

Remplacement de la clé DNSSEC de la racine

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 octobre 2026

<https://www.bortzmeyer.org/remplacement-cle-dnssec-2026.html>

Aujourd'hui, la racine du DNS, qui était signée avec la clé 20326 a changé, et utilise désormais la clé 38696.

Rien d'extraordinaire et aucun problème sérieux n'est attendu. Après tout, ce n'est pas le premier remplacement de la clé DNSSEC de la racine. Notez que, malgré la demande de bien des gens, la nouvelle clé est toujours du RSA (alors que les gros TLD utilisent souvent ECDSA). La nouvelle clé, 38696, a été largement publiée depuis longtemps donc est normalement connue de tous les résolveurs (en particulier grâce au RFC 5011¹ mais aussi à la mise à jour de paquets comme `dns-root-data` sur Debian ou `dnssec-anchors` sur Arch).

La situation avant le remplacement peut être vue sur DNSviz <<https://dnsviz.net/d/root/asuS0A/dnssec/>>, ou bien avec `dig` :

```
% dig . DNSKEY
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.18.39-0ubuntu0.24.04.7-Ubuntu <<>> . DNSKEY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7696
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
; .      IN DNSKEY

;; ANSWER SECTION:
.      83906 IN DNSKEY 256 3 8 (
```

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc5011.txt>

```

AwEAAcorNxC9t0ue1ZenPjVMRuJlQ2YLBj0pR/4XMjH
by9vr03cRxFsKnWpxeg5PL384D9VeQdS1bjrGyTsHtoa
gzI3NiXfd8sjHMOonZxu5pp/+UBI7tasYgVMMdUim1Yu
/c+t30d1Qw/v6NYLNNonywTu6HuUh7Y1sZRq/GZcrxLE
NXHQoyKpOrOr8R3+qd6wK69IKB80ZBztKX9rdEqKJk+y
YXjEzZz0zkAFthmNgCreAoU9PVlU66dyOsaLjf3wKU1U
m9SNOKs+tK6LuSmRbK6+1T/tPaRaMBSEuv2G6vXfnJlu
yMbGvtpRn/YDcvTjrp6DzE6XyF44QdwJ3oKx4ek=
) ; ZSK; alg = RSASHA256 ; key id = 8763
.
83906 IN DNSKEY 256 3 8 (
AwEAAeCYD6Z7WWKVLeuWgowKP+3g+Gs1cnLKq7a3CaQx
