Konzept geregeltes Zertifikat ausgestellt für eine Behörde / Zusammenarbeit mit dem eGov Signaturvalidator

Auftraggeber	BK-DTI
Projektleiter	Peter von Dach /D. Buffat
Autoren	D. Buffat, M. Caduff, I. Metz, P. von Dach
Klassifizierung	Nicht klassifiziert, **Intern,** Vertraulich, GEHEIM
Status	In Arbeit, in Prüfung, **Genehmigt**
Version	1.5

Änderungsverzeichnis

Datum	Version	Änderung	Autor
24.11.2016	0.1	erstellt	D. Buffat, ISB
16.01.2017	0.2	Input J. Böhlen, ISB	D. Buffat, ISB
09.02.2017	0.3	Input TAV	D. Buffat, ISB
11.04.2017	0.4	Input SwissSign	D. Buffat, ISB
24.05.2017	0.5	Version zum Review ISB, BIT	D. Buffat, ISB
19.06.2017	0.6	Version Review CSP	D. Buffat, ISB
15.08.2017	0.9	Version zur Prüfung	D. Buffat, ISB
24.08.2017	0.91	Input BIT PKI	D. Buffat ISB
05.09.2017	0.92	Input BAKOM	D. Buffat ISB
05.09.2017	0.93	Input SwissSign	D. Buffat ISB
05.09.2017	0.94	Version zur Prüfung	D. Buffat ISB
02.08.2018	0.95	Präzisierungen	I. Metz
21.08.2018	0.96	Input Swiss Gov PKI	I. Metz
21.08.2018	0.961	Version Review ISB	P. von Dach ISB
05.10.2018	0.97	Input BJ (Ch. Bloch & St. Jau)	I. Metz
14.03.2019	0.98	Input BAKOM und SG-PKI des BIT («Synthese-Dokument»)	P. von Dach ISB, I. Metz
19.05.2019	0.99x	Input BAKOM und SG-PKI des BIT	I. Metz
30.12.2019	1.0	Einarbeitung Feedback QuoVadis	P. von Dach ISB

Datum	Version	Änderung	Autor
27.04.2021	1.1	Aktualisieren der Versionen von Normen und Standards in Kap. 6	P. von Dach BK-DTI
12.01.2022	1.2	Aktualisieren der Versionen von Normen und Standards in Kap. 6 im Rahmen Vernehmlassung der TAV	P. von Dach BK-DTI
29.01.2024	1.3	Vereinfachungen	M. Caduff, I. Metz
09.02.2024	1.3x	Ergänzungen Alte Textpassagen überarbeitet	BK-DTI
04.03.2024	1.4x	Vor-Finalisierung Version 1	Dominik Kornacki BK-DTI, BAKOM
09.04.2024	1.5	Final	BAKOM, BK-DTI

Inhaltsverzeichnis

1 Zweck des Dokumentes

Im ZertES, VZertES und TAV liegen keine rechtlich verbindlichen Grundlagen vor, um das Zertifikat einer Behörde von einem Zertifikat einer anderen UID-Einheit zu unterscheiden. Damit im Validator eine elektronische Signatur in geeigneter Form überprüft und zudem untersucht werden kann, ob das Zertifikat von einer Behörde stammt, braucht es im Zertifikat eine eindeutige Kennung.

Der Validator soll einerseits die Einhaltung von (gesetzlichen) Vorgaben überprüfen und andererseits für die Nutzer (Personen, welche ein amtlich gesiegeltes Dokument prüfen wollen) eine verständliche Aussage machen, welche Behörde das Dokument gesiegelt hat. Solche Werkzeuge sind sehr wichtig, um das Vertrauen in die elektronische Signatur, bzw. die elektronischen Siegel zu fördern. Dadurch werden letztlich auch die Bestrebungen hinsichtlich E-Government unterstützt.

Das vorliegende Dokument ist ein Konzept für die Ausgestaltung von Zertifikaten von Behörden. Teile dieses Dokumentes werden Eingabe finden in gesetzliche Grundlagen beziehungsweise in weiteren Dokumenten. Diese sind:

- Die revidierte TAV (TAV - Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate)
- Erläuterungen zur TAV
- Wegleitung für Behörden zur Nutzung des Validators.

