Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Administration fédérale des contributions AFC

RS 641.201.511.1 / Annexe

Prescriptions techniques et administratives

pour

les services de certification dans le cadre de l'OeIDI en rapport avec l'émission de certificats se fondant sur des signatures avancées

Deuxième édition: 14 décembre 2009
remplace la première édition du 12 octobre 2007
Entrée en vigueur: 1er janvier 2010

Eigerstrasse 65
3003 Berne
www.estv.admin.ch

Table des matières

Pour faciliter la lecture du document, le masculin générique est utilisé pour désigner les deux sexes.

1 Généralités

1.1 Bases légales et champ d'application

Les présentes prescriptions techniques et administratives (PTA) se fondent sur:

- la loi sur la TVA (LTVA) [1]
- l'ordonnance régissant la TVA (OTVA) [2]
- l'ordonnance du DFF concernant les données et informations électroniques (OelDI) [3]
- la loi sur les services de certification dans le domaine de la signature électronique (SCSE) [4]
- l'ordonnance sur les services de certification dans le domaine de la signature électronique (OSCSE) [5]
- l'ordonnance de l'OFCOM sur les services de certification dans le domaine de la signature électronique [6]

Elles précisent les conditions et les exigences de base définies dans la loi [1] et les ordonnances [2], [3] que doit remplir un fournisseur de services de certification (CSP) reconnu, lorsqu'il délivre des certificats électroniques [3] ou qu'il fournit d'autres services en rapport avec les signatures électroniques [3].

La reconnaissance d'un CSP est décrite au chapitre 2.

1.2 Références

[1] RS 641.20, LTVA

Loi fédérale du 12 juin 2009 régissant la taxe sur la valeur ajoutée (loi sur la TVA)

[2] RS 641.201, OTVA

Ordonnance du 27 novembre 2009 régissant la TVA

[3] RS 641.201.511, OelDI

Ordonnance du DFF du 11 décembre 2009 concernant les données et informations électroniques

[4] RS 943.03, SCSE

Loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique (loi sur la signature électronique)

[5] RS 943.032, OSCSE

Ordonnance du 3 décembre 2004 sur les services de certification dans le domaine de la signature électronique (ordonnance sur la signature électronique)

[6] RS 943.032.1

Ordonnance de l'OFCOM du 6 décembre 2004 sur les services de certification dans le domaine de la signature électronique, 3^{e} édition du 13 novembre 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 (avril 2002)

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

[10] UIT-T Recommandation X.509 (2000) – ISO 9594-8:2001 (4e édition)

Technologies de l'information - Interconnexion des systèmes ouverts - L'annuaire: cadre général des certificats de clé publique et d'attribut *(Information technology – Open systems interconnection – The Directory: Public key and attribute certificate frameworks)*

[11] ITSEC Version 1.2 (28 juin 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] RS 220, CO

Loi fédérale du 30 mars 1911 complétant le Code civil suisse (Livre cinquième: Droit des obligations)

Les documents référencés peuvent être obtenus auprès des organisations figurant au chapitre 1.2 des PTA-SCSE [6].

Ces prescriptions peuvent être téléchargées sur Internet www.estv.admin.ch ou demandées à l'adresse suivante:

Prescriptions techniques et administratives (RS 641.201.511.1 / Annexe)	Office fédéral des constructions et de la logistique 3003 Berne http://www.bbl.admin.ch

1.3 Abréviations

AFC	Administration fédérale des contributions
CPS	*Certification practice statement* - Déclaration des pratiques de certification
CSP	*Certification Service Provider* - Fournisseur de services de certification
DFF	Département fédéral des finances
DFJP	Département fédéral de justice et police
DN	*Distinguished Name* - Nom absolu
ElDI-V	Verordnung des EFD über elektronische Daten und Informationen
FIPS	*Federal Information Processing Standards*
ICD	*International Code Designator*

