Passage de mes zones DNS à des signatures à courbes elliptiques

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 juillet 2024

https://www.bortzmeyer.org/rollover-algorithm-opendnssec.html

---

Vous l'avez peut-être remarqué, mes zones DNS personnelles (comme bortzmeyer.org, que vous utilisez pour lire ce blog </>) viennent de changer d'algorithme de signature cryptographique. RSA a été remplacé par ECDSA.

Pourquoi ce grand remplacement ? Les signatures DNSSEC faites avec ECDSA (RFC 6605[1]) sont plus petites, ce qui peut présenter des avantages dans certains cas (mais ne va évidemment pas diminuer l'empreinte environnementale de mes zones). Mais, surtout, l'avis de la grande majorité des experts en cryptographie (je ne fais pas partie de ces experts, très loin de là, donc je leur fais confiance) est que la cryptographie sur courbes elliptiques, qui est à la base d'ECDSA, est plus sûre, surtout face aux futures évolutions de la cryptanalyse, que le traditionnel RSA. Vous noterez d'ailleurs que beaucoup de zones DNS importantes ont changé, par exemple .com. De même, .fr a migré il y a plusieurs années <https://www.afnic.fr/observatoire-ressources/papier-expert/resolutions-2020-lafnic-se-me> et c'est uniquement la paresse qui m'avait jusque là empêché d'en faire autant. (La racine du DNS, elle, est toujours en RSA, car il est bien plus compliqué de changer une clé que tous les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> de la planète doivent connaitre, et ce malgré le RFC 5011.)

J'ai un peu hésité à passer à ECDSA car il dépend d'une courbe elliptique, la P-256, conçue par la NSA et normalisée par le NIST, et à utiliser plutôt EdDSA (RFC 8080). Mais, autant tous les résolveurs DNSSEC <https://www.bortzmeyer.org/resolveur-dns.html> acceptent aujourd'hui aussi bien ECDSA que RSA, autant Ed25519 reste moins répandu.

Une fois la décision prise, comment faire ? Comme toujours avec le DNS, il faut tenir compte du fait que la réjuvénation <https://www.bortzmeyer.org/dns-propagation.html> n'est pas instantanée. Si on change brutalement les clés qu'on publie, on risque que certains résolveurs aient encore

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6605.txt

dans leur mémoire des clés qui ne valideront pas les signatures récentes (ou bien le contraire). Que l'on change les clés ou, comme ici, les algorithmes, il faut procéder à ce remplacement ("*rollover*") en intégrant les contraintes temporelles (RFC 6781 et RFC 7583).

Suivre manuellement ces contraintes (ajouter la nouvelle clé, attendre le TTL, ajouter l'enregistrement DS dans la zone parente, attendre qu'il soit publié, attendre le TTL, retirer l'ancien DS, attendre, retirer l'ancienne clé…) est pénible et le risque d'erreur est très élevé. Il faut donc automatiser, ce que j'ai fait. Mes zones DNS personnelles sont gérées avec OpenDNSSEC et c'est donc lui qui a fait tout le travail.

Prenons l'exemple de la zone `cyberstructure.fr`. DNSviz `<https://dnsviz.net/>` va nous montrer ses différents états (l'archivage des anciennes mesures et la facilité de navigation dans cet historique font partie des grandes forces de DNSviz). Elle était signée uniquement avec RSA `<https://dnsviz.net/d/cyberstructure.fr/ZYBFoQ/dnssec/>`. (Les erreurs signalées par DNSviz sont dues au non-respect du RFC 9276, j'y reviendrai.) Le 17 juin 2024, je change la configuration OpenDNSSEC. Dans ce logiciel, chaque zone gérée l'est selon une politique choisie par l'administrateur système. La politique utilisée, nommée `default` était d'utilise RSA. Je crée une nouvelle politique, nommée, sans imagination, `new`. Dans la syntaxe XML du fichier de configuration d'OpenDNSSEC, le fichier `kasp.xml` contient :

```
<Policy name="new">
<Description>A new policy with ECDSA</Description>
...
                <Keys>
                        ...
                        <!-- Parameters for KSK only -->
                        <KSK>
                                <Algorithm length="512">13</Algorithm>
                                <Lifetime>P3Y</Lifetime>
                                <Repository>SoftHSM</Repository>
                                <ManualRollover/>
                        </KSK>

                        <!-- Parameters for ZSK only -->
                        <ZSK>
                                <Algorithm length="512">13</Algorithm>
                                <Lifetime>P90D</Lifetime>
                                <Repository>SoftHSM</Repository>
                                <!-- <ManualRollover/> -->
                        </ZSK>
                </Keys>
...
```

