ITAR est officiellement publié, pour aider au déploiement de DNSSEC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 février 2009. Dernière mise à jour le 22 décembre 2010

https://www.bortzmeyer.org/itar-dnssec.html

Un problème classique de DNSSEC est qu'il faut connaître au moins une clé publique pour commencer la validation. Si la racine du DNS est signée, on configure logiquement dans son résolveur DNS la clé publique de la racine, largement diffusée. Mais, aujourd'hui, la racine n'est pas signée (cela a été fait en juillet 2010) et cette signature, qui dépend du gouvernement états-unien, est bloquée par des considérations essentiellement politiciennes. Alors, en attendant, une nouvelle méthode est disponible, ITAR <https://itar.iana.org/>. Elle a finalement servi deux ans, avant sa suppression en novembre 2010.

DNSSEC, normalisé dans les RFC 4033 [1] et suivants, permet de résoudre certaines failles de sécurité du DNS comme l'empoisonnement de caches <https://www.bortzmeyer.org/faille-dns-empoisonnement.html>. Pour cela, les enregistrements DNS sont signés avec une clé cryptographique privée. Si on connait la clé publique correspondante, on peut alors valider la signature. Il existait deux méthodes pour connaître les clés publiques :

— Les rassembler à la main en cherchant sur les sites Web des titulaires comme <https://www.ripe.net/projects/disi/keys/>. C'est long et pénible, d'autant plus que les clés sont régulièrement remplacées.
— Utiliser DLV ("*DNSSEC Lookaside Validation*", RFC 5074), bien plus simple.

Une troisième méthode a été annoncée le 17 février par l'IANA : ITAR <https://itar.iana.org/>. C'est un dépôt des clés publiques de TLD, vérifiées par l'IANA. Il est distribué sous différents formats et on peut le récupérer et le valider, par exemple ainsi :

```
% wget https://itar.iana.org/anchors/anchors.mf
% wget https://itar.iana.org/anchors/anchors.mf.sig
% gpg anchors.mf.sig
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4033.txt

(La dernière étape, vérifier avec GPG, est probablement sans intérêt puisque la clé PGP de l'IANA n'est pas signée <https://www.icann.org/en/general/pgp-keys.htm#iana-itar> et qu'il n'y a aucun moyen de la valider.) Une fois cela fait, ce fichier peut être utilisé pour configurer son résolveur, par exemple pour Unbound <https://www.bortzmeyer.org/unbound.html> :

```
trust-anchor-file: "anchors.mf"
```

En fait, cette annonce n'est pas si importante que cela : d'abord, ITAR ne stocke que les clés des TLD. On n'y trouvera donc pas celles de `ripe.net` ou des `in-addr.arpa`, citées plus haut, ni celles des nombreux domaines signés dans des TLD non signés comme `sources.org`. Mais, surtout, le registre DLV de l'ISC <https://www.isc.org/solutions/dlv> copie automatiquement ITAR toutes les nuits et l'intègre dans leur base. utiliser DLV suffit donc. La publication d'ITAR est donc plutôt un geste politique de la part de l'ICANN, qui tient à affirmer sa candidature à la signature de la racine. ITAR a été officiellement fermée <https://itar.iana.org/> en 2010.