eCH-0091 – Norme de signature et de chiffrement XML

Nom	Norme de signature et de chiffrement XML
eCH- nombre	eCH-0091
Catégorie	Norme
Stade	Défini
Version	2.0.0
Statut	Approuvé
Date de décision	2021-03-02
Date de publication	2021-03-10
Remplace la version	1.0 – Major Change
Conditions préalables	-
Annexes	-
Langues	Allemand (original), français (traduction)
Auteurs	Groupe spécialisé SAGA Büchler Georg (KOST) Müller Adrian (SwissSign AG), Muster Daniel (it-rm IT Riskmanagement GmbH) Niederberger Marcel (ESTV) von Niederhäuser Michael (Bit) Rötzer Hubert Schmid Josef Waldegger Hans-Peter (Swisscom) Groupe spécialisé XML version 1 Daniel Muster (Initiant dieses Themas) Willy Müller Claude Eisenhut, Eisenhut Informatik Alexander Pina, Unisys Schweiz AG Eric Dubuis, Berner Fachhochschule Gilles Maitre Stephan Fischli, Berner Fachhochschule
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

Les objets XML peuvent être protégés par diverses méthodes (signatures, chiffrements) spécialement normalisées pour XML. Les problèmes apparaissent notamment lorsqu'il faut également protéger des documents entiers contenant des renvois vers des images, schémas ou autres informations sur la mise en page (layout), contenus dans ces documents.

Le présent document s'emploie d'une part à mettre en évidence les problèmes et à proposer des solutions puis, d'autre part, à adapter les normes XML existantes aux circonstances propres à la cyberadministration en Suisse. C'est la protection des documents administratifs basés sur XML qui est ici au cœur des préoccupations.

Sommaire

Remarque

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

1 Introduction

1.1 Statut

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

1.2 But du document

Le présent document alerte sur les problèmes (de sécurité) susceptibles de survenir lors du chiffrement et de la signature de documents et objets XML, et propose des solutions visant à résoudre ces problèmes, se concentrant ce faisant sur le cas des documents administratifs XML.

La particularité des documents administratifs est de pouvoir et devoir être considérés comme détachés de toute communication ou tout échange de données; et ce, à l'inverse d'une annonce SOAP ou SAML par exemple. Il s'agit là d'une application XML parmi tant d'autres.

La signature et le chiffrement de documents administratifs XML et d'objets XML consistent à les signer et à les chiffrer dans leur intégralité (ce qui signifie en incluant toutes les informations pertinentes pour la sécurité), puis à les déchiffrer et à les reconstituer de manière à ce que les composants de la signature demeurent inchangés et que la signature reste valide et contrôlable dans un délai prévu.

Les chapitres qui suivent mettent l'accent sur les documents administratifs XML, avec des préconisations pour les applications XML dans la communication de données:

- Chapitre 2 «Explication de la problématique»
- Chapitre 3 « Risques et mesures »
- Chapitre 4 «Précision des normes existantes»
- Chapitre 5 «Alternatives»
- Annexe A «Vue d'ensemble constitution de signature XML»

1.3 Terminologie des recommandations

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

- **MUST:** This word, or the terms «REQUIRED» or «SHALL», mean that the definition is an absolute requirement of the specification.
- **MUST NOT**: This phrase, or the phrase «SHALL NOT» mean that that definition is an absolute prohibition of the specification.
- **SHOULD:** This word, or the adjective «RECOMMENDED», mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**: This phrase, or the phrase «NOT RECOMMENDED» mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY**: This word, or the adjective «OPTIONAL», means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

> An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

1.4 Sélection des normes

Les normes européennes font autorité dans l'environnement du prestataire de services de certification reconnu selon la SCSE. Il n'existe toutefois aucune norme ETSI qui couvre le présent cas de figure. Les recommandations exposées dans ces pages sont par conséquent basées sur les normes du W3C en matière de signature et de chiffrement XML. Concernant la validité à long terme des signatures électroniques XML, des normes XML correspondantes (série XAeDS) ont été élaborées et publiées par l'ETSI, les normes W3C mentionnées servant de base aux explications complémentaires relatives à la validité à long terme des signatures XML dans les normes ETSI évoquées.

2 Explication de la problématique

La norme [CWA 14170] resp. [CWA 14171] expose les risques survenant lors de la création resp. de la vérification d'une signature électronique et les mesures de sécurité pouvant / devant être mises en œuvre à cet égard. Le format de signature de base n'est pas pris en compte à cet égard. Concernant les formats de signature spécifiques tels que CMS ou XML, les normes correspondantes de l'ETSI, TS 119 102-1 V1.2.1 par exemple, devraient être consultées en priorité.

A contrario des normes CWA précédemment évoquées, le présent document se cantonne notamment à l'aspect suivant:

> «What you see is what you will sign or what you verify is what you see.» Une règle qui vaut aussi uniquement dans le contexte des objets XML. Les sous-chapitres qui suivent reviennent de façon succincte sur ce qu'il faut précisément y entendre.

Contrairement aux normes précédemment évoquées, les problèmes de chiffrement des documents XML sont pour leur part explicités ici, en particulier le chiffrement des documents et objets XML signés.

2.1 Problèmes concernant la signature XML

Le problème avec la signature XML est que la signature, le cas échéant, couvre uniquement l'objet principal, et pas l'intégralité du document, en particulier les sous-objets tels que schémas, CSS File ou images éventuellement contenus. Il est alors possible de modifier l'apparence (présentation) du document sans que la signature sous l'objet principal ne perde sa validité, en modifiant ou en substituant des sous-objets par exemple. Une situation à l'origine de vulnérabilités majeures au niveau de la sécurité.

Scénario d'une attaque possible: Carl crée un document avec l'objet principal A, au format XML ou HTML par exemple. Dans un sous-objet L (un fichier CSS par exemple), il définit la façon dont les polices (contenu de l'objet) doivent être affichées à l'écran. L'objet principal A et le sous-objet L sont liés par un renvoi interne dans l'objet principal A.

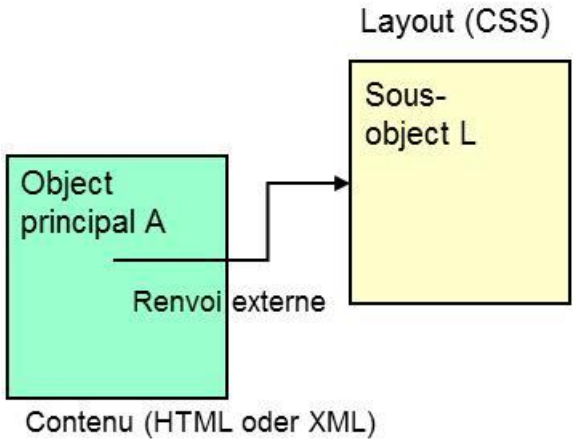


Figure 1 Séparation du contenu et de la mise en page pour un document

Carl a défini les informations de mise en page (layout) dans le sous-objet L (au format CSS par exemple) de sorte que certains passages s'affichent en texte blanc sur fond blanc. Il soumet à Alice le document avec les informations de mise en page L . De son côté, Alice se contente de signer l'objet principal A, mais pas le sous-objet L (le fichier CSS dans ce cas précis) et renvoie à Carl l'objet principal A signé.

Carl convertit le sous-objet L en L', de sorte que les passages de texte et les mots blancs s'affichent à présent à l'écran avec une police noire sur fond blanc. Il est ainsi en mesure de présenter un «document» qui lui convient et qui est signé par Alice, mais que cette dernière n'a pas pu voir sous cette forme. Une situation rendue possible uniquement parce que la signature est limitée au seul objet principal, pas aux sous-objets afférents.

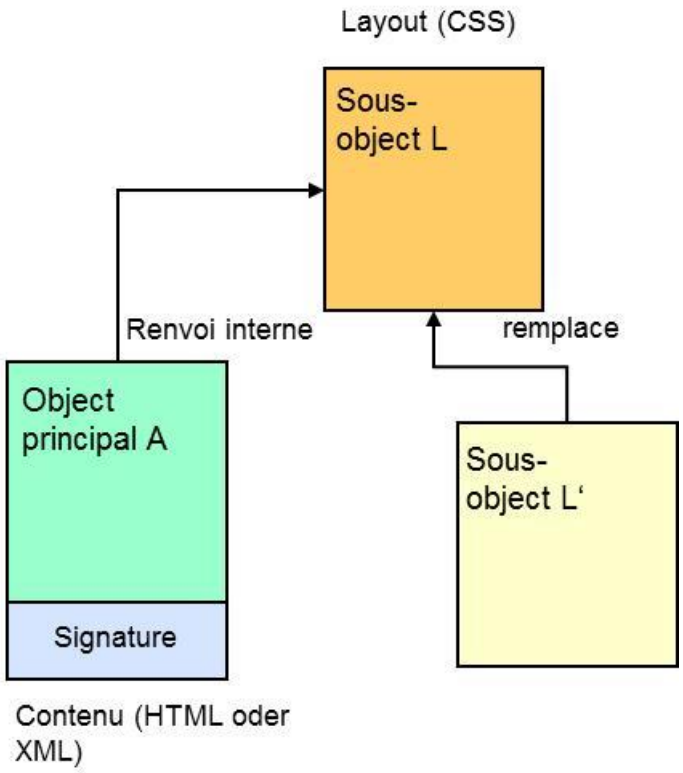


Figure 2 Substitution de contenus, la signature reste bien valide

Dans le cas de documents signés, la présentation ou l'apparence ne doit pas changer sans que cela rende la signature non valide.

Le moment de la signature du document varie en fonction des exigences de sécurité concernées en matière d'authenticité, d'intégrité, de nature contraignante et de traçabilité. Le présent document se garde toutefois de préciser les exigences de sécurité applicables et, par conséquent, le moment où un document doit être signé.

Il existe par exemple d'autres scénarios ou processus qui exigent une signature du document complet, et pas uniquement de l'objet principal, et une présentation complète du document signé.

