eCH-0250 – La préservation de la validité des signatures dans un PDF

Nom	La préservation de la validité des signatures dans un PDF
eCH-nombre	eCH-0250
Catégorie	Norme
Degré de maturité	Défini
Version	1.0.0
Statut	Approuvé
Date de décision	2023-03-07
Date de publication	2023-02-13
Remplace la version	–
Conditions préalables	ETSI TS 102 778-1 à -6 ETSI EN 319 142-1 à -2 ISO 32000-1 et -2, Document Management — Portable document format Adobe ® XFA: XML Forms Architecture (XFA) Specification Version 2.5 eCH-0220 et CH-0230
Annexes	-
Langues	Allemand (original), français (traduction)
Auteurs	Groupe spécialisé Technologie (par ordre alphabétique) Georg Büchler (CECO) Daniel Muster (it-rm IT-Riskmanagement GmbH) Marcel Niederberger (AFC) Michael von Niederhäusern (BIT) Hubert Rötzer Erich Vogt
Éditeur / distribution	Association eCH, Mainaustrasse 30, case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

La présente norme fournit des instructions relatives à la préservation de la validité des signatures électroniques dans un document PDF, de sorte que la signature électronique dans les documents PDF à conserver puisse être vérifiée avec fiabilité au cours de cette période. À 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.

La présente 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 et recommandations sous-jacentes suivantes:

- ETSI EN 319 142-1
- ETSI EN 319 142-2
- ISO-32000-1 et ISO 32000-2
- CECO (https://kost-ceco.ch/cms/bienvenue.html)

Concernant les attributs, éléments et objets sélectionnés dans ce cas de figure, une attention particulière a été portée à ce que le concept de «conservation» des signatures électroniques dans un document PDF ou ses composants se fonde - si possible - intégralement sur des informations 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.

ou:

- Recommandations de l'Union européenne (https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/Standards+and+specifications) Les recommandations de l'UE sur le sujet traité ici font référence aux normes ETSI mentionnées ci-dessus.
- Recommandations du CECO

Il est en outre fait référence à la norme ETSI EN 319 102-1 concernant la vérification des documents signés de manière électronique. Aucun acte législatif fédéral ne vient toutefois régir ce point, qui n'est pas couvert par la présente norme.

Table des matières

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 Champ d'application

Le champ d'application est: partout où des signatures dans un document PDF ou ses composants doivent être conservées 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.

La préservation de la validité des documents signés électroniquement implique que même après des années, la signature en question 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 ensuite été révoqué.
- Le certificat a été révoqué pour d'autres motifs.
- Les algorithmes cryptographiques utilisés pour la signature peuvent être déclarés moins sûrs, ce qui peut conduire à la révocation des clés existantes et incitera probablement à augmenter la longueur des clés.

Ces cas et d'autres encore, ainsi que leurs répercussions sur la vérification ultérieure de la signature électronique sont expliqués dans [1] .

1.3 Objectif(s) et délimitation

1.3.1 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 créée. Voir également l'article 2, al. c et d, de la SCSE.

Un document où a été apposée aujourd'hui une signature électronique valide, réglementée ou qualifiée, est assorti d'informations en continu de telle sorte que

- il peut être établi de manière fiable, dans le délai de conservation stipulé dans les dispositions respectives, que le certificat correspondant était bien valide au moment de la création de la

signature électronique.
- 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.

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 période 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 102 778-2 à 5, ETSI EN 319 142-1 et -2 définissent les différences étapes de 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).

En résumé: La méthode proposée ici doit permettre d'aboutir à la préservation de la validité des signatures électroniques de sorte qu'après sa création, sa réception et sa vérification, la signature électronique puisse encore être généralement reconnue pendant la période de conservation. Cela peut également (le cas échéant) 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 conservées 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 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 et de l'ISO ont été prises en compte.

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

1.3.2 La voie vers l'objectif

La préservation de la validité des signatures dans un document PDF devrait d'abord être normalisée sous la forme d'un profil sur la base des normes ETSI suivantes:

- ETSI TS 102 778-1 à 6

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.)

Plus récentes, les normes suivantes ont été adoptées par l'ETSI et l'ISO concernant la préservation de la validité des documents PDF signés électroniquement:

- ETSI EN 319 142-1
- ETSI EN 319 134-2
- ISO 32000-2 (PDF 2.0)

Le point de départ de ce document est cependant la norme ETSI TS 102 778-1 à 6 et ISO 32000-2, parce que:

- elles sont explicites et contiennent des informations complémentaires permettant de mieux saisir la problématique.

- Les normes ETSI EN 319 142-1 et ETSI EN 319 142-2 pour lesquelles l'introduction à la problématique est plus difficile et certains thèmes/problèmes, comme le format PDF à utiliser, ne sont pas expliqués.

Les normes ETSI EN 319 142-1 et ETSI EN 319 142-2 sont ensuite prises en compte dans le présent document.. Les normes ETSI désignées «EN» dans le titre priment toutefois sur celles avec «TS».

Les normes ETSI EN 319 142-1 et ETSI EN 319 142-2 sont recommandées dans l'Union européenne pour la préservation de la validité des signatures électroniques dans un PDF: https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/Standards+and+specifications

1.3.3 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 ou d'un objet.» 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. Les mesures visant à protéger l'intégrité des documents PDF signés lors de leur archivage/conservation ne constituent toutefois pas le but premier de la présente norme.

1.4 Contenu, structure du document

Ce document constitue un profil de la norme ETSI et ISO sous-jacente. À 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 4 suivant répertorie les remarques pertinentes pour les chapitres correspondants dans les normes ETSI, les intitulés des sous-chapitres renvoyant ici aux sous-chapitres des normes ETSI respectives.

1.5 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.

1.6 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, ISO et les directives de l'UE internationalement reconnues et préserve la confidentialité du contenu.

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.)

2 Terminologie/recommandations concernant les signatures dans un PDF

Ce document explique et définit une certaine terminologie dans le contexte des signatures dans un PDF et établit des normes pour le format PDF.

2.1 Signatures dans un PDF

Un PDF peut être signé au moyen d'une signature CMS ou les objets XML qu'il contient le cas échéant, peuvent être signés avec une signature XML. Un profil pour la préservation de la validité des signatures au format CMS ou XML est donc créé ici.

L'ETSI normalise la préservation de la validité des signatures dans un PDF (PAdES) respectivement pour les signatures CMS et les signatures XML dans les normes suivantes.

- ETSI EN 319 142-1 pour les signatures CMS contenues dans le PDF
- ETSI EN 319 142-2, outre les signatures CMS, pour les signatures XML contenues dans le PDF

Tandis que l'ISO s'en charge pour la signature CMS dans ISO 32000-2.

Remarque: Les signatures normalisées par l'ETSI dans un PDF sont au format CMS ou au format XML. Les normes visant la préservation de la validité des signatures dans un PDF sont désignées par l'ETSI sous le nom de «PDF Advanced Electronic Signature», en abrégé «PAdES» dans le titre.

2.1.1 PDF avec signatures CMS

Une signature CMS peut contenir le document PDF ou être intégrée à un document PDF. Se référer à la norme eCH-0220 pour la première concernant la préservation de la validité. Seul ce dernier est pris en considération dans le présent document comme dans les normes ETSI mentionnées. Toute référence à avenir aux signatures CMS renvoie à une signature CMS intégrée dans un PDF, voir ETSI TS 102 778-1 chapitre 4.

À la différence des signatures CMS selon le RFC 5652, un PDF ne peut contenir deux signatures CMS ayant signé le même. La signature CMS suivante dans un PDF comprend le contenu à signer, y compris toutes les signatures précédentes, voir ETSI TS 102 778-1 chapitre 4.4. Une contre-signature (countersignature en anglais) au sens de la norme RFC 5652 n'est par conséquent pas envisageable.

Définition: Als PDF-Signatur wird eine CMS-Signatur in einem PDF bezeichnet, welche zu Kapitel 12.8 in ISO 32000-1 (PDF 1.7) oder in ISO 32000-2 (PDF 2.0) konform ist.

MUST NOT: l'utilisation de signatures PDF dont la version est antérieure à ISO 32000-1 (PDF 1.7) est interdite. Le certificat pour la vérification de la signature PDF pour PDF 1.6 notamment est déposé ailleurs dans le PDF qu'avec PDF 1.7 ou 2.0.

Concernant les formes de signatures PDF, voir CHAPITRE 2.4 «Types de signatures PDF».

2.1.2 PDF avec signatures XML

XML Forms Architecture (XFA) est un jeu de spécifications XML propriétaires. XFA peut être intégré dans les documents PDF à partir de PDF 1.5. Die Summe aller XML-Objekte in einem PDF wird als XFA-Form bezeichnet. Adobe a spécifié l'intégration de XFA dans un PDF dans Adobe ® XFA: XML Forms Architecture (XFA) Specification version 2.5, (June 2007). Aussi bien la forme XFA en tant que tout que les différents objets XML de la forme XFA peuvent être assortis d'une signature XML.

Remarque concernant l'utilisation mixte des signatures CMS et XML dans un document XFA tirée de la norme ETSI TS 102 778-1 à ce sujet:

> *Data encoded in XML may be carried within a PDF document. This may be used, for example, to carry PDF form data mapped into the PDF document using the XML Forms Architecture (XFA [i.2]). An XML signature, using the XAdES [3] format, may be applied to this data.*
>
> *The XML data, with or without an XML/XAdES signature, may be also signed along with the rest of the PDF document using a PDF signature as described above.* ***Once signed with a PDF signature further information cannot be added directly to any XAdES Signature***

> ***that may be present.*** *Where a XAdES signature is applied using XFA the related validation data may be provided using PDF data structures to support long term validation (see clause 5.8). However, if raw XML structures are used (i.e. not using XFA) once a XAdES signature has been placed within a document signed with a PDF Signature* ***it cannot be extended to support long term validation*** *(see clause 5.6).*

Concernant XAdES (XML Advanced Electronic Signature) voir eCH-0230.