L'algorithme de numéro 13 est ECDSA (RSA est le numéro 8, cf. le registre IANA `<https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml#dns-sec-alg-numbers-`
On change ensuite la configuration de la zone (dans `zonelist.xml`) :

```
<Zone name="cyberstructure.fr">
    <Policy>new</Policy>
    ...
```

On recharge alors OpenDNSSEC :

`https://www.bortzmeyer.org/rollover-algorithm-opendnssec.html`

```
% sudo ods-enforcer zonelist import
...
Updated zone cyberstructure.fr successfully
```

Les nouvelles clés ECDSA (rappel : algorithme 13) sont alors créées par OpenDNSSEC :

```
% sudo ods-enforcer key list --verbose --zone cyberstructure.fr
Keys:
Zone:                          Keytype: State:    Date of next transition: Size: Algorithm: CKA_ID:
cyberstructure.fr              KSK      active    2024-06-18 10:53:01      2048  8          2d63a8cc9f68602d5b9
cyberstructure.fr              ZSK      active    2024-06-18 10:53:01      1024  8          b8e16f9a3aad96676ae
cyberstructure.fr              KSK      publish   2024-06-18 10:53:01      512   13         02e0ddf994431d5fa3d
cyberstructure.fr              ZSK      ready     2024-06-18 10:53:01      512   13         cebc635b489780d2fdd
```

Elles n'apparaissent pas dans le DNS immédiatement, il faut attendre leur passage en état `ready` (regardez la colonne "*Date of next transition*"). Une fois que c'est fait, DNSviz nous montre le nouvel état <https://dnsviz.net/d/cyberstructure.fr/ZnCPgg/dnssec/>, avec pour l'instant les clés ECDSA publiées mais qui ne seront pas utilisées pour la validation.

Pensez aussi à recharger le signeur d'OpenDNSSEC (`ods-signer update --all`). Dans le DNS, on note que les deux ZSK ("*Zone-signing key*") signent (même si, pour l'instant, les signatures ECDSA ne servent à rien) :

```
% dig @ns4.bortzmeyer.org. cyberstructure.fr SOA
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18279
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 8, ADDITIONAL: 1
...
;; ANSWER SECTION:
cyberstructure.fr. 7200 IN SOA ns4.bortzmeyer.org. hostmaster.bortzmeyer.org. (
2024061703 ; serial
7200       ; refresh (2 hours)
3600       ; retry (1 hour)
604800     ; expire (1 week)
3600       ; minimum (1 hour)
)
cyberstructure.fr. 7200 IN RRSIG SOA 13 2 7200 (
20240701143938 20240617155301 54500 cyberstructure.fr.
CW/V6zSkMn/cC8E2hUHYlaSparKbOgc03CRcbOecTOMY
HxMTavaExj9fvvkH3srNrP9Kx/VYRQsi4YrjMFH6DA== )
cyberstructure.fr. 7200 IN RRSIG SOA 8 2 7200 (
20240701143938 20240617155301 11668 cyberstructure.fr.
UCskHbeGjx20Bqo+9IyczDaHrEZ83uBYQsjDy/Etqngy
QeCH1gADMbsl3VaBPHiLDd8MIVkzH2I73/jEUo2R22wq
KPtSTsGHQ8I2vPff5ylplqJFXVUitiyGcEYVaAtI3hAk
eijaGI6J3nAdcYuAxFo9Gi+WRCEmTRcL8RZAjCo= )
```

On voit notamment que la signature ECDSA est plus petite, ce qui était une des motivations pour ce remplacement. Et les clés ?

```
% dig @ns4.bortzmeyer.org. cyberstructure.fr DNSKEY
...
```

