eCH-0230 – Préservation de la validité des signatures électroniques au format XML

Nom	Préservation de la validité des signatures électroniques au format XML
eCH-nombre	eCH-0230
Catégorie	Norme
Stade	Défini
Version	1.0.0
Statut	Approuvé
Date de décision	2021-03-02
Date de publication	2021-03-10
Remplace la version	-
Condition préalable	ETSI TS 101 903 V1.4.2 ETSI EN 319 132-1 V1.1.1 ETSI EN 319 132-2 V1.1.1 SCSE (Loi fédérale sur les services de certification dans le domaine de la signature électronique) eCH-0091
Annexes	
Langues	Allemand (original), français (traduction)
Auteurs	Groupe spécialisé Technologie Büchler Georg (CECO) Müller Adrian (SwissSign AG) Muster Daniel (it-rm IT-Riskmanagement GmbH) Niederberger Marcel (AFC) von Niederhäuser Michael (BIT) Rötzer Hubert 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 XML, de sorte que la signature électronique des documents XML 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 à la signature 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 CMS ou PDF. Le format de signature électronique traité dans ces pages est basé sur la norme W3C «XML Signature and Processing» version 1.1 et sur la norme eCH-0091.

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 101 903 V1.4.2
- ETSI EN 319 132-1 V1.1.1
- ETSI EN 319 132-2 V1.1.1

Concernant les éléments XML sélectionnés dans ce cas de figure, une attention particulière a été portée à ce que le concept de «conservation» des objets XML et des documents XML assortis d'une signature électronique se fonde intégralement sur des éléments et des attributs émanant d'institutions généralement reconnues, tout en restant, dans la mesure du possible, 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.
- des normes ETSI sur le thème en question

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

Sommaire

1 Introduction 6
1.1 Statut 6
1.2 Champ d'application 6
1.3 Situation de départ 6
1.4 Objectif(s) et délimitation 7
1.4.1 Objectif 7
1.4.2 Délimitation 8
1.5 Contenu, structure du document 8
1.6 Références croisées 9
1.7 Terminologie de la recommandation 9
1.8 Terminologie 9
1.8.1 Signature 9
1.8.2 Elément XML et objet XML 9
1.9 Remarque 10
2 Concernant les composants 10
2.1 Certificats 10
2.1.1 Origine 10
2.1.2 Validité temporelle 10
2.1.3 Format certificats 10
2.2 Horodatage 10
2.2.1 Qualité de l'horodatage 10
2.2.2 Format d'horodatage 11
2.2.3 Informations de vérification concernant l'horodatage 11
2.3 Format des réponses OSCP 12
2.4 Format de signature XML 13
3 Profil 13
3.1 ETSI TS 101 903 V1.4.2 13
3.1.1 Format XAdES 13
3.1.2 Remarque liminaire 13

3.1.3 Eléments couverts par la signature 13
3.1.3.1 Chapitre 7.2.2 SigningCertificate 13
3.1.3.2 Chapitre 7.2.3 SignaturePolicyIdentifier 14
3.1.3.3 Informations non confirmées par un organisme reconnu 14
3.1.3.4 Chapitre 7.2.6 CommitmentTypeIndication 14
3.1.3.5 Chapitre 7.2.5 DataObjectFormat 14
3.1.3.6 Chapitre 7.2.9 AllDataObjectsTimeStamp 15
3.1.3.7 Chapitre 7.2.10 IndividualDataObjectsTimeStamp 15
3.1.4 Eléments non couverts par la signature 15
3.1.4.1 Chapitre 7.2.4 CounterSignature 15
3.1.4.2 Chapitre 7.3 SignatureTimeStamp 15
3.1.4.3 Chapitre 7.4.1 CompleteCertificateRefs 15
3.1.4.4 Chapitre 7.4.2 CompleteRevocationRefs 15
3.1.4.5 Chapitre 7.4.3 AttributeCertificateRefs 16
3.1.4.6 Chapitre 7.4.4 AttributeRevocationRefs 16
3.1.4.7 Chapitre 7.5.2 RefsOnlyTimeStamp 16
3.1.4.8 Chapitre 7.5.1 SigAndRefsTimeStamp 16
3.1.4.9 Chapitre 7.6.1 CertificateValues 16
3.1.4.10 Chapitre 7.6.2 RevocationValues 16
3.1.4.11 Chapitre 7.6.3 AttrAuthoritiesCertValues 17
3.1.4.12 Chapitre 7.6.4 AttributeRevocationValues 17
3.1.4.13 Chapitre 8.2 ArchiveTimeStamp 17
3.1.4.14 Chapitre 8.1 TimeStampValidationData 17
3.2 ETSI EN 319 132-1 V1.1.1 17
3.2.1 Remarque liminaire 17
3.2.2 Eléments couverts par la signature 18
3.2.2.1 Chapitre 5.2.2 SigningCertificateV2 18
3.2.2.2 Chapitre 5.2.5 SignatureProductionPlaceV2 18
3.2.2.3 Chapitre 5.2.6 SignerRoleV2 18
3.2.3 Eléments non couverts par la signature 18
3.2.3.1 Chapitre 5.5.3 RenewedDigests 18

