BAKOM
OFCOM
UFCOM
UFCOM

RS xxx.xxx.xxx / x.xx

Prescriptions techniques et administratives concernant

les services de certification dans le domaine de la signature électronique

1ère édition: xx.xx.xxxx *[Projet du 1.6.04]*

Entrée en vigueur: xx.xx.xxxx

BAKOM Bundesamt für Kommunikation
OFCOM Office fédéral de la communication
UFCOM Ufficio federale delle communicazioni
UFCOM Uffizi federal da communicaziuns

Zukunftstrasse 44 / Rue de l'Avenir 44
Postfach / Case postale
CH-2501 Biel/Bienne
www.bakom.ch / www.ofcom.ch

Table des matières

1 Généralités

1.1 Champ d'application

Les présentes prescriptions techniques et administratives 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 xxxxxxxx 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 principe 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 XXXXXX, SCSE
Loi fédérale du 19 décembre 2003 sur services de certification électronique dans le domaine de la signature électronique

[2] RS xxx.xxx, OSCSE
Ordonnance du xxxxxxxx sur les services de certification électronique 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

[6] ETSI TS 101 456 v1.2.1 (2002-04)
Policy requirements for certification authorities issuing qualified certificates

[7] TTP.NL Guidance on ETSI TS 101 456 (30 mai 2002)

[8] CWA 14167-1 (Novembre 2001)
Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements

[9] 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

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

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

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

[13] ISO/IEC 15408 :1999
Information technology – Security techniques. Evaluation criteria for IT security

[14] ETSI TS 101 862, v1.3.1 (2004-03)
Qualified Certificate Profile

Les recommandations ITU-T peuvent être obtenues auprès de l'Union internationale des télécommunications (UIT), Place des Nations, 1211 Genève 20 (www.itu.int).

Les normes de l'ISO peuvent être obtenues auprès du Secrétariat central de l'Organisation internationale de normalisation, 1, rue de Varembé, 1211 Genève (www.iso.ch).

Les normes ETSI peuvent être obtenues auprès de l'Institut européen des normes de télécommunication, 650 route des Lucioles, 06921 Sophia Antipolis, France (www.etsi.org).

Les documents du CEN peuvent être obtenues auprès du Comité européen de normalisation, 36 rue de Stassart, B - 1050 Brussels, Belgique (http://www.cenorm.be).

Les textes de loi avec références RS sont publiés dans le recueil systématique des lois fédérales disponible sur le site internet www.bk.admin.ch et peuvent être obtenus auprès de l'Office central fédéral des imprimés et matériel (OCFIM), CH-3003 Berne.

Les prescriptions techniques et administratives peuvent être obtenues auprès de l'OFCOM, rue de l'Avenir 44, case postale, 2501 Bienne (www.ofcom.ch).

1.3 Abréviations

CB	*Certification Bodies* – Organisme de reconnaissance
CEN	Comité européen de normalisation
CP	*Certification Policy* - Politique de certification
CPS	*Certification Pratice 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]
QC	*Qualified Certificate* – Certificat qualifié
RFC	*Request for Comments*
RS	Recueil systématique
SAS	Service d'Accréditation Suisse
SCSE	Loi 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 prescriptions techniques et administratives, 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 ;

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 » doit être interprété comme « certificat qualifié » ;

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

Clé de vérification de signature : des données telles que des codes ou des clés cryptographiques publiques, qui sont 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 pratiques de certification 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 conforme à l'art. 6, al. 2 SCSE 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 du code d'activation (ou mot de passe) permettant d'activer l'usage de la clé privée ;

Fournisseur de services de certification (CSP) : 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 CSP aux fins d'établir l'existence de données numériques à un moment précis ;

Liste des certificats annulés (CRL) : une liste contenant tous les numéros de série des certificats qui ont été annulés avant que la date de validité 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 en fonction d'un algorithme de signature ;

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 ;
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 : le titulaire de la clé de signature correspondant à la clé de vérification de signature qui figure dans le certificat ;

Utilisateur de certificat: personne qui agit en se fiant aux signatures électroniques vérifiées en utilisant ce certificat.

2 Principe de 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]; article 2, lettre g et article 3, alinéa 2).

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. Elle suppose l'existence d'au moins un organisme de reconnaissance accrédité. A défaut, le service d'accréditation suisse (SAS) reconnaît lui-même 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 la SCSE [1], article 20, alinéa 1, les présentes prescriptions techniques et administratives 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].

