) Liefert die CSP sichere Signatur- und Siegelerstellungseinheiten, muss sie diese gemäss der Spezifikation ETSI EN 319 411-2 [3], Kapitel 6.5.1 *Key Pair Generation and Installation,* 6.5.2 *Private Key Protection and Cryptographic Module Engineering Controls* und 6.5.4 *Activation Data,* handhaben.

d) Ein System zur Generierung von elektronischen Signaturen und Siegeln mittels einer Einheit, die sich nicht im Besitz der Zertifikatinhaberin oder dem Zertifikatinhaber befindet, gilt als sichere Signaturerstellungseinheit im Sinne von Artikel 6 ZertES [1], wenn sie den Anforderungen der Norm CEN/TS 419241 [13] entspricht. Das System muss die Authentifizierung der Inhaberin oder des Inhabers des privaten kryptografischen Schlüssels gemäss der in der Norm CEN/TS 419241 [13] beschriebenen Stufe 2 (*Level 2 sole control*) gewährleisten.

2.3 Verwaltung geregelter Zertifikate

2.3.1 Ausstellung, Verwaltung und Ungültigerklärung geregelter Zertifikate für Dritte

a) Die CSP muss die Antragstellerinnen und Antragsteller eines Zertifikats registrieren und die Zertifikate entsprechend der Spezifikation ETSI EN 319 411-2 [3], Kapitel 6.1 *Publication and Repository Responsibilities*, 6.2 *Identification and Authentication,* 6.3 *Certificate Life-Cycle Operational Requirements*, verwalten und für ungültig erklären.

b) Die CSP muss das Zertifikat für ungültig erklären, wenn die die Berufsbefähigung bestätigende Stelle nach Kapitel 2.3.2 Buchstabe h sie informiert, dass die Bestätigung nicht mehr gültig ist.

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

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

e) Die Suspendierung von Zertifikaten ist nicht erlaubt.

2.3.2 Format von geregelten Zertifikaten

a) Die CSP muss geregelte Zertifikate von natürlichen Personen entsprechend der Norm ETSI EN 319 412-2 [15] generieren.

b) Die CSP muss geregelte Zertifikate von UID-Einheiten entsprechend der Norm ETSI EN 319 412-3 [16] generieren.

c) Die CSP muss geregelte Zertifikate, die sich auf Websites beziehen, gemäss der Norm ETSI EN 319 412-4 [17] generieren.

d) Der Hinweis "*regulated certificate*" gibt an, dass es sich um ein geregeltes Zertifikat handelt, und muss gemäss der Norm RFC 5280 [19] Kapitel 4.2.1.4, im Feld *explicitText* der Erweiterung *certificatePolicies* enthalten sein.

e) Die einheitliche Unternehmens-Identifikationsnummer im Sinne des UIDG muss bei den UID-Einheiten gemäss der Norm ETSI EN 319 412-1 [14], Kapitel 5.1.4, angegeben werden.

f) Das Bit 1 (*contentCommitment*) der Erweiterung *keyUsage* darf nur für geregelte Zertifikate von natürlichen Personen aktiviert werden.

g) In geregelten Zertifikaten, die sich auf einen Signatur- oder Siegelprüfschlüssel beziehen, muss der Hinweis, dass der private kryptografische Schlüssel durch eine sichere Signatur- und Siegelerstellungseinheit geschützt ist, in Form eines Objektbezeichners (OID) gemäss der Norm ETSI EN 319 412-5 [18], Kapitel 4.2.2, angegeben sein.

h) Wenn eine berufliche Befähigung im geregelten Zertifikat erwähnt werden muss, muss entsprechend dem Dokument RFC 5280 [19], Kapitel 4.2, der Sequenz *tbsCertificate* das Attribut *Admission* hinzugefügt werden.

