# RFC 6493 : The RPKI Ghostbusters Record

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 février 2012

Date de publication du RFC : Février 2012

https://www.bortzmeyer.org/6493.html

---

Les certificats de la RPKI, qui permettent de sécuriser le routage sur l'Internet <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html> en prouvant un droit à utiliser telle ou telle adresse IP, ne portent pas en clair de nom de titulaire. Cela peut être un problème dans certains cas opérationnels. Par exemple, une route reçue en BGP est refusée par le routeur, l'administrateur réseaux enquête, découvre un certificat qui a expiré, et voudrait prévenir le responsable qu'il a fait une boulette. Mais comment trouver le responsable ? Ou, selon la phrase culte du film "*Ghostbusters*", « "*Who you gonna call ?*" ». Ce RFC résout le problème en permettant de mettre une vCard dans le certificat, indiquant qui contacter en cas de problème.

Il n'y a guère de doute que ce genre de problèmes sera fréquent. La RPKI permet de distribuer des certificats numériques disant « le titulaire de la clé privée de ce certificat est responsable du préfixe IP 2001:db8:137::/48 ». Ce certificat est ensuite utilisé pour signer les ROA ("*Route Origin Authorization*") qui indiquent quel AS peut annoncer ce préfixe. Si on se fie à l'expérience du déploiement d'autres technologies à base de cryptographie dans l'Internet (par exemple DNSSEC), il y aura des problèmes : préfixes trop génériques, interdisant des annonces plus spécifiques, certificats expirés, oubli de créer un nouvel ROA lorsqu'on contracte avec un nouveau transitaire BGP, etc. Ceux et celles qui détecteront les problèmes auront donc besoin de contacter les responsables, dans l'espoir qu'ils agissent.

Or, les métadonnées dans les certificats de la RPKI ne contiennent pas d'identificateurs utilisables par les humains (cf. RFC 6484 [1]). D'où l'idée de ce RFC, de mettre une vCard (plus exactement un profil restrictif des vCards du RFC 6350) dans un objet RPKI signé (la description de la syntaxe générique de ces objets est dans le RFC 6488).

Arrivé à ce stade, vous vous demandez peut-être « pourquoi un nouveau format au lieu d'utiliser les données des RIR, telles que publiées via whois ? ». La réponse est que l'enregistrement "*Ghostbusters*"

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6484.txt

identifie le responsable du certificat, qui n'est pas forcément le même que celui de la ressource (adresse IP ou numéro d'AS). Et puis, en pratique, les bases des RIR ne sont pas toujours correctes. Comme le chemin de mise à jour de l'enregistrement "*Ghostbuster*" est différent, peut-être sera-t-il parfois correct lorsque la base du RIR ne le sera pas ?

De toute façon, l'enregistrement "*Ghostbuster*" est facultatif. Un certificat peut en avoir zéro, un ou davantage. La section 3 du RFC fournit un exemple :

```
BEGIN:VCARD
VERSION:4.0
FN:Human's Name
ORG:Organizational Entity
ADR;TYPE=WORK:;;42 Twisty Passage;Deep Cavern;WA;98666;U.S.A.
TEL;TYPE=VOICE,TEXT,WORK;VALUE=uri:tel:+1-666-555-1212
TEL;TYPE=FAX,WORK;VALUE=uri:tel:+1-666-555-1213
EMAIL:human@example.com
END:VCARD
```

En fait, cette vCard est embarquée dans un objet de la RPKI, qu'on peut lire avec des outils comme openssl. Voici un exemple sur un objet réel :

```
%  openssl asn1parse -inform DER \
         -in b-hiK-PPLhH4jThJ700WoJ3z0Q8.gbr
...
   60:d=5  hl=3 l= 139 prim: OCTET STRING      :BEGIN:VCARD
VERSION:3.0
EMAIL:michael.elkins@cobham.com
FN:Michael Elkins
N:Elkins;Michael;;;
ORG:Cobham Analytic Solutions
END:VCARD
...
```

Ce n'est évidemment pas très convivial comme moyen d'y accéder mais il semble que la boîte à outils RPKI du RIPE-NCC ne permet pas de les afficher mieux. Idem pour la suite rcynic. (Voir mon article sur les outils RPKI <https://www.bortzmeyer.org/rpki-tests.html>.)

Le sous-ensemble de vCard qui est accepté dans les chasseurs de fantômes est décrit en section 4. La définition est très restrictive : ne sont acceptées que les propriétés `VERSION` (qui doit valoir au moins 4, vous noterez que les enregistrements réels cités plus haut sont donc illégaux), `FN`, `ORG`, `ADR`, `TEL` et `EMAIL` (un enregistrement qui inclus `N`, comme ci-dessus, est donc illégal).

Ensuite (section 5), la vCard est embarquée dans un objet CMS signé (RFC 6488 ; la validation de ces enregistrements se fait de la même façon que pour les autres objets de la RPKI). Le type (OID) est 1.2.840.113549.1.9.16.1.35, ce qu'on voit dans la sortie d'`openssl` :

```
% openssl asn1parse -inform DER \
     -in owCgRbSAAkKS9W-MFbSAd7Bru2c.gbr
...
   44:d=4  hl=2 l=  11 prim: OBJECT            :1.2.840.113549.1.9.16.1.35
   57:d=4  hl=3 l= 195 cons: cont [ 0 ]
   60:d=5  hl=3 l= 192 prim: OCTET STRING      :BEGIN:VCARD
VERSION:3.0
ADR:;;5147 Crystal Springs;Bainbridge Island;Washington;98110;US
EMAIL:randy@psg.com
FN:Randy Bush
N:Bush;Randy;;;
ORG:RGnet\, LLC
TEL:+1 206 356 8341
END:VCARD
```

L'objet CMS est enfin mis dans un fichier d'extension <https://www.iana.org/assignments/rpki/rpki.xml#name-schemes> .gbr. Fin 2011, on n'en trouvait que très peu dans les dépôts de la RPKI.

Attention, toutes ces données sont publiques. Comme le rappelle la section 8, sur la sécurité, publier ses informations dans un enregistrement "*Ghostbuster*" et vous risquez d'être harcelé par des commerciaux au téléphone ou bien spammé.

D'autre part, l'entité qui signe l'objet ne garantit nullement que les informations sont correctes. Elle garantit juste que ces informations ont bien été mises par le titulaire de la ressource (préfixe IP ou AS) correspondante. Celui-ci a pu mettre un numéro de téléphone ou une adresse de courrier bidon...