ISO	*International Standardization Organization* - Organisation internationale de normalisation
ITSEC	*Information Technology Security Evaluation Criteria* - critères destinés à évaluer le degré de sécurité des systèmes d'information
LTVA	Loi sur la TVA [1]
OelDI	Ordonnance du DFF concernant les données et informations électroniques [3] ; Ordinanza del DFF concernente dati ed informazioni elettronici ; Ordinance of the FDF on Electronic Data and Information
OFCOM	Office fédéral de la communication
OID	*Object Identifier* - Identificateur d'objet
OTVA	Ordonnance régissant la TVA [2]
OSCSE	Ordonnance sur les services de certification dans le domaine de la signature électronique [5]
PTA	Prescriptions techniques et administratives
PTA-SCSE	Annexe à l'ordonnance de l'OFCOM sur les services de certification dans le domaine de la signature électronique [6]
RDN	*Relative Distinguished Name* - Nom relatif
RFC	*Request for Comments*
RS	Recueil systématique du droit fédéral
SCSE	Loi sur les services de certification dans le domaine de la signature électronique [4]
UIT-T	*International Telecommunication Union. Telecommunication Standardization Sector* - Union internationale des télécommunications. Secteur de la normalisation des télécommunications.

1.4 Définitions

Dans les présentes PTA:

Sont «applicables par analogie» les dispositions qui s'appliquent aux certificats qualifiés conformément aux PTA-SCSE [6] et qui sont aussi valables pour les certificats délivrés selon les présentes prescriptions.

On entend par «certificat», un certificat qui remplit les exigences mentionnées à l'art. 2, al. 2, OelDI [3] et qui est délivré aux conditions des présentes PTA.

2 Reconnaissance des CSP

Un CSP qui délivre des certificats en vertu des dispositions des présentes PTA doit être inscrit sur une liste de fournisseurs reconnus au sens de l'art. 5 SCSE [4] conformément à toutes les normes contenues dans la SCSE [4], l'OSCSE [5] et dans les PTA-SCSE [6].

3 Exigences fondamentales

3.1 Principe

Les présentes PTA se fondent sur les PTA-SCSE [6] et les complètent en indiquant quelles sont les exigences et les conditions devant être remplies pour l'émission, la gestion et l'utilisation de certificats dans le cadre de l'OelDI [3].

Pour émettre des certificats conformément aux présentes PTA, le CSP doit appliquer les mêmes processus opérationnels et organisationnels et utiliser la même infrastructure technique que ceux utilisés pour l'émission de certificats qualifiés en vertu de la SCSE [4].

3.2 Organisation et principes opérationnels

Les dispositions du chapitre 3.2 des PTA-SCSE [6] s'appliquent, sauf celles en rapport avec les services dont il est question au chapitre 3.5 des PTA-SCSE [6]. Les documents importants pour les titulaires de certificats doivent être rédigés dans une langue officielle. En plus des documents mentionnés au chapitre 3.2, lettre c) des PTA-SCSE [6], le CSP doit aussi joindre les documents suivants aux audits internes qu'il doit effectuer chaque année pour vérifier la conformité de ses activités:

- OelDI [3],
- les présentes PTA.

Les défauts relevés au cours des audits internes à effectuer tous les ans doivent être corrigés (complément au chapitre 3.2, lettre d) des PTA-SCSE [6]).

À la demande de l'AFC, les rapports finaux et tous les documents référencés doivent lui être remis.

3.3 Gestion des clés

3.3.1 Gestion des clés du CSP

Les dispositions du chapitre 3.3.1 des PTA-SCSE [6] sont applicables par analogie.

3.3.2 Elaboration de la clé pour le requérant de certificat

a) Les dispositions du chapitre 3.3.2, lettre a), des PTA-SCSE [6] sont applicables par analogie lorsque le CSP élabore lui-même la paire de clés du requérant.

b) Les dispositions du chapitre 3.3.2, lettre b), des PTA-SCSE [6] sont applicables par analogie lorsque le CSP élabore lui-même la paire de clés du requérant.

c) Lorsque le requérant de certificat élabore lui-même sa paire de clés, le CSP doit s'assurer au niveau technique ou, si ce n'est pas possible, au niveau organisationnel, que cette paire de clés a été élaborée dans un dispositif sécurisé de création de signature tel que défini au chiffre 3.3.3 des présentes PTA.

3.3.3 Dispositifs sécurisés de création de signature

a) Toutes les opérations en relation avec la clé de signature d'un certificat conforme à l'OeIDI [3] doivent se dérouler exclusivement au sein d'un dispositif sécurisé de création de signature. La clé de signature peut être exportée d'une manière sécurisée à des fins de sauvegarde, à condition qu'elle bénéficie d'une protection équivalente à celle assurée par le dispositif sécurisé et que toute utilisation en dehors de ce dispositif soit exclue.