Les prescriptions techniques et administratives font plus particulièrement référence à la spécification ETSI TS 101 456 [6] *Policy requirements for certification authorities issuing qualified certificates* pour laquelle un guide utile à l'évaluation de la conformité existe sous la dénomination *TTP.NL Guidance on ETSI TS 101 456* [7].

3.2 Environnement et gestion opérationnelle

3.2.1 Organisation

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

b) Toutes les années, le CSP doit mener des audits internes pour vérifier la conformité:

- à la SCSE [1], à l'OSCSE [2] et aux présentes prescriptions techniques et administratives,
- à la politique de certification (CP),
- à la déclaration des pratiques de certification (CPS).

3.2.2 Gestion des politiques

Le CSP doit gérer ses politiques 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*
Déclaration des pratiques de certification (CPS)	ETSI TS 101 456 [6], chapitres 6.1, *Certification authority obligations* ; 7.1, *Certification pratice statement*
Politique de gestion en matière de sécurité	ETSI TS 101 456 [6] 7.4.1, *Security Management*

3.2.3 Gestion de la sécurité

La politique et les pratiques du CSP relatives à la gestion de la sécurité doivent être conformes à la spécification ETSI TS 101 456 [6], chapitre 7.4.1, *Security management*.

3.2.4 Classification et gestion des actifs

La politique et les pratiques du CSP relatives à la classification et à la gestion des actifs doivent être conformes à la spécification ETSI TS 101 456 [6], chapitre 7.4.2, *Asset classification and management*.

3.2.5 Sécurité relative au personnel

La politique et les pratiques concernant la sécurité relative au personnel doivent être mises en œuvre en conformité avec la spécification ETSI TS 101 456 [6], chapitre 7.4.3, *Personnel security*.

3.2.6 Sécurité physique de l'environnement

La politique et les pratiques du CSP relatives à la sécurité physique doivent être conformes à la spécification ETSI TS 101 456 [6], chapitre 7.4.4, *Physical and environmental security*.

3.2.7 Gestion opérationnelle

Le CSP doit mettre en œuvre des pratiques conformes à la spécification ETSI TS 101 456 [6], chapitre 7.4.5, *Operations management* pour s'assurer que ses systèmes sont exploités correctement et de manière sûre.

3.2.8 Accès aux systèmes et aux informations

La politique et les pratiques du CSP relatives à la gestion des accès à ses systèmes et à ses informations doivent être conformes à la spécification ETSI TS 101 456 [6], chapitre 7.4.6, *System access management*.

3.2.9 Systèmes

a) Le CSP doit mettre en œuvre des systèmes et produits conformes au document CWA 14167-1 [8] ou à un profil de protection défini en accord avec la norme ISO/IEC 15408 :1999 [13].

b) La politique et les pratiques relatives à la mise en œuvre et à la maintenance des systèmes et produits doivent être conformes à la spécification ETSI TS 101 456 [6], chapitre 7.4.7, *Trustworthy systems deployment and maintenance*.

3.2.10 Continuité opérationnelle

La politique et les pratiques du CSP relatives à la gestion de la continuité opérationnelle doivent être conformes à la spécification ETSI TS 101 456 [6], chapitre 7.4.8, *Business continuity management.*

3.2.11 Cessation d'activité

La politique et les pratiques du CSP prévues en cas de cessation d'activité doivent être conformes à la spécification ETSI TS 101 456 [6], chapitre 7.4.9, *CA termination*.

3.2.12 Journaux des activités

La politique et les pratiques du CSP relatives aux journaux des activités doivent être conformes à la spécification ETSI TS 101 456 [6], chapitres 7.4.10, *Compliance with legal requirements* et 7.4.11 *Recording of information concerning qualified certificates*.

3.3 Gestion des clés

3.3.1 Génération des clés du CSP

Le CSP doit générer ses propres clés conformément à la spécification ETSI TS 101 456 [6], chapitre 7.2.1, *Certification authority key generation*.

3.3.2 Conservation de la clé de signature du CSP

Le CSP doit conserver sa clé de signature conformément à la spécification ETSITS 101 456 [6], chapitre 7.2.2, *Certification authority key storage, backup and recovery*.

