Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement,
des transports, de l'énergie et de la communication DETEC

Office fédéral de la communication OFCOM

Prescriptions techniques et administratives concernant

les services de certification dans le domaine de la signature électronique

RS 943.032.1

3ème édition : 2006
Entrée en vigueur : 2006

Table des matières

1 Généralités

1.1 Champ d'application

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

- la loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique (SCSE) [1],
- l'ordonnance du 3 décembre 2004 sur les services de certification dans le domaine de la signature électronique (OSCSE) [2],

Dans la mesure du nécessaire et de l'admissible, elles précisent les conditions préalables et les exigences essentielles découlant de la loi et de l'ordonnance, que doit respecter, afin d'être reconnu, le fournisseur de services de certification (CSP) qui délivre des certificats électroniques qualifiés ou qui fournit d'autres services en rapport avec les signatures électroniques.

Le système de la reconnaissance est décrit au chapitre 2.

Une grande partie de ce document est basée sur les principes et les procédures qui sont décrits dans les normes internationales référencées au chapitre 1.2.

1.2 Références

[1] RS 943.03, SCSE
Loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique

[2] RS 943.032, OSCSE
Ordonnance du 3 décembre 2004 sur les services de certification dans le domaine de la signature électronique

[3] RS 946.51, LETC
Loi fédérale du 6 octobre 1995 sur les entraves techniques au commerce

[4] RS 946.512, OAccD
Ordonnance du 17 juin 1996 sur le système suisse d'accréditation et la désignation de laboratoires d'essais et d'organismes d'évaluation de la conformité, d'enregistrement et d'homologation (Ordonnance sur l'accréditation et la désignation, OAccD)

[5] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques
(JO L 13 du 19.1.2000, p. 12)

[6] ETSI TS 101 456, v1.4.1 (2006-01)
Policy requirements for certification authorities issuing qualified certificates

[7] ITU-T Recommendation X.509 (2000) - ISO 9594-8:2001 (4 ème édition)
Information technology – Open systems interconnection – The Directory : Public key and attribute certificate frameworks

[8] RFC 3280 (Avril 2002)
Internet X.509 Public Key Infrastructure - Certificate and CRL Profile

[9] RFC 3739 (Mars 2004)
Internet X.509 Public Key Infrastructure - Qualified Certificates Profile

[10] ETSI TS 102 023, v1.1.1 (2002-04)
Policy requirements for time-stamping authorities

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

[12] ETSI TS 101 862, v1.3.2 (2004-06)
Qualified Certificate Profile

[13] FIPS 140-2 (25.5.01)
Security Requirements for Cryptographic Modules

[14] ITSEC Version 1.2 (28 juin 1991)
Information Technology Security Evaluation Criteria

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

[16] ETSI TS 101 861, v1.3.1 (2006-01)
Time Stamping Profile

[17] CWA 14167-3 (2004)
Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)

[18] RFC 3279 (April 2002)
Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[19] FIPS 140-1 (11.1.94)
Security Requirements for Cryptographic Modules

[20] EN 45012 :1998
Exigences générales relatives aux organismes gérant l'évaluation et la certification/enregistrement des systèmes qualité (Guide ISO/CEI 62:1996)

[21] ISO/IEC 27001:2005
Information technology – Security techniques – Information security management systems - Requirements

Les documents référencés peuvent être obtenus auprès des organisations suivantes :

