Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
**Eidgenössische Steuerverwaltung ESTV**

SR 641.201.511.1 / Anhang

Technische und administrative Vorschriften

für

# Zertifizierungsdienste im Bereich der ElDI-V im Zusammenhang mit der Ausstellung von Zertifikaten basierend auf fortgeschrittenen Signaturen

Ausgabe 2: 14. Dezember 2009
ersetzt Ausgabe 1 vom 12. Oktober 2007
Inkrafttreten: 1. Januar 2010

Eigerstrasse 65
3003 Bern
www.estv.admin.ch

## Inhaltsverzeichnis


1 Allgemeines ..... 3
1.1 Gesetzliche Grundlagen und Geltungsbereich ..... 3
1.2 Referenzen ..... 3
1.3 Abkürzungen ..... 4
1.4 Definitionen ..... 5
2 Anerkennung der CSP ..... 5
3 Grundlegende Anforderungen ..... 5
3.1 Grundsatz ..... 5
3.2 Organisation und operative Grundsätze ..... 5
3.3 Verwaltung der Schlüssel ..... 6
3.3.1 Verwaltung der Schlüssel der CSP ..... 6
3.3.2 Generierung des Schlüssels der Antragstellerin ..... 6
3.3.3 Sichere Signaturerstellungseinheiten ..... 6
3.4 Verwaltung der Zertifikate ..... 7
3.4.1 Registrierung, Verwaltung und Ungültigerklärung von Zertifikaten für Dritte ..... 7
3.4.2 Format der Zertifikate für Inhaberinnen ..... 7
3.4.3 Verwaltung des Zertifikats der CSP für die unter diesen TAV ausgestellten Zertifikate ..... 9
4 Namensgebung der Inhaberin ..... 10
4.1 Zertifikatsdatenfelder ..... 10
4.1.1 Allgemeines ..... 10
4.1.2 Benennung der Organisation ..... 12
4.2 Überprüfung der Angaben in den Zertifikaten ..... 13
4.2.1 Überprüfung der Angaben über natürliche Personen ..... 13
4.2.2 Überprüfung der Angaben über Organisationen ..... 13
4.2.3 Überprüfung der Angaben über die Beziehung der natürlichen Person zur Organisation ..... 14
4.2.4 Überprüfung der Zertifikatsdaten ..... 14
5 Verzeichnisdienste für Zertifikate ..... 16
6 Verwendungszweck und Verantwortlichkeiten ..... 17
6.1 Verwendungszweck ..... 17
6.2 Ungültigerklärung von Zertifikaten ..... 17
6.2.1 Pflichten der CSP ..... 17
6.2.2 Pflichten der Zertifikatsinhaberin ..... 17
6.3 Verantwortlichkeiten ..... 17
7 Kennzeichnung eines ElDI-V Zertifikats ..... 18
7.1 Allgemeines ..... 18
7.2 CPS ..... 18


Begriffe, die eine weibliche und eine männliche Form aufweisen können, werden in diesem Dokument nicht unterschieden, sondern in der einen oder anderen Form verwendet. Sie sind somit als gleichwertig zu betrachten.

# 1 Allgemeines

## 1.1 Gesetzliche Grundlagen und Geltungsbereich

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

- das Bundesgesetz über die Mehrwertsteuer (MWSTG) [1]
- die Mehrwertsteuerverordnung (MWSTV) [2]
- die Verordnung des EFD über elektronische Daten und Informationen (ElDI-V) [3]
- das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) [4]
- die Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES) [5]
- die Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur [6]

Soweit als nötig und zulässig präzisieren sie die in Gesetz [1] und Verordnungen [2], [3] definierten Voraussetzungen und grundlegenden Anforderungen, die eine anerkannte Anbieterin von Zertifizierungsdiensten (CSP) erfüllen muss, die elektronische Zertifikate [3] ausstellt oder andere Dienste im Bereich der elektronischen Signaturen [3] anbietet.

Die Anerkennung einer CSP wird in Kapitel 2 beschrieben.

## 1.2 Referenzen


[1] SR 641.20, MWSTG

Bundesgesetz vom 12. Juni 2009 über die Mehrwertsteuer

[2] SR 641.201, MWSTV

Mehrwertsteuerverordnung vom 27. November 2009

[3] SR 641.201.511, ElDI-V

Verordnung des EFD vom 11. Dezember 2009 über elektronische Daten und Informationen

[4] SR 943.03, ZertES

Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur

[5] SR 943.032, VZertES

Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur

[6] SR 943.032.1

Verordnung vom 6. Dezember 2004 des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur, Ausgabe 3 vom 13. November 2006

[7] FIPS 140-1 (11.1.94)

Security Requirements for Cryptographic Modules

[8] FIPS 140-2 (25.5.01)

Security Requirements for Cryptographic Modules

[9] RFC 3280 (April 2002)

Internet X.509 Public Key Infrastructure - Certificate and CRL Profile

[10] 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

[11] ITSEC Version 1.2 (28. Juni 1991)

Information Technology Security Evaluation Criteria

[12] ISO/IEC 15408:2005

Information technology – Security techniques. Evaluation criteria for IT security

[13] ISO/IEC 6523-1:1998

Information technology - Structure for the identification of organizations and organization parts - Part 1: Identification of organization identification schemes

[14] RFC 4043 (Mai 2005)

Internet X.509 Public Key Infrastructure - Permanent Identifier

[15] SR 220, OR

Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)

Die Dokumente können bei den in Kapitel 1.2 TAV-ZertES [6] aufgeführten Organisationen bezogen werden.