3.3.3 Distribution de la clé de vérification de signature du CSP

Le CSP doit distribuer sa clé de vérification de signature conformément à la spécification ETSI TS 101 456 [6], chapitre 7.2.3, *Certification authority public key distribution*.

3.3.4 Utilisation de la clé de signature du CSP

a) Le CSP doit utiliser sa clé de signature conformément à la spécification ETSI TS 101 456 [6], chapitre 7.2.5, *Certification authority key usage*.

b) Le CSP doit cesser d'utiliser une paire de clés si la période de validité est expirée ou si la clé de signature est compromise ou présumée compromise.

3.3.5 Destruction de la clé de signature du CSP

Le CSP doit détruire sa clé de signature conformément à la spécification ETSI TS 101 456 [6], chapitre 7.2.6, *End of CA key live cycle*.

3.3.6 Remplacement de la clé de signature du CSP

Le CSP doit procéder au remplacement de sa clé de signature conformément à la spécification ETSI TS 101 456 [6], chapitre 7.4.8, *Business continuity management and incident handling*.

3.3.7 Manutention des équipements cryptographiques

Le CSP doit veiller à ce que la manutention des équipements cryptographiques soit conforme à la spécification ETSI TS 101 456 [6], chapitres 7.2.2, *Certification authority key storage, backup and recovery* ; 7.2.7, *Life cycle management of cryptographic hardware used to sign certificates* ; 7.2.9, *Secure-Signature-Creation device preparation*.

3.3.8 Génération des clés du requérant de certificat

a) Dans le cas où le CSP génère lui-même la paire de clé 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 requérant du certificat génère lui-même sa paire de clés, le CSP doit veiller à ce que cette dernière a bien été générée dans un dispositif sécurisé de création de signature tel que défini au 3.3.9“ du présent document.

3.3.9 Dispositifs sécurisés de création de signature

a) Le CSP doit utiliser et fournir aux requérants de certificats des dispositifs sécurisés de création de signature développés selon un profil de protection qui est conforme à l'art. 6, al. 2, SCSE [1].

b) Le CSP doit procéder à la manutention des dispositifs sécurisés de création de signature conformément à la spécification ETSI TS 101 456 [6], chapitre 7.2.9, *Secure-signature-creation device preparation*.

3.4 Gestion des certificats

3.4.1 Enregistrement

a) Le CSP doit procéder à l'enregistrement du requérant de certificat conformément à la spécification ETSI TS 101 456 [6], chapitre 7.3.1, *Subject registration*.

3.4.2 Génération des certificats

a) Le CSP doit générer les certificats dont le format est conforme au chapitre 3.4.3.1.

b) Le CSP doit générer les certificats en conformité avec la spécification ETSI TS 101 456 [6], chapitre 7.3.3, *Certificate Generation*.

3.4.3 Format des certificats

Tout en respectant les spécificités imposées par la SCSE [1], les exigences du présent chapitre sont basées sur la spécification ETSI 101 862 [14].

3.4.3.1 Champs du certificat

Le CSP doit générer des certificats conformément aux dispositions du présent chapitre.

Description	Champs/extension/attribut	Contenu
Numéro de série	**serialNumber**	Le numéro de série du certificat selon les documents ITU-T X.509 [9], chapitre 7 et RFC 3280 [10] chapitre 4.1.2.2.
Nom/pseudonyme et qualités spécifiques du titulaire	**subject** **title**	Le nom ou le pseudonyme de la personne physique qui est le titulaire de la clé de signature et ses qualités spécifiques pour représenter une personne morale déterminée, selon le document RFC 3739 [11] chapitres 3.1.2.
Clé et algorithme de vérification de signature	**subjectPublicKeyInfo**	La clé et l'identifiant de l'algorithme de vérification de signature du titulaire de certificat selon le document RFC 3280 [10], chapitre 4.1.2.7.
Durée de validité	**validity**	La durée de validité du certificat selon le document RFC 3280 [10], chapitre 4.1.2.5.
Nom du CSP et pays d'établissement du CSP	**Issuer** **countryName**	Le nom du CSP et le pays d'établissement du CSP selon le document RFC 3739 [11], chapitre 3.1.1.
Signature électronique qualifiée du CSP	**signatureValue**	La signature électronique qualifiée du CSP selon le document RFC 3280 [10], chapitre 4.1.1.3.
La mention du caractère reconnu ou non du fournisseur	**issuerAltName**	L'extension issuerAltName selon le document RFC 3280 [10], chapitre 4.2.1.8 doit contenir les informations suivantes O = EA O = SAS O = « Nom de l'organisme de reconnaissance » CN = « Nom du fournisseur »
Domaine d'utilisation	**keyUsage**	Domaine d'utilisation selon les documents ITU-T X.509 [9] chapitre 8.2.2.3 et RFC 3280 [10], chapitre 4.2.1.3. Seul le bit no 1 doit être monté pour indiquer que le certificat est utilisé pour la vérification de la signature.
Points de distribution de la liste des certificats annulés	**cRLDistributionPoints**	Points de distribution de la liste des certificats annulés selon les documents ITU-T X.509 [9] chapitre 8.6.2.1 et RFC 3280 [10], chapitre 4.2.1.14
Valeur des	**QCStatements**	La valeur limite maximale des transactions sont

