eCH-0220 – Préservation de la validité des signatures électroniques au format CMS

Nom	Préservation de la validité des signatures électroniques au format CMS
eCH-nombre	eCH-0220
Catégorie	Norme
Stade	Défini
Version	2.0.0
Statut	Approuvé
Date de décision	2021-03-02
Date de publication	2021-03-10
Remplace la version	1.0 – Minor Change
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 pas impliqué dans la version 2.0 Büchler Georg (CECO) Bütler Christian (BJ) pas impliqué dans la version 2.0 Müller Adrian (SwissSign AG) nouveau pour la version 2.0 Muster Daniel (it-rm IT-Riskmanagement GmbH) Niederberger Marcel (AFC) von Niederhäusern Michael (BIT) Schmid Josef Waldegger Hans-Peter (Swisscom AG)
Editeur / 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 fournit des instructions relatives à la préservation de la validité des documents signés de manière électronique au format CMS, de sorte que la signature électronique des documents à conserver puisse être vérifiée avec fiabilité au cours de cette période. A long terme signifie que la signature peut être vérifiée en conséquence, même au-delà du terme de la période de validité du certificat correspondant par exemple, et qu'elle peut être généralement acceptée dès lors que la vérification est réussie. La validité d'un certificat peut expirer après son terme ou après que le propriétaire du certificat a demandé sa révocation par exemple.

Il existe d'autres formats de signature tels que les signatures XML ou PDF. Le format de signature électronique examiné ici est basé sur la norme RFC 5652.

Cette norme tient compte de la Loi fédérale sur les services de certification dans le domaine de la signature électronique (SCSE) et constitue un profil des normes ETSI sous-jacentes suivantes:

- 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

Concernant les attributs sélectionnés dans ce cas de figure, une attention particulière a été portée à ce que le concept de «conservation» des documents assortis d'une signature électronique se fonde intégralement sur des attributs émanant d'institutions généralement reconnues, tout en restant aussi simple que possible. Les informations provenant d'institutions généralement reconnues peuvent être des renseignements couverts par des réglementations fédérales par exemple, tels que:

- des certificats couverts par la SCSE
- des services d'horodatage fournis par des services de certification agréés selon la SCSE.

Il est fait référence à la norme ETSI EN 319 102-1 V1.1.1 concernant la vérification des documents signés de manière électronique.

Sommaire

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

Approuvé: le document a été approuvé par le Comité des experts. Il a pouvoir normatif pour le domaine d'utilisation défini dans le domaine de validité donné.

1.2 Différence par rapport à la version 1.0

La différence principale porte sur le titre de la présente norme qui a été adapté afin de pouvoir la distinguer de la norme eCH-0230. Quelques ajustements ont également été effectués dans un souci d'assurer la compatibilité avec la norme eCH.

1.3 Champ d'application

La préservation de la validité des documents ou objets signés de manière électronique au format XML devrait d'abord être normalisée sous la forme d'un profil sur la base des normes ETSI suivantes:

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

Définition: Un profil spécifie l'application d'une norme en particulier ou d'un groupe de normes. (a profile specifies the use of a particular standard, or group of standards.)

Partout où des documents assortis d'une signature électroniques doivent être conservés pendant des jours, des semaines, voire des années, de sorte que même au-delà de cette période, leur signature électronique puisse être contrôlée avec fiabilité et acceptée une fois vérifiée avec succès.

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

Plus récentes, les normes suivantes ont été adoptées par l'ETSI concernant la préservation de la validité des documents signés de manière électronique:

- 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.
- Les normes ETSI EN 319 122-1 V1.1.1 et ETSI EN 319 122-2 V1.1.1 sont plus difficiles pour s'attaquer à la problématique.

Les normes 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 ensuite prises en compte dans le présent document.

1.4 Situation de départ

La préservation de la validité des documents signés de manière électronique implique que même des années plus tard, la signature en question puisse être vérifiée avec fiabilité et continue d'être reconnue comme valide dès lors qu'elle a été précédemment jugée comme telle. Entre l'apposition de la signature électronique et la nouvelle vérification ultérieure de la signature du document conservé et signé de manière électronique, les événements suivants, par exemple, peuvent se produire, compliquant de fait l'acceptation a posteriori des signatures électroniques:

- Le certificat avec la clé publique pour la vérification de la signature électronique, en bref le certificat de contrôle, n'est plus valide.
- Le certificat racine pour le certificat de contrôle n'est plus valide.
- La clé de signature privée a été compromise et le certificat a ensuite été révoqué.
- Le certificat a été révoqué pour d'autres motifs.