Diese TAV können unter www.estv.admin.ch heruntergeladen werden oder sind unter folgender Adresse erhältlich:

| | |
|---|---|
| Technische und administrative Vorschriften (SR 641.201.511.1 / Anhang) | Bundesamt für Bauten und Logistik<br>3003 Bern<br>http://www.bbl.admin.ch |

## 1.3 Abkürzungen

| | |
|---|---|
| BAKOM | Bundesamt für Kommunikation |
| CPS | Certification practice statement |
| CSP | Certification Service Provider |
| DN | Distinguished Name |
| EFD | Eidgenössisches Finanzdepartement |
| EJPD | Eidgenössisches Justiz- und Polizeidepartment |
| ElDI-V | Verordnung des EFD über elektronische Daten und Informationen [3] |
| ESTV | Eidgenössische Steuerverwaltung |
| FIPS | Federal Information Processing Standards |
| ICD | International Code Designator |
| ISO | International Standardization Organization |
| ITSEC | Information Technology Security Evaluation Criteria |
| ITU-T | International Telecommunication Union. Telecommunication Standardization Sector |

| | |
|---|---|
| MWSTG | Bundesgesetz über die Mehrwertsteuer [1] |
| MWSTV | Mehrwertsteuerverordnung [2] |
| OelDI | Ordonnance du DFF concernant les données et informations électroniques / Ordinanza del DFF concernente dati ed informazioni elettronici / Ordinance of the FDF on Electronic Data and Information |
| OID | Object Identifier |
| RDN | Relative Distinguished Name |
| RFC | Request for Comments |
| SR | Systematische Rechtssammlung |
| TAV | Technische und administrative Vorschriften |
| TAV-ZertES | die Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur [6] |
| VZertES | Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur [5] |
| ZertES | Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur [4] |

## 1.4 Definitionen

In diesen TAV bedeuten:

*sinngemäss:* Für nach diesen TAV ausgegebene Zertifikate gleichwertig anwendbare Bestimmungen wie sie für qualifizierte Zertifikate nach der TAV-ZertES [6] gelten.

*Zertifikat:* Zertifikat, das die Anforderungen von Artikel 2 Absatz 2 ElDI-V [3] erfüllt und unter den Bestimmungen dieser TAV ausgegeben wird.

# 2 Anerkennung der CSP

Eine CSP, die Zertifikate nach den Bestimmungen dieser TAV ausgibt, muss im Verzeichnis der anerkannten Anbieterinnen nach Artikel 5 ZertES [4] mindestens nach allen Normen von ZertES [4], VZertES [5] und TAV-ZertES [6] eingetragen sein.

# 3 Grundlegende Anforderungen

## 3.1 Grundsatz

Diese TAV stützen sich auf die TAV-ZertES [6] und ergänzen diese um die Anforderungen und Bestimmungen für die Ausstellung, Verwaltung und Verwendung von Zertifikaten im Bereich der ElDI-V [3].

Für die Ausgabe von Zertifikaten nach diesen TAV muss die CSP die gleichen organisatorischen und operativen Verfahren anwenden sowie die gleiche technische Infrastruktur nutzen wie für die Ausgabe von qualifizierten Zertifikaten nach ZertES [4].

## 3.2 Organisation und operative Grundsätze

Es gelten die in der TAV-ZertES [6] Kapitel 3.2 aufgeführten Bestimmungen. Ausgenommen solche, die mit den in Kapitel 3.5 TAV-ZertES [6] genannten Diensten in Zusammenhang ste-

hen. Dokumente, die für Zertifikatsinhaber von Bedeutung sind, sind in einer Amtssprache abzufassen. Zusätzlich zu den in den TAV-ZertES [6] Kapitel 3.2 Abschnitt c) aufgeführten Dokumenten muss die CSP die folgenden Dokumente in die jährlich durchzuführenden, internen Audits über die Konformität ihrer Aktivitäten einbeziehen:

- ElDI-V [3]
- diese TAV

Die bei den jährlichen internen Audits festgestellten Mängel sind zu beheben (Ergänzung zu den Ausführungen unter Kapitel 3.2 Abschnitt d) der TAV-ZertES [6]).

Auf Verlangen sind der ESTV die Prüfberichte einschliesslich aller referenzierten Dokumente einzureichen.

## 3.3 Verwaltung der Schlüssel

### 3.3.1 Verwaltung der Schlüssel der CSP

Die in der TAV-ZertES [6], Kapitel 3.3.1 aufgeführten Bestimmungen gelten sinngemäss.

### 3.3.2 Generierung des Schlüssels der Antragstellerin

a) In den Fällen, in denen die CSP selber das Schlüsselpaar der Antragstellerin generiert, gelten die in der TAV-ZertES [6], Kapitel 3.3.2 Abschnitt a) aufgeführten Bestimmungen sinngemäss.

b) In den Fällen, in denen die CSP selber das Schlüsselpaar der Antragstellerin generiert, gelten die in der TAV-ZertES [6], Kapitel 3.3.2 Abschnitt b) aufgeführten Bestimmungen sinngemäss.

c) In den Fällen, in denen die Antragstellerin eines Zertifikats ihr Schlüsselpaar selber generiert, muss die CSP technisch, oder, falls technisch nicht möglich, organisatorisch sicherstellen, dass Letzteres in einer sicheren Signaturerstellungseinheit generiert wurde, wie sie in Kapitel 3.3.3 dieses Dokuments definiert ist.