---

https://www.bortzmeyer.org/rollover-algorithm-opendnssec.html

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51884
;; flags: qr aa rd; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
cyberstructure.fr. 7200 IN DNSKEY 257 3 8 (
AwEAAddHCFxVIpXyRRVCBh4zHt22o3ReQzk+Avi5J+c2
hLnB2zSB7obXWsxj0fZSeyYE4VAClJ5/7TF687gRjVRW
3cNTsJ9mrQzbLbuxL3nnIKWZRrVKWg9RpKHDul9QL1EC
trgum18SK9QpRnywZx8kM0zFviu75Df2636wT1YcQZUz
KDXRE0IGg6r9qGMcq6PXL3woDPoVmv3H7SvXZjlj/2zI
nMvQo15Y0Y7kO6Epng9qgnJaZeTrTo4OtzIPMSOahFMJ
YD8AxlsT5yN7lQZSRMJDYjJ1HC+PgyLMnz7y+iwvVLMZ
6IVr1yeYbCp+inTHi+qn9fRJSIjirWJWb/7sHdk=
) ; KSK; alg = RSASHA256 ; key id = 63130
cyberstructure.fr. 7200 IN DNSKEY 256 3 8 (
AwEAAcGW9K353z/T1ZKstnQ4Y0ricKlmb2DyVEE0Dcrc
St/fNVdB3g2Y9tlXh9oQH0RzNK2UqIAm2PxmAleeWOZp
8qzYdtWZj5O/4VXtLkjAwOUuinjaYIfDskcuue/pg+cT
ilQhXnh/sKktyci4wtFIDZLBL7gYyiZSFrR4DCwcpITr
) ; ZSK; alg = RSASHA256 ; key id = 11668
cyberstructure.fr. 7200 IN DNSKEY 257 3 13 (
zyVnEtBlrgWpNtDUnhPIikEIUaAj+/VwHfC7j1jpWeqa
fAE04Mx9nXDFhznhDD0uvIFpY3se9wefPddNZJDVCA==
) ; KSK; alg = ECDSAP256SHA256 ; key id = 10825
cyberstructure.fr. 7200 IN DNSKEY 256 3 13 (
s+HVObz03Vzug26yX3KjlyXbpMcCzoD/8CblfTR2zQsi
e35hf2DBwLarHOCcMpu6X5+FgHMsOwmvaSJH/AzZCA==
) ; ZSK; alg = ECDSAP256SHA256 ; key id = 54500
cyberstructure.fr. 7200 IN RRSIG DNSKEY 13 2 7200 (
20240701061231 20240617155301 10825 cyberstructure.fr.
EbgfiMIxj2zhVgnAD2MPf4fZ6PZjCT4iZMhMgUb6EK/m
o8foczgd9PFotvcaaQxaE6rybMiOvhRETbIrX9IeCA== )
cyberstructure.fr. 7200 IN RRSIG DNSKEY 8 2 7200 (
20240701061231 20240617155301 63130 cyberstructure.fr.
qTI+5RbOnuWfpkXgTSiYEv04An19XjxP1vGyYEnD5ao0
zaexw3yh1xhNGlsqFU1XLkADTilpt1w60qO/9lshE3kD
eA73s6u03hsrLxL71YjvUEU68pO/iT4LxhpYY0P1gCPX
rdiM50mYauiSQROnt5UeQ0wJ/Q4NSl4fQrko1cHcymcD
05JeCS4e2gq7HlCQsn2rTQTwP2A0d9ccYBe02rPziTP4
HnyEAcBqATHPU1U+yqd5OZLYkJh+mGJTFFHoXfxYSqKu
6C86KVV5wtrX+bCxcNGrdRiyGI0FSDioXQG7p1+/oLYf
j6vQnfns9INHEH2uY6P6LdJX4GTFKq3gpg== )

;; Query time: 0 msec
;; SERVER: 2001:4b98:dc0:41:216:3eff:fe27:3d3f#53(ns4.bortzmeyer.org.) (UDP)
;; WHEN: Mon Jun 17 18:53:46 CEST 2024
;; MSG SIZE  rcvd: 1048
```

Ouf, ça en fait, des données à envoyer. Mais ce n'est que transitoire.

À la prochaine étape (tout se déroule automatiquement et est géré par OpenDNSSEC), la clé ECDSA est prête :

```
% sudo ods-enforcer key  list --verbose --zone cyberstructure.fr
Keys:
Zone:                          Keytype: State:    Date of next transition: Size: Algorithm: CKA_ID:
cyberstructure.fr              KSK      retire    waiting for ds-gone      2048  8          2d63a8cc9f68602
cyberstructure.fr              ZSK      active    2024-09-15 18:53:01      1024  8          b8e16f9a3aad966
cyberstructure.fr              KSK      ready     waiting for ds-seen      512   13         02e0ddf994431d5
cyberstructure.fr              ZSK      active    2024-09-15 18:53:01      512   13         cebc635b489780c
```

Maintenant, il va falloir travailler, l'étape suivante ne peut pas être automatisée. Il faut prévenir la zone parente (dans le cas de `.fr`, via le BE) et indiquer à OpenDNSSEC (qui ne sait pas faire de requête DNS lui-même) quand l'enregistrement DS arrivera. On lui demande d'exporter la clé :

---

https://www.bortzmeyer.org/rollover-algorithm-opendnssec.html

```
% sudo ods-enforcer key  export --zone cyberstructure.fr
```

(Si votre BE et/ou votre registre demande le DS et pas le DNSKEY, il faudra ajouter `--ds` à la commande.) On indique alors la nouvelle clé dans l'interface du BE (Web ou API). Attention à soigner cette étape : cette clé va désormais être utilisée pour la validation, il ne faut pas se tromper. On patiente ensuite le temps que le registre ait bien mis à jour la zone parente et, lorsque notre DS est dans le DNS, on prévient OpenDNSSEC :

```
% sudo ods-enforcer key ds-seen --keytag 10825   --zone cyberstructure.fr
1 KSK matches found.
1 KSKs changed.