   En outre, les dispositifs sécurisés de signature doivent être conformes aux exigences complémentaires suivantes:

   - Ils ne doivent entraîner aucune modification du contenu à signer;
   - Le certificat (ou le renvoi clair à ce certificat) doit être présent dans le dispositif;
   - La clé de signature correspondant au certificat ne doit pas pouvoir être utilisée avant d'avoir été activée par les données d'activation;
   - Des tentatives d'activation incorrectes et consécutives doivent pouvoir être détectées;
   - Lorsqu'un nombre prédéterminé de tentatives d'activation incorrectes et consécutives a été atteint, l'usage de la clé de signature doit être bloqué. Ce nombre prédéterminé ne peut être supérieur à quatre;
   - Le déblocage d'une clé nécessite une procédure exigeant l'introduction de données d'activation correctes.

b) La certification des dispositifs sécurisés de création de signature doit répondre

   - à la certification selon FIPS 140-1 [7] ou FIPS 140-2 [8] niveau 3 ou supérieur, ou
   - au niveau d'évaluation EAL 4 de la norme ISO/IEC 15408:2005 [12], augmenté des composants d'assurance AVA_MSU.3 (*vulnerability assessment, analysis and testing of insecure states*) et AVA_VLA.4 (*vulnerability assessment, highly resistant*), ou
   - au niveau d'évaluation E3 élevé du document ITSEC [11].

c) Les dispositions du chapitre 3.3.3, lettre c), des PTA-SCSE [6] sont applicables.

3.4 Gestion des certificats

3.4.1 Enregistrement, gestion et annulation des certificats de tiers

Les dispositions du chapitre 3.4.1 des PTA-SCSE [6] sont applicables par analogie.

3.4.2 Format des certificats des titulaires

a) Les dispositions du chapitre 3.4.2, lettre a), des PTA-SCSE [6] sont applicables.

b) Conformément à l'art. 2, al. 2, let. a, OeIDI [3] et au chapitre 4.1 du document RFC 3280 [9], le CSP doit ajouter les champs suivants à la séquence «tbsCertificate»:

Description	Champ	Contenu
Version	version	Les dispositions du chapitre 3.4.2, lettre b), des PTA-SCSE [6] sur le champ «version» sont applicables.
Numéro de série du certificat	serialNumber	Les dispositions du chapitre 3.4.2, lettre b), des PTA-SCSE [6] sur le champ «serialNumber» sont applicables.
Identifiant de l'algorithme de signature utilisé pour signer le certificat	signature	Les dispositions du chapitre 3.4.2, lettre b), des PTA-SCSE [6] sur le champ «signature» sont applicables.
Nom et pays d'établissement du CSP	issuer	Les dispositions du chapitre 3.4.2, lettre b), des PTA-SCSE [6] sur le champ «issuer» sont applicables.

Durée de validité du certificat	validity	Les dispositions du chapitre 3.4.2, lettre b), des PTA-SCSE [6], sur le champ «validity» sont applicables.
Raison sociale du titulaire et, si nécessaire, qualités spécifiques du titulaire	subject	Les dispositions du chapitre 3.4.2, lettre b), des PTA-SCSE [6] sur le champ «subject» sont applicables. Le chapitre 4 des présentes PTA règle l'attribution des noms.
Clé et algorithme de vérification de la signature du titulaire du certificat	subjectPublicKeyInfo	Les dispositions du chapitre 3.4.2, lettre b), des PTA-SCSE [6] sur le champ «subjectPublicKeyInfo» sont applicables.

c) Le CSP doit inclure les extensions suivantes de la séquence «tbsCertificate» conformément au chapitre 4.2 du document RFC 3280 [9]:

Description	Extension critique	Nom de l'extension	Contenu
Identifiant de la clé du CSP qui a signé le certificat	Non	authorityKeyIdentifier	Les dispositions du chapitre 3.4.2, lettre c), des PTA-SCSE [6] sur l'extension «authorityKeyIdentifier» sont applicables.
Identifiant de la clé du requérant	Non	subjectKeyIdentifier	D'après le chapitre 4.2.1.2 du document RFC 3280 [9]
Domaine d'utilisation du certificat	Oui	keyUsage	D'après le chapitre 8.2.2.3 du document UIT-T X.509 [10] et le chapitre 4.2.1.3 du document RFC 3280 [9]. ▪ Mettre bit 0 (digitalSignature) pour indiquer que le certificat sert à vérifier les signatures électroniques. ▪ Mettre bit 1 (contentCommitment / nonRepudiation) pour indiquer que le certificat est utilisé pour la non-répudiation des transactions effectuées. ▪ Il n'est pas permis de mettre d'autres bits.
Politique de certification	Non	certificatePolicies	Les dispositions du chapitre 3.4.2. lettre c), des PTA-SCSE [6] sur l'extension «certificatePolicies» sont applicables. Le chapitre 7 des présentes PTA règle l'utilisation de l'extension «certificatePolicies».
Point de distribution de la liste des certificats annulés	Non	cRLDistributionPoints	D'après le chapitre 8.6.2.1 du document UIT-T X.509 [10], et du chapitre 4.2.1.14 du document RFC 3280 [9], ▪ Un «DistributionPoint» doit indiquer un «DistributionPointName» du type «uniformResourceIdentifier» en utilisant le protocole http. Les champs «reasons» et «cRLIssuer» doivent manquer. ▪ Il est possible d'indiquer d'autres «DistributionPoints».
Point d'accès au certificat du CSP	Non	authorityInfoAccess	Les dispositions du chapitre 3.4.2, lettre c), des PTA-SCSE [6] sur l'extension «authorityInfoAccess» sont applicables.

d) Le CSP peut inclure les extensions suivantes dans la séquence «tbsCertificate» conformément au chapitre 4.2, du document RFC 3280 [9]:

Description	Extension critique	Nom de l'extension	Contenu
Numéro d'identification du registre du commerce	Non	subjectAltName	0..1, otherName Numéro d'identification attribué à tous les sujets enregistrés au registre du commerce (art. 936a CO [15]). Spécification: ▪ type-id à attribuer à l'OID: 1.3.169 L'ICD 169 [13] sous la branche 1 (iso) 3 (identified organization) correspond à un OID d'après RFC 4043 annexe B.3 [14]. ▪ La valeur «OtherName» doit être codée ASN-1 PrintableString.
Adresse e-mail	Non	subjectAltName	0..n, rfc822Name Le CSP doit vérifier chaque adresse.

D'autres extensions peuvent être ajoutées à la suite des extensions précitées à condition que le CSP en ait vérifié le contenu et qu'elles respectent les dispositions du document RFC 3280 [9].

3.4.3 Gestion du certificat du CSP pour un certificat délivré selon les présentes PTA

a) Les dispositions du chapitre 3.4.3, lettre a), des PTA-SCSE [6] sont applicables par analogie.

b) Les dispositions du chapitre 3.4.3, lettre b), des PTA-SCSE [6] sont applicables par analogie.

c) Les dispositions du chapitre 3.4.3, lettre c), des PTA-SCSE [6] sont applicables par analogie.

d) Pour son propre certificat, le CSP doit s'assurer que les extensions non critiques suivantes figurent dans la séquence «tbsCertificate» conformément au chapitre 4.2 du document RFC 3280 [9]:

- authorityKeyIdentifier. Cette extension n'est pas obligatoire s'il s'agit d'un certificat portant sa propre signature;
- subjectKeyIdentifier;
- certificatePolicies;
- cRLDistributionPoints. Cette extension ne doit pas exister s'il s'agit d'un certificat portant sa propre signature et si le champ «cRLIssuer» n'est pas utilisé.

4 Désignation du titulaire

Les documents et attestations de la Principauté de Liechtenstein sont assimilés à ceux cités dans ce chapitre[1].

Principauté de Liechtenstein	Désignation
Abréviation pour l'administration fiscale.	STV
Attestation que l'assujetti reçoit après son inscription au registre des assujettis à la TVA.	Extrait de l'inscription au registre de la TVA.
Il n'y a pas de liste officielle des communes.	Vaduz, Balzers, Planken, Schaan, Triesen, Triesenberg, Eschen, Gamprin, Mauren, Ruggell, Schellenberg
Autorité qui rend une décision de nomination.	Les agents de droit public ne sont pas élus, mais engagés par décision de l'organe compétent.

4.1 Champs de données du certificat

4.1.1 Généralités

Les certificats émis dans le cadre des présentes PTA comprennent des champs de données pour différents acteurs économiques. Ces champs sont explicités et illustrés par un exemple après le tableau suivant. La manière dont les indications des champs de données sont vérifiées au moment de la demande de certificat est décrite au chiffre 4.2.

Les acteurs économiques comprennent notamment les sujets fiscaux selon la LTVA [1].