2.1.3 Formes de signatures CMS dans un PDF

Voir à ce sujet le CHAPITRE 4.2 «ETSI TS 102 778-1».

2.1.4 Types des signatures XML dans un PDF

Voir à ce sujet le CHAPITRE 4.6 «ETSI TS 102 778-5».

2.2 Format PDF

Prendre des dispositions visant à la préservation de la validité d'une signature PDF des années durant n'est pas judicieux dès lors que le format PDF sous-jacent n'est pas compatible avec l'archivage. Le format PDF/A a été spécifié dans la norme ISO 19005 pour l'archivage d'un fichier PDF.

Les différentes versions de PDF/A font l'objet ci-dessous d'explications dans le contexte de la préservation de la validité des signatures PDF.

2.2.1 PDF/A-1

MUST NOT: L'utilisation du format PDF/A-1 (ISO 19005-1) basé sur PDF 1.4 n'est plus autorisé eu égard à l'archivage de documents signés électroniquement, lorsque la validité de la signature selon les procédures suggérées ici doit être préservée. Justification correspondante tirée d'ETSI TS 102 778-1 chapitre 46:

> «As PDF/A-1 is based on Adobe PDF 1.4 and not on ISO 32000-1, it does not fully support all of its features available to digital signatures - specifically lacking are embedded revocation information and time-stamping. However, since such features are not explicitly forbidden there is nothing that prevents a PDF/A-1 conforming writer from putting these extended features into a file - but there should be no expectation that a PDF/A-1 conforming reader will process them accordingly. A PDF/A-1 conforming reader is, however, free to implement functionality beyond that specified in PDF/A-1.»

2.2.2 PDF/A-2

SHOULD: Le format PDF/A-2 (ISO 19005-2) basé sur la norme ISO-32000-1 (PDF 1.7) doit être utilisé dans l'optique d'un archivage de documents signés électroniquement.

Justification de la recommandation d'un «SHOULD» plutôt qu'un «MUST»:

> Les normes ETSI renvoient à la norme ISO 32000-1 (PDF 1.7) concernant la constitution de la signature. La norme ISO 32000-1 (PDF 1.7) peut être utilisée de telle manière qu'elle soit compatible avec ISO 19005-2 (PDF/A-2). Toutefois, la norme ISO 32000-1 (PDF 1.7) ne regroupe/normalise pas l'intégralité des propriétés (Features en anglais) qui sont nécessaires à

l'application des normes ETSI TS 102 778-1 à -4 et ETSI EN 319 142-1 à -2. La préservation de la validité de la signature PDF nécessite une extension non conforme à la norme ISO 32000-1, voir ETSI EN 319 142-1 V1.1.1 (2016-04), chapitre 5.4.1.

Le CECO préconise pour l'archivage d'utiliser, si possible, le PDF/A-2 au niveau de conformité U (PDF/A-2u). Trois compléments à ce sujet:

- La formulation de PDF/A-2a étant plus stricte que celle de PDF/A-2u, le niveau de conformité a fonctionne est bien entendu lui aussi acceptable. Cependant, il est relativement difficile de générer un tel niveau de conformité.
- Par principe, tous les niveaux de conformité de la version 2 sont jugés compatibles avec l'archivage. Ce point est stipulé en conséquence dans le catalogue des formats de fichiers d'archivage (https://kost-ceco.ch/cms/pdf-a-2_fr.html).
- À l'heure de rédiger le présent document, la norme ISO 32000-1 (PDF 1.7) respectivement PDF/A-2 demeure le format le plus récent pris en charge dans la pratique.

2.2.3 PDF/A-3

MUST NOT: L'utilisation du format PDF/A-3 (ISO 19005-3) est interdite en vue d'un archivage du document, car il ne s'y prête pas, voir: «Management Summary zur KOST-Studie: PDF/A-2 et PDF/A-3: Was ist neu?» [6].

2.2.4 PDF/A-4

MAY:Le format PDF/A42 (ISO 19005-4) basé sur la norme ISO-32000-2 (PDF 2.0) pourrait être utilisé à l'avenir dans l'optique d'un archivage de documents signés électroniquement.

La norme ISO 32000-2 (PDF 2.0) a spécifié dans une norme les caractères (ETSI) nécessaires à la préservation de la validité des signatures PDF et peut être utilisée de manière à être compatible avec ISO 19005-4 (PDF/A-4). Dans le domaine PDF/A4, toutefois, certaines ambiguïtés subsistent en ce qui concerne l'archivage, comme le montrent à présent les explications suivantes.

PDF/A-4 (ISO 19005-4) a été publié en novembre 2020. Il n'existe que deux niveaux de conformité concernant PDF/A-4:

- PDF/A-4f autorise également les fichiers joints qui ne correspondent pas à PDF/A.
- PDF/A-4e pour le domaine Engineering permet l'intégration de contenus 3D

Le CECO n'a pas encore étudié la compatibilité de PDF/A-4 avec l'archivage. Il ressort toutefois d'une comparaison avec les versions précédentes ce qui suit:

- PDF/A-4f: Le niveau de conformité F (ou subsidiary profile F) est à éviter, par analogie avec les considérations relatives à PDF/A-3, voir https://kost-ceco.ch/cms/pdf-a-3_fr.html.
- PDF/A-4e: Concernant le niveau de conformité E, qui supplante PDF/E, le CECO n'est pas encore en mesure de se prononcer. Rien ne semble s'opposer à ce que PDF/A-4e soit compatible avec l'archivage.

Il s'agit donc à présent de définir dans quelle mesure la norme ISO 19005-4 (PDF/A-4e) convient à l'archivage conformément aux prescriptions fédérales suisses. Si la norme ISO 19005-4 (PDF/A-4) ne permet pas de satisfaire pleinement aux prescriptions fédérales, il est conseillé de stipuler dans un

profil comment les règles édictées par le CECO peuvent être satisfaites. Autrement dit, quelles parties de la norme ISO 19005-4 (PDF/A-4) satisfont aux exigences en matière d'archivage conformément aux prescriptions fédérales suisses.

La création d'un tel profil ne constitue toutefois pas le sujet de cette norme.

Si PDF/A-4 (ISO 19005-4) se révèle compatible avec l'archivage, on préférera ce format basé sur ISO-32000-2 (PDF 2.0) à PDF/A-2 (ISO 19005-2) basé sur ISO-32000-1 (PDF 1.7) pour la préservation de la validité des signatures PDF. Une fois établie la compatibilité de PDF/A-4 avec l'archivage, la norme sera adaptée en conséquence et en temps utile. À l'heure de rédiger la présente norme, toutefois, PDF/A-4 demeure une norme purement théorique qui n'est donc pas encore appliquée dans la pratique.

Remarque: L'Union européenne (UE) recommande ETSI EN 319 142-1 et -2, autrement dit une extension propriétaire à ISO 32000-1; voir au sujet de la conformité eIDAS https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/Standards+and+specifications

Elle s'abstient toutefois de se prononcer concernant la norme ISO 32000-2, mais sa recommandation est antérieure à 2020. La norme ISO 32000-2 n'a été publiée qu'en décembre 2020.

2.3 XFA

Définition: XFA (XML Forms Architecture) est un format de fichier/d'objet reposant sur la spécification suivante: XML Forms Architecture (XFA) Specification version 2.5, (June 2007), Adobe Systems Incorporated. XFA peut être intégré dans un PDF ou se présenter sous la forme d'un objet XML.

Dans le langage courant, PDF désigne notamment un fichier selon la norme ISO 32000-1 ainsi que XFA, qui est intégré dans un PDF.

Remarque: Adobe ne prend plus XFA en charge, qui est donc considéré comme obsolète pour la norme ISO 32000-2 (PDF 2.0). La norme portant sur la validité à long terme des signatures, des recommandations sont tout de même émises à ce sujet dans le chapitre 4.6 sans que celles-ci n'aient pour autant valeur normative.

2.4 Types de signatures PDF

Une distinction est établie entre les signatures PDF suivantes:

a) usage right signature
b) certification signature et
c) approval signature

Lorsque les signatures susmentionnées sont créées, elles doivent être apposées dans un PDF dans l'ordre indiqué ci-dessus, les deux premières signatures (usage rights, certification) ne devant pas figurer dans le PDF ou une fois seulement.

a) usage right signature: Une usage right (UR) signature permet de définir les fonctionnalités pouvant être utilisées dans un lecteur PDF.

MUST NOT: l'utilisation des usage rights (UR) signatures est interdite.

b) certification signature: Une certification signature, aussi appelée author signature, sert à définir les modifications pouvant être apportées au document une fois la certification signature apposée, sans pour autant que la signature en perde sa validité. Ainsi le PDF signé peut être assorti de commentaires par exemple, sans que la validité de la signature n'en soit affectée.

La définition des modifications possibles pouvant être apportées à un PDF après une signature PDF ne doit apparaître qu'une seule fois dans le PDF pour les deux versions ISO 32000-1 et 32000-2.

c) approval signature: Un PDF peut contenir autant d'approval signatures que souhaité. Il est également possible de définir les champs précis dans le PDF pouvant être modifiés ultérieurement sans que la signature perde sa validité.