transactions		indiquées dans l'extension QCStatements selon le document RFC 3739 [11], chapitre 3.2.6, sous la forme d'un identifiant (OID) de déclaration tel que défini dans le document ETSI TS 101 862 [14], chapitre 5.2.2.
Mention précisant qu'il s'agit d'un Certificat Qualifié	**QCStatements**	L'information qu'il s'agit d'un certificat qualifié est présente dans l'extension QCStatements selon le document RFC 3739 [11], chapitre 3.2.6, sous la forme d'un identifiant (OID) de déclaration tel que défini dans le document ETSI TS 101 862 [14], chapitre 5.2.1.
Indicateur précisant que la clé de signature est protégée par un dispositif sécurisé de création de signature (SSCD)	**QCStatements**	L'extension précise que la clé de signature est protégée par un SSCD au sens de l'annexe III de la Directive Européenne [5]. Cette information est présente dans l'extension QCStatements selon le document RFC 3739 [11], chapitre 3.2.6, sous la forme d'un identifiant (OID) de déclaration tel que défini dans le document ETSI TS 101 862 [14], chapitre 5.2.4.

3.4.4 Renouvellement et mise à jour du certificat

Le CSP doit renouveler et mettre à jour un certificat conformément à la spécification ETSI TS 101 456 [6], chapitre 7.3.2, *Certificate renewal, rekey and update*.

3.4.5 Annulation du certificat

a) Le CSP doit annuler les certificats conformément à la spécification ETSI TS 101 456 [6], chapitre 7.3.6*, Certificate revocation and suspension*.

b) Le CSP qui annule un certificat doit mettre à jour toutes les informations qu'il détient relatives à l'état de ce certificat. Si le CSP publie des listes de certificats annulés (CRL), il devra y faire figurer tout certificat annulé.

3.4.6 Diffusion des certificats

a) Suite à la génération, le CSP doit rendre disponible le certificat à son titulaire.

b) Dans le cas où le CSP met à disposition un service d'annuaire, il doit s'assurer que le titulaire consent à la publication de son certificat dans l'annuaire. Il doit par ailleurs informer le titulaire qu'il peut retirer en tout temps son consentement à la publication du certificat dans l'annuaire

c) Dans le cas où le CSP met à disposition un service d'annuaire, il doit en assurer la disponibilité conformément à la spécification ETSI TS 101 456 [6], chapitre 7.3.5, *Certificate dissemination*.

3.4.7 Publication de l'état des certificats

Le CSP doit s'assurer que l'information relative à l'état annulé du certificat soit disponible à son titulaire et aux utilisateurs de certificat conformément à la spécification ETSI TS 101 456 [6], chapitre 7.3.6, *Certificate revocation and suspension*.

3.4.8 Information relatives aux conditions d'utilisation des certificats

Le CSP doit informer les titulaires et les utilisateurs de certificats concernant les conditions d'utilisations conformément à la spécification ETSI TS 101 456 [6], chapitre 7.3.4, *Dissemination of terms and conditions*.

3.5 Système d'horodatage

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 102 023 [12].

Bienne, le (*même date que « édition » en première page*)

OFFICE FÉDÉRAL DE LA COMMUNICATION

Le directeur :

Marc Furrer