RFC 4398 : Storing Certificates in the Domain Name System (DNS)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 avril 2006

Date de publication du RFC : Mars 2006

http://www.bortzmeyer.org/4398.html

Il existe de nombreux moyens de distribuer les certificats utilisés en cryptographie, comme les serveurs de clé de PGP. Notre RFC en ajoute un nouvau, le DNS.

Les certificats étant protégés par leur signature, le transport n'a pas besoin d'être fiable. On peut donc se servir du DNS, même sans DNSSEC. C'est ce que faisait le RFC 2538 [1] que notre RFC a légèrement remis à jour.

Notre RFC crée donc un nouveau type d'enregistrement DNS , `CERT` et définit le format pour y mettre des certificats comme ceux de X.509 ou de OpenPGP. Il contient également une section, la 3, pour discuter du nom à donner à ces enregistrements. (Par exemple l'adresse de courrier pour un certificat OpenPGP, donc ma propre clé PGP, dès que je saurai l'encoder proprement, pourrait être publiée sous `stephane.bortzmeyer.org`.) Mais je ne connais pas encore de logiciel de cryptographie capable de récupérer un certificat via le DNS.

Un bon tutoriel sur la publication de clés PGP dans le DNS est « *"How to publish PGP keys in DNS"* <http://gushi.livejournal.com/524199.html> ».

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2538.txt`