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

Février 2022

Prescriptions techniques et administratives sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (2e édition)

Rapport explicatif

1 Introduction

Le présent document fournit les explications relatives aux modifications introduites dans la 2ème édition (2022) des prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (PTA).

2 Modifications

Ch. 1.2

De nouvelles normes ou de nouvelles versions de normes référencées dans la précédente édition des PTA ont été publiées par le comité européen de normalisation (CEN) et par l'institut européen des normes de télécommunication (ETSI). Ces développements sont pris en compte dans la 2ème édition des PTA.

Le tableau suivant présente la correspondance entre les anciennes et les nouvelles références :

Référence dans la 1ère édition des PTA (2017)	**Nouvelle référence dans la 2ème édition des PTA (2022)**
ETSI EN 319 411-2 V2.1.1 (2016-02) *Policy requirements for trust service providers issuing EU qualified certificates*	ETSI EN 319 411-2 V2.4.1 (2021-11) *Policy requirements for trust service providers issuing EU qualified certificates*
EN 419211-3:2013 *Protection profiles for secure signature creation device. Part 3: Device with key import*	EN 419211-3:2014 *Protection profiles for secure signature creation device. Part 3: Device with key import*
CEN/TS 419 241:2014 *Security Requirements for Trustworthy Systems Supporting Server Signing*	EN 419 241-1:2018 *Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements* EN 419 241-2:2019 *Protection Profile for QSCD for Server Signing* TS 119 431-1 V1.2.1 (2021-05) *Policy and Security Requirements for TSP Service Components Operating a Remote QSCD / SCD* EN 419221-5:2018 *Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services*
ETSI EN 319 412-1 V1.1.1 (2016-02) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*	ETSI EN 319 412-1 V1.4.4 (2021-05) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*
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*	ETSI EN 319 412-2 V2.2.1 (2020-07) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons*

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*	ETSI EN 319 412-3 V1.2.1 (2020-07) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons*
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	ETSI EN 319 412-4 V1.2.1 (2021-11) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
ETSI EN 319 412-5 V2.1.1 (2016-02) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*	ETSI EN 319 412-5 V2.3.1 (2020-04) *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

Les nouvelles versions des normes comprennent en principe en annexe la description des modifications effectuées. Des explications relatives aux modifications les plus importantes figurent dans les chapitres suivants.

Ch. 2.1.1

Le titre du ch. 7 de la norme ETSI EN 319 411-2 est complété en conformité avec cette dernière.

Ch. 2.2.2, let. a)

La référence au ch. 6.5.2 de la norme ETSI EN 319 411-2 est supprimée car ce chapitre de la norme ne comprend pas d'exigence relative à la génération des clés du requérant de certificat par le CSP dont il est question au ch. 2.2.2 des PTA.

Ch. 2.2.2, let. b)

La référence à FIPS 140-3 est ajoutée car les certifications FIPS de modules crytographiques sont dorénavant effectuées selon cette norme. La référence à FIPS 140-2 est maintenue pour prendre en compte les certifications précédemment effectuées.

La référence au document CWA 14169 est supprimée car ce dernier a été remplacé par la série de normes EN 419 211 (cf. Introduction dans EN 419 211-1 ainsi que l'annexe de la décision d'exécution (UE) 2016/650 de la Commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.1).

[1] JO L 109 du 26.4.2016, pp. 40–42

Ch. 2.2.3, let. a) et b)

Dans ce chapitre également, la référence au document CWA 14169 est supprimée car ce dernier a été remplacé par la série de normes EN 419211 (cf. ci-dessus).

La suppression de la référence au document CWA 14169 permet de supprimer également la référence à la version 2005 de la norme ISO/IEC 15408 qui figurait dans ce chapitre uniquement pour déterminer le niveau des certifications de produits effectuées en conformité des exigences figurant dans le document CWA 14169.

