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

Annexe de l'ordonnance de l'OFCOM du 23 novembre 2016 sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (RS 943.032.1)

Prescriptions techniques et administratives

concernant

les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques

1ère édition : 23.11.2016
Entrée en vigueur : 1.1.2017

Table des matières

1 Généralités

1.1 Champ d'application

Les présentes prescriptions techniques et administratives (PTA) constituent l'annexe de l'ordonnance de l'OFCOM du 23 novembre 2016 sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (RS 943.032.1). Elles se fondent sur :

- l'art. 21, al. 2, de la loi du 18 mars 2016 sur la signature électronique (SCSE) [1],
- les art. 3, al. 2, 4, al. 1, 10 et 15 de l'ordonnance du 23 novembre 2016 sur la signature électronique (OSCSE) [2].

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 qualifiés et qui peut fournir d'autres services dans le domaine de la signature électronique et des autres applications des certificats numériques.

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 du 18 mars 2016 sur la signature électronique

[2] RS 943.032, OSCSE
Ordonnance du 23 novembre 2016 sur la signature électronique

[3] ETSI EN 319 411-2 V2.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[4] FIPS 140-2 (2001)
Security Requirements for Cryptographic Modules

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

[6] EN 419211-2:2013
Protection profiles for secure signature creation device. Part 2: Device with key generation

[7] EN 419211-3:2013
Protection profiles for secure signature creation device. Part 3: Device with key import

[8] EN 419211-4:2014
Protection profiles for secure signature creation device. Part 4: Extension for device with key generation and trusted channel to certificate generation application

[9] EN 419211-5:2014
Protection profiles for secure signature creation device. Part 5: Extension for device with key generation and trusted channel to signature creation application

[10] EN 419211-6:2014
Protection profiles for secure signature creation device. Part 6: Extension for device with key import and trusted channel to signature creation application

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

[12] ISO/IEC 15408-3:2008
Information technology – Security techniques. Evaluation criteria for IT security —Part 3: Security assurance components

[13] CEN/TS 419241:2014
Security Requirements for Trustworthy Systems Supporting Server Signing

[14] ETSI EN 319 412-1 V1.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

[15] ETSI EN 319 412-2 V2.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[16] ETSI EN 319 412-3 V1.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[17] ETSI EN 319 412-4 V1.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

[18] ETSI EN 319 412-5 V2.1.1 (2016-02)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[19] RFC 5280 (mai 2008)
Internet X.509 Public Key Infrastructure - Certificate and CRL Profile

[20] Common PKI Specifications for Interoperable Applications. Version 2.0 – 20 January 2009

[21] ETSI EN 319 421 V1.1.1 (2016-03)
Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

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

Les documents référencés peuvent être obtenus auprès des organisations suivantes :

Textes de loi avec références RS	Office fédéral des constructions et de la logistique (OFCL) Service de diffusion des publications fédérales CH-3003 Berne www.bundespublikationen.admin.ch
Documents ETSI	ETSI, Institut européen des normes de télécommunication 650 route des Lucioles 06921 Sophia Antipolis, France www.etsi.org
Documents FIPS	National Institute of Standards and Technology (NIST) csrc.nist.gov/publications
Documents du CEN	Comité européen de normalisation (CEN) 36, rue de Stassart B - 1050 Brussels, Belgique www.cenorm.be
Normes EN	Association suisse de normalisation (SNV) Bürglistr. 29 CH-8400 Winterthur www.snv.ch
Normes de l'ISO	Secrétariat central de l'Organisation internationale de normalisation (ISO)

	1, rue de Varembé 1211 Genève www.iso.org
Documents RFC	Internet Engineering Task Force (IETF) www.ietf.org
Common PKI Specifications for Interoperable Applications	T7 (Arbeitsgemeinschaft von deutschen Trustcenterbetreibern und Zertifizierungsdiensteanbietern) www.t7ev.org
Prescriptions techniques et administratives	OFCOM Rue de l'Avenir 44 Case postale 2501 Bienne www.ofcom.admin.ch

