DNSSEC: Rollin’, Rollin’, Rollin’

Ralph Dolmans
ralph@nlnetlabs.nl

Martin Hoffmann
martin@nlnetlabs.nl

https://www.nlnetlabs.nl/
DNS – resolving IPv6 address for nlnetlabs.nl

Resolver

. (root) zone

nl zone

nlnetlabs.nl zone
AAAA 2a04:b900::10:0:10
Answer with DNSSEC signature

;; QUESTION SECTION:

;nlnetlabs.nl.  IN  AAAA

;; ANSWER SECTION:
nlnetlabs.nl.  10200  IN  AAAA  2a04:b900::1:0:0:10

nlnetlabs.nl.  10200  IN  RRSIG  AAAA  8 2 10200 20180529005003 20180501005003 42393 nlnetlabs.nl. HcAuIC0d5eCYZYwsoEDymzQOBRR5SmhJUZwv6n[...]

https://www.nlnetlabs.nl/
DNSSEC authentication chain

. (root) zone
  . DNSKEY – KSK
  . DNSKEY – ZSK
  . RRSIG(DNSKEY)

.nl zone
  nl DNSKEY – KSK
  nl DNSKEY – ZSK
  nl RRSIG(DNSKEY)

nlnetlabs.nl zone
  nlnetlabs.nl DNSKEY – KSK
  nlnetlabs.nl DNSKEY – ZSK
  nlnetlabs.nl RRSIG(DNSKEY)
  nlnetlabs.nl AAAA
  nlnetlabs.nl RRSIG(AAAA)
Root KSK roll

- Original timeline:
  - 26\(^{th}\) October 2016 – new key created
    - Keytag 20326
  - 11\(^{th}\) July 2017 – new key published in root zone
    - Start in-band update mechanism
  - 11\(^{th}\) October 2017 – use new key to sign root DNSKEY rrset
    - Validation will fail for users that only have KSK2010 as TA
Root KSK roll

- Original timeline:
  - 26th October 2016 – new key created
  - 11th July 2017 – new key published in root zone
  - 11th October 2017 – use new key to sign root DNSKEY rrset

Validation will fail for users that only have KSK2010 as TA.

172800 IN DNSKEY 257 3 8 (AwEAAaz/tAm8yTn4Mfeh5eyl96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHIFlExOLAjr5emLvN7SWXgnLh4+B5xQINVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVlrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLY A4/iBmSVIzuDWfdRUsfhHdY6+cn8HFRm+2hM8AnXGxws 9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=) ; KSK; alg = RSASHA256; key id = 20326
Updating DNSSEC Trust Anchors

- Manually
- Outside DNS protocol (e.g. software update)
- In DNS protocol → RFC5011 (“Automated Updates of DNS Security (DNSSEC) Trust Anchors”)
  - Using trust in existing TA to start trusting another key
  - New root TA in resolvers on 11th August 2017

https://www.nlnetlabs.nl/
RFC8145 Trust Anchor Reports for All Root Servers

- Number of sources reporting trust anchor data
- Number of sources reporting only KSK-2010
- Percentage of sources reporting only KSK-2010

Number of sources reporting trust anchor data:

- 01-Sep-17
- 01-Oct-17
- 01-Nov-17
- 01-Dec-17
- 01-Jan-18
- 01-Feb-18

Percentage of sources reporting only KSK-2010:

- 01-Sep-17
- 01-Oct-17
- 01-Nov-17
- 01-Dec-17
- 01-Jan-18
- 01-Feb-18

https://www.nlnetlabs.nl/
Root key sentinel (draft-ietf-dnsop-kskroll-sentinel)

- User impact on root key roll
  - root-key-sentinel-is-ta-20326
  - root-key-sentinel-not-ta-20326
  - Some bogus domain

- In Unbound, BIND and Knot resolver

- No results available yet

https://www.nlnetlabs.nl/
## RFC 5011 in Open Source Resolvers

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unbound</td>
<td>PowerDNS Recursor</td>
</tr>
<tr>
<td>Bind</td>
<td>Dnsmasq</td>
</tr>
<tr>
<td>Knot Resolver</td>
<td>systemd-resolved</td>
</tr>
</tbody>
</table>

https://www.nlnetlabs.nl/
Test Scenarios

- Happy Path
- Un-publish before signing
- Roll-back after signing
- Revocation of old key
- Early re-introduction of old key
- Un-revoked old key
- Late re-introduction of old key
- Missing new key
- Non-writeable state directory

- Resolver restarts
- Restarts with non-writable state directory
- Late installation with old key only
- Late installation with both keys
- Post-roll installation with old key only
- Post-roll installation with new key only
- Happy path with forwarding to a non-validating resolver
- Happy path while forwarding to a non-DNSSEC resolver

https://www.nlnetlabs.nl/
# Unbound

## Versions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>First production release</td>
<td>1.0.0</td>
<td>2008-05-20</td>
</tr>
<tr>
<td>RFC 5011 since</td>
<td>1.4.0</td>
<td>2009-11-26</td>
</tr>
<tr>
<td>Latest release</td>
<td>1.7.1</td>
<td>2018-05-03</td>
</tr>
<tr>
<td>Current Debian stable</td>
<td>1.6.0</td>
<td>2016-12-15</td>
</tr>
</tbody>
</table>

[https://www.nlnetlabs.nl/](https://www.nlnetlabs.nl/)
Unbound

Findings

Late Installation

- Only trusts the new trust anchor after the 30 days’ hold down.
- Even if the new trust anchor is provided on installation.
- Fixed in 1.6.5 (2017-08-21).

