RFC 8410 : Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 février 2019

Date de publication du RFC : Août 2018

https://www.bortzmeyer.org/8410.html

Ce RFC spécifie l'utilisation des courbes elliptiques Curve25519 et Curve448 dans PKIX, c'est-à-dire dans les certificats utilisés notamment pour TLS. Il réserve des identifiants pour les algorithmes, comme `Ed25519`.

Les courbes elliptiques Curve25519 et Curve448 sont normalisées dans le RFC 7748 [1]. Elles sont utilisées pour diverses opérations cryptographiques comme la signature. L'algorithme EdDSA, utilisant ces courbes, est, lui, dans le RFC 8032. Quand on écrit « Ed25519 », cela veut dire « EdDSA avec la courbe Curve25519 ». D'autre part, quand on écrit « X25519 », cela signifie « échange de clés Diffie-Hellman avec la courbe Curve25519 ».

Un certificat suivant le profil PKIX du RFC 5280 contient une clé publique, pour un algorithme cryptographique donné. Il faut donc un identificateur formel pour cet algorithme. Sa syntaxe est celle d'un OID, par exemple `1.2.840.113549.1.1.1` (cf. RFC 8017) pour RSA. Notre RFC définit (section 3) quatre nouveaux identificateurs :

- `id-X25519:1.3.101.110` (ou, en détaillé, {`iso(1) identified-organization(3) thawte(101) id-X25519(110)`}) ; notez qu'il avait été enregistré par Thawte, depuis racheté par Symantec, ce qui explique pourquoi le RFC remercie Symantec,
- `id-X448:1.3.101.111`,
- `id-Ed25519:1.3.101.112`,
- `id-Ed448:1.3.101.113`.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7748.txt`

Le RFC recommande aussi des noms plus sympathiques que les OID, OID qu'on ne peut vraiment pas montrer aux utilisateurs. Ces noms sont ceux décrits plus haut, comme Ed25519 pour EdDSA avec Curve25519. Si on ne sait pas quelle courbe est utilisée, on dit simplement « EdDSA » pour la signature, et « ECDH » pour l'échange de clés Diffie-Hellman.

Les nouveaux identificateurs et OID sont désormais dans le le registre IANA `<https://www.iana.org/assignments/smi-numbers/smi-numbers.xml#smi-numbers-1.3.101>`.

Le RFC fournit aussi des structures ASN.1, avec des exemples en section 10.

Notez qu'OpenSSL, avec `openssl x509 -text`, ou GnuTLS, avec `certtool --certificate-info`, n'affichent pas les OID, seulement les identificateurs texte.