Le scénario précédemment dépeint, évoquant un emploi abusif de la signature électronique, suggère que la démarche est intentionnelle. Il a été exposé ici afin d'illustrer et de mieux faire comprendre le problème à traiter. Le fait que certains passages du document soient échangés, modifiés ou supprimés et ne puissent donc plus être correctement reconstitués ni vérifiés comme prévu peut également être imputable à de la négligence et à de l'imprudence.

2.2 Problèmes lors du chiffrement

Des problèmes apparaissent avec le chiffrement XML d'un document (administratif) en XML selon la norme W3: Soit que des parties (sous-objets) du document ne sont pas présentes, soit des sous-objets du document, tels que des images, sont transmis involontairement sous forme de texte clair. Le document entier avec tous ses sous-objets devrait être chiffré afin d'empêcher, d'une part, que les contenus sensibles dans les sous-objets soient disponibles en texte clair et puissent être visualisés, et, d'autre part, de permettre de tirer des conclusions quant aux contenus sensibles des objets chiffrés à partir des sous-objets non chiffrés.

2.3 Modèle

À la différence des deux normes [CWA 14170] et [CWA 14171], le modèle présenté ici pour la constitution et la vérification de la signature est nettement plus simple, car seul un aspect plus restreint doit y être traité.

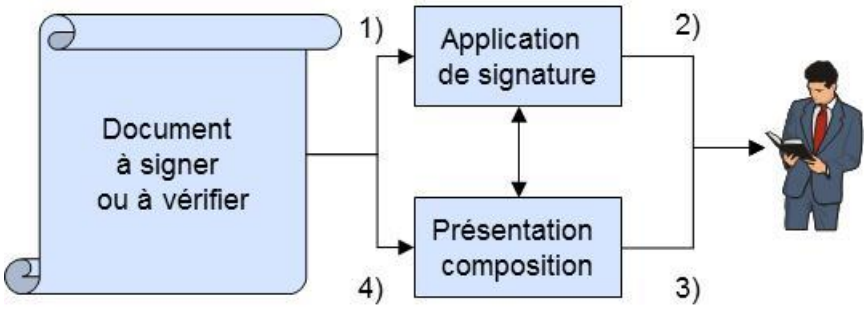


Figure 3 Modèle pour la création et la vérification de la signature

L'application de signature vérifie et signe (1) les objets et met le résultat à la disposition de l'utilisateur (2). La reconstruction ou la composition reconstitue le document qui doit être signé ou vérifié (4) par l'utilisateur (3). Remarque: La reconstruction et l'affichage du document peuvent toutefois faire également partie de l'application de signature. Dans le cas contraire, la composition est lancée par l'application de signature et le document correspondant à signer est alors affiché.

Le document lui-même peut être constitué de, outre l'objet principal, plusieurs sous-objets tels que

- Images
- Schéma
- Code référencé (indirectement)
- Instructions pour transformer le document
- Instructions de formatage
- Autres objets XML ou composants de ces derniers

De la façon dont la société de communication définit au préalable ces points précis dépend en grande partie de ce que la composition doit faire, comment et ce qui doit être présenté. Mais pour que le document complet soit réellement protégé par la signature de l'utilisateur, il faut a minima que tout ce qui importe pour la composition et la présentation correctes du document soit signé.

La manière dont un document est reconstitué et, surtout, la façon dont le document est présenté correctement ou protégé n'entrent toutefois pas dans le périmètre couvert par ce document eCH. Le présent document eCH vise simplement à apporter des compléments et à formuler des préconisations sur la manière dont l'ensemble du document XML peut être signé avec une signature XML et intégralement protégé en termes de confidentialité.

3 Risques et mesures

Les cas d'application pour les risques examinés ici sont répartis entre

- Signature XML
- Chiffrement XML
- Signature XML avec chiffrement XML

Dans les cas évoqués, on établit une distinction selon qu'un document est traité de manière entièrement automatisée ou que l'apposition de la signature électronique ou le chiffrage est initié par un utilisateur.

3.1 Informations liminaires concernant la signature XML

La norme relative à la signature XML «W3C-Sig» autorise les 3 types de signatures XML suivants:

- **Detached:** La signature pointe soit vers un élément XML hors de la hiérarchie XML, dans laquelle l'élément de signature XML est intégré, soit vers un fichier externe quelconque pouvant être référencé à l'aide d'un URI (selon cette procédure, la référence de signature pointe vers un élément XML ne se trouvant pas le long du chemin de l'élément de signature vers la racine du document).

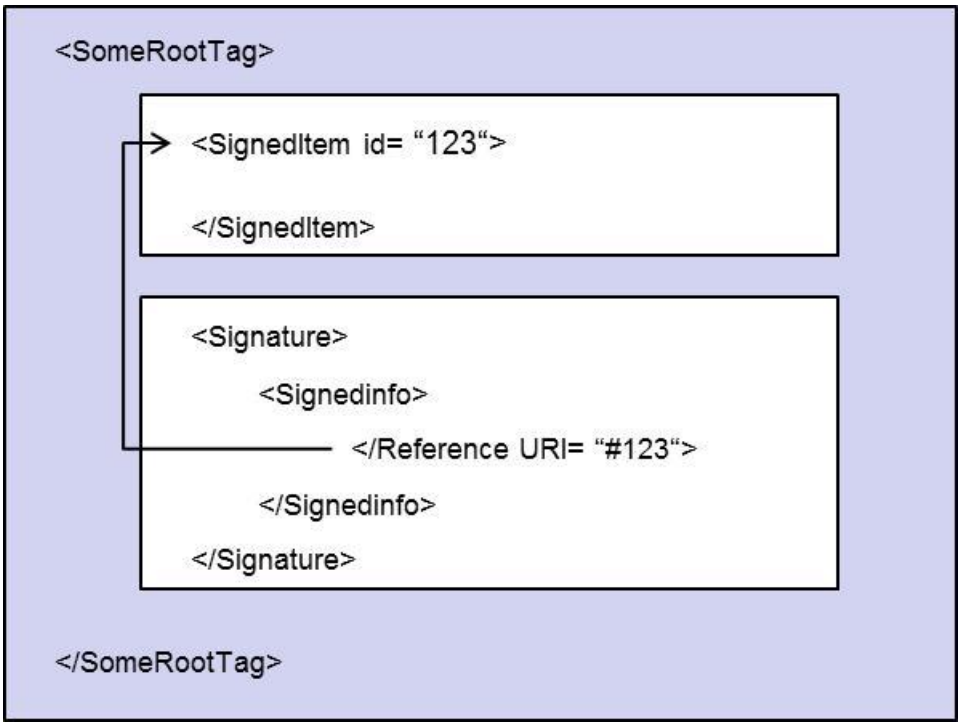


Figure 4 Detached Signature (première forme)

Cette procédure permet également que la référence de la signature pointe vers une ressource située hors du document XML.

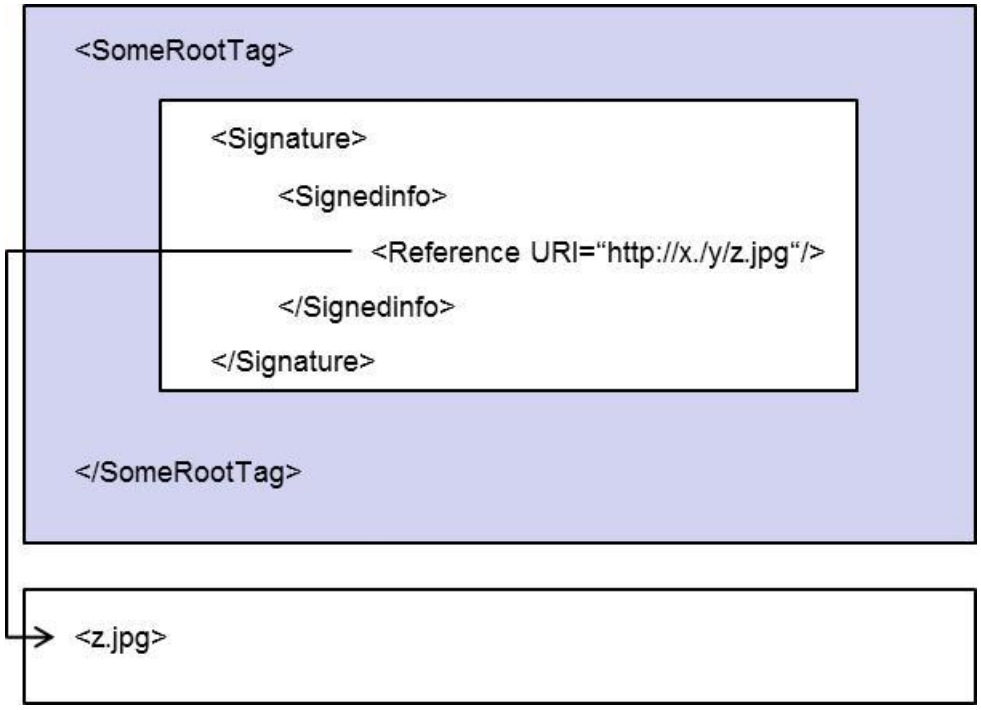


Figure 5 Detached Signature (deuxième forme)

- **Enveloped:** La signature pointe vers un élément parent dans la hiérarchie XML dans laquelle est intégré l'élément de signature XML (dans cette procédure, la référence de la signature pointe vers un élément XML parent de la signature).

