RFC 6487 : A Profile for X.509 PKIX Resource Certificates

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 février 2012

Date de publication du RFC : Février 2012

http://www.bortzmeyer.org/6487.html

La norme de certificats numériques X.509 est d'une telle complexité (comme beaucoup de productions des comités de l'UIT) qu'il est à peu près impossible de la mettre en œuvre complètement et correctement. La plupart de ses utilisations se font sur un **profil** de la norme, c'est-à-dire une restriction des usages possibles. De tels profils ont permis l'utilisation pratique de X.509, notamment sur l'Internet. Le profil décrit dans ce RFC a été conçu pour les certificats décrivant le « droit d'utilisation » des **ressources** Internet, ce qui veut dire, dans le monde du routage, les adresses IP et numéros d'AS (collectivement : les INR pour "*Internet Number Resources*"). Ces certificats ainsi profilés seront ensuite ceux utilisés pour la RPKI, afin de sécuriser le routage sur l'Internet <http://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>.

Rappelons le principe : des certificats sont émis par une autorité, l'AC. Ces certificats suivent le profil décrit ici, qui est lui-même dérivé du profil PKIX du RFC 5280[1], de loin le plus répandu sur l'Internet. Ces certificats permettent à l'autorité de dire « le titulaire de ce certificat a le droit d'utiliser les adresses 2001:db8:f33::/48, par exemple de les annoncer en BGP », en utilisant les extensions INR du RFC 3779. L'engin qui va valider les routes (c'est typiquement une machine spécialisée, agissant pour le compte d'un routeur) fera une validation X.509 de la chaîne des certificats, plus quelques vérifications spécifiques aux INR (par exemple, dans certains cas, le certificat peut autoriser une route plus spécifique) et dira ensuite si la route est valide, ou bien si elle est émise par un attaquant (ou un maladroit qui a mal configuré BGP).

Donc, un certificat de la RPKI est un certificat PKIX. Les principaux points de notre nouveau profil (section 4) sont le fait que le sujet est un nom choisi par l'AC, la présence obligatoire des extensions INR ("*Internet Number Resources*") du RFC 3779 (le certificat prouve le droit d'usage des préfixes IP indiqués dans ces extensions), et l'indication d'un dépôt accessible en rsync où se trouvent les CRL. Les sections 2 à 6 donnent tous les détails sur ces points.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5280.txt

Quant à la validation des certificats, elle fait l'objet de la section 7, qui précise les points généraux de la section 6 du RFC 5280. Notamment, un certificat peut être accepté même si le préfixe d'adresses présenté est plus spécifique (davantage de bits dans le masque).

La section 8 explique ensuite (et justifie) les principaux choix qui ont été faits lors de la conception de ce profil. Par exemple, notre profil ne permet **pas** d'utiliser des extensions X.509 autres que celles décrites dans ce RFC. Le but est d'utiliser les certificats dans un environnement bien défini, pour un usage limité, et il s'agit donc de limiter au maximum les risques de non-interopérabilité (un problème fréquent avec X.509, norme conçue par un comité et d'une très grande complexité ; bien des parties de la norme n'ont jamais été testées sur le terrain et nul ne sait comment réagiraient les implémentations). En outre, la RPKI est conçu pour être utilisée dans un contexte opérationnel (le routage sur l'Internet) et il était donc raisonnable de sacrifier l'extensibilité.

Quant au choix du nom du sujet, la RPKI n'étant pas centralisée, et n'ayant pas de système d'allocation arborescente des noms, on ne peut pas espérer avoir des noms uniques. Le RFC conseille donc aux AC (les RIR et les opérateurs réseau) d'adopter un schéma de nommage qui garantisse l'unicité au sein d'une même AC (rappelez-vous que, contrairement à l'utilisation de X.509 dans le cas de TLS, le nom du sujet n'est pas utilisé par la RPKI et n'est donc pas vérifié). Cela peut même être une valeur aléatoire comme un UUID.