BERTSCH explique ces cas et d'autres, ainsi que leurs répercussions sur la vérification ultérieure de la signature électronique.

1.5 Objectif(s) et délimitation

1.5.1 Objectif

Le présent document ainsi que les normes ETSI sous-jacentes devrait rendre les points suivants possibles.

Si l'on prend le cas d'un document signé de manière électronique et réglementé selon la SCSE et d'un sceau réglementé selon la SCSE, il devrait être possible de déterminer avec fiabilité si le certificat de signature correspondant était valide au moment où la signature a été apposée. Voir également l'article 2, al. c et d, du SCSE.

Un document qui a été pourvu aujourd'hui d'une signature électronique valide, réglementée ou qualifiée devrait être joint en continu à des informations de telle sorte

- qu'au cours de la période de conservation prescrite par les dispositions correspondantes ou le délai de conservation prescrit par la législation, il peut être établi avec fiabilité que la signature ainsi que le certificat correspondant étaient bien valides au moment où la signature électronique a été créée.
- qu'au cours de la période et du délai spécifiés, la responsabilité relative à la fourniture de cette signature électronique peut être affectée avec fiabilité à une personne physique ou morale.

Et ce, sous réserve que les informations jointes, le document et la signature électronique n'aient pas subi la moindre modification dans l'intervalle. La valeur de preuve ou la pertinence de la signature électronique devrait ainsi être préservée. Par exemple, la responsabilité selon l'art. 59a du CO ne devrait pas devenir obsolète parce que la durée de validité du certificat correspondant a expiré et que, par conséquent, la valeur de preuve de la signature électronique concernée est remise en cause.

Les normes EN 319 192-1 V1.1.1 et ETSI TS 101 903 V1.4.2 définissent les différences étapes de la vérification d'une signature électronique. Comme le précise la présente norme, les étapes de vérification requises afin que la signature soit jugée valide et par conséquent acceptée dépendent des règles en matière de signature (signature policy en anglais).

Au final, la méthode proposée ici doit permettre d'aboutir à la préservation de la validité des signatures électroniques de sorte qu'après la création ou la réception d'une signature électronique valide, sa vérification et donc la signature puissent encore être généralement acceptées pendant la période de conservation. Cela peut également être le cas lors d'une procédure administrative ou judiciaire contestée.

Par analogie: selon l'article 14 de l'OGéo, les géodonnées de base doivent être conservés de manière à en maintenir *l'état* et la *qualité*. Les géodonnées de base sont sauvegardées conformément aux normes reconnues et selon l'état de la technique. En particulier, les données sont exportées par période dans des formats de données appropriés pour être conservées de manière sécurisée.

Le profil traité ici repose sur des normes reconnues et correspond à l'état de la technique car les normes adoptées les plus récentes de l'ETSI ont été prises en compte.

Remarque: Les délais de conservation et de prescription mentionnés dans ces pages dépassent, dans la plupart des cas, la durée de validité du certificat pour la vérification de la signature du document ou du fichier et, le cas échéant, aussi la durée de validité d'un ou de plusieurs certificats dans la chaîne de certificats (certification path en anglais).

1.5.2 Délimitation

Il est important de préciser à cet égard: une signature électronique n'est pas à même de protéger l'intégrité, c'est-à-dire l'inaltérabilité, d'un document. Cela signifie que la signature ne doit pas être considérée comme une mesure excluant la modification du document. (il ne s'agit donc pas d'une mesure préventive destinée à protéger l'intégrité d'un document).

Elle permet de repérer avec fiabilité si le document a été modifié après la création de la signature correspondante et donc s'il y a eu ou non violation de l'intégrité. (il s'agit donc d'un moyen de détecter si l'intégrité a été violée).

Il est par conséquent indispensable de protéger l'intégrité (inaltérabilité) des documents signés de manière électronique. Toutefois, le présent document n'a pas vocation à proposer des mesures visant à protéger l'intégrité des documents signés lors de l'archivage/la conservation, ni des formats de fichiers des 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 pages. Ces points font l'objet de normes ETSI distinctes:

- 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

1.6 Contenu, structure du document

Ce document constitue un profil de la norme ETSI sous-jacente. A ce stade, il est simplement fait mention de ce qui:

- n'est pas pertinent ou pas particulièrement pertinent pour la **cyberadministration**

- ou devrait être amélioré.