Qpv8bfuFVI0WnG33qaSH/Mw9IBgifrdf4XY/DQLnyBJ
9MfaOyAwuEaEmYJ+GQPiwVfstGwSAlMcfJUtTgq2H
uu74KARhtA8wPo/N3XcyYQtNhZ+qCM5NBb3ecx/naw6s
Yab9LxS6f2cU0q03++BP5Ks0Uef8WJCa/lizCYE+vMkw
oltV+tENa3hpXiZ7jle/xdgaZrPi5ZGmyLVI34g1XVYr
NlsCCtMnVfQIfzW5STFQFsQpizczyFn9r3LzSxxPCNwd
lCG84bER0Bmdwqbf6Tanv+FxMOavrahk j4wIy5k=
) ; ZSK; alg = RSASHA256 ; key id = 57780
.
83906 IN DNSKEY 257 3 8 (
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTO
iWlvkIbzxef3+/4RgWQ7HrxRixHlFlExOLAjr5emLvN
7SWXgnLh4+B5xQlNVz80g8kvArMtNR0xVQuCaSnIDdD5
LKyWbRd2n9WGe2R8PzqCmr3EgVLRjyBxWezF0jLHwVN8
efS3rCj/EWgviWgb9tarPVUDK/b58Da+sqqls3eNbuV7
pr+eoZG+SrDK6nWeL3c6H5Apzx7LjVclutIdsIXxuOLY
A4/ilBmSVIzuDwfdRufhHdY6+cn8HFRm+2hM8AnXGXws
9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
) ; KSK; alg = RSASHA256 ; key id = 20326
.
83906 IN DNSKEY 257 3 8 (
AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC
6rXTsDc449/cidltPKyGwCJNnOAlFNKF2jBosZBU5eeH
spaQWomOE1ZsjICMQMC3aeHbGiShvZsx4wMYSjH8e7Vr
hbu6irwCzVBAPESjbUdpWWmEnhathWu1jo+siFUiRAAx
m9qyJNg/wOZqqzL/dL/q8PkcRU5oUKEpUge71M3ej2/7
CPqpDVwuMoTvoB+ZOT4YeGyxMvHmbrx1FzGOHOijtzn+
ulTQNatX2XBuzZNQ1K+s2CXkPIZo7s6JgZyvaBevYtxP
vYLw4z9mR7K2vaF18UYH9Z9GnuUeayffKC73PYc=
) ; KSK; alg = RSASHA256 ; key id = 38696
.
83906 IN RRSIG DNSKEY 8 0 172800 (
20261022000000 20261001000000 20326 .
ARGOMBDyLkr5oQdR5OaIeoeBti1KWEX/LY/jZ1RRXwF0
f0eRZaljFpyVKFuZMzpafSYVs7eLOYjVYwJ3iENn4AEh
vX9iaKmWu3XpSSV0D6bhv5D6bk4GVPJ7NGTnA21r4fc9
lq9UD1kK1Q3jYJsxZSoQgJExDBfzwQUwleYLLPpi7TQf
+zAlwakHy2mkWnX1+bKDyrQ/p5ra4fgo/Pu7F47FXqRZ
EJ+K9o/TwA+nJn3RMS6dPaS46ERBSWHIeJAzQvNQELI4
pAbdVp3d3N33R2C5MxX6kUzNku8CtyXGYukSi9LK9GT3
nrH9O97tDADq01z78aPnj1+6hLTgMkiupw== )

;; Query time: 2 msec
;; SERVER: 192.168.2.254#53(192.168.2.254) (TCP)
;; WHEN: Sat Oct 10 13:00:22 CEST 2026
;; MSG SIZE rcvd: 1414

