RFC 6482 : A Profile for Route Origin Authorizations (ROAs)

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/6482.html

Un nouveau sigle va devoir être appris par les administrateurs réseaux et sera sans doute souvent prononcé dans les discussions sur les listes de diffusion d'opérateurs : **ROA**, pour "*Route Origin Authorizations*", ces objets signés cryptographiquement qui permettent à un routeur BGP de valider l'origine d'une route. Dans la très longue liste des RFC décrivant ce système de sécurité <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>, notre court RFC 6482 [1] décrit le format des ROA.

Ces **ROA** ("*Route Origin Authorizations*") sont, à bien des égards, le cœur du système de sécurisation du routage de l'Internet (dont l'architecture générale est décrite dans le RFC 6480). Ils expriment des autorisations d'annonce, par exemple « L'AS 64641 est autorisé à annoncer le préfixe 192.0.2.0/24 » et sont signés par le titulaire de la ressource (ici, le titulaire du préfixe 192.0.2.0/24).

Le format des ROA est tiré de la norme CMS (RFC 5652), précisée par le profil générique des objets de la RPKI, dans le RFC 6488. Ce dernier RFC précise, dans sa section 4, les points spécifiques à normaliser pour chaque classe d'objets de la RPKI. Dans le cas des ROA, ces blancs sont remplis ainsi :

— L'OID de la classe « ROA » est 1.2.840.113549.1.9.16.1.24 (section 2),
— Le contenu du ROA est composé (section 3) d'un numéro d'AS (celui qui est autorisé à être à l'origine de la route) et d'un ou plusieurs préfixes IP (un seul dans l'exemple plus haut), qui sont les préfixes où cet AS peut être à l'origine,
— Des règles de validation spécifiques au ROA sont indiquées (section 4).

Le contenu précis, tel qu'indiqué dans la section 3, est, en ASN.1 :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6482.txt

```
RouteOriginAttestation ::= SEQUENCE {
   version [0] INTEGER DEFAULT 0,
   asID  ASID,
   ipAddrBlocks SEQUENCE (SIZE(1..MAX)) OF ROAIPAddressFamily }
```

où `asID` est le numéro d'AS, et `ipAddrBlocks` la liste des préfixes. Les `ROAIPAddressFamily` sont composées de `ROAIPAddress` et celles-ci ont un attribut intéressant, `maxLength`, qui indique la longueur maximale des sous-préfixes que peut annoncer cet AS. Par exemple, en IPv6, un `maxLength` de 56 indiquera qu'on peut annoncer un /56 mais pas un /60. L'autre attribut d'une `ROAIPAddress` est le préfixe, représenté selon les règles du RFC 3779.

La section 4 décrit quant à elle les règles de validation spécifiques aux ROA : aux règles génériques des objets de la RPKI, elle ajoute l'obligation de vérifier que les adresses indiquées dans le ROA figurent bien dans le certificat signataire (c'est-à-dire que c'est bien le titulaire des adresses qui a émis le ROA). Mais il vaut mieux consulter le RFC 6483 pour avoir tous les détails.

À noter qu'on ne peut mettre qu'une seule signature par ROA. Une des vives discussions du groupe de travail SIDR `<http://tools.ietf.org/wg/sidr>` avait porté sur la possibilité de signatures multiples, afin de gérer certaines relations complexes entre clients et opérateurs, mais cela avait finalement été rejeté.

On peut récupérer tous les ROA des préfixes RIPE en `<https://certification.ripe.net/certification/public/all-roas>`. Si on en télécharge un, on peut afficher ce contenu avec l'outil du même RIPE-NCC :

```
% certification-validator  --print -f  roa-5574190.roa
Content type: 1.2.840.113549.1.9.16.1.24
Signing time: 2011-01-11T19:04:18.000Z
ASN: AS559
Prefixes:
    193.5.26.0/23 [24]
    193.5.152.0/22 [24]
    193.5.168.0/22 [24]
    193.5.22.0/24
    193.5.54.0/23 [24]
    193.5.58.0/24
    193.5.60.0/24
    193.5.80.0/21 [24]
```

ou bien avec l'outil de l'ARIN, rcynic :

```
% print_roa /home/bortzmeyer/tmp/roa-5574190.roa
Certificates:   1
CRLs:           0
SignerId[0]:    b6:6f:5a:10:d5:7f:ed:6d:b1:62:96:2c:cb:92:35:bb:5d:f8:c3:ca [Matches certificate 0] [signing
eContentType:   1.2.840.113549.1.9.16.1.24
version:        0 [Defaulted]
asID:           559
 addressFamily: 1
     IPaddress: 193.5.26.0/23-24
     IPaddress: 193.5.152.0/22-24
     IPaddress: 193.5.168.0/22-24
     IPaddress: 193.5.22.0/24
     IPaddress: 193.5.54.0/23-24
     IPaddress: 193.5.58.0/24
     IPaddress: 193.5.60.0/24
     IPaddress: 193.5.80.0/21-24
```

Comme les ROA sont en CMS, on peut aussi tenter sa chance avec des logiciels qui traitent du CMS générique. Ils ne comprendront pas tout mais pourront au moins afficher une partie de la structure :

```
% openssl asn1parse -inform DER -in RFZr0zO7xjc1bNCEVboVjI8JZlw.roa
    0:d=0  hl=2 l=inf  cons: SEQUENCE
    2:d=1  hl=2 l=   9 prim: OBJECT            :pkcs7-signedData
...
 1340:d=7  hl=2 l=   9 prim: OBJECT            :contentType
 1351:d=7  hl=2 l=  13 cons: SET
 1353:d=8  hl=2 l=  11 prim: OBJECT            :1.2.840.113549.1.9.16.1.24
 1366:d=6  hl=2 l=  28 cons: SEQUENCE
 1368:d=7  hl=2 l=   9 prim: OBJECT            :signingTime
 1379:d=7  hl=2 l=  15 cons: SET
 1381:d=8  hl=2 l=  13 prim: UTCTIME           :110406122632Z
 1396:d=6  hl=2 l=  47 cons: SEQUENCE
...
```

De même, les outils génériques ASN/1 comme dumpasn1 <http://www.cs.auckland.ac.nz/~pgut001/dumpasn1.c> peuvent permettre de récupérer une partie de l'information dans le ROA. D'autres outils pour jouer avec les ROA sont présentés dans mon article sur les logiciels de la RPKI <https://www.bortzmeyer.org/rpki-tests.html>.

Un exposé d'Arnaud Fenioux à l'assemblée générale du France-IX en septembre 2017 montrait l'utilisation de ces ROA au France-IX <http://www.afenioux.fr/doc/presentations/FranceIX-GM-2017.pdf>.