RFC 9255 : The 'I' in RPKI Does Not Stand for Identity

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 juin 2022

Date de publication du RFC : Juin 2022

https://www.bortzmeyer.org/9255.html

Un très court RFC pour un simple rappel, qui ne devrait même pas être nécessaire : les identités utilisées dans la RPKI, la base des identités qui sert aux techniques de sécurisation de BGP, n'ont pas de lien avec les identités attribuées par l'État et ne doivent pas être utilisées pour, par exemple, signer des documents « officiels » ou des contrats commerciaux.

Le RFC 6480 [1] décrit cette RPKI : il s'agit d'un ensemble de certificats et de signatures qui servent de base pour des techniques de sécurité du routage comme les ROA du RFC 6482 ou comme le BGPsec du RFC 8205. Les objets de la RPKI servent à établir l'autorité sur des ressources Internet (INR, "*Internet Number Resources*", comme les adresses IP et les numéros d'AS). Le RFC 6480, section 2.1, dit clairement que cela ne va pas au-delà et que la RPKI ne prétend pas être **la** source d'identité de l'Internet, ni même une source « officielle ».

Prenons un exemple concret, un certificat choisi au hasard dans les données du RIPE-NCC (qu'on peut récupérer avec rsync en `rsync://rpki.ripe.net/repository`). Il est au format DER donc ouvrons-le :

```
%  openssl x509 -inform DER -text -in  ./DEFAULT/ztLYANxsM7afpHKR4vFbM16jYA8.cer
Certificate:
    Data:
        ...
        Serial Number: 724816122963 (0xa8c2685453)
        Validity
            Not Before: Jan  1 14:04:04 2022 GMT
            Not After : Jul  1 00:00:00 2023 GMT
        Subject: CN = ced2d800dc6c33b69fa47291e2f15b335ea3600f
...
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6480.txt`

```
X509v3 extensions:
    ...
    sbgp-ipAddrBlock: critical
        IPv4:
          51.33.0.0/16
          ...
    sbgp-autonomousSysNum: critical
        Autonomous System Numbers:
          206918
          ...
```

Je n'ai pas tout montré, mais seulement les choses importantes :

— Il n'y a pas de vraie identité dedans, le sujet a manifestement été généré automatiquement,
— Il couvre un certain nombre de ressources (INR, "*Internet Number Resources*"), comme le préfixe IP `51.33.0.0/16`, utilisant les extensions du RFC 3779.

Ce certificat dit simplement que l'entité qui a la clé privée (RFC 5280) correspondante (une administration britannique, dans ce cas) a autorité sur des ressources comme l'AS 206918. Rien d'autre.

Mais, apparemment, certaines personnes n'avaient pas bien lu le RFC 6480 et croyaient que cet attirail PKIesque leur permettait également de signer des documents sans lien avec les buts de la RPKI, voire n'ayant rien à voir avec le routage. Et d'autant plus que des gens croient que le I dans RPKI veut dire "*Identity*" (il veut en fait dire "*Infrastructure*"). Il a ainsi été suggéré que les clés de la RPKI pouvaient être utilisées pour signer des LOA demandant l'installation d'un serveur dans une baie.

Pourquoi est-ce que cela serait une mauvaise idée ? Il y a plusieurs raisons mais la principale est qu'utiliser la RPKI pour des usages en dehors du monde restreint du routage Internet est que cela exposerait les AC de cette RPKI à des risques juridiques qu'elles n'ont aucune envie d'assumer. Et cela compliquerait les choses, obligeant sans doute ces AC à déployer des processus bureaucratiques bien plus rigides. Si on veut connaitre l'identité officielle (que le RFC nomme à tort « identité dans le monde réel ») d'un titulaire de ressources Internet, on a les bases des RIR, qu'on interroge via RDAP ou autres protocoles. (C'est ainsi que j'ai trouvé le titulaire de `51.33.0.0/16`.) Bien sûr, il y a les enregistrements "*Ghostbusters*" du RFC 6493 mais ils sont uniquement là pour aider à trouver un contact opérationnel, pas pour indiquer l'identité étatique du titulaire. Même les numéros d'AS ne sont pas l'« identité » d'un acteur de l'Internet (certains en ont plusieurs).

Notons qu'il y a d'autres problèmes avec l'idée de se servir de la RPKI pour signer des documents à valeur légale. Par exemple, dans beaucoup de grandes organisations, ce ne sont pas les mêmes personnes qui gèrent le routage et qui gèrent les commandes aux fournisseurs. Et, au RIPE-NCC, les clés privées sont souvent hébergées par le RIPE-NCC, pas par les titulaires, et le RIPE-NCC n'a évidemment pas le droit de s'en servir pour autre chose que le routage.

Bref, n'utilisez pas la RPKI pour autre chose que ce pour quoi elle a été conçue.