Recommandations ITU-T	Union internationale des télécommunications (UIT) Place des Nations 1211 Genève 20 http://www.itu.int
Normes de l'ISO	Secrétariat central de l'Organisation internationale de normalisation (ISO) 1, rue de Varembé 1211 Genève http://www.iso.ch
Spécifications ETSI	ETSI, Institut européen des normes de télécommunication 650 route des Lucioles 06921 Sophia Antipolis, France http://www.etsi.org
CWA du CEN	Comité européen de normalisation (CEN) 36, rue de Stassart B - 1050 Brussels, Belgique http://www.cenorm.be
Documents FIPS	National Institute of Standards and Technology (NIST) http://csrc.nist.gov/publications
Textes de loi avec références RS	Office fédéral des constructions et de la logistique (OFCL) Service de diffusion des publications fédérales CH-3003 Berne http://www.publicationsfederales.ch
Les prescriptions techniques et	OFCOM

administratives	rue de l'Avenir 44 case postale 2501 Bienne http://www.ofcom.ch/
Directive 1999/93/CE du Parlement européen	Union européenne http://www.europa.eu.int/eur-lex/fr/search/search_lif.html
Document ITSEC	Bundesamt für Sicherheit in der Informationstechnik (BSI) http://www.bsi.de/zertifiz/itkrit/itsec.htm
Documents RFC	Internet Engineering Task Force (IETF) http://www.ietf.org/
Norme EN	Institut allemand de la normalisation (DIN) http://www.din.de

1.3 Abréviations

CA	*Certification Authority* – Autorité de certification
CB	*Certification Body* – Organisme de certification appelé organisme de reconnaissance dans les présentes PTA
CEN	Comité européen de normalisation
CP	*Certification Policy* - Politique de certification
CPS	*Certification Practice Statement* – Déclaration des pratiques de certification
CRL	*Certificate Revocation List* - Liste des certificats annulés
CSP	*Certification Service Provider* – Fournisseur de service de certification
CWA	*CEN Workshop Agreement* - Accord d'atelier du CEN
EA	*European Accreditation*
EESSI	*European Electronic Signature Standardisation Initiative* – Initiative européenne pour la standardisation de la signature électronique
ETSI	*European Telecommunications Standards Institute* - Institut européen des normes de télécommunication
IETF	*Internet Engineering Task Force*
ISO	*International Standardization Organization* - Organisation internationale de normalisation
ITU-T	*International Telecommunication Union. Telecommunication Standardization Sector* - Union internationale des télécommunications. Secteur de la normalisation des télécommunications.
LETC	Loi sur les entraves techniques au commerce [3]
METAS	Office fédéral de métrologie et d'accréditation
OAccD	Ordonnance sur l'accréditation et la désignation [4]
OFCOM	Office fédéral de la communication
OID	*Object identifier* – Identificateur d'objet
OSCSE	Ordonnance sur les services de certification dans le domaine de la signature électronique [2]
PTA	Prescriptions techniques et administratives
QC	*Qualified Certificate* – Certificat qualifié
RFC	*Request for Comments*
RS	Recueil systématique
SAS	Service d'Accréditation Suisse
SCSE	Loi fédérale sur les services de certification dans le domaine de la signature électronique [1]
SSCD	*Secure-signature-creation device* – Dispositif sécurisé de création de signature

TS *Technical specification* – Spécification technique

1.4 Définitions

Au sens des présentes PTA, on entend par :

Annulation du certificat : un service du fournisseur de services de certification qui supprime la validité d'un certificat avant l'échéance de ce dernier ;

Autorité de certification (CA) : voir la définition de « fournisseur de services de certification »

Certificat numérique: une attestation électronique qui lie une clé de vérification de signature au nom d'une personne. Dans le présent document, le terme « certificat » utilisé seul doit être interprété comme « certificat qualifié » ;

Certificat qualifié : un certificat numérique qui remplit les conditions de l'art. 7, SCSE [1] ;

Clé de vérification de signature : des données, telles que des codes ou des clés cryptographiques publiques, utilisées pour vérifier une signature électronique ;

Clé de signature : des données uniques, telles que des codes ou des clés cryptographiques privées, que le titulaire utilise pour composer une signature électronique ;

Déclaration des pratiques de certification (CPS) : énoncé des règles et lignes directrices effectivement mises en œuvre par le fournisseur de services de certification pour l'émission de certificats. La CPS définit les équipements, les politiques et les procédures utilisés par le fournisseur de services de certification pour être conforme à la politique de certification qu'il a adoptée ;