SHOULD: Avant de réaliser une approval signature, il faut s'assurer de la validité des certificats pour la vérification des signatures PDF précédemment réalisées.

SHOULD NOT: Si tous ne sont pas valides, plus aucune signature PDF ne doit être jointe.

Remarque: Il est possible d'ajouter un horodatage de document, dont la compatibilité avec le PDF est établie de façon standard uniquement à partir de la norme ISO 32000-2, indépendamment de la manière dont ont été définies auparavant les restrictions dans le PDF au moyen de la certification signature ou de l'approval signature.

SHOULD NOT: Après un horodatage de document, il n'est plus nécessaire de joindre une approval signature. Des précautions doivent être prises en ce sens lors de la réalisation de l'horodatage de document.

2.5 Sécurité des PDF et des signatures PDF

2.5.1 Constatation

MUST: Si une signature PDF n'a pas pour simple vocation d'authentifier le document, mais également de constater un point précis, la signature doit alors couvrir le document dans son intégralité. Toute modification ultérieure apportée au document doit invalider la signature PDF du document. À ceci près qu'un horodatage de document ou une approval signature de plus peut être joint(e) à des fins de contre-signature du document déjà signé.

Il peut être possible par exemple de le configurer de telle manière que la certification signature n'apparaisse pas dans le document.

MUST: Dans le cas d'un titre, une personne physique doit pouvoir reconnaître toutes les signatures (PDF) à l'écran.

Remarque: Concernant la notion de titre, se reporter à l'art. 110 al. 4 et 5 CP et à l'art. 177 CPC. Pour obtenir des explications à ce sujet en lien avec le droit pénal, voir [5] Commentaire p. 1126, concernant le droit civil, voir [7], p. 318.

2.5.2 Risques liés au PDF

Un PDF peut servir à lancer des attaques, voir [3]. De la capacité du lecteur PDF à les reconnaître dépend le succès de ces dernières. Tous les lecteurs ne sont pas aptes à reconnaître et donc re-

pousser aussi efficacement de telles attaques. C'est en tout cas ce qui ressort du document susmentionné [3]. Les exigences auxquelles doit satisfaire le lecteur varient en fonction des exigences de sécurité et des mesures de défense en place. Les exigences minimales imposées à un lecteur dépassant le cadre de la présente norme, elles ne sont pas abordées ici.

Remarque: L'étude dans [3] a été réalisée sur la base du format PDF 1.7 (ISO-32000-1).

2.5.3 Risques dans la vérification des signatures PDF

Une signature PDF peut protéger l'authenticité et l'intégrité du document dans son ensemble ou en partie seulement. Il est toutefois nécessaire que les modifications de la partie protégée par la signature soient détectées lors de la vérification de la signature et signalées à l'utilisateur ou l'utilisatrice. Tous les lecteurs ne répondent cependant pas à ces exigences avec la même efficacité, voir [4].

Remarque: L'étude a été réalisée sur la base du format PDF 1.7 (ISO-32000-1).

MUST: Un lecteur de PDF doit pouvoir reconnaître les modifications de la partie protégée par la signature lors de la vérification de la signature et les signaler en conséquence à l'utilisateur/trice.

SHOULD: Il s'agit d'établir un profil de ce qui doit être contrôlé dans le PDF (signé) avant de commencer la vérification de la signature. Ce n'est toutefois pas le sujet de la présente norme.

2.5.4 Références externes

MUST: Toutes les informations nécessaires à la composition et à la présentation du document PDF doivent être contenues dans le PDF proprement dit.

En conséquence de quoi:

> **MUST NOT**: Aucune référence externe important pour l'apparence ou la pertinence du document PDF ne doit être intégrée.
>
> **MUST NOT**: L'importation dynamique d'informations externes ne doit pas être effectuée, voir ISO 32000-1 chapitre 7.11.4.1.

Exemple JavaScript:

> **MUST NOT**: Toute importation dynamique de programme JavaScript externe est proscrite, voir chapitre 3.6.1 dans [2]. L'importation dynamique signifie: que l'on trouve, dans le document, une référence à un programme JavaScript externe au PDF, qui est chargé à l'ouverture du document PDF et s'y exécute.
>
> Qui plus est:
>
> **MUST:** Toutes les actions JavaScript doivent être couvertes par la première signature PDF, qui a valeur de constatation. Les modifications apportées aux actions JavaScript ainsi qu'à leurs paramètres doivent avoir pour effet d'invalider la signature PDF, voir également le CHAPITRE 2.5.5 «Legal Content Attestation».

2.5.5 Legal Content Attestation

Le Legal Content Attestation Dictionary permet de spécifier, avant d'apposer la certificate signature, combien d'éléments d'un type donné, susceptibles de modifier l'apparence (en anglais appearance)

chez le destinataire du PDF (signé), sont conservés dans le PDF. Autrement dit le destinataire du document PDF signé peut y voir autre chose que celui qui a fourni/réalisé la certification signature.

SHOULD: Une Legal Content Attestation doit être jointe à une certification signature.

> Extrait des normes ISO-32000-1 CHAPITRE 12.8.5 et ISO-32000-2 CHAPITRE 12.8.2.2.1 «A certification signature should have a legal attestation dictionary.»

MUST: Dans le cas où une Legal Content Attestation est jointe, les renseignements qu'elle contient concernant un type doivent concorder avec le nombre d'éléments de ce type réellement présents dans le PDF en question.

MUST: Le Signature Handler doit s'enquérir de la présence ou non d'une opposition correspondante et l'annoncer en conséquence.

Voici un profil pour une Legal Attestation, sous réserve qu'elle soit insérée, lorsque le document doit être archivé ou est un acte, le tableau suivant étant extrait de la norme ISO 32000-2 (tableau 264). Dans la norme ISO 32000-1, il s'agit du tableau 259.

MUST: Sur la base, notamment, des explications fournies au CHAPITRE 2.5.4 «Références externes», le profil à appliquer pour la Legal Content Attestation est le suivant.

Entry	Value /Explanation	Recommendation
JavaScriptActions	The number of ECMAScript actions found in the document	E (entrée requise)
LaunchActions	The number of launch actions found in the document.	E. La valeur DOIT être 0.
URIActions	The number of URI actions found in the document	E. La valeur DOIT être 0.
MovieActions	The number of movie actions found in the document	E. La valeur DOIT être 0.
SoundActions	The number of sound actions found in the document	E. La valeur DOIT être 0.
HideAnnotationActions	The number of hide actions found in the document	E. La valeur DOIT être 0.
GoToRemoteActions	The number of remote go-to actions found in the document	E. La valeur DOIT être 0.
AlternateImages	The number of alternate images found in the document	E. La valeur DOIT être 0.
ExternalStreams	The number of external streams found in the document.	E. La valeur DOIT être 0.
TrueTypeFonts	The number of TrueType fonts found in the document.	Aucune restriction

Entry	Value /Explanation	Recommendation
ExternalRefXobjects	The number of reference XObjects found in the document	E. La valeur DOIT être 0.
ExternalOPIdicts	The number of OPI dictionaries found in the document	E. La valeur DOIT être 0.
NonEmbeddedFonts	The number of non-embedded fonts found in the document	E. La valeur DOIT être 0.
DevDepGS_OP	The number of references to the graphics state parameter OP found in the document	E. La valeur DOIT être 0.
DevDepGS_HT	The number of references to the graphics state parameter HT found in the document	E. La valeur DOIT être 0.
DevDepGS_TR	The number of references to the graphics state parameter TR found in the document	E. La valeur DOIT être 0.
DevDepGS_UCR	The number of references to the graphics state parameter UCR found in the document	E. La valeur DOIT être 0.
DevDepGS_BG	The number of references to the graphics state parameter BG found in the document	E. La valeur DOIT être 0.
DevDepGS_FL	The number of references to the graphics state parameter FL found in the document	E. La valeur DOIT être 0.
Annotations	The number of annotations found in the document	E. La valeur DOIT être 0.
OptionalContent	*true* if optional content is found in the document	E. La valeur DOIT être 0
Attestation	An attestation, created by the author of the document, explaining the presence of any of the other entries in this dictionary or the presence of any other content affecting the legal integrity of the document.	E: MAY

Tableau 1: Recommandations relatives aux paramètres respectifs pour «Legal Contest Attestation».

2.6 Autres signatures pertinentes

Pour la thématique traitée à cet endroit, des signatures autres que la signature figurant dans un document pdf sont également abordées, notamment les signatures relatives aux

- 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).

2.7 Notion d'information de vérification

Les informations de vérification correspondent à des renseignements permettant de vérifier la signature et la validité du certificat concerné au moment de la création de la signature. Il s'agit de:

- Certificat de signature par lequel peut être vérifiée la signature PDF, mais également la chaîne de certificats pour la vérification du certificat de signature (voir art. 2 al. c SCSE)
- Statut de la validité d'un certificat de signature comme dans une réponse OCSP ou dans un CRL, ainsi que les certificats pour la vérification de ces renseignements
- Renseignements temporels fiables sous la forme d'un horodatage, ainsi que les certificats pour la vérification de la signature de l'horodatage

2.8 Défis/synthèse

2.8.1 Information de vérification

Les normes ETSI portant sur la préservation de la validité des signatures PDF et des signatures XFA reposent sur ISO-32000-1. Toutefois, la norme ISO 32000-1 (PDF 1.7) ne contient pas tous les caractères pour la préservation de la validité des signatures PDF. C'est la raison pour laquelle des extensions, qui ne figurent pas dans la norme ISO-32000-1 (PDF 1.7), ont été introduites dans la norme ISO 32000-2 (PDF 2.0). Il s'agit notamment de

- Horodatage de document
- Document Security Store (DSS), dans lequel les informations peuvent être mises en paquet pour une vérification à long terme (en anglais Long Time Validation, LTV en abrégé).
- Sous-filtres supplémentaires, pour déterminer notamment les algorithmes à utiliser

Les fonctions/caractères désormais inclus(es) dans la norme ISO 32000-2 (PDF. 2.0) ont été adoptées par l'ETSI.

