RFC 8543 : Extensible Provisioning Protocol (EPP) Organization Mapping

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 avril 2019

Date de publication du RFC : Mars 2019

https://www.bortzmeyer.org/8543.html

L'industrie des noms de domaine est d'une grande complexité. Les utilisateurs s'y perdent facilement entre registres, bureaux d'enregistrement, hébergeurs DNS, revendeurs divers, sociétés qui développent des sites Web, prête-noms pour protéger la vie privée, etc. Cette complexité fait qu'il est difficile de savoir qui est responsable de quoi. Dans le contexte d'EPP, protocole d'**avitaillement** de noms de domaine (création, modification, suppression de noms), il n'y avait jusqu'à présent pas de moyen de décrire ces acteurs. Par exemple, l'ajout d'un enregistrement DS dépend d'actions de l'hébergeur DNS, qui n'est pas forcément le BE. Mais ces hébergeurs DNS n'étaient pas définis et connus. Désormais, avec ce nouveau RFC, on peut utiliser EPP pour l'avitaillement d'objets « organisation ».

EPP (RFC 5730[1]) est le protocole standard d'avitaillement de noms de domaine, permettant à un **client** (en général le BE) de créer des **objets** dans un **registre**, en parlant au serveur EPP. EPP permettait déjà des objets de type « contact » RFC 5733, identifiant les personnes ou les organisations qui assuraient certaines fonctions pour un nom de domaine. Par exemple, le contact technique était la personne ou l'organisation à contacter en cas de problème technique avec le nom de domaine.

Désormais, avec notre nouveau RFC 8543, une nouvelle catégorie ("*mapping*") d'objets est créée, les organisations. On peut ainsi utiliser EPP pour enregistrer l'hébergeur DNS d'un domaine (qui peut être le titulaire du domaine, mais ce n'est pas toujours le cas, ou qui peut être le BE, mais ce n'est pas systématique). Ce nouveau RFC décrit donc une extension à EPP, qui figure désormais dans le registre des extensions <https://www.iana.org/assignments/epp-extensions/epp-extensions.xml> (cf. RFC 7451).

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 utilise XML et tout ici va donc être spécifié en XML, avec un nouvel espace de noms XML, `urn:ietf:params:xml:ns:epp:org-1.0`, abrégé en `org` dans le RFC (mais rappelez-vous que le vrai identificateur d'un espace de noms XML est l'URI, pas l'abréviation). Le nouvel espace de noms est désormais dans le registre des espaces de noms `<https://www.iana.org/assignments/xml-registry/xml-registry.xml#schema>`.

La section 3 de notre RFC décrit les attributs d'une organisation (notez que le vocabulaire est trompeur : ils s'appellent attributs mais ne sont pas des attributs XML). Mais commençons par un exemple, décrivant le BE nommé « Example Registrar Inc. » :

```
<org:infData
    xmlns:org="urn:ietf:params:xml:ns:epp:org-1.0">
    <org:id>registrar1362</org:id>
    <org:roid>registrar1362-REP</org:roid>
    <org:role>
      <org:type>registrar</org:type>
      <org:status>ok</org:status>
      <org:status>linked</org:status>
      <org:roleID>1362</org:roleID>
    </org:role>
    <org:status>ok</org:status>
    <org:postalInfo type="int">
      <org:name>Example Registrar Inc.</org:name>
      <org:addr>
        <org:street>123 Example Dr.</org:street>
        <org:city>Dulles</org:city>
        <org:sp>VA</org:sp>
        <org:cc>US</org:cc>
      </org:addr>
    </org:postalInfo>
    <org:voice x="1234">+1.7035555555</org:voice>
    <org:email>contact@organization.example</org:email>
    <org:url>https://organization.example</org:url>
    <org:contact type="admin">sh8013</org:contact>
    <org:contact type="billing">sh8013</org:contact>
    <org:contact type="custom"
       typeName="legal">sh8013</org:contact>
    <org:crID>ClientX</org:crID>
    <org:crDate>1999-04-03T22:00:00.0Z</org:crDate>
    <org:upID>ClientX</org:upID>
    <org:upDate>1999-12-03T09:00:00.0Z</org:upDate>
</org:infData>
```

Voyons maintenant quelques-uns des attributs possibles.

