eCH-0220 Préservation de la validité des signatures électroniques sur les documents

Nom	Préservation de la validité des signatures électroniques sur les documents
eCH- nombre	eCH-0220
Catégorie	Norme
Stade	Défini
Version	1.0
Statut	Annulé
Date de décision	2018-06-06
Date de publication	2018-11-23
Remplacé version	-
Condition préalable	ETSI TS 101 733 V2.2.1 ETSI TS 119 122-1 V1.01 ETSI TS 119 122-2 V1.01 ETSI EN 319 192-1 V1.1.1 ETSI EN 319 192-2 V1.1.1 SCSE (Loi fédérale sur les services de certification dans le domaine de la signature électronique)
Annexes	-
Langues	Allemand (original), français (traduction)
Auteurs	Groupe spécialisé Technologie Böhlen Jörg (UPIC) Büchler Georg (KOST) Bütler Christian (OFJ) Erz Peter (UPIC) Muster Daniel (it-rm IT-Riskmanagement GmbH) Niederberger Marcel (MWST) von Niederhäusern Michael (BIT) Schmid Josef (Sopra Steria AG) Waldegger Hans-Peter (Swisscom)
Éditeur / Distribution	Association eCH, Mainaustrasse 30, case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

La présente norme doit servir de guide pour la préservation de la validité des documents signés électroniquement en vue de permettre un contrôle fiable de la signature électronique des documents au cours de cette période. A long terme, cela signifie par exemple que la signature peut donc être vérifiée même au terme de la durée de validité du certificat correspondant et être reconnue de manière générale si le contrôle se révèle positif. La validité d'un certificat peut par exemple expirer au terme la durée prévue ou suite à une demande de révocation émanant du propriétaire du certificat.

Le présent document s'appuie sur la loi fédérale sur les services de certification dans le domaine de la signature électronique (SCSE) et propose un profil des normes ETSI suivantes qui ont servi de base:

- ETSI TS 101 733 V2.2.1
- ETSI TS 119 122-1 V1.0.1
- ETSI TS 119 122-2 V1.0.1
- ETSI EN 319 192-1 V1.1.1
- ETSI EN 319 192-2 V1.1.1

Les attributs choisis l'ont été en veillant à ce que le concept global de «conservation» des documents signés électroniquement repose, autant que faire se peut, sur des attributs d'institutions généralement reconnues et se distingue par la plus grande simplicité possible. Les informations généralement reconnues sont par exemple des renseignements réglementés par les dispositions fédérales tels que:

- les certificats régis par la SCSE
- les services d'horodatage fournis par des services de certification reconnus selon la SCSE.

Il est fait référence à la norme ETSI EN 319 102-1 V1.1.1 concernant le contrôle de documents signés électroniquement.

Sommaire

1 Introduction 6
1.1 Statut 6
1.2 Champ d'application 6
1.3 Situation initiale 7
1.4 But(s) et délimitation 7
1.4.1 Objectif 7
1.4.2 Délimitation 8
1.5 Contenu, structure du document 9
1.6 Références croisées 9
1.7 Terminologie de la recommandation 9
1.8 Concept 10
1.9 Remarque 10
2 Profil 11
2.1 Remarques liminaires 11
2.1.1 Certificats 11
2.1.1.1 Origine 11
2.1.1.2 Validité temporelle 11
2.1.2 Horodatage 11
2.1.2.1 Qualité de l'horodatage 11
2.1.2.2 Format de l'horodatage 11
2.1.3 Signature 12
2.1.3.1 Format 12
2.1.3.2 Type de signature 12
2.1.3.3 Informations à joindre au document concernant l'horodatage 12
2.2 ETSI TS 101 733 V2.2.1 13
2.2.1 Chapitre 4 13
2.2.1.1 Remarque liminaire 13
2.2.1.2 Chapitre 4.2 Signature Policies 14
2.2.1.3 Chapitre 4.4.3.3 EXtended Electronic Signature with Time Type 2 (CAdES-X Type 2) 14
2.2.2 Chapitre 5 Electronic Signature Attributes 14
2.2.2.1 Chapitre 5.7.3 ESS signing-certificate Attribute 14
2.2.2.2 Chapitre 5.7.3.2 ESS signing-certificate-v2 Attribute 14
2.2.2.3 Chapitre 5.7.3.3 signing-certificate Attribute 14
2.2.2.4 Chapitre 5.8.1 signature-policy-identifier 14
2.2.2.5 Chapitre 5.9.1 signing-time 14
2.2.2.6 Chapitre 5.9.2 countersignature 15

2.2.2.7 Chapitre 5.10.1 content-reference Attribute ... 15
2.2.2.8 Chapitre 5.11.1 commitment-type-indication Attribute ... 15
2.2.2.9 Chapitre 5.11.2 signer-location Attribute ... 15
2.2.2.10 Chapitre 5.11.3 signer-attributes Attribute ... 15
2.2.2.11 Chapitre 5.11.4 content-time-stamp Attribute ... 15
2.2.3 Chapitre 6 ... 16
2.2.3.1 Chapitre 6.1.1 signature-time-stamp Attribute ... 16
2.2.3.2 Chapitre 6.2.1 complete-certificate-references Attribute ... 16
2.2.3.3 Chapitre 6.2.2 complete-revocation-references Attribute ... 16
2.2.3.4 Chapitre 6.2.3 attribute-certificate-references Attribute ... 16
2.2.3.5 Chapitre 6.2.4 attribute-revocation-references Attribute ... 16
2.2.3.6 Chapitre 6.3.3 certificate-values Attribute ... 16
2.2.3.7 Chapitre 6.3.4 revocation-values Attribute ... 16
2.2.3.8 Chapitre 6.3.5 CAdES-C-time-stamp Attribute ... 16
2.2.3.9 Chapitre 6.3.6 time-stamped-certs-crls-references Attribute Definition ... 16
2.2.3.10 Chapitre 6.4.1 archive-time-stamp Attribute ... 16
2.2.3.11 Chapitre 6.4.2 ats-hash-index Attribute ... 16
2.2.3.12 Chapitre 6.4.3 archive-time-stamp-v3 Attribute ... 17
2.2.3.13 Chapitre 6.5.1 long-term-validation Attribute ... 17
2.3 ETSI TS 119 122-1 V1.0.1 ... 17
2.3.1.1 Chapitre 5.2.6.1 signer-attributes-v2 attribute ... 17
2.3.1.2 Chapitre 5.2.6.2 claimed-SAML-assertion ... 17
2.3.1.3 Chapitre 5.5.2 The ats-hash-index-v2 Attribute ... 17
2.4 ETSI TS 119 122-2 V1.0.1 ... 17
2.5 ETSI EN 319 122-1 V1.1.1 ... 18
2.5.1.1 Chapitre 5.5.2 The ats-hash-index-v3 Attribute ... 18
2.6 ETSI EN 319 122-2 V1.1.1 ... 18
2.7 ETSI TS 119 122-3 V1.1.1 ... 18
2.8 Complément ... 18
2.8.1 Calcul de la valeur de hachage pour l'horodatage de l'archive ... 18
2.8.2 Traitement des informations de contrôle ... 18
2.8.3 Informations concernant le statut du certificat de la signature du document ... 20
2.8.4 Contrôle de la signature ... 20
3 Synthèse ... 21
4 Autres répercussions concernant la préservation de la validité ... 22
4.1 CSP ... 22
4.2 Application de signature ... 22