Les certificats délivrés à des titulaires de certificat qui ne peuvent pas être désignés par un nom répondant aux règles suivantes doivent être émis à un nom admissible du titulaire de certificat. De plus, une affectation sans la moindre ambiguïté doit être assurée et toute confusion avec une personne physique, une personne morale ou une unité d'organisation doit être exclue.

[1] Traité du 28 octobre 1994 entre la Confédération suisse et la Principauté de Liechtenstein relatif à la taxe sur la valeur ajoutée dans la Principauté de Liechtenstein (RS 0.641.295.142)

Description	RDN	Contenu
Organization	O	Raison sociale (voir chiffre 4.1.2).
Organizational Unit	$OU_{0..n}$	Désignation plus précise de l'unité d'organisation (nom de la filiale, division, etc.) affectée au certificat. Plusieurs champs OU peuvent être indiqués.
Organizational Unit	OU_{n+1}	L'indication suivante est obligatoire si le certificat est utilisé dans les buts indiqués à l'art. 9 OelDI [3]: ▪ **Third Party Services (art. 9 OelDI)** Tiers en général selon l'art. 9 OelDI Cette indication n'est pas permise si le certificat n'est pas utilisé effectivement dans ce but.
Common Name	CN	▪ **Personnes physiques** Le CN doit contenir le prénom et le nom de la personne physique ▪ **Acteurs économiques** Le CN doit contenir les indications du RDN O. Le CN peut contenir en outre d'autres indications précisant l'utilisation du certificat.
Locality	L	Désignation de la commune où l'entreprise a son siège.
State/Province	SP	Désignation du canton où l'entreprise a son siège.
Country	C	Abréviation du pays selon ISO 3166-1. Elle désigne le pays où l'entreprise désignée par le RDN O a son siège.
EmailAddress	$E_{0..1}$	0..1, rfc822Name Le CSP doit vérifier l'adresse e-mail.

Les dispositions du chapitre 4.1.2.6 du RFC 3280 [9] sont applicables. Ensemble, les RDN indiqués composent le champ du certificat intitulé «subject Distinguished Name». D'autres RDN qui désignent plus précisément le titulaire du certificat peuvent être ajoutés à la suite des RDN déjà indiqués. Le CSP doit vérifier le contenu des RDN ajoutés qui ne doit pas être en contradiction avec les RDN obligatoires.

Exemple:

```
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
```

Un «subject Distinguished Name» déterminé ne peut être affecté qu'à une seule identité déterminée (le cas échéant plusieurs fois pour différents certificats).

Vu la diversité des organisations qui peuvent requérir ce genre de certificat, les champs ci-dessus doivent être remplis en fonction du type d'organisation. Le contenu des champs pour les différents types d'organisation est décrit ci après.

4.1.2 Désignation de l’organisation

4.1.2.1 Acteurs économiques inscrits au registre du commerce (RC)

Description	RDN	Contenu
Organization	O	Raison sociale d’après l’extrait du registre du commerce.

4.1.2.2 Raison individuelle (personne physique), pas inscrite au RC

Raison individuelle (personne physique), qui ne doit pas être inscrite au registre du commerce. Il s’agit essentiellement des professions libérales. Ex.: avocats, notaires, etc.

Description	RDN	Contenu
Organization	O	Nom de la raison individuelle d’après l’extrait d’inscription de l’AFC.

4.1.2.3 Société simple, pas inscrite au RC

La société simple est constituée par contrat. Ses membres peuvent être aussi bien des personnes physiques que des personnes morales. La société simple ne possède pas la personnalité juridique, mais la TVA la considère comme un sujet fiscal. Dans la construction, le consortium est une forme importante de la société simple. Il s’agit de la réunion contractuelle de deux ou plusieurs entreprises de construction pour exécuter un projet de construction d’une certaine envergure.

Description	RDN	Contenu
Organization	O	Nom de la société simple d’après l’extrait d’inscription de l’AFC ou d’après le contrat de société.

4.1.2.4 Collectivités publiques (communes), pas inscrites au RC

En plus des communes politiques (commune municipale), il existe par exemple également des communes bourgeoises et des paroisses. Il n’est pas possible d’énoncer des règles abstraites et générales pour déterminer la personne qui peut agir au nom de la commune. La surveillance des communes est réglée par les cantons et peut différer d’un canton à l’autre. Il faut encore tenir compte d’une particularité: pour la TVA, l’assujetti enregistré n’est pas obligatoirement la commune dans son ensemble, mais certains de ses services qui fournissent des prestations imposables.