En outre, les informations de vérification concernant le statut de la signature CMS selon la norme ISO-32000-1 (PDF 1.7) sont jointes en tant qu'attribut signé «PDF - propriétaire» ASN.1, cet attribut n'étant pas conforme aux normes CAdES de l'ETSI. Selon la norme ISO 32000-1 (PDF 1.7), les informations de vérification doivent être intégrées lors de la création de la signature.

Remarque: L'ajout a posteriori d'informations de vérification supplémentaires lors de la signature PDF aurait pour conséquence d'invalider la signature.

2.8.2 Archivage

Avec la préservation de la validité des signatures PDF, on cherche bien souvent à archiver également le document. La norme ISO 19005-x contient des normes à cet égard et le CECO a également émis des recommandations en ce sens.

2.8.3 Harmonisation des normes entre elles

Les normes ne sont pas harmonisées entre elles. L'attribut «signature-policy-identifier», par exemple, doit être ajouté selon la norme ISO-32000-2 (PDF 2.0) en tant qu'attribut signé de la signature PDF, alors qu'il peut être ajouté comme attribut signé selon la norme ETSI EN 319 142-1.

2.8.4 Actualité des normes

Les normes ISO 32000-2 (PDF 2.0) et ISO 19005-4 (PDFA/4) n'ont été publiées qu'en 2020. Des retards sont donc à prévoir dans la mise en œuvre dans Reader et Writer.

2.8.5 Sécurité du format PDF en tant que tel

Jusqu'à il y a encore quelques années, le format PDF était considéré comme «sûr». Cependant, une porte d'entrée peut être intégrée dans un PDF et favoriser les attaques contre la sécurité du système informatique, voir à ce sujet les CHAPITRES 2.5.2, 2.5.3, 2.5.4.

2.8.6 Produits

Le PDF Reader devrait également pouvoir comprendre et contrôler ce le PDF Writer qu'écrit. Il est attendu du PDF Reader qu'il prenne en charge toutes les formes des normes, dans ce cas précis, les normes ETSI correspondantes, ISO-32000-1 (PDF 1.7) et ISO-32000-2 (PDF 2.0). Ce faisant, il doit également pouvoir être capable de reconnaître toute modification apportée aux champs dans le PDF couverts par la signature PDF.

2.8.7 Signature PDF

D'ordinaire, des attributs non signés tels qu'une réponse OCSP peuvent être joints sans encombre à la signature CMS une fois la signature apposée. Cela n'est pas possible avec la signature PDF, qui est intégrée au PDF. Des attributs CMS non signés ajoutés a posteriori à la signature PDF ont pour effet d'invalider la signature PDF.

3 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.

3.1 Certificats

3.1.1 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), faute de quoi, la «conservation» fiable et généralement reconnue des documents signés électroniquement pourrait se révéler beaucoup plus difficile, voire impossible. La normalisation de ce dernier n'entre (pour le moment) pas dans le champ d'application du présent document.

3.1.2 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 [1].

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

3.1.3 Format certificats

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

3.2 Horodatage

3.2.1 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 doivent être utilisés (art. 2, let. j, SCSE).

3.2.2 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: La norme ETSI TS 101 903 V1.4.2 prévoit encore la possibilité d'ajouter des horodatages au format XML, voir chapitre 7.1.4.2. Leur utilisation n'est pas donc pas autorisée dans ce contexte, notamment parce qu'ils ne sont pas reconnus du point de vue légal.

3.3 Format des réponses OSCP

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

SHOULD: La chaîne de certificats permettant de vérifier la signature de l'OCSP doit être jointe à la réponse OCSP.

La chaîne de certificats pour la vérification de la réponse OCSP doit être soit jointe à la signature CMS de la réponse OCSP en tant qu'attribut non signé dans «certificate-values» et «revocation-values» . Soit la réponse OCSP en tant que telle ou sa chaîne de certificats peuvent être classées a posteriori dans le Document Security Store (DSS). Dans le DSS, la réponse OCSP et la chaîne de

certificats correspondante peuvent aussi être classées dans un champ séparé.

Dans le cas d'une signature XML, la chaîne de certificats pour la réponse OCSP peut être jointe à l'élément XML «RevocationValues».

3.4 Format de signature XML

Tiré de la norme eCH-0230, CHAPITRE 2.4:

> **MUST:** Une signature XML doit correspondre à la norme XML Signature Syntax de W3C. 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. Concernant la réservation de la validité des signatures XML, voir eCH-0230

3.5 Format de la signature CMS

Concernant les formats CMS voir eCH-0220.

3.6 Horodatage

3.6.1 Horodatage d'une signature PDF

Contrairement à CAdES (voir eCH-0220), on ne recense pour les signatures PDF que les 3 types d'horodatage suivants:

- Inhaltszeitstempel (engl. content timestamp). Il s'agit de l'horodatage de ce qu'il faudra signer ultérieurement. Il atteste ainsi que la date à laquelle a été réalisée la signature est bien ultérieure (à l'heure indiquée dans l'horodatage).
- Horodatage de signature (signature timestamp) qui couvre la signature). Il atteste ainsi que la signature a bien été réalisée avant un moment précis (heure indiquée dans l'horodatage).
- Horodatage de document qui couvre l'intégralité du document PDF. L'horodatage du document correspond à peu près à l'horodatage des archives pour CAdES et à une signature PDF couvrant le document, à ceci près que la signature n'a pas été produite par l'utilisateur ou l'utilisatrice, mais par le service d'horodatage. Cependant, l'ISO ne prend en charge, de manière standard, l'horodatage de document qu'à compter de la norme ISO-32000-2 (PDF 2.0).

Remarque: Eine PDF-Signatur ist in einem PDF-Dokument eingebettet. Ainsi, l'ajout a posteriori d'informations supplémentaires à la signature PDF est impossible sans rendre la signature invalide.

Illustration: La signature CMS peut en principe être assortie d'informations supplémentaires (attributs non signés) sans que la signature CMS ne s'en trouve invalidée. Pour la signature PDF, une forme particulière de la signature CMS, cela n'est pas possible, sinon la signature PDF n'est pas valide. Cela s'explique par le fait que la signature PDF est intégrée dans le PDF, voir ETSI TS102 778 chapitre 4.

3.6.2 Horodatage dans les objets XML

Se reporter au tableau 1 dans la norme eCH-0230 pour en savoir plus sur les formes/contenus possibles des horodatages. Il existe en outre une possibilité d'ajouter un horodatage de document à un document XFA intégré dans un PDF.

4 Profil

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

4.1 Principes

4.1.1 Recommandations concernant la signature XML

voir à ce sujet eCH-0230 et eCH-0091.

4.1.2 Recommandations concernant la signature PDF

SHOULD: Voir à ce sujet eCH-0220. À la différence des normes ETSI relatives au PAdES, seule la version dans le RFC 5652 doit être prise en charge lors de la création d'une signature CMS.

MUST NOT: l'utilisation de signatures au format PKCS#1 n'est pas autorisée.

Motif: PKCS#1 signatures are deprecated with 32000-2 (PDF 2.0).

4.1.3 Classement de l'information de vérification

ISO 32000-2 (PDF 2.0) connaît les 4 endroits différents suivants, où une information de vérification peut être déposée pour la vérification des signatures PDF et pour la vérification des signatures de l'information de vérification:

1. Dans «Cert» dans le Signature Dictionary (pour la chaîne de certificat) pour la vérification de la signature PDF en tant que telle.
2. Als unsigniertes Attribut bei der CMS-Signatur
3. ASN.1 Objet «adbe-revocationInfoArchival», où la réponse OCSP et le CRL peuvent être mis en paquet.
4. Dans le Document Security Store (DSS)

ISO 32000-1 (PDF 1.7) connaît 1, 2 et 3, ISO 32000-2 recommande 2, 3, 4, alors que ETSI ne prend en charge que 2 et 4.

Remarque: «Cert» et «adbe-revocationInfoArchival» sont des objets signés, autrement dit ils sont couverts par la signature PDF. Concernant «adbe-revocationInfoArchival», voir ISO 32000-1, chapitre 12.8.3.3.1.

4.1.3.1 Document Security Store

Le contenu et la propriété du Document Security Store (DSS) sont décrits au CHAPITRE 12.8.4.3 «Document Security Store (DSS)» dans ISO 32000-2. L'interaction entre DSS et HDD y est illustrée à la figure 86 et aux figures 2 et 3 de la norme ETSI EN 319 142-1.

4.1.3.2 Recommandations

MUST NOT:«Cert» ne doit pas être utilisé.

SHOULD NOT: «adbe-revocationInfoArchival» ne devrait pas être utilisé.

Justification:

- Cet objet n'est pas traité par les normes ETSI EN 319 142-1 et ETSI EN 319 142-2.
- «adbe-revocationInfoArchival» ne permet pas d'attester que le certificat était valide avant que la signature soit réalisée. Hormis si un horodatage est effectué immédiatement après, mais dont les informations de vérification ne sont pas contenues dans «adbe-revocationInfoArchival».

SHOULD: Le certificat de vérification de la signature PDF devrait être joint, de même que la chaîne de certificats servant à la vérification de ce certificat. Des informations concernant le statut du certificat devraient également être jointes. Les informations doivent, dans la mesure du possible, être jointes à la signature CMS pour être compatibles avec la norme ISO 32000-1, sinon dans le DSS.