3.2.3.2 Chapitre 5.2.10 SignaturePolicyStore 19
3.3 ETSI EN 319 132-2 V1.1.1 19
4 Complément 19
4.1 Calcul de la valeur hash pour l'horodatage des archives 19
4.2 Traitement des informations de vérification 19
4.3 Informations concernant le statut de certificat de la signature du document 21
4.4 Vérification de la signature 21
5 Synthèse des recommandations 21
6 Autres aspects relatifs à la préservation de la validité 23
6.1 CSP 23
6.2 Application de signature 23
7 Sécurité 23
8 Exclusion de responsabilité - droits de tiers 24
9 Droits d'auteur 24
Annexe A – Références & bibliographie 25
Annexe B – Collaboration & vérification 26
Annexe C – Abréviations et glossaire 26
Annexe D – Modifications par rapport à la version précédente 28
Annexe E – Liste des tableaux 28

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

Proposition: le document doit être présenté au comité d'experts à 02.03.2021 en vue de son approbation, mais n'est pas encore valable d'un point de vue normatif.

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 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 de la norme ETSI suivante:

- ETSI TS 101 903 V1.4.2

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 XML et des objets XML 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.

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

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

C'est pourtant la norme ETSI TS 101 903 V1.4.2, dans sa dernière version, qui a servi de point de départ au présent document:

- elle est explicite et contient des informations complémentaires pour bien comprendre le problème.
- Les normes ETSI EN 319 132-1 et V1.1.1 et ETSI EN 319 132-2 V1.1. sont plus difficiles pour s'attaquer à la problématique.

Les normes ETSI EN 319 132-1 et V1.1.1 et ETSI EN 319 132-2 V1.1.1 sont ensuite prises en compte dans le présent document.

1.3 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 (au moment de la création) 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 alors été révoqué.
- Le certificat a été révoqué pour d'autres motifs.

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

1.4 Objectif(s) et délimitation

1.4.1 Objectif

Le présent document ainsi que les normes ETSI sous-jacentes rendent 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, de la SCSE.

Un document qui a été pourvu aujourd'hui d'une signature électronique valide, réglementée ou qualifiée est 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 ETSI TS 119 102-1 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).

1.4.2 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 dont il est ici question sont, d'une part, les signatures XML de documents XML ou d'objets XML. D'autre part, des informations supplémentaires telles qu'un horodatage, des certificats, une liste de révocation de certificats (CRL) ou une réponse OCSP sont nécessaires à des fins de contrôle. Ces renseignements sont toutefois signés au format CMS.

La préservation de la validité pour les signatures électroniques au format CMS ou les signatures électroniques sur un document PDF ne sont pas traitées 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 319 102-1 V1.1.1.
- ETSI EN 319 102-2 V1.1.1.

1.5 Contenu, structure du document

Ce document est 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.

1.6 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.

1.7 Terminologie de la recommandation

Les directives dans le présent document sont indiquées selon la terminologie de RFC 2119. Dans ce contexte, les expressions suivantes apparaissant en LETTRES MAJUSCULES en tant que mots, ont les significations suivantes (citation tirée du 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 Terminologie

1.8.1 Signature

Pour le thème traité ici, les signatures autres que la signature sur un document XML ou un objet XML 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 (Certificate Revocation List en anglais, CRL en abrégé).

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

1.8.2 Elément XML et objet XML

Un élément XML resp. un objet XML est ici désigné par le terme élément ou objet.

1.9 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 principal 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.

2.1.3 Format certificats

MUST: Les certificats réglementés resp. qualifiés doivent être conformes aux dispositions des PTA, chapitre 2.3.2 ou 2.3.3.

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 horodateurs 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 NOT: Les normes ETSI TS 101 903 V1.4.2 prévoient encore la possibilité d'ajouter des horodatages au format XML, voir chapitre 7.1.4.2. Par conséquent, leur utilisation n'est pas autorisée dans ce contexte, notamment parce qu'ils ne sont pas (légalement) reconnus.

2.2.3 Informations de vérification 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.

Exception faite des cas où cette information est intégrée à un élément XML prévu à cet effet.

Le tableau suivant énumère les éléments traités ici qui contiennent des horodatages (colonne 1) Dans la colonne 2, où peuvent **encore** être conservés les certificats pour la vérification de l'horodatage dans les *éléments pour la signature de document ou d'objet*. La colonne 3 regroupe les informations utilisées pour créer la valeur hash qui est envoyée au service d'horodatage.

