

RFC 9038 : Extensible Provisioning Protocol (EPP) Unhandled Namespaces

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 mai 2021

Date de publication du RFC : Mai 2021

<https://www.bortzmeyer.org/9038.html>

Le protocole EPP, qui sert notamment lors de la communication entre un registre (par exemple de noms de domaine) et son client, est extensible : on peut rajouter de nouveaux types d'objets et de nouvelles informations. Normalement, le serveur EPP n'envoie au client ces nouveautés que si le client a annoncé, lors de la connexion, qu'il savait les gérer. Et s'il ne l'a pas fait, que faire de ces données, ces *"unhandled namespaces"* ? Ce nouveau RFC propose de les envoyer quand même, mais dans un élément XML prévu pour des informations supplémentaires, et qui ne devrait donc rien casser chez le client.

Le but est de rester compatible avec l'EPP standard, tel que normalisé dans le RFC 5730¹. Prenons l'exemple de l'extension pour DNSSEC du RFC 5910. Comme toutes les extensions EPP, elle utilise les espaces de noms XML. Cette extension particulière est identifiée par l'espace de noms `urn:ietf:params:xml:ns:secDNS`. À l'établissement de la connexion, le serveur annonce les extensions connues :

```
<greeting
  <svcMenu>
    ...
    <svcExtension>
      <extURI>urn:ietf:params:xml:ns:secDNS-1.1</ns0:extURI>
```

Et le client annonce ce qu'il sait gérer :

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

```

<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <login>
  ...
    <svcs>
      <svcExtension><extURI>urn:ietf:params:xml:ns:secDNS-1.1</extURI></svcExtension>
  ...

```

(<svcExtension> est décrit dans le RFC 5730, sections 2.4 et 2.9.1.1). Ici, le serveur a annoncé l'extension DNSSEC et le client l'a acceptée. Tout le monde va donc pouvoir envoyer et recevoir des messages spécifiques à cette extension, comme l'ajout d'une clé :

```

<extension>
  <update xmlns="urn:ietf:params:xml:ns:secDNS-1.1">
    <add xmlns="urn:ietf:params:xml:ns:secDNS-1.1">
      <dsData xmlns="urn:ietf:params:xml:ns:secDNS-1.1">
        ...
        <digest xmlns="urn:ietf:params:xml:ns:secDNS-1.1">076CF6DA3692EFE72434EA1322177A7F07023400E4D...
      ...

```

Mais, si le client ne gère pas une extension (et ne l'a donc pas indiquée dans son <login>), que peut faire le serveur s'il a quand même besoin d'envoyer des messages spécifiques à cette extension inconnue du client, ce "*unhandled namespace*" ? C'est particulièrement important pour la messagerie EPP (commande <poll>) puisque le serveur peut, par exemple, mettre un message dans la boîte sans connaître les capacités du client, mais cela peut affecter également d'autres activités.

La solution de notre RFC est d'utiliser un élément EPP déjà normalisé (RFC 5730, section 2.6), <extValue>, qui permet d'ajouter des informations que le client ne pourra pas analyser automatiquement, comme par exemple un message d'erreur lorsque le serveur n'a pas pu exécuter l'opération demandée. Notre RFC étend cet <extValue> au cas des espaces de noms non gérés. Le sous-élément <value> contiendra l'élément XML appartenant à l'espace de noms que le client ne sait pas gérer, et le sous-élément <reason> aura comme contenu un message d'information dont la forme recommandée est NAMESPACE-URI not in login services où NAMESPACE-URI est le "*unhandled namespace*". Par exemple, le RFC cite un cas où le registre ne gère pas l'extension DNSSEC du RFC 5910 et répond :

```

<response>
  ...
  <extValue>
    <value>
      <secDNS:infData
        xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
        <secDNS:dsData>
          ...
          <secDNS:digest>49FD46E6C4B45C55D4AC</secDNS:digest>
        </secDNS:dsData>
      </secDNS:infData>
    </value>
    <reason>
      urn:ietf:params:xml:ns:secDNS-1.1 not in login services
    </reason>
  </extValue>

```

(Le RFC a aussi un autre exemple, avec l'extension de rédemption du RFC 3915.)

Ce RFC ne change pas le protocole EPP : il ne fait que décrire une pratique, compatible avec les clients actuels, pour leur donner le plus d'informations possible. Toutefois, pour informer tout le monde, cette pratique fait l'objet elle-même d'une extension, `urn:ietf:params:xml:ns:epp:unhandled-namespaces-1.0`, que le serveur va inclure dans son `<greeting>` et que le client mettra dans sa liste d'extensions acceptées. (Cet espace de nom a été mis dans le registre IANA `<https://www.iana.org/assignments/xml-registry/xml-registry.xml#ns>` créé par le RFC 3688. L'extension a été ajoutée au registre des extensions EPP `<https://www.iana.org/assignments/epp-extensions/epp-extensions.xml#epp-extensions-1>` introduit par le RFC 7451.) De toute façon, le client a tout intérêt à inclure dans sa liste toutes les extensions qu'il gère **et** à regarder s'il y a des `<extValue>` dans les réponses qu'il reçoit (même si la commande EPP a été un succès); cela peut donner des idées aux développeurs sur des extensions supplémentaires qu'il serait bon de gérer. Quant au serveur, il est bon que son administrateur regarde s'il y a eu des réponses pour des *"unhandled namespaces"* et prenne ensuite contact avec l'administrateur du client pour lui signaler ce manque.

Notez que ce RFC s'applique aux extensions portant sur les objets manipulés en EPP (par exemple les noms de domaine) et à celles portant sur les séquences de commandes et de réponses EPP, mais pas aux extensions portant sur le protocole lui-même (cf. RFC 3735).

Question mises en œuvre de ce RFC, le SDK de Verisign inclut le code nécessaire `<https://www.verisign.com/en_US/channel-resources/domain-registry-products/epp-sdks/index.xhtml>` (dans le fichier `gen/java/com/verisign/epp/codec/gen/EPPFullExtValuePollMessageFilter.java`). D'autre part, le registre du `.ch` utilise ce concept d'espaces de noms inconnus pour indiquer au BE les changements d'un domaine provoqués par l'utilisation du CDS du RFC 7344, puisque ces changements ne sont pas passés par EPP.