SHOULD: Les informations concernant la vérification de la signature et le statut du certificat de signature, comme la liste de révocation de certificat (CRL) ou les réponses OCSP, doivent être jointes dans une qualité aussi importante que possible. Les informations doivent avoir été vérifiées et considérées comme valides au moment de la création de la signature PDF.

SHOULD: Le statut du certificat doit être spécifié de façon prioritaire au moyen de réponses OCSP.

Remarque: Si ces réponses ne sont pas jointes à la signature PDF lors de la création de cette dernière, elles ne pourront plus être intégrées à la signature PDF par la suite. Des attributs non signés ajoutés a posteriori à la signature PDF ont pour effet d'invalider la signature PDF.

Dans le cas où les informations de vérification n'ont pas été jointes avant la signature, elles peuvent encore être complétées plus tard dans le PDF via le Document Security Store Dictionary (DSS), voir ETSI TS 102 778-4.

4.1.4 Vérification de la signature PDF

Les CHAPITRES 12.8.3.4.5 à 12.8.3.4.8 de la norme ISO 32000-2 stipulent des exigences concernant la vérification de la signature PDF.

MUST: Ces exigences minimales pour la vérification d'une signature électronique doivent être respectées.

4.2 ETSI TS 102 778-1

ETSI TS 102 778-1 propose un aperçu de la thématique des signatures PDF et des signatures XML dans un PDF. ETSI TS 102 778-2 à 4 aborde la préservation de la validité des signatures au format CMS.

4.3 ETSI TS 102 778-2

Cette norme définit des directives générales portant sur la réalisation d'une signature PDF.

4.3.1 Sous-filtre pour les signatures PDF

Des «sous-filtres» permettent de définir, entre autres, le jeu possible d'algorithmes pouvant être utilisés pour la constitution de la signature PDF. La norme ISO 32000-2 (tableau 260) prend en charge davantage de classes de sous-filtres et d'algorithmes que la norme ISO 32000-1 (tableau 257).

Contrairement à la norme ISO 32000-1, la norme ISO 32000-2 reconnaît encore les sous-filtres «ETSI.CAdES.detached» et «ETSI.RFC3161».

MUST NOT: Le sous-filtre «ETSI.RFC3161» étant prévu uniquement pour l'horodatage des documents, il ne doit pas être utilisé lors de la constitution de la signature PDF (selon ISO-32000-2).

SHOULD: Il faut utiliser les sous-filtres figurant dans la norme ISO-32000-1 à des fins de compatibilité. Ceci étant:

MUST NOT:L'utilisation du sous-filtre «adbe.x509.rsa_sha1» n'est pas autorisée.

MUST: Dans le cas où une signature PDF doit être réalisée avec des courbes elliptiques, le sous-filtre «ETSI.CAdES.detached» doit être utilisé. Ce n'est qu'avec la norme ISO-32000-2 (PDF 2.0) que, pour la première fois, les courbes elliptiques sont prises en charge par défaut. Ce sous-filtre est notamment prévu à cet effet.

4.3.2 seed value (signature field, certificate)

Extrait de la norme ETSI EN 319 142-2 V1.1.1, annexe A8:

> When preparing a document or form to be signed in the future, the author of the form can add to the signature field some additional entries (ISO 32000-1 [1], clause 12.7.4.5, table 232) including one called a seed value dictionary. A seed value dictionary (ISO 32000-1 [1], clause 12.7.4.5, table 234) contains information that conveys a set of rules (or policies) that the form's author wishes the signature handler to enforce at the time the signature is applied. These wishes can be specified either as requirements or recommendations.

Le seed value Dictionary sert à contrôler le traitement des documents dans le cadre de la fourniture d'une signature électronique ainsi que sa forme. Par exemple, la seed value peut servir à définir quel algorithme de Hash utiliser pour la signature.

La seed value fait référence aux informations contenues dans le PDF, voir tableau 234 et 235 dans ISO 32000-1 et dans [2], CHAPITRE 6.1.2. Les tableaux 237 et 238 dans la norme ISO 32000-2 décrivent ce qui peut être contrôlé avec quelle version de PDF.

MAY: La seed value peut être ajoutée.

MUST: Dans le cas où la seed value est ajoutée, les règles qu'elle contient doivent concorder avec les recommandations faites dans le présent document. Autrement dit le Signature Handler doit être capable de suivre les règles stipulées dans la seed value, voir également CHAPITRE 4.2.6 ETSI EN 319 142-2.

Le CHAPITRE 5.1.3 expose sous forme de synthèse quelles propriétés ou quelles configurations peut avoir la seed value pour se conformer aux recommandations émises dans la présente norme.

4.4 ETSI TS 102 778-3

ETSI TS 102 778-2 définit la formation de signature. ETSI TS 102 778-3 est considérée comme une extension visant la préservation de la validité des signatures dans un PDF. Les extensions discutées dans ETSI TS 102 778-3 contiennent toutefois des attributs qui doivent être couverts par la signature CMS et qui ne peuvent être ajoutés a posteriori.

4.4.1 Attributs CMS (obligatoires) en discussion

4.4.1.1 Attribut content-type

Contrairement à ETSI EN 319 122-1, la valeur de l'attribut content-type est prescrite.

MUST: La valeur «id-data» doit être utilisée.

4.4.1.2 message-digest Attribut

MUST: L'attribut Message-digest doit être joint.

4.4.1.3 Attributs signature-policy-identifier

La recommandation dans ETSI EN 319 142-1 va à l'encontre des recommandations formulées dans la norme ISO 32000-2 (PDF2.0) p. 582.

Si selon la norme ETSI EN 319 142-1, l'attribut à signer peut être inclus, selon ISO 32000-2, il doit être contenu dans la signature CMS.

SHOULD NOT: Les références externes aux informations relatives à une signature ne doivent pas être contenues.

4.4.1.4 Référence au certificat de vérification de signature

voir à ce sujet les remarques relatives aux attributs ESS signing certificate et ESS signing-certificate - v2 dans eCH-0220.

4.4.2 signature-time-stamp

MUST:L'attribut signature-time-stamp avec un horodatage qui y est contenu selon le CHAPITRE 3.2.1 «Qualité de l'horodatage» doit être contenu.

Remarque: Une signature qualifiée au sens de l'art. 12 al. 2^{bis} CO requiert un horodatage de cette classe de qualité.

4.4.3 Autres attributs

Parmi les possibilités, on peut placer des informations identiques ou similaires à différents endroits.

1. dans le texte du document
2. Renseignements supplémentaires dans le Signature Dictionary du PDF
3. comme dans un attribut CMS également.

Il est par exemple possible d'indiquer le lieu où a été apposée la signature ou son motif.

SHOULD: Ces informations, si elles existent, doivent être insérées dans l'ordre indiqué ci-dessus. La possibilité d'insérer ensuite l'information doit être écartée. Motif de la priorisation préconisée: L'information jouit auprès de l'utilisateur ou de l'utilisatrice d'une plus grande visibilité pour 1) que pour 2), et pour 2) que pour 3).

Voir chapitre 3.1.2.8 dans eCH-0220 pour des explications et les intentions du signataire.

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

La norme ETSI EN 319 142-2, dont la portée normative est supérieure à celle de la norme ETSI TS 102 778-3, stipule p. 9 al. c ce qui suit:

> «Some signature attributes found in CAdES [2] have the same or similar meaning as keys in the Signature Dictionary described in ISO 32000-1. For signature attributes and keys that have the same or similar meaning only one of them should be used according to the requirements set in table defined in clause 6.3 in the present document.»

Cette affirmation peut être en contradiction avec les recommandations formulées dans la norme ETSI TS 102 778-3. En effet, selon la norme ETSI TS 102 778-3, les attributs dans les chapitres 4.5.3 à 4.5.7 et 4.5.9, 4.5.10 ne doivent pas y être insérés.

Concernant les attributs qui peuvent être joints à la signature par le signataire, renvoi est fait à ce qui suit dans le chapitre 3.1.2.10 eCH-0220:

> **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.

Pour les références aux policies, voir le chapitre 3.1.2.4 dans eCH-0220:

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

4.5 ETSI TS 102 778-4

Il s'agit pour l'essentiel de normaliser ici la réalisation de l'horodatage d'un document PDF. Cette norme a été supplantée par ETSI EN 319 142-1 et 2.

4.6 ETSI TS 102 778-5

Remarque: Tel qu'évoqué précédemment au CHAPITRE 2.3 «XFA», Adobe ne prend plus XFA en charge, qui est donc considéré comme obsolète pour la norme ISO 32000-2 (PDF 2.0). Ce sous-chapitre ne revêt par conséquent aucun caractère normatif.

La norme ETSI TS 102 778-5 normalise l'utilisation et la préservation de la validité des signatures XML des objets XML dans un objet XFA et la signature XML via un objet XFA. L'objet XFA est alors intégré dans un PDF.

4.6.1 Formes de signatures XML dans un document XFA

Il existe en principe 3 formes de signatures XML dans un PDF:

1. Signature XML d'objets XML dans un XFA, intégré dans un PDF
2. Signature XML d'un objet XFA, intégré dans un PDF
3. Signature PDF d'un PDF avec un objet XFA ou objets XML qui y sont contenus

La préservation de la validité des items 1 et 2 est spécifiée dans la norme dont il est ici question, tandis que cette dernière est normalisée dans ETSI TS 102 778-4, resp. dans ETSI EN 319 142-1 et ETSI EN 319 142-2.