2 Ausgangslage

Dokumente und Daten werden mit der laufenden Entwicklung der Büroautomation immer häufiger elektronisch ausgetauscht. Dies zeigt sich zunehmend mit Transaktionen, die mit drei Zeichen abgekürzt werden wie B2B, B2C, C2G, G2C, G2G, G2B, B2G, C2C. Dabei werden die Abkürzungen G2G, G2B, B2G, G2C und C2G in der Regel mit E-Government umschrieben, also der Beziehung der Administration zu den Bürgern und zur Privatwirtschaft.

Schnell ist eine Offerte, eine Rechnung oder ein Bericht etc. auf dem PC erstellt und via E-Mail dem Partner zugestellt. Auch im «Behörden zu Bürger» Verkehr (C2G, G2C) werden immer öfter elektronische Dokumente ausgetauscht. Da behördliche Dokumente in der Regel wichtige Informationen enthalten, besteht das Bedürfnis, die Herkunft und die Integrität (Unveränderthеit) der Dokumente überprüfbar zu machen. Dies wird mit einer elektronischen Signatur der Dokumente gewährleistet.

Um dies zu ermöglichen, wurde im Auftrag vom Bundesamt für Justiz (BJ) eine erste Version eines Signatur-Validators erstellt. In Mandanten erlaubte dieser eine elektronische Signatur von behördlichen Dokumenten zu überprüfen. Dabei wurde die Gültigkeit des elektronischen Zertifikates zum Zeitpunkt des Signierens, die Berechtigung, das vorgelegte Dokument mit dem elektronischen Zertifikat zu signieren und die Unversehrtheit des Dokumentes geprüft. Das Resultat dieser Prüfung konnte in einem (elektronisch signierten) Report dokumentiert werden.

Im Rahmen des E-Government Strategie Schweiz wurde ein neuer eGov Signaturvalidator entwickelt. Mit diesem können auch Urkunden und elektronisch signierte Dokumente von Verwaltungsstellen der Kantone und Gemeinden der Schweiz validiert werden.

Basierend auf dem aktuell gültigen ZertES [1] und der dazu gehörenden VZertES [2], können geregelte Zertifikate für juristische Personen und UID-Einheiten (Behörden) ausgestellt

werden. Die für eine UID Einheit (Behörde) ausgestellte geregelten Zertifikate ermöglichen Behörden, Dokumente in ihrem Namen rechtsverbindlich elektronisch zu signieren. Das geregelte Siegel ist das Ergebnis des Signaturvorgangs.

In der ZertES (Art. 2 Abs. d.) wird das geregelte elektronische Siegel wie folgt definiert:

„Geregeltes elektronisches Siegel: Eine fortgeschrittene elektronische Signatur, die unter Verwendung einer sicheren Siegelerstellungseinheit nach Artikel 6 erstellt wurde und auf einem geregelten, auf eine UID-Einheit nach Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 20103 über die Unternehmens-Identifikationsnummer (UIDG) ausgestellten und zum Zeitpunkt der Erzeugung des elektronischen Siegels gültigen Zertifikat beruht.“

Zu beachten ist, dass ein geregeltes Zertifikat ausgestellt für eine Behörden nur ausgestellt werden kann, wenn die entsprechende Behörde einen UID-Eintrag besitzt.

3 Geregeltes Zertifikat ausgestellt für eine Behörde (Behördensiegel)

Behörden (Verwaltungsstellen) sollen mit einem geregelten Zertifikat ausgestellt für eine Behörde zusammen mit einem qualifizierten Zeitstempel (ZertES Art 2j) Dokumente elektronisch signieren respektive siegeln können. Bis jetzt mussten amtliche Dokumente mittels persönlicher qualifizierter elektronischer Signatur von Mitarbeitern signiert werden. Neu können Behörden amtliche Dokumente mit einem geregelten elektronischen Zertifikat (Siegel) versehen werden. Dies kann zu signifikanten Vereinfachungen im Behördenverkehr untereinander aber auch im Verkehr zu Unternehmen und Bürgern führen.

