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 2: 17. Februar 2022
Inkrafttreten: 15. März 2022

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 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 anbietet, 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
Bundesgesetz 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 V2.4.1 (2021-11)
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) / FIPS 140-3 (2019)
Security Requirements for Cryptographic Modules

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

[6] EN 419211-3:2014
Protection profiles for secure signature creation device. Part 3: Device with key import

[7] 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

[8] 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

[9] 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

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

[11] ETSI TS 119 431-1 V1.2.1 (2021-05)
Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

[12] EN 419241-1:2018
Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements

[13] EN 419241-2:2019
Protection Profile for QSCD for Server Signing

[14] EN 419221-5:2018
Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services

[15] ETSI TS 119 461 V1.1.1 (2021-07)
Policy and security requirements for trust service components providing identity proofing of trust service subjects

[16] ETSI EN 319 412-1 V1.4.4 (2021-05)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

[17] ETSI EN 319 412-2 V2.2.1 (2020-07)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[18] ETSI EN 319 412-3 V1.2.1 (2020-07)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[19] ETSI EN 319 412-4 V1.2.1 (2021-11)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

[20] ETSI EN 319 412-5 V2.3.1 (2020-04)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[21] CA/Browser-Forum Guidelines for the Issuance and Management of Extended Validation Certificates, Version 1.7.8

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

[23] T7 Common PKI Specifications for Interoperable Applications. Version 2.0 – 20 January 2009

[24] 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

[25] 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
Guidelines for the Issuance and Management of Extended Validation Certificates	CAB Forum https://cabforum.org/

1.3 Abkürzungen

CEN	*Comité européen de normalisation* – Europäisches Komitee für Normung
CP	*Certification Policy* – Zertifizierungspolitik
CPS	*Certification Practice 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 Infrastructure* – 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	Bundesgesetz 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 Practice Statement and Certificate Policies* und 7 *Framework for the definition of other certificate policies built on the present document.*

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 Norm 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 Norm ETSI EN 319 411-2 [3], Kapitel 6.5.1 *Key Pair Generation and Installation,* und 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 oder gemäss den Anforderungen in Dokument FIPS 140-3 [4] Stufe 3 oder höher;
- in einem System, das die in Dokument EN 419211-2 [5], EN 419211-4 [7] oder EN 419211-5 [8] festgelegten Anforderungen erfüllt und nach der Prüfstufe EAL 4 der Norm ISO/IEC 15408-3:2008 [10], erweitert um die Versicherungselemente AVA_VAN.5 (*Advanced methodical vulnerability analysis*), oder gemäss gleichwertigen anerkannten Prüfungskriterien im Sicherheitsbereich geprüft wurde;
- in einem System, das nach der Prüfstufe EAL 4 der Norm ISO/IEC 15408-3:2008 [10], erweitert um das Versicherungselement AVA_VAN.5 (*Advanced methodical vulnerability*

analysis), oder gemäss gleichwertigen anerkannten Prüfungskriterien im Sicherheitsbereich geprüft wurde; 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 zur Verfügung stellen, 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] gewährleistet:

- EN 419211-2 [5]
- EN 419211-3 [6]
- EN 419211-4 [7]
- EN 419211-5 [8]
- EN 419211-6 [9]

b) Die Zertifizierung der sicheren Signatur- und Siegelerstellungseinheiten muss für alle unter a) aufgeführten Anforderungen gemäss Prüfstufe EAL 4 der Norm ISO/IEC 15408-3:2008 [10], erweitert um das Versicherungselement AVA_VAN.5 (*Advanced methodical vulnerability analysis*), erfolgen.

c) Stellt die CSP sichere Signatur- und Siegelerstellungseinheiten zur Verfügung, muss sie diese gemäss der Norm ETSI EN 319 411-2 [3], Kapitel 6.5.1 *Key Pair Generation and Installation* 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 des Zertifikatinhabers befindet, gilt als sichere Signaturerstellungseinheit im Sinne von Artikel 6 ZertES [1], wenn sie:

- die Anforderungen der Spezifikation ETSI TS 119 431-1 [11] erfüllt, wenn sie als Teil eines Dienstes verwendet wird, der den Inhaberinnen und Inhabern von geregelten Zertifikaten zur Verfügung gestellt wird;
- den Anforderungen der Norm EN 419241-1 [12] entspricht und die Authentifizierung der Inhaberin oder des Inhabers des privaten kryptografischen Schlüssels gemäss der in dieser Norm beschriebenen Stufe 2 (*Sole control assurance level 2*, SCAL2) gewährleistet, und
- ein kryptografisches Modul entsprechend den Anforderungen der Norm EN 419221-5 [14] und ein Signaturaktivierungsmodul entsprechend den Anforderungen der Norm EN 419241-2 [13] enthält, die beide nach der Prüfstufe EAL 4 der Norm ISO/IEC 15408-3:2008 [10], erweitert um die Versicherungselemente AVA_VAN.5 (*Advanced methodical vulnerability analysis*), geprüft wurden, oder ein kryptografisches Modul und ein Signaturaktivierungsmodul enthält, die ähnliche Sicherheitsziele wie jenen der Normen EN 419221-5 [14] und EN 419241-2 [13] erfüllen.

e) Wurde ein privater kryptografischer Schlüssel für die Nutzung gesperrt, darf die CSP diese erst freigeben, nachdem sie sich vergewissert hat, dass der Antrag auf Freigabe von der Schlüsselinhaberin oder dem Schlüsselinhaber stammt.

2.3 Verwaltung geregelter Zertifikate

2.3.1 Ausstellung, Verwaltung und Ungültigerklärung geregelter Zertifikate

a) Die CSP muss die Antragstellerinnen und Antragsteller eines Zertifikats entsprechend der Norm ETSI EN 319 411-2 [3], Kapitel 6.2 *Identification and Authentication,* und entsprechend den allgemeinen Anforderungen der Spezifikation ETSI TS 119 461 [15], Kapitel 5 *Operational risk assessment*, 6 *Policies and practices* und 7 *Identity proofing service management and operatio*n registrieren. Darüber hinaus gelten die spezifischen Anforderungen von Kapitel 9.1 *Use cases for identity proofing to Baseline LoIP – Introduction* und die folgenden Kapitel der Spezifikation ETSI TS 119 461 [15]:

- für die Ausstellung eines geregelten Zertifikats auf eine natürliche Person (Art. 5 sowie 7 Abs. 1 und 3 VZertES [2]): Kapitel 9.2 *Use cases for identity proofing of natural person*, mit Ausnahme von Kapitel 9.2.4 *Use case for identity proofing by authentication using eID means*, sowie die einschlägigen Anforderungen von Kapitel 8, auf die verwiesen wird; betreffend Kapitel 9.2.5 *Use Case for identity proofing using digital signature with certificate*: Es werden nur qualifizierte elektronische Signaturen im Sinne von Artikel 2 Buchstabe e ZertES [1] in dem in Artikel 7 Absatz 3 Buchstabe b VZertES [2] vorgesehenen Fall akzeptiert, und nur die Anforderung COL-8.2.5-01, auf die in der Anforderung USE-9.2.5-02 verwiesen wird, sowie die Anforderungen VAL-8.3.5-01 und VAL-8.3.5-02, auf die in der Anforderung USE-9.2.5-03 verwiesen wird, sind anwendbar;
- die Ausstellung eines geregelten Zertifikats auf eine natürliche Person, die eine UID-Einheit vertritt (Art. 5 und 7 Abs. 1 VZertES [2]), oder auf eine UID-Einheit, die keine natürliche Person ist (Art. 6 und 7 Abs. 1 und 3 VZertES [2]): Kapitel 9.4 *Use case for identity proofing of natural person representing legal person* sowie die einschlägigen Anforderungen von Kapitel 8, auf die verwiesen wird; zur Überprüfung der Identität der natürlichen Person, die die Ausstellung des geregelten Zertifikats beantragt, gilt Kapitel 9.2 *Use cases for identity proofing of natural person* sowie die einschlägigen Anforderungen von Kapitel 8, auf die verwiesen wird, mit Ausnahme von Kapitel 9.2.4 *Use case for identity proofing by authentication using eID means*; betreffend Kapitel 9.2.5 *Use case for identity proofing using digital signature with certificate*: Es werden nur qualifizierte elektronische Signaturen im Sinne von Artikel 2 Buchstabe e ZertES [1] in dem in Artikel 7 Absatz 3 Buchstabe a VZertES ([2]) genannten Fall und unter den dort und in Artikel 6 VZertES [2]) festgelegten Bedingungen akzeptiert.