Elément avec horodatage	**Information sur les certificats (alternative)**	**Eléments pour la valeur hash**
AllDataObjectsTimeStamp	CertificateValues, XAdESv141:TimeStampValidationData.	Toutes les références dans l'élément ds:SignedInfo selon W3C-Sig, hors référence à cet objet lui-même. Voir chapitre 7.2.9 dans ETSI TS 101 903 V1.4.2
IndividualDataObjectsTimeStamp	CertificateValues, XAdESv141:TimeStampValidationData.	Eléments au choix des références dans AllDataObjectsTimeStamp, voir chapitre 7.2.10 dans ETSI TS 101 903 V1.4.2
SignatureTimeStamp	CertificateValues XAdESv141:TimeStampValidationData	ds:SignatureValue Element, selon W3C-Sig voir chapitre 7.3 dans ETSI TS 101 903 V1.4.2

Elément avec horodatage	Information sur les certificats (alternative)	Eléments pour la valeur hash
RefsOnlyTimeStamp	CertificateValues, XAdESv141:TimeStampValidationData.	CompleteCertificateRefs, CompleteRevocationRefs, le cas échéant, AttributeCertificateRefs and AttributeRevocationRefs, voir chapitre 7.5.2 dans ETSI TS 101 903 V1.4.2
SigAndRefsTimeStamp	CertificateValues, XAdESv141:TimeStampValidationData.	ds:SignatureValue, SignatureTimeStamp, CompleteCertificateRefs, CompleteRevocationRefs, le cas échéant, AttributeCertificateRefs, AttributeRevocationRefs, voir chapitre 7.5.1 dans ETSI TS 101 903 V1.4.2
XAdESv1.3.2:ArchiveTimeStamp		Le format de cet horodatage a été défini dans une version antérieure (1.3.2). Il a toutefois été remplacé par xadesv141:ArchiveTimeStamp. Voir chapitre 7.7 dans ETSI TS 101 903 V1.4.2
xadesv141:ArchiveTimeStamp	XAdESv141:TimeStampValidationData	Tous les éléments préalablement créés, dont les objets référencés pour la signature XML. Voir chapitre 8.2.1 dans ETSI TS 101 903 V1.4.2

Tableau 1: Informations concernant les horodatages

ds: Il s'agit du préfixe d'espace de nom selon W3C-Sig pour la signature XML.
xadesv141: est un préfixe d'espace de nom selon ETSI TS 101 903 V1.4.2.

Le tableau révèle que seul l'horodatage des archives protège le document ou l'objet signé contre un affaiblissement des valeurs hash utilisées pour signer le document.

Remarque: Les horodatages suivants sont partie intégrante de la signature XML, dont la validité est à préserver.

- AllDataObjectsTimeStamp
- IndividualDataObjectsTimeStamp

Les informations de vérification de l'horodatage dans la colonne 2 ne sont toutefois pas couvertes par la signature.

2.3 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 RevocationValues.

MUST: La réponse OCSP doit être accompagnée d'informations permettant de vérifier la signature OCSP 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 CMS de la réponse OCSP en tant qu'information non signée par la réponse OCSP, entre autres dans les attributs certificate-values et revocation-values.

Exception faite des cas où cette information est intégrée à un élément XML prévu à cet effet.

2.4 Format de signature XML

MUST: Une signature XML doit correspondre à W3C-Sig. Se reporter à la norme ETSI TS 101 903 V1.4.2 et eCH-0091 pour savoir ce qui peut/doit ou ne devrait/doit pas faire partie de la signature.

3 Profil

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

3.1 ETSI TS 101 903 V1.4.2

3.1.1 Format XAdES

Ce profil pour préserver la validité des signatures électroniques a pour point de départ les informations de vérification/éléments qui sont représentés par les figures G5 et G6 du chapitre G.1.2 de la norme ETSI TS 101 903 V1.4.2. Les formats représentés dans les figures G1 à G4 ne contiennent pas encore suffisamment d'informations concernant les intentions poursuivies ici.

L'objectif est que toutes les informations entrant en ligne de compte pour la vérification d'une signature électronique soient aussi proches que possible.

3.1.2 Remarque liminaire

ETSI TS 101 903 V1.4.2 spécifie les noms et la signification d'autres éléments qui ne figurent certes pas dans sig W3C, mais n'en sont pas moins pertinents pour les présentes fins.

MUST: Ces éléments doivent être intégrés à la structure (schéma) définie par ETSI TS 101 903 V1.4.2.

On fait en outre la distinction entre les éléments,

- qui sont protégés/enregistrés par la signature à préserver.
- qui sont pertinents pour la préservation de la validité de la signature mais qui ne sont pas couverts par la signature.