5 Considérations de sécurité 22
6 Exclusion de responsabilité - droits de tiers 23
7 Droits d'auteur 23
Annexe A – Références & bibliographie 24
Annexe B – Collaboration & vérification 24
Annexe C – Abréviations & glossaire 25
Annexe D – Modifications par rapport à la version précédente 26
Annexe E – Liste des tableaux 26

Remarque

En vue d'une meilleure lisibilité et compréhension, seul le genre masculin est utilisé pour la désignation des personnes dans le présent document. Cette formulation s'applique également aux femmes dans leurs fonctions respectives.

1 Introduction

1.1 Statut

Annulé: Le document a été retiré de eCH. Il ne doit plus être utilisé.

1.2 Champ d'application

La préservation de la validité des documents signés électroniquement requiert une normalisation basée sur et prenant la forme d'un profil des normes suivantes de l'ETSI:

- ETSI TS 101 733 V2.2.1
- ETSI TS 119 122-1 V1.01
- ETSI TS 119 122-2 V1.01

Le champ d'application couvre tous les documents signés électroniquement devant encore être conservés pendant des jours, des semaines voire des années, afin de pouvoir en contrôler avec fiabilité la signature électronique, même une fois passé ce délai, et les accepter lorsque ce contrôle est réussi.

Remarque: ETSI TS 119 122-1 V1.01 et ETSI TS 119 122-2 V1.01 sont des mises à jour et compléments (engl. Updates) de la norme ETSI TS 101 733 V2.2.1, sans pour autant être explicites par elle-même.

Les normes suivantes, plus actuelles, ont été adoptées par l'ETSI concernant la préservation de la validité des documents signés électroniquement:

- ETSI EN 319 122-1 V1.1.1
- ETSI EN 319 122-2 V1.1.1
- ETSI TS 119 122-3 V1.1.1

Cependant, ce document **s'appuyait** tout d'abord sur la norme **ETSI TS 101 733 V2.2.1** dans sa version en vigueur, parce que:

- elle est explicite et contient des informations complémentaires permettant de mieux saisir la problématique.
- ETSI EN 319 122-1 V1.1.1 et ETSI EN 319 122-2 V1.1.1 sont plus difficiles pour s'initier à la problématique.

ETSI TS 119 122-3 V1.1.1, ETSI EN 319 122-2 V1.1.1 et ETSI TS 119 122-3 V1.1.1 sont prises en compte dans la suite de ce document.

1.3 Situation initiale

Concernant la préservation de la validité des documents signés électroniquement, il devrait être possible de contrôler avec fiabilité la signature servant de base, même après plusieurs années, et de continuer à l'accepter comme étant valide, dès lors qu'elle avait été considérée comme tel auparavant. Des événements susceptibles de compliquer l'acceptation ultérieure des signatures électroniques peuvent se produire entre le moment de l'exécution de la signature électronique et le nouveau contrôle - a posteriori - de la signature du document signé électroniquement et conservé:

- le certificat avec la clé publique pour la vérification de la signature électronique – le certificat de contrôle en abrégé – n'est plus valide.
- le Root Certificate (certificat racine) pour le certificat de contrôle n'est plus valide.
- la clé de signature privée a été compromise et le certificat a donc été révoqué.
- le certificat a été révoqué pour d'autres motifs.

BERTSCH s'emploie à exposer ce cas précis ainsi que d'autres cas et leurs répercussions sur le contrôle a posteriori de la signature électronique.

1.4 But(s) et délimitation

1.4.1 Objectif

Le présent document et les normes ETSI de base ont vocation à rendre les points suivants possibles.

Dans le cas d'un document signé électroniquement et d'un cachet régi par la SCSE, il doit être possible de déterminer, de façon fiable, si le certificat de signature correspondant était bien valide au moment où a été générée cette signature.

Des informations devraient être jointes en continu à un document aujourd'hui pourvu d'une signature électronique valide, réglée ou qualifiée afin que

- au cours de la période de conservation stipulée par les dispositions en vigueur ou dans le délai d'expiration liée à la responsabilité civile, il soit possible de constater de façon fiable que la signature comme le certificat correspondant étaient bien valides au moment où a été générée la signature électronique.
- au cours de la période et dans les délais mentionnés, la responsabilité pour l'exécution de cette signature électronique puisse être imputée de manière fiable à une personne morale ou physique.

Et ce sous réserve que les informations jointes, le document et la signature électronique correspondante demeurent inchangés dans l'intervalle, le but étant ici de veiller à ce que la signature électronique reste probante et pertinente. Ainsi la responsabilité prévue par l'article 59a CO ne devrait pas être frappée de caducité parce que le délai de validité du certificat correspondant est écoulé.

