JOSE, la cryptographie pour JSON

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 mai 2015

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

Le format JSON a largement remplacé XML dans les applications Web et sert aujourd'hui de base à plein d'applications. Il était donc logique qu'on cherche à la sécuriser par la cryptographie et c'est le rôle du groupe de travail JOSE <https://tools.ietf.org/wg/jose> ("*JavaScript Object Signing and Encryption*") de l'IETF qui vient de publier une série de normes sur la signature et le chiffrement de textes JSON.

Un premier RFC avait déjà débroussaillé le terrain en expliquant les scénarios d'usage et le cahier des charges, c'était le RFC 7165 [1]. Les nouveaux RFC, eux, définissent les normes techniques. Ce sont :

- RFC 7518 : "*JSON Web Algorithms (JWA)*" décrit les registres où sont stockés les identificateurs des algorithmes de cryptographie utilisables.
- RFC 7517 : "*JSON Web Key (JWK)*" explique le format des clés.
- RFC 7515 : "*JSON Web Signature (JWS)*" expose le mécanisme de signature cryptographique, qui permet d'authentifier des documents JSON.
- RFC 7516 : "*JSON Web Encryption (JWE)*" normalise le chiffrement, grâce auquel les textes JSON peuvent rester confidentiels.
- RFC 7520 : "*Examples of Protecting Content using JavaScript Object Signing and Encryption (JOSE)*" est simplement un recueil d'exemples.
- En même temps que les RFC du groupe JOSE <https://tools.ietf.org/wg/jose> ont été publiés une autre série du groupe OAUTH <https://tools.ietf.org/wg/oauth> décrivant notamment des utilisations de JOSE dans le contexte d'OAuth. C'est par exemple le cas du RFC 7519, "*JSON Web Token (JWT)*", bien décrit dans cette série d'articles <https://www.primfx.com/json-web-token-jwt-guide-complet>.

Si vous voulez une très bonne explication de JOSE, avec plein d'explications simples, il y a l'article de Jan Rusnacko <https://securityblog.redhat.com/2015/04/01/jose-json-object-signing-and-encryp>. Un exposé au contraire très critique de JOSE a été fait par Fraser Tweedale <https://www.pass-the-salt.org/files/talks/16-jose.pdf>.

Si vous voulez plutôt pratiquer, il existe de nombreuses mises en œuvre de JOSE :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7165.txt

— En Python, il y a la bibliothèque nommée `jose` (<https://pypi.python.org/pypi/jose/> et <https://github.com/Demonware/jose>). « *"This library implements JWS and JWEs along with a subset of the encryption / authentication algorithms recommended by the JOSE framework."* » Sa documentation <http://jose.readthedocs.org/en/latest/> contient de nombreux exemples.
— En Java/JBoss, il y a aussi du JOSE (<https://docs.jboss.org/resteasy/docs/3.0.6.Final/userguide/html/ch40.html>). Toujours en Java, il y a le code de Connect2id (<http://connect2id.com/products/nimbus-jose-jwt>) et celui de 4j (<https://bitbucket.org/b_c/jose4j/wiki/Home>).
— En .NET, il existe aussi JOSE et JWT (<https://www.nuget.org/packages/jose-jwt/>).
— D'autres mises en œuvre se trouvent en <https://openid.net/developers/libraries/#jwt>

Merci à Virginie Galindo pour sa relecture.