Diffusion des certificats : un service du fournisseur de services de certification qui, après la génération d'un certificat, le rend disponible à son titulaire ainsi qu'à ses utilisateurs si le titulaire du certificat l'y autorise ;

Dispositif sécurisé de création de signature : un dispositif selon l'art. 6, al. 2 SCSE [1] et configuré pour mettre en application la clé de signature que le titulaire d'un certificat utilise pour créer une signature électronique ;

Enregistrement : un service du fournisseur de services de certification qui consiste à vérifier l'identité et si nécessaire les attributs de tout requérant de certificat avant la génération de son certificat ou la remise des données d'activation (ou mot de passe) permettant d'activer l'usage de la clé de signature ;

Fournisseur de services de certification (CSP) ou **autorité de certification (CA) :** un organisme qui certifie des données dans un environnement électronique et qui délivre à cette fin des certificats numériques ;

Génération des certificats : un service du fournisseur de services de certification qui génère un certificat numérique en se basant sur le nom du requérant du certificat et ses éventuels attributs qui sont vérifiés lors de l'enregistrement ;

Gestion de l'état des certificats : un service du fournisseur de services de certification qui permet aux utilisateurs d'un certificat de vérifier si ce dernier n'a pas été annulé ;

Horodatage : un service du fournisseur de services de certification qui délivre une attestation munie de la date, de l'heure et de la signature qualifiée du fournisseur de services de certification aux fins d'établir l'existence de données numériques à un moment précis ;

Liste des certificats annulés (CRL) : une liste signée par le fournisseur de services de certification contenant tous les numéros de série des certificats qui ont été annulés avant que la date de fin de validité du certificat ne soit échue ;

Organisme de reconnaissance : un organisme qui, selon les règles de l'accréditation, est habilité à reconnaître et à surveiller les fournisseurs de services de certification ;

Paire de clés : une clé de signature et la clé de vérification de signature associée liées mathématiquement l'une à l'autre par un algorithme asymétrique ;

Politique de certification (CP): un ensemble précis de règles qui prescrivent l'applicabilité d'un certificat à une collectivité et/ou à une classe d'applications particulières ayant des exigences communes en matière de sécurité ;

Politique en matière de sécurité (SP) : un ensemble de règles et de directives élaborées en fonction d'une analyse de risques pour réduire la probabilité des incidents (mesures préventives) et pallier les effets de ces derniers (mesures correctives), afin de protéger les ressources identifiées comme sensibles pour le fournisseur de services de certification électronique. Les spécifications d'une stratégie et d'une politique en matière de sécurité permettent de définir clairement le niveau de sécurité à atteindre globalement pour un système d'information et spécifiquement pour chaque élément de l'architecture de sécurité ;

Signature électronique ou **signature** : des données électroniques qui sont jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier l'authenticité de ces dernières ;

Signature électronique qualifiée : une signature électronique qui satisfait aux exigences suivantes :

1. être liée uniquement au titulaire ;
2. permettre d'identifier le titulaire ;
3. être créée par des moyens que le titulaire puisse garder sous son contrôle exclusif ;
4. être créée par un dispositif sécurisé de création de signature au sens de l'art. 6, al. 1 et 2 SCSE [1] ;
5. être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ;
6. être basée, au moment de sa création, sur un certificat qualifié valable ;