### 3.3.3 Sichere Signaturerstellungseinheiten

a) Alle Operationen, die im Zusammenhang mit dem Signaturschlüssel eines ElDI-V [3] konformen Zertifikates stehen, dürfen ausschliesslich innerhalb einer sicheren Signaturerstellungseinheit erfolgen. Der Signaturschlüssel darf für Backupzwecke in gesicherter Weise exportiert werden, sofern der Signaturschlüssel gleichwertig geschützt ist wie in der sicheren Signaturerstellungseinheit und ausgeschlossen werden kann, dass er ausserhalb dieser genutzt werden kann.

   Die sicheren Signaturerstellungseinheiten müssen zudem folgende zusätzliche Anforderungen erfüllen:

   - Sie dürfen den zu signierenden Inhalt nicht ändern;
   - Das Zertifikat (oder der eindeutige Verweis auf dieses Zertifikat) muss im System vorhanden sein;
   - Der dem 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 Freigabe eines gesperrten Schlüssels setzt ein Verfahren voraus, bei dem die Eingabe von korrekten Aktivierungsdaten erforderlich ist.

b) Die Zertifizierung der sicheren Signaturerstellungseinheit muss
   - entweder die Zertifizierung nach FIPS 140-1 [7] oder FIPS 140-2 [8] Stufe 3 oder höher umfassen,
   - oder die Prüfstufe EAL 4 der Norm ISO/IEC 15408:2005 [12] 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 [11] umfassen.

c) Es gelten die in der TAV-ZertES [6], Kapitel 3.3.3 Abschnitt c) aufgeführten Bestimmungen.

## 3.4 Verwaltung der Zertifikate

### 3.4.1 Registrierung, Verwaltung und Ungültigerklärung von Zertifikaten für Dritte

Die in der TAV-ZertES [6], Kapitel 3.4.1 aufgeführten Bestimmungen gelten sinngemäss.

### 3.4.2 Format der Zertifikate für Inhaberinnen

a) Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt a) aufgeführten Bestimmungen.

b) Entsprechend Artikel 2 Absatz 2 Buchstabe a ElDI-V [3] und dem Dokument RFC 3280 [9], Kapitel 4.1, muss die CSP der Sequenz tbsCertificate folgende Felder hinzufügen:

| Beschreibung | Feld | Inhalt |
|---|---|---|
| Version | version | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt b) aufgeführten Bestimmungen über das Feld „version“. |
| Seriennummer des Zertifikats | serialNumber | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt b) aufgeführten Bestimmungen über das Feld „serialNumber“. |
| Objektbezeichner des Signaturalgorithmus, der für das Signieren des Zertifikats benutzt wurde | signature | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt b) aufgeführten Bestimmungen über das Feld „signature“. |
| Name der CSP<br>Niederlassungs-Staat der CSP | issuer | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt b) aufgeführten Bestimmungen über das Feld „issuer“. |
| Gültigkeitsdauer des Zertifikats | validity | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt b) aufgeführten Bestimmungen über das Feld „validity“. |
| Firma der Inhaberin, und wenn nötig, spezifische Attribute der Inhaberin | subject | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt b) aufgeführten Bestimmungen über das Feld „subject“.<br>Die Namensgebung ist in Kapitel 4 dieser TAV geregelt. |
| Schlüssel und Algorithmus zur Prüfung der Signatur der Inhaberin des Zertifikats | subjectPublicKeyInfo | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt b) aufgeführten Bestimmungen über das Feld „subjectPublicKeyInfo“. |

c) Entsprechend dem Dokument RFC 3280 [9], Kapitel 4.2, muss die CSP der Sequenz tbsCertificate folgende Erweiterungen hinzufügen:

| Beschreibung | Kritische Erweiterung | Name der Erweiterung | Inhalt |
|---|---|---|---|
| Identifikator des Schlüssels der CSP, die das Zertifikat signiert hat | Nein | authorityKeyIdentifier | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt c) aufgeführten Bestimmungen über die Erweiterung „authorityKeyIdentifier“. |
| Identifikator des Schlüssels der Antragstellerin | Nein | subjectKeyIdentifier | Nach dem Dokument RFC 3280 [9], Kapitel 4.2.1.2. |
| Geltungsbereich des Zertifikats | Ja | keyUsage | Nach den Dokumenten ITU-T X.509 [10], Kapitel 8.2.2.3 und RFC 3280 [9], Kapitel 4.2.1.3.<br>▪ Bit Nr. 0 (digitalSignature) setzen, um anzuzeigen, dass das Zertifikat zur Überprüfung der elektronischen Signaturen verwendet wird.<br>▪ Bit Nr. 1 (contentCommitment / nonRepudiation) setzen, um anzuzeigen, dass das Zertifikat zur Nicht-Abstreitbarkeit von getätigten Transaktionen verwendet wird.<br>▪ Das Setzen weiterer Bits ist nicht erlaubt. |
| Zertifizierungspolitik | Nein | certificatePolicies | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt c) aufgeführten Bestimmungen über die Erweiterung „certificatePolicies“.<br>Die Verwendung der Erweiterung „certificatePolicies“ ist in Kapitel 7 dieser TAV geregelt. |
| Verteilungspunkt der Liste der ungültig erklärten Zertifikate | Nein | cRLDistributionPoints | Nach den Dokumenten ITU-T X.509 [10], Kapitel 8.6.2.1 und RFC 3280 [9], Kapitel 4.2.1.14.<br>▪ Ein „DistributionPoint“ muss einen DistributionPointName vom Typ „uniformResourceIdentifier“ unter Verwendung des http Protokolls angeben. Die Felder „reasons“ und „cRLIssuer“ müssen fehlen.<br>▪ Die Angabe von weiteren „DistributionPoints“ ist optional. |
| Zugangspunkt zum Zertifikat der CSP | Nein | authorityInfoAccess | Es gelten die in der TAV-ZertES [6], Kapitel 3.4.2 Abschnitt c) aufgeführten Bestimmungen über die Erweiterung „authorityInfoAccess“. |