Le chapitre 2 suivant répertorie les remarques pertinentes pour les chapitres correspondants des normes ETSI, les intitulés des sous-chapitres renvoyant ici aux sous-chapitres des normes ETSI respectives.

1.7 Références croisées

Les références croisées à l'intérieur du présent document commencent par «CHAPITRE», c'est-à-dire en LETTRES MAJUSCULES. Les références croisées vers des «chapitres», c'est-à-dire en lettres minuscules, renvoient aux chapitres de documents externes.

1.8 Terminologie de la recommandation

Les directives dans le présent document sont indiquées selon la terminologie de [RFC2119]. Dans ce contexte, les expressions suivantes apparaissant en LETTRES MAJUSCULES en tant que mots, ont les significations suivantes (citation tirée 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.)

1.9 Autres signatures

Pour le thème traité ici, les signatures autres que la signature sur un document ou un fichier sont également abordées, à savoir les signatures pour les

- horodatages
- Réponses OCSP (online Certificate Status Protocol)(informations sur le statut des certificats)
- Certificats
- Liste des révocations de certificats (en anglais Certificate Revocation List, CRL en abrégé).

À des fins de différenciation, les signatures sur un document ou un fichier sont désignées de manière sobre en tant que signatures dont la validité doit être préservée. Il s'agit du thème du présent document

1.10 Remarque

Des compositions d'attributs autres que celles qui sont proposées dans les normes, voire d'autres procédures visant à préserver la validité des documents signés de manière électronique seraient envisageables, de sorte que leurs signatures puissent aussi être vérifiées avec fiabilité même durant la période d'archivage/de conservation.

Cette proposition repose sur les normes ETSI internationalement reconnues.

2 Concernant les composants

Ce chapitre recommande la manière dont les principaux composants pour la préservation de la validité des signatures électroniques doivent en principe être appliqués ou obtenus.

2.1 Certificats

2.1.1 Origine

La préservation de la validité des documents signés (de manière électronique) a pour objectif de garantir que la nature juridiquement contraignante et la pertinence d'une signature (électronique) perdurent à long terme. Et notamment de pouvoir attester que le contenu du document a bien été signé par une partie.

SHOULD: La signature d'un document à archiver doit être vérifiée au moyen d'un certificat défini selon la SCSE (art. 2, let. g et h, SCSE). Dans le cas contraire, la «conservation» fiable et généralement reconnue des documents signés de manière électronique serait nettement plus difficile et se trouve (pour le moment) hors du champ d'application de ce document.

2.1.2 Validité temporelle

MUST NOT: Un certificat ne doit pas être valide plus longtemps et plus tôt que le certificat CA de niveau supérieur suivant dans la chaîne de certificats. Le modèle de validité X.509.v3 pour la vérification du certificat est ici pertinent, voir ITU-T X.509 chapitre 7.7 Certification path. Ce modèle de validité est appelé modèle *shell* (voir également BERTSCH).

Il est défendu d'antidater un certificat réglementé ou qualifié, à savoir de faire en sorte que la validité du certificat précède sa date de délivrance. Cela pourrait s'apparenter à une constatation fausse.

2.2 Horodatage

2.2.1 Qualité de l'horodatage

La méthode proposée ici concernant la préservation de la validité des documents signés de manière électronique repose sur l'utilisation de l'horodatage.

MUST: Seuls les horodatages qualifiés selon la SCSE et émanant d'un CSP (prestataire de services de certification) reconnu selon la SCSE peuvent être utilisés (art. 2, let. j, SCSE).

2.2.2 Format d'horodatage

MUST: Le format des horodatages doit être conforme à la disposition dans les PTA, chapitre 2.4, al. b. Les PTA stipulent que les horodatages générés doivent être conformes à la norme ETSI EN 319

422.

MUST: Les horodatages doivent être signés au format CMS. Concernant CMS, voir RFC 5652.

2.3 Signature

2.3.1 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.

2.3.2 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 la norme ETSI TS 101 733 V2.2.1.

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

2.3.3 Informations à joindre au document concernant l'horodatage

La signature d'un horodatage est elle aussi vérifiée au moyen d'une chaîne de certificats. Ces certificats, y compris, le cas échéant, le renseignement de leur statut, sont également conservés à des fins de vérification ultérieure de l'horodatage. Au même titre que les certificats pour la vérification de la signature électronique du document ou du fichier. Le cas échéant, le document devrait/doit être archivé ou conservé plus longtemps que la période de validité des certificats qui sont requis pour la vérification de la signature d'horodatage.