La norme EN 319 192-1 V1.1.1 définit les différentes étapes de contrôle destinées à vérifier une signature électronique. Tel que cela déjà été mentionné dans cette norme, les étapes de

contrôle devant être considérées comme valides afin que la signature soit acceptée dépendent des règles relatives à la signature (engl. signature policy).

In fine, la méthode proposée a pour but de préserver la validité des signatures électroniques afin qu'une fois une signature électronique établie ou reçue, son contrôle et donc la signature en elle-même puissent encore être acceptés de manière générale durant toute la période de conservation. Et ce, le cas échéant, même en cas de procédure administrative ou juridique dans le cadre d'un litige.

Par analogie, l'article 14 OGéo préconise que les géodonnées de base soient conservées de telle manière que le *volume* et la *qualité* en soient préservées. Les géodonnées de base sont alors sauvegardées en suivant des normes reconnues et selon l'état actuel de la technique. Il convient en particulier de changer périodiquement les données de lieu de stockage, de les conserver en toute sécurité sous des formats appropriés.

Le profil traité dans ces lignes repose sur des normes reconnues et est conforme à l'état de la technique, les normes les récentes adoptées par l'ETSI ont été prises en compte.

Remarque: dans la plupart des cas, les délais de conservation et de prescription mentionnés ici dépassent la validité du certificat pour la vérification de la signature de document ou de fichier, le cas échéant, la durée de validité d'un ou de plusieurs certificats dans la chaîne de certificats également (engl. certification path).

1.4.2 Délimitation

Il est important de préciser à ce stade qu'une signature électronique ne saurait protéger l'intégrité, à savoir l'inaltérabilité d'un document. Cela signifie que la signature ne constitue nullement une mesure de modification du document (elle n'a donc aucune valeur préventive visant à protéger de l'intégrité d'un document).

Elle peut repérer, de manière fiable, si le document a subi des modifications après la création de la signature correspondante et donc s'il a été porté ou non atteinte à cette intégrité (elle constitue à ce titre un moyen de détecter les atteintes portées à l'intégrité).

Il est par conséquent indispensable de protéger l'intégrité (inaltérabilité) des documents signés électroniquement. Le présent document n'a cependant vocation à proposer ni des mesures visant à protéger l'intégrité des documents signés lors de l'archivage/la conservation, ni des formats de données pour les documents à signer.

Les signatures électroniques abordées dans ces pages sont des signatures apposées sur des documents ou fichiers électroniques et des signatures devant permettre de contrôler, des années durant, les documents signés électroniquement et conservés, tels qu'un horodatage, des certificats, une liste de révocation des certificats (CRL) ou une réponse OCSP par exemple. Il s'agit là de signatures selon le format CMS.

La préservation de la validité des signatures électroniques sur un document PDF ou un fichier XML n'est pas traitée dans ces lignes. L'ETSI aborde la question de leur normalisation dans les normes suivantes:

- ETSI EN 319 142-1 V1.1.1
- ETSI EN 319 142-2 V1.1.1
- ETSI EN 319 132-1 V1.1.1
- ETSI EN 319 132-2 V1.1.1

1.5 Contenu, structure du document

Ce document est un profil de la norme ETSI ayant servi de base. Est mentionné dans ces lignes uniquement ce qui:

- n'est pas pertinent pour la **cyberadministration** ou l'est tout particulièrement
- ou devrait être amélioré.

Le chapitre 2 suivant répertorie les remarques correspondantes aux différents chapitres dans les normes ETSI, le titre des sous-chapitres se référant ici aux sous-chapitres des différentes normes ETS.

1.6 Références croisées

Les références croisées dans ce document commencent par «CHAPITRE», en MAJUSCULES donc. Les références croisées identifiées par «Chapitre» se rapportent à des chapitres de documents externes.

1.7 Terminologie de la recommandation

Les directives dans ce document sont indiquées conformément à la terminologie exposée dans [RFC2119], les expressions utilisées étant les suivantes, identifiées par des MAJUSCULES comme mots avec les significations ci-après (tiré de RFC 2119):

- **MUST**: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT**: This phrase, or the phrase "SHALL NOT", mean that that definition is an absolute prohibition of the specification.
- **SHOULD**: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY**: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

1.8 Concept

La thématique traitée dans ces lignes aborde également des signatures autres que la signature sur un document ou sur un fichier, notamment des signatures en cas d'horodatage, des réponses OCSP (online Certificate Status Protocol) (informations de statut sur les certificats), des certificats ou listes de révocation de certificat (engl. Certificate Revocation List, CRL en abrégé). Pour les distinguer, les premières citées sont désignées par le terme signature de document ou de fichier.

1.9 Remarque

Des compositions d'attribut autres que celles proposées dans les normes voire même d'autres procédures de préservation de la validité des documents signés électroniquement seraient possibles afin que leurs signatures puissent être contrôlées de manière fiable au cours de la période d'archivage/de conservation également.

Toutefois, le but est ici de calquer, autant que faire se peut, la proposition exposée dans ces lignes sur les normes ETSI ayant servi de base.

2 Profil

2.1 Remarques liminaires

2.1.1 Certificats

2.1.1.1 Origine

La préservation de la validité des documents signés (électroniquement) a pour principal objectif de préserver sur le long terme la force juridique et la pertinence d'une signature (électronique), de permettre notamment d'attester qu'une partie a bien signé le contenu du document.

SHOULD: la signature d'un document à archiver devrait être vérifiée au moyen d'un certificat défini selon la SCSE (art. 2 al. g et h SCSE). A défaut, la «conservation» fiable et généralement reconnue des documents signés électroniquement s'en trouverait nettement compliquée et sort (actuellement) du périmètre (engl. scope) de ce document.

2.1.1.2 Validité temporelle

MUST NOT: un certificat ne doit pas être valide plus longtemps ni plus tôt que le certificat CA supérieur le plus proche dans la chaîne de certificats. Le modèle de validité X.509.v3 pour la vérification du certificat est pertinent à cet égard, voir ITU-T X.509 chapitre 7.7 Certification path. Ce modèle de validité est appelé modèle de coque (voir également «Digitale Signaturen», Andreas Bertsch, 2012, Springerverlag.)