```

Les deux clés (KSK, "Key Signing Zone") sont publiées (ainsi que les clés de signature de la zone, ZSK "Zone Signing Zone", 8763, et la 57780 qui va bientôt être retirée <<https://mastodns.net/@diffroot/117422895898245760>>) mais seule 20326 signe les clés.

Depuis le remplacement, DNSviz nous montre la nouvelle situation <<https://dnsviz.net/d/root/asuYPQ/dnssec/>>. Et avec dig, nous avons (on demande directement à un serveur faisant autorité <<https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>> car les résolveurs <<https://www.bortzmeyer.org/resolveur-dns.html>> ont presque tous encore l'ancienne signature en mémoire) :

<https://www.bortzmeyer.org/remplacement-cle-dnssec-2026.html>

```
% dig @k.root-servers.net . DNSKEY

; <<>> DiG 9.18.39-0ubuntu0.24.04.7-Ubuntu <<>> @k.root-servers.net . DNSKEY
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 35242
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
; .      IN DNSKEY

;; ANSWER SECTION:
.      172800 IN DNSKEY 256 3 8 (
      AwEAAcorNxNc9t0uelZenPjVMRujlQ2YLBj0pR/4XMjh
      by9vr03cRxFSKnWpXeg5PL384D9VeqdS1bjrGyTsHtoa
      gzI3NiXfd8sjHMONZxu5pp/+UBIg7tasYgVMMdUiM1Yu
      /c+t30dlQw/v6NYLNnOnywTu6HuUh7Y1sZRq/GZcrxLE
      NXHQoyKpOrOr8R3+qd6wK69IKB80ZBZtkX9rdEqKjk+y
      YXjEzZz0zkAFthmNgCreAoU9PVlU66dyOsaLjf3wKULU
      m9SNOKs+tK6LuSmRbK6+1T/tPaRaMBSEuv2G6vXfnJ1u
      yMbGvtpRn/YDcvTjrp6DzE6XyF44QdwJ3oKx4ek=
      ) ; ZSK; alg = RSASHA256 ; key id = 8763
.      172800 IN DNSKEY 257 3 8 (
      AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTO
      iWlvkIbzxef3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN
      7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5
      LKYwbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHVVN8
      efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuV
      pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdIXxuOLY
      A4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws
      9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
      ) ; KSK; alg = RSASHA256 ; key id = 20326
.      172800 IN DNSKEY 257 3 8 (
      AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC
      6rXTsDc449/cidltPKyGwCJNnOAlFNKF2jBosZBU5eeH
      spaQWomOElZsjICMQMC3aeHbGiShvZsx4wMYSjH8e7Vr
      hbU6irwCzVBAPesjbUdpWWmEnhathWuljo+siFUiRAAX
      m9qyJNg/wOZqqzL/dL/q8PkcRU5oUKEpUge7lM3ej2/7
      CPqpdVwuMoTvoB+ZOT4YeGyxMvHmbrxlFzGOHOijtzn+
      ulTQNatX2XBuzZNQ1K+s2CXkPIZo7s6JgZyvaBevYtxP
      vYlW4z9mR7K2vaF18UYH9Z9GNUUeayffKC73PYc=
      ) ; KSK; alg = RSASHA256 ; key id = 38696
.      172800 IN RRSIG DNSKEY 8 0 172800 (
      20261101000000 20261011000000 38696 .
      1lXxlp+gWc4h/F9G8UPj3VXhNDQoZrco3Piivk7YMKs7
      pi8B+CBQHHPO/QNw+VfpNq7CtBDA6gxucyia1ZZx8yM0
      oLve7qJKgPuRVNnw5AOegtdxy+NKSy8rT6XNtCdM2gL9
      EmqKux+/JNATbZG2efGkVpHuirkq0Vs1bvYglVl6fvHb
      qoHpffjbnHVheuKpq+HvdsZOphoEJu74Y4lpYNBNTJijG
      gaJnJ64AUMPbMfu76uLi68CcWKDGWhzCNeSwnSjK7CA6
      aKte5StW61NuzONv8mvzqMX0epPQ7lXJ9Y/685081Bd
      zAYK3yMAfTOqL4EgluNZQAtAAh9bseJVyw== )

;; Query time: 25 msec
;; SERVER: 2001:7fd::1#53(k.root-servers.net) (UDP)
;; WHEN: Sun Oct 11 16:03:26 CEST 2026
;; MSG SIZE rcvd: 1139
```

Toujours les deux clés publiées, mais seule 38696 signe.