MUST: L'horodatage doit être accompagné d'informations permettant de vérifier la signature d'horodatage et de déterminer si le certificat correspondant était bien valide au moment de la création de l'horodatage. Ces informations doivent être jointes à la signature de l'horodatage en tant qu'information non signée par l'horodatage, notamment, dans les attributs certificate-values et revocation-values, voir également le dernier paragraphe ETSI TS 119 122-1 V1.0.1, chapitre A.1.1.2, ainsi que la page 26 au centre, 2^{e} point, et dans ETSI EN 319 122-1 V1.1.1, page 28. Le tableau suivant répertorie les objets d'information traités ici, qui contiennent des horodatages (colonne 1). Dans la colonne 2, où peuvent **encore** être conservés ou contenus les certificats pour la vérification de l'horodatage dans les *attributs pour la signature de document ou de fichier,* nécessaires à la vérification. La colonne 3 regroupe les informations utilisées pour créer la valeur hash qui est envoyée au service d'horodatage.

Objet avec horodatage	Information sur les certificats (alternative)	Information pour la valeur hash
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» au niveau de 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 des archives		Toutes les informations chronologiquement antérieures

Tableau 1: Informations concernant les horodatages

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

2.4 Format des réponses OSCP

MUST: Le format de la réponse OCSP doit être conforme à la norme RFC 6960.

Les réponses OCSP sont contenues dans un sous-élément correspondant de l'élément Revocation-Values.

MUST/SHOULD: La réponse OCSP doit être accompagnée d'informations permettant de vérifier la signature et de déterminer si le certificat correspondant était bien valide au moment de la création de la réponse OCSP. Ces informations doivent être jointes à la signature de la réponse OCSP en tant qu'informations non signées par la réponse OCSP, entre autres dans les attributs certificate-values et revocation-values.

3 Profil des normes ETSI concernées

Ce chapitre définit pour les normes ETSI respectives ce qu'il faut utiliser et comment les appliquer.

3.1 ETSI TS 101 733 V2.2.1

3.1.1 Chapitre 4 Vue d'ensemble

3.1.1.1 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.

3.1.1.2 Chapitre 4.2 Signature Policies

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

De plus, les dispositions fédérales en vigueur (SCSE, OSCSE, PTA) priment à cet égard.

3.1.1.3 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 autorisé, contrairement au format de type 1 au chapitre 4.4.3.2.

3.1.2 Chapitre 5 Electronic Signature Attributes

Remarque: 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.***

3.1.2.1 Chapitre 5.7.3 ESS signing-certificate Attribute

SHOULD NOT: cet attribut ne devrait plus être utilisé. On lui préférera la version v2 qui permet d'utiliser des fonctions hash autres que SHA-1, voir également le chapitre 5.7.3.2.

3.1.2.2 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.

3.1.2.3 Chapitre 5.7.3.3 signing-certificate Attribute

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

3.1.2.4 Chapitre 5.8.1 signature-policy-identifier

SHOULD NOT: les Policies ne devraient pas être référencées dans la signature. En conséquence, cet attribut ne devrait plus être utilisé.

3.1.2.5 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 certain moment 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: Il convient plutôt d'utiliser l'attribut content-time-stamp décrit au chapitre 5.11.4.

3.1.2.6 Chapitre 5.9.2 countersignature

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

3.1.2.7 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.

3.1.2.8 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. Pour cette raison, cet attribut ne devrait plus être utilisé.

3.1.2.9 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. En outre, les renseignements, qui sont soulevés par le signataire, peuvent être contournés sans trop de difficultés, et sont à ce titre peu fiables. C'est la raison pour laquelle cet attribut ne devrait plus être utilisé. Voir également le chapitre C.3.4 concernant ces attributs appelés claimed attributes en anglais.

3.1.2.10 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 renseignements, qui sont soulevés par le signataire, ne peuvent généralement plus être attestés ultérieurement et devraient donc être évités.

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

3.1.2.11 Chapitre 5.11.4 content-time-stamp Attribute

MUST: dans l'éventualité où il est pertinent, d'un point de vue légal, que la signature ait été établie plus tard qu'à un certain moment et que ceci doit, le cas échéant, être également attesté de manière fiable, cet attribut doit être utilisé.