b) Ausländische Identitätskarten, die für die Einreise in die Schweiz anerkannt werden, sind im vom Staatssekretariat für Migration (SEM) veröffentlichten Dokument «Übersicht der Ausweis- und Visumvorschriften nach Staatsangehörigkeit[1]» (Anhang CH-1, Liste 1) mit «ID» bezeichnet. Um zu überprüfen, ob es sich bei dem von der Antragstellerin oder dem Antragsteller eines Zertifikats vorgelegten Dokument um einen Reisepass oder eine Identitätskarte handelt, muss die CSP auf eine offizielle Quelle zurückgreifen, in der die Besonderheiten und Sicherheitsmerkmale von Identitätsdokumenten beschrieben werden, wie z. B. auf das öffentliche Online-Register echter Identitäts- und Reisedokumente PRADO[2].

c) Die CSP muss die Zertifikate entsprechend der Norm ETSI EN 319 411-2 [3], Kapitel 6.1 *Publication and Repository Responsibilities*, 6.3 *Certificate Life-Cycle Operational Requirements*, verwalten und für ungültig erklären.

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

e) Die CSP, die ein Zertifikat für ungültig erklärt, muss die ihr vorliegenden Informationen über den Status dieses Zertifikats aktualisieren.

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

g) 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 [17] generieren.

b) Die CSP muss geregelte Zertifikate von UID-Einheiten entsprechend der Norm ETSI EN 319 412-3 [18] generieren.

c) Die CSP muss geregelte Zertifikate, die sich auf Websites beziehen, gemäss der Norm ETSI EN 319 412-4 [19] generieren.

d) Der Hinweis «*regulated certificate*» gibt an, dass es sich um ein geregeltes Zertifikat handelt, und muss gemäss dem Dokument RFC 5280 [22], Kapitel 4.2.1.4, im Feld *explicitText* der Erweiterung *certificatePolicies* enthalten sein. Das Zertifikat enthält ausserdem die in Kapitel 4.2.1

[1] https://www.sem.admin.ch > Publikationen & Service > Weisungen und Kreisschreiben > VII. Visa > Ausweis- und Visumvorschriften nach Staatsangehörigkeit (Anhang CH-1, Liste 1)

[2] https://www.consilium.europa.eu/de > Dokumente und Veröffentlichungen > PRADO > Suche nach Land des Dokuments

der Norm ETSI EN 319 412-5 [20] genannte Erklärung (*statement*) sowie die in Kapitel 4.2.4 der Norm ETSI EN 319 412-5 [20] beschriebene Erklärung (*statement*). In der letztgenannten Erklärung (*statement*) muss der Ländercode «CH» aufgeführt sein.

e) Falls das Attribut *surname* in einem auf eine natürliche Person ausgestellten geregelten Zertifikat verwendet wird, muss es den vollständigen Namen enthalten, wie er im Identitätsdokument oder im qualifizierten Zertifikat angegeben ist, die zum Nachweis der Identität der Antragstellerin oder des Antragstellers eines Zertifikats herangezogen werden.

f) Falls das Attribut *givenname* in einem auf eine natürliche Person ausgestellten geregelten Zertifikat verwendet wird, muss es sämtliche Vornamen enthalten, wie sie im Identitätsdokument oder im qualifizierten Zertifikat angegeben sind, welche zum Nachweis der Identität der Antragstellerin oder des Antragstellers eines Zertifikats herangezogen werden.

g) Die einheitliche Unternehmens-Identifikationsnummer im Sinne des UIDG muss bei den UID-Einheiten gemäss der Norm ETSI EN 319 412-1 [16], Kapitel 5.1.4, angegeben werden. In Übereinstimmung mit dieser Norm muss der Nummer die Zeichenfolge «NTRCH-» vorangestellt werden.

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

i) 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 [20], Kapitel 4.2.2, angegeben sein.

j) Wenn eine berufliche Befähigung im geregelten Zertifikat erwähnt werden muss, muss entsprechend dem Dokument RFC 5280 [22], Kapitel 4.2, der Sequenz *tbsCertificate* die Erweiterung *Admission* gemäss dem Dokument Common PKI Specification [23], Tabelle 29b, 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 [23], Tabelle 29b, als *directoryName* mit den unten aufgeführten 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 [23], Tabelle 29b, definiert werden.
   Zusätzlich muss die OID der beruflichen Befähigung im Datenfeld *professionOID* der Sequenz *professionInfo* gemäss dem Dokument Common PKI Specification [23], Tabelle 29b, definiert werden.

k) Gegebenenfalls wird das Attribut *title* des Feldes *subject* gemäss dem Dokument RFC 5280 [22], 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.

l) 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 [22], Kapitel 4.2.1.4, festgelegt ist.

m) Der Hinweis zur Obergrenze der Transaktionen wird gegebenenfalls gemäss der Norm ETSI EN 319 412-5 [20], Kapitel 4.3.2, angegeben.