Description	RDN	Contenu
Organization	O	Nom de la commune d’après la liste officielle des communes.
Organizational Unit	OU	Nom du service d’après l’extrait d’inscription de l’AFC.

4.1.2.5 Autres acteurs économiques qui ne sont pas inscrits au RC (p. ex. associations)

Ces acteurs sont désignés d’après les mêmes règles que celles en vigueur pour les raisons individuelles.

Description	RDN	Contenu
Organization	O	Nom selon l’extrait d’inscription de l’AFC.

4.2 Vérification des données contenues dans les certificats

a) Avant d'émettre un certificat, le CSP doit exiger du requérant qui demande l'émission d'un certificat dans le cadre de ces dispositions qu'il se présente personnellement et qu'il prouve son identité au moyen d'un ou de plusieurs papiers d'identité officiels et valables avec photographie (carte d'identité, passeport). Avant d'émettre le certificat, le CSP doit en outre établir le droit du requérant de demander un certificat au nom de l'entreprise pour laquelle il travaille.

b) Le CSP peut déléguer son obligation d'identifier le requérant à des tiers (bureau d'enregistrement). Il répond de la bonne exécution de cette tâche par le bureau d'enregistrement.

4.2.1 Vérification des données sur des personnes physiques

Le requérant doit présenter une pièce d'identité officielle avec signature.

4.2.2 Vérification des données sur des organisations

Le requérant doit présenter les documents permettant d'établir le nom et le siège de la société.

4.2.2.1 Acteurs économiques inscrits au RC

La vérification se fait sur la base d'un extrait du registre du commerce certifié conforme, dont la date ne doit pas être supérieure à trois mois.

4.2.2.2 Raison individuelle (personne physique), pas inscrite au RC

La vérification se fait d'après l'extrait d'inscription de l'AFC[2].

4.2.2.3 Société simple, pas inscrite au RC

La vérification se fait d'après le contrat de société et d'après l'extrait d'inscription de l'AFC[2]. Si les associés sont des personnes morales, il faut présenter en plus les extraits du registre du commerce certifiés conformes. La date de ces extraits ne doit pas être supérieure à trois mois.

4.2.2.4 Collectivités publiques (communes), pas inscrites au RC

La vérification se fait sur la base de la copie de la décision de nomination ou de l'attestation de l'autorité cantonale compétente. La commune doit figurer sur la liste officielle des communes.

4.2.2.5 Autres acteurs économiques qui ne sont pas inscrits au RC (p. ex. associations)

La vérification se fait d'après l'extrait d'inscription de l'AFC [2] et, par exemple, d'après les statuts de l'association, l'acte de fondation de la fondation ou d'autres documents.

4.2.3 Vérification des données sur le rapport de la personne physique à l'organisation

Le CSP vérifie le rapport existant entre la personne physique et l'organisation.

4.2.3.1 Acteurs économiques inscrits au RC

L'autorisation de requérir un certificat au nom d'une société enregistrée au registre du commerce doit être prouvée au moyen d'un extrait du registre du commerce certifié conforme dont la date n'est pas supérieure à trois mois. Le requérant doit y figurer comme représentant autorisé de la société ou disposer d'une procuration signée de la main du ou des représentants autorisés de la société. Une procuration est nécessaire notamment lorsque la société citée dans

[2] Le siège ne ressort pas forcément de l'extrait d'inscription de l'AFC. Dans ce cas, il faut exiger d'autres documents permettant de déterminer le siège.

l’extrait du registre du commerce ne peut être représentée que collectivement. Les pouvoirs de représentation de la personne qui donne la procuration doivent être vérifiés sur la base de l’extrait du registre du commerce.

4.2.3.2 Raison individuelle (personne physique), pas inscrite au RC

Le droit de requérir un certificat au nom d’une raison individuelle doit être prouvé au moyen d’un document d’identité officiel (carte d’identité, passeport) et de l’extrait d’inscription de l’AFC.