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 certificat racine différent pour les horodatages suivants.

3.1.3 Chapitre 6

Ce chapitre définit les renseignements à joindre à la signature en tant que telle, de sorte que la signature puisse toujours être vérifiée même après que le certificat correspondant a perdu sa validité.

3.1.3.1 Chapitre 6.1.1 signature-time-stamp Attribute

MUST: Cet attribut doit être joint.

3.1.3.2 Chapitre 6.2.1 complete-certificate-references Attribute

MUST: Cet attribut doit être joint.

3.1.3.3 Chapitre 6.2.2 complete-revocation-references Attribute

MUST: Cet attribut doit être joint.

3.1.3.4 Chapitre 6.2.3 attribute-certificate-references Attribute

MUST: Cet attribut doit être joint, lorsque le certificat d'attribut pour la signature est pertinent du point de vue légal.

Remarque: Peu employés en Suisse, les certificats d'attribut ne sont pas proposés par un organisme reconnu (CSP). La SCSE ne règle pas la question des certificats d'attribut.

3.1.3.5 Chapitre 6.2.4 attribute-revocation-references Attribute

MUST: Cet attribut doit être joint, lorsque le certificat d'attribut pour la signature est pertinent du point de vue légal.

Remarque: Peu employés en Suisse, les certificats d'attribut ne sont pas proposés par un organisme reconnu (CSP). La SCSE ne règle pas la question des certificats d'attribut.

3.1.3.6 Chapitre 6.3.3 certificate-values Attribute

MUST: Cet attribut doit être joint.

Remarque: Peu employés en Suisse, les certificats d'attribut ne sont pas proposés par un organisme reconnu (CSP). La SCSE ne règle pas la question des certificats d'attribut.

3.1.3.7 Chapitre 6.3.4 revocation-values Attribute

MUST: Cet attribut doit être joint.

Remarque: Peu employés en Suisse, les certificats d'attribut ne sont pas proposés par un organisme reconnu (CSP). La SCSE ne règle pas la question des certificats d'attribut.

3.1.3.8 Chapitre 6.3.5 CAdES-C-time-stamp Attribute

MUST: Cet attribut doit être joint.

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.

3.1.3.9 Chapitre 6.4.1 archive-time-stamp Attribute

SHOULD NOT: Cet attribut ne devrait plus être utilisé conformément à la norme ETSI TS 119 122-1 chapitre A.2.4.

3.1.3.10 Chapitre 6.4.2 ats-hash-index Attribute

SHOULD NOT: Cet attribut ne devrait plus être utilisé conformément à la norme ETSI TS 119 122-1 chapitre A.2.6.

3.1.3.11 Chapitre 6.4.3 archive-time-stamp-v3 Attribute

SHOULD: cet attribut devrait être utilisé.

3.1.3.12 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.

3.2 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.

3.2.1 Chapitre 5.2.6.1 signer-attributes-v2 attribute

SHOULD NOT: les claimed attributes ne devraient pas être utilisés. Les renseignements, qui sont soulevés par le signataire, ne peuvent généralement plus être attestés ultérieurement et doivent donc 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, il est possible que la structure de la signature ne soit pas conforme aux CMS (RFC 5652), une signature XML par exemple

3.2.2 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. Le document eCH-0230 propose la description d'un profil permettant de préserver la validité des signatures XML.

3.2.3 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 3.4.1.

3.3 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 que dans certaines conditions. A cela devrait impérativement s'ajouter encore les attributs relatifs à l'horodatage des archives.

3.4 ETSI EN 319 122-1 V1.1.1

3.4.1 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.

3.5 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.

3.6 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.

4 Complément

Elle est complétée, outre le formatage et les renseignements corrects, par ce qui est pertinent pour la préservation de la validité. Il s'agit du calcul de la valeur hash, du traitement des informations de vérification, des informations sur le statut du certificat et d'une remarque relative à la vérification de la signature.

4.1 Calcul de la valeur hash pour l'horodatage d'archive

SHOULD: pour l'horodatage des archives, 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 hash 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: dans l'éventualité où l'attribut long-term-validation a cependant été déjà utilisé pour l'horodatage des archives, la valeur hash 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 hash lors du contrôle de l'attribut.

4.2 Traitement des informations de vérification

Les informations de vérification sont des informations utilisées afin de vérifier les signatures concernées, telles que les certificats, les listes de révocation, les réponses OCSP et les horodatages 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)

MUST: Le système de conservation doit joindre toutes les informations nécessaires à la vérification de toutes les signatures.