1.3 Abréviations

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
EAL	*Evaluation Assurance Level* – Niveau de garantie de l'évaluation
EN	*European Normative* – Normatif européen
ETSI	*European Telecommunications Standards Institute* - Institut européen des normes de télécommunication
FIPS	*Federal Information Processing Standards*
IDE	Numéro d'identification des entreprises
IEC	*International Electrotechnical Commission* – Commission électrotechnique internationale
IETF	*Internet Engineering Task Force*
ISO	*International Standardization Organization* - Organisation internationale de normalisation
LIDE	Loi fédérale sur le numéro d'identification des entreprises
OID	*Object identifier* – Identificateur d'objet
OSCSE	Ordonnance sur la signature électronique [2]
PIN	*Personal Identification Number* – Numéro d'identification personnel
PKI	*Public Key Infrastruktur* – Infrastructure à clé publique
RFC	*Request for Comments*
RS	Recueil systématique
SCSE	Loi sur la signature électronique [1]

2 Exigences essentielles

2.1 Organisation et principes opérationnels

2.1.1 Politique de certification et déclaration des pratiques de certification

Le CSP élabore et gère une politique de certification (CP) ainsi qu'une déclaration des pratiques de certification (CPS) conformément à la norme ETSI EN 319 411-2 [3], chapitres 5 *General provisions on Certificate Pratice Statement* and *Certificate Policies* et 7 *Framework for the definition of other certificate policies*.

2.1.2 Gestion de la sécurité

Le CSP met en œuvre un système de gestion de la sécurité conformément à la norme ETSI EN 319 411-2 [3], chapitres 6.4 *Facility, Management, and Operational Controls*, 6.5.5 *Computer Security Controls*, 6.5.6 *Life Cycle Security Controls*, 6.5.7 *Network Security Controls*.

2.1.3 Aspects financiers et légaux

Les pratiques du CSP sont conformes à la norme ETSI EN 319 411-2 [3], chapitre 6.8 *Other Business and Legal Matters*.

2.1.4 Autres aspects organisationnels et opérationnels

Les pratiques du CSP sont conformes à la norme ETSI EN 319 411-2 [3], chapitre 6.9 *Other Provisions*.

2.2 Gestion des clés

2.2.1 Gestion et utilisation des clés du CSP

Le CSP doit gérer et utiliser ses propres clés conformément à la norme ETSI EN 319 411-2 [3], chapitres 6.5.1 *Key Pair Generation and Installation*, 6.5.2 *Private Key Protection and Cryptographic Module Engineering Controls*, 6.5.3 *Other Aspects of Key Pair Management*, 6.5.4 *Activation Data.*

2.2.2 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 norme ETSI EN 319 411-2 [3], chapitres 6.5.1 *Key Pair Generation and Installation,* 6.5.2 *Private Key Protection and Cryptographic Module Engineering Controls,* 6.5.4 *Activation Data*.

b) Dans le cas où le CSP génère la paire de clés du requérant, la génération des clés doit être réalisée dans l'un des dispositifs suivants :

- dispositif certifié conforme aux exigences identifiées dans le document FIPS 140-2 [4] niveau 3 ou supérieur ;
- dispositif remplissant les exigences identifiées dans le document CWA 14169 [5] et évalué au niveau EAL 4 de la norme ISO/IEC 15408:2005 [11] augmenté des composants d'assurance ADV-IMP.2 (*implementation of the TSF*), AVA-CCA.1 (*vulnerability assessment, covert channel analysis*) et AVA_VLA.1 (*vulnerability assessment, highly resistant*) ou les composants d'assurance correspondants de la norme ISO/IEC 15408-3:2008 [12] ;
- dispositif remplissant les exigences identifiées dans la norme EN 419211-2 [6], EN 419 211-4 [8] ou EN 419211-5 [9] et évalué au niveau EAL 4 de la norme ISO/IEC 15408-3:2008 [12] augmenté des composants d'assurance AVA_VAN.5 (*Advanced methodical vulnerability analysis*) ou des critères d'évaluation équivalents reconnus en matière de sécurité ;
- dispositif évalué au niveau EAL 4 de la norme ISO/IEC 15408-3:2008 [12] augmenté des composants d'assurance AVA_VAN.5 (*Advanced methodical vulnerability analysis*) ou des critères d'évaluation équivalent reconnus en matière de sécurité. Dans ce cas, une cible d'évaluation remplissant les exigences définies dans les documents susmentionnés doit être fournie.

