RFC 5910 : Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 mai 2010

Date de publication du RFC : Mai 2010

https://www.bortzmeyer.org/5910.html

Le protocole EPP d'avitaillement d'un registre (par exemple un registre de noms de domaine), normalisé dans le RFC 5730[1], manipule des objets qui sont des instances d'une classe (nommée "*mapping*"). Par exemple, il existe une classe (un "*mapping*") pour les noms de domaine, décrite dans le RFC 5731. Notre RFC 5910 décrit, lui, une extension EPP à ce "*mapping*" permettant de spécifier les données nécessaires à DNSSEC, notamment la clé publique d'une zone signée. Il remplace le RFC 4310 et les changements sont assez sérieux.

DNSSEC, normalisé dans le RFC 4033, utilise la même délégation que le DNS. La zone parente d'une zone signée délègue en indiquant la clé publique de sa zone fille. Plus exactement, la zone parente publie un condensat cryptographique de la clé publique de la zone fille, l'enregistrement **DS** (pour "*Delegation Signer*"), normalisé dans la section 5 du RFC 4034 (voir aussi le rappel en section 3.1 de notre RFC 5910).

Lorsqu'un bureau d'enregistrement crée un nom de domaine signé, ou bien informe le registre qu'un domaine est désormais signé, comment indique t-il ce DS ? Il y a plusieurs façons, et notre RFC propose d'utiliser EPP.

L'extension nécessaire est résumée en section 3. Elle fonctionne en ajoutant des éléments à la classe Domaine du RFC 5731. La clé peut être transmise directement, ou bien on peut envoyer le condensat cryptographique de la clé (le RFC 6781 explique pourquoi le condensat, le futur DS, devrait être obligatoire alors que la clé serait facultative, mais notre RFC ne le suis pas complètement, contrairement à son prédécesseur). Les deux méthodes, selon qu'on transmet le condensat ou la clé, sont détaillées dans la section 4. Voici un exemple d'une clé transmise sous forme d'un condensat :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5730.txt

```
   <secDNS:dsData>
     <secDNS:keyTag>12345</secDNS:keyTag>
     <secDNS:alg>3</secDNS:alg>
     <secDNS:digestType>1</secDNS:digestType>
     <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
   </secDNS:dsData>
```

Le RFC prévoit également que le registre de la zone parente peut également récupérer la clé dans le DNS (enregistrement DNSKEY) pour tester si le condensat reçu est correct (et il est donc recommandé que ladite DNSKEY soit publiée **avant** de prévenir le parent par EPP). La clé transmise au registre doit être une clé de confiance, c'est-à-dire avoir le bit SEP à 1 (cf. RFC 3757). En terminologie moderne, cette clé doit être une KSK ("*Key Signing Key*").

Les commandes EPP pour gérer cette information font l'objet de la section 5. Ainsi, les réponses à `<info>` doivent désormais contenir un élément `<secDNS:infData>`, qui contient lui-même des éléments comme `<secDNS:dsData>` qui a son tour contient les champs qu'on trouve dans un enregistrement DS comme `<secDNS:keyTag>` (un pseudo-identificateur de la clé), `<secDNS:alg>` (l'algorithme utilisé), etc. L'espace de noms `urn:ietf:params:xml:ns:secDNS-1.1` (ici avec le préfixe `secDNS`) est enregistré dans le registre IANA `<https://www.iana.org/assignments/xml-registry/ns.html>` (voir section 8). (Le nom utilisé dans le RFC 4310 était `secDNS-1.0`.) Voici un exemple de réponse à `<info>` sur le domaine `example.com` :

```
<resData>
...
<domain:name>example.com</domain:name>
...
<extension>
  <secDNS:infData
   xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
    <secDNS:dsData>
      <secDNS:keyTag>12345</secDNS:keyTag>
      <secDNS:alg>3</secDNS:alg>
      <secDNS:digestType>1</secDNS:digestType>
      <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
    </secDNS:dsData>
  </secDNS:infData>
</extension>
```

Le condensat est de type SHA1 (`<digestType>1</digestType>`), la clé elle-même étant DSA/SHA1 (`<alg>3</alg>`).

L'extension DNSSEC permet évidemment de créer un domaine signé, avec `<create>` (section 3.2.1) :

```
<domain:create>
  <domain:name>example.com</domain:name>
  ...
  <extension>
  <secDNS:create xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
  <secDNS:dsData>
    <secDNS:keyTag>12345</secDNS:keyTag>
    <secDNS:alg>3</secDNS:alg>
    <secDNS:digestType>1</secDNS:digestType>
```

```
    <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
    <!-- <secDNS:keyData>, la clé elle-même, est *facultatif* -->
  </secDNS:dsData>
</secDNS:create>
 ...
```

Une fois le domaine ainsi créé, le registre publiera typiquement un enregistrement DS comme :

```
example.com.  IN DS 12345 3 1 49FD46E6C4B45C55D4AC
```

Bien sûr, on peut aussi ajouter DNSSEC à un domaine existant, ou bien changer une clé existante. Cela se fait avec `<update>` :

```
    <domain:update>
        <domain:name>example.com</domain:name>
    ...
    <extension>
      <secDNS:update
       xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
        <secDNS:add>
          <secDNS:dsData>
            <secDNS:keyTag>12346</secDNS:keyTag>
            <secDNS:alg>3</secDNS:alg>
            <secDNS:digestType>1</secDNS:digestType>
            <secDNS:digest>38EC35D5B3A34B44C39B</secDNS:digest>
            <!-- <secDNS:keyData>, la clé elle-même, est *facultatif* -->
          </secDNS:dsData>
        </secDNS:add>
      </secDNS:update>
     ...
```

Et, en utilisant `<secDNS:rem>` au lieu de `<secDNS:add>`, on peut retirer une délégation sécurisée (« dé-signer » le domaine).

Comme la grande majorité des extensions et "*mappings*" d'EPP, celle-ci est spécifiée en utilisant la syntaxe formelle des W3C schemas, ici en section 4.

Le premier RFC sur cette extension EPP était le RFC 4310. Les sections 2 et 4 sont entièrement nouvelles. La première décrit les mécanismes de migration pour ceux qui avaient déjà déployé le précedent RFC. La section 4 décrit la nouvelle interface pour les clés. Le nouveau RFC était nécessaire en raison d'une bogue dans le précédent : lors de la suppression d'une délégation signée, le RFC 4310 disait (dans sa section 3.2.5) que la délégation pouvait être indiquée par le "*key tag*" (section 5.1.1 du RFC 4034) or celui-ci, un simple condensat cryptographique de la clé, n'est pas forcément unique, vue sa faible taille. La section 5.2.5 contient le nouveau texte. Parmi les autres changements, l'introduction du concept de "*data interface*" (section 4), qui unifie la façon de passer les clés (ou leurs condensats) du client EPP au serveur. Il y a enfin quelques changements moins cruciaux, décrits dans l'annexe A.

À noter que la mise en œuvre EPP du registre brésilien inclus désormais notre RFC 5910 : `<http://registro.br/epp/download-EN.html>`.