L'exigence relative au nombre prédéterminé de tentatives d'activation incorrectes et consécutives est supprimée car la certification de produit exigée dans ce même chapitre confirme que le dispositif de création de signature est conforme à des exigences suffisantes pour l'utilisation prévue.

L'exigence à laquelle le CSP doit se conformer en cas de blocage de l'usage de la clé cryptographique privée est déplacée en e) car elle ne vise pas directement le dispositif de création de signature dont il est question à la lettre a). Il s'agit plutôt d'une exigence relative à un processus opérationnel que le CSP doit mettre en œuvre lorsqu'il offre un tel service de déblocage.

Ch. 2.2.3, let. c)

Les PTA font référence au ch. 6.5.1 de la norme ETSI EN 319 411-2. Dans la nouvelle version de cette dernière, de nouvelles exigences relatives aux mesures à prendre lorsqu'un dispositif de création de signature perd sa certification ont été ajoutées.

La référence au ch. 6.5.2 de la norme ETSI EN 319 411-2 est supprimée car ce chapitre de la norme ne comprend pas d'exigence relative à la génération des clés du requérant de certificat par le CSP dont il est question au ch. 2.2.3 des PTA.

Ch. 2.2.3, let. d)

La lettre d) précise les exigences relatives aux services de signatures qui peuvent être utilisés pour la génération de signatures électroniques et de cachets. Dans le cadre de ces services, la clé de signature du titulaire du certificat est stockée et est utilisée dans l'infrastructure d'un fournisseur de services sous le contrôle exclusif du titulaire de la clé de signature et du certificat. De tels services sont parfois également désignés par « signing services », « signature in the cloud » ou encore « signing server ». Dans les PTA, il est question de « dispositif que le titulaire de certificat n'a pas en sa possession ». Il s'agit en effet généralement d'un système comprenant un module cryptographique par lequel la signature est générée et un module d'activation de la signature qui assure que la clé de signature soit utilisée sous le contrôle exclusif de son titulaire.

Après l'entrée en vigueur de la 1ère édition des PTA, les experts du CEN et de l'ETSI ont poursuivi leurs travaux de normalisation concernant ces systèmes. Les nouvelles normes ETSI TS 119 431-1, EN 419241-1, EN 419241-2 et EN 419221-5 ont été publiées et sont dorénavant reconnues pour l'évaluation des services de signatures. Les PTA doivent donc être adaptées pour prendre en compte ces développements. La nouvelle spécification ETSI TS 119 431-2 ne s'applique pas aux éléments qui font partie de l'environnement du dispositif de création de signature mis en œuvre dans le cadre d'un service de signature (cf. EN 419241 ch. 1.2, 3.10, 5.13.2 et ETSI TS 119 431-2 ch. 4.3). Pour cette raison, elle n'est pas mentionnée au ch. 2.2.3, let. d).

La désignation du niveau d'assurance requis pour accéder à un tel service est adaptée afin qu'elle corresponde à la nouvelle désignation SCAL-2 mentionnée dans la norme EN 419241-1.

Il existe dans le marché des services de signatures qui mettent en œuvre un système dont les composants ont précédemment été évalués selon d'autres critères pour la génération de signatures électroniques et de cachets. Ces systèmes sont tolérés en tant que dispositifs sécurisés de création de signatures électroniques et de cachets au sens de l'art. 6, al. 2 SCSE, pour autant qu'ils soien conformes à des objectifs de sécurité similaires à ceux des normes EN 419241-2 et EN 419221-5. A l'instar des pays européens qui tolèrent les services de signature, on assure ainsi une transition jusqu'à ce que les normes EN 419241-2 et EN 419221-5 se soient imposées pour l'évaluation de tels systèmes. Lorsqu'il en sera ainsi, la Commission européenne prévoit d'adapter sa décision d'exécution (UE) 2016/650[2] pour y mentionner ces nouvelles normes qui seront alors applicables dans le cadre de la certification de ces dispositifs de création de signature. Ces normes seront ensuite applicables dans le cadre de l'évaluation des dispositifs de création de signature. Une nouvelle révision des PTA sera alors nécessaire afin d'harmoniser les exigences suisses à celles des pays européens.