Se reporter au chapitre 5, ETSI TS 101 903 V1.4.2 pour connaître l'espace de noms à utiliser.

3.1.3 Eléments couverts par la signature

3.1.3.1 Chapitre 7.2.2 SigningCertificate

Selon la norme, il est possible d'utiliser l'élément «SigningCertificate» si l'utilisateur a recours à différents certificats avec la même clé publique. Cet élément inclut des références au certificat qui devrait être utilisé pour vérifier la signature.

MUST NOT: Cet élément ne doit pas être utilisé.

Justification: Il ne faut pas créer de certificats différents avec la même clé publique.

3.1.3.2 Chapitre 7.2.3 SignaturePolicyIdentifier

L'élément «SignaturePolicyIdentifier» permet de faire référence aux règles devant être appliquées à cette fin.

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

Les dispositions fédérales en vigueur (SCSE, OSCSE, PTA) priment à cet égard.

3.1.3.3 Informations non confirmées par un organisme reconnu

Les éléments suivants contiennent des informations que le signataire a jointes mais qui n'ont pas été confirmées par un organisme reconnu.

- SigningTime: Heure à laquelle a été créée la signature (chapitre 7.2.1). Cette indication de temps est fournie par le signataire.
- SignatureProductionPlace: Lieu où a été créée la signature (chapitre 7.2.7).
- SignerRole: Rôle du signataire lors de la création de signature (chapitre 7.2.8).

MAY: Ces éléments peuvent être joints.

Les informations contenues dans les éléments peuvent également être consultées depuis l'horodatage, les certificats d'attribut, les certificats ou le document à signer.

Une indication de temps par le signataire ne saurait suffire à fournir une justification ou une démonstration reconnue de la nature contraignante de l'indication de temps. Dans le cas où le fait que la signature ait été créée après un certain moment est juridiquement pertinent, les informations contenues dans les éléments ci-dessus ne suffisent plus. En conséquence de quoi:

MUST: Un horodatage reconnu doit être joint:

3.1.3.4 Chapitre 7.2.6 CommitmentTypeIndication

L'élément «CommitmentTypeIndication» contient les informations que le signataire reconnaît par sa signature.

MAY: Cet élément peut être utilisé.

Ce que le signataire reconnaît, cependant, doit toujours être issu des informations XML qu'il signe ou du contexte.

3.1.3.5 Chapitre 7.2.5 DataObjectFormat

L'élément «DataObjectFormat» contient des renseignements concernant les fichiers ou les objets XML qui doivent être signés.

MAY:Cet élément peut être utilisé.

Lorsque l'élément est utilisé, les points suivants doivent être respectés.

SHOULD: Tout d'abord, les informations contenues dans le ds:Object doivent être consignées au moyen d'attributs. Ce n'est que lorsque cela n'est pas suffisant pour certaines applications que cet élément peut être utilisé.

3.1.3.6 Chapitre 7.2.9 AllDataObjectsTimeStamp

L'élément «AllDataObjectsTimeStamp» contient un horodatage reconnu pour tous les objets qui doivent encore être signés. Cela prouve que la signature a été créée après un certain moment.

MUST: Dans le cas où il faut prouver que la signature a été créée après un certain moment, cet élément doit alors être inclus dans la signature.

3.1.3.7 Chapitre 7.2.10 IndividualDataObjectsTimeStamp

L'élément «IndividualDataObjectsTimeStamp» contient un horodatage reconnu portant sur des parties des objets à signer. Cela prouve que la signature sur ces objets a été créée après un certain moment.

SHOULD NOT: Cet élément ne devrait pas être utilisé.

SHOULD: L'élément «AllDataObjectsTimeStamp» devrait être préféré à cet élément et inséré.

3.1.4 Eléments non couverts par la signature

3.1.4.1 Chapitre 7.2.4 CounterSignature

Comme l'indique la terminologie anglaise, l'élément «CounterSignature» contient une contre-signature du document signé.

Un attribut peut être inséré dans l'élément CounterSignature/ds:Signature/ds:SignedInfo/ds:Reference pour indiquer que l'on a ici à faire à une contre-signature.

SHOULD: L'attribut devrait être utilisé.

SHOULD: Les informations de vérification pour la contre-signature, tels les certificats, doivent être ajoutées dans CounterSignature/ds:Signature/ en tant qu'éléments non couverts par la contre-signature.

3.1.4.2 Chapitre 7.3 SignatureTimeStamp

L'élément «SignatureTimeStamp» contient un horodatage qui prouve que la signature a bien été créée après un certain moment. L'élément ds:SignatureValue est intégré dans l'horodatage.

MUST: Cet élément doit être intégré.

