RFC 6931 : Additional XML Security Uniform Resource Identifiers (URIs)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 avril 2013

Date de publication du RFC : Avril 2013

https://www.bortzmeyer.org/6931.html

Il existe tout un ensemble de normes pour assurer la sécurité de documents XML, par exemple les protéger contre la lecture non autorisée, ou bien permettre leur authentification. Ces normes dépendent d'algorithmes cryptographiques identifiés par un URI. Ce RFC met à jour la liste précédente de ces URI (qui était dans le RFC 4051 [1]) et crée un registre des identificateurs d'algorithmes <https://www.iana.org/assignments/xml-security-uris/xml-security-uris.xml>.

Ces normes de sécurité de XML étaient à l'origine un travail conjoint de l'IETF et du W3C. C'était par exemple le cas des signatures XML du RFC 3275, du XML canonique des RFC 3076 ou RFC 3741. Elles sont désormais maintenues par le W3C qui a produit des versions plus récentes (par exemple pour les signatures XML <http://www.w3.org/TR/2013/PR-xmldsig-core1-20130124/>, le XML canonique <http://www.w3.org/TR/2008/REC-xml-c14n11-20080502/> ou le chiffrement XML <http://www.w3.org/TR/2013/PR-xmlenc-core1-20130124/>).

Dans un monde dynamique comme celui de la cryptographie, où les progrès de la cryptanalyse nécessitent des changements d'algorithmes, les normes ne sont pas liées à un algorithme particulier. Elles permettent l'agilité cryptographique (le changement d'algorithme) et il faut donc pouvoir indiquer quel algorithme est utilisé pour signer ou chiffrer un document donné. Pour une norme W3C, on ne s'étonnera pas que l'indication se fait par le biais d'un URI. Ceux-ci commencent désormais par le préfixe http://www.w3.org/2007/05/xmldsig-more# (les anciens algorithmes pouvant avoir d'autres préfixes). Ces nouveaux algorithmes (avec 2007/05 dans leur identificateur) sont relativement rares dans ce RFC : on n'invente quand même pas un bon algorithme de cryptographie tous les jours et la plupart des exemples dans cet article utilisent donc le vieux préfixe. Rappelez-vous qu'il s'agit

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4051.txt

d'URI, pas forcément d'URL et que vous n'obtiendrez donc pas forcément un résultat en pointant votre navigateur Web vers `http://www.w3.org/2001/04/xmlenc#sha256`.

Notons que notre RFC 6931 ne prend pas position sur la qualité cryptographique des algorithmes : il fournit un moyen de les désigner sans ambiguité, c'est tout. Si on veut étudier cette qualité cryptographique, il faut lire d'autres documents (comme le RFC 6194 pour SHA-1).

Un exemple d'un ancien algorithme est MD5 pour calculer les condensats cryptographiques. Son URI est `http://www.w3.org/2001/04/xmldsig-more#md5`. Sa sécurité est aujourd'hui sérieusement battue en brèche (cf. RFC 6151). Autre exemple d'un algorithme qui était déjà dans le RFC 4051, SHA-384, identifié par `http://www.w3.org/2001/04/xmldsig-more#sha384`.

Un exemple d'un nouvel algorithme pour la condensation cryptographique ? Le NIST ayant récemment annoncé que le vainqueur du concours « SHA-3 » était Keccak, des URI utilisant le nouveau préfixe ont été créés pour lui, par exemple `http://www.w3.org/2007/05/xmldsig-more#sha3-512` (regardez bien : `sha-3` et plus `sha`, et la nouvelle date dans le préfixe).

Il existe aussi des identificateurs pour les MAC combinés avec une condensation, par exemple `http://www.w3.o`
(RFC 6234).

Et pour les signatures avec un système à clé publique ? L'identificateur indique l'algorithme de cryptographie asymétrique et celui de condensation, par exemple `http://www.w3.org/2001/04/xmldsig-more#rsa`
(voir aussi le RFC 3447). SHA-256 n'est pas tout récent et, si vous cherchez un algorithme enregistré par notre nouveau RFC, pourquoi pas Whirlpool avec `http://www.w3.org/2007/05/xmldsig-more#rsa-whirlpo`
Si on trouve RSA ennuyeux, il existe aussi des identificateurs pour un algorithme à courbes elliptiques (RFC 6090 mais notez ses errata <http://www.rfc-editor.org/errata_search.php?rfc=6090>), ECDSA, par exemple `http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512`.

Enfin, il y a les algorithmes de chiffrement symétrique. Par exemple, Camellia (RFC 3713) sera identifié par `http://www.w3.org/2001/04/xmldsig-more#camellia256-cbc`. Le plus récent SEED (RFC 4269) sera `http://www.w3.org/2007/05/xmldsig-more#seed128-cbc`.

Voici pour la cryptographie. Mais les normes de sécurité XML prévoient aussi une étape de canonicalisation avant chiffrement ou signature, et là aussi, il y a plusieurs algorithmes, identifiés par des URI comme `http://www.w3.org/2000/09/xmldsig#minimal` ou `http://www.w3.org/2006/12/xmlc14n11#W`

Quelle est la politique d'allocation dans le nouveau registre ? La section 5 décrit celle du W3C (le préfixe `http://www.w3.org/2007/05/xmldsig-more#` est figé, a priori, on n'y mettra pas de nouveaux algorithmes) et celle de l'IETF : comme il est facile d'obtenir un URI (n'importe qui peut en créer un), la seule question est celle de leur enregistrement. Il se fera après un examen par un expert (voir le RFC 5226 pour les politiques d'allocation IETF) après publication d'un texte décrivant le nouvel algorithme.

Quels changements depuis la version précédente de ce RFC, le RFC 4051 ? L'annexe A les liste. Les principaux, à mon avis, sont :

— Ajout des algorithmes Whirlpool, RIPEMD-160, et SEED,
— Ajout de SHA-3,
— Création du registre IANA.