S'ils offrent de tels services de signatures, les CSP devront se conformer aux exigences du ch. 2.2.3, let. d) dans les 6 mois qui suivent l'entrée en vigueur. Jusqu'à l'échéance de ce délai, l'exigence correspondante prévue aux ch. 2.2.3, let. d) de la 1ère édition des prescriptions techniques et administratives du 23 novembre 2016 reste applicable (cf. ch. 3).

Ch. 2.3.1, let. a)

L'ETSI a récemment publié la spécification ETSI TS 119 461 pour préciser les exigences relatives aux vérifications d'identités effectuées par le fournisseur de services en présence de la personne à identifier ou à distance.

Ce document répond à la demande des pays européens (cf. ch. 2, *Position Paper On the review of the eIDAS Regulation - FESA's answer to the European Commission's consultation* http://www.fesa.eu/public-documents/FESA_Position_Paper_eIDAS_2020_Review.pdf) et à la recommandation de l'agence européenne de cybersécurité ENISA (cf. ch. 5, *ENISA Report - REMOTE ID PROOFING Analysis of Methods to carry out identity proofing remotely* https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing) de préciser les exigences relatives à l'identification à distance.

La référence à cette nouvelle spécification est ajoutée dans les PTA avant tout afin de préciser l'art. 7, al. 1, OSCSE et de faciliter l'évaluation de processus d'identification à distance, notamment par le biais d'une communication audiovisuelle en temps réel (communication vidéo). Ce développement répond à la demande croissante des fournisseurs de services de certification et de leurs clients de simplifier le processus d'identification. La nouvelle spécification de l'ETSI concrétise également les art. 5 et 6 OSCSE s'agissant de la vérification de l'identité des requérants de certificats en présence de la personne.

Suivant la situation de fait, différentes exigences de la spécification technique s'appliquent. La 2ème édition des PTA part des cas d'utilisation (*use cases*) décrits au chapitre 9 de la spécification de l'ETSI. Les cas d'utilisation du chapitre 9.2 (*use cases for identity proofing of natural person*) s'appliquent à la vérification de l'identité d'une personne physique demandant la délivrance d'un certificat réglementé pour elle-même, avec mention ou non de qualités spécifiques au sens de l'art. 7, al. 3, let. a,

[2] JO L 109 du 26.4.2016, pp. 40–42

SCSE. Le cas d'utilisation 9.4 (*use case for identity proofing of natural person representing legal person*) s'applique quant à lui à la vérification de l'identité tant d'une personne physique demandant la délivrance d'un certificat réglementé en vue de représenter une entité IDE que d'une personne physique demandant la délivrance d'un certificat réglementé pour une entité IDE qui n'est pas une personne physique. Le cas d'utilisation 9.3 (*use case for identity proofing of legal person*) n'est pas applicable en droit suisse, dans la mesure où la SCSE ne prévoit pas qu'une entité IDE puisse demander directement la délivrance d'un certificat réglementé sans se faire représenter par une personne physique habilitée (cf. art. 9, al. 1, let. b, SCSE).

Les exigences du chapitre 8 de la spécification de l'ETSI complètent les cas d'utilisation des chapitres 9.2 et 9.4 compte tenu du contexte légal préexistant et du processus d'identification, en présence de la personne ou à distance, qui est mis en œuvre. En particulier, les exigences relatives aux registres publics (*trusted registers as supplementary evidence*) s'appliquent au registre du commerce ou au registre IDE dans la mesure où elles complètent les dispositions des art. 5 et 6 OSCSE. Il en va de même des exigences relatives aux documents et attestations (*documents and attestations as supplementary evidence*) en ce qui concerne la confirmation de l'organisme compétent ou l'approbation de l'entité IDE (art. 9, al. 2 et 3, SCSE) lorsque les qualités spécifiques ou les pouvoirs de représentation ne sont pas mentionnés dans l'extrait du registre du commerce, ou encore en ce qui concerne la procuration écrite prévue à l'art. 6, al. 1, OSCSE.