Re-introduction of Old Key

- accepts the old key after remove and add hold-downs.
Unbound
Operational

RFC 5011 needs to be explicitly enabled

- trust-anchor-file v. auto-trust-anchor-file

Non-writable state directory

- initially: logs error and carries on until next restart
- 1.5.4 (2015-07-09): logs error and stops
# cat /var/lib/unbound/root.key
; autotrust trust anchor file
; ;id: . 1
; ;last_queried: 1525860779 ; ;Wed May  9 12:12:59 2018
; ;last_success: 1525860779 ; ;Wed May  9 12:12:59 2018
; ;next_probe_time: 1525901662 ; ;Wed May  9 23:34:22 2018
; ;query_failed: 0
; ;query_interval: 43200
; ;retry_time: 8640.
.172800  IN  DNSKEY  257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAYkMgJzkKTQiW1vkIbzxieF3/+4RqWoq7HrxRixHlFlEXOLAJf7amLvN7SwXg3nLh4+B5xQ
1NV28qGkvsArMtNROxVQuCaSnIdd5LKvWrBd2n9Gew2R8PzgCm33GvLrryBxwEsF0jJhvwV8efS3rCj/dEcIwgb9ta7rPVUDK/
b58Da+Sq9ls3eNbu7vpr+eoZG+SrDK6nWeL3c6H5Apzx7LjVc1u7idSIxSU0LYA4/11BmSViZuDFWdRufHhY6+cn8HFRm+2h8M8AnXGxw9555KrUB5qiylGa8sux2Nn6UuwNR1AkUTV74bU= ;{id = 20326 (ksk), size = 2048b} ; ;state=2 [ VALID ] ; ;count=0 ; ;lastchange=1525860756 ; ;Wed May  9 12:12:36 2018
23800  IN  DNSKEY  257 3 8
AwEAAaqAIklVzrpC6ia7qEzaIQR9+9W29euxhJhVVLOv0bSEW008gcCjFFVOUTf6v58flJwBd0YI0EzrAcQqBGCzh/
RSti08og0NnfnL2MTJkoxXbfDaUeVp0707Ye5D71Z7wA0YnVYDXY/VHL496M/QZxkif5/Efucp2gafD6sRs6CxoP068lsVpYjR0ZsWzziapAav9d1Zc6hX7ICJBBtuA6G3LQpzW5h0A2hzaCmMjJPJ8LbqF6dsV6oBOqguol0sGI
cG0Yl7OyqDxf257relS0ageu+iBAdTTJ25AsRTAoub880NGcmLmqrAmRLKBp1dfwYhYB4N7knNnulq1A+Uk11hzo= ;{id = 19036 (ksk), size = 2048b} ; ;state=2 [ VALID ] ; ;count=0 ; ;lastchange=1525860756 ; ;Wed May  9 12:12:36 2018

Do I have the new KSK?

new KSK

old KSK

auto-trust-anchor-file
## Bind 9

### Versions

<table>
<thead>
<tr>
<th>Version Type</th>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>First production release</td>
<td>9.0.0</td>
<td>2000-09-16</td>
<td></td>
</tr>
<tr>
<td>First still usable release*</td>
<td>9.6.2</td>
<td>2010-03-01</td>
<td>*supporting RSASHA256</td>
</tr>
<tr>
<td>RFC 5011 since</td>
<td>9.7.0</td>
<td>2010-02-16</td>
<td></td>
</tr>
<tr>
<td>RFC 5011 working since*</td>
<td>9.7.1</td>
<td>2010-06-17</td>
<td>*according to our test</td>
</tr>
<tr>
<td>Latest release</td>
<td>9.12.1</td>
<td>2018-03-14</td>
<td></td>
</tr>
<tr>
<td>Current Debian stable</td>
<td>9.10.3</td>
<td>2015-09-16</td>
<td></td>
</tr>
</tbody>
</table>
Bind 9

Findings

Re-introduction of Old Key

- initially: accepts the old key even before the hold-downs have passed.
- 9.10.2 (2015-02-25): never accepts revoked keys again

Post-roll Installation with Old Key

- initially: resolver goes insecure instead of bogus
- 9.10.4 (2016-04-28): fixed

https://www.nlnetlabs.nl/
Bind 9

Operational

RFC 5011 needs to be explicitly enabled

- `trusted-keys` v. `managed-keys`

Non-writable state directory

- Initially: repeatedly logs and carries on; upon restart goes insecure
- 9.8.1 (2011-08-31): logs error once and carries on; upon restart goes bogus
Bind 9
Do I have the new KSK?