3.1.4.3 Chapitre 7.4.1 CompleteCertificateRefs

L'élément «CompleteCertificateRefs» contient toutes les références aux certificats nécessaires à la vérification de la signature à un certain moment.

MAY: Cet élément peut être inclus, mais ne doit pas être vide.

A la différence de la norme CAeDS ETSI EN 319 122-2, cette information n'est pas requise par la norme pour le format XAdES-T.

3.1.4.4 Chapitre 7.4.2 CompleteRevocationRefs

L'élément «CompleteRevocationRefs» contient toutes les références aux listes de révocation (CRL), nécessaires à la vérification de la signature à un certain moment.

MAY: Cet élément peut être inclus, mais ne doit pas être vide.

A la différence de la norme CAeDS ETSI EN 319 122-2, cette information n'est pas requise par la norme pour le format XAdES-T.

3.1.4.5 Chapitre 7.4.3 AttributeCertificateRefs

L'élément «AttributeCertificateRefs» contient toutes les références aux certificats d'attribut nécessaires à la vérification des attributs à un certain moment.

SHOULD NOT Cet élément ne devrait pas être inclus, mais ne doit pas être vide.

A la différence de la norme CAeDS ETSI EN 319 122-2, cette information n'est pas requise par la norme pour le format XAdES-T, dans le cas où des certificats d'attribut sont joints.

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.

3.1.4.6 Chapitre 7.4.4 AttributeRevocationRefs

L'élément «AttributeRevocationRefs» contient toutes les références aux listes de révocation des attributs nécessaires à la vérification des attributs à un certain moment.

MAY: Cet élément peut être inclus, mais ne doit pas être vide.

A la différence de la norme CAeDS ETSI EN 319 122-2, cette information n'est pas requise par la norme pour le format XAdES-T, dans le cas où des certificats d'attribut sont joints.

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.

3.1.4.7 Chapitre 7.5.2 RefsOnlyTimeStamp

Dans l'élément «RefsOnlyTimeStamp» se trouve un horodatage sur les éléments qui contiennent les informations référencées (CompleteCertificateRefs, CertificateRevocationRefs, AttributeCertificateRefs, AttributeRevocationRefs)

SHOULD NOT: L'horodatage prévu dans cet élément ne devrait pas être créé,

Les informations enregistrées par cet horodatage sont déjà couvertes par «SigAndRefsTimeStamp».

3.1.4.8 Chapitre 7.5.1 SigAndRefsTimeStamp

Dans l'élément «SigAndRefsTimeStamp» se trouve un horodatage sur:

- la signature elle-même (ds:SignatureValue)
- SignatureTimeStamp et
- les éléments qui contiennent les informations référencées pour la vérification des signatures Il s'agit de CompleteCertificateRefs, CertificateRevocationRefs et, si des certificats d'attribut y figurent, AttributeCertificateRefs, AttributeRevocationRefs)

MUST: L'horodatage prévu dans l'élément doit être créé et inséré.

3.1.4.9 Chapitre 7.6.1 CertificateValues

L'élément «CertificateValues» contient les certificats permettant de vérifier les signatures existantes.

MUST: Les certificats pour la vérification de signature doivent être insérés dans cet élément s'ils ne sont pas déjà conservés dans un endroit autre que celui prévu à cet effet.

3.1.4.10 Chapitre 7.6.2 RevocationValues

L'élément «RevocationValues» contient les listes de révocation pour la vérification des certificats.

MUST: Les listes de révocation pour la vérification des certificats doivent être insérés dans cet élément s'ils ne sont pas déjà conservés dans un endroit autre que celui prévu à cet effet.

3.1.4.11 Chapitre 7.6.3 AttrAuthoritiesCertValues

L'élément «AttrAuthoritiesCertValues» contient les certificats de vérification des attributs et les certificats d'attributs.

MUST: Ces certificats doivent être insérés dans l'élément «AttrAuthoritiesCertValues» dans le cas où des certificats d'attribut sont utilisés.

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.

3.1.4.12 Chapitre 7.6.4 AttributeRevocationValues

L'élément «AttributeRevocationValues» contient les listes de révocation pour la vérification des attributs et des certificats d'attributs.

MUST: Ces listes de révocation pour la vérification des certificats d'attribut doivent être insérées dans l'élément «AttributeRevocationValues» dans le cas où des certificats d'attribut sont utilisés.

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.

3.1.4.13 Chapitre 8.2 ArchiveTimeStamp

L'élément «ArchiveTimeStamp» contient un horodatage des archives.

MUST: Cet horodatage des archives doit être intégré; et ce au format selon ETSI EN 319 122-1 V1.1.1.

3.1.4.14 Chapitre 8.1 TimeStampValidationData

Dans l'élément «TimeStampValidationData», des informations de vérification peuvent être insérées à des fins de vérification d'un horodatage. Pour chaque horodatage, un élément séparé doit être créé et une référence correspondante à cet horodatage doit être incluse.