<https://www.bortzmeyer.org/remplacement-cle-dnssec-2026.html>

Vu la mémorisation des données par les résolveurs, tout va continuer à marcher comme avant. Voici la situation sur un résolveur quelconque, il reste 83[Caractère Unicode non montré²]548 secondes avant l'expiration :

```
% dig . DNSKEY
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.18.39-0ubuntu0.24.04.7-Ubuntu <<>> . DNSKEY
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 30170
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;.      IN DNSKEY

;; ANSWER SECTION:
.      83548 IN DNSKEY 257 3 8 (
  AwEAAz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTO
  iWlvkIbzxef3+/4RgW0q7HrxRixHlFlExOLAJr5emLvN
  7SWXgnLh4+B5xQlNVz8Og8kvArMtNR0xVQuCaSnIDdD5
  LKyWbRd2n9WGe2R8PzgCmr3EgVLRjyBxWezF0jLHwVN8
  efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuV7
  pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVcluTidsIXxuOLY
  A4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGxws
  9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
  ) ; KSK; alg = RSASHA256 ; key id = 20326
.      83548 IN DNSKEY 257 3 8 (
  AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC
  6rXTsDc449/cidltphyGwCJNnOAlFNKF2jBosZBU5eeH
  spaQWomOE1ZsjICMQMC3aeHbGiShvZsx4wMYSjH8e7Vr
  hbu6irwCzVBAPESjbUdpWWmEnhathWu1jo+siFUiRAAx
  m9qyJNg/wOZqqzL/dL/q8PkcRU5oUKEpUge7lM3ej2/7
  CPqpDvWuMoTvoB+ZOT4YeGyxMvHmbrxlFzGOHOijtzn+
  ulTQNatX2XBuzZNQ1K+s2CXkPIZo7s6JgZyvaBevYtxP
  vYLw4z9mR7K2vaF18UYH9Z9GnuUeayffKC73PYc=
  ) ; KSK; alg = RSASHA256 ; key id = 38696
.      83548 IN DNSKEY 256 3 8 (
  AwEAAcorNxC9t0ue1ZenPjVMruj1Q2YLBj0pR/4XMjH
  by9vr03cRxFsKnWpxeg5PL384D9VeqdS1bjrGyTsHtoa
  gzI3NiXfD8sjHMonZxu5pp/+UBIg7tasYgVMMdUiM1Yu
  /c+t30dlQw/v6NYLnnOnyWtu6HuUh7Y1sZRq/GZcrxLE
  NXHQoyKpOrOr8R3+qd6wK69IKB80ZBztKX9rdEqKJk+y
  YXjEZzZ0zkAFthmNgCreAoU9PVLU66dyOsaLjf3wKULU
  m9SNOKs+tK6LuSmRbK6+1T/tPaRaMBSEuv2G6vXfnJlu
  yMbGvtpRn/YDcvTjrp6DzE6XyF44QdwJ3oKx4ek=
  ) ; ZSK; alg = RSASHA256 ; key id = 8763
.      83548 IN DNSKEY 256 3 8 (
  AwEAAeCYD6Z7WWKVLeuWgowKP+3g+Gs1cnLKq7a3CaQx
  Qpv8bfuFVIOwnG33qaSH/Mw9IBgfrdzf4XY/DQLnyBJ
  9MfaOyAWuEaEmYJ+GQPiwVfstGwSA1McFFJUttTgq2H
  uu74KARhtA8wPo/N3XcyYQtNhZ+qCM5NBb3ecx/naw6s
  Yab9LxS6f2cU0q03++BP5Ks0Uef8WJCa/lizCYE+vMkw
  oltV+tENa3hpXiZ7jle/xdgaZrPi5ZGmyLVI34g1XVYr
  NlsCCTmNvFQIfzW5STFQFsQpizczyFn9r3LzSxxPCNwd
  lCG84bER0Bmdwqbf6Tanv+FxMOavrahkj4wIy5k=
  ) ; ZSK; alg = RSASHA256 ; key id = 57780
.      83548 IN RRSIG DNSKEY 8 0 172800 (
  20261022000000 20261001000000 20326 .
  ARGOMBDyLkr5oQdR5OaIeoeBti1KWEX/LY/jZlRRXwF0
```

2. Car trop difficile à faire afficher par $\LaTeX$

<https://www.bortzmeyer.org/remplacement-cle-dnssec-2026.html>

```
f0eRZaljFpyVKFuZMzpafSYVs7eLOYjVyWJ3iENn4AEh
vX9iaKmWu3XpSSV0D6bhv5D6bk4GVPJ7NGTnA2lr4fC9
lq9UD1kK1Q3jYJsxZSoQgjExDBfzwQUw1eYLLPPI7TQf
+zAlwakHy2mkWnX1+bKDyrQ/p5ra4fgo/Pu7F47FXqRZ
EJ+K9o/TwA+nJn3RMS6dPaS46ERBSWHIeJAzQvNQELI4
pAbdVp3d3N33R2C5MxX6kUzNku8CtyXGYukSi9LK9GT3
nrH9O97tDADq01z78aPnjl+6hLTgMkiupw== )
```

```
;; Query time: 2 msec
;; SERVER: 192.168.2.254#53(192.168.2.254) (TCP)
;; WHEN: Sun Oct 11 16:31:33 CEST 2026
;; MSG SIZE rcvd: 1414
```

Au fur et à mesure que le TTL expire, les résolveurs vont récupérer la nouvelle signature des clés (et, normalement, tout se passera bien, les utilisateurs ne verront rien).