4.2.3.3 Société simple, pas inscrite au RC

Le droit de requérir un certificat au nom d’une société simple doit être prouvé au moyen du contrat de société. Le requérant doit être cité comme associé dans le contrat de société. Si l’associé est une personne morale, il faut en plus produire un extrait du registre du commerce certifié conforme. La date de cet extrait ne doit pas être supérieure à trois mois. Le requérant doit y figurer comme représentant de la société ou disposer d’une procuration signée de la main de la ou des personnes habilitées à représenter la société. Une procuration est nécessaire notamment lorsque la société citée dans l’extrait du registre du commerce ne peut être représentée que collectivement. Les pouvoirs de représentation de la personne qui donne la procuration doivent être vérifiés sur la base de l’extrait du registre du commerce.

4.2.3.4 Collectivités publiques (communes), pas inscrites au RC

Le droit de requérir un certificat au nom d’une commune doit être prouvé par une copie de la décision de nomination (p. ex. maire) ou par une attestation de l’autorité cantonale compétente.

4.2.3.5 Autres acteurs économiques qui ne sont pas inscrits au RC (p. ex. associations)

Le droit de requérir un certificat au nom d’un acteur économique doit être prouvé à l’aide des documents adéquats. Ils doivent désigner les organes que l’acteur économique est habilité à représenter envers l’extérieur et la personne titulaire de cette fonction au moment de la requête.

4.2.4 Vérification des données du certificat

Le CSP vérifie les demandes de certificat selon les tableaux suivants.

4.2.4.1 Acteurs économiques inscrits au RC

Description	RDN	Contenu
Organization	O	Extrait du registre du commerce certifié conforme
Organizational Unit	$OU_{0..n}$	Attestation écrite des représentants autorisés
Organizational Unit	OU_{n+1}	Attestation écrite de la fonction du certificat selon le chiffre 4.1
Common Name	CN	Le CN doit contenir les indications du RDN O
Locality	L	Extrait du registre du commerce certifié conforme
State/Province	SP	Extrait du registre du commerce certifié conforme
Country	C	Extrait du registre du commerce certifié conforme
EmailAddress	$E_{0..1}$	Attestation écrite des représentants autorisés

4.2.4.2 Raison individuelle (personne physique)

Description	RDN	Contenu
Organization	O	Extrait d'inscription de l'AFC
Organizational Unit	$OU_{0..n}$	Attestation écrite des représentants autorisés
Organizational Unit	OU_{n+1}	Attestation écrite de la fonction du certificat selon le chiffre 4.1
Common Name	CN	Le CN doit contenir les indications du RDN O
Locality	L	Extrait d'inscription de l'AFC
State/Province	SP	Extrait d'inscription de l'AFC
Country	C	Extrait d'inscription de l'AFC
EmailAddress	$E_{0..1}$	Attestation écrite des représentants autorisés

4.2.4.3 Société simple

Description	RDN	Contenu
Organization	O	Extrait d'inscription de l'AFC
Organizational Unit	$OU_{0..n}$	Attestation écrite des représentants autorisés
Organizational Unit	OU_{n+1}	Attestation écrite de la fonction du certificat selon le chiffre 4.1
Common Name	CN	Le CN doit contenir les indications du RDN O
Locality	L	Extrait d'inscription de l'AFC
State/Province	SP	Extrait d'inscription de l'AFC
Country	C	Extrait d'inscription de l'AFC
EmailAddress	$E_{0..1}$	Attestation écrite des représentants autorisés

4.2.4.4 Collectivités publiques (communes)

Description	RDN	Contenu
Organization	O	Extrait d'inscription de l'AFC
Organizational Unit	$OU_{0..n}$	Attestation écrite des représentants autorisés
Organizational Unit	OU_{n+1}	Attestation écrite de la fonction du certificat selon le chiffre 4.1
Common Name	CN	Le CN doit contenir les indications du RDN O
Locality	L	Liste officielle des communes de la Suisse
State/Province	SP	Liste officielle des communes de la Suisse
Country	C	Schweiz ou Suisse ou Svizzera ou désignation du pays selon les conventions internationales (art. 3, let. a, LTVA [1])
EmailAddress	$E_{0..1}$	Attestation écrite des représentants autorisés

4.2.4.5 Autres acteurs économiques qui ne sont pas inscrits au RC (p. ex. associations)

Description	RDN	Contenu
Organization	O	Extrait d'inscription de l'AFC
Organizational Unit	$OU_{0..n}$	Attestation écrite des représentants autorisés
Organizational Unit	OU_{n+1}	Attestation écrite de la fonction du certificat selon le chiffre 4.1
Common Name	CN	Le CN doit contenir les indications du RDN O
Locality	L	Extrait d'inscription de l'AFC ou selon chiffre 4.2.3.5
State/Province	SP	Extrait d'inscription de l'AFC ou selon chiffre 4.2.3.5
Country	C	Extrait d'inscription de l'AFC ou selon chiffre 4.2.3.5
EmailAddress	$E_{0..1}$	Attestation écrite des représentants autorisés