Il est interdit d'antidater un certificat réglé ou qualifié, ce qui signifie que le certificat aurait été valide avant même sa date de délivrance. Une telle façon de faire équivaut à produire un faux.

2.1.2 Horodatage

2.1.2.1 Qualité de l'horodatage

On utilise des horodatages pour la méthode proposée ici concernant la préservation de la validité des documents signés électroniquement.

MUST: les seuls horodatages utilisés doivent être qualifiés par la SCSE, délivrés par un CSP (fournisseur de services de certification) reconnu selon la SCSE (art. 2 al. j SCSE).

2.1.2.2 Format de l'horodatage

MUST: le format de l'horodatage doit remplir les exigences de la disposition des [PTA], chapitre 2.4 § b. D'après les [PTA], les horodatages produits doivent correspondre à la norme ETSI EN 319 422.

MUST: les horodatages doivent être signés au format CMS. Voir RFC 5652 concernant les CMS.

2.1.3 Signature

2.1.3.1 Format

A l'exception des certificats, les seules signatures électroniques traitées ici sont au format Cryptographic Message Syntax (CMS) (voir RFC 5652 concernant la CMS). Ce point concerne également les horodatages et les réponses OCSP.

2.1.3.2 Type de signature

SHOULD: différents types de signature – dont detached, embedded signatures – doivent être pris en charge, au même titre que les signatures supplémentaires sur le document ou sur le fichier comme une Counter Signature; voir également chapitre C.5 «Multiple Signatures» dans ETSI TS 101 733 V2.2.1.

Remarque: concernant les *detached signatures*, il est possible de traiter la signature séparée du document.

2.1.3.3 Informations à joindre au document concernant l'horodatage

La signature d'un horodatage est également vérifiée au moyen d'une chaîne de certificats. Ces certificats, et éventuellement leur statut également, doivent aussi être conservés à des fins de contrôle ultérieur de l'horodatage. Là encore comme les certificats pour le contrôle de la signature électronique de document ou de fichier. Le cas échéant, le document devrait/doit être archivé ou conservé au-delà de la durée de validité des certificats nécessaires au contrôle de la signature de l'horodatage.

SHOULD: les informations permettant de contrôler la signature de l'horodatage et de déterminer si le certificat correspondant était bien valide au moment de la création de l'horodatage, doivent être jointes à l'horodatage. Ces informations doivent être jointes à la signature de l'horodatage en tant qu'informations non signées de l'horodatage, notamment dans les attributs certificate-values et revocation-values, voir également le dernier chapitre ETSI TS 119 122-1 V1.0.1, chapitre A.1.1.2, ainsi que la page 26 au centre, 2ème point, ainsi que dans ETSI EN 319 122-1 V1.1.1, page 28.

Le tableau suivant répertorie les objets d'information traités dans ces pages et contenant des horodatages (colonne 1). La colonne 2, où peuvent être déposés ou «empaquetés» les certificats pour le contrôle de l'horodatage **encore** en tant qu'*attributs non signés pour la signature du document ou du fichier*, pouvant être nécessaires à la vérification. La colonne 3 dresse quant à elle la liste des informations entrant en ligne de compte dans la détermination de la valeur de hachage, qui est envoyée au service d'horodatage.

Objet avec horodatage	Info certificat (alternative)	Information pour la valeur de hachage
content-time-stamp	certificate-values, revocation-values pour la signature du document ou du fichier, complete-certificate-references, complete-revocation-references. Ceci uniquement si l'information n'a pas déjà été jointe en tant qu'attribut non signé à la signature d'horodatage.	Le document à signer. Concernant la valeur de «messageImprint» an l'horodatage voir ETSI EN 319 122-1 V1.1.1 chapitre 5.2.8 2 derniers points.
signature-time-stamp		SignatureValue
CAdES-C-time-stamp		SignatureValue, signature-time-stamp, complete-certificate-references, complete-revocation-references
time-stamped-certs-crls-references		complete-certificate-references, complete-revocation-references
Horodatage de l'archive		Toutes les informations préalablement

Tableau 1: Informations concernant les horodatages

Il ressort de ce tableau que seul l'horodatage de l'archive protège le document signé d'une baisse de la valeur de hachage correspondante utilisée pour signer le document. Ce n'est toutefois le cas que si une autre fonction de hachage est utilisée pour former la valeur de hachage à envoyer au service d'horodatage de l'archive que celle servant à constituer la signature. Les certificats d'attribut, au même titre que leurs informations de contrôle notamment, sont également enregistrés via l'horodatage de l'archive. Les valeurs de hachage pour la demande adressée aux services d'horodatage devraient être reconnues comme étant suffisamment sûres.

2.2 ETSI TS 101 733 V2.2.1

2.2.1 Chapitre 4

2.2.1.1 Remarque liminaire

Seul le format CAdES-A au chapitre 4.4.4.1, avec la modalité de type 1 du chapitre 4.4.3.2, sert les fins du présent document.

Le profil présenté ici ne tient compte d'aucun service time-mark. Pour en savoir plus sur le terme time-mark, se reporter au chapitre 3.1.

2.2.1.2 Chapitre 4.2 Signature Policies

SHOULD NOT: les Policies ne devraient pas être référencées dans la signature. Dans le cas contraire, il faudrait les archiver séparément.

Par ailleurs, les règles fédérales en vigueur à cet égard s'appliquent (SCSE, OSCSE, [PTA]).

2.2.1.3 Chapitre 4.4.3.3 EXtended Electronic Signature with Time Type 2 (CAdES-X Type 2)

MUST NOT: l'utilisation de ce format n'est pas autorisée, contrairement au format de type 1 du chapitre 4.4.3.2.

