RFC 4641 : DNSSEC Operational Practices

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 octobre 2006

Date de publication du RFC : Septembre 2006

https://www.bortzmeyer.org/4641.html

Comme avec toute technique fondée sur la cryptographie, le protocole DNSSEC impose, non seulement des bons algorithmes et une mise en œuvre correcte, mais surtout des procédures rigoureuse et soigneusement exécutées. C'est le but de ce RFC, qui remplace le RFC 2541 [1] et a lui-même été remplacé par le RFC 6781, et qui explique tout ce à quoi doivent s'attendre les registres qui déploieraient DNSSEC.

Notre RFC rappelle donc des concepts de base du DNS (notamment le fait que la propagation des modifications n'est pas instantanée) puis rappelle les différentes clés utilisées par DNSSEC et leurs caractéristiques souhaitables (longueur, période maximale pendant laquelle on les utilise, lieu de stockages, etc).

Il explique ensuite les considérations temporelles (DNSSEC utilise le temps et nécessite des horloges bien synchronisées, par exemple par NTP).

Enfin, le RFC étudie le "*rollover*", le remplacement d'une clé. Les clés ne pouvant pas raisonnablement être utilisées éternellement, il faut prévoir à l'avance les remplacements périodiques et aussi, hélas les remplacements en urgence en cas de compromission. Il faut apporter beaucoup de soin à ce remplacement, si on veut éviter que, pendant une certaine période, les données publiées dans le DNS soient invalides et donc rejetées par un résolveur DNS paranoïaque (il faut publier la nouvelle clé suffisamment à l'avance pour qu'elle soit présente partout ou bien signer tous les enregistrements avec les deux clés, l'ancienne et la nouvelle).

Le DNS étant hiérarchique, il faut veiller, lors de toutes les manipulations, à bien rester synchronisé avec le gérant de la zone parente, dont les enregistrements de type DS ("*delegation signer*") pointeront vers notre clé.

Bref, pour un registre, déployer DNSSEC, ce n'est pas uniquement signer la zone : c'est aussi mettre en place des procédures de sécurité, analogues à celle d'une autorité de certification.

Le RFC 6781 a depuis remplacé ce RFC et est donc la version actuelle sur les questions opérationnelles liées à DNSSEC.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2541.txt