Es ist eine Zielsetzung von e-Government, solche Bürger - Behörden Beziehungen zu fördern indem amtliche Dokumente überprüft werden können.

Bestandteil der Prüfung sind unter anderem die kryptografischen Prüfungen wie die Prüfung der Unversehrtheit des Dokumentes als auch die Gültigkeit des Zertifikats zum Zeitpunkt des Signierens des Dokumentes.

Damit der Validator signierte respektive gesiegelte Behördendokument eindeutig überprüfen kann, müssen im verwendeten Zertifikat (siehe dazu Kap. 3.2) und im signierten Dokument (siehe dazu Kap. 4) maschinenlesbare Informationen enthalten sein.

3.1 Aufbau eines Zertifikates nach X.509

Ein elektronisches Zertifikat weist gemäss X.509 (Standards für PKI) [29] eine Struktur mit den folgenden Bestandteilen auf:

```
Version
Seriennummer
Signaturalgorithmus
Aussteller
Zeitliche Gültigkeit
Antragsteller (Subject nach [18])
Öffentlicher Schlüssel-Algorithmus
Länge des öffentlichen Schlüssels
Öffentlicher Schlüssel
```

und weiteren Informationen.

Der Besitzer des Zertifikates wird im Abschnitt Antragsteller definiert. Der Antragsteller wird in Form eines „Distinguished Name“ gemäss X.509 beschrieben.

Die Attribute für den Distinguished Name (DN) sind in der ITU-T X.520 im Kapitel 6.4 „*Organizational attribute types*“ beschrieben und in der TAV [4] für die Schweiz präzisiert.

Ein Zertifikat, das ZertES konform ausgestellt worden ist, enthält im Abschnitt Antragsteller die notwendigen Informationen, um den Inhaber eindeutig zu bezeichnen.

Damit bei einer automatisierten Prüfung des Siegels eines elektronisch signierten Dokumentes die ausstellende Behörde eindeutig bestimmen kann, werden gewisse Anforderungen an den Inhalt des Abschnittes Antragsteller (=Subject) (=“Distinguished Name“ DN) gestellt.

In der TAV [4] wird in Art 2.3.2b das Format von geregelten Zertifikaten von UID-Einheiten vorgeschrieben. Dabei wird auf die ETSI Norm EN 319 412-3 [18] verwiesen.

Dies heisst für die Behördenzertifikate, dass

- die Behörde im UID-Register[1] registriert sein muss und damit über eine UID Nummer verfügt
- im Feld `OrganizationName (O)` der Name wie im UID-Register hinterlegt wird
- im Feld `OrganizationIdentifier (OI)` die UID Nummer der Behörde hinterlegt wird
- im Feld `OrganizationalUnit (OU)` eine Behörden-Identifikationsnummer hinterlegt wird
- im Feld `businessCategory (OID)` das Zertifikat der Kategorie Behörde zugeordnet wird

3.2 Vorgaben für den Distinguished Name im Zertifikat

3.2.1 Übersicht[2]

Ein Zertifikat, das ZertES konform ausgestellt worden ist, enthält im Abschnitt Antragsteller (=“Distinguished Name“ DN) die notwendigen Informationen, um den Inhaber eindeutig zu bezeichnen.

In der folgenden Tabelle sind Pflichtfelder gemäss TAV grau hinterlegt, die in diesem Dokument spezifizierten Felder zur Identifikation einer Behörde sind gelb hinterlegt.

Beschreibung	RDN	Inhalt
`OrganizationName`	**O**	Der O muss mit dem Namen im UID-Register übereinstimmen. *Dieses Feld ist obligatorisch.*
`OrganizationIdentifier`	**OI**	UID Nummer der ausstellenden Behörde (gemäss UID-G) im von ZertES verlangten Format. *Dieses Feld ist obligatorisch.*

[1] https://www.uid.admin.ch/

[2] Aus diesem Abschnitt kommt der Teil betreffend die Felder OrganizationalUnit OU_{n+1} und businessCategory in die TAV. Die restlichen Felder sind von der TAV beziehungsweise der referenzierten Normen schon abgehandelt.