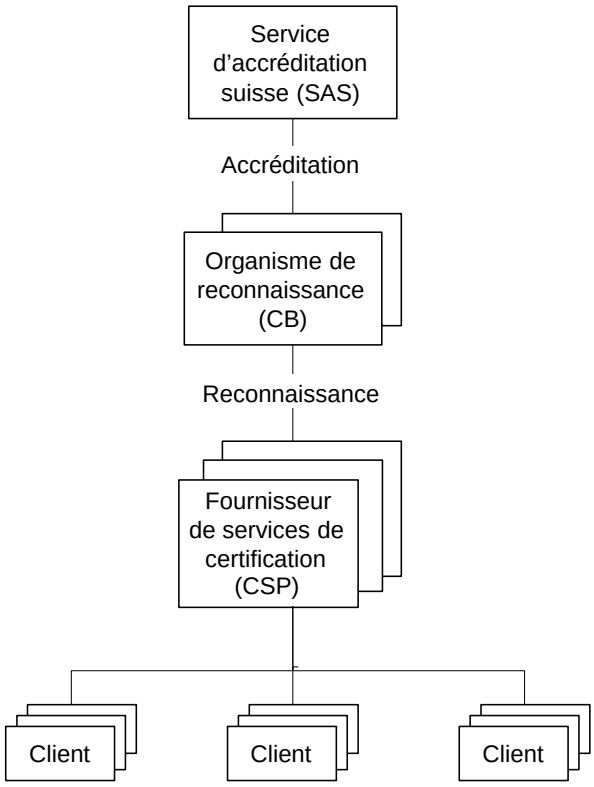
Titulaire du certificat : personne physique, titulaire de la clé de signature correspondant à la clé de vérification de signature qui figure dans le certificat ;

Utilisateur de certificat: personne ou processus qui se fie aux signatures électroniques vérifiées en utilisant ce certificat ;

2 Système pour la reconnaissance des CSP

La reconnaissance des CSP est le fait d'un organisme de reconnaissance (CB) accrédité au sens du système suisse d'accréditation découlant de la LETC [3] et de l'OAccD [4].

Pour se faire accréditer dans le but de reconnaître les fournisseurs de services de certification, les organismes de reconnaissance doivent remplir les critères de la norme européenne EN 45012 [20]. La reconnaissance des CSP suppose l'existence d'au moins un organisme de reconnaissance accrédité. A défaut, l'Office fédéral de la communication (OFCOM) reconnaît les fournisseurs de services de certification.



Les organismes de reconnaissance accrédités sont mentionnés sur le site Internet du SAS (www.sas.ch/) sur lequel figure également la liste des fournisseurs de services de certification reconnus.

3 Exigences essentielles

3.1 Principe

Dans l'objectif de favoriser l'interopérabilité et l'harmonisation internationale et en vertu de l'art. 20, al. 1, SCSE [1], les présentes PTA sont basées sur les spécifications et normes de l'EESSI (Initiative européenne pour la standardisation de la signature électronique) qui trouvent leur fondement dans la directive européenne 1999/93/CE [5].

Ces PTA font plus particulièrement référence à la spécification ETSI TS 101 456 [6] *Policy requirements for certification authorities issuing qualified certificates*.

3.2 Organisation et principes opérationnels

a) L'organisation du CSP doit être conforme à la spécification ETSI TS 101 456 [6], chapitre 7.5, *Organizational*

b) Le CSP doit gérer ses principes opérationnels en conformité avec les références suivantes :

Politiques de certification (CP)	ETSI TS 101 456 [6], chapitres 6.1, *Certification authority obligations* ; 8.1, *Qualified certificate policy management*
Politique d'horodatage	ETSI TS 102 023 [10], chapitre 6.1.1 *TSA obligations - General*
Déclaration des pratiques de certification (CPS)	ETSI TS 101 456 [6], chapitres 6.1, *Certification authority obligations* ; 7.1, *Certification practice statement*
Déclaration des pratiques d'horodatage	ETSI TS 102 023 [10], chapitre 6.1.1 *TSA obligations – General ;* 7.1.1 *TSA Practice Statement*
Politique de gestion en matière de sécurité	ETSI TS 101 456 [6], chapitre 7.4.1, *Security Management* ETSI TS 102 023 [10], chapitre 7.4.1, *Security Management*

c) Toutes les années, le CSP doit mener des audits internes au sens du chapitre 6 de la norme ISO/IEC 27001 [21] pour vérifier la conformité de ses activités:

- à la SCSE [1], à l'OSCSE [2] et aux présentes PTA ;
- à la politique de certification (CP) ;
- à la politique d'horodatage ;
- à la déclaration des pratiques de certification (CPS) ;
- à la déclaration des pratiques d'horodatage.

d) Les audits internes doivent faire l'objet d'enregistrements mettant en évidence tout changement constaté par rapport aux documents susmentionnés. Ces enregistrements doivent être conservés.

e) Les politiques et les pratiques du CSP doivent être conformes à la spécification ETSI TS 101 456 [6], chapitre 7.4, *CA Management and Operation*.

f) Tout équipement réparé et identifié lors de l'analyse de risque comme élément critique du point de vue de la sécurité doit être examiné, configuré et remis en service par deux employés de confiance conformément à une procédure documentée.

g) Le CSP doit documenter un plan de continuité des activités en cas de sinistre tenant compte des aspects suivants :

- détermination des procédures d'urgence en fonction du type de sinistre ;
- documentation des procédures déclenchées après un sinistre (plan de secours) ;
- documentation des procédures permettant de poursuivre l'activité sur un site de secours (plan de reprise) ;
- documentation des procédures permettant de reprendre l'activité normale sur le site d'origine ;
- identification des tâches et des personnes responsables pour chaque procédure ;
- conditions nécessaires pour l'activation de l'une des procédures ;
- formation et sensibilisation des employés concernés ;
- moyens à mettre en œuvre pour tester régulièrement ces procédures ;
- mise à jour des procédures en fonction des résultats des tests ou de l'expérience acquise lors d'un sinistre.

h) Le CSP doit évaluer à intervalles réguliers l'actualité et l'efficacité de son plan de continuité. En fonction de cette évaluation, le CSP doit mettre à jour son plan de continuité.

i) Le CSP doit tenir à jour et sauvegarder régulièrement toutes les informations nécessaires au rétablissement de ses activités après un sinistre. En outre, le CSP doit pouvoir reconstituer ces informations telles qu'elles existaient à l'instant de la dernière sauvegarde.

3.3 Gestion des clés

3.3.1 Gestion des clés du CSP

a) Le CSP doit gérer et utiliser ses propres clés conformément à la spécification ETSI TS 101 456 [6], chapitre 7.2, *Public key infrastructure - Key management life cycle*.

b) Le CSP doit veiller à ce que la manutention des équipements cryptographiques soit conforme à la spécification ETSI TS 101 456 [6], chapitre 7.2, *Public key infrastructure - Key management life cycle*.

3.3.2 Génération des clés du requérant de certificat par le CSP

a) Dans le cas où le CSP génère la paire de clés du requérant, cette génération doit être conforme à la spécification ETSI TS 101 456 [6], chapitre 7.2.8, *CA provided subject key management services*.

b) Dans le cas où le CSP génère la paire de clés du requérant, la génération des clés doit être réalisée dans un dispositif qui:

- remplit les exigences identifiées dans le document FIPS 140-1 [19] ou FIPS 140-2 [13] niveau 3 ou supérieur, ou
- remplit les exigences identifiées dans le document CWA 14167-3 [17], ou
- est évalué au niveau EAL 4 de la norme ISO/IEC 15408 :1999 [11] augmenté des composants d'assurance ADV_IMP.2 (implementation of the TSF), AVA_CCA.1 (vulnerability assessment, covert channel analysis) et AVA_VLA.4 (vulnerability assessment, highly resistant), ou
- est évalué au niveau d'évaluation E3 haut du document ITSEC [14].

Dans les deux derniers cas, une cible d'évaluation remplissant les exigences définies dans le document CWA 14167-3 [17] doit être fournie.

3.3.3 Dispositifs sécurisés de création de signature

a) Le CSP doit fournir aux requérants de certificats ou s'assurer que les requérants de certificats utilisent des dispositifs sécurisés de création de signature conformes aux exigences minimales de l'art. 6, al. 2 de la SCSE [1]. Le document CWA 14169 [15] est réputé assurer la conformité aux exigences de l'art. 6, al. 2 de la SCSE [1].