d) Entsprechend dem Dokument RFC 3280 [9], Kapitel 4.2, kann die CSP der Sequenz tbsCertificate folgende Erweiterungen hinzufügen:

| Beschreibung | Kritische Erweiterung | Name der Erweiterung | Inhalt |
|---|---|---|---|
| Handelsregister-Identifikationsnummer | Nein | subjectAltName | 0..1, otherName<br>Identifikationsnummer, die allen im Handelsregister eingetragenen Subjekten zugeteilt wird (OR Art. 936a [15]).<br><br>Spezifikation:<br>▪ type-id zuzuweisender OID: 1.3.169. Der ICD 169 [13] unter dem Ast 1 (iso) 3 (identified organization) entspricht nach RFC 4043 Anhang B.3. [14] einem OID.<br>▪ Der OtherName Wert muss ASN-1 PrintableString codiert sein. |
| Email Adresse | Nein | subjectAltName | 0..n, rfc822Name<br>Jede aufgeführte Email-Adresse muss von der CSP überprüft werden. |

Weitere Erweiterungen dürfen an die zuvor aufgeführten Erweiterungen nachfolgend angefügt werden, sofern deren Inhalte von der CSP entsprechend überprüft werden und die Erweiterungen den Bestimmungen des Dokumentes RFC 3280 [9] entsprechen.

### 3.4.3 Verwaltung des Zertifikats der CSP für die unter diesen TAV ausgestellten Zertifikate

a) Die in der TAV-ZertES [6], Kapitel 3.4.3 Abschnitt a) aufgeführten Bestimmungen gelten sinngemäss.

b) Die in der TAV-ZertES [6], Kapitel 3.4.3 Abschnitt b) aufgeführten Bestimmungen gelten sinngemäss.

c) Die in der TAV-ZertES [6], Kapitel 3.4.3 Abschnitt c) aufgeführten Bestimmungen gelten sinngemäss.

d) Für ihr eigenes Zertifikat muss die CSP sicherstellen, dass entsprechend dem Dokument RFC 3280 [9] Kapitel 4.2, die folgenden nicht kritischen Erweiterungen der Sequenz tbsCertificate vorhanden sind:

- authorityKeyIdentifier. Falls es sich um ein selbst signiertes Zertifikat handelt, ist diese Angabe optional;
- subjectKeyIdentifier;
- certificatePolicies;
- cRLDistributionPoints. Falls es sich um ein selbst signiertes Zertifikat handelt und das Feld „cRLIssuer“ nicht verwendet wird, darf diese Erweiterung nicht vorhanden sein.

# 4 Namensgebung der Inhaberin

Den in diesem Kapitel aufgeführten Dokumenten und Bescheinigungen gleichgestellt sind solche des Fürstentums Liechtenstein[1].

| Fürstentum Liechtenstein | Bezeichnung |
|---|---|
| Abkürzung für die Steuerverwaltung. | STV |
| Bestätigung, die der Steuerpflichtige nach erfolgtem Eintrag ins Register der Mehrwertsteuerpflichtigen erhält. | Bescheinigung über die Eintragung ins Mehrwertsteuerregister. |
| Es wird kein amtliches Gemeindeverzeichnis geführt. | Vaduz, Balzers, Planken, Schaan, Triesen, Triesenberg, Eschen, Gamprin, Mauren, Ruggell, Schellenberg |
| Behörde, die eine Wahlverfügung erlässt. | Die öffentlich-rechtlichen Bediensteten werden nicht durch Wahlverfügung gewählt, sondern durch Beschluss der zuständigen Organe angestellt. |

## 4.1 Zertifikatsdatenfelder

### 4.1.1 Allgemeines

Die Zertifikate, die im Rahmen dieser TAV ausgestellt werden, enthalten die folgenden Datenfelder, die im Anschluss an nachstehende Tabelle für verschiedene Wirtschaftssubjekte näher erläutert und durch ein Beispiel veranschaulicht werden. Wie die Angaben in den Datenfeldern bei der Antragstellung auf Richtigkeit überprüft werden, wird im Abschnitt 4.2 zusammengefasst beschrieben.

Unter Wirtschaftssubjekte fallen insbesondere auch die Steuersubjekte nach dem MWSTG [1].

Zertifikate, die an Zertifikatsinhaber ausgegeben werden, die nicht unter die nachfolgenden Regeln für die Namensgebung fallen, müssen auf einen zulässigen Namen des Zertifikatinhabers ausgestellt werden. Zudem muss eine eindeutige Zuordnung möglich sein und eine Verwechslung mit natürlichen und juristischen Personen oder Bezeichnungen von Organisationseinheiten ausgeschlossen werden.

