RFC 6492 : A Protocol for Provisioning Resource Certificates

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/6492.html

La RPKI est l'infrastructure de création et de distribution de certificats pour les titulaires de ressources Internet (essentiellement les adresses IP), afin de sécuriser le routage sur l'Internet <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>. Ce RFC normalise un protocole de communication pour réclamer ces certificats (avitaillement, ou "*provisioning*"). Il sera typiquement utilisé entre les RIR et les LIR.

Les termes exacts utilisés par le RFC sont Émetteur ("*Issuer*"), en général un RIR, qui va donc être une AC, et Destinataire ("*Subject*"), qui sera un FAI ou autre opérateur réseau. Le RIR distribue des INR ("*Internet Number Resource*", ce sont les adresses IP et les numéros d'AS, collectivement nommés Ressources) et les certificats prouvant le droit du Destinataire à utiliser ces INR. Notez qu'un Destinataire peut être Émetteur pour des ressources qu'il redistribuera, par exemple à des opérateurs plus petits.

Le trafic attendu rend nécessaire d'automatiser l'avitaillement des certificats. Cela se fait avec un simple protocole (section 3), qui est une extension de HTTP. Le client HTTP fait une requête `POST` (RFC 7231 [1], section 4.3.4), de type MIME `application/rpki-updown`. Le protocole est strictement requête/réponse (synchrone). Aussi bien le corps de la requête, que celui de la réponse du serveur, sont au format CMS (RFC 5652), encodé en DER. Le profil CMS est défini en section 3.1. CMS permet de transporter les signatures des différents objets (et les métadonnées associées comme la date de signature) mais le gros du contenu est un élément XML stocké dans le CMS sous le nom de `RPKIXMLProtocolObject`.

Cet élément XML est forcément `<message>`. Il forme l'essentiel de la requête ou de la réponse. Sa grammaire est décrite en Relax NG en section 3.7.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7231.txt`

Quelles sont les opérations possibles ? Elles sont indiquées par l'attribut `type` de la requête. Par exemple, le client peut demander une liste des ressources que lui a alloué le serveur, avec `type="list"`. La réponse arrivera sous forme d'une séquence d'éléments `<class>`. Ou bien il peut demander un certificat pour une nouvelle ressources avec `type="issue"`.

Naturellement, vu que tout le but de l'exercice est d'augmenter la sécurité du routage dans l'Internet, les implémenteurs et les utilisateurs de ce RFC devraient bien faire attention à la section 4, qui couvre la sécurité de ce protocole d'avitaillement. Le RFC précise que l'Émetteur et le Destinataire doivent s'authentifier (par les siognatures contenues dans les messages CMS), en utilisant des lettres de créance qu'ils ont échangé précédemment (par un moyen non spécifié). On note que TLS n'est pas utilisé par ce protocole (ce fut une chaude discussion au sein du groupe de travail), CMS fournissant tous les services de sécurité nécessaires.

Je ne connais pas encore de mise en œuvre publique de ce protocole mais plusieurs RIR ont annoncé qu'ils auraient des serveurs prêts pour la sortie du RFC.