2.2.2 Chapitre 5 Electronic Signature Attributes

Remarque: les objets de signature ASN.1 définis au chapitre 5 sont des renseignements, qui sont majoritairement enregistrés par la signature électronique. ***Les renseignements suivants sont par conséquent pertinents pour l'application de la signature.***

2.2.2.1 Chapitre 5.7.3 ESS signing-certificate Attribute

SHOULD NOT: cet attribut ne devrait plus être utilisé. On lui préférera la version v2 parce qu'elle permet d'utiliser encore d'autres fonctions de hachage que SHA-1, voir également le chapitre 5.7.3.2.

2.2.2.2 Chapitre 5.7.3.2 ESS signing-certificate-v2 Attribute

SHOULD: cet attribut devrait être utilisé.

MUST: soit l'attribut signing-certificate ESS, soit le signing-certificate-v2 ESS doivent être utilisés en fonction de la norme.

2.2.2.3 Chapitre 5.7.3.3 signing-certificate Attribute

SHOULD NOT: cet attribut ne devrait plus être utilisé. Voir également le chapitre A.2.2 dans ETSI TS 119 122-1 V1.01.

2.2.2.4 Chapitre 5.8.1 signature-policy-identifier

SHOULD NOT: les Policies ne devraient pas être référencées dans la signature. Cet attribut ne devrait par conséquent pas être utilisé.

2.2.2.5 Chapitre 5.9.1 signing-time

SHOULD NOT: dans l'éventualité où il est pertinent, d'un point de vue légal, que la signature ait été établie plus tard qu'à un moment précis et que ceci devrait également être attesté de manière fiable, cet attribut ne devrait pas être utilisé. Il s'agit d'un attribut prétendu par le signataire, engl. claimed attribute.

SHOULD: l'attribut content-time-stamp au chapitre 5.11.4 devrait être utilisé à la place.

2.2.2.6 Chapitre 5.9.2 countersignature

MAY: cet attribut est utilisé afin de contresigner électroniquement un document déjà signé électroniquement.

2.2.2.7 Chapitre 5.10.1 content-reference Attribute

SHOULD NOT: aucune référence à d'autres documents ne devrait figurer dans la signature. Dans le cas contraire, il faudrait également archiver les documents référencés en conséquence et les joindre au document signé.

2.2.2.8 Chapitre 5.11.1 commitment-type-indication Attribute

SHOULD NOT: les explications et intentions remises avec la signature devraient être extraites du document à signer. C'est la raison pour laquelle cet attribut ne devrait pas être utilisé.

2.2.2.9 Chapitre 5.11.2 signer-location Attribute

SHOULD NOT: pour des raisons légales, les renseignements concernant l'endroit où se trouve le signataire lors de l'exécution d'une signature devraient être apparents dans le document signé électroniquement. De plus, les points de renseignements, qui sont soulevés par le signataire, peuvent être aisément contournés et ne sont donc pas fiables. C'est la raison pour laquelle cet attribut ne devrait pas être utilisé. Voir également le chapitre C.3.4 concernant ces attributs, appelés engl. claimed attributes.

2.2.2.10 Chapitre 5.11.3 signer-attributes Attribute

SHOULD: les signer-attributes-v2 devraient être utilisés à la place, voir chapitre 5.2.6.1 dans ETSI TS 119 122-1 V1.01.

En cas d'utilisation, il faut faire attention aux points suivants.

SHOULD NOT: les claimed attributes ne devraient pas être utilisés. Les points de renseignements, qui sont soulevés par le signataire, ne peuvent plus ensuite être attestés de manière fiable dans la plupart des cas et devraient par conséquent être évités.

MUST: les certified Attributes doivent être utilisés dans le cas où les renseignements dans l'attribut Certificat sont pertinents pour la signature.

2.2.2.11 Chapitre 5.11.4 content-time-stamp Attribute

MUST: cet attribut doit être utilisé dans l'éventualité où il est pertinent du point de vue légal que la signature ait été établie après un moment précis et que ceci puisse, le cas échéant, être également attesté de manière fiable.

SHOULD: *dans le cas où le service d'horodatage n'a pas fourni à l'horodatage les informations relatives au contrôle de la signature d'horodatage, celui-ci devrait encore être joint.*

Remarque: cette information est importante parce que le certificat relatif à l'horodatage peut avoir un Root Certificate différent pour les horodatages suivants.

2.2.3 Chapitre 6

2.2.3.1 Chapitre 6.1.1 signature-time-stamp Attribute

MUST: Cet attribut doit être joint.

2.2.3.2 Chapitre 6.2.1 complete-certificate-references Attribute

MUST: Cet attribut doit être joint.

2.2.3.3 Chapitre 6.2.2 complete-revocation-references Attribute

MUST: Cet attribut doit être joint.

2.2.3.4 Chapitre 6.2.3 attribute-certificate-references Attribute

MUST: Cet attribut doit être joint lorsque l'attribut Certificat revêt une importance juridique pour la signature.

2.2.3.5 Chapitre 6.2.4 attribute-revocation-references Attribute

MUST: Cet attribut doit être joint lorsque l'attribut Certificat revêt une importance juridique pour la signature.

2.2.3.6 Chapitre 6.3.3 certificate-values Attribute

MUST: Cet attribut doit être joint.

2.2.3.7 Chapitre 6.3.4 revocation-values Attribute

MUST: Cet attribut doit être joint.

2.2.3.8 Chapitre 6.3.5 CAdES-C-time-stamp Attribute

MUST: Cet attribut doit être joint.

2.2.3.9 Chapitre 6.3.6 time-stamped-certs-crls-references Attribute Definition

MUST NOT: cet attribut ne doit pas être utilisé parce qu'il crée simplement un horodatage via les références du certificat et les références aux listes de révocation. Il est donc préférable d'utiliser l'attribut CAdES-C-time-stamp.

2.2.3.10 Chapitre 6.4.1 archive-time-stamp Attribute

SHOULD NOT: cet attribut ne devrait plus être utilisé selon ETSI TS 119 122-1 Chapitre A.2.4.

2.2.3.11 Chapitre 6.4.2 ats-hash-index Attribute

SHOULD NOT: cet attribut ne devrait plus être utilisé selon ETSI TS 119 122-1 Chapitre A.2.6.