Une organisation a un **identificateur**, indiqué par l'élément XML `<org:id>`, attribué par le registre (c'est `registrar1362` dans l'exemple). Il a aussi un ou plusieurs **rôles**, dans l'élement XML `<org:role>`. Un même acteur peut avoir plusieurs rôles (par exemple il est fréquent que les BE soient également hébergeurs DNS). Le rôle inclut un **type**, qui peut valoir :

- `registrar` : BE, comme dans le cas ci-dessus,
- `reseller` : revendeur, par exemple l'organisation à laquelle le titulaire du nom de domaine achète un domaine n'est pas toujours un « vrai » BE, ce peut être un revendeur,
- `privacyproxy` : un prête-nom qui, en se mettant devant l'utilisateur, permet de protéger sa vie privée,
- et enfin `dns-operator`, l'hébergeur DNS.

D'autres types pourront apparaitre dans le futur, ils sont indiqués dans un registre IANA <https://www.iana.org/assignments/epp-extension-role-values/epp-extension-role-values.xml#epp-extension-role-values-1>, des nouveaux types seront ajoutés en suivant la procédure « Examen par un expert » du RFC 8126.

Notez qu'au début du travail à l'IETF sur cette extension, seul le cas des revendeurs était prévu. Après des discussions sur l'importance relative des différents acteurs, il a été décidé de prévoir d'autres types que les seuls revendeurs.

Il y a aussi dans l'objet un ou plusieurs état(s), <org:status>, qui peut valoir notamment :

— ok, l'état normal, celui du BE dans l'exemple ci-dessus,
— terminated, quand l'organisation va être retirée de la base et ne peut plus être utilisée (c'est le cas d'un BE qui n'est plus accrédité),
— linked, qui indique que cette organisation est liée à d'autres objets, et ne doit donc pas être supprimée.

Il existe également un attribut <org:parent>, qui indique une relation avec une autre organisation. Par exemple, un revendeur aura une relation <org:parent> vers le BE dont il est revendeur. (Dans l'exemple plus haut, il n'y a pas de <org:parent>.)

La section 4 du RFC présente ensuite les commandes EPP qui peuvent être appliquées à ces objets « organisation ». <check> permet au client EPP de savoir s'il pourra créer un objet, <info> lui donnera les moyens de s'informer sur une oranisation (l'exemple en XML ci-dessus était le résultat d'une commande EPP <info>) et bien sûr une commande <create> et une <delete>. Voici <create> en action, pour créer un objet de rôle « revendeur » (notez que, cette fois, il a un parent) :

```
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <create>
      <org:create
        xmlns:org="urn:ietf:params:xml:ns:epp:org-1.0">
        <org:id>res1523</org:id>
        <org:role>
          <org:type>reseller</org:type>
        </org:role>
        <org:parentId>1523res</org:parentId>
        <org:postalInfo type="int">
          <org:name>Example Organization Inc.</org:name>
          <org:addr>
            <org:street>123 Example Dr.</org:street>
            <org:city>Dulles</org:city>
            <org:sp>VA</org:sp>
            <org:cc>US</org:cc>
          </org:addr>
        </org:postalInfo>
        <org:voice x="1234">+1.7035555555</org:voice>
        <org:email>contact@organization.example</org:email>
        <org:url>https://organization.example</org:url>
        <org:contact type="admin">sh8013</org:contact>
        <org:contact type="billing">sh8013</org:contact>
      </org:create>
    </create>
  </command>
</epp>
```

Le schéma complet, en syntaxe XML Schema, figure dans la section 5 du RFC.

Question mise en œuvre de cette extension EPP, Verisign l'a ajouté dans son SDK, disponible en ligne <https://www.verisign.com/en_US/channel-resources/domain-registry-products/epp-sdks>. CNNIC a une implémentation, mais non publique.