4.6.2 Principes

Pour simplifier, XFA est un objet basé sur XML qui peut être intégré dans un PDF ou se présenter sous la forme d'un document XML.

Remarque: Dans ETSI TS 102 778-5, CHAPITRE 1, note 3:

> «Readers should be aware that although PDF documents are addressed for human beings, XFA forms, being them based on XML, may be consumed by software applications.»

Note, suggestion: XFA propose aux utilisateurs/trices (personnes physiques) une possibilité limitée de voir ce qu'il/elle signe, raison pour laquelle un XFA pourrait d'abord être converti en PDF/A-2. Ce document serait ensuite signé par l'utilisateur ou l'utilisatrice. Dans un souci de ne pas trop restreindre les possibilités de traitement des données après la conversion du XFA en un PDF/A-2 ou, le cas échéant, en un PDF/A-4, les données peuvent être enregistrées dans un code-barres ou un code QR et intégrées au PDF avant la réalisation de la signature.

Indication dans la norme ETSI TS 102 778-5, CHAPITRE 1, note 1:

> «Implementers should be aware that any subsequent approval signature (see ISO 32000-1 [4] clause 12.8.1) as specified in TS 102 778-2 [i.7], TS 102 778-3 [i.8] or TS 102 778-4 [i.9] also signs the embedded signed XML document. Any upgrade of the XAdES signature of the present document to support validation long after the expiration of the signing certificate or other extended features such a countersignatures (e.g. using XAdES-C or XAdES-X or XAdES-A) would invalidate the aforementioned approval signatures. Implementers should also be aware that certification signatures (see ISO 32000-1 [4] clause 12.8.1) as specified in TS 102 778-2 [i.7], TS 102 778-3 [i.8] or TS 102 778-4 [i.9] signing the embedded signed XML document, may be used in conjunction with the DocMDP dictionary, allowing changes in the embedded signed XML document (by upgrading the XAdES signatures, for example) without invalidating such signatures.»

La signature a pour but et vocation de reconnaître les modifications dans le document et d'affecter le document au signataire. Or, cela va désormais à l'encontre de la possibilité d'apporter des modifications dans le document sans pour autant que la signature ne s'en trouve invalidée. C'est pourquoi il est ici fait référence aux recommandations indiquées au CHAPITRE 4.9 du présent document.

La norme eCH-0091 stipule notamment les aspects à prendre en compte lors de la création d'une signature XML. Autres recommandations portant sur la signature XML relatives à XFA dans le CHAPITRE 4.9 du présent document.

4.6.3 Profil

Les recommandations ici établies ont été dépassées par la norme ETSI EN 319 142-2. (tel qu'évoqué précédemment, les normes désignées «EN» dans le titre priment sur celles avec «TS»). Le profil pour les autres thématiques traitées dans la norme ETSI TS 102 778-5 est exposé au CHAPITRE 4.9 «ETSI EN 319 142-2».

4.7 ETSI TS 102 778-6

Cette norme définit ce qui doit se présenter au lecteur d'un document PDF signé comme résultat

d'une vérification de signature.

MUST: Toutes les exigences décrites dans la norme ETSI TS 102 778-6 doivent être remplies.

4.8 ETSI EN 319 142-1

ETSI EN 319 142-1 normalise les attributs/informations qui peuvent/devraient/doivent ou ne devraient pas être ajoutés au document PDF avec une ou plusieurs signatures PDF. Dies mit dem Ziel, dass die Gültigkeit der PDF-Signaturen nachweislich bewahrt werden kann. La préservation de la validité repose sur le fait que, lors de la création de l'horodatage du document, toutes les informations nécessaires à la vérification des signatures PDF réalisées et des réponses OCSP et CRL reçues auparavant sont collectées et enregistrées dans le PDF. Les formes de l'horodatage des documents ETSI EN 319 142-1 sont en outre normalisées.

Des compléments à la norme sont répertoriés et les recommandations dans la norme sont évaluées différemment dans la suite du document.

4.8.1 Gestion/collecte des informations de vérification en tant que telles

MUST NOT: Aucune référence à des informations de vérification enregistrées hors du PDF et pertinentes pour le contrôle ne doit être contenue. Le dernier horodatage de document réalisé y fait exception. Les informations de vérification correspondantes ne doivent être jointes qu'avant la réalisation de l'horodatage suivant.

MUST: Les informations de vérification (certificats CA) pour la vérification des signatures OSCP ou CRL doivent également être jointes.

MAY: Les informations de vérification appartenant à la signature OCSP peuvent être jointes à la signature OCSP dans un PDF selon la norme ISO-32000-1 (PDF 1.7).

MAY: Les informations de vérification appartenant à la signature CRL peuvent être jointes à la signature dans un PDF selon la norme ISO-32000-1 (PDF 1.7).

SHOULD: Conformément à la norme ISO-32000-2 (PDF 2.0), les informations de vérification pour la signature OCSP et pour la CRL devraient être classées dans le Document Security Store (DSS).

4.8.2 Horodatage des documents

4.8.2.1 Sous-filtre pour horodatage de documents (HDD)

MUST: Le sous-filtre «ETSI.RFC3161» doit être utilisé pour les horodatages de documents.

Remarque: D'après les normes ISO 32000-2 et ETSI, ce filtre doit être utilisé. La norme ISO 32000-1 ne connaît pas l'horodatage des documents ni ce sous-filtre.

4.8.2.2 Anfertigen des 1. Horodatage des documents (HDD)

Sous réserve que cela ne soit pas déjà stipulé ailleurs:

> **MUST:** Juste avant la réalisation de l'horodatage du document, les informations de vérification les plus récentes (OCSP, CRL) concernant le statut des certificats pour les signatures PDF doivent être collectées et enregistrées dans le DSS du PDF.

Qui plus est, la chaîne de certificats pour les signatures PDF doit être classée, au même titre que les chaînes de certificats pour la vérification des réponses OCSP ou de la CRL.

MUST: Toutes les signatures, dont la certification signature, doivent être valides avant la création du premier horodatage du document.

MUST NOT: Dans le cas contraire, aucun horodatage de document ne peut être créé.

SHOULD NOT: Dans le cas où toutes les signatures ne sont plus valides avant le premier horodatage du document, la signature PDF ne doit plus être acceptée.

4.8.2.3 Réalisation du 2e horodatage de document et supplémentaires

Avant de réaliser l'horodatage de document suivant:

MUST: Les informations de vérification (CRL, OCSP) permettant de vérifier la signature de l'horodatage de document doivent être enregistrées.

MUST: La chaîne de certificats servant à la vérification de la signature de l'horodatage du document ainsi que la signature des réponses OSCP et de la CRL doit être collectée et classée.

MUST: La validité de l'horodatage du document précédent doit être vérifiée.

SHOULD: Si le HDD n'est plus considéré comme valide, il ne faut pas en réaliser et insérer un autre.

4.8.3 Autre évaluation des recommandations

4.8.3.1 Chiffrement

Le chapitre 5.5 de la norme EN 319 142-1 évoque un chiffrement qui doit être effectué avant l'apposition de la signature. Hier gilt es zu unterscheiden.

MUST: Dès lors que la signature est utilisée à des fins de constatation, elle doit être apposée avant le chiffrement. C'est en principe la validité, non pas de ce qui a été chiffré, mais bien de ce qui a été constaté qui doit être préservée.

SHOULD: Si la signature sert uniquement à l'authenticité, elle doit être réalisée après le chiffrement. Le risque que le destinataire déchiffre quoique ce soit dont il ne peut pas attribuer l'origine s'en trouve ainsi réduit.

4.8.3.2 content-time-stamp

content-time-stamp est un attribut signé. Il contient une indication fiable de l'heure t sous la forme d'un horodatage, qui doit permettre de prouver que la signature PDF a bien été créée après cet instant t.

SHOULD NOT: L'attribut content-time-stamp ne devrait pas être utilisé. Les normes ISO-32000-1 (PDF 1.7) et -2 (PDF 2.0) ne définit pas ce point et il peut être contenu selon la norme EN 319 142-1 (MAY).

Remarque: La recommandation à ce sujet diffère de la norme eCH-0220.

4.8.3.3 signature-time-stamp

MUST:L'attribut signature-time-stamp avec un horodatage qui y est contenu selon le chapitre 3.2.1 «Qualité de l'horodatage» doit être contenu.

Remarque: Une signature qualifiée au sens de l'art. 12 al. 2bis CO requiert un horodatage de cette classe de qualité.

4.8.3.4 Renseignements concernant le signataire

SHOULD NOT: Les renseignements tels le lieu, le motif de la fourniture de la signature et l'adresse de contact du signataire ne doivent pas être mentionnés en tant que métadonnées de la signature PDF, mais être extraits du document, voir également à ce sujet le CHAPITRE 4.4.3 «Autres attributs»

4.9 ETSI EN 319 142-2

Tel qu'évoqué précédemment au CHAPITRE 2.3 «XFA», Adobe ne prend plus XFA en charge, qui est donc considéré comme obsolète pour la norme ISO 32000-2 (PDF 2.0). Ce sous-chapitre ne revêt par conséquent aucun caractère normatif.

4.9.1 Compléments généraux

MUST: Die Zertifikatskette zur Prüfung der XML-Signatur muss der XML-Signatur beigefügt werden.

MUST: L'horodatage de la signature (SignatureTimeStamp) doit être joint à la signature XML.