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

- n'entraîner aucune altération du contenu à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer ;
- le certificat qualifié (ou la référence non ambiguë à ce certificat) doit être présent dans le dispositif ;
- la clé de signature correspondant au certificat qualifié ne doit pas pouvoir être utilisée avant d'avoir été activée par des données d'activation ;
- des tentatives d'activation incorrectes et consécutives doivent 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 saurait être supérieur à quatre ;
- seule une procédure spécifique nécessitant à la fois l'intervention du CSP et la présentation de données d'activation correctes doit permettre de débloquer l'usage d'une clé de signature ayant fait l'objet d'un blocage.

b) La certification des dispositifs sécurisés de création de signature doit être obtenue pour l'ensemble des exigences ci-dessus :

- au niveau d'évaluation EAL 4 de la norme ISO/IEC 15408 :1999 [11] augmenté des composants d'assurance AVA_MSU.3 (vulnerability assessment, analysis and testing of insecure states), AVA_VLA.4 (vulnerability assessment, highly resistant), ou
- au niveau d'évaluation E3 haut du document ITSEC [14].

c) Si le CSP fournit les dispositifs sécurisés de création de signature, il doit procéder à leur manutention conformément à la spécification ETSI TS 101 456 [6], chapitre 7.2.9, *Secure-signature-creation device preparation*.

d) Lorsqu'un dispositif de création de signature est exploité dans un environnement sécurisé, il est considéré comme dispositif sécurisé de création de signature utilisable pour la création de signatures électroniques qualifiées au sens de la SCSE pour autant que les exigences suivantes sont remplies :

- le CSP doit s'assurer que le dispositif de création de signature est certifié selon FIPS 140-2 niveau 3 ou supérieur ;
- le CSP doit s'assurer que le dispositif de création de signature et le serveur contenant l'application de signature sont séparés logiquement de tout composant qui n'est pas en rapport avec la création de la signature;
- le CSP doit s'assurer que l'exploitation du dispositif de création de signature est effectuée par le titulaire du certificat ou sous son mandat formel dûment autorisé ;
- le CSP doit s'assurer que l'exploitation du dispositif de création de signature est effectuée en mettant en œuvre les contrôles mentionnés à l'annexe A de la norme ISO/IEC 27001 [21] et qui ont été identifiés comme nécessaires en fonction de l'analyse de risque ;
- le CSP doit s'assurer que l'accès à l'environnement sécurisé ainsi que l'accès au dispositif de création de signature et à l'application de signature sont contrôlés et journalisés de manière compréhensible.

3.4 Gestion des certificats

3.4.1 Enregistrement, gestion et annulation des certificats de tiers

a) Le CSP doit procéder à l'enregistrement du requérant de certificat et gérer les certificats des titulaires conformément à la spécification ETSI TS 101 456 [6], chapitre 7.3, *Public Key Infrastructure - Certificate Management Life Cycle*.

b) Le CSP qui annule un certificat doit mettre à jour toutes les informations qu'il détient relatives à l'état de ce certificat.

c) Le CSP doit obtenir l'accord du titulaire du certificat avant de publier les causes d'annulation d'un certificat.

d) Le CSP doit établir des listes de certificats annulés (CRL) comprenant les champs tbsCertList, signatureAlgorithm et signatureValue conformément au document RFC 3280 [8], chapitre 5.1.

e) Dans les CRL, le CSP doit inclure les champs suivants à l'intérieur de la séquence tbsCertList conformément au document RFC 3280 [8], chapitre 5.1. :

- version, dont la valeur est 1 pour indiquer qu'il s'agit d'une CRL version 2 ;
- signature ;
- issuer ;
- thisUpdate ;
- nextUpdate ;
- revokedCertificates, comprenant le numéro de série du certificat et la date d'annulation;

f) Dans les CRL, le CSP doit inclure les extensions non-critiques authorityKeyIdentifier et cRLNumber à l'intérieur de la séquence tbsCertList conformément au document RFC 3280 [8], chapitre 5.2.

g) L'annulation est définitive. La suspension de certificats n'est pas autorisée.