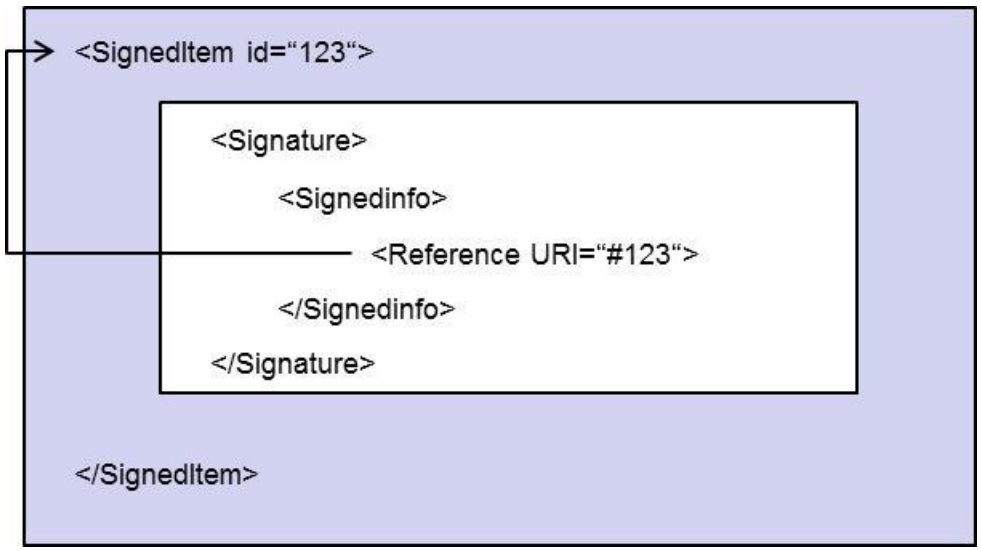


Figure 6 Enveloped Signature

- **Enveloping:** La signature contient l'information qui a été signée en tant qu'élément enfant de l'élément de signature XML (dans cette procédure, l'information à signer est enveloppée dans la signature).

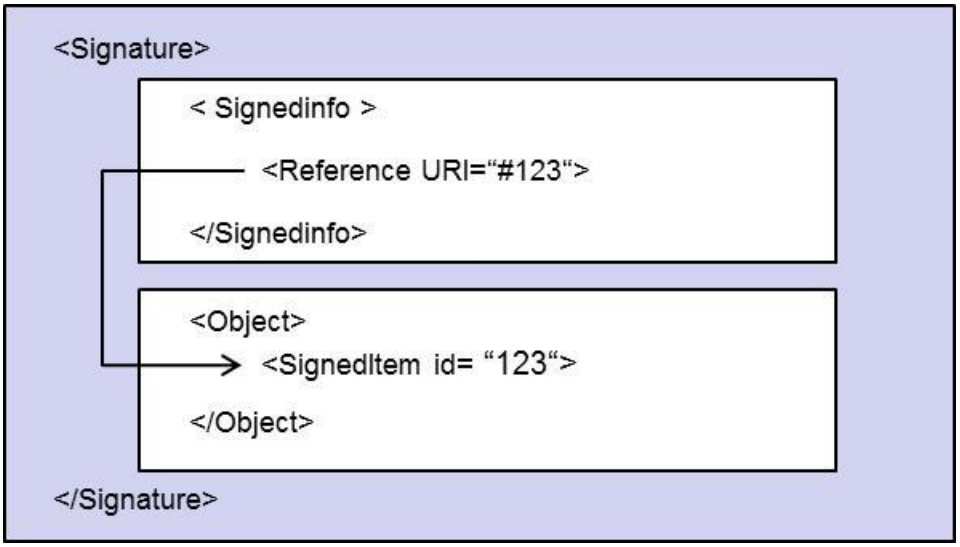


Figure 7 Enveloping Signature

Une signature XML peut être une combinaison de detached, enveloped et aussi enveloping.

La norme W3C sur le chiffrement XML autorise les 3 types de chiffrement XML suivants:

- le chiffrement du contenu d'un élément XML
- le chiffrement d'un élément XML et de son contenu
- le chiffrement de n'importe quel objet pouvant également avoir des éléments XML.

3.2 Risques

Les risques autres que ceux énumérés ici ne manquent pas dans le contexte du chiffrement et de la signature. Les mesures à prendre pour y parvenir n'entrent toutefois pas dans le cadre couvert par le présent document.

Signature

Lors de la création de la signature, il existe un risque que les objets pertinents pour la sécurité (du document) ne soient pas tous signés. Ainsi, seul l'objet principal est signé, pas les objets sur lesquels porte un renvoi en interne par exemple. Les parties sensibles (sous-objets) du document et donc, éventuellement, son apparence peuvent ainsi être modifiées sans que la signature sous le document supposé perde sa validité.

Chiffrement

Concernant le chiffrement, il existe un risque que tous les objets du document devant être protégés ne soient pas chiffrés. Ainsi, seul l'objet principal est chiffré, pas les sous-objets sur lesquels porte un renvoi en interne par exemple. Les informations sensibles contenues dans les sous-objets peuvent être divulguées de façon involontaire et, le cas échéant, permettre de tirer des conclusions quant à l'objet chiffré à partir des sous-objets non chiffrés.

3.3 Signature

Remarque concernant le tableau suivant: les possibilités de voir les risques mentionnés au chapitre 4.2.1 survenir sont répertoriées dans les cas d'application.

3.3.1 Signature de l'utilisateur déclenché

No	Cas d'application	Mesure	Remarque
1	**Envoi de documents signés**. Le document n'est pas signé dans son intégralité, mais seulement en partie ou uniquement l'objet principal. Les éléments essentiels du document, tels que les sous-objets sur lesquels porte un renvoi en interne, peuvent être échangés sans que la signature perde sa validité.	**MUST:** Au minimum, tous les objets sur lesquels porte un renvoi en interne doivent faire partie de la signature (couverts par la signature).	Concernant le traitement des renvois, voir également le chapitre 4.1.3 « Traitement des renvois internes »

No	Cas d'application	Mesure	Remarque
2	**Remplissage d'un formulaire via une connexion en ligne.** Un formulaire est rempli en ligne sur l'écran. Les renseignements qui y sont indiqués sont signés puis transmis en ligne au serveur en vue d'un traitement ultérieur. L'utilisateur est alors confronté à un double problème: il ne peut pas pleinement reconnaître ce qu'il signe et, dans certaines circonstances, il ne peut pas archiver ce qu'il a signé.	Les alternatives disponibles sont les suivantes: 1. **MUST:** Tous les objets sur lesquels porte un renvoi en interne doivent faire partie de la signature (couverts par la signature). 2. **MUST:** Le document XML doit être intégralement converti en un objet PDF/A-1 ou PDFA/A-2. Cet objet doit ensuite être signé par l'utilisateur selon le RFC 5652. Les deux formats de fichier sont prescrits par l'OAAE dans le cadre de l'authentification des actes publics.	Concernant le traitement des renvois, voir également le chapitre 4.1.3 « Traitement des renvois internes »

No	Cas d'application	Mesure	Remarque
3	**Envoi de documents signés avec le code de programme**. En XML, mais plus particulièrement dans les documents dont l'objet principal est en HTML, un code exécutable tel ActiveX, JavaScript ou des applets Java peuvent être inclus. Les paramètres et ainsi l'apparence du document peuvent y être modifiés sans que la validité de la signature change.	**MUST:** Avant la signature, l'application de sécurité doit émettre une mise en garde alertant sur la présence d'un code de programme dans le document administratif. **SHOULD NOT:** Un document administratif ne devrait pas contenir le moindre code exécutable. Lorsqu'un document contient du code, il doit être exclu de la signature. Un document incluant un tel contenu ne devrait pas être signé par l'utilisateur.	**Remarque:** Le cas décrit ici est à distinguer de l'application «Code Signing». Code Signing doit permettre d'attester de l'origine du programme en signant le programme lui-même. Ici, on cherche cependant à éviter que des modifications involontaires puissent être apportées au document (administratif), la signature sous le document gardant sa validité même une fois les modifications effectuées. Voir aussi le chapitre 4.1.2 « Programmes contenus dans le document »

3.3.2 Processus entièrement automatisé

	Cas d'application	Mesure	Remarque
1	**Authenticité des documents**	**MUST:** Les informations pertinentes pour l'authenticité et l'intégrité doivent être signées, soit également tous les objets sur lesquels porte un renvoi en interne.	Dans le cas de processus entièrement automatisés, des procédures autres qu'une signature peuvent être utilisées afin de protéger l'authenticité des documents XML, que dans le cas de processus initiés par l'utilisateur ou destinés à un utilisateur, voir à ce sujet le chapitre 4.2.7.3 « HMAC ».

	Cas d'application	Mesure	Remarque
2	**Interaction entre l'application XML et la vérification de la signature XML.** La flexibilité inhérente au format XML permet d'insérer la signature à un endroit différent dans l'objet principal. La signature ne peut/doit toutefois pas perdre sa validité. Dans le cas de signatures XML créées et vérifiées automatiquement, comme pour SAML ou SOAP par exemple, il existe alors un risque que les éléments couverts par la signature ne soient pas transmis à l'application. En conséquence de quoi, l'application accepte par inadvertance des composants que la signature ne protège pas. Une attaque est appelée «XML Wrapping» lorsque l'application est délibérément amenée - contrairement à ce qui était prévu - à recevoir, accepter et traiter des composants non couverts par la signature. Voir à ce sujet les documents suivants [McAu], [Soetal] par exemple.	**MUST:** Le schéma XML doit être vérifié. Il s'agit de vérifier, entre autres choses, que la signature XML, au même titre que les objets à signer, se trouve bien à l'endroit prévu par le schéma. Le schéma à utiliser doit être conservé en lieu sûr, c'est-à-dire à l'abri de toute modification ou remplacement. **SHOULD:** Le schéma, ou mieux encore la valeur hash de celui-ci, devrait faire partie de la signature. **MUST:** À supposer que l'application doive traiter des informations pertinentes pour la sécurité et couvertes par la signature. L'application de sécurité doit ensuite vérifier que cette information a bien été saisie par la signature. Et ce, avant qu'elle transmette ces informations à l'application. **SHOULD:** Ce qui doit être signé dans l'objet principal devrait être référencé au moyen d'un chemin XPATH absolu. Seules les expressions de la version 1.0 sans fonctions ni opérateurs devraient être utilisées pour la référence.	

	Cas d'application	Mesure	Remarque
3	**Attaques de type Denial of Service.** Le chapitre 2.1 XML Signature Best Practices répertorie toute une série d'attaques de type Denial of Services avec des signatures XML.	**SHOULD:** Les mesures, qui y sont énumérées, devraient être suivies dès lors que des faiblesses correspondantes sont constatées.	