# rndc secroots
# cat /var/cache/bind/bind/named.secroots
09-May-2018 11:01:55.792

Start view _default

./RSASHA256/20326 ; managed
./RSASHA256/19036 ; managed

new KSK
old KSK

It does 5011

https://www.nlnetlabs.nl/
## Knot Resolver

### Versions

<table>
<thead>
<tr>
<th>Version Description</th>
<th>Version</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>First production release</td>
<td>1.0.0</td>
<td>2016-06-21</td>
</tr>
<tr>
<td>RFC 5011 since</td>
<td>1.0.0</td>
<td>*</td>
</tr>
<tr>
<td>Latest release</td>
<td>2.3.0</td>
<td>2018-04-23</td>
</tr>
<tr>
<td>Current Debian stable</td>
<td>1.2.0</td>
<td>2017-01-25</td>
</tr>
</tbody>
</table>

* in our tests first working in 1.2.0, faulty in 1.2.2, then working again in 1.5.0

[https://www.nlnetlabs.nl/](https://www.nlnetlabs.nl/)
Knot Resolver

Findings*

Re-introduction of old key
- accepts the old key after remove and add hold-downs

Late installation with old key only
- 1.2.0: accepts the new key during the add hold-down but not after
- 1.2.5: accepts the new key for one day only

Revocation of old key
- 1.5.0: accepts the old key for only day after removal from DNSKEY record.

* last test was on 1.2.0

https://www.nlnetlabs.nl/
Knot Resolver

Operational

Trust anchors are always update via RFC 5011. \o/

Non-writable state directory

- initially: stops at start with permission denied
- 1.5.1: same message but keeps running and goes bogus one day late
- 2.0.0: stops at start again.

- Resolver restarts
  - 1.2.0: add hold-down restart with every restart if trust anchor is kept but config directory recreated, otherwise bogus three days after key roll.
  - 2.0.0: fixed

https://www.nlnetlabs.nl/
Knot Resolver

Do I have the new KSK?

```
# cat /etc/knot-resolver/root.key

172800 DNSKEY 257 3 8
AwEAAagAIK1VZrpC6Ia7gEzah0R+9W29euxhJhVVL0yQbSEW008gcCjFFVQUTf6v58f
LjwBd0YI0EzrAcQqBGCzh/RStIo08g0NfniL2MTJRkxoXbfDaUeVPQuYehg37NzwAJQ9VnMVDxP/VHL496M/
QZxkJf57
Efucp2gDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LqzW5
h0A2h2zCTMjJPJ8LfqF6dsV6oBQzgu0sGlcG0y170yQdXfZ57re1S0ageu+ipAdTTJ
25AsRTAoub80NGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ; Valid: ;
KeyTag:19036

172800 DNSKEY 257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTQiW1vkbzxeF3+/4RqWoq7Hr
xRixHlFlEXOLAJr5emLvN7SWXgnLh4+B5xQ1NVz80g8kvArMtNROxVQuCaSnGDdD5LKy
yWbRd2n9WGe2R8PzqCmr3EgVLrjyBxWezf0jLHwVN8efS3rCj/
EwgwWgb9tarpVUDK/b58Da+sqq7s3eNbu7vr+eoZG+SvDK6nWeL3c6H5Apzx7LjVc1uTIdsIXxu0LYA4/
IlBmSVIzuDWFdRUFhDdY6+cn8HFRm+2hM8AnXGws9555KrUB5qihyLGa8subX2Nn6U
wNR1AkUT74bU= ; Valid: ; KeyTag:20326
```
PowerDNS Recursor

Do I have the new KSK?

# rec_constrol get-tas
Configured Trust Anchors:

19036 8 2 49aac11d7b6f6446702e54a1607371607a1a41855200fd2ce1cdde32f24e8fb5
20326 8 2 e06d44b80b8f1d39a95c0b0d7c65d08458e880409bbc683457104237c7f8ec8d

20326 missing?

- upgrade to at least 4.0.5
- https://doc.powerdns.com/recursor/dnssec.html#trust-anchors

https://www.nlnetlabs.nl/
Dnsmasq

Do I have the new KSK?

• Configuration includes somewhere:

```
dnssec
trust-anchor=.,19036,8,2,49AAC1...
trust-anchor=.,20326,8,2,E06D44...
```
systemd-resolved

Do I have the new KSK?

- Root trust anchors are baked into the source.
- New KSK added in version 233 (2017-03-12), probably backported in various stable distributions.
- src/resolve/resolved-dns-trust-anchor.c

```c
static int dns_trust_anchor_add_builtin_positive(DnsTrustAnchor *d) {
    /* ... */
    r = add_root_ksk(answer, key, 20326, /* ... */);
    /* ... */
}
```

https://www.nlnetlabs.nl/
What happens next?

ICANN proposed to proceed to roll on October 11 this year.

- Public comment period ended April 1.
- 20 comments, mostly in favor of going ahead.
- Final plan should be published any day now.