# RFC 8360 : Resource Public Key Infrastructure (RPKI) Validation Reconsidered

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 avril 2018

Date de publication du RFC : Avril 2018

https://www.bortzmeyer.org/8360.html

---

La RPKI est un ensemble de formats et de règles pour certifier qui est le titulaire d'une ressource Internet, une ressource étant un préfixe d'adresses IP, un numéro de système autonome, etc. La RPKI est utilisée dans les mécanismes de sécurisation <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html> de BGP, par exemple pour vérifier qu'un AS est bien autorisé à être à l'origine d'un préfixe donné. Les règles initiales de la RPKI pour valider un certificat était trop strictes et ce RFC les assouplit légèrement (normalement, en gardant le même niveau de sécurité).

La RPKI est normalisée dans le RFC 6480[1]. Elle prévoit notamment un système de certificats par lequel une autorité affirme qu'une autorité de niveau inférieur a bien reçu une délégation pour un groupe de ressources Internet. (On appelle ces ressources les INR, pour "*Internet Number Resource*".) La validation des certificats est décrite dans le RFC 6487. L'ancienne règle était que le certificat de l'autorité inférieure ne devait lister que des ressources qui étaient dans le certificat de l'autorité qui signait (RFC 6487, section 7.2, notamment la condition 6 de la seconde énumération). En pratique, cette règle s'est avérée trop rigide, et la nouvelle, décrite dans notre RFC 8360 est que le certificat de l'autorité inférieure n'est accepté que pour des ressources qui étaient dans le certificat de l'autorité qui signait. S'il y a d'autres ressources, le certificat n'est plus invalide, simplement, ces ressources sont ignorées. Dit autrement, l'ensemble des ressources dont la « possession » est certifiée, est l'intersection des ressources du certificat de l'autorité parente et de celui de l'autorité fille. Cette intersection se nomme VRS, pour "*Verified Resource Set*".

Voici d'abord une chaîne de certificats qui était valide avec l'ancienne règle, et qui l'est toujours :

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

```
Certificate 1 (trust anchor):
Issuer TA,
Subject TA,
Resources 192.0.2.0/24, 198.51.100.0/24,
      2001:db8::/32, AS64496-AS64500

Certificate 2:
Issuer TA,
Subject CA1,
Resources 192.0.2.0/24, 198.51.100.0/24, 2001:db8::/32

Certificate 3:
Issuer CA1,
Subject CA2,
Resources 192.0.2.0/24, 198.51.100.0/24, 2001:db8::/32

ROA 1:
Embedded Certificate 4 (EE certificate):
Issuer CA2,
Subject R1,
Resources 192.0.2.0/24
```

La chaîne part d'un certificat (TA, pour "*Trust Anchor*", le point de départ de la validation). Elle aboutit à un ROA ("*Route Origin Authorization*", cf. RFC 6482). Chaque certificat est valide puisque chacun certifie un jeu de ressources qui est un sous-ensemble du jeu de ressources de l'autorité du dessus. Idem pour le ROA.

Et voici par contre une chaîne de certificats qui était invalide selon les anciennes règles, et est désormais valide avec les règles de notre RFC 8360 :

```
Certificate 1 (trust anchor):
Issuer TA,
Subject TA,
Resources 192.0.2.0/24, 198.51.100.0/24,
     2001:db8::/32, AS64496-AS64500

Certificate 2:
Issuer TA,
Subject CA1,
Resources 192.0.2.0/24, 2001:db8::/32

Certificate 3 (invalid before, now valid):
Issuer CA1,
Subject CA2,
Resources 192.0.2.0/24, 198.51.100.0/24, 2001:db8::/32

ROA 1 (invalid before, now valid):
Embedded Certificate 4 (EE certificate, invalid before, now valid):
Issuer CA2,
Subject R1,
Resources 192.0.2.0/24
```

La chaîne était invalide car le troisième certificat ajoutait `198.51.100.0/24`, qui n'était pas couvert par le certificat supérieur. Désormais, elle est valide mais vous noterez que seuls les préfixes `192.0.2.0/24` et `2001:db8::/32` sont couverts, comme précédemment (`198.51.100.0/24` est ignoré). Avec les règles de notre nouveau RFC, le ROA final est désormais valide (il n'utilise pas `198.51.100.0/24`). Notez que les nouvelles règles, comme les anciennes, n'autoriseront jamais l'acceptation d'un ROA pour des ressources dont l'émetteur du certificat n'est pas titulaire (c'est bien le but de la RPKI). Ce point est

important car l'idée derrière ce nouveau RFC de rendre plus tolérante la validation n'est pas passée toute seule à l'IETF.

Un cas comme celui des deux chaînes ci-dessus est probablement rare. Mais il pourrait avoir des conséquences sérieuses si une ressource, par exemple un préfixe IP, était supprimée d'un préfixe situé très haut dans la hiérarchie : plein de certificats seraient alors invalidés avec les règles d'avant.

La section 4 de notre RFC détaille la procédure de validation. Les anciens certificats sont toujours validés avec l'ancienne politique, celle du RFC 6487. Pour avoir la nouvelle politique, il faut de nouveaux certificats, identifiés par un OID différent. La section 1.2 du RFC 6484 définissait `id-cp-ipAddr-asNumber / 1.3.6.1.5.5.7.14.2` comme OID pour l'ancienne politique. La nouvelle politique est `id-cp-ipAddr-asNumber-v / 1.3.6.1.5.5.7.14.3` et c'est elle qui doit être indiquée dans un certificat pour que lui soient appliquées les nouvelles règles. (Ces OID sont dans un registre IANA `<https://www.iana.org/assignments/smi-numbers/smi-numbers.xml#smi-numbers-1.3.6.1.5.5.7.14>`.) Comme les logiciels existants rejetteront les certificats avec ces nouveaux OID, il faut adapter les logiciels avant que les AC ne se mettent à utiliser les nouveaux OID (cf. section 6 du RFC). Les changements du RFC n'étant pas dans le protocole mais uniquement dans les règles de validation, le déploiement devrait être relativement facile.

Le cœur des nouvelles règles est dans la section 4.2.4.4 de notre RFC, qui remplace la section 7.2 du RFC 6487. Un nouveau concept est introduit, le VRS ("*Verified Resource Set*"). C'est l'intersection des ressources d'un certificat et de son certificat supérieur. Dans le deuxième exemple plus haut, le VRS du troisième certificat est {`192.0.2.0/24`, `2001:db8::/32`}, intersection de {`192.0.2.0/24`, `2001:db8::/32`} et {`192.0.2.0/24`, `198.51.100.0/24`, `2001:db8::/32`}. Si le VRS est vide, le certificat est invalide (mais on ne le rejette pas, cela peut être un cas temporaire puisque la RPKI n'est pas cohérente en permanence).

Un ROA est valide si les ressources qu'il contient sont un sous-ensemble du VRS du certificat qui l'a signé (si, rappelons-le, ce certificat déclare la nouvelle politique). La règle exacte est un peu plus compliquée, je vous laisse lire le RFC pour les détails. Notez qu'il y a également des règles pour les AS, pas seulement pour les préfixes IP.

La section 5 du RFC contient davantage d'exemples, illustrant les nouvelles règles.