2.2.3.12 Chapitre 6.4.3 archive-time-stamp-v3 Attribute

SHOULD: cet attribut devrait être utilisé.

2.2.3.13 Chapitre 6.5.1 long-term-validation Attribute

SHOULD NOT: cet attribut ne devrait plus être utilisé selon ETSI TS 119 122-1 chapitre A.2.5, voir également ETSI EN 319 122 V1.1.1 chapitre A.2.5.

2.3 ETSI TS 119 122-1 V1.0.1

ETSI TS 101 733 référence encore l'ancienne norme RFC 3852 concernant les CMS. La nouvelle norme RFC 5652 devrait toutefois être utilisée en cas de doute, voir ETSI TS 119 122-1.

2.3.1.1 Chapitre 5.2.6.1 signer-attributes-v2 attribute

SHOULD NOT: les claimed attributes ne devraient pas être utilisés. Les renseignements, qui sont fournis par le signataire, ne peuvent plus ensuite être attestés de manière fiable dans la plupart des cas et devraient par conséquent être évités.

MUST: *les certified attributes doivent être utilisés dans le cas où les renseignements dans l'attribut certificat sont pertinents pour la signature.*

MUST NOT: les confirmations complémentaires signées par des tiers ne doivent pas être utilisées. D'une part, ces confirmations devraient être archivées, d'autre part, la structure de la signature n'est éventuellement pas conforme aux CMS (RFC 5652), une signature XML par exemple

2.3.1.2 Chapitre 5.2.6.2 claimed-SAML-assertion

MUST NOT: elle contient une confirmation SAML des attributs fournis par le signataire. Afin de conférer à cette confirmation une certaine force probante, il convient de la signer. SAML présente toutefois une structure XML et ainsi sa signature une signature XML. L'archivage et le contrôle à long terme des signatures XML se trouvent (encore) hors de l'objectif et du périmètre de ce document.

2.3.1.3 Chapitre 5.5.2 The ats-hash-index-v2 Attribute

SHOULD NOT: cet attribut ne devrait plus être utilisé pour la préservation de la validité des signatures électroniques.

SHOULD: l'attribut The ats-hash-index-v3 devrait être utilisé à la place, voir CHAPITRE 2.5.1.1.

2.4 ETSI TS 119 122-2 V1.0.1

Le tableau A.1. en page 13 et les remarques correspondantes en page 14 offrent une synthèse des attributs traités. Le plus souvent, la colonne intitulée «Presence in E-X-L level» n'est toutefois pertinente pour ce propos uniquement dans certaines conditions. A cela devrait impérativement s'ajouter encore les attributs relatifs à l'horodatage de l'archive.

2.5 ETSI EN 319 122-1 V1.1.1

2.5.1.1 Chapitre 5.5.2 The ats-hash-index-v3 Attribute

SHOULD: cet attribut devrait être utilisé à des fins de préservation à long terme de la validité.

Pour le reste, il n'y a eu aucun changement majeur par rapport à la norme ETSI TS 119 122-1 pour les thèmes traités dans ces lignes.

2.6 ETSI EN 319 122-2 V1.1.1

Il n'y a eu aucun changement majeur par rapport à la norme ETSI TS 119 122-2 pour les thèmes traités dans ces lignes.

2.7 ETSI TS 119 122-3 V1.1.1

Cette norme stipule notamment comment les objets référencés en externe peuvent être enregistrés par un horodatage. Dans ce profil, aucune référence externe au document ne devrait être traitée dans un souci de simplicité.

2.8 Complément

2.8.1 Calcul de la valeur de hachage pour l'horodatage de l'archive

SHOULD: pour l'horodatage de l'archive, l'attribut archive-time-stamp-v3 devrait être utilisé en combinaison avec l'attribut ats-hash-index-v3.

MUST: dans ce cas, la procédure décrite dans ETSI EN 319-122 V1.1.1 page 28 doit être utilisée pour calculer la valeur de hachage pour la demande au service d'horodatage.

Remarque: les documents externes de la figure 1 concernant le processus d'élaboration de hachage sont uniquement les documents «detached». Les autres documents externes ne devraient être ni référencés ni impliqués dans l'élaboration de hachage.

MUST: si l'attribut long-term-validation a cependant été déjà utilisé pour l'horodatage de l'archive, la valeur de hachage doit être calculée au niveau du service d'horodatage selon ETSI TS 101 733 V2.2.1, page 49. Il est nécessaire de calculer à nouveau cette valeur de hachage lors du contrôle de l'attribut.

2.8.2 Traitement des informations de contrôle

Les informations de contrôle sont des informations, qui sont utilisées afin de contrôler les signatures impliquées, comme les certificats, les listes de révocation, les réponses OCSP et l'horodatage après la création de la signature électronique (les informations sur l'horodatage, jointes au document et prises en compte par la signature électronique, comme pour l'attribut content-time-stamp, y font exception).

SHOULD: le système de conservation devrait joindre ces informations.

SHOULD NOT: cela ne devrait pas relever de la compétence de l'application de la signature.

(il peut y avoir des applications de signature qui joignent encore une réponse OCSP à la signature).

Une procédure sur la façon et l'endroit où ces informations doivent être jointes est à présent recommandée.

- Les références de certificat et CRL correspondantes devraient être mises à jour avant que la valeur de hachage ne soit générée pour la demande de l'horodatage dans l'attribut CAdES-C-time-stamp. Cela signifie que les attributs complete-certificate-references et complete-revocation-references devraient être complétées. Ensuite, la valeur de hachage doit être générée pour la demande d'horodatage, l'horodatage être pris en compte, l'attribut CAdES-C-time-stamp être préparé et joint à la signature du document ou du fichier en tant qu'attribut non signé.

  Remarque: les références des informations de contrôle pour l'horodatage content-time-stamp doivent être intégrées aux attributs complete-certificate-references et complete-revocation-references, dans l'éventualité où l'horodatage serait présent et où cette information n'aurait pas encore été jointe à la signature d'horodatage en tant qu'attribut non signé, voir à ce sujet également ETSI EN 319 122-1 V1.1.1 chapitre A.1.1.1, note 4, chapitre A.1.2.1, note 6.