3.4 Chiffrement XML

Remarque concernant le tableau suivant: les possibilités de voir les risques mentionnés au chapitre 4.2.2 survenir sont répertoriées dans les cas d'application.

3.4.1 Le chiffrement est déclenché par l'utilisateur

No	Cas d'application	Mesure	Remarque
1	**Chiffrement des documents XML**. Ce n'est pas tout le document qui est chiffré, mais seulement des parties de celui-ci ou uniquement l'objet principal. En conséquence de quoi, certaines parties du document sont transmises en texte clair. Il devient alors possible de tirer des conclusions quant aux objets chiffrés.	**MUST:** Tous les objets sensibles sur lesquels porte un renvoi en interne doivent être chiffrés avec l'objet principal.	
2	**Remplissage d'un formulaire via une connexion en ligne chiffrée.**	**MUST:** Il faut faire bien attention à ce que tous les objets du formulaire et tous les renseignements fournis soient chiffrés.	Le problème est que les objets du document ne sont pas tous transmis chiffrés, par exemple via la connexion TLS, mais échangés via une connexion HTTP distincte non chiffrée.

3.4.2 Chiffrement entièrement automatisé des documents XML

No	Cas d'application	Mesure	Remarque
1	**Échange de documents XML chiffrés**.	Deux mesures équivalentes sont disponibles: 1. **MUST:** Tous les objets appartenant au document, sur lesquels porte un renvoi en interne, doivent être chiffrés. 2. **MUST:** L'échange, la connexion servant à la communication par exemple, doit être chiffré. Tous les objets sur lesquels porte un renvoi en interne doivent également être acheminés sous forme chiffrée.	Dans le cas d'un échange de données automatisé, il n'est pas nécessaire d'inclure à chaque fois toutes les informations relatives au document, comme les schémas par exemple.
2	**Concernant les documents automatiquement chiffrés** Dès lors que le schéma d'un objet XML chiffré est connu, il est possible de tirer des conclusions quant au texte clair de l'objet chiffré.	**SHOULD:** Le schéma relatif à un objet chiffré devrait être traité de façon confidentielle.	

3.5 Signature avec chiffrement

On part du principe que si le document est chiffré, ce n'est pas le cas de la connexion servant à la communication. Il faudrait en outre préciser si le document doit d'abord être signé puis chiffré ou inversement.

No	Cas d'application	Mesure	Remarque
1	**Échange de documents XML chiffrés et préalablement signés**. L'utilisation de Detached Signature, qui n'est pas chiffrée, permet notamment une attaque de type Brute Force accélérée, car il est possible d'effectuer un contrôle de plausibilité accéléré pour une clé de déchiffrement candidate.	**SHOULD:** On devrait également chiffrer la Detached Signature lorsque le document non chiffré ou l'objet afférent fait partie de la signature et est chiffré.	
2	**Échange d'objets XML (automatiquement) chiffrés et préalablement signés.** S'il existe une valeur hash d'un composant à chiffrer, et que celle-ci n'est pas également chiffrée, cela permet un contrôle de plausibilité accéléré d'une possible clé de déchiffrement.	**SHOULD:** Les valeurs hash correspondant aux objets à chiffrer devraient également être chiffrées, sous réserve que la valeur hash repose sur le texte clair de l'objet à chiffrer. Si ces valeurs hash font partie de l'objet de signature à chiffrer, ces valeurs devraient elles aussi être chiffrées.	Voir W3C XML Signature Best Practices

No	Cas d'application	Mesure	Remarque
3	**Échange de documents XML chiffrés et signés a posteriori.** Lorsque le chiffrement précède la signature, l'on pense savoir d'où provient l'annonce et qu'aucune modification (lors de l'acheminement) n'y a été apportée. Toute modification serait immédiatement repérée, car la valeur de la fonction hash diffère. Mais si, a contrario, la signature précède le chiffrement, l'on peut par exemple attester de ce qui a été signé. L'annonce peut en outre être enregistrée et conservée non chiffrée, mais signée par les deux parties. À la réception des documents, toutefois, aucune présélection (spam par exemple) ne peut être effectuée avant le déchiffrement, car on ignore qui est l'expéditeur du document. Par exemple, des éléments sans intérêt (publicité par exemple) peuvent avoir été chiffrés pour le destinataire (le fait qu'une annonce ait été chiffrée ne signifie pas, tant s'en faut, que cette même annonce contient des informations confidentielles.)	**MUST:** Pour des raisons d'archivage, la création de la signature contraignante doit être antérieure au chiffrement pour les documents (juridiquement) contraignants (une telle signature constitue alors une forme authentique). **SHOULD:** Le document devrait d'abord être signé, puis chiffré et à nouveau signé. **SHOULD NOT:** Lorsqu'un objet chiffré est signé, il devrait être possible de vérifier la signature avec un certificat régi selon la SCSE. **MUST:** L'utilisation doit permettre de constater qu'une telle signature ne garantit pas le contenu (Content) des informations chiffrées, mais simplement l'authenticité et l'intégrité lors de l'envoi (à l'instar d'un horodatage ou d'un accusé de réception) **Remarque:** La SCSE réglemente la création de certificats avec les signatures correspondantes, les autres lois l'utilisation de la signature.	Une signature réglementée induit une implication juridique couverte par la loi. Il est donc généralement nécessaire, si ce n'est obligatoire, de conserver ce qui a été signé en conséquence et d'en permettre la lecture ultérieure à des tiers autorisés. Dans certaines circonstances, cette possibilité peut ne plus exister, dès lors que le fichier a été chiffré. La signature après le chiffrement est destinée uniquement à protéger l'authenticité et l'intégrité, pas à certifier le texte clair existant. Par conséquent, cette signature doit être vérifiée au moyen d'un certificat dépourvu de Content Commitment.

4 Précision des normes existantes

Le présent chapitre fournit des renseignements complémentaires relatifs aux différentes mesures de la signature XML et du chiffrement XML. Il repose, pour ce faire, sur les normes correspondantes de l'IETF et du W3C. Ces normes doivent par principe être considérées comme contraignantes. Il n'empêche que certains aspects techniques des normes sont complétés ici et, si nécessaire, adaptés aux spécificités suisses, en d'autres termes une recommandation différente des normes est émise le cas échéant.

Les renseignements ne sont fournis à ce stade que lorsque l'avis du GS ne coïncide pas avec les normes ou lorsque la norme a insuffisamment défini, voire pas défini du tout un point particulier.

Important: concernant la sécurité informatique des données d'application, la sécurité ne peut être dissociée de l'application, voir également les chapitres 3 et 4 [SOAP Security with Attachements]. C'est également ce qui ressort des explications suivantes.

Les sous-chapitres suivants sont classés selon le processus décrit ci-dessous sur la façon de protéger les fichiers et objets XML:

- le cas échéant, le document est préalablement traité avant que des signatures y soient apposées. Se reporter au chapitre 5.1 pour savoir pourquoi cela est nécessaire.
- Le document est signé, si nécessaire.
- Le cas échéant, le document est ensuite chiffré.
- Le cas échéant, le document chiffré est signé.
- Le document est remis au destinataire.
- La signature liée au document est vérifiée.
- Le document est déchiffré.
- La signature sous le document est vérifiée.
- Le document est reconstitué séparément.

La manière dont se déroulent les différentes étapes ci-dessus est décrite dans les normes RFC et W3C correspondantes.

4.1 Prétraitement du document

4.1.1 Séparation du document

Il convient, dans la mesure du possible, d'éviter l'imbrication des signatures au sein d'un même document.

SHOULD: Dans la mesure du possible, les objets à signer doivent être séparés, ce qui signifie décomposés en sous-objets, afin d'éviter toute imbrication des signatures. Il est à noter à cet égard que le document est déjà disponible sous une forme normalisée selon le format XML.

Motif: Les signatures imbriquées compliquent la vérification et l'archivage des documents signés électroniquement.

4.1.2 Programmes contenus dans le document

Ici, on cherche à éviter que des modifications puissent être apportées au document, sans que la si-

gnature sous le document conserve sa validité même une fois les modifications effectuées. Une signature protège le document tant dans son origine que son intégrité.

SHOULD: Les documents (administratifs) à signer devraient être conçus de telle manière que, dans le contexte ou l'application concernés, ils ne contiennent ni ne fassent référence à aucun programme (macros, etc.) exécuté lorsque le document administratif est présenté.

Dans le contexte correspondant, il faut vérifier le contenu du programme dans les documents XML. Ce contrôle doit être vérifié au moyen de programmes ayant été certifiés pour l'application correspondante. Toutefois, pour qu'un tel contrôle soit judicieux, encore faut-il élaborer une description avec un schéma correspondant pour l'application.

Dans l'éventualité où le document contiendrait de tels programmes, un message d'alerte en ce sens devrait être affiché pour l'utilisateur dans le cas de processus pas entièrement automatisés.

SHOULD NOT: Si le document contient des programmes, aucune signature ne devrait être créée et le processus de création de signatures devrait être interrompu.

Motif: Les programmes contenus dans le document peuvent le modifier de sorte que sa présentation une fois signé diffère de son apparence au moment de la vérification de la signature, alors même que la signature conserve sa validité.

4.1.3 Traitement des renvois internes

Le but recherché est que le document signé puisse être reconstitué à partir de ses composants (objets) en différents endroits et à différents moments.

MUST: Avant d'engager le processus de signature, il faut faire attention à ce que tous les renvois internes présents dans le document soient répertoriés de manière non pas absolue, mais bien relative.

Motif: C'est là la seule façon pour le destinataire de reconstituer le document tel qu'il a été signé sans rien y changer. Ainsi lorsqu'un renvoi interne est par exemple répertorié de manière absolue et pointe vers un répertoire chez l'expéditeur, il en résulte les inconvénients suivants:

- le destinataire ne peut reconstituer ni faire présenter le document tel que signé, car peut-être ne dispose-t-il pas des autorisations relatives à l'endroit où a été conservé l'objet sur lequel porte le renvoi.
- Dans le cas où l'accès aux objets sur lesquels porte le renvoi, l'objet sur lequel porte un renvoi peut alors être transmis en texte clair lorsque le document est présenté au destinataire.
- Le destinataire ne peut enregistrer le document dans son intégralité tel que signé et le reconstituer ultérieurement à partir des données ainsi sauvegardées sans rien changer au document. Les modifications apportées au document rendent toutefois la signature non valide.