4.9.2 Signature XML via un objet XFA ou un objet XML dans un PDF

En principe, la validité des signatures XML des objets peut être préservée dans un objet XFA ou via un objet XFA selon la norme eCH-0230. Toutefois cela ne fonctionne plus dès lors qu'une signature PDF a été créée avant ou après. La préservation de la validité d'une signature PDF requiert un horodatage de document. Suite à un horodatage de document, il n'est plus possible de mettre à jour la signature XML avec un horodatage selon eCH-0230 (XAdES). Une telle mise à jour aurait pour effet d'invalider l'horodatage du document ou de la signature PDF.

4.9.3 LTV d'une signature XML avec HDD (de PDF)

La préservation de la validité d'une signature XML (d'un document XML ou d'un objet XML) dans un PDF peut être réalisée via l'horodatage de document et le Document Security Store (DSS) comme pour une signature PDF.

Pour savoir comment y parvenir, se reporter à l'annexe A informelle de la norme ETSI TS 102 778-5 V1.1.2.

Remarque: Il est nécessaire d'établir la LTV avec un HDD via un PDF avec XFA intégré ou des objets XML par exemple après une signature PDF.

5 Condensé

Les tableaux suivants offrent une synthèse des attributs pertinents traités dans le présent document.

5.1 Signature PDF

5.1.1 Attributs CMS

Le tableau suivant présente les attributs concernant une signature CMS dans un PDF. Il peut en résulter des recommandations divergeant de la norme eCH-0220.

N°	Attribut	Signé	Rec.	Rem
1.	Attribut content-type	J	M	Valeur: «id-data»
2.	countersignature	J	MN	
3.	content-hints Attribute	J	MN	
4.	signature-policy-identifier	J	SN	B, PDF-SIG
5.	commitment-type-indication Attribute	J	SN	B, PDF-SIG
6.	signer-location Attribute	J	SN	C, PDF-SIG
7.	Attributs content-time-stamp	J	SN	
8.	signature-time-stamp Attribute	N	M	
9.	attribute-certificate-references Attribute	N	M, B	
10.	attribute-revocation-references Attribute	N	M, B	
11.	certificate-values Attribute	N	M, B	2)
12.	revocation-values Attribute	N	MAY, B	1) via HDD
13.	CAdES-C-time-stamp Attribute	N	MN	
14.	time-stamped-certs-crls-references Attribute	N	MN	
15.	archive-time-stamp Attribute	N	MN	
16.	ats-hash-index Attribute	N	MN	
17.	archive-time-stamp-v3 Attribute	N	MN	
18.	long-term-validation Attribute	N	MN	
19.	signer-attributes-v2 attribute	J	MAY	C
20.	claimed-SAML-assertion	N	MN	
21.	ats-hash-index-v2 attribute	N	MN	
22.	signer-attributes Attribute	J	SN	C
23.	ats-hash-index-v3 attribute	N	MN	

Tableau 2: Synthèse des recommandations concernant les attributs CMS

Légende

A = Alternative
B = 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.
HDD = Horodatage de document PDF
O = OUI
M = MUST
MN = Must NOT
N = Non
NE = Évoqué dans la norme, mais pas traité ici car aucun avis contraire.
PDF-SIG l'information peut également être jointe à la signature dans le PDF
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
1) Les informations de révocation peuvent également être insérées a posteriori via le DSS avant la création du HDD.
2) Le certificat de signature au minimum devrait être joint à la signature. D'autres informations de vérification (chaîne de certificats) peuvent être insérées par la suite via le DSS.

SHOULD NOT: Dans le cas où les attributs de la signature PDF ont été joints, l'information ne devrait également pas être encore contenue comme attribut dans la signature CMS, et inversement.

Remarque: Dans le cas où les attributs CMS n'ont pas été joints à la signature CMS, ils ne peuvent ajoutés a posteriori, car la signature PDF aurait alors perdu toute validité.

5.1.2 Im PDF als Metadaten der PDF-Signatur mitgegeben

Le tableau suivant répertorie les attributs PDF pouvant être joints à la signature PDF en tant que métadonnées:

N°	Attribut	Signé	Rec.	Rem
1	Reason	J	SN	Er
2	Location	J	SN	Er, C
3	Legal Content Attestation	J	S	
4	Exigence imposée au certificat concernant la vérification de la signature PDF (OID dans le certificat X.509 v3)	J	MAY, B	1)
5	Détermination du créateur de l'horodatage	J	MAY	
6	Heure de la signature	J	SN	C, 2)
7	Contact	J	SN	Er

Tableau 3: Synthèse des recommandations concernant les attributs qui peuvent être ajoutés à la signature CMS.

Légende

A = Alternative
B = 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.
CMS = Info peut être contenue dans la signature CMS.

Er = l'info devrait être contenue dans le document PDF.
O = OUI
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
1) L'exigence doit ressortir du contexte juridique.
2) L'horodatage de la signature est pertinent à cet égard.

5.1.3 seed value

5.1.3.1 signature field seed value

Key	Value/Explanation/Justification pour recommandation	Recommendation
Type	The type of PDF object that this dictionary describes; if present, shall be SV for a seed value dictionary.	MUST
Ff	A set of bit flags specifying the interpretation of specific entries in this dictionary. A value of 1 for the flag indicates that the associated entry is a required constraint. Justification: Il contient des directives obligatoires.	MUST
Filtre	The signature handler that shall be used to sign the signature field, beginning with PDF 1.7	SHOULD
SubFilter	An array of names indicating encodings to use when signing. The first name in the array that matches an encoding supported by the signature handler shall be the encoding that is actually used for signing. Les Subfilter et les Encoding devraient, si possible, être définis	MUST
DigestMethod	An array of names indicating acceptable digest algorithms to use while signing. This property is only applicable if the digital credential signing contains RSA public/private keys.	SHOULD
V	The minimum required capability of the signature field seed value dictionary parser. A value of 1 specifies that the parser shall be able to recognise all seed value dictionary entries in a PDF 1.5 file. A value of 2 specifies that it shall be able to recognise all seed value dictionary entries specified. A value of 3 specifies that it shall be able to recognise all seed value dictionary entries specified in PDF 2.0 and earlier.	MAY
Cert	A certificate seed value dictionary containing information about the characteristics of the certificate that shall be used when signing.	SHOULD

Key	Value/Explanation/Justification pour recommandation	Recommendation
Reasons	An array of text strings that specifying possible reasons for signing a document. If specified, the reasons supplied in this entry replace those used by interactive PDF processors.	MAY
MDP	A dictionary containing a single entry whose key is P and whose value is an integer between 0 and 3. A value of 0 defines the signature as an approval signature (see 12.8, «Digital signatures»). The values 1 through 3 shall be used for certification signatures and correspond to the value of P in a DocMDP transform parameters dictionary.	MUST
TimeStamp	(facultatif; PDF 1.6) A timestamp dictionary containing two entries: 1. URL An ASCII string specifying the URL of a timestamping server, providing a timestamp that is compliant with Internet RFC 3161 as updated by Internet RFC 5816. 2. Ff An integer whose value is 1 (the signature shall have a timestamp) or 0 (the signature need not have a timestamp). Default value: 0. Si des renseignements sont fournis à ce sujet, la 2e valeur dans ce contexte doit être fixée sur 1. L'URL est facultative.	MAY
LegalAttestation	An array of text strings specifying possible legal attestations (see 12.8.7, «Legal content attestations»). The value of the corresponding flag in the Ff entry indicates whether this is a required constraint	MAY
AddRevInfo	A flag indicating whether revocation checking shall be carried out. If AddRevInfo is true, the PDF processor shall perform the following additional tasks when signing the signature field: • Perform revocation checking of the certificate (and the corresponding issuing certificates) used to sign. • Include the revocation information within the signature value. If AddRevInfo is true and the Ff entry indicates this is a required constraint, then the preceding tasks shall be performed. If they cannot be performed, then signing shall fail.	MUST

Key	Value/Explanation/Justification pour recommandation	Recommendation
LockDocument	(Ab PDF 2.0) A name value supplying the author's intent for whether the signing dialogue should allow the user to lock the document at the time of signing. Justification: En raison de la compatibilité avec PDF 1.7 non.	SHOULD NOT
AppearanceFilter	(facultatif à partir de PDF 2.0) A text string naming the appearance that shall be used when signing the signature field. En raison de la compatibilité avec PDF 1.7 non.	SHOULD NOT

Tableau 4: Recommandations concernant le signature field seed value dictionary

5.1.3.2 certificate seed value

Key	Value/Explanation/Justification pour recommandation	Recommendation
Type	The type of PDF object that this dictionary describes	MUST
Ff	A set of bit flags specifying the interpretation of specific entries in this dictionary. A value of 1 for the flag means that a signer shall be required to use only the specified values for the entry. Justification: Il contient des directives obligatoires.	MUST
Subject	An array of byte strings containing DER-encoded X.509v3 certificates that are acceptable for the verification of the signature	MAY
SignaturePolicyOID	Feature in PDF 2.0: The string representation of the OID of the signature policy to use when signing. La compatibilité avec la PDF 1.7 Signature Handler Signature Policy devrait être évidente à partir du contexte ou des règles au moment de la fourniture de la signature.	SHOULD NOT
SignaturePolicyHashValue	Feature in PDF 2.0: The computed hash value of the signature policy Justification: La compatibilité avec PDF 1.7 Signature Handler Signature Policy doit être évidente à partir du contexte ou des règles au moment de la fourniture de la signature.	SHOULD NOT
SignaturePolicyHashAlgorithm	Feature in PDF 2.0: The hash function used to compute the value of the SignaturePolicyHashValue entry.	MUST, dans le cas où la Signature Policy est utilisée.