MUST:L'élément «TimeStampValidationData», avec une référence correspondante à l'élément d'horodatage des archives, doit contenir les certificats pour la vérification de l'horodatage des archives correspondant.

MUST: Dans le cas où des informations de vérification doivent être jointes à un horodatage qui n'est pas un horodatage d'archives, la règle est la suivante: Cet élément avec une référence correspondante à l'élément avec l'horodatage en question doit contenir les certificats pour la vérification de cet horodatage. Dans la mesure où les certificats correspondants ne sont pas déjà répertoriés dans un autre élément.

3.2 ETSI EN 319 132-1 V1.1.1

3.2.1 Remarque liminaire

Ici aussi, on fait la distinction entre les éléments couverts par la signature à préserver et les informations à joindre pour la préservation de la signature. Cette dernière information n'est pas une partie intégrante de cette signature.

Les éléments et objets couverts par la signature sont subordonnés à l'élément «SignedProperties».

Voir chapitre 4.2 concernant l'espace de noms à utiliser.

Ce sous-chapitre comporte uniquement des compléments et des remarques relatives à la norme ETSI TS 101 903 V1.4.2 précédemment abordée.

3.2.2 Eléments couverts par la signature

3.2.2.1 Chapitre 5.2.2 SigningCertificateV2

Selon la norme, il est possible d'utiliser l'élément «SigningCertificateV2» si l'utilisateur a recours à différents certificats avec la même clé publique. Cet élément inclut des références au certificat qui devrait être utilisé pour vérifier la signature.

MUST NOT: Cet élément ne doit pas être utilisé.

Justification: Il ne faut pas créer de certificats différents avec la même clé publique.

3.2.2.2 Chapitre 5.2.5 SignatureProductionPlaceV2

L'élément «SignatureProductionPlace» comme l'élément «SignatureProductionPlaceV2» peuvent être ajoutés au choix et ensemble.

MAY: L'élément peut être utilisé.

L'information qui y figure peut également être consultée dans le document à signer.

3.2.2.3 Chapitre 5.2.6 SignerRoleV2

L'élément «SignerRole» comme l'élément «SignerRoleV2» peuvent être ajoutés au choix et ensemble. Pour l'élément «SignerRoleV2», des confirmations (Assertions en anglais) peuvent être insérées en supplément.

MAY: L'élément peut être utilisé pour inclure une annonce SAML par exemple.

MUST: Dans le cas où une annonce SAML est pertinente pour l'évaluation de la signature, elle doit figurer de manière exhaustive, c'est-à-dire non référencée, dans l'élément SignerRoleV2. Il faut à cet égard tenir compte des points suivants:

SHOULD: Toutes les informations concernant le rôle devraient être contenues non référencées dans l'annonce SAML.

SHOULD: Les certificats pour la vérification de la signature SAML devraient être joints à la signature SAML en tant qu'élément non signé.

MUST NOT:Ces certificats ne doivent pas être joints, après la création d'une signature, à une signature qui y est contenue. Faute de quoi, la signature n'est pas valide.

3.2.3 Eléments non couverts par la signature

3.2.3.1 Chapitre 5.5.3 RenewedDigests

L'élément RenewedDigests contient les valeurs hash, recalculées avec une autre fonction hash, d'objets référencés dans l'élément ds:Manifest via l'élément ds:Reference. La signification de l'élément ds:Reference est décrite dans W3C-Sig.

Conformément à la norme eCH-0091, l'élément ds:Manifest ne doit pas être utilisé.

MUST NOT: L'intégration de cet élément est par conséquent proscrite.

3.2.3.2 Chapitre 5.2.10 SignaturePolicyStore

L'élément «SignaturePolicyStore» peut contenir soit une référence à la Policy sous-jacente, soit à la Policy elle-même.

SHOULD: Lorsqu'une Policy est judicieuse, la Policy intégrale dans un objet doit alors être contenue dans cet élément.

Dans le cas où une Policy est insérée, alors:

MUST: Toutes les informations nécessaires à la vérification de la signature de la Policy doivent être jointes à la signature de Policy. Cela doit être effectué avant la création du premier horodatage des archives.

3.3 ETSI EN 319 132-2 V1.1.1

La norme ETSI EN 319 132-2 V1.1.1 spécifie, sous la forme d'un tableau, les éléments qui peuvent être inclus et doivent être joints pour les formats de signature XAeDS correspondants. Dans le présent document, le concept retenu se contente de joindre juste la quantité d'informations nécessaires pour atteindre l'objectif défini au CHAPITRE 1.4 .

- La norme est la base pour prolonger le tableau du CHAPITRE 5 «Synthèse des recommandations».