Beschreibung	RDN	Inhalt
CommonName	**CN**	Allgemein gebräuchlicher Name der Verwaltungsstelle. Der Name muss für den Empfänger des elektronisch gesiegelten Dokumentes sprechend sein und wird bei einer automatisierten Prüfung eines elektronisch gesiegelten Dokumentes ggf. in einem Prüfberichtbericht aufgeführt. *Dieses Feld ist obligatorisch.*
OrganizationalUnit	**$OU_{n=1..2}$**	Nähere Bezeichnung der Organisationseinheit (Departement, Abteilung, etc.), die dem Zertifikat zugeordnet ist. Es können bis zu 2 OU Felder angegeben werden *Diese Felder sind optional.*
OrganizationalUnit	**OU_{n+1}**	Behörden-Identifikation: GE – Rechtsform der UID Einheit *Dieses Feld ist obligatorisch.*
businessCategory	**OID: 2.5.4.15**	Dieses Feld enthält die Zeichenkette "Government Entity" *Dieses Feld ist obligatorisch.*
Locality	**L**	Bezeichnung der Gemeinde, in der die Behörde gemäss dem Eintrag im UID-Register Sitz hat. *Dieses Feld ist optional.*
State/Province	**ST**	Bezeichnung des Kantons in der die Behörde gemäss dem Eintrag im UID-Register. *Dieses Feld ist optional.*
CountryName	**C**	Länderkürzel nach ISO 3166-1. Es bezeichnet das Land der unter dem RDN „O“ bezeichneten Behörde. → „CH“ für die Schweiz. *Dieses Feld ist obligatorisch.*
SubjectAltName	2.5.29.17 rfc822Name	rfc822Name (E-Mail-Adresse). E-Mail-Adresse, die bei einer automatisierten Prüfung eines elektronisch gesiegelten Dokumentes ggf. in einem Prüfbericht aufgeführt wird, um die Auskunftstelle für den signierten Dokumententyp anzuzeigen. *Dieses Feld ist optional.*

3.2.2 Mehrsprachigkeit in den Zertifikaten

In einigen Anwendungsfällen wird die Mehrsprachigkeit der Felder `Organization`, `CommonName` und `OrganizationalUnit` in den Zertifikaten gewünscht. Die ETSI Norm [5] weist zwar darauf hin, dass die Beschränkung der Feldlänge auf 64 Zeichen nur noch für das Feld `CountryName` gilt. Um Inkompatibilitäten bei Software, die noch von 64 Zeichen ausgeht, zu verhindern, sollten für den Anwendungsfall der Mehrsprachigkeit die Felder `Organization`, `CommonName` und `OrganizationalUnit` nicht in allen Sprachvarianten befüllt werden. Stattdessen sollen pro Sprache unterschiedliche Zertifikate ausgestellt werden.

3.2.3 Details[3]

`OrganizationName (O)`:

Als Inhalt für das Feld muss der Name (bzw. die Übersetzung) der Verwaltungseinheit im UID-Register zur entsprechenden UID Nummer gewählt werden.

`OrganizationIdentifier (OI)`:

Gemäss ZertES, Art 7e muss eine Unternehmens-Identifikationsnummer gemäss UIDG [1] im Zertifikat enthalten sein. Die TAV schreibt vor, dass die UID Nummer im Feld „`OrganizationIdentifier`“ hinterlegt wird. Die CSP sind verpflichtet, diese Angabe zu überprüfen.

Als Inhalt für das Feld ist „NTRCH-CHE-nnn.nnn.nnn“ zu wählen, wobei „CHE-nnn.nnn.nnn“ die UID-Nummer der UID-Einheit bezeichnet.

`CommonName (CN)`:

Hier ist der allgemein gebräuchliche Name der Behörde einzutragen. Z.B. Staatskanzlei des Kantons Bern; Kantonale Verwaltung Zug; Verwaltungsgericht Freiburg; Bezirksverwaltung Appenzell, Liegenschaften & Betriebe (DS14); Gemeindeverwaltung Bellach.

Die Information im `CommonName` wird bei einer automatisierten Prüfung eines elektronisch gesiegelten Dokumentes ggf. in einem Prüfberichtbericht als Name der ausstellenden Behörde aufgeführt.