3.4.2 Format des certificats des titulaires

a) Le CSP doit générer des certificats comprenant les champs tbsCertificate, signatureAlgorithm et signatureValue conformément au document RFC 3280 [8], chapitre 4.1.

b) Le CSP doit inclure les champs suivants à l'intérieur de la séquence tbsCertificate conformément à l'art. 7 de la SCSE [1] et au document RFC 3280 [8], chapitre 4.1 :

Description	Champ	Contenu
Version	**version**	Selon le document RFC 3280 [8], chapitre 4.1.2.1. Ce champ doit prendre la valeur 2 pour indiquer qu'il s'agit d'un certificat de version 3.
Numéro de série du certificat	**serialNumber**	Selon les documents ITU-T X.509 [7], chapitre 7 et RFC 3280 [8], chapitre 4.1.2.2.
Identifiant de l'algorithme de signature utilisé pour signer le certificat	**signature**	Selon les documents RFC 3280 [8], chapitre 4.1.2.3 et RFC 3279 [18]
- Nom du CSP, - Pays d'établissement du CSP	**issuer**	Selon le document RFC 3280 [8], chapitre 4.1.2.4
Durée de validité du certificat	**validity**	Selon le document RFC 3280 [8], chapitre 4.1.2.5.

- Nom ou pseudonyme et - si nécessaire, les qualités spécifiques du titulaire	**subject**	Selon le document RFC 3739 [9], chapitre 3.1.2.
Clé et algorithme de vérification de la signature du titulaire de certificat	**subjectPublicKeyInfo**	Selon les documents RFC 3280 [8], chapitre 4.1.2.7 et RFC 3279 [18].

c) Le CSP doit inclure les extensions suivantes de la séquence tbsCertificate conformément au document RFC 3280 [8], chapitre 4.2.

Description	Extension critique	Nom de l'extension	Contenu
Identifiant de la clé du CSP qui a signé le certificat	Non	**authorityKeyIdentifier**	Selon le document RFC 3280 [8], chapitre 4.2.1.1.
Domaine d'utilisation du certificat	Oui	**keyUsage**	Selon les documents ITU-T X.509 [7], chapitre 8.2.2.3 et RFC 3280 [8], chapitre 4.2.1.3. Seul le bit no 1 doit être monté pour indiquer que le certificat est utilisable exclusivement pour vérifier des signatures électroniques qui engagent le signataire.
- Politique de Certification - Domaine d'utilisation, si nécessaire	Non	**certificatePolicies**	Selon le document RFC 3280 [8], chapitre 4.2.1.5. Cette extension doit inclure le champ policyQualifiers, à l'intérieur duquel les qualificatifs CPS Pointer et User Notice permettent respectivement de pointer vers les pratiques de certification du CSP et la notice à destination des utilisateurs.
- Mention du caractère reconnu ou non du CSP, - Nom de l'organisme de reconnaissance	Non	**issuerAltName**	Dans l'extension issuerAltName selon RFC 3280 [8], chapitre 4.2.1.8 des certificats qualifiés qu'ils génèrent, les CSP reconnus font figurer le nom de l'organisme de reconnaissance dans la forme suivante: - Organisme de reconnaissance SCSE: « Nom de l'organisme de reconnaissance » Les traductions suivantes sont autorisées : « ZertES-Anerkennungsstelle », « Organismo di riconoscimento FiEle » ou « ZertES Recognition Body ». Les CSP non reconnus font figurer la mention suivante dans l'extension issuerAltName selon RFC 3280 [8], chapitre 4.2.1.8 des certificats qualifiés qu'ils génèrent: - Organisme de reconnaissance SCSE: (CSP non reconnu) Les traductions suivantes sont autorisées : « ZertES-Anerkennungsstelle : (nicht anerkannte CSP) », « organismo di riconoscimento FiEle: (CSP non