Les exigences des chapitres 5, 6, 7 et 9.1 sont quant à elles applicables dans tous les cas. A noter que la vérification à distance de l'identité d'une personne physique par des moyens d'identification électronique (eID; *use case* 9.2.4), si elle constitue bien une méthode d'identification à distance couverte par l'art. 7, al. 1, OSCSE, ne peut pas être autorisée, contrairement à ce qui avait été prévu dans la consultation des milieux concernés, dans la mesure où l'eID n'est pas mentionné à l'art. 5, al. 1, OSCSE en tant que document de nature à prouver l'identité des personnes qui demandent un certificat réglementé (cf. art. 9, al. 4, SCSE). Quant à l'utilisation d'une signature électronique (*use case* 9.2.5), elle n'est possible que dans les cas visés et aux conditions prévues à l'art. 7, al. 3, OSCSE.

Une évaluation de la conformité d'une méthode d'identification selon la spécification ETSI TS 119 461 par un organisme d'évaluation de la conformité étranger est possible. La reconnaissance en Suisse de telles évaluations étrangères est possible compte tenu des accords dans le domaine de l'accréditation (*Multilateral Agreement - MLA*). L'organisme d'évaluation de la conformité étranger devrait être accrédité par l'organisme d'accréditation de son pays pour pouvoir effectuer des évaluations selon la spécification ETSI TS 119 461.

Dans le cadre des processus de reconnaissance et de surveillance, l'organisme de reconnaissance selon la SCSE (KPMG) se basera sur le rapport d'évaluation de la conformité étranger. Il vérifiera en outre que les conditions et restrictions spécifiques définies au ch. 2.3.1, let. a) soient bien respectées.

Dans le cadres des réévaluations ou des audits de surveillance, l'organisme de reconnaissance se basera également sur le rapport d'évaluation de la conformité, si la validité du rapport n'est pas échue.

Ch. 2.3.1, let. b)

Les cartes d'identité étrangères admises pour prouver l'identité des personnes qui demandent un certificat ainsi que les moyens permettant de vérifier la validité des documents d'identité présentés aux CSP suscitent régulièrement des questions. Des précisions quant aux sources officielles à consulter lors de la vérification de tels documents sont ajoutées au chapitre 2.3.1.

Ch. 2.3.1, let. c)

Selon le ch. 6.3.10 de la nouvelle version de la norme ETSI EN 319 411-2 référencée et de la norme ETSI EN 319 411-1 qui la précise, le CSP est libre de fournir le service OCSP ou de publier des listes de certificats révoqués (CRL). La fourniture du service OCSP est toutefois exigée pour les certificats TLS/SSL. La référence au ch. 6.3.10 de la norme ETSI EN 319 411-2 ne constitue pas une modification des PTA. Ce développement est tout de même mentionné dans ces explications puisqu'il est susceptible d'offrir davantage de flexibilité aux fournisseurs de services.

Ch. 2.3.2, let. d)

La nouvelle version de la norme EN 319 412-5 prévoit dorénavant des déclarations (*statements*) pour des certificats émis selon les réglementations des pays tiers. Les CSP devront insérer ces déclarations (*statements*) dans les certificats réglementés dans les 3 mois qui suivent l'entrée en vigueur, afin d'indiquer qu'il s'agit de certificats conformes aux règles suisses. Jusqu'à l'échéance de ce délai, l'exigence correspondante prévue aux ch. 2.3.2, let. d) de la 1ère édition des prescriptions techniques et administratives du 23 novembre 2016 reste applicable (cf. ch. 3).

Ch. 2.3.2, let. e) et f)

Des précisions sont ajoutées concernant la manière de mentionner les noms et prénoms dans les certificats réglementés car les normes référencées ne sont pas assez détaillées à ce propos.

