

|                                |  |
|--------------------------------|--|
| <b>Statut du document</b>      | W3C Working Draft et IETF  |
| <b>Titre</b>                   | XML-Signature Syntax and Processing  |
| <b>Mot clé</b>                 | Attestation  |
| <b>Source</b>                  | W3C <a href="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/">http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/</a> et IETF <a href="http://www.w3.org/Signature/">http://www.w3.org/Signature/</a>  |
| <b>Date de publication</b>     | 28 février 2000  |
| <b>Nombre de pages</b>         | 34   |
| <b>Langue</b>                  | Anglais  |
| <b>Lien avec autres normes</b> | La syntaxe XML offre un levier de contrôle précis pour rassembler les parties d'un document, pour délimiter avec précision ce qui doit faire partie d'un document et de la responsabilité de sa signature.   |
| <b>Situation actuelle</b>      | Dernier appel aux commentaires en cours. Recommandation au printemps de 2000 est probable.   |
| <b>Description</b>             | <p>XML-Signature précise les règles de syntaxe et de traitement pour créer et représenter les signatures numériques d'une façon adaptée à la complexité admissible pour les documents XML sur le Web et à une diversité de situations commerciales.</p> <p>On a en particulier voulu rendre possible l'inclusion de la signature numérique dans le document lui-même en plus de pouvoir l'attacher au document comme une étiquette, et même de pouvoir inclure le document dans l'étiquette de signature numérique. On a aussi voulu qu'une signature puisse être apposée simultanément « sur » plusieurs documents (référéncés dans un <i>manifeste</i>). On a voulu que la signature puisse être réalisée en utilisant l'un ou l'autre des algorithmes existants et futurs de cryptographie. Enfin, il fallait délimiter avec précision le <i>modus operandi</i> pour l'entrée automatique des données du document source, quand il est en XML, dans l'algorithme de prise d'empreinte (<i>hashing</i>).</p> <p>La signature XML peut être présentée selon une vue structurelle et une vue fonctionnelle. La vue fonctionnelle est présentée d'abord pour faciliter la compréhension.</p> <p>La <u>production</u> de la signature XML se déroule en six étapes de traitement :</p> <ul style="list-style-type: none"> <li>- <b>Effectuer les transformations</b> : l'objet à signer peut être un document XML avec diverses transformations (Java, XSLT, Xpath, Xpointer, filtrage, encodage) qui doivent toutes être exécutées pour uniformiser les objets à signer avant que ne soit calculée leur empreinte. Un utilisateur signe généralement un document tel qu'il le voit, i.e. après que les transformations aient été effectuées.</li> <li>- <b>Calculer l'empreinte</b> : un algorithme est utilisé pour calculer l'empreinte de l'objet à signer (SHA1, HMAC-SHA1, MD5).</li> <li>- <b>Encoder</b> : étape technique d'encodage en Base64 de toute valeur d'empreinte numérique obtenue à l'étape de traitement précédente.</li> <li>- <b>Assemblage de SignedInfo</b> : insertion de la valeur d'empreinte dans l'élément SignedInfo avec plusieurs autres renseignements énumérés ci-après dans la structure de la signature.</li> <li>- <b>Régulariser le contenu rassemblé</b> : la régularisation ou « canonicalisation » (du latin <i>canonicalis</i>, qui signifie « en accord avec un canon ou règle ») est une</li> </ul> |

|  |   |
|--|---|
|  | <p>étape conditionnelle au contexte. Elle est effectuée par un algorithme qui par exemple régularisera le calcul des espaces blancs en fin de ligne, normalisera le jeu de caractères, etc. Alors que les transformations (dont une obligatoire de canonicalisation) portent sur l'objet à signer (ou document) à la première étape, ici c'est le contenu de SignedInfo, de ce qui sera effectivement signé avec la clé privée de l'utilisateur à l'étape suivante, qui se trouve régularisé.</p> <ul style="list-style-type: none"> <li>- <b>Calculer la signature</b> : L'algorithme de signature (DSA, RSA, ECDSA) applique la clé privée du signataire au contenu régularisé de SignedInfo et produit la valeur de la signature (<i>SignatureValue</i>).</li> </ul> <p>La <u>structure</u> de la signature XML est composée de quatre éléments :</p> <ul style="list-style-type: none"> <li>- <b>SignedInfo</b> : élément obligatoire qui contient les données réellement signées et qui sont constituées des noms des algorithmes utilisées pour la canonicalisation, pour la prise d'empreinte (<i>digest</i>) et pour la signature. Tous les algorithmes connus et dont la conformité mathématique peut être établie peuvent ainsi être utilisés dans un souci d'ouverture maximale du protocole. <i>SignedInfo</i> contient aussi une section d'identification de l'adresse et du type de l'objet source devant être signé, une liste des transformations à lui appliquer, ainsi que le nom de l'algorithme de prise d'empreinte, et la valeur de l'empreinte numérique pour cet objet. L'indication du type de l'objet permet d'indiquer des attributs de signature ou encore de regrouper en une liste des documents ou ressources dans un <i>manifeste</i> qui permet de circonscrire les multiples parties à signer en bloc lorsque le contexte l'exige.</li> <li>- <b>SignatureValue</b> : élément obligatoire qui contient la valeur effectivement obtenue pour la signature numérique comme résultat de l'algorithme de signature.</li> <li>- <b>KeyInfo</b> : élément facultatif sur le certificat de clé publique du signataire afin de permettre au récipiendaire d'obtenir la ou les clés nécessaires à la validation de la signature.</li> <li>- <b>Object</b> : élément facultatif permettant d'insérer le contenu au complet de l'objet signé dans la signature.</li> </ul> |
|--|---|

**Remarque** Collaboration W3C et IETF est exceptionnelle et souligne l'importance de fondements techniques solides.

#### Lexique anglais-français

|          |                     |  |
|----------|---------------------|--|
| Digest   | Empreinte numérique | <i>Hash algorithm</i> se traduit corollairement comme <i>algorithme de prise d'empreinte</i> |
| Manifest | Manifeste           |  |
| Label    | Étiquette           | Contexte de <i>Dsig label</i> et de PICS, où <i>label</i> a le sens d'étiquette.             |

**Rédacteur :** Richard Parent  
**Organisation source :** Secrétariat du Conseil du trésor  
**Date de publication :** 21 août 2000  
**Raison d'être :** Connaissance technologique  
**Programme gouvernemental :** Inforoutes et ressources informationnelles  
**Nom du modificateur :**  
**Date de dernière modification :**

Note numéro :

5