[1] Vertrag vom 28. Oktober 1994 zwischen dem Fürstentum Liechtenstein und der Schweizerischen Eidgenossenschaft betreffend die Mehrwertsteuer im Fürstentum Liechtenstein (SR 0.641.295.142)

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Firma (siehe Abschnitt 4.1.2). |
| Organizational Unit | $OU_{0..n}$ | Nähere Bezeichnung der Organisationseinheit (Filialname, Abteilung, etc.), die dem Zertifikat zugeordnet ist. Es können mehrere OU Felder angegeben werden. |
| Organizational Unit | $OU_{n+1}$ | Falls das Zertifikat für Zwecke nach Artikel 9 ElDI-V [3] eingesetzt wird, ist folgender Eintrag zwingend:<br>▪ **Third Party Services (art. 9 OelDI)**<br>Dritter allgemein nach Artikel 9 ElDI-V<br>Falls das Zertifikat nicht auch tatsächlich für diesen Zweck eingesetzt wird, ist diese Angabe nicht zulässig. |
| Common Name | CN | ▪ **Natürliche Person**<br>Der CN muss den Vornamen und Namen der natürlichen Person beinhalten<br>▪ **Wirtschaftssubjekte**<br>Der CN muss die Angaben vom RDN O enthalten. Zusätzlich kann der CN weitere Angaben enthalten, die den Einsatz des Zertifikates erläutern. |
| Locality | L | Bezeichnung der Gemeinde, in der die Firma den Sitz hat. |
| State/Province | SP | Bezeichnung des Kantons, in dem die Firma den Sitz hat. |
| Country | C | Länderkürzel nach ISO 3166-1. Es bezeichnet das Land des Firmensitzes der unter dem RDN „O“ bezeichneten Firma. |
| EmailAddress | $E_{0..1}$ | 0..1, rfc822Name<br>Die Email-Adresse muss von der CSP überprüft werden. |

Es gelten die Bestimmungen nach RFC 3280 [9], Kapitel 4.1.2.6. Die aufgeführten RDN bilden zusammen das Zertifikatsfeld „subject Distinguished Name“. Weitere RDN, die den Zertifikatsinhaber näher bestimmen, dürfen an die bereits aufgeführten RDN angefügt werden. Die Inhalte müssen von der CSP überprüft werden und dürfen den aufgeführten RDN nicht widersprechen.

Zur Konstruktion dieses Feldes folgendes Beispiel:

```
O=Muster AG/OU=Filiale der Muster AG/OU=e-Services/
OU=Third Party Services (art. 9 OelDI)/CN=Muster AG e-Services/
L=Kloten/SP=Zurich/C=CH/E=info@musterag4711.ch
```

Ein bestimmter „subject Distinguished Name“ darf jeweils nur einer bestimmten Identität (dieser ggf. mehrfach für verschiedene Zertifikate) zugeordnet werden.

Entsprechend den unterschiedlichen Organisationsformen, die ein solches Zertifikat beantragen, sind die obigen Zertifikatsfelder unterschiedlich zu belegen. Der Feldinhalt für die einzelnen Organisationsformen wird nachstehend beschrieben:

## 4.1.2 Benennung der Organisation

### 4.1.2.1 Wirtschaftssubjekte mit Handelsregistereintrag

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Name der Firma nach dem eingereichten Handelsregisterauszug. |

### 4.1.2.2 Einzelfirma (natürliche Person), nicht im Handelsregister eingetragen

Einzelfirma (natürliche Person), die nicht in das Handelsregister eingetragen werden muss. Hier handelt es sich vor allem um die freien Berufe wie z. B. Rechtsanwälte, Notare usw.

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Name der Einzelfirma nach der eingereichten Eintragungsbescheinigung der ESTV. |

### 4.1.2.3 Einfache Gesellschaft, nicht im Handelsregister eingetragen

Die einfache Gesellschaft entsteht durch Vertrag. Deren Mitglieder können sowohl natürliche als auch juristische Personen sein. Die einfache Gesellschaft besitzt keine Rechtspersönlichkeit, wird von der Mehrwertsteuer aber als Steuersubjekt betrachtet. Wichtige Erscheinungsform der einfachen Gesellschaft ist die so genannte Arbeitsgemeinschaft (ARGE) im Bauwesen. Dies ist der vertragliche Zusammenschluss zweier oder mehrerer Baufirmen zur Realisierung eines grösseren Bauprojektes.

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Name der einfachen Gesellschaft nach der eingereichten Eintragungsbescheinigung der ESTV oder nach dem Gesellschaftsvertrag . |

### 4.1.2.4 Gemeinwesen (Gemeinden), nicht im Handelsregister eingetragen

Neben den politischen Gemeinden (Einwohnergemeinden) existieren z.B. auch Bürgergemeinden und Kirchgemeinden. Zur Bestimmung, wer für die Gemeinde handeln kann, ist eine generell abstrakte Aussage nicht möglich. Die Aufsicht über die Gemeinden ist kantonal geregelt und kann von Kanton zu Kanton unterschiedlich sein. Als weitere Besonderheit ist zu beachten, dass bei der Mehrwertsteuer nicht zwingend die Gemeinde als Ganzes, sondern einzelne Dienststellen, die steuerbare Leistungen erbringen, als Mehrwertsteuerpflichtige eingetragen werden.