L'application de signature n'est pas chargée de joindre toutes les informations de vérification. (certaines applications de signature tel Adobe Signature peuvent joindre une réponse OCSP à la signature

Une procédure est recommandée à ce stade afin de savoir comment et où joindre ces informations.

- Avant de créer la valeur hash pour la demande de l'horodatage dans l'attribut CAdES-C-time-stamp, les références correspondantes aux certificats et au CRL devraient d'abord être mises à jour. Cela signifie que les attributs complete-certificate-references et complete-revocation-references devraient être complétés. La valeur hash doit ensuite être créée pour la demande d'horodatage, l'horodatage être obtenu, l'attribut CAdES-C-time-stamp être créé et joint à la signature du document ou du fichier en tant qu'attribut non signé.

  Remarque: les références des informations de vérification 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 avec les informations de vérification pour les signatures de document ou de fichier doivent être complétés et joints à la signature du document ou du fichier en tant qu'attributs non signés.

  Remarque: les informations de vérification pour l'horodatage content-time-stamp doivent être intégrées aux attributs certificate-values et 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 le cas où les certificats d'attributs sont pertinents pour la signature du document ou du fichier, les attributs signer-attributes-v2, attribute-certificate-references et attribute-revocation-references doivent alors être mis à jour et joints à la signature du document ou du fichier en tant qu'attribut non signé.
- Avant de joindre le premier horodatage des archives, les informations de vérification des horodatages devraient être collectées et jointes à la signature d'horodatage préalablement créée en tant qu'attribut non signé pour l'horodatage lui-même. 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.

Cela devrait également être effectué en conséquence pour les signatures OCSP des réponses OCSP.

- Le premier horodatage des archives doit être créé.
- Concernant le deuxième horodatage des archives, les informations de vérification 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 Remarques après le premier Bullet Point. Aucune information supplémentaire ne doit être jointe par crainte que le déroulement de la vérification de la signature se solde par un échec, le calcul des valeurs hash 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 des archives, un autre horodatage des archives doit être créé avec le nouveau certificat de contrôle correspondant.

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

SHOULD: Les réponses OCSP fournissent le statut actuel d'un certificat selon le RFC 6960 et satisfont aux exigences de l'art. 9 al. 2 OSCSE. En conséquence, ces informations devraient être préférées aux CRL concernant la signature du document.

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

4.4 Vérification de la signature

Le SCSE et ses prescriptions d'exécution se contentent de régir le processus de délivrance des certificats, le CO le processus de création de la signature, mais pas sa vérification.

ETSI EN 319 102-1 V1.1.1 cite des procédures relatives à la manière de vérifier 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.

Un complément à ce sujet:

- ETSI EN 319 122-1 V1.1.1., chapitre 5.5.2 alinéa 3 doit également être pris en compte concernant la vérification de l'horodatage des archives .
- Un horodatage B représente la preuve suivante, voire une preuve d'existence (Proof of Existence en anglais, POE en abrégé: «Les informations A, dont la valeur hash a été envoyée au service d'horodatage et a été utilisée afin de produire l'horodatage B à l'instant T, étaient disponibles avant l'instant T».

Si aucune déclaration d'invalidité des informations A ou de parties de celles-ci n'a été publiée avant ledit instant T, on peut raisonnablement partir du principe selon lequel l'information A dans son ensemble était valide avant l'instant T. Et ce, sous réserve que l'horodatage B puisse toujours être vérifié avec un certificat valide. Dans le cas contraire, des précautions sont à prendre, ce qui signifie que des horodatages supplémentaires doivent être joints afin de prolonger la période d'acceptation de l'horodatage B.

5 Synthèse des recommandations

Le tableau suivant offre une synthèse des attributs pertinents traités ici.