4.2 Création de signatures

Le processus de création de signatures est décrit dans la norme W3C-Sig. Se reporter à l'annexe A pour voir une représentation graphique du processus en question.

4.2.1 Choix du type de signature

Comme chacun sait, il existe 3 types de signatures XML disponibles (Enveloped, Enveloping, Detached). On trouve également des formes hybrides entre les signatures Enveloping et Detached.

MUST: Le type Enveloping ou Detached doit être utilisé lors de la signature de plus d'un objet.

MUST NOT: Dans le cas où d'autres informations couvertes par la signature, telles que répertoriées par la norme ETSI EN 319 132-1 V1.1.1, sont ajoutées, l'utilisation d'une signature Enveloped ne doit

pas être autorisée.

4.2.2 Signature

Si seules des parties du document sont signées, les autres parties peuvent être remplacées sans que la signature perde sa validité et que la protection de l'intégrité en soit donc compromise.

MUST: La signature doit couvrir toutes les parties du document administratif pertinentes pour la sécurité.

Les objets XML, ou mieux leur valeur hash, peuvent être inclus à la signature au moyen de l'élément Manifest. Selon la norme, la signature peut cependant être aussi considérée comme valide lorsque les valeurs hash contenues dans le Manifest ne concordent plus avec les objets qui y sont référencés.

MUST NOT: L'élément Manifest ne doit pas être utilisé. Tout ce qui entre dans la signature doit alors pouvoir aussi être validé en conséquence.

4.2.3 Transformation des objets

La norme W3C-Sig décrit la transformation comme le traitement de l'objet avant que la valeur hash (Message Digest ou la somme de contrôle cryptographique) soit générée via l'objet transformé, voir également l'annexe A (représentation graphique simplifiée de la signature XML).

MUST: Une «canonicalization» des sous-objets XML et de l'objet principal XML doit être effectuée. Pour les données binaires (Binaries en anglais) externes, comme les images, il faut utiliser un encodage Base64.

MUST NOT: Pour des raisons de sécurité, tant la méthode XSLT que les autres procédures répertoriées dans la norme ne doivent pas être appliquées.

Remarque concernant les transformations: la distinction suivante doit être faite à propos des transformations:

1. les transformations définies comme l'encodage Base64, la «canonicalization» mentionnée dans la norme W3C-Sig.
2. les transformations dont le comportement peut être configuré dans le document
3. les transformations dont le comportement peut certes être configuré, mais la configuration est définie hors du contexte du document.

Les deux derniers types de transformation (2,3) posent un problème de sécurité pour la signature. En effet, le résultat de la transformation est difficile à contrôler et donc, tout vérification de signature est réussie en fonction du résultat. Exemple: on transforme chaque objet en un certain texte T. Une somme de contrôle est donc préparée pour ce texte T. Si l'on modifie l'objet XML, la signature conserve sa validité parce que cet objet aussi est transformé en texte T précédemment défini et la somme de contrôle en résultant reste intacte. L'utilisateur devrait donc voir ce qui est signé après la transformation, voir W3C-Sig chapitre 8.1.3.

Autre motif: Voir chapitre 8.1 de la norme [RFC 3275].

Le document [SOAP Security] d'OASIS, p. 36 Rz 1185 et suivantes recense les avantages et inconvénients, y compris et à l'exclusion de la «canonicalization». Pour simplifier, l'on peut dire qu'une «canonicalization» exclusive devrait être appliquée lorsque la signature devrait être sortie de son contexte tout en en préservant la validité. Si une signature peut être sortie de son contexte et conserver sa validité, il existe un risque d'attaques de type XML Wrapping

Cohérence et importance: concernant la spécification des éléments et de leurs attributs, **aucune**

spécification DTD ne peut être intégrée aux objets XML, sous peine de les détruire lors de la «canonicalization». À cette fin, il faut utiliser des schémas XML, faute de quoi ces renseignements concernant la structure ne seront pas intégrés à la signature XML et par conséquent, leur authenticité et leur intégrité ne sont pas protégées.

4.2.4 Remarque relative aux algorithmes cryptographiques

Les normes ENISA et BSI comportent des recommandations au sujet des procédures cryptographiques, ainsi que de leur longueur de clé. On y trouve les procédures préconisées tant par les normes mentionnées que par la W3C-Sig. En cas d'utilisation d'autres méthodes que la méthode standard W3C-Sig, il faut définir un URI approprié et en convenir.

4.2.5 Algorithmes pour les sommes de contrôle des objets

Les normes du W3C répertorient les algorithmes (fonctions hash) pour le Message Digest (somme de contrôle cryptographique). Celles qui doivent être utilisées sont précisées pour des raisons de sécurité.

Si le choix de la procédure de production de la somme de contrôle (au moyen d'un URI standardisé) doit être spécifié, les procédures de la norme W3C correspondante font autorité.

MUST: Seules les fonctions hash SHA-256, SHA-384, SHA-512 répertoriées dans le W3C doivent être utilisées.

SHOULD: Le même algorithme de somme de contrôle cryptographique (Message Digest en anglais) devrait être utilisé pour tous les documents à inclure dans la signature.

Motif: Pour simplifier, la création de somme de contrôle cryptographique utilisée pour constituer la signature est aussi forte que l'algorithme le plus faible utilisé pour créer le Message Digest.

4.2.6 «Canonicalization» des éléments de somme de contrôle

Les valeurs hash des différents documents et d'autres renseignements à leur sujet sont d'abord préparés (sérialisées notamment), voir également l'annexe A (représentation graphique simplifiée de la signature XML). Le résultat est ensuite signé, mais la préparation des données n'est pas enregistrée.

Il est donc important à cet égard d'utiliser la même préparation lors de la vérification de la signature que lors de la production. Dans le cas contraire, la vérification de la signature aboutit à un résultat non valide (erroné).

MUST: Les méthodes de «canonicalization», qui sont spécifiées dans la norme W3C-Sig, doivent être prises en charge.

MUST NOT: Pour des raisons de sécurité, toute autre méthode de «canonicalization» est à proscrire.

La préférence va à une «canonicalization», qui tient compte des espaces de noms des objets à signer, ce qui signifie qui les joint dans le cas où ils n'y sont pas présents.

Le chapitre 8.1 de la norme [RFC 3275], et W3C-Sig, ainsi que le chapitre 4.2.3 «Transformation des objets» décrivent les dangers associés à la «canonicalization» et la transformation.

4.2.7 Procédure pour la signature

4.2.7.1 Algorithmes

Concernant le choix des algorithmes pour la somme de contrôle, voir chapitre 4.2.5.

SHOULD: L'algorithme de hash pour la création de la somme de contrôle des objets devrait être identique à l'algorithme de hash pour la création de la signature.

4.2.7.2 Procédure asymétrique

DOIT: Dans l'environnement utilisateur, il faut faire attention à ce que la Crypto Card soit compatible avec les algorithmes et les longueurs de clé appropriés afin de constituer la signature. Les PTA répertorient les exigences relatives à la Crypto Card.

SHOULD: Dans l'environnement serveur, un module HSM devrait être utilisé pour la conservation en toute sécurité des clés privées et pour les opérations avec celles-ci.

Les normes du W3C répertorient les algorithmes asymétriques (fonctions hash) pour le Message Digest (somme de contrôle cryptographique). Celles qui doivent être utilisées sont précisées pour des raisons de sécurité.

MUST: Les RSA avec une longueur de clé d'au moins 2048 Bits doivent être pris en charge.

SHOULD: La procédure DSA (courbes elliptiques, logarithme discret) devrait être prise en charge.

MUST: Dans le cas où la procédure DSA est utilisée, il faut faire attention à ce que le nombre de valeurs possibles dans la procédure asymétrique soit au moins aussi important que le nombre de valeurs hash possibles.

Motif: Dans le cas contraire, des collisions peuvent se produire dès la constitution de la signature. Les valeurs hash possibles de la procédure hash sont réduites aux valeurs possibles de la procédure asymétrique. L'IETF RFC 6979 propose des exemples qui viennent contredire ce qui est décrit dans ces pages. Pourtant, contrairement à ce document, rien n'y indique qu'il ne faudrait pas procéder de la sorte. Il est donc question ici d'une liste de mauvais exemples, ce qui n'était pas l'intention du RFC 6979.

4.2.7.3 HMAC

La norme du W3C énumère les algorithmes (fonctions hash) pour l'authenticité avec un HMAC. La norme prévoit que l'authenticité puisse également être sécurisée au moyen d'un HMAC.

MUST: Seules les fonctions hash SHA-256, SHA-384, SHA-512 répertoriées dans le W3C doivent être utilisées.

MUST NOT: Si un processus à authentifier n'est pas totalement automatisé, la procédure HMAC ne doit pas être utilisée.

Motif: La gestion des clés ne devrait pas être proposée à l'utilisateur pour la conservation sûre des clés.

MUST: La clé pour le HMAC doit avoir une longueur minimale de 128 bits.

Motif: Les clés moins longues générées de façon aléatoire sont jugées peu sûres aujourd'hui.

SHOULD NOT: La clé utilisée afin de constituer le HMAC ne devrait pas être la même que la clé utilisée pour le chiffrement.

MUST NOT: Le HMAC ne doit pas être utilisé pour l'authenticité lorsque l'objet correspondant doit être conservé de telle manière que l'authenticité ne doive pas perdre sa validité.

Motif: La clé permettant de créer et de vérifier la valeur du HMAC devrait elle aussi être conservée. Il est impossible par la suite de déterminer laquelle des parties a généré la valeur HMAC.

4.2.8 Renseignements concernant le signataire

Selon la norme, des renseignements concernant le signataire, sa clé pour la vérification de signatures et son certificat peuvent être joints.

MUST: Dans le cas où des renseignements sur le signataire et sa clé publique sont fournis, les seuls

renseignements devant être utilisés sont ceux contenus dans le certificat X.509.