`OrganizationalUnit (OU`$_{n=1..2}$`)`:

Name der Behörde, die entsprechende Dokumente ausstellt (Departement, Amt, Gericht…).

`OrganizationalUnit (OU`$_{n+1}$`)`:

Dieses Feld enthält die Rechtsform der schweizerischen Behörde gemäss UID-Register. Damit kann automatisiert festgestellt werden, dass das Zertifikat einer Behörde zuzuordnen ist, und dass damit signierte Dokumente somit von einer schweizerischen Behörde stammen. Für Zertifikate von UID-Einheiten, die keine schweizerische Behörde sind, darf kein OU-Feld erstellt werden, das mit ‘GE -‘, gefolgt von einem Code, beginnt. Die Rechtsformen, die als schweizerische Behörde gelten, sind abschliessend definiert (vgl. unten).

Dieses Feld wird als utf8String kodiert und identifiziert die Behörde nach dem folgenden Schema (regulärer Ausdruck in Perl-Syntax):

^GE\x{20}\x{2D}\x{20}(0117|02\d{2})$

wo GE für die Kurzform von Government Entity, \x{20} für das ISO-8859-1 ASCII Zeichen mit hexadezimalem Wert 0x20 (Space), \x{2D} für das ISO 8859-1 Zeichen mit hexadezimalem Wert 0x2D (Hyphen-Minus) und (0117|02\d{2}) für den vierstelligen Code der Rechtsform der UID-Einheit. Zulässige Rechtsform sind: 0117[4] und alle mit Präfix 02 gemäss eCH-0097 [31]. Die maximale Länge des Feldes gemäss obiger Definition beträgt 9 Zeichen.

[3] In die TAV wird vom BAKOM nur der Teil des Abschnittes übernommen werden, der das für die Behördenidentifikation genutzte Feld spezifiziert.

[4] Ausstellung der Behördenzertifikate für Rechtsformen 0117 beschränkt sich auf die «Rechtlich verselbstständigte Körperschaften, Anstalten und Stiftungen» laut Anhang des RVOV unter dem jeweiligen Departements Kapitel. (https://www.fedlex.admin.ch/eli/cc/1999/170/de#annex_1)

Beispiele:
GE - 0220
bezeichnet die Verwaltung des Bundes, z.B. das Bundesamt für Justiz

GE - 0117
bezeichnet ein Institut des öffentlichen Rechts, z.B. das Institut für Geistiges Eigentum.

`businessCategory (OID: 2.5.4.15):`
Bezeichnung der Geschäftskategorie. Gemäss [32] kann dieses Feld eine der folgenden Zeichenketten enthalten: "Private Organization", "Government Entity", "Business Entity" oder "Non-Commercial Entity". Für Behörden muss, falls das Feld vorhanden ist, die Zeichenkette "Government Entity" verwendet werden. Als Behörden gelten dabei UID-Einheiten mit den unter OU_{n+1} definierten Codes. Andere UID-Einheiten dürfen den Inhalt «Government Entity» nicht enthalten.

`Locality (L):`
Bezeichnung der Gemeinde gemäss dem Amtlichen Gemeindeverzeichnis der Schweiz des BFS [27], in der die Behörde gemäss dem Eintrag im UID-Register den Sitz hat.

`State/Province (ST):`
Bezeichnung des Kantons gemäss dem Amtlichen Gemeindeverzeichnis der Schweiz des BFS [27], in der die Behörde gemäss dem Eintrag im UID-Register den Sitz hat.

`SubjectAltName` (2.5.29.17, rfc822Name):
Diese E-Mail-Adresse wird bei einer automatisierten Prüfung eines elektronisch gesiegelten Dokumentes ggf. in einem Prüfberichtbericht aufgeführt, um die Auskunftstelle für den signierten Dokumententyp anzuzeigen. Diese Adresse wird vom Antragsteller definiert und muss vom CSP verifiziert werden.