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Name der Gemeinde nach dem amtlichen Gemeindeverzeichnis. |
| Organizational Unit | OU | Name der Dienststelle nach der eingereichten Eintragungsbescheinigung der ESTV. |

### 4.1.2.5 Andere, nicht im Handelsregister eingetragene, Wirtschaftssubjekte (z. B. Vereine)

Die Benennung richtet sich nach den Regeln wie für Einzelfirmen.

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Name nach der eingereichten Eintragungsbescheinigung der ESTV. |

## 4.2 Überprüfung der Angaben in den Zertifikaten

a) Die CSP müssen von der Antragstellerin, die einen Antrag auf Ausstellung eines Zertifikats im Rahmen dieser Bestimmungen stellt, verlangen, dass sie vor Ausstellung des Zertifikats persönlich erscheint und den Nachweis ihrer Identität mit einem oder mehreren gültigen amtlichen Ausweispapieren mit Lichtbild (Personalausweis, Reisepass) erbringt. Des Weiteren muss die CSP - vor Ausstellung des Zertifikats - prüfen, ob die Antragstellerin berechtigt ist, im Namen des Unternehmens, für das sie tätig ist, ein Zertifikat zu beantragen.

b) Die CSP können ihre Aufgabe zur Identifikation einer Antragstellerin an Dritte delegieren (Registrierungsstellen). Sie haften für die korrekte Ausführung der Aufgabe durch die Registrierungsstelle.

### 4.2.1 Überprüfung der Angaben über natürliche Personen

Die Antragstellerin hat ein gültiges amtliches Ausweisdokument mit Unterschriftszug vorzulegen.

### 4.2.2 Überprüfung der Angaben über Organisationen

Die Antragstellerin hat entsprechende Dokumente vorzulegen, mit denen Name und Sitz der Firma festgestellt werden können.

#### 4.2.2.1 Wirtschaftssubjekte mit Handelsregistereintrag

Die Prüfung erfolgt nach dem beglaubigten Handelsregisterauszug, der nicht älter als drei Monate sein darf.

#### 4.2.2.2 Einzelfirma (natürliche Person), nicht im Handelsregister eingetragen

Die Prüfung erfolgt nach der Eintragungsbescheinigung der ESTV[2].

#### 4.2.2.3 Einfache Gesellschaft, nicht im Handelsregister eingetragen

Die Prüfung erfolgt nach dem Gesellschaftsvertrag und der Eintragungsbescheinigung der ESTV[2]. Handelt es sich bei den Gesellschaftern um juristische Personen, müssen zusätzlich die beglaubigten Handelsregisterauszüge vorgelegt werden. Diese dürfen nicht älter als drei Monate sein.

#### 4.2.2.4 Gemeinwesen (Gemeinden), nicht im Handelsregister eingetragen

Die Prüfung erfolgt nach der Kopie der Wahlverfügung oder der Bestätigung durch die zuständige kantonale Behörde. Die Gemeinde muss im amtlichen Gemeindeverzeichnis eingetragen sein.

#### 4.2.2.5 Andere, nicht im Handelsregister eingetragene, Wirtschaftssubjekte (z. B. Vereine)

Die Prüfung erfolgt nach der Eintragungsbescheinigung der ESTV[2] und z. B. den Vereinsstatuten, der Stiftungsurkunde oder anderen Dokumenten.

---

[2] Der Sitz ergibt sich nicht in jedem Fall aus der Eintragungsbescheinigung der ESTV. In diesem Fall sind andere Dokumente notwendig, die geeignet sind, um den Sitz festzustellen.

### 4.2.3 Überprüfung der Angaben über die Beziehung der natürlichen Person zur Organisation

Die CSP prüft die Beziehung der natürlichen Person zur Organisation.

#### 4.2.3.1 Wirtschaftssubjekte mit Handelsregistereintrag

Die Berechtigung, im Namen einer im Handelsregister eingetragenen Firma ein Zertifikat zu beantragen, muss mit einem beglaubigten Handelsregisterauszug belegt werden. Der beglaubigte Handelsregisterauszug darf nicht älter als drei Monate sein. Die Antragstellerin muss darin als Vertretungsberechtigte des Unternehmens genannt sein oder über eine Vollmacht verfügen, die von dem oder den Vertretungsberechtigten des Unternehmens eigenhändig unterzeichnet wurde. Eine Vollmacht ist beispielsweise nötig, wenn die im Handelsregisterauszug genannte Firma nur gemeinschaftlich vertreten werden kann. Die Vertretungsberichtigung vom Vollmachtgeber muss nach dem Handelsregisterauszug geprüft werden.

#### 4.2.3.2 Einzelfirma (natürliche Person), nicht im Handelsregister eingetragen

Die Berechtigung, im Namen einer Einzelfirma ein Zertifikat zu beantragen, muss mit einem amtlichen Ausweisdokument (Personalausweis, Reisepass) und der Eintragungsbescheinigung der ESTV belegt werden.