Ch. 2.3.2, let. g)

Puisque le ch. 5.1.4 de la norme ETSI EN 319 412-1 mentionne deux possibilités différentes pour faire figurer les numéros d'identification des personnes morales, une précision est fournie concernant la manière d'indiquer le numéro unique d'identification des entreprises qui doit figurer dans les certificats réglementés fournis aux entités IDE. Si nécessaire, les CSP devront adapter leur pratique dans les 3 mois qui suivent l'entrée en vigueur. Jusqu'à l'échéance de ce délai, l'alternative mentionnée au même chapitre de la norme référencée reste applicable (cf. ch. 3).

Ch. 2.3.2, let. h)

Le nom donné au bit numéro 1 de l'extension *keyUsage* est complété puisque les normes X.509 et IETF RFC 5280 utilisent des noms différents pour désigner ce bit.

Ch. 2.3.2, let. j)

Les références sont précisées.

Ch. 2.3.2, let. l)

La référence au chapitre correspondant du document RFC 5280 est corrigée.

Ch. 2.3.3, let. b)

Le nom donné au bit numéro 1 de l'extension *keyUsage* est complété puisque les normes X.509 et IETF RFC 5280 utilisent des noms différents pour désigner ce bit.

Ch. 2.3.3, let. c)

La norme ETSI EN 319 412-5 a été adaptée afin que la déclaration indiquant qu'il s'agit d'un certificat qualifié soit également applicable aux certificats qualifiés émis dans les pays qui ne sont pas membres de l'Union européenne. Ce développement est donc pris en compte. Les CSP devront insérer ces déclarations (*statements*) dans les certificats qualifiés qu'ils émettent dans les 3 mois qui suivent l'entrée en vigueur. Jusqu'à l'échéance de ce délai, l'exigence correspondante prévue aux ch. 2.3.3, let. c) de la 1ère édition des prescriptions techniques et administratives du 23 novembre 2016 reste applicable (cf. ch. 3).

Ch. 2.3.4

Le chapitre 2.3.4 de la première édition des PTA est déplacé au ch. 2.3.5.

De nouvelles exigences relatives à la fourniture de certificats réglementés aux autorités communales, cantonales ou fédérales sont introduites au ch. 2.3.4 des PTA à la demande du Secteur Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale (anciennement Unité de pilotage informatique de la Confédération UPIC).

Ces nouvelles exigences sont reprises du concept *Konzept geregeltes Behördenzertifikat / Zusammenarbeit mit dem eGov Signaturvalidator* La version actuelle de ce concept sera disponible sur la page web de l'OFCOM[3] Le ch. 5.2 de ce concept mentionne notamment les sources auxquelles les CSP peuvent se référer pour vérifier les informations qui doivent figurer dans un certificat réglementé délivré à une autorité.

Les CSP devront émettre les certificats réglementés d'autorités communales, cantonales ou fédérales selon ces nouvelles règles dans les 3 mois qui suivent l'entrée en vigueur (cf. ch. 3).

[3] https://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/communication-numerique/signature-electronique.html

Ch. 2.3.5, let. c)

Ce chapitre reprend le contenu du ch. 2.3.4 de la première édition de ses PTA.

Comme au ch. 2.3.2, let. g), une précision est fournie concernant la manière d'indiquer le numéro unique d'identification des entreprises. Si nécessaire, les fournisseurs de services de certification reconnus devront adapter leur pratique dans les 3 mois qui suivent l'entrée en vigueur. Jusqu'à l'échéance de ce délai, l'alternative mentionnée au même chapitre de la norme référencée reste applicable (cf. ch. 3).

Ch. 2.3.5, let. d)

La référence au ch. 6.5.1 de la norme ETSI EN 319 411-2 est ajoutée car des exigences relatives à la gestion des certificats réglementés du CSP y figurent.

Ch. 3

Comme indiqués dans les chapitres correspondants du présent document, des délais de mise en œuvre sont prévus afin que les CSP disposent de suffisamment de temps pour adapter leurs processus opérationnels.