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 des archives

La manière de calculer la valeur hash envoyée au service d'horodatage des archives est décrite au chapitre 8 de la norme ETSI TS 101 903 V1.4.2.

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. (en sont exclues les informations d'horodatage jointes au document et couvertes par la signature électronique, comme pour les horodatages dans les éléments «AllDataObjectsTimeStamp» et «IndividualDataObjectsTimeStamp».)

MUST: Le système de conservation doit joindre tous les certificats pour la vérification de la (des) signature(s) dans les éléments RevocationValues CertificateValues.

Cette règle peut ne pas s'appliquer lorsque les certificats sont déjà inclus ailleurs. Pour la contre-signature, la réponse OCSP ou l'horodatage par exemple. Il est possible d'insérer déjà les informations de vérification pour les signatures mentionnées dans cette signature.

L'application de signature n'est pas chargée de joindre toutes les informations de vérification. (cer-

taines 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.

- Dans le cas où l'horodatage est joint dans «RefsOnlyTimeStamp», les références correspondantes aux certificats, CRL doivent être préalablement mises à jour. Dans le cas où les références aux certificats d'attribut ainsi qu'à leur liste d'invalidité sont également incluses, celles-ci doivent elles aussi être mises à jour. Cela signifie qu'il faut compléter les éléments CompleteCertificateRefs, CompleteRevocationRefs, le cas échéant, AttributeCertificateRefs et AttributeRevocationRefs. Remarque: Cet horodatage ne devrait pas être utilisé.
- La valeur hash doit ensuite être créée pour la demande d'horodatage, l'horodatage être obtenu, l'élément RefsOnlyTimeStamp être créé et joint à la signature du document ou du fichier en tant qu'élément non signé.
- Avant de créer la valeur hash pour la demande de l'horodatage dans l'élément SigAndRefsTimeStamp, les références correspondantes aux certificats, CRL doivent d'abord être mises à jour. Dans le cas où les références aux certificats d'attribut ainsi qu'à leur liste d'invalidité sont également incluses, celles-ci doivent elles aussi être mises à jour. Cela signifie qu'il faut compléter les éléments CompleteCertificateRefs, CompleteRevocationRefs, le cas échéant, AttributeCertificateRefs et AttributeRevocationRefs. **Les références répertoriées ne doivent être mises à jour que si aucun horodatage «RefsOnlyTimeStamp» n'a été préalablement créé.**
- La valeur hash doit ensuite être créée pour la demande d'horodatage, l'horodatage être obtenu, l'élément SigAndRefsTimeStamp être créé et joint à la signature du document ou du fichier en tant qu'élément non signé.
- Les éléments CertificateValues, RevocationValues 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'éléments non signés.
- Dans le cas où les certificats d'attributs sont pertinents pour la signature du document ou du fichier, les éléments AttrAuthoritiesCertValues, AttributeRevocationValues doivent alors être mis à jour et joints à la signature du document ou de l'objet en tant qu'élément 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'élément non signé pour l'horodatage lui-même ou dans les éléments CertificateValues, RevocationValues.*
  Par conséquent, cela devrait également être effectué pour les signatures OCSP des réponses OCSP préalablement créées.
- Le premier horodatage des archives doit être créé.
- Concernant le deuxième horodatage des archives, les informations*, qui sont nécessaires à la vérification de l'horodatage des archives précédent*, doivent être mises à jour en premier lieu. Il faut ensuite, à partir de celui-ci, joindre un élément XAdESv141:TimeStampValidationData supplémentaire. Une référence à l'horodatage des archives précédent doit être intégrée à cet élément.

MUST: Avant l'expiration du certificat pour la vérification de l'horodatage des archives le plus récent, un autre horodatage des archives doit être créé et le certificat de contrôle correspondant doit être

joint.

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 faut veiller à ce que la CRL qui suit chronologiquement soit utilisée, c'est-à-dire la CRL créée après l'horodatage de la signature «SignatureTimeStamp». Ensuite, la validité du certificat doit, le cas échéant, être à nouveau vérifiée.

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 TS 101 903, chapitre G.2, répertorie les façons dont les éléments correspondants doivent être vérifiés. La norme ETSI TS 119 102-1 expose les processus de vérification

Un complément à ce sujet: 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	Elément	Signé	Rec.	Rem
1.	SigningCertificate	O	MN	
2.	SigningCertificateV2	O	MN	
3.	SigningTime	O	MAY	C
4.	SignatureProductionPlace	O	MAY	C
5.	SignatureProductionPlaceV2	O	MAY	C
6.	SignerRole	O	MAY	C
7.	SignerRoleV2	O	MAY	C
8.	CommitmentTypeIndication	O	MAY	C