#### 4.2.3.3 Einfache Gesellschaft, nicht im Handelsregister eingetragen

Die Berechtigung, im Namen einer einfachen Gesellschaft ein Zertifikat zu beantragen, muss mit dem Gesellschaftsvertrag belegt werden. Die Antragstellerin muss im Gesellschaftsvertrag als Gesellschafterin genannt sein. Handelt es sich bei der Gesellschafterin um eine juristische Person, muss zusätzlich ein beglaubigter Handelsregisterauszug vorgelegt werden. Dieser darf nicht älter als drei Monate sein. Die den Antrag stellende Person muss darin als Vertretungsberechtigte der Gesellschafterin genannt sein oder über eine Vollmacht verfügen, die von dem oder den Vertretungsberechtigten des Unternehmens eigenhändig unterzeichnet wurde. Eine Vollmacht ist beispielsweise nötig, wenn die im Handelsregisterauszug genannte Firma nur gemeinschaftlich vertreten werden kann. Die Vertretungsberichtigung der Vollmachtgeberin muss aufgrund des Handelsregisterauszuges geprüft werden.

#### 4.2.3.4 Gemeinwesen (Gemeinden), nicht im Handelsregister eingetragen

Die Berechtigung, im Namen der Gemeinde ein Zertifikat zu beantragen, muss mit einer Kopie der Wahlverfügung (z. B. Gemeindepräsident) oder mit einer Bestätigung durch die zuständige kantonale Behörde belegt werden.

#### 4.2.3.5 Andere, nicht im Handelsregister eingetragene, Wirtschaftssubjekte (z. B. Vereine)

Die Berechtigung, im Namen eines Wirtschaftssubjektes ein Zertifikat zu beantragen, muss mit geeigneten Dokumenten nachgewiesen werden. Daraus muss sich ergeben, welche Organe das Wirtschaftssubjekt gegen aussen vertreten dürfen und welche Person diese Funktion im Zeitpunkt des Antrages innehat.

### 4.2.4 Überprüfung der Zertifikatsdaten

Die CSP prüft die Zertifikatsanträge nach den folgenden Tabellen.

#### 4.2.4.1 Wirtschaftssubjekte mit Handelsregistereintrag

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Beglaubigter Handelsregisterauszug |
| Organizational Unit | $OU_{0..n}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |
| Organizational Unit | $OU_{n+1}$ | Schriftliche Bestätigung der Funktion des Zertifikats nach Abschnitt 4.1 |
| Common Name | CN | Der CN muss die Angaben vom RDN O enthalten |
| Locality | L | Beglaubigter Handelsregisterauszug |
| State/Province | SP | Beglaubigter Handelsregisterauszug |
| Country | C | Beglaubigter Handelsregisterauszug |
| EmailAddress | $E_{0..1}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |

#### 4.2.4.2 Einzelfirma (natürliche Person)

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Eintragungsbescheinigung der ESTV |
| Organizational Unit | $OU_{0..n}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |
| Organizational Unit | $OU_{n+1}$ | Schriftliche Bestätigung der Funktion des Zertifikats nach Abschnitt 4.1 |
| Common Name | CN | Der CN muss die Angaben vom RDN O enthalten |
| Locality | L | Eintragungsbescheinigung der ESTV |
| State/Province | SP | Eintragungsbescheinigung der ESTV |
| Country | C | Eintragungsbescheinigung der ESTV |
| EmailAddress | $E_{0..1}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |

#### 4.2.4.3 Einfache Gesellschaft

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Eintragungsbescheinigung der ESTV |
| Organizational Unit | $OU_{0..n}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |
| Organizational Unit | $OU_{n+1}$ | Schriftliche Bestätigung der Funktion des Zertifikats nach Abschnitt 4.1 |
| Common Name | CN | Der CN muss die Angaben vom RDN O enthalten |
| Locality | L | Eintragungsbescheinigung der ESTV |
| State/Province | SP | Eintragungsbescheinigung der ESTV |
| Country | C | Eintragungsbescheinigung der ESTV |
| EmailAddress | $E_{0..1}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |

#### 4.2.4.4 Gemeinwesen (Gemeinden)

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Eintragungsbescheinigung der ESTV |
| Organizational Unit | $OU_{0..n}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |
| Organizational Unit | $OU_{n+1}$ | Schriftliche Bestätigung der Funktion des Zertifikats nach Abschnitt 4.1 |
| Common Name | CN | Der CN muss die Angaben vom RDN O enthalten |
| Locality | L | Amtliches Gemeindeverzeichnis |
| State/Province | SP | Amtliches Gemeindeverzeichnis |
| Country | C | Schweiz oder Suisse oder Svizzera, oder Landesbezeichnung nach Staatsvertrag (Art. 3 Bst. a MWSTG [1]) |
| EmailAddress | $E_{0..1}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |

#### 4.2.4.5 Andere nicht im Handelsregister eingetragene Wirtschaftssubjekte (z. B. Vereine)

| Beschreibung | RDN | Inhalt |
|---|---|---|
| Organization | O | Eintragungsbescheinigung der ESTV |
| Organizational Unit | $OU_{0..n}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |
| Organizational Unit | $OU_{n+1}$ | Schriftliche Bestätigung der Funktion des Zertifikats nach Abschnitt 4.1 |
| Common Name | CN | Der CN muss die Angaben vom RDN O enthalten |
| Locality | L | Eintragungsbescheinigung der ESTV oder nach Abschnitt 4.2.3.5 |
| State/Province | SP | Eintragungsbescheinigung der ESTV oder nach Abschnitt 4.2.3.5 |
| Country | C | Eintragungsbescheinigung der ESTV oder nach Abschnitt 4.2.3.5 |
| EmailAddress | $E_{0..1}$ | Schriftliche Bestätigung durch Vertretungsberechtigten |