Beispiel:

```
CN=Gesetzestexte des Kantons Bern
O=Staatskanzlei des Kantons Bern
OU=Staatskanzlei
OU=Bern
OU = GE - 0221
2.5.4.15 = Government Entity
L=Bern
ST=Bern
C=CH
OI=NTRCH-CHE-105.620.392
2.5.29.17: Kennzeichen = 0, Länge = xx
Alternativer Antragstellername
   RFC822-Name= info@sta.be.ch
```

3.2.4 Verwendungszweck der Felder in den Zertifikaten

Die Inhalte der einzelnen Felder in den Zertifikaten werden für unterschiedliche Zwecke verwendet. Das in der nachfolgenden Tabelle gelb hinterlegte Feld dient bei einer automatisierten Prüfung dazu, ein mit einem Zertifikat elektronisch gesiegeltes Dokument anhand des Inhaltes des Feldes als von einer schweizerischen Behörde stammend zu qualifizieren. Die grau hinterlegten Felder haben einen informativen Charakter für Menschen, die eine elektronische Signatur analysieren. Diese Felder werden bei einer automatisierten Prüfung eines elektronisch gesiegelten Dokumentes ggf. in einem Prüfberichtbericht als zusätzliche Information aufgeführt.

Beschreibung	RDN	Verwendungszweck
`OrganizationName`	**O**	Zur Information.
`OrganizationIdentifier`	**OI**	Zur Information.
`CommonName`	**CN**	Zur Information.
`OrganizationalUnit`	**$OU_{n=1..2}$**	Zur Information.
`OrganizationalUnit`	**OU_{n+1}**	Massgeblich für die automatisierte Zuordnung zu einer Behörde.
`businessCategory`	**2.5.4.15**	Für die Kennzeichnung, dass das Zertifikat für ein Behörde ausgestellt wurde.
`Locality`	**L**	Zur Information.
`State/Province`	**ST**	Zur Information.
`CountryName`	**C**	Zur Information.
`SubjectAltName`	2.5.29.17 rfc822Name	Zur Information.

4 Vorgaben für signierte Dokumente

Mit der Verwendung der Behörden-Identifikationsnummer (`OrganizationalUnit`, **OU_{n+1}**) als Feld im Zertifikat kann bei einer automatisierten Prüfung anhand des Inhaltes des Feldes ein Dokument als von einer schweizerischen Behörde stammend qualifiziert werden. Zusammen mit weiteren Feldern (insb. OI) kann die konkrete Behörde identifiziert werden.

Um ein Dokument einem konkreten Prozess innerhalb dieser Behörde zuzuordnen, kann die Behörde beim Signiervorgang eine Prozess-Identifikation in die Signatur des PDF-Dokumentes einfügen. Dazu soll der Eintrag ‘Reason’ im Signature Dictionary des PDF-Dokumentes (siehe [30], p. 467, Tabelle 252) verwendet werden.

Es ist die Verantwortung der Behörde, sicherzustellen, dass die Prozess-Identifikation *innerhalb der Behörde* eindeutig verwendet wird. Eindeutigkeit kann etwa erreicht werden, wenn als Bezeichner beispielsweise die ID der Leistung gemäss eCH-0070 (Leistungsinventar eGov CH [28]) gewählt wird.

Der alleinige Inhalt dieses Eintrags ist ISO 8859-1 kodiert (siehe [30], Kap. 7.9.2.2) und nach dem folgenden Schema (regulärer Ausdruck) definiert:

^Process\x{20}\x{2D}\x{20}[0-9A-Za-z-]{1,36}$

wo \x{20} für das ISO 8859-1 Zeichen mit hexadezimalem Wert 0x20 (Space) und \x{2D} für das ISO 8859-1 Zeichen mit hexadezimalem Wert 0x2D (Hyphen-Minus) steht.

