

RFC 8544 : Organization Extension for the Extensible Provisioning Protocol (EPP)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 avril 2019

Date de publication du RFC : Avril 2019

<https://www.bortzmeyer.org/8544.html>

Le RFC 8543¹ étendait le format utilisé par le protocole d'avitaillement EPP, afin d'ajouter le concept d'« organisation », une entreprise, association ou agence qui joue un rôle dans la création et gestion d'objets enregistrés, notamment les noms de domaine. Ce RFC 8544 ajoute une extension au protocole EPP pour affecter ces organisations à un domaine, contact ou autre objet enregistré.

Prenons l'exemple le plus connu (quoique EPP puisse servir à d'autres), celui de l'industrie des noms de domaine. Souvent, le registre reçoit des demandes d'un BE, via le protocole EPP. Mais d'autres organisations peuvent jouer un rôle, en plus du BE. Il y a par exemple l'hébergeur DNS (qui n'est pas forcément le BE) ou bien un revendeur du BE, ou bien un « anonymisateur » qui, pour protéger la vie privée des participants, est placé entre le participant et le monde extérieur. Ces différents acteurs (cf. RFC 8499, section 9, pour la terminologie) sont décrits par les nouvelles classes d'objets du RFC 8543. Notre RFC 8544 permet d'utiliser ces classes. Une fois les objets « organisation » créés au registre, on peut les attacher à un nom de domaine ou à un contact, par exemple pour dire « ce nom de domaine a été acheté via le revendeur X ».

L'espace de noms XML est `urn:ietf:params:xml:ns:epp:orgext-1.0` (et est enregistré dans le registre IANA <<https://www.iana.org/assignments/xml-registry/xml-registry.xml#schema>>). L'extension à EPP est notée dans le registre des extensions EPP <<https://www.iana.org/assignments/epp-extensions/epp-extensions.xml>>. Dans les exemples qui suivent, l'espace de noms est abrégé `orgext`. Les organisations ont un identificateur (le `<org:id>` du RFC 8543), et cet identificateur sera un attribut `<orgext:id>` des objets comme par exemple le domaine. Pour chaque rôle (revendeur, hébergeur DNS, etc, cf. RFC 8543, section 7.3), le domaine a au plus un attribut identifiant une organisation.

La section 4 du RFC décrit les ajouts aux commandes et réponses EPP. Par exemple, pour `<info>`, la commande ne change pas mais la réponse a désormais en plus des attributs `<orgext:id>`. Voici un exemple :

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc8543.txt>

```

<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <response>
    <result code="1000">
      <msg lang="en-US">Command completed successfully</msg>
    </result>
    <resData>
      <domain:infData
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>example.com</domain:name>
        ...
      </resData>
    <extension>
      <orgext:infData
        xmlns:orgext="urn:ietf:params:xml:ns:epp:orgext-1.0">
        <orgext:id role="reseller">reseller1523</orgext:id>
        <orgext:id role="privacyproxy">proxy2935</orgext:id>
      </orgext:infData>
    </extension>
    <trID>
      <clTRID>ngcl-IvJjzMZc</clTRID>
      <svTRID>test142AWQONJZ</svTRID>
    </trID>
  </response>
</epp>

```

Ici, le domaine a été avitaillé via le revendeur « reseller1523 » et est protégé par l'« anonymisateur » « proxy2935 ».

Bien sûr, la commande EPP <create> est également modifiée, pour pouvoir créer un domaine avec les organisations associées. Ici, le revendeur « reseller1523 » crée un domaine :

```

<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <create>
      <domain:create
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>example.com</domain:name>
        <domain:period unit="y">3</domain:period>
        ...
      </create>
    <extension>
      <orgext:create
        xmlns:orgext="urn:ietf:params:xml:ns:epp:orgext-1.0">
        <orgext:id role="reseller">reseller1523</orgext:id>
      </orgext:create>
    </extension>
  </command>
</epp>

```

De la même façon, on peut mettre à jour les organisations associées à un objet, avec <update>. Ici, on ajoute un « anonymiseur » :

```

<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>

```

```
<update>
  <domain:update
    xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
    <domain:name>example.com</domain:name>
  </domain:update>
</update>
<extension>
  <orgext:update
    xmlns:orgext="urn:ietf:params:xml:ns:epp:orgext-1.0">
    <orgext:add>
      <orgext:id role="privacyproxy">proxy2935</orgext:id>
    </orgext:add>
  </orgext:update>
</extension>
</command>
</epp>
```

Et ici on retire le revendeur (pas besoin d'indiquer son identificateur, rappelez-vous qu'il ne peut y avoir qu'une seule organisation par rôle) :

```
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <update>
      <domain:update
        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name>example.com</domain:name>
      </domain:update>
    </update>
    <extension>
      <orgext:update
        xmlns:orgext="urn:ietf:params:xml:ns:epp:orgext-1.0">
        <orgext:rem>
          <orgext:id role="reseller"/>
        </orgext:rem>
      </orgext:update>
    </extension>
  </command>
</epp>
```

La syntaxe complète (au format XML Schema) figure dans la section 5 du RFC.

Question mise en œuvre, cette extension est dans le SDK de Verisign, accessible avec leurs autres logiciels pour registres <https://www.verisign.com/en_US/channel-resources/domain-registry-products/epp-sdks>. CNNIC a également inclus cette extension, dans leur code interne.