RFC 7218 : Adding acronyms to simplify DANE conversations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 avril 2014

Date de publication du RFC : Avril 2014

https://www.bortzmeyer.org/7218.html

Le système DANE permet de publier des clés cryptographiques ou des certificats dans le DNS, en les authentifiant avec DNSSEC. Ces clés ou certificats sont mis dans un enregistrement de type **TLSA** et cet enregistrement comprend plusieurs champs portant des valeurs numériques. Jusqu'à ce RFC, il n'existait pas d'acronymes standards pour désigner les valeurs possibles, ce qui rendait difficile la communication entre humains, et le choix des noms de variables dans les programmes. Ce nouveau RFC ne change pas le système DANE mais décrit simplement ces acronymes standards.

Voici un exemple actuel d'enregistrement TLSA (enregistrement DANE) :

```
_443._tcp.fedoraproject.org. 300 IN TLSA 0 0 1 (
D4C4C99819F3A5F2C6261C9444C62A8B263B39BC6ACC
E35CDCABE272D5037FB2 )
```

Les champs dont les valeurs sont ici 0, 0 et 1 sont les champs dont on souhaite pouvoir parler plus facilement. La norme DANE, le RFC 6698 [1], ne définit pas de noms courts pour les valeurs. Par exemple, le deuxième champ, le Sélecteur, qui vaut 0 ici, peut prendre deux valeurs, que le RFC 6698 nomme "*Full certificate*" et `SubjectPublicKeyInfo`, alors que notre nouveau RFC 7218 propose d'ajouter les acronymes `Cert` et `SPKI`. Dans le futur, on peut même imaginer que les logiciels puissent charger directement une zone DNS où les valeurs numériques seraient remplacées par ces acronymes (et dig pourrait les afficher au lieu des valeurs numériques actuelles).

Le registre IANA en est donc modifié pour y inclure ces acronymes. Le champ « Utilisation du certificat » ("*Certificate usage*"), sans doute celui où il y a eu le plus de confusions et de discussions, peut prendre les valeurs :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6698.txt`

— 0, contrainte sur l'AC, désormais `PKIX-TA`,
— 1, contrainte sur le certificat, désormais `PKIX-EE` (EE pour "*End Entity*"),
— 2, déclaration de l'AC, désormais `DANE-TA`,
— 3, déclaration du certificat, désormais `DANE-EE`.

Notez le regroupement des acronymes en deux groupes : les acronymes commençant par `PKIX` sont les utilisations où on fait toujours la validation PKIX classique (RFC 5280) et ceux commençant par `DANE` sont ceux où on n'utilise plus le modèle de validation de X.509, on est purement dans un monde DANE.

Le champ « Sélecteur » ("*Selector*"), lui, peut être :
— 0, le certificat complet, désormais `Cert`,
— 1, la clé seule, désormais `SPKI`.

Et le champ « Méthode de correspondance » ("*Matching type*", et merci à Romain Tartière pour avoir trouvé une erreur dans mon article original) :
— 0, valeur brute des données, désormais `Full`,
— 1, condensat SHA-256 des données, désormais (logiquement) `SHA2-256`,
— 2, condensat SHA-512 des données, désormais `SHA2-512`.

La section 3 donne des exemples d'enregistrements affichés avec ces acronymes. Pour celui cité plus haut, ce serait :

```
_443._tcp.fedoraproject.org. 300 IN TLSA PKIX-TA Cert SHA2-256 (
D4C4C99819F3A5F2C6261C9444C62A8B263B39BC6ACC
E35CDCABE272D5037FB2 )
```

Les humains étant particulièrement sensibles aux noms, les discussions ont été longues quant au choix des acronymes. Tout le monde était d'accord qu'il vallait mieux des acronymes que des nombres, simplement, chacun avait les siens comme favoris.

Pour la petite histoire, une bonne partie de la démarche menant à ce RFC vient de l'introduction de DANE dans Postfix. Viktor Dukhovni, en faisant ce travail, a découvert DANE et signalé à l'IETF nombre de problèmes et de limites, et notamment la difficulté à ne manipuler que des valeurs numériques, par exemple dans les documentations.