Beispiele:

Process - Strafregister

Process - 204[5]

Process - 1c7aed48-adff-4dcd-a510-84ebdf4b273b

5 Anforderungen an die Certificate Service Provider (CSP)

5.1 Anforderungen an die CSP

Der CSP hat die folgenden Überprüfungen vor der Ausstellung des geregelten Behördenzertifikates durchzuführen:

- Gemäss ZertES Art 9, 1b wird vom Antragsteller persönliches Erscheinen gefordert. Es ist ein Nachweis sowohl für die eigene Identität (Pass oder Identitätskarte) als auch für die Vertretungsvollmacht zu erbringen.
- Vertretungsvollmacht auf Gültigkeit überprüfen:
  Mit der Einsichtnahme in das UID-Register im Internet beziehungsweise anhand des vom BFS beglaubigten aktuellen Auszugs soll überprüft werden, ob die Bezeichnung der UID-Einheit und die im Zertifikat anzugebende UID übereinstimmen (Art. 7 Abs. 2 Bst. c und e ZertES). Es geht also nicht darum, die Vertretungsbefugnisse der Person zu kontrollieren, die ein geregeltes Zertifikat für eine UID-Einheit beantragt. Diese Befugnisse müssen mit einer schriftlichen Vollmacht begründet werden, sofern sie nicht im Handelsregister eingetragen sind (Art. 6 Abs. 1 Satz 2 VZertES). Zu diesem Thema wird im erläuternden Bericht zur Totalrevision der VZertES folgendes festgehalten (aus dem Französischen übersetzt):

  Bei nicht im Handelsregister eingetragenen UID-Einheiten müssen die Anbieterinnen von Fall zu Fall beurteilen, ob das Gesuch um Ausstellung eines Zertifikates von den berechtigten Personen unterzeichnet worden ist. Bei Behörden können die Anbieterinnen in der Regel davon ausgehen, dass die internen Vorschriften bezüglich der Zeichnungsberechtigungen eingehalten wurden. Dennoch kann von den Anbieterinnen verlangt werden, die Online-Verzeichnisse des Bundes, der Kantone und der Gemeinden zu konsultieren.

  Zur Überprüfung der Vertretungsbefugnisse der Person, die die Ausstellung eines geregelten Zertifikates für eine Behörde beantragt, gibt es kein Instrument, das mit dem Handelsregister vergleichbar ist. Die Zeichnungsberechtigungen sind nämlich nicht in

[5] 204 ist die ID für die Leistung «Strafregisterauszug – ausstellen» gemäss eCH-0070 [28]

den Verzeichnissen des Bundes, der Kantone und der Gemeinden, sondern in nicht öffentlichen internen Regelungen festgelegt. Daher ist es nicht möglich, ein präziseres Überprüfungsverfahren für die Behörden vorzusehen.
➔ In Kap. 5.2 wird aufgezeigt, wie die CSP diese Informationen verifizieren können.

- UID Nummer und UID Eintrag im UID-Register mit den vorliegenden Angaben des Antragstellers überprüfen.
- Der Eintrag im Feld `CommonName` wird als Referenz für die Bezeichnung der Behörde des signierten Dokuments verwendet und ist im Dokument bei Verwendung sichtbarer Signaturen ersichtlich. Der CSP überprüft, dass dieser Name für den Empfänger des Dokumentes präzise und verständlich ist.
- Im Feld OU_{n+1} wird die Rechtsform der Behörde gemäss Kapitel 3.2 identifiziert. Der CSP prüft die vom Antragsteller gelieferte Bezeichnung auf Plausibilität. Alle zur Plausibilitätsprüfung erforderlichen Informationen sind dem UID Eintrag im UID-Register zu entnehmen.
- Wenn der Antragsteller im Feld `SubjectAltName` E-Mail-Adressen eingetragen haben will, so muss der CSP diese Adressen auf ihre Gültigkeit prüfen.

5.2 Hilfsmittel für die Überprüfung durch die CSP

Die Angaben für die Behörden können dem UID-Register (https://www.uid.admin.ch) entnommen werden:

- Offizieller Name der Behörde sowie die offiziellen Übersetzungen des Namens
- Die Rechtsform ist dem UID-Eintrag unter 'Weitere Identifikationsmerkmale > Rechtsform' zu entnehmen. Als Behörde gelten UID-Einheiten mit folgenden Codes für die Rechtsform: 0117, alle beginnend mit 02.

Das Handelsregister gibt bei Verwaltungen und Behörden keine Auskunft über die Zeichnungsberechtigten. Dazu müssen andere Hilfsmittel beigezogen werden.