2.2.3 Dispositifs sécurisés de création de signatures et de cachets

a) Le CSP doit fournir aux requérants de certificats ou s'assurer que les requérants de certificats utilisent des dispositifs sécurisés de création de signatures et de cachets conformes aux exigences minimales de l'art. 6, al. 2, SCSE [1]. Les documents suivants sont réputés assurer la conformité aux exigences de l'art. 6, al. 2, SCSE [1] :

- CWA 14169 [5]
- EN 419211-2 [6]
- EN 419211-3 [7]
- EN 419211-4 [8]
- EN 419211-5 [9]
- EN 419211-6 [10]

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

- lorsqu'un nombre prédéterminé de tentatives d'activation incorrectes et consécutives a été atteint, l'usage de la clé cryptographique privée doit être bloqué. Ce nombre ne saurait être

supérieur à 4 tentatives pour une longueur de PIN de 6 signes. Pour un PIN plus long, il peut être supérieur à 4 dans la mesure où la documentation mise à disposition par le développeur du dispositif sécurisé de création de signatures et de cachets certifié le prévoit;

- le CSP ne peut débloquer l'usage de la clé cryptographique privée qu'après avoir vérifié que la demande de déblocage émane du titulaire des clés.

b) La certification des dispositifs sécurisés de création de signatures et de cachets doit être obtenue pour l'ensemble des exigences mentionnées à la let. a :

- au niveau EAL 4 de la norme ISO/IEC 15408:2005 [11] augmenté des composants d'assurance ADV-IMP.2 (*implementation of the TSF*), AVA-CCA.1 (*vulnerability assessment, covert channel analysis*) et AVA_VLA.1 (*vulnerability assessment, highly resistant*), ou

- au niveau d'évaluation EAL 4 de la norme ISO/IEC 15408-3:2008 [12] augmenté du composant d'assurance AVA_VAN.5 (*Advanced methodical vulnerability analysis*).

c) Si le CSP fournit les dispositifs sécurisés de création de signatures et de cachets, il doit procéder à leur manutention conformément à la norme ETSI EN 319 411-2 [3], chapitres 6.5.1 *Key Pair Generation and Installation,* 6.5.2 *Private Key Protection and Cryptographic Module Engineering Controls* et 6.5.4 *Activation Data*.

d) Un système permettant de générer des signatures électroniques et des cachets au moyen d'un dispositif qui n'est pas en possession du titulaire du certificat de signature est considéré comme dispositif sécurisé de création de signatures au sens de l'art. 6 SCSE [1] pour autant qu'il soit conforme aux exigences de la norme CEN/TS 419241 [13]. Le système doit assurer l'authentification du titulaire de la clé cryptographique privée selon le niveau 2 (*Level 2 sole control*) décrit dans le document CEN/TS 419241 [13].

2.3 Gestion des certificats réglementés

2.3.1 Délivrance, gestion et annulation des certificats réglementés de tiers

a) Le CSP doit procéder à l'enregistrement du requérant de certificat ainsi que gérer et annuler les certificats des titulaires conformément à la norme ETSI EN 319 411-2 [3], chapitres 6.1 *Publication and Repository Responsibilities*, 6.2 *Identification and Authentication,* 6.3 *Certificate Life-Cycle Operational Requirements*.

b) Le CSP doit annuler le certificat lorsque l'organisme ayant confirmé la qualification professionnelle selon le ch. 2.3.2 let. h l'informe que l'attestation n'est plus valable.

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

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

e) La suspension de certificats n'est pas autorisée.