  Important: il est interdit de modifier l'horodatage content-time-stamp lorsqu'il fait déjà partie de la signature du document, car il appartient à un attribut signé.

- Les attributs certificate-values, revocation-values doivent être complétés avec les informations de contrôle pour les signatures de document ou de fichier et être joints à la signature de document ou de fichier en tant qu'attributs non signés.

  Remarque: les informations de contrôle pour l'horodatage content-time-stamp doivent être intégrées aux attributs certificate-values, revocation-values, dans l'éventualité où l'horodatage serait présent et où cette information n'aurait pas encore été jointe à la signature d'horodatage en tant qu'attribut non signé, voir à ce sujet également ETSI EN 319 122-1 V1.1.1 chapitre A.1.1.2, note 2, chapitre A.1.2.2, note.

- Dans l'éventualité où les certificats d'attribut seraient pertinents pour la signature de document ou de fichier, les attributs signer-attributes-v2, attribute-certificate-references et attribute-revocation-references doivent être mis à jour et joints à la signature de document ou de fichier en tant qu'attribut non signé.

- Avant de joindre le premier horodatage de l'archive, les informations de contrôle pour la vérification de l'horodatage devraient être recueillies et jointes en tant qu'attribut non signé à la signature d'horodatage préalablement générée. Sont concernés l'horodatage signature-time-stamp, CAeDS-C-time-stamp. Cela signifie que les attributs certificate-values, revocation-values doivent être générés pour les signatures d'horodatage et être joints à la signature d'horodatage en tant qu'attribut non signé, voir également ETSI EN 319 122-1 V1.1.1 page 27 alinéa après la note 4.

  Par analogie, ceci devrait être également fait pour les signatures OCSP des réponses OCSP.

- Le premier horodatage de l'archive doit être créé.

- Concernant le deuxième horodatage de l'archive, les informations de contrôle de l'horodatage précédent de l'archive doivent être mises à jour et jointes à la signature d'horodatage précédente en tant qu'attribut non signé, voir également ETSI EN 319 122-1

V1.1.1, page 28 Remarque après le premier Bullet Point. Aucune information supplémentaire ne doit être jointe par crainte que le déroulement du contrôle de la signature se solde par un échec, le calcul des valeurs de hachage pertinentes pour le contrôle pouvant aboutir à un autre résultat.

MUST: au plus tard avant l'expiration du certificat pour la vérification de l'horodatage de l'archive, un autre horodatage d'archive doit être créé avec un nouveau certificat de contrôle correspondant.

2.8.3 Informations concernant le statut du certificat de la signature du document

SHOULD: Les réponses OCSP fournissent selon RFC 6960 le statut actuel d'un certificat et satisfont aux exigences exposées par l'article 9 § 2 de l'OSCSE. C'est la raison pour laquelle cette information devrait être privilégiée par rapport à la CRL pour la signature de document.

Lors de l'ajout d'une CRL, il faudrait veiller à utiliser la CRL le plus proche dans le temps. Le cas échéant, le certificat devrait être à nouveau contrôlé par la suite.

2.8.4 Contrôle de la signature

Faute de règles contraignantes, on ne sait pas très bien ce qu'il faut contrôler comme étant réussi ou valide pour qu'une signature électronique conservée soit acceptée en cas de procédure litigieuse. C'est en tout cas ce qui ressort de l'expérience pratique dans le domaine légal et administratif.

ETSI EN 319 102-1 V1.1.1 cite des procédures relatives à la manière de contrôler les signatures électroniques conservées. Celles figurant sous «Signatures with Long-Term Validation Material» et «Signatures with Long-Term Availability and Integrity of Validation Material» sont pertinentes pour notre propos, voir également annexe B.

Pour compléter à ce sujet:

a. ETSI EN 319 122 V1.1.1., chapitre 5.5.2 alinéa 3 doit également être pris en compte concernant le contrôle de l'horodatage de l'archive.

b. Un horodatage B représente le justificatif suivant voire la preuve de l'existence (engl. Proof of Existence, POE en abrégé): «Les informations A, dont la valeur de hachage a été envoyée au service d'horodatage et utilisée pour générer l'horodatage B au moment T, étaient présentes avant le moment T.»

   Lorsqu'aucune déclaration d'invalidité concernant les informations A ou certaines parties de ces informations n'a été publiée avant le moment donné T, on peut légitimement supposer que l'information A était valide dans son ensemble avant le moment T. Et ce, dans la mesure où l'horodatage B peut toujours être vérifié au moyen d'un certificat valide. Dans le cas contraire, il faut prendre des mesures, ce qui signifie joindre des horodatages supplémentaires afin de prolonger la durée d'acceptation de l'horodatage B.

3 Synthèse

Le tableau fournit une synthèse des attributs pertinents traités dans ces lignes.

No	Attribut	Signé	Recom.	Rem.
1.	ESS signing-certificate Attribute	J	SN	
2.	ESS signing-certificate-v2	J	S	
3.	message-digest attribute	N	M	NE
4.	Other signing-certificate Attribute	J	SN	
5.	signature-policy-identifier	J	SN	
6.	mime-type	J	MAY	
7.	signing-time	J	SN	C
8.	countersignature	J	MAY	
9.	content-reference Attribute	J	SN	NE
10.	content-hints Attribute	J	MAY	
11.	commitment-type-indication Attribute	J	SN	
12.	signer-location Attribute	J	SN	C
13.	signer-attributes Attribute	J	SN	CLA
14.	content-time-stamp	J	M, B	
15.	signature-time-stamp Attribute	N	M	
16.	complete-certificate-references Attribute	N	M	
17.	complete-revocation-references Attribute	N	M	
18.	attribute-certificate-references Attribute	N	M, B	
19.	attribute-revocation-references Attribute	N	M, B	
20.	certificate-values Attribute	N	M	
21.	revocation-values Attribute	N	M	
22.	CAdES-C-time-stamp Attribute	N	M	
23.	time-stamped-certs-crls-references Attribute	N	MN	
24.	archive-time-stamp Attribute	N	SN	
25.	ats-hash-index Attribute	N	SN	
26.	archive-time-stamp-v3 Attribute	N	S	
27.	long-term-validation Attribute	N	SN	
28.	signer-attributes-v2 attribute	J	S	CLA
29.	claimed-SAML-assertion	N	SN	CLA
30.	ats-hash-index-v2 attribute	N	SN	

31.	ats-hash-index-v3 attribute	N	S	

Tableau 2: Synthèse des recommandations des attributs traités dans ce document

Légende

B = présent dans certaines conditions

Rem. = remarque

C = contient un claimed attribute du signataire. Ce renseignement fourni par le signataire ne peut être vérifié d'emblée par un tiers.

