RFC 7958 : DNSSEC Trust Anchor Publication for the Root Zone

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 septembre 2016

Date de publication du RFC : Août 2016

https://www.bortzmeyer.org/7958.html

Le mécanisme d'authentification des informations DNS nommé DNSSEC repose sur la même structure arborescente que le DNS : une zone publie un lien sécurisé vers les clés de ses sous-zones. Un résolveur DNS validant n'a donc besoin, dans la plupart des cas, que d'une seule clé publique, celle de la racine. Elle lui servira à vérifier les clés des TLD, qui serviront à valider les clés des domaines de deuxième niveau et ainsi de suite. Reste donc à configurer la clé de la racine dans le résolveur : c'est évidemment crucial, puisque toute la sécurité du système en dépend. Si un résolveur est configuré avec une clé fausse pour la racine, toute la validation DNSSEC est menacée. Comment est-ce que l'ICANN, qui gère la clé principale de la racine, publie cette clé cruciale ? Six ans après la signature de la racine du DNS, c'est enfin documenté, dans ce RFC. (Il a depuis été remplacé par le RFC 9718[1].)

Cela donne une idée de la vitesse des processus ICANN, organisation qui produit beaucoup de papier. Notez que ce nouveau RFC documente l'existant, déjà mis en œuvre, et ne prétend pas décrire la meilleure méthode. Notez aussi que ce format et cette méthode de distribution pourraient changer à l'avenir.

Si vous voulez réviser DNSSEC d'abord, outre les RFC de base sur ce système (RFC 4033, RFC 4034, RFC 4035...), notez surtout le RFC 6781, qui décrit les questions opérationnelles liées au bon fonctionnement de DNSSEC.

Les clés publiques configurées dans les résolveurs qui valident avec DNSSEC, sont appelées « points de départ de la confiance » "*trust anchors*". Un point de départ de la confiance est une clé dont l'authenticité est admise, et non pas dérivée d'une autre clé, via une chaîne de signatures. Il en faut au moins un, celui de la racine, bien que certains résolveurs en ajoutent parfois deux ou trois pour des zones

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9718.txt

qu'ils veulent vérifier indépendamment. Lorsque le résolveur recevra une réponse de la racine, signée, il l'authentifiera avec la clé publique de la racine (le point de départ de la confiance). S'il veut vérifier une réponse d'un TLD, il l'authentifiera avec la clé publique du TLD, elle-même signée (et donc authentifiée) par la clé de la racine. Et ainsi de suite même pour les zones les plus profondes.

(Notez qu'il existe deux clés pour la plupart des zones, la KSK - "*Key Signing Key*", et la ZSK - "*Zone Signing Key*", mais on ne s'intéresse ici qu'aux KSK, c'est elles qui sont signées par la zone parente, et configurées comme points de départ de la confiance.)

La gestion de la clé de la racine par l'ICANN est décrite dans leur DNSSEC Practice Statement `<https://www.iana.org/dnssec/icann-dps.txt>`.

Le RFC rappelle aussi qu'il y a d'autres possibilités d'installation d'un point de départ de la confiance. Par exemple, si un tel point a été configuré une fois, ses remplacements éventuels peuvent être faits via le RFC 5011.

La section 2 du RFC décrit le format des clés publiées par l'IANA. Les trois formats, en fait :
— Un fichier XML contenant les condensats des clés, utilisant le format de présentation du RFC 4034. Leur syntaxe formelle est exprimé en Relax NG, le schéma est en section 2.1.1 du RFC.
— Des certificats PKIX (RFC 5280),
— Des CSR au format PKCS#10 (RFC 2986).
Voici un exemple du fichier XML (à ne pas prendre comme s'il faisait autorité, évidemment) :

```
<TrustAnchor id="AD42165F-3B1A-4778-8F42-D34A1D41FD93" source="http://data.iana.org/root-anchors/root-anchor
 <Zone>.</Zone>
 <KeyDigest id="Kjqmt7v" validFrom="2010-07-15T00:00:00+00:00">
  <KeyTag>19036</KeyTag>
  <Algorithm>8</Algorithm>
  <DigestType>2</DigestType>
  <Digest>
  49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
  </Digest>
 </KeyDigest>
</TrustAnchor>
```

L'élément `<KeyTag>` indique l'identifiant de la clé, actuellement 19036, comme on peut le voir avec dig :

```
% dig +multi +nodnssec DNSKEY .
...
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
.   147724 IN DNSKEY 257 3 8 (
    AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQ
    bSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh
                                ...
    ) ; KSK; alg = RSASHA256; key id = 19036
...
```

L'attribut `id` de l'élément `<KeyDigest>` sert à identifier un condensat particulier, et est utilisé pour nommer les autres fichiers. Par exemple, le certificat PKIX va se trouver dans le fichier `Kjqmt7v.crt`.

Pour produire un enregistrement DS à partir de ce fichier XML, il suffit de mettre `<KeyTag>`, `<Algorithm>`, `<DigestType>` et `<Digest>` bout à bout. Par exemple, avec le fichier XML ci-dessus, cela donnerait :

```
. IN   DS   19036  8   2  49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
```

(Des résolveurs comme Unbound acceptent ce format, pour le point de confiance de départ.)

Quant aux certificats, ils sont encodés en DER et signés par l'ICANN et leur champ `SubjectPublicKeyInfo` est la clé publique DNSSEC. Voici ce qu'en voit OpenSSL :

```
% openssl x509 -text -inform DER -in Kjqmt7v.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 7 (0x7)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=ICANN, CN=ICANN DNSSEC CA/emailAddress=dnssec@icann.org
        Validity
            Not Before: Jun 11 18:43:20 2014 GMT
            Not After : Jun 10 18:43:20 2017 GMT
        Subject: O=ICANN, OU=IANA, CN=Root Zone KSK 2010-06-16T21:19:24+00:00/1.3.6.1.4.1.1000.53=. IN DS 19036
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
     ...
            X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:8F:B2:42:69:C3:9D:E4:3C:FA:13:B9:FF:F2:C0:A4:EF:D8:0F:E8:22
            X509v3 Subject Key Identifier:
                41:1A:92:FA:1B:56:76:1E:62:2B:71:CD:1A:FD:BB:43:99:5F:09:C9
    Signature Algorithm: sha256WithRSAEncryption
    ...
```

Comment récupérer le fichier XML de manière à être sûr de son authenticité ? C'est ce que spécifie la section 3 du RFC : on utilise HTTPS. L'URL est `https://data.iana.org/root-anchors/root-anchors.xml`.

Une autre solution (section 4) est de le récupérer en HTTP et de le vérifier avec une des signatures fournies : l'une est en CMS (RFC 5652) - son URL est `https://data.iana.org/root-anchors/root-anchors.p7s`, l'autre est en PGP (RFC 9580) - son URL est `https://data.iana.org/root-anchors/root-anchors.asc`. Cette signature PGP devrait être abandonnée à l'avenir.

Pour les amateurs d'histoire, l'annexe A rappelle que la clé actuelle, la 19036, a été générée au cours d'une cérémonie à Culpeper, le 16 juin 2010. Elle a été publiée dans le DNS pour la première fois le 15 juillet 2010.

Sinon, l'ISOC a écrit un bon article sur ce RFC `<http://www.internetsociety.org/deploy360/blog/2016/09/new-rfc-7958-dnssec-trust-anchor-publication-for-the-root-zone/>`, moins technique.