2.3.2 Format des certificats réglementés

a) Le CSP doit générer des certificats réglementés de personnes physiques conformément à la norme ETSI EN 319 412-2 [15].

b) Le CSP doit générer des certificats réglementés d'entités IDE conformément à la norme ETSI EN 319 412-3 [16].

c) Le CSP doit générer des certificats réglementés qui se rapportent à des sites web conformément à la norme ETSI EN 319 412-4 [17].

d) La mention « *regulated certificate* » indiquant que le certificat est délivré à titre de certificat réglementé doit figurer dans le champ *explicitText* de l'extension *certificatePolicies* selon la norme RFC 5280 [19], ch. 4.2.1.4.

e) Le numéro unique d'identification des entreprises au sens de la LIDE doit être mentionné pour les entités IDE selon la norme ETSI EN 319 412-1 [14], ch. 5.1.4.

f) Le bit 1 (*contentCommitment*) de l'extension *keyUsage* ne doit être activé que pour les certificats réglementés de personnes physiques.

g) Dans les certificats réglementés qui se rapportent à une clé de vérification de signature ou de cachet, la mention indiquant que la clé cryptographique privée est protégée par un dispositif sécurisé de création de signatures et de cachets doit figurer sous forme d'un identifiant (OID) selon la norme ETSI EN 319 412-5 [18], ch. 4.2.2.

h) Si nécessaire, une qualification professionnelle est mentionnée dans le certificat réglementé en insérant l'attribut *Admission* dans la séquence *tbsCertificate* conformément au document RFC 5280 [19], chapitre 4.2.

L'organisme qui confirme la qualification professionnelle (art. 5, al. 2, OSCSE [2]) doit être mentionné en tant que *directoryName* dans le champ de données *admissionAuthority* conformément au document Common PKI Specification [20], tableau 29b avec les attributs indiqués ci-dessous et dans le même ordre :
- *organizationName*: nom de l'organisme ;
- *countryName*: pays de l'organisme ;
- *postalAddress*: adresse de l'organisme.

Le certificat réglementé ne peut comprendre qu'une qualification professionnelle. La qualification professionnelle du titulaire du certificat doit être définie en utilisant le champ de données *professionItems* dans la séquence *professionInfo* conformément au document Common PKI Specification [20], tableau 29b.
L'OID de la qualification professionnelle doit de plus être défini en utilisant le champ de données

professionOID dans la séquence *professionInfo* conformément au document Common PKI Specification [20], tableau 29b.

i) Si nécessaire, l'attribut *title* du champ *subject* selon le document RFC 5280 [19], ch. 4.1.2.6 est utilisé de manière explicite pour indiquer que le titulaire du certificat réglementé est habilité à représenter l'entité IDE désignée au moyen de l'attribut *organization* du même champ *subject*.

j) Si nécessaire, le domaine d'utilisation pour lequel le certificat réglementé est prévu est décrit dans la politique de certification identifiée dans l'extension *certificatePolicies* selon le document RFC 5280 [19], ch. 4.2.1.5.

k) Si nécessaire, la mention valeur limite des transactions est mentionnée selon la norme ETSI EN 319 412-5 [18], ch. 4.3.2.

2.3.3 Exigences supplémentaires applicables au format des certificats qualifiés

a) Le CSP doit générer des certificats qualifiés conformément à la norme ETSI EN 319 412-2 [15].

b) Seul le bit 1 (*contentCommitment*) de l'extension *keyUsage* doit être utilisé.

c) La mention «*qualified certificate*» indiquant que le certificat est délivré à titre de certificat qualifié doit figurer dans le champ *explicitText* de l'extension *certificatePolicies* selon la norme RFC 5280 [19], ch. 4.2.1.4. Le certificat comprend en sus la déclaration décrite au ch. 4.2.3 de la norme ETSI EN 319 412-5 [18].

2.3.4 Gestion du certificat du CSP utilisé pour l'émission de certificats réglementés

a) Le CSP doit générer ses propres certificats réglementés conformément à la norme IETF RFC 5280 [19].

b) La mention «*regulated certificate*» indiquant que le certificat est délivré à titre de certificat réglementé doit figurer dans le champ *explicitText* de l'extension *certificatePolicies* selon la norme RFC 5280 [19], ch. 4.2.1.4.

c) Le numéro unique d'identification des entreprises au sens de la LIDE doit être mentionné selon la norme ETSI EN 319 412-1 [14], ch. 5.1.4.

2.4 Système d'horodatage qualifié

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 qualifié conforme à la norme ETSI EN 319 421 [21].

b) Le système d'horodatage qualifié devra délivrer des contremarques de temps conformes au document ETSI EN 319 422 [22].

Biel/Bienne, le 23 novembre 2016

OFFICE FÉDÉRAL DE LA COMMUNICATION

Philipp Metzger
Directeur