L'annexe A du RFC fournit un exemple d'un certificat à ce profil. Mais on peut aussi l'obtenir en regardant un vrai certificat de la RPKI avec openssl (attention, il faut s'assurer qu'il ait été compilé avec l'option `enable-rfc3779`, ce qui n'est pas le cas chez Debian <`http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=630790`>):

```
% openssl x509 -inform DER -text -in \
    ./RPKI-repository/33/36711f-25e1-4b5c-9748-e6c58bef82a5/1/wdWccNZAgvBWFvBZNDJDWLtf-KQ.cer
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 78697736 (0x4b0d508)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=u75at9r0D4JbJ3_SFkZXD7C5dmg
        Validity
            Not Before: May 13 07:43:52 2011 GMT
            Not After : Jul  1 00:00:00 2012 GMT
        Subject: CN=wdWccNZAgvBWFvBZNDJDWLtf-KQ
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:99:d8:66:8b:26:15:22:fd:8e:45:c2:32:79:eb:
                    a4:36:d0:6d:47:18:34:d4:ad:17:bf:6f:82:d7:a3:
                    85:d9:80:ea:9f:59:31:6d:da:9f:b5:e0:36:67:e0:
                    f0:00:1b:96:2d:71:3e:5f:35:e0:f9:98:ee:fa:9f:
                    3e:6b:ab:9e:18:a6:ad:3c:fd:7a:50:6d:a5:42:4c:
                    bd:2d:02:f0:2a:7a:e6:66:bf:d5:b1:83:f1:19:02:
                    fe:90:21:d2:e3:b3:cc:91:a4:a6:6f:70:be:65:62:
                    7f:97:c1:43:2e:2c:a5:b2:14:79:e0:f5:5e:4b:c2:
                    aa:ed:13:d0:f2:4d:47:ac:53:fd:82:78:ef:c9:cd:
                    94:ea:52:10:56:88:80:bc:ca:ad:92:46:ef:4c:ae:
                    aa:ae:ae:02:d6:af:ae:2a:4e:dc:8b:c9:43:57:27:
                    84:1f:5a:82:ff:d7:24:ac:25:67:66:5f:70:d1:d6:
                    45:4b:a5:1d:c2:6f:bf:ae:14:3d:e4:2b:50:35:72:
                    ea:52:1c:b2:7d:15:12:15:07:d1:86:bb:2b:4b:ba:
                    47:1c:3e:37:b7:2c:ab:a6:4e:d3:16:54:84:96:92:
                    37:b6:6c:5c:3b:61:f1:73:9e:9c:9b:b8:ad:33:f8:
                    e0:19:9e:6a:dc:30:a6:45:90:f7:90:bb:d2:f9:65:
                    5b:53
                Exponent: 65537 (0x10001)
```

```
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                C1:D5:9C:70:D6:40:82:F0:56:16:F0:59:34:32:43:58:BB:5F:F8:A4
            X509v3 Authority Key Identifier:
                keyid:BB:BE:5A:B7:DA:F4:0F:82:5B:27:7F:D2:16:46:57:0F:B0:B9:76:68

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            Authority Information Access:
                CA Issuers - URI:rsync://rpki.ripe.net/ta/u75at9r0D4JbJ3_SFkZXD7C5dmg.cer

            Subject Information Access:
                CA Repository - URI:rsync://rpki.ripe.net/repository/72/f82cc3-00a3-4229-92ff-e5992b4b3fad/1/
                1.3.6.1.5.5.7.48.10 - URI:rsync://rpki.ripe.net/repository/72/f82cc3-00a3-4229-92ff-e5992b4b3fad

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:rsync://rpki.ripe.net/repository/33/36711f-25e1-4b5c-9748-e6c58bef82a5/1/u75at9r0D4JbJ3_SF

            X509v3 Certificate Policies: critical
                Policy: 1.3.6.1.5.5.7.14.2

            sbgp-ipAddrBlock: critical
                IPv4:
                  81.27.128.0/20
                IPv6:
                  2a00:8980::/32

    Signature Algorithm: sha256WithRSAEncryption
        8f:03:51:23:44:85:92:42:54:37:a2:22:53:66:0a:ab:be:a7:
        ...
        2e:31:d5:0d
-----BEGIN CERTIFICATE-----
MIIFLDCCBBSgAwIBAgIEBLDVCDANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDDBt1
...
-----END CERTIFICATE-----
```

Voyez notamment :

— Le sujet (nom du titulaire du certificat) unique, ici `CN=wdWccNZAgvBWFvBZNDJDWLtf-KQ` généré à partir d'un condensat cryptographique,
— L'indication de l'endroit où on peut récupérer les CRL (`rsync://rpki.ripe.net/repository/33/36711f-25` `SFkZXD7C5dmg.crl`),
— Le certificat de l'AC (`rsync://rpki.ripe.net/ta/u75at9r0D4JbJ3_SFkZXD7C5dmg.cer`),
— Les extensions du RFC 3779, ici le bloc mal nommé `sbgp-ipAddrBlock`, qui contient un préfixe IPv4 et un IPv6 (attention, pour les voir, il faut un `openssl` compilé avec la bonne option).