No	Attribut	Signé	Rec.	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	

No	Attribut	Signé	Rec.	Rem
31.	ats-hash-index-v3 attribute	N	S	

Tableau 2: Synthèse des recommandations des attributs traités ici

Légende

C = disponible dans certaines conditions
Rem. = Remarque
C = contient un «claimed attribute» du signataire. Ces renseignements fournis par le signataire ne sont pas faciles à vérifier par un tiers.
CLA = Peut contenir «claimed attribute» du signataire, qui ne doit pas être inséré
O = OUI
M = MUST
MN = Must NOT
N = Non
NE = Evoqué dans la norme, mais pas traité ici car pas aucun avis contraire.
S = SHOULD
Signé = partie intégrante de la signature du document ou du fichier à archiver, ce qui signifie que le contenu de l'attribut est inclus dans le calcul hash pour la signature.
SN = SHOULD NOT

6 Autres aspects relatifs à la préservation de la validité

Ce chapitre présente d'autres composants exerçant une influence sur la validité des signatures électroniques. Il s'agit des CSP (Certificate Service Provider) et de l'application de signature.

6.1 CSP

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

En outre, les restrictions relatives à la période de validité d'un certificat doivent être respectées, voir CHAPITRE 2.1.2.

Remarques: Dans le cas du concept exposé dans ces pages, le CSP n'est pas tenu d'observer des délais de conservation, à ceci près qu'il doit fournir des informations servant à la vérification de la validité des certificats qu'il délivre.

6.2 Application de signature

Tous les attributs mentionnés ici, qui doivent être signés avec le document, font partie intégrante du processus de signature. En conséquence de quoi, les caractéristiques correspondantes doivent être intégrées dans l'application de signature.

7 Sécurité

Ce document traite de la préservation de la validité des documents signés de manière électronique, afin de pouvoir déterminer, à un moment ultérieur, si le certificat était valable pour la vérification de la signature au moment de l'apposition de la signature électronique. Il s'agit là d'un thème qui relève de

la sécurité informatique. D'autres thématiques en lien avec la sécurité informatique en sont délibérément exclus, car bien que pertinents, ils risqueraient de rendre les modalités ingérables.

8 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 règlementations applicables.

9 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
ETSI EN 319 102-1 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

Annexe – Collaboration & vérification

Moretti Thomas Damals QuoVadis

Müller Adrian Damals Cyber Identity, aktuell SwissSign AG

Annexe C – Abréviations et glossaire

Al.	Alinéa
Archivage	Conservation sûre et permanente de documents dans des archives ayant une valeur juridique, administrative, politique, économique, historique, culturelle, sociale ou scientifique.
Chiff.	Chiffre
CMS	Cryptographic Message Syntax, voir RFC 5652
CO	Loi fédérale complétant le Code civil suisse (livre cinquième: droit des obligations) du 30 mars 1911 RS 220

Conservation	Gestion organisée et systématique de l'information d'affaires pour une période de temps raisonnable (finie), en tenant compte des exigences juridiques, opérationnelles ou historiques.
CRL	Certificate Revocation List
CSP	Certification Service Provider
ETSI	European Telecommunications Standards Institute
Let.	Lettre
LIDE	Loi fédérale sur le numéro d'identification des entreprises du 18 juin 2010, RS 431.03
OCSP	Online Certificate Status Protocol
OGéo	Ordonnance sur la géoinformation du 21 mai 2008, 510.620
Olico	Ordonnance concernant la tenue et la conservation des livres de comptes du 24 avril 2002 (au 1er janvier 2013), RS 221.431
OSCSE	Ordonnance sur les services de certification dans le domaine de la signature électronique et autres applications de certificats numériques, du 23 novembre 2016, RS 943.032
POE	Proof of Existence
PTA	Prescriptions techniques et administratives sur les services de certification dans le domaine de la signature électronique et autres applications de certificats numériques, du 23 novembre 2016, RS 943.032.1
RFC	Request for Comments (norme IETF)
RS	Numéro du recueil systématique du droit
SAML	Security Assertion Markup Language
SCSE	Loi fédérale sur les services de certification dans le domaine de la signature électronique et autres applications de certificats numériques, du 18 mars 2016 (version en vigueur au 1er janvier 2017), RS 943.03
TSP	Trusted Service Provider
XML	Extended Markup Language

Annexe D – Modifications par rapport à la version précédente

Par rapport à la version 1.0, aucune recommandation n'a été jointe ni modifiée à la présente version. La seule précaution prise a consisté à s'assurer que cette version était bien compatible avec la norme eCH 0230. Sont notamment concernés l'intitulé de la norme, la numérotation des chapitres, des remarques: ou des explications.

Des précisions/améliorations ont en outre été apportées à la langue.

Request	Chapitre	Page	Adaptation
	Titre	1	Changement de titre
	2.2.	10	Complément
	4.2	17	Extension
	4.4	19	Extension

Annexe E– Liste des tableaux