% sudo ods-enforcer key  list --verbose --zone cyberstructure.fr
Keys:
Zone:                           Keytype: State:    Date of next transition: Size: Algorithm: CKA_ID:
cyberstructure.fr               KSK      retire    waiting for ds-gone      2048  8          2d63a8cc9f68602d5b9
cyberstructure.fr               ZSK      active    2024-06-21 14:06:08      1024  8          b8e16f9a3aad96676ae
cyberstructure.fr               KSK      active    2024-06-21 14:06:08      512   13         02e0ddf994431d5fa3d
cyberstructure.fr               ZSK      active    2024-06-21 14:06:08      512   13         cebc635b489780d2fdd
```

Parfait, la KSK ("*Key-signing key*") ECDSA est désormais active. La KSK RSA va être retirée. Regardons d'abord le nouvel état <https://dnsviz.net/d/cyberstructure.fr/ZnKNxA/dnssec/>. Il y a deux DS et deux clés actives.

On va maintenant retirer l'ancien DS. On le supprime via l'interface du BE puis, lorsque le registre a mis la zone à jour :

```
% sudo ods-enforcer key ds-gone --keytag 63130    --zone cyberstructure.fr
1 KSK matches found.
1 KSKs changed.

% sudo ods-enforcer key  list --verbose --zone cyberstructure.fr
Keys:
Zone:                           Keytype: State:    Date of next transition: Size: Algorithm: CKA_ID:
cyberstructure.fr               KSK      retire    2024-06-21 14:06:08      2048  8          2d63a8cc9f68602d5b9
cyberstructure.fr               ZSK      active    2024-06-21 14:06:08      1024  8          b8e16f9a3aad96676ae
cyberstructure.fr               KSK      active    2024-06-21 14:06:08      512   13         02e0ddf994431d5fa3d
cyberstructure.fr               ZSK      active    2024-06-21 14:06:08      512   13         cebc635b489780d2fdd
```

Plus qu'un seul DS <https://dnsviz.net/d/cyberstructure.fr/ZnKqkA/dnssec/>, mais l'ancienne clé RSA est toujours là, pour les résolveurs qui auraient des anciennes informations dans leur mémoire.

Enfin, les clés et signatures RSA seront automatiquement supprimées du DNS lorsqu'elles sont devenues inutiles, ce qui nous mène au dernier état <https://dnsviz.net/d/cyberstructure.fr/ZnkyNA/dnssec/>, lorsque le remplacement est terminé. Les clés disparaitront ensuite du trousseau d'OpenDNSSEC (mais cela prendra davantage de temps).

```
% sudo ods-enforcer key list --verbose --zone cyberstructure.fr
Keys:
Zone:                           Keytype: State:    Date of next transition: Size: Algorithm: CKA_ID:
cyberstructure.fr               KSK      retire    2024-07-06 08:09:09      2048  8          2d63a8cc9f68602d5b9
cyberstructure.fr               ZSK      retire    2024-07-06 08:09:09      1024  8          b8e16f9a3aad96676ae
cyberstructure.fr               KSK      active    2024-07-06 08:09:09      512   13         02e0ddf994431d5fa3d
cyberstructure.fr               ZSK      active    2024-07-06 08:09:09      512   13         cebc635b489780d2fdd
```

---

https://www.bortzmeyer.org/rollover-algorithm-opendnssec.html

Voici le résultat :

Ah, et j'avais dit qu'il y avait des erreurs dues au non-respect du RFC 9276, qui a changé les paramètres recommandés pour les enregistrements NSEC3 (RFC 5155). C'est exact, donc il a fallu également modifier cela dans notre politique :

```
<!-- Régime sans sel, et sans itérations -->
<NSEC3>
...
       <Hash>
         <Algorithm>1</Algorithm>
         <Iterations>0</Iterations>
         <Salt length="0"/>
       </Hash>
</NSEC3>
```

Quelques liens intéressants :

— Le wiki d'OpenDNSSEC <https://wiki.opendnssec.org/howto/>,
— Le remplacement d'algorithme qu'avait fait le RIPE <https://labs.ripe.net/author/anandb/dnssec-algorithm-roll-over/> (manuellement…),
— Un autre récit de remplacement utilisant OpenDNSSEC <https://toutetrien.lithio.fr/article/remplacement-de-ksk-et-changement-algorithme-avec-opendnssec/>,