Die Stelle, die eine berufliche Befähigung bestätigt (Art. 5 Abs. 2 VZertES [2]), muss im Datenfeld *admissionAuthority* gemäss dem Dokument Common PKI Specification [20], Tabelle 29b, als *directoryName* mit den folgenden Attributen in der folgenden Reihenfolge benannt werden:
- *organizationName*: Name der Stelle
- *countryName*: Land der Stelle
- *postalAddress*: Adresse der Stelle

Das geregelte Zertifikat darf nur eine berufliche Befähigung beinhalten. Die berufliche Befähigung der Zertifikatsinhaberin oder des Zertifikatsinhabers muss durch Verwendung des Datenfeldes *professionItems* in der Sequenz *professionInfo* gemäss dem Dokument Common PKI Specification [20], Tabelle 29b, definiert werden.
Zusätzlich muss die OID der beruflichen Befähigung im Datenfeld *professionOID* der Sequenz *professionInfo* gemäss dem Dokument Common PKI Specification [20], Tabelle 29b, definiert werden.

i) Gegebenenfalls wird das Attribut *title* des Feldes *subject* gemäss dem Dokument RFC 5280 [19], Kapitel 4.1.2.6, explizit verwendet, um anzugeben, dass die Inhaberin oder der Inhaber des geregelten Zertifikats befugt ist, die mit dem Attribut *organization* im selben Feld *subject* bezeichnete UID-Einheit zu vertreten.

j) Gegebenenfalls wird der Geltungsbereich, für den das geregelte Zertifikat vorgesehen ist, in der Zertifizierungspolitik umschrieben, die in der Erweiterung *certificatePolicies* gemäss dem Dokument RFC 5280 [19], Kapitel 4.2.1.5, festgelegt ist.

k) Der Hinweis Obergrenze der Transaktionen wird gegebenenfalls gemäss Norm ETSI EN 319 412-5 [18], Kapitel 4.3.2, angegeben.

2.3.3 Zusätzliche Anforderungen an das Format qualifizierter Zertifikate

a) Die CSP muss qualifizierte Zertifikate gemäss der Norm ETSI EN 319 412-2 [15] generieren.

b) Nur das Bit 1 (*contentCommitment*) der Erweiterung *keyUsage* darf verwendet werden.

c) Der Hinweis "*qualified certificate*" gibt an, dass es sich um ein qualifiziertes Zertifikat handelt, und muss gemäss der Norm RFC 5280 [19], Kapitel 4.2.1.4, im Feld *explicitText* der Erweiterung *certificatePolicies* angegeben sein. Das Zertifikat enthält ausserdem die in Kapitel 4.2.3 der Norm ETSI EN 319 412-5 [18] beschriebene Erklärung.

2.3.4 Verwaltung des für die Ausstellung geregelter Zertifikate verwendeten Zertifikats der CSP

a) Die CSP muss ihre eigenen geregelten Zertifikate gemäss der Norm IETF RFC 5280 [19] generieren.

b) Der Hinweis "*regulated certificate*" gibt an, dass es sich um ein geregeltes Zertifikat handelt, und muss gemäss Kapitel 4.2.1.4 der Norm RFC 5280 [19] im Feld *explicitText* der Erweiterung *certificatePolicies* angegeben sein.

c) Die einheitliche Unternehmens-Identifikationsnummer im Sinne des UIDG muss gemäss der Norm ETSI EN 319 412-1 [14], Kapitel 5.1.4, angegeben werden.

2.4 Qualifizierter Zeitstempel

a) Um eine Bestätigung zur Feststellung der Existenz von digitalen Daten zu einem bestimmten Zeitpunkt auszustellen, muss die CSP auf ein qualifiziertes Datierungssystem zurückgreifen, das der Spezifikation ETSI EN 319 421 [21] entspricht.

b) Das qualifizierte Datierungssystem muss Zeitstempel erzeugen, die dem Dokument ETSI EN 319 422 [22] entsprechen.

Biel/Bienne, den 23. November 2016

BUNDESAMT FÜR KOMMUNIKATION

Philipp Metzger
Direktor