CLA = peut contenir un «claimed attribute» du signataire, qui ne devrait pas être inséré.

J = OUI

M = MUST

MN = Must NOT

N = non

NE = Mentionné dans la norme, mais non traité dans ce document, faute d'autres avis.

S = SHOULD

Signé = composant de la signature de document ou de fichier à archiver, cela signifie que le contenu de l'attribut est pris en compte dans le calcul de hachage pour la signature.

SN = SHOULD NOT

4 Autres répercussions concernant la préservation de la validité

4.1 CSP

Les CSP doivent tenir compte du fait que les signatures dans l'horodatage et dans la réponse OCSP sont créées au format CMS.

Il faut en outre respecter les restrictions relatives à la durée de validité d'un certificat, voir CHAPITRE 2.1.1.2.

Remarques: concernant le concept exposé dans ce document, le CSP n'est pas tenu de respecter de délais de conservation particuliers, hormis le fait qu'il doit contribuer par des informations à la vérification de la validité des certificats qu'il a lui-même émis.

4.2 Application de signature

Tous les attributs évoqués ici, qui doivent être signés avec le document, sont partie intégrante du processus de signature. Les caractéristiques correspondantes doivent par conséquent être intégrées à l'application de signature.

5 Considérations de sécurité

Ce document traite de la préservation de la validité des documents signés électroniquement afin de permettre de déterminer bien plus tard si le certificat était valide pour le contrôle des

signatures au moment de l'exécution de la signature électronique. Ce thème relève en soi du domaine de la sécurité informatique. D'autres thèmes de sécurité informatiques sont délibérément exclus de ces pages en gardant à l'esprit que bien que pertinents, ils risquent de déborder du propos.

6 Exclusion de responsabilité - droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association **eCH** mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des réglementations applicables.

7 Droits d'auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s'engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu'à l'association **eCH**, pour une utilisation et un développement sans restriction dans le cadre des buts de l'association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes **eCH** sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s'appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & bibliographie

BERTSCH	Andreas Bertsch, Digitale Signaturen, Springer Verlag, 2001, ISBN 978 3540 423515
ETSI EN 319 102 V1.1.1.	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures
ETSI EN 319 122-1 V1.1.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
ETSI EN 319 122-2 V1.1.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures
ETSI EN 319 422 V1.1.1	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
ETSI TS 101 733 V2.2.1	Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
ETSI TS 119 122-1 V1.0.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
ETSI TS 119 122-2 V 1.0.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures
ETSI TS 119 122-3 V1.1.1	Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES
ITU-T X.509	Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, 10/2012
RFC 3161	Time-Stamp Protocol
RFC 5652	Cryptographic Message Syntax Format
RFC 6960	Online Certificate Status Protocol – OCSP

Remarque: les normes indiquées ici reposent quant à elles sur une série d'autres ETSI, ITU ou de normes RFC. Elles y sont cependant répertoriées.

Annexe B – Collaboration & vérification

Outre les collaborateurs, dont le nom figure sur la page de garde de ce document sous la rubrique Auteurs, les personnes suivantes ont contribué à la vérification:

Gabi Daniel	Chancellerie fédérale
Moretti Thomas	QuoVadis
Müller Adrian	Cyber Identity

Annexe C – Abréviations & glossaire

[PTA]	Prescriptions techniques et administratives sur les services de certification dans le domaine de la signature électronique et autres applications des certificats numériques du 23 novembre 2016, RS 943.032.1
§	Paragraphe
Archivage	Conservation sûre et durable de documents dans des archives, représentant un intérêt juridique, administratif, politique, économique, historique, culturel, social ou scientifique.
Conservation	Gestion organisée et systématique des informations d'affaire pour une période adéquate (définie) en tenant compte des exigences légales, opérationnelles ou historiques.
Al.	Lettre
CMS	Cryptographic Message Syntax, voir RFC 5652
CRL	Certificate Revocation List
CSP	Certification Service Provider
ETSI	European Telecommunications Standards Institute
Olico	Ordonnance sur la tenue et conservation des livres de comptes du 24 avril 2002 (version du 1 janvier 2013), SR 221.431
OGéo	Ordonnance sur la géoinformation du 21 mai 2008, 510.620
OCSP	Online Certificate Status Protocol
OR	Loi fédérale du 30 mars 1911 complétant le Code civil suisse (cinquième partie: droits des obligations). RS 220
POE	Proof of Existence
RFC	Request for Comments (IETF Standard)
SAML	Security Assertion Markup Language
RS	Recueil systématique du droit fédéral
TSP	Trusted Service Provider
OSCSE	Ordonnance sur les services de certification dans le domaine de la signature électronique et autres applications des certificats numériques du 23 novembre 2016, RS 943.032
XML	Extended Markup Language
SCSE	Loi fédérale sur les services de certification dans le domaine de la signature électronique et autres applications des certificats numériques, du 18 mars 2016 (version du 1 janvier 2017), RS 943.03
Ziff.	Chiffre

Annexe D – Modifications par rapport à la version précédente

Il s'agit de la première version.

Annexe E – Liste des tableaux

Tableau 1: Informations concernant les horodatages 13

Tableau 2: Synthèse des recommandations des attributs traités dans ce document 22