Motif: Les renseignements dans les certificats sont (reconnus) fiables.

Remarque: Les autres formes de certificats, tels les certificats PGP ou SPKI, ne sont guère utilisées en Suisse et ne sont pas non plus autorisées en lien avec la signature électronique équivalente à la signature manuscrite et pour la création d'un cachet électronique.

4.2.9 Affichage pour l'utilisateur

Les applications peuvent afficher pour l'utilisateur, qui vérifie la signature, des renseignements supplémentaires concernant le signataire.

MUST: Si les renseignements relatifs à l'entité signataire (tels que la personne, l'institution ou le service) sont affichés pour le destinataire, le logiciel doit alors vérifier si les renseignements fournis concordent bien avec les informations figurant dans le certificat à utiliser afin de vérifier la signature. Si les deux renseignements ne concordent pas, cela doit être signalé par un message d'alerte lors de la vérification de la signature.

SHOULD: La signature ne devrait pas être acceptée dès lors que les renseignements ne concordent pas.

Motif: Voir [RFC 3850] ou W3C-Sig chapitre 8.1.

4.2.10 Renseignements concernant les sous-objets

Conformément à la norme W3C-Sig, l'inclusion de renseignements concernant le type (MIME Type) des objets à signer est permise.

SHOULD: Les renseignements concernant le type des objets à signer devraient être joints.

Motif: Les renseignements concernant le type d'objet facilitent la composition du document.

MUST: Dès lors que des renseignements sont fournis, la norme correspondante [RFC 3023] doit être respectée.

Motif: Les renseignements non normalisés concernant le type d'objet compliquent l'interopérabilité et, par conséquent, la composition de l'objet.

4.2.11 Indication de temps

Les indications de temps non reconnues concernant la signature, par exemple les indications de temps faites par le signataire, ne sont que peu opportunes, parce qu'une indication de temps dans ce contexte cherche à justifier, voire prouver quelque chose. Les indications de temps reconnues sont établies au moyen d'un horodatage provenant d'un organisme indépendant reconnu.

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

Motif: Ces horodatages sont les seuls reconnus à coup sûr.

MUST: Dans le cas où il faut prouver qu'une signature a été créée avant ou après un moment précis, les éléments XML correspondants de la norme ETSI EN 319 132-1 V1.1.1 doivent être utilisés et intégrés à la structure (schéma) qui y est prescrite (AllDataObjectsTimeStamp, SignatureTimeStamp).

Contre-signature

SHOULD: Une contre-signature devrait être créée - tel que décrit par la norme ETSI EN 319 132-1 V1.1.1 - et insérée à l'endroit correspondant.

4.2.12 Autres renseignements

SHOULD: Si des informations complémentaires, comme spécifiées dans la norme ET319 132-1 V1.1.1, sont ajoutées à la signature ou au signataire et si ces informations font partie intégrante de la signature, cela devrait être fait conformément à la norme susmentionnée.

4.3 Chiffrement

4.3.1 Points fondamentaux

La norme XML Encryption Standard permet de chiffrer des documents complets ou uniquement des parties de ceux-ci, et ce au moment de la signature, cf. W3C Standard [Decryption Transforms for XML-Signature]. La norme W3C sur le chiffrement XML autorise les 3 types de chiffrement XML suivants:

- Le chiffrement du contenu d'un élément XML
- Le chiffrement d'un élément XML et de son contenu
- Le chiffrement de n'importe quel objet pouvant également avoir des éléments XML.

MUST: Toutes les informations (confidentielles) liées à la sécurité contenues dans le document administratif doivent être chiffrées.

Motif: Si des parties du document pertinentes pour la sécurité (confidentielles) sont disponibles en texte clair, des données sensibles peuvent être divulguées, avec le risque qu'elles parviennent entre de mauvaises mains.

SHOULD: Les informations, qui permettent de tirer des conclusions concernant la clé de chiffrement utilisée ou le texte chiffré, devraient également être chiffrées.

Motif: Les valeurs de somme de contrôle ou les signatures ne devraient pas être en texte clair. Cela permet notamment une attaque de type Brute Force accélérée à l'encontre du chiffrement, car il est possible d'effectuer un contrôle de plausibilité accéléré pour une clé de déchiffrement candidate.

Les renseignements concernant la structure de l'objet chiffré (tel MIME ou JPEG) doivent eux aussi être chiffrés, car cela peut également permettre de tirer des conclusions quant à la clé de chiffrement.

4.3.2 Renseignements concernant les sous-objets

Selon la norme W3C sur le chiffrement XML, l'ajout de renseignements en texte clair concernant le type d'objet (type MIME) des fichiers à chiffrer est permis.

SHOULD NOT: Des renseignements plus détaillés en texte clair concernant le type (MIME type) des sous-objets à chiffrer ne devraient pas être fournis en texte clair. Dans le cas où les éléments contiendraient des renseignements concernant les objets, ceux-ci devraient également être chiffrés.

Motif: Les informations relatives aux objets chiffrés doivent être omises, parce qu'elles risquent de compromettre la sécurité du chiffrement et donc la confidentialité.

4.3.3 Préparation des données à chiffrer

L'ensemble du document administratif doit, le cas échéant, être préparé de manière à être indépendant du contexte dans lequel il se trouvait auparavant. Dans le cas contraire, il existe un risque que les sous-objets soient involontairement conservés sous forme chiffrée et ne soient donc plus accessibles à d'autres personnes autorisées. Les renvois dans l'objet XML doivent ensuite être adaptés en conséquence. Si le document administratif devait également être signé avant le chiffrement, alors la signature ne doit être utilisée que lorsque le document administratif dépend du contexte, dans le cas contraire la signature perd toute validité.

Les procédures préconisées pour le chiffrement des objets XML sont les suivantes:

- Chiffrement XML, dans le cas où l'objet principal à chiffrer est constitué d'un objet principal.
- Tous les sous-objets et l'objet principal sont insérés dans un fichier ZIP. Celui-ci est ensuite chiffré. On peut chiffrer le fichier ZIP directement selon la norme CMS (Cryptographic Message Syntax [RFC 5652]).
- Encoder l'objet en Base64, l'insérer dans un fichier XML puis chiffrer la partie correspondante de l'objet.

L'utilisation de Cipher Reference est moins recommandée lors du chiffrement voir chapitre 3.3.1 de la norme WC3 [XML Encryption].

SHOULD NOT: Les objets signés ne devraient jamais être modifiés. Si, toutefois, les objets signés doivent être transformés pour une raison quelconque avant d'être chiffrés, les règles suivantes doivent s'appliquer:

MUST: Dans le cas où la «canonicalization» est appliquée aux données à chiffrer, alors la même méthode de canonicalization doit être appliquée au chiffrement XML que celle utilisée pour constituer la signature.

Motif: Contrairement à la signature, la préparation (la «canonicalization») des données avant le chiffrement modifie l'objet d'origine. C'est pourquoi il faut faire attention à ce que cette préparation des données ne détruise pas la signature déjà apposée sur le document non chiffré.

Le cas échéant, il est possible de préparer d'abord les documents XML, devant être aussi bien signés et chiffrés, pour le chiffrement, puis de les signer, et seulement à ce moment-là de les signer. Concernant la problématique de la «canonicalization» dans le cadre de la signature, de plus amples informations sont fournies sur http://www.w3.org/Security/.

Exemple d'incompatibilité et d'utilisation conforme à la norme: Dans le cas de la «canonicalization» pour la constitution ultérieure d'une signature, la méthode appliquée y est recommandée et laisse les objets XML en l'état. Pour le chiffrement, la méthode utilisée appelée «canonicalization» est recommandée par le W3C et supprime les commentaires. Avec pour effet de rendre la signature non valide une fois le déchiffrement réalisé.

4.3.4 Algorithmes pour le chiffrement

Tous les algorithmes de chiffrement XML énumérés dans la norme W3C doivent par principe être compatibles.

SHOULD NOT: Si l'objet est toujours assorti d'une information d'authentification (HMAC, signature) après le chiffrement, le Galois Counter Mode (GCM) ne devrait pas être utilisé.

Motif: D'autres clés doivent par principe être utilisées pour l'authentification et le chiffrement, voir également le chapitre 4.4 XML Signature Best Practices.

4.3.5 Accord/convention de clés (Key Agreement)

La norme W3C sur le chiffrement XML offre également la possibilité d'échanger des clés avec la structure de signature XML et de chiffrement XML ou de s'entendre sur une clé.

SHOULD NOT: Key Agreement (accord de clés)

Motif: Outre l'utilisation d'objets XML à cette fin, il existe à cet effet d'autres technologies conviviales et surtout normalisées, dont TLS.

MUST: Si, toutefois, un accord de clés est mis en œuvre via un objet XML, il doit être entièrement automatique, de sorte qu'un utilisateur n'ait pas à se soucier de la gestion des clés.

Motif: La gestion des clés ne devrait pas être proposée à l'utilisateur pour des raisons de sécurité lors du stockage des clés.

4.3.6 Transfert de clé

SHOULD NOT: Concernant le transfert de clés, la version 1.5 de RSA PKCS1 ne devrait pas être prise en charge - contrairement à la norme W3C, voir BSI TR-02102-1, page 19.

SHOULD:RSA-OAEP devrait être soutenu, voir à ce sujet BSI TR-02102-1, page 19.

Concernant RSA-OAEP et RSA PKCS 1, voir RFC 3447.

5 Alternatives

Comme l'indique le chapitre précédent, la XML Security ne peut pas être considérée comme totalement détachée de l'application XML, voir également les chapitres 3 et 4 [SOAP Security with Attachements]. Cela signifie que la sécurité doit être adaptée à l'application et inversement. Avec à la clé, des difficultés considérables dans les applications et mises en œuvre pratiques.

Afin d'éviter les problèmes liés aux signatures XML (qualifiées), le document XML - dans le cas d'INCA-Mail de la Poste Suisse - est converti en document PDF puis signé. Les PDF dans les versions plus anciennes et les PDF/A offrent l'avantage pour l'utilisateur de voir quelle signature il vérifie, d'afficher les données selon les besoins et de constater les modifications pertinentes pour la sécurité.