2.3.3 Zusätzliche Anforderungen an das Format qualifizierter Zertifikate

Für qualifizierte Zertifikate gelten zusätzlich zu den Kapiteln 2.3.1 und 2.3.2 die folgenden Formatanforderungen:

a) Die CSP muss qualifizierte Zertifikate gemäss der Norm ETSI EN 319 412-2 [17] generieren.

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

c) Der Hinweis «*qualified certificate*» gibt an, dass es sich um ein qualifiziertes Zertifikat handelt, und muss gemäss dem Dokument RFC 5280 [22], Kapitel 4.2.1.4, im Feld *explicitText* der Erweiterung *certificatePolicies* angegeben sein. Das Zertifikat enthält ausserdem die in Kapitel 4.2.1 der Norm ETSI EN 319 412-5 [20] genannte Erklärung (*statement*) sowie die in Kapitel 4.2.4 der Norm ETSI EN 319 412-5 [20] beschriebene Erklärung (*statement*). In der letztgenannten Erklärung (*statement*) muss der Ländercode «CH» aufgeführt sein.

2.3.4 Zusätzliche Anforderungen an das Format der auf Behörden ausgestellten geregelten Zertifikate

Für geregelte Zertifikate, die auf Behörden ausgestellt werden, gelten zusätzlich zu den Kapiteln 2.3.1 und 2.3.2 die folgenden Formatanforderungen:

a) In geregelten Zertifikaten, die an Behörden ausgestellt werden, muss die Bezeichnung der Behörden im Feld *OrganizationalUnit* angegeben sein. Dieses Feld muss als *utf8String* nach dem folgenden Schema kodiert sein:

- für Behörden auf Bundesebene:
GE\x{20}\x{2D}\x{20}0220\x{20}\x{2D}\x{20}**\w{3,40}**

wobei **GE** für die Kurzform von *Government Entity* und **\w{3,40}** für das Amtskürzel als alphanumerische Zeichenkette mit 3 bis max. 40 Zeichen (UTF-8) steht; die maximale Länge des Feldes gemäss obiger Definition beträgt 52 Zeichen;

- für Behörden auf kantonaler Ebene:
GE\x{20}\x{2D}\x{20}0221\x{20}\x{2D}\x{20}**[A-Z]{2}**\x{20}\x{2D}\x{20}**\w{3,40}**

wobei **GE** für die Kurzform von *Government Entity*, **[A-Z]{2}** für das zweistellige Kantonskürzel gemäss dem Amtlichen Gemeindeverzeichnis der Schweiz des Bundesamtes für Statistik (BFS)[3] und **\w{3,40}** für das Amtskürzel als alphanumerische Zeichenkette mit 3 bis max. 40 Zeichen (UTF-8) steht; die maximale Länge des Feldes gemäss obiger Definition beträgt 47 Zeichen;

- für Behörden auf Bezirksebene:
GE\x{20}\x{2D}\x{20}0222\x{20}\x{2D}\x{20}**[A-Z]{2}**\x{20}\x{2D}\x{20}**\d{5,6}**\x{20}\x{2D}\x{20}**\w{3,39}**

wobei **GE** für die Kurzform von *Government Entity*, **[A-Z]{2}** für den Sitzkanton als zweistelliges Kantonskürzel gemäss dem Amtlichen Gemeindeverzeichnis der Schweiz des Bundesamtes für Statistik (BFS)[4], **\d{5,6}** für die fünf- bis sechsstellige Historisierungsnummer der Sitzgemeinde gemäss dem Amtlichen Gemeindeverzeichnis der Schweiz des Bundesamtes für Statistik (BFS) und **\w{3,39}** für das Amtskürzel als alphanumerische Zeichenkette mit 3 bis max. 39 Zeichen (UTF-8) steht; die maximale Länge des Feldes gemäss obiger Definition beträgt 64 Zeichen;

- für Behörden auf kommunaler Ebene:
GE\x{20}\x{2D}\x{20}0223\x{20}\x{2D}\x{20}**\d{5,6}**\x{20}\x{2D}\x{20}**\w{3,40}**

wobei **GE** für die Kurzform von *Government Entity*, **\d{5,6}** für die fünf- bis sechsstellige Historisierungsnummer der Gemeinde gemäss dem Amtlichen Gemeindeverzeichnis der Schweiz des Bundesamtes für Statistik (BFS)[5] und **\w{3,40}** für das Amtskürzel als alphanumerische Zeichenkette mit 3 bis max. 40 Zeichen (UTF-8) steht; die maximale Länge des Feldes gemäss obiger Definition beträgt 60 Zeichen.