			riconosciuto) » ou « ZertES Recognition Body : (unrecognised CSP)»
Points de distribution de la liste des certificats annulés	Non	**cRLDistributionPoints**	Selon les documents ITU-T X.509 [7], chapitre 8.6.2.1 et RFC 3280 [8], chapitre 4.2.1.14. Le champ reasons doit être absent.
Point d'accès au certificat du CSP	Non	**AuthorityInformation Access**	Selon le document RFC 3280 [8], chapitre 4.2.2.1.
Mention précisant que le certificat est délivré à titre de certificat qualifié	Oui/Non	**qcStatements**	Sous la forme d'un identifiant (OID) tel que défini dans le document ETSI TS 101 862 [12], chapitre 5.2.1.
Mention précisant que la clé de signature est protégée par un dispositif sécurisé de création de signature (SSCD)	Oui/Non	**qcStatements**	Sous la forme d'un identifiant (OID) tel que défini dans le document ETSI TS 101 862 [12], chapitre 5.2.4.
Valeur limite des transactions, si nécessaire	Oui/Non	**qcStatements**	Sous la forme d'un identifiant (OID) tel que défini dans le document ETSI TS 101 862 [12], chapitre 5.2.2.

Tout en respectant les spécificités imposées par l'art. 7 SCSE [1], les exigences du présent chapitre sont basées sur la spécification ETSI TS 101 862 [12].

3.4.3 Gestion du certificat du CSP

a) Le CSP doit s'assurer que son certificat comprenne les champs tbsCertificate, signatureAlgorithm et signatureValue conformément au document RFC 3280 [8], chapitre 4.1.

b) Pour son certificat, le CSP doit s'assurer que les champs suivants soient inclus à l'intérieur de la séquence tbsCertificate conformément au document RFC 3280 [8], chapitre 4.1. :

- version, dont la valeur est 2 pour indiquer qu'il s'agit d'un certificat version 3 ;
- serialNumber ;
- signature ;
- issuer ;
- validity ;
- subject;
- subjectPublicKeyInfo ;

c) Pour son certificat, le CSP doit s'assurer que les extensions critiques suivantes de la séquence tbsCertificate soient présentes conformément au document RFC 3280 [8], chapitre 4.2. :

- keyUsage, pour laquelle les bits 5 et 6 doivent être montés ;
- basicConstraints, dont le champ « cA boolean » doit prendre la valeur TRUE ;
- qcStatements, mentionnant que le certificat est qualifié selon le chapitre 3.4.2, let. c du présent document.

d) Pour son certificat, le CSP doit s'assurer que les extensions non-critiques suivantes soient présentes à l'intérieur de la séquence tbsCertificate conformément au document RFC 3280 [8], chapitre 4.2 :

- authorityKeyIdentifier ;
- certificatePolicies ;
- issuerAltName selon chapitre 3.4.2, let. c du présent document ;

- crlDistributionPoints.

3.5 Système d'horodatage

a) Pour délivrer une attestation aux fins d'établir l'existence de données numériques à un moment précis, le CSP doit avoir recours à un système d'horodatage conforme à la spécification ETSI TS 102 023 [10].

b) Le système d'horodatage devra délivrer des contremarques de temps conformes au document ETSI TS 101 861 [16].

c) Le CSP doit signer chaque contremarque de temps au moyen d'une clé réservée uniquement à cet effet. Le certificat correspondant à cette clé doit contenir l'identifiant « id-kp-timeStamping » dans l'extension « Extended Key Usage » selon le RFC 3280 [8], chapitre 4.2.1.13.

Bienne, le

OFFICE FÉDÉRAL DE LA COMMUNICATION

Le directeur :

Martin Dumermuth