5 Services d'annuaires pour les certificats

a) Le CSP s'assure que la validité de tous les certificats émis dans le cadre des présentes PTA puisse être vérifiée en tout temps au moyen d'une procédure courante et fiable.

b) En outre, il peut offrir un service d'annuaire permettant à tout intéressé de rechercher et de consulter les certificats émis dans le cadre des présentes PTA.

c) Les pouvoirs publics peuvent consulter ces données gratuitement.

d) Le CSP doit pouvoir mettre à disposition les certificats émis dans le cadre des présentes PTA pendant 11 ans au moins à partir de l'échéance des certificats.

e) Le CSP doit être en mesure d'indiquer les informations nécessaires à la vérification des certificats émis dans le cadre des présentes PTA et qui ne sont plus valables pendant 11 ans au moins à partir de l'échéance de ces certificats, au moyen de listes des certificats bloqués ou d'une procédure de vérification accessible en ligne. Tous les certificats bloqués doivent figurer sur la liste actualisée, pendant 11 ans au moins à partir de leur échéance.

f) L'accès aux certificats et aux listes de certificats bloqués enregistrés dans le service d'annuaire doit être assuré en ligne en tout temps, compte tenu des disponibilités techniques et sans frais supplémentaires pour les intéressés.

6 But d’utilisation et responsabilités

Le requérant est tenu d’adopter les dispositions sur l’utilisation et sur les responsabilités découlant de l’usage du certificat émis dans le cadre des présentes PTA et énumérées ci-dessous.

6.1 But d’utilisation

D’une manière générale, l’utilisation des certificats émis dans le cadre des présentes PTA est permise pour établir une signature au sens de l’OelDI [3] dans les buts prévus par cette ordonnance.

Cette restriction n’exclut cependant pas l’usage du certificat pour d’autres buts régis par le droit commercial dans la mesure où les certificats exigés pour ces buts ne doivent pas répondre à des exigences plus élevées.

6.2 Annulation de certificats

6.2.1 Obligations des CSP

Les dispositions de l’article 10 SCSE [4] sont applicables par analogie.

6.2.2 Obligations du titulaire de certificats

Le titulaire du certificat ou la personne qui le représente doit demander au CSP l’annulation d’un certificat (par écrit, par téléphone en mentionnant un mot de passe convenu ou en se présentant personnellement avec une pièce d’identité officielle) sans indiquer de motifs,

a) si la clé de signature a été perdue, volée ou est compromise;

b) s’il soupçonne que des personnes ou des systèmes non autorisés ont accès à la clé de signature ou sont en mesure de la manipuler;

c) si des données du certificat ne sont plus valables;

d) si le certificat n’a plus d’utilité.

6.3 Responsabilités

a) L’utilisation des certificats délivrés en Suisse dans le cadre des présentes PTA est régie par le droit suisse.

b) La responsabilité du requérant et celle du CSP s’apprécient selon les exigences du ch. 4.2.

c) Par l’utilisation du certificat, le titulaire désigné dans le RDN O est engagé envers les tiers: il répond donc de tous les actes commis en relation avec le certificat ou son utilisation. Le titulaire du certificat est responsable d’édicter par écrit les instructions internes nécessaires et de les faire respecter. Ces instructions doivent contenir des dispositions sur l’utilisation de la clé de signature et du certificat, sur l’accès à la clé de signature, sur le dispositif sécurisé de création de signature ainsi que sur la déclaration d’annulation du certificat.

7 Identification d’un certificat OelDI

7.1 Généralités

Les certificats qui sont émis dans le cadre des présentes PTA doivent contenir l’indication («explicitText») en quatre langues (D, F, I, E) dans le champ «UserNotice» du «certificatePolicies»:

```
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
```

L’identifiant correspondant pour le „CertPolicyId“ doit être géré par le CSP et ne peut être utilisé que pour identifier les certificats émis dans le cadre des présentes PTA.

7.2 CPS

Le CPS du CSP doit renvoyer explicitement à l’OelDI [3] et aux présentes PTA.

Berne, le 14 décembre 2009

Administration fédérale des contributions

Urs Ursprung
Directeur