[3] https://www.bfs.admin.ch/bfs/de/home/grundlagen/agvch.html
[4] https://www.bfs.admin.ch/bfs/de/home/grundlagen/agvch.html
[5] https://www.bfs.admin.ch/bfs/de/home/grundlagen/agvch.html

Falls kein offizielles Amtskürzel existiert, wird die offizielle Bezeichnung der Behörde bis zur maximalen Feldlänge verwendet.

b) Falls das Feld *businessCategory* (OID: 2.5.4.15) gemäss den Richtlinien des CA/Browser-Forums *Guidelines for the Issuance and Management of Extended Validation Certificates* [21] in einem geregelten Behörden-Zertifikat verwendet wird, muss es den Hinweis «*Government Entity»* enthalten.

2.3.5 Verwaltung der für die Ausstellung geregelter Zertifikate verwendeten Zertifikate der CSP

Die Kapitel 2.3.1 und 2.3.2 gelten nicht für geregelte Zertifikate, die die CSP auf sich selbst ausstellt. Für solche Zertifikate gelten die folgenden Anforderungen:

a) Die CSP muss ihre eigenen geregelten Zertifikate gemäss dem Dokument RFC 5280 [22] generieren.

b) Der Hinweis «*regulated certificate»* gibt an, dass es sich um ein geregeltes Zertifikat handelt, und muss gemäss dem Dokument RFC 5280 [22], Kapitel 4.2.1.4, im Feld *explicitText* der Erweiterung *certificatePolicies* enthalten sein.

c) Die einheitliche Unternehmens-Identifikationsnummer im Sinne des UIDG muss gemäss der Norm ETSI EN 319 412-1 [16], Kapitel 5.1.4, angegeben werden. In Übereinstimmung mit dieser Norm muss der Nummer die Zeichenfolge «NTRCH-» vorangestellt werden.

d) Die CSP muss ihre Zertifikate gemäss der Norm ETSI EN 319 411-2 [3], Kapitel 6.5.1 *Key Pair Generation and Installation*, verwalten.

2.4 Qualifizierter Zeitstempel

a) Zur Ausstellung einer Bestätigung, wonach digitale Daten zu einem bestimmten Zeitpunkt existiert haben, muss die CSP auf ein qualifiziertes Datierungssystem zurückgreifen, das der Norm ETSI EN 319 421 [24] entspricht.

b) Das qualifizierte Datierungssystem muss Zeitstempel erzeugen, die dem Dokument ETSI EN 319 422 [25] entsprechen.

3 Umsetzungsfristen

- Die CSP müssen die Anforderungen nach den Kapiteln 2.3.2 Buchstabe d und 2.3.3 Buchstabe c bis spätestens 15. Juni 2022 umsetzen; bis zu diesem Datum bleiben die entsprechenden Anforderungen nach den Kapiteln 2.3.2 Buchstabe d und 2.3.3 Buchstabe c der ersten Ausgabe der technischen und administrativen Vorschriften vom 23. November 2016 anwendbar.
- Die CSP müssen die Anforderungen nach den Kapiteln 2.3.2 Buchstabe g und 2.3.5 Buchstabe c bis spätestens 15. Juni 2022 umsetzen; bis zu diesem Datum bleibt die im selben Kapitel der referenzierten Norm erwähnte Alternative anwendbar.
- Die CSP müssen die Anforderungen nach Kapitel 2.3.4 bis spätestens 15. Juni 2022 umsetzen.
- Die CSP müssen die Anforderungen nach Kapitel 2.2.3 Buchstabe d bis spätestens 15. September 2022 umsetzen; bis zu diesem Datum bleibt die entsprechende Anforderung nach Kapitel 2.2.3 Buchstabe d der ersten Ausgabe der technischen und administrativen Vorschriften vom 23. November 2016 anwendbar.

Biel/Bienne, den 17. Februar 2022

BUNDESAMT FÜR KOMMUNIKATION

Bernard Maissen
Direktor