9.	DataObjectFormat	O	MAY	C
10.	SignaturePolicyIdentifier	O	SN	
11.	AllDataObjectsTimeStamp	O	B	
12.	IndividualDataObjectsTimeStamp	O	SN	
13.	SignatureTimeStamp	N	M	
14.	CompleteCertificateRefs	N	B	
15.	CompleteRevocationRefs	N	B	
16.	AttributeRevocationRefs	N	B	
17.	AttributeRevocationRefs	N	B	
18.	CounterSignature	N	B	
19.	SigAndRefsTimeStamp	N	M	
20.	RefsOnlyTimeStamp element	N	SN	
21.	CertificateValues	N	M	
22.	RevocationValues	N	M	
23.	RenewedDigests	N	MN	
24.	AttrAuthoritiesCertValues	N	B	
25.	AttributeRevocationValues	N	B	
26.	SignaturePolicyStore	N	B	
27.	ArchiveTimeStamp	N	M	
28.	TimeStampValidationData	N	M	

Tableau 2: Synthèse des recommandations des éléments 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 ou ne sont pas reconnus.

O = OUI

M = MUST

MN = MUST NOT

N = Non

S = SHOULD

Signé = partie intégrante de la signature du document ou du fichier à archiver, ce qui signifie que le contenu de l'élément 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

Il est important de noter 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 éléments mentionnés ici, qui doivent être signés avec le document ou l'objet, font partie intégrante du processus de signature. En conséquence de quoi, les fonctions correspondantes doivent être intégrées dans l'application de signature.

7 Sécurité

Ce document traite de la préservation de la validité des objets XML et documents XML 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 relevant 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

Littérature spécialisée

BERTSCH	Andreas Bertsch, Digitale Signaturen, Springer Verlag, 2001

eCH (www.ech.ch)

eCH-0018	XML Best Practices
eCH-0036	Dokumentation für den XML-orientierten Datenaustausch
eCH-0091	eCH-0091: Standard zu XML-Signatur und Verschlüsselung

ETSI (www.etsi.org)

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 EN 319 132-1 V1.1.1	Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
ETSI EN 319 132-2 V1.1.1	Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Building blocks and XAdES baseline signatures
ETSI TS 119 102-1 V1.2.1	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation (2018-08)
ETSI TS 101 903 V1.4.2	Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)

ITU (www.itu.int)

ITU-T X.509	Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, 10/2012

Normes IETF (www.ietf.org)

RFC 3023	XML Media Types
RFC 3076	Canonical XML version 1.0
RFC 3161	Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)
RFC 3275	XML Signature Syntax and Processing
RFC 3741	Exclusive XML Canonicalization, version 1.0
RFC 3986	Uniform Resource Identifier (URI): Generic Syntax
RFC 4452	The «info» URI Scheme for Information Assets with Identifiers in Public Namespaces
RFC 5652	Cryptographic Message Syntax (CMS)

RFC 6960 Online Certificate Status Protocol – OCSP

W3C Standards (www.w3c.org)

Canonical XML Version 1.0 et 1.1 Recommendation mars 2001 et mai 2008

Exclusive XML Canonicalization Version 1.0 Recommendation, juillet 2002

XML Path Language (XPath) Version 1.0

XML Schema Part 1: Structures Second Edition. 28 octobre 2004. W3C Recommendation

XML Schema Part 2: Datatypes Second Edition. 28 octobre 2004. W3C Recommendation

XML Signature Best Practices Working Group Note, avril 2013

XML Signature Syntax and Processing Recommendation version 1.1, 11 avril 2013

OASIS Standards (www.oasis-open.org)

Security Assertion Markup Language (SAML) v2.0

Remarque: Les normes spécifiées ici sont quant à elles basées sur un ensemble d'autres normes ETSI, UIT, W3C ou RFC. Celles-ci y sont toutefois répertoriées.

Actes législatifs

LIDE: Loi fédérale sur le numéro d'identification des entreprises du 18 juin 2010, RS 431.03

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

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

SCSE: Loi fédérale du 18 mars 2016 Loi fédérale sur les services de certification dans le domaine de la signature électronique et autres applications de certificats numériques (RS 943.03)

Annexe B – Collaboration & vérification

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

Al.	Alinéa
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
ds:	Préfixe d'espace de nom selon W3C-Sig
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, voir RFC 6960
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 (état 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
W3C-Sig	XML Signature Syntax and Processing Recommendation version 1.1, 11 avril 2013
XAdES	XML Advanced Electronic Signature. Pour en savoir plus à ce sujet, voir ETSI TS 101 904 V.1.4.2
XAdES-T	XML advanced Electronic Signature with Timestamp. Pour en savoir plus à ce sujet, voir ETSI TS 101 904 V.1.4.2
XML	Extended Markup Language

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 12

Tableau 2: Synthèse des recommandations des éléments traités ici 22