L'inconvénient de la dernière approche évoquée est que si l'objet PDF est bien signé et ainsi authentifié et protégé en termes d'intégrité, les fichiers XML en revanche ne le sont pas. La protection des objets XML peut toutefois se révéler nécessaire en vue du traitement ultérieur du contenu. Approche de solution possible:

conserver tout ce qui a trait au document XML et qui est pertinent à cet égard, indépendamment du contexte ou de l'environnement. Il faut, le cas échéant, ajuster les renvois internes, dans le cas où ils sont répertoriés non pas de manière relative, mais bien absolue dans le document d'origine. Le tout est ensuite compressé (zippé) puis empaqueté dans un fichier ZIP. Ce fichier est alors signé et, si nécessaire, chiffré selon la norme RFC correspondante [RFC 5652].

La signature d'un fichier ZIP dans l'environnement utilisateur a pour inconvénient que l'utilisateur ne peut pas voir précisément ce qu'il a signé, mais uniquement le fichier ZIP. Ce n'est pas le fichier ZIP, mais son contenu décompressé qui est affiché pour l'utilisateur.

La compression du fichier n'empêche pas davantage la création de documents administratifs XML d'apparence identique pour certaines applications, mais dotés d'une valeur hash différente.

6 Sécurité

Aucune

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.

Anhang A – Aperçu de la formation de la signature XML

Le graphique suivant montre de manière très simplifiée comment une signature XML est créée:

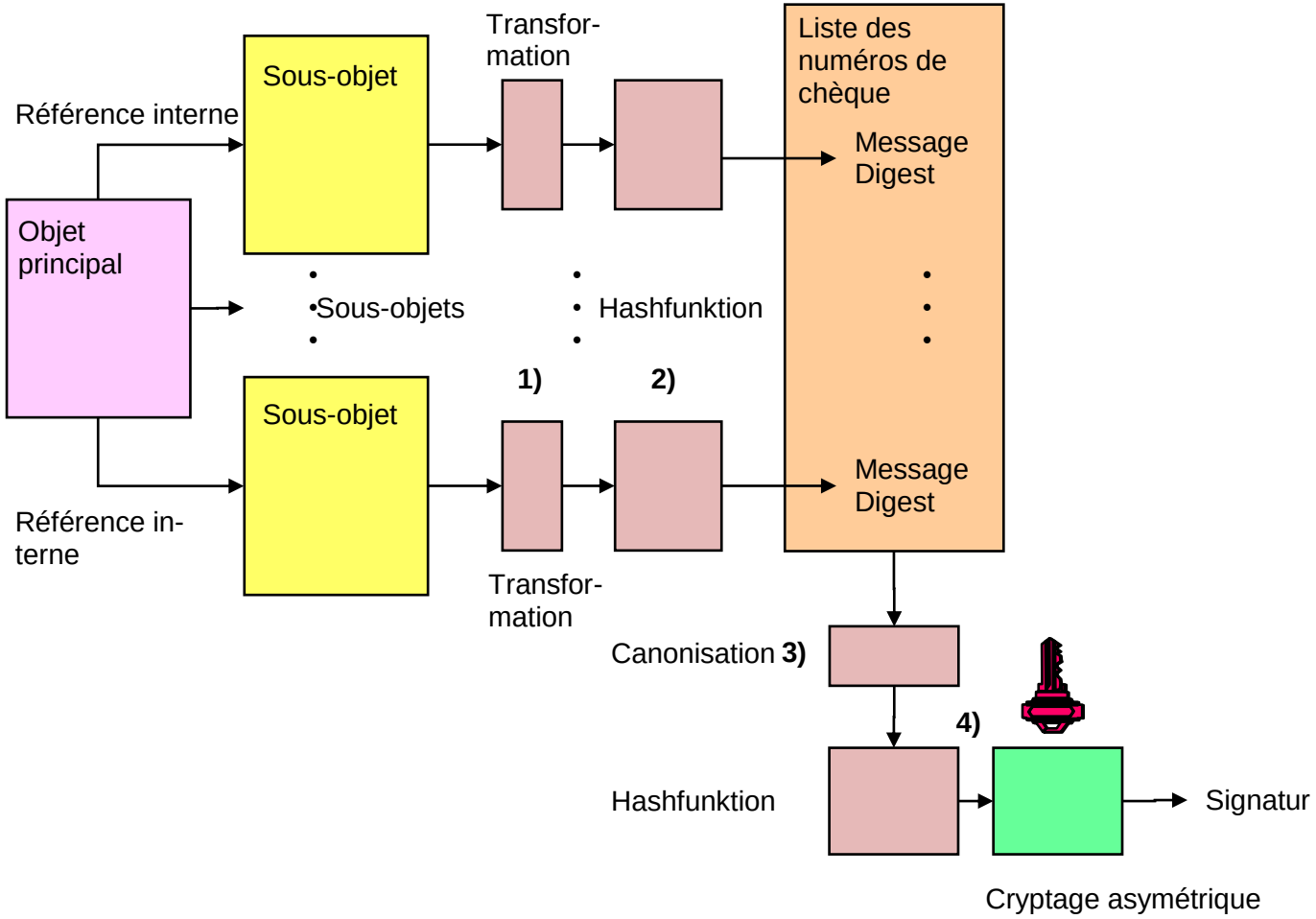


Figure 8 Signaturbildung

La signature est créée en 4 étapes:

1. Tous les objets à signer sont soumis à une ou plusieurs transformations, selon lesquelles, selon la norme W3C-Sig, les transformations pour les objets respectifs peuvent être différentes.
2. Von allen transformierten Objekten wird je eine kryptographische Prüfsumme (Message Di-gest) hergestellt, wobei gemäss W3C-Sig Standard das Verfahren zur Herstellung der Prüf-summe für die jeweiligen Objekte unterschiedlich gewählt werden kann. In diesem Dokument wird aber empfohlen, jeweils das gleiche Verfahren einzusetzen.
3. La liste des condensés de message (valeurs de hachage ou sommes de contrôle) est ensuite canonisée.
4. La signature est alors créée par la "canonisation". Selon la norme W3C-Sig, une méthode de production de la somme de contrôle pour la signature différente de celle de l'étape 2 précédente pourrait être utilisée ici. Dans ce document, cependant, il est recommandé de toujours utiliser la même procédure pour générer une somme de contrôle pour chaque signature.

Remarque: Des informations supplémentaires sont fournies pour chaque objet à partir duquel une somme de contrôle est produite et celles-ci sont répertoriées dans la liste afin qu'elles puissent être affectées à l'objet, telles que:

- Référence à l'objet à partir duquel la somme de contrôle a été générée.
- Informations sur le processus de transformation
- Informations sur le type d’objet
- Informations sur l'algorithme utilisé pour générer la somme de contrôle

Des informations supplémentaires peuvent être données pour la signature, telles que

- Informations sur le certificat, qui sont nécessaires pour vérifier la signature.
- Informations sur l'entité qui a créé la signature.

Annexe B – Références & bibliographie

Littérature spécialisée

[McAu]	Michael MacIntosh, Paula Austel, XML Signature Wrapping Attacks and Countermeasures
[MOV]	Alfred Menezes, Paul van Orschot, Vanstone Scott, Handbook of Applied Cryptography, CRC Press 1996, ISBN 0 8493 8523 7 http://cacr.math.uwaterloo.ca/hac/
[Nem]	Mark O'Neal, et al, Web Services Security, Mc Graw Hill/ Osborne, 2003, ISBN 0 07 222471 1
[Sch]	Schneier Bruce, Angewandte Kryptographie, Addison Wesley, 1. édition 1996, ISBN 3 89319 854 7
[Soetal]	Juray Somorovsky, Andreas Mayer at al, On Breaking SAML: Be Whoever You Want to be

eCH (www.ech.ch)

eCH-0018	XML Best Practices
eCH-0036	Documentation concernant l'échange de données orienté XML

ETSI (www.etsi.org))

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

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 3447	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
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 6979	Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)

W3C Standards (www.w3C.org)

Canonical XML Version 1.0 und 1.1 Recommendation March 2001 and May 2008

Decryption Transforms for XML Signature Recommendation, December 2002

Describing Media Content of Binary Data in XML W3C Working Group Note, May 2005

Exclusive XML Canonicalization Version 1.0 Recommendation, July 2002

XML Encryption and Syntax Processing Recommendation, Version 1.1, April 2013

XML Path Language (XPath) Version 1.0

XML Schema Part 1: Structures Second Edition. 28 October 2004

XML Schema Part 2: Datatypes Second Edition. 28 October 2004

XML Signature Best Practices Working Group Note, April 2013

XML Signature Syntax and Processing Recommendation Version 1.1, 11 April 2013

XSLT 2.0 and XQuery 1.0 Serialization (Second Edition) Recommendation, December 2010

CEN Standards

CWA 14170: CEN (European Committee for Standardization), Security Requirements for Signature Creation Applications, May 2004

CWA 14171 CEN (European Committee for Standardization), General Guidelines for electronic signature verification, May 2004

ENISA (www.enisa.europa.eu)

Algorithms, key size and parameters report - 2014, November 2014, European Union Agency for Network and Information Security Agency

BSI (www.bsi.de)

Procédures cryptographiques: recommandations et longueurs de clé, BSI TR-02102-1, version: 2019-01, statut: 22 février 2019

OASIS Standards (www.oasis-open.org)

Security Assertion Markup Language (SAML) v2.0

Web Services Security, SOAP Messages with Attachments (SwA) Profile 1.1, February 2006

Web Services Security, SOAP Messages Security 1.1, February 2006

Actes législatifs

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

OAAE: Ordonnance du DFJP sur l'établissement d'actes authentiques électroniques et la légalisation électronique du 8 décembre 2017, RS 211.435.11

OSCSE: Ordonnance sur les services de certification dans le domaine de la signature électronique et autres applications de certificats numériques, du 23 novembre 2016, RS 943.032

PTA: Prescriptions techniques et administratives sur les services de certification dans le domaine de la signature électronique et autres applications de certificats numériques, du 23 novembre 2016, RS 943.032.1