Key	Value/Explanation/Justification pour recommandation	Recommendation
SignaturePolicyCommitmentType	Feature in PDF 2.0: If the SignaturePolicyOID is present, this array defines the commitment types that may be used within the signature policy. Justification: La compatibilité avec la PDF 1.7 Signature Handler Signature Policy devrait être évidente à partir du contexte ou des règles au moment de la fourniture de la signature.	SHOULD NOT
SubjectDN	An array of dictionaries, each specifying a Subject Distinguished Name (DN) that shall be present within the certificate for it to be acceptable for signing.	MAY
KeyUsage	An array of ASCII strings, where each string specifies an acceptable key-usage extension in the certificate for the signature verification. En cas d'utilisation, le certificat doit contenir uniquement les éléments suivants, servant à la vérification de la signature: 1 digitalSignature 2 non-Repudiation	MAY
Issuer	An array of byte strings containing DER-encoded X.509v3 certificates of acceptable issuers.	MAY
OID	An array of byte strings that contain Object Identifiers (OIDs) of the certificate policies that shall be present in the signing certificate.	MAY
URL	A URL, the use for which shall be defined by the URLType entry. Tout référencement d'informations pertinentes est interdit.	MUST NOT
URLType	(facultatif; PDF 1.7) A name indicating the usage of the URL entry. Tout référencement d'informations pertinentes pour le contenu du document est interdit.	MUST NOT

Tableau 5: Recommandations concernant certificate seed value dictionary

5.2 Composant de l'horodatage de documents

Le tableau suivant propose une synthèse des recommandations relatives à l'horodatage de documents.

N°	Attribut	Signé	Rec.	Rem
1	Certificate (certificats des signatures PDF ou horodatage jusqu'à présent) dans DSS	J	M, B	1)
2	CRL (certificats des signatures PDF ou horodatage jusqu'à présent) dans DSS	J	M	
3	Réponse OCSP (validité des certificats pour la vérification des signatures) dans DSS	J	M	
4	Name (renseignement concernant le service d'horodatage) dans le PDF signature dictionary	J	SN	
5	Location (renseignement concernant le service d'horodatage) dans le PDF signature dictionary	J	SN	
6	Reason (renseignement concernant le service d'horodatage) dans le PDF signature dictionary	J	SN	
7	Contact (renseignement concernant le service d'horodatage) dans le PDF signature dictionary	J	SN	
8	Subfilter	J	M	Valeur = «ETSI.RFC3161»

Tableau 6: Synthèse des recommandations concernant les attributs qui peuvent être ajoutés à la signature CMS.

Légende

A = Alternative
B = disponible dans certaines conditions
Rem = Remarque
M = MUST
N = Non
SN = SHOULD NOT
1) Dans le cas où les certificats pour la vérification des signatures n'ont pas déjà été joints aux signatures correspondantes, ils doivent être inclus ici. Il convient de veiller à ce que les certificats n'apparaissent pas à deux reprises. Le certificat pour la vérification de la signature doit toutefois être joint à la signature via l'attribut «certificate-values», mais pas la chaîne de certificats CA.

5.3 Signature avec XML

Ce sous-chapitre n'est pas normatif.

5.3.1 Signature d'objets XML dans XFA intégré dans un PDF

Les règles de eCH-0230 peuvent en principe être appliquées. Il est à noter toutefois que: l'ajout des éléments XML correspondants peut avoir pour effet d'invalider les signatures PDF préalablement apposées. Cela signifie que dès que l'on insère une signature PDF ou un HDD, les objets XML saisis par la signature devraient rester inchangés.

5.3.2 Signature PDF via le XFA intégré au PDF

Le tableau suivant présente les attributs pour une signature XML pour lesquels existe une recommandation différente de eCH-0230. La raison en est que la LTV des signatures XML doit être atteinte

dans le cas présent au moyen du HDD.

N°	Élément	Signé	Rec.	Rem
1	CompleteCertificateRefs	N	MN	
2	CompleteRevocationRefs	N	MN	
3	SigAndRefsTimeStamp	N	MN	1)
4	RefsOnlyTimeStamp element	N	MN	1)
5	RevocationValues	N	B	2)
6	ArchiveTimeStamp	N	MN	1)
7	TimeStampValidationData	N	MN	1)

Tableau 7: Synthèse des recommandations concernant les attributs qui peuvent être ajoutés à la signature XML concernant un XFA (intégré dans un PDF).

Légende

B = disponible dans certaines conditions
Rem = Remarque
M = MUST
MN = Must NOT
N = Non
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.
1) La solution au problème réside dans l'horodatage du document.
2) Les informations concernant la révocation des signatures dont la validité doit être préservée par l'horodatage à réaliser doivent être jointes immédiatement avant le premier horodatage du document.

6 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 valide 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. .

7 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.

8 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/Paper

[1]	Andreas Bertsch, Digitale Signaturen, Springer Verlag, 2001
[2]	Digital Signatures Workflow Guide, A guide for workflow owners, 28.9.2012
[3]	Jens Müller et al, Ruhr University, Dangerous Paths, on Security and Privacy of the Portable Document Format, 2021
[4]	Karsten Meyer, Security of PDF Signatures, Master Thesis, Ruhr University, 2018
[5]	Trechsel/Pieth, Schweizerisches Strafgesetzbuch, 2. Auflage, Dike Verlag, 2013
[6]	Management Summary zur KOST-Studie: PDF/A-2 et PDF/A-3: Was ist neu?, https://kost-ceco.ch/cms/dl/9f3da1f53a75e54c2323a1bb6947fc2a/Summary_PDFA-2_PDFA-3_v1.0.pdf
[7]	Isaak Meier, Schweizerische Zivilprozessordnung, Schulthess Verlag, 2010

Adobe (www.adobe.com)

Adobe ® XFA: XML Forms Architecture (XFA) Specification version 2.5, (June 2007), Adobe Systems Incorporated

ISO 32000-1: Document management - Portable document format - Part 1: PDF 1.7. Remarque: Peut être obtenu gratuitement sur Internet.

eCH (www.ech.ch)

eCH-0091	Norme de signature XML et chiffrement
eCH-0220	Préservation de la validité des signatures électroniques au format CMS
eCH-0230	Préservation de la validité des signatures XML

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 319 132-1 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 EN 319 142-1	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
ETSI EN 319 142-2	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles
ETSI EN 319 422 V1.1.1	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

ETSI TS 101 903 V1.4.2	Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)
ETSI TS 102 778-1 à -5	Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1 to 5
ETSI TS 119 102-1 V1.2.1	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation (2018-08)

ISO (www.iso.org)

ISO 19005-1	ISO 19005-1 (2005): Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1).
ISO 19005-2	ISO 19005-2 2011 Document management — Electronic document file format for long-term preservation — Part 2: Use of ISO 32000-1 (PDF/A-2)
ISO 19005-4	ISO 19005-4 2020, Document management — Electronic document file format for long-term preservation — Part 4: Use of ISO 32000-2 (PDF/A-4)
ISO 32000-1	Document management - Portable document format - Part 1: PDF 1.7. Remarque: Peut être obtenu gratuitement sur Internet.
ISO 32000-2	Document management - Portable document format - Part 2: PDF 2.0

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

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

CP: Code pénal suisse du 21 décembre 1937, RS 311.0, en vigueur depuis le 1er janvier 1942

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

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

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)

CPC: Code de procédure civile du 19 décembre 2008 (RS 272)

Annexe B – Collaboration & vérification

Amrhyn Peter	Swisscom AG
Röthlisberger Claire	CECO

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.
Art.	Article
ASN.1	Abstract Syntax Notation One
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.
Let.	Lettre
CA	Certification Authority
CAdES	CMS Advanced Electronic Signature
CMS	Cryptographic Message Syntax, voir RFC 5652
CRL	Certificate Revocation List
CSP	Certification Service Provider
DSS	Document Security Store
HDD	Horodatage de document
eIDAS	electronic Identification, Authentication and trust Services, EU Regulation 910/2014 of 23 July 2014

Al.	Alinéa
ETSI	European Telecommunications Standards Institute
Olico	Ordonnance concernant la tenue et la conservation des livres de comptes du 24 avril 2002 (au 1er janvier 2013), RS 221.431
OGéo	Ordonnance sur la géoinformation du 21 mai 2008, 510.620
IETF	Internet Engineering Task Force
ISO	International Standardisation Organisation
LTV	Long Term Validation
OCSP	Online Certificate Status Protocol, voir RFC 6960
OID	Object Identifier
CO	Loi fédérale complétant le Code civil suisse (livre cinquième: droit des obligations) du 30 mars 1911 RS 220
PAdES	PDF Advanced Electronic Signature
Pdf	Portable Document Format
POE	Proof of Existence
RFC	Request for Comments (norme IETF)
SAML	Security Assertion Markup Language
RS	Numéro du recueil systématique du droit
RS	Recueil systématique du droit fédéral suisse
CP	Code pénal suisse du 21 décembre 1937, RS 311.0, en vigueur depuis le 1er janvier 1942
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
TSP	Trusted Service Provider
not.	notamment
LIDE	Loi fédérale sur le numéro d'identification des entreprises du 18 juin 2010, RS 431.03
UR	usage rights signature
URL	Uniform Resource Locator
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
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
XFA	XML Forms Architecture
XML	Extended Markup Language

Al.	Alinéa
XML Signature Syntax	XML Signature Syntax and Processing Recommendation version 1.1, 11 avril 2013
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
Chiff.	Chiffre
CPC	Code de procédure civile du 19 décembre 2008 (RS 272)

Annexe D – Modifications par rapport à la version précédente

Il s'agit de la première version.

Annexe E – Liste des illustrations

Annexe F – Liste des tableaux