Le nouveau type de données DNS WALLET

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 juillet 2024

https://www.bortzmeyer.org/wallet-rrtype.html

Contrairement au cliché mille fois répété (mais faux), le DNS ne sert pas qu'à « traduire des noms de domaine en adresses IP ». Il est d'un usage général et permet de récupérer, indexées par un nom de domaine, diverses informations. Un nouveau type d'information vient d'être officiellement enregistré, WALLET, pour indiquer l'adresse d'un portefeuille de cryptomonnaie.

La capacité du DNS à résoudre un nom de domaine en divers types d'informations vient d'un champ des requêtes et réponses DNS, le **type** (ou, en plus long, le "*RR type*", pour "*Resource Record type*"). Décrit dans la section 3.2.2 du RFC 1035 [1], ce type peut prendre des valeurs diverses : AAAA pour les adresses IP, SVCB pour les serveurs d'un service donné, LOC pour une position, TXT pour du texte libre, etc.

Il est important de noter que cette liste des types possibles n'est pas figée. Elle est enregistrée dans un registre IANA <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-4> et on peut ajouter des types à ce registre, en suivant la procédure décrite dans le RFC 6895. Cette procédure est délibérement très légère : le demandeur documente le nouveau type, envoie la demande à l'IANA, celle-ci la fait examiner par un expert (actuellement [Caractère Unicode non montré [2]]lafur Gu[Caractère Unicode non montré]mundsson) et s'il n'y a pas de problèmes, le nouveau type est enregistré. Bien que la procédure soit libérale, on ne peut pas dire qu'il y ait eu une bousculade depuis la sortie du RFC 6895, la plupart des types enregistrés ayant suivi un chemin plus classique de normalisation.

Mais le nouveau WALLET, désormais ajouté au registre IANA, a utilisé le chemin simple ; une documentation <https://www.iana.org/assignments/dns-parameters/WALLET/wallet-completed-template> un examen par l'expert et hop, c'est enregistré. Comme les types ont un numéro en plus de leur nom (c'est ce numéro qui figure dans les paquets DNS), le 262 a été alloué. Que contient un enregistrement DNS de type WALLET ? Deux champs, une chaine de caractères qui identifie la cryptomonnaie utilisée

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1035.txt
2. Car trop difficile à faire afficher par LaTeX

(BTC pour Bitcoin, ETH pour Ethereum, etc) et une autre chaine de caractères qui contient l'adresse d'un compte.

L'encodage dans les paquets est identique à celui des enregistrements de type TXT : une suite de chaines de caractères est encodée en un octet qui indique la longueur de la chaine puis la suite d'octets de la chaine. Ainsi, "BTC" (pour Bitcoin) sera encodé {3, 66, 84, 67}, les trois derniers octets étant les codes ASCII.

J'ai ainsi ajouté au DNS mon adresse Bitcoin <https://www.bortzmeyer.org/bitcoin-blog.html>, sous bortzmeyer.fr. Mais attention, comme le type WALLET est récent (créé le 21 juin 2024), la plupart des logiciels ne le connaissent pas. Pour le mettre dans le fichier de zone du serveur primaire, j'ai dû utiliser la méthode des « types inconnus » du RFC 3597 :

```
@ IN TYPE262 \# 39 03425443 223148744E4A365A4655633979753975327141774234744764477750516173514761 78
```

(39 octets, le premier groupe fait trois octets, les trois lettres de "BTC", regardez la table ASCII. Vous pouvez utiliser le script Python pour produire cet encodage.) Et c'est également ainsi que dig l'affichera (le type WALLET n'étant pas connu, il a fallu donner son numéro, 262) :

```
% dig bortzmeyer.fr TYPE262
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26302
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
bortzmeyer.fr. 86400 IN TYPE262 \# 39 ( 03425443223148744E4A365A4655633979753975327141774234744764477750516173514761 78 )
...
```

Pour le formater plus joliment, en attendant que dig soit mis à jour, j'ai écrit un petit script (en ligne sur https://www.bortzmeyer.org/files/wallet-dns.py) en Python (utilisant la bibliothèque dnspython <https://www.dnspython.org/>) :

```
% wallet-dns.py bortzmeyer.fr
bortzmeyer.fr
Code: BTC ; Address: 1HtNJ6ZFUc9yu9u2qAwB4tGdGwPQasQGax
```

Et voilà, l'adresse est joliment affichée. (Une gestion assez minimale de ce type est en cours de développement dans dnspython <https://github.com/rthalley/dnspython/commit/e5e9f5e8722da521

PS : il existe aussi cette alternative <https://bips.dev/353/>.