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

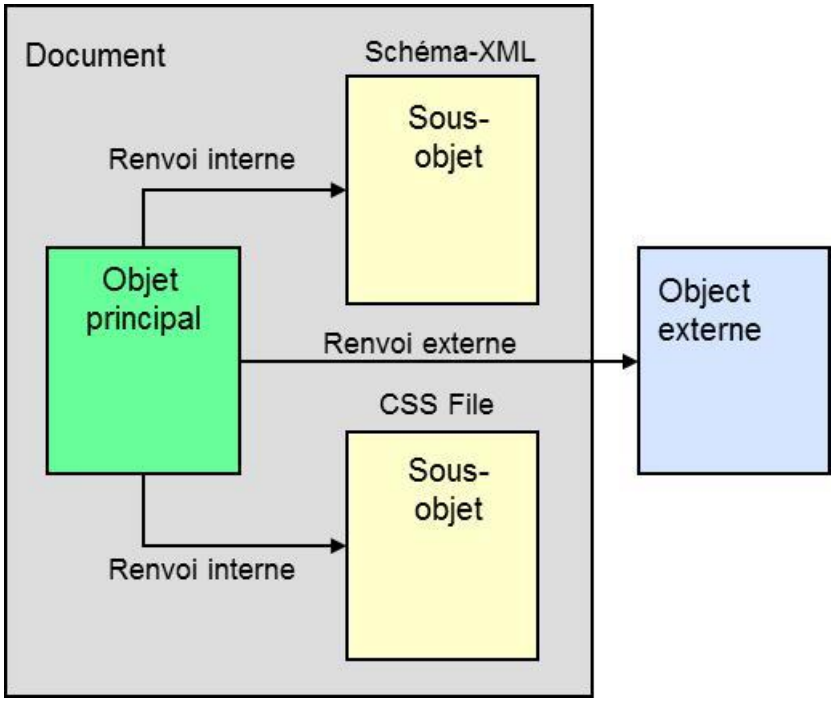
Annexe C – Collaboration & vérification

Annexe D – Abréviations et glossaire

Glossaire

«Canonicalization»	Selon le système d'exploitation, un même objet XML peut se présenter différemment. Avec la signature, on cherche cependant à déterminer non seulement l'origine de l'objet, mais également à protéger l'intégrité (la possibilité de constater un changement) de l'objet. Afin d'éviter qu'un même objet XML ne soit présenté de manière différente sur les systèmes d'exploitation distincts, on pratique sur l'objet XML une «canonicalization». Une fois la canonicalization effectuée, la composition de l'objet en question est la même, à l'octet près, sur les différents systèmes. Les normes traitant de la «canonicalization» sont [RFC 3076], [RFC 3741] ou les normes W3C à cet égard, pour n'en citer que quelques-unes.
Cachet électronique réglementé	Conformément à l'art. 2 let. d de la SCSE, une signature électronique avancée créée au moyen d'un dispositif sécurisé de création de cachet conformément à l'art. 6 de la SCSE, et basée sur un certificat réglementé délivré à une entité IDE conformément à l'art. 3 al. 1 let. c de la loi fédérale du 18 juin 2010 portant sur le numéro d'identification des entreprises (LIDE) et valable au moment de la création du cachet électronique;
Certificat qualifié	Certificat numérique répondant aux exigences de l'article 8 de la SCSE.
Document	Le document est constitué de l'objet principal et des sous-objets correspondants (sur lesquels porte un renvoi *en interne*). Un document XML est un document dont l'objet principal présente une structure XML.
Document d'administration	Un document que les acteurs impliqués dans un processus administratif s'envoient mutuellement afin de déclencher, d'enregistrer, de traiter ou de régler un cas d'affaires spécifique. Ils doivent être archivés à des fins de garantie de la traçabilité. Les exemples en sont: formulaires de demande remplis, actes législatifs, évaluations, rapports, extraits de registre, etc.
Document d'administration XML	Un document d'administration dont l'objet principal présente une structure XML.

Document XML	Un document dont l'objet principal présente une structure XML.
Objet principal	Objet d'origine d'où partent les renvois explicites. Objet qui contient l'élément racine.
Renvoi	Un renvoi dans un objet fait référence, soit *implicitement* soit *explicitement,* à un autre objet ou à une instruction de commande. Un renvoi implicite fait référence à un objet qui n'existe pas ou à une instruction de commande qui n'a pas été écrite, mais à quelque chose de préalablement convenu au sein de la société de communication. Un renvoi existant vers une instruction de commande resp. un objet est, par exemple, un renvoi vers un code en JavaScript ou un schéma XML. Un renvoi implicite est par exemple le renseignement: <site web xmlns:html="http://www.w3.org/TR/REC-html40"> Chaque élément au sein de l'élément «site web», qui commence par <html: > est interprété comme une information en HTML. Concernant les renvois explicites, on distingue entre renvois internes et externes au document. Les renvois internes au document sont des renvois à des sous-objets (des fichiers par exemple) faisant partie du document, comme des schémas ou des images. Les renvois externes, cependant, sont des renvois à des objets externes (objets principaux ou sous-objets) qui contiennent des informations complémentaires, mais qui ne sont pas indispensables à l'interprétation du document. Un exemple de renvoi externe est une indication de source inscrite en HTML ou XML, par exemple. Voir à ce sujet l'illustration suivante:



Remarque: Quant à savoir ce qui relève désormais d'un renvoi externe ou interne, la réponse dépend des intentions de l'auteur du document XML, de la communauté de communication ou de la plateforme de communication.

Signature qualifiée	Voir l'article 2, let. e, de la SCSE: Signature électronique réglementée basée sur un certificat qualifié.
Sous-objet	Objet sur lequel porte un renvoi *en interne*, tel un fichier CSS ou un fichier image par exemple.
Transformation	La transformation, au sens où l'entend la norme W3C-Sig, signifie que l'objet est filtré, traité ou canonisé de la manière souhaitée avant que la somme de contrôle cryptographique (valeur hash) soit calculée pour l'objet modifié par la transformation.
Types de signature	Les types de signature normalisés et les plus répandus dans la technique sont les suivants: a. Cryptographic Message Syntax RFC 5652, les versions antérieures sont: PKCS#7 Signature s. [RFC 2315], nouvelle norme pour IETF CMS (Cryptographic Message Syntax [RFC 3852] b. XML Signature voir W3C-Sig Les deux signatures reposent pour l'essentiel sur un même principe technique. Elles diffèrent toutefois quant aux informations complémentaires jointes à la signature et à la manière dont elles sont structurées.

Abréviations

Al.	Alinéa
Ch.	Chiffre
CSS	Cascading Style Sheets Language
DTD	Document Type Definition
ETSI	European Telecommunications Standards Institute
GRDDL	Gleaning Resource Descriptions from Dialects of Languages
HMAC	Keyed-Hash Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IRI	Internationalized Resource Identifier
Let.	Lettre
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
RDDL	Resource Directory Description Language
RDF	Resource Description Framework
resp.	respectivement
RSA	Rivest Shamir Adleman Public Key Algorithm
SAML	Security Assertion Markup Language (SAML) v2.0
SOAP	Service Oriented Application Protocol

SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
URI	Universal Resource Identifier
W3C	World Wide Web Consortium
W3C-Sig	XML Signature Syntax and Processing Recommendation version 1.1, 11 avril 2013
XHTML	Extensible Hypertext Markup Language
XLink	Extensible Linking Language
XML	Extensible Markup Language
XSLT	XSL Transformations

Annexe E – Modifications par rapport à la version précédente

Request	Chapitre	Page	Adaptation
	Page de titre		De la Best Practice à la norme. Pour connaître le motif, voir la remarque ci-dessous.
	0	7	Liste modifiée (Annexe B mise de côté)
	3.3.2	16	Ajout des lignes 2 et 3 dans le tableau
	3.4.2	19	Ajout de la ligne 2 dans le tableau
	3.5	19	Ajout de la ligne 3 dans le tableau
	4.2.1	23	Recommandation «MUST NOT» ajoutée
	4.2.3	24	Paragraphe « Motif » supprimé pour la transformation des objets
	4.2.4	25	Ajouté
	4.2.7.3	26	Complément aux procédures asymétriques et pour la conservation des clés privées
	4.2.11	27	Recommandation complémentaire
	4.2.12	28	Recommandation complémentaire
	4.3.4	29	Recommandation complémentaire
	4.3.5	29	«Accord clé …» repoussé vers l'arrière
	4.3.6	30	Recommandation complémentaire
	Annexe B		Complément/suppression dans la littérature technique, ajout des RFC ETSI et IETF, mise à jour des normes

Request	Chapitre	Page	Adaptation
			W3C, ajout d'une norme BSI et de normes ENISA, extension des renseignements concernant les actes législatifs
	Annexe D		Ajout au glossaire
	Annexe D		Adaptation de la liste des abréviations

Remarque: Du statut de Best Practice, le document est passé à celui de norme. Compte tenu notamment de l'importance du sujet en question, il a vocation à devenir une norme. L'une des problématiques traitées dans ces pages, qui se pose en raison des liens entre les objets XML, figure au top 10 des thématiques de l'OWASP. Voir les points 3 et 4 sur https://owasp.org/www-project-top-ten/.

En outre, la problématique de la présentation d'un document XML à l'utilisateur est expliquée et des préconisations de solution sont avancées. La norme XML correspondante du W3C n'aborde pas ce point. Dans ce contexte, on peut en déduire par analogie des recommandations pour les signatures d'e-mail avec contenu HTML.

A contrario des normes précédemment évoquées, le présent document précise également qu'il existe des incompatibilités entre les normes W3C en ce qui concerne le chiffrement post-signature. Or, ces normes n'en disent rien.

Par ailleurs, des recommandations ont été formulées concernant les indications de temps et la vérification d'une signature. Si les recommandations portant la vérification de la signature n'apparaissent pas dans une norme, elles n'en figurent pas moins dans des publications scientifiques, voir [Soetal] par exemple.

Annexe E – Liste des illustrations