# 5 Verzeichnisdienste für Zertifikate

a) Die CSP stellt sicher, dass die Gültigkeit aller im Rahmen dieser TAV ausgestellten Zertifikate, mit einem gebräuchlichen Verfahren jederzeit zuverlässig überprüft werden kann.

b) Sie kann zudem einen Verzeichnisdienst anbieten, über den jedermann die im Rahmen dieser TAV ausgestellten Zertifikate dieser Anbieterin suchen und abrufen kann.

c) Abfragen der öffentlichen Hand sind unentgeltlich.

d) Die CSP muss Zertifikate, die im Rahmen dieser TAV ausgestellt wurden, während mindestens elf Jahren ab Ablauf der Zertifikate bereitstellen können.

e) Die CSP muss die Informationen zur Überprüfung von nicht mehr gültigen Zertifikaten, die im Rahmen dieser TAV ausgestellten wurden, während mindestens elf Jahren ab Ablauf der Zertifikate über Sperrlisten oder andere gängige Onlinestatusüberprüfungsverfahren angeben können. Alle gesperrten Zertifikate müssen über einen Zeitraum von mindestens elf Jahren nach Ablauf ihrer Gültigkeit weiter in der jeweils aktuellen Sperrliste geführt werden.

f) Der Zugriff auf im Verzeichnisdienst eingetragene Zertifikate und Sperrlisten ist online unter Berücksichtigung der technischen Verfügbarkeit jederzeit und ohne zusätzliche Kosten für den Anfragesteller zu gewährleisten.

# 6 Verwendungszweck und Verantwortlichkeiten

Die CSP hat die nachstehenden Nutzungsbestimmungen und Verantwortlichkeiten für die Verwendung der Zertifikate, die im Rahmen dieser TAV ausgestellt werden, der Antragstellerin zu überbinden.

## 6.1 Verwendungszweck

Generell ist die Nutzung der unter diesen TAV ausgestellten Zertifikate für Signaturerstellung im Sinne der ElDI-V [3] und im Zusammenhang mit der ElDI-V [3] stehende Zwecke zulässig.

Die vorerwähnte Nutzungsbeschränkung schliesst jedoch nicht aus, dass das Zertifikat für andere handelsrechtliche Zwecke verwendet wird, sofern an die für diese Belange erforderlichen Zertifikate keine höheren Anforderungen gestellt werden.

## 6.2 Ungültigerklärung von Zertifikaten

### 6.2.1 Pflichten der CSP

Die in Artikel 10 ZertES [4] aufgeführten Bestimmungen gelten sinngemäss.

### 6.2.2 Pflichten der Zertifikatsinhaberin

Die Zertifikatsinhaberin oder die Person, die sie vertritt, hat, ohne Angabe von Gründen, einen Antrag zur Ungültigerklärung eines Zertifikates (schriftlich, telefonisch unter Nennung eines vereinbarten Sperrkennwortes oder durch persönliches Erscheinen mit amtlichem Ausweisdokument) an die CSP einzureichen, falls

a) der Signaturschlüssel verloren, gestohlen oder kompromittiert wurde;

b) der Verdacht besteht, dass unberechtigte Personen oder Systeme Zugriff auf den Signaturschlüssel haben oder ihn manipulieren können;

c) Angaben im Zertifikat ungültig geworden sind;

d) keine Verwendung mehr für das Zertifikat besteht;

## 6.3 Verantwortlichkeiten

a) Die Verwendung von im Rahmen dieser TAV ausgestellten Zertifikaten in der Schweiz richtet sich nach schweizerischem Recht.

b) Die Verantwortung der Antragstellerin und der CSP richten sich nach den in Kapitel 4.2 festgehaltenen Anforderungen.

c) Gegenüber Dritten wird die im RDN O genannte Zertifikatsinhaberin durch die Verwendung des Zertifikats gebunden. Sie ist für alle Handlungen verantwortlich, die im Zusammenhang mit dem Zertifikat oder dessen Nutzung begangen werden. Die Zertifikatsinhaberin ist für den Erlass schriftlicher, organisationsinterner Weisungen und deren Einhaltung verantwortlich. Diese Weisungen müssen Bestimmungen über den Einsatz des Signaturschlüssels und des Zertifikats, den Zugang zu Signaturschlüssel und sicheren Signaturerstellungseinheit sowie die allfällige Ungültigkeitserklärung des Zertifikats enthalten.

# 7 Kennzeichnung eines ElDI-V Zertifikats

## 7.1 Allgemeines

Zertifikate, die im Rahmen dieser TAV ausgestellt werden, müssen den viersprachigen (D, F, I und E) Eintrag als „explicitText“ im Feld „UserNotice“ der „certificatePolicies“ enthalten:

```
gestuetzt auf Art. 2 Abs. 2 ElDI-V;
en vertu de l'art. 2 al. 2 OelDI;
visto l'art. 2 cpv. 2 OelDI;
based on art. 2 para. 2 OelDI;
SR 641.201.511 / RS 641.201.511
Schweiz/Suisse/Svizzera/Switzerland
```

Der entsprechende Objektbezeichner für die „CertPolicyId“ muss unter der Verwaltung der CSP liegen und darf ausschliesslich für die Kennzeichnung von Zertifikaten verwendet werden, die unter diesen TAV ausgestellt werden.

## 7.2 CPS

Die CPS der CSP muss explizit auf die ElDI-V [3] und auf diese TAV verweisen.

Bern, 14. Dezember 2009

Eidgenössische Steuerverwaltung

Urs Ursprung
Direktor