Über den Link https://www.ch.ch/de/sicherheit-und-recht/behordenadressen können die aktuellen Verzeichnisse der Behörden aufgerufen werden. Mit den folgenden Beispielen sollen Hinweise gegeben werden, wie die zeichnungsberechtigte Person gefunden werden kann. Die in den Beispielen aufgeführten Namen entsprechen dem Stand vom 25.01.2024.

Antragsteller	Weg zur zeichnungsberechtigten Person
Mitarbeiter Bundeskanzlei	https://www.ch.ch/de/behordenadressen/ ➔ Adressen der Bundesbehörden ➔ Staatskalender ➔ Bundeskanzlei →Stab Bundeskanzler → Leiter (Andres Ledergerber)
Mitarbeiter Amt für Informatik und Organisation Zug	https://www.ch.ch/de/behordenadressen/ ➔ Adressen der kantonalen Behörden -> Zug ➔ Organisationen → Kantonale Verwaltung → Finanzdirektion → Amt für Informatik und Organisation → Leitung → Amtsleiter (Stephan Arnold)
Staatskanzlei des Kantons Bern	https://www.ch.ch/de/behordenadressen/ ➔ Adressen der kantonalen Behörden → Bern ➔ Teilbereiche → Staatskanzlei ➔ Staatsschreiber (Christoph Auer)

Antragsteller	Weg zur zeichnungsberechtigten Person
Mitarbeiter der Direktion für Finanzen, Personal und Informatik Stadt Bern	https://www.ch.ch/de/behordenadressen/ ➔ Adressen der Gemeindeverwaltungen → Bern → www.bern.ch ➔ Politik und Verwaltung → Behördenverzeichnis → Direktion für Finanzen, Personal und Informatik
Mitarbeiter Gemeindever-waltung Wileroltigen	https://www.ch.ch/de/behordenadressen/ ➔ Adressen der Gemeindeverwaltungen → www.wileroltigen.ch ➔ Politik & Behörde → Gemeinderat → Verzeichnis der gewählten Exekutive

6 Referenzen und weiterführende Literatur

[1] SR 943.03 ZertES: Gesetz vom 18. März 2016 über die elektronische Signatur (Stand 1.1.2017)

[2] SR 943.032 VZertES: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES) vom 23. November 2016 (Stand 1.1.2017)

[3] BBL 2014 1001 Botschaft zur Totalrevision des Bundesgesetzes über die elektronische Signatur ZertES vom 15.1.2014

[4] SR 943.032.1 TAV - Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23.11.2016 (Stand 1.1.2017)

[5] 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

[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] RFC 5280 (Mai 2008) Internet X.509 Public Key Infrastructure - Certificate and CRL Profile Common PKI Specifications for Interoperable Applications. Version 2.0 – 20 January 2009

[22] 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

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

[24] ITU-T X.520 Recommendation ITU-T X.520 (2019-10): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types"

[25] ETSI TS 102 853 V1.2.1 (2014-12) Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies

[26] SR 172.010.1 Regierungs- und Verwaltungsorganisationsverordnung (RVOV) vom 25. November 1998 (Stand vom 1. Januar 2022)

[27] Amtliches Gemeindeverzeichnis der Schweiz, https://www.bfs.admin.ch/bfs/de/home/grundlagen/agvch.html

[28] eCH-0070: Leistungsinventar eGov CH, Version 4.1.0, Publiziert am 04.03.2021. https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0070

[29] X509: Public-Key Cryptography Standards (PKCS) #1 RSA Cryptography Specifications Version 2.2 (2016-11) [RFC8017].

https://www.rfc-editor.org/rfc/pdfrfc/rfc8017.txt.pdf

[30] Document management — Portable document format — Part 1: PDF 1.7. First Edition 2008-7-1.
https://www.adobe.com/content/dam/acom/en/devnet/pdf/pdfs/PDF32000_2008.pdf

[31] eCH-0097: Datenstandard Unternehmensidentifikation, Version 5.2.0, Publiziert am 02.07.2021.
https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0097

[32] CA/Browser Forum: Guidelines For The Issuance And Management Of Extended Validation Certificates. Version 1.7.5, 05. April 2021.
https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.7.5.pdf