KSK algorithm rollover for .nl

Stefan Ubbink | FOSDEM 2024, Brussels

3 February 2024

Public
Agenda

1. Why
2. Preparation
3. Planning
4. Executing
5. Measurements

Photo by Stefan Ubbink
Why?

- Using a safer algorithm
- Keeping up with new recommendations
- Enough support in resolvers
- Smaller DNSSEC answers

Source: https://dnsthought.nlnetlabs.nl
Preparation

• New Thales HSM for better ECDSA performance
• Test, test, test
  • Normal run on test setup, using a fakeroot
  • Local DNSviz
• Lab setup with fast policy
• Acceptance with real data and policy
  0 Memory usage
  0 Time needed for validation of the signed zone
Planning

• Based on acceptance run
• Dependencies
  • External parties (IANA)
  • ZSK rollover
Planning

• 4 July: preparation
• 5 July: change OpenDNSSEC policies
• 11 July: Add algo 13 DS to the root zone
• 14 July*: check algo 13 path
• 17 July*: remove algo 8 DS from the root zone
• 19 July*: delete algo 8 keys from OpenDNSSEC.

* dependent on external parties

Photo by Alexander Schimmeck on Unsplash
Executing

- Use written plan with commands and checks
- Continual checking
- DNsViz at strategic times
- Go-No go

<table>
<thead>
<tr>
<th>When</th>
<th>.nl size (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before</td>
<td>4.5</td>
</tr>
<tr>
<td>During</td>
<td>6.4</td>
</tr>
<tr>
<td>After</td>
<td>3.7</td>
</tr>
</tbody>
</table>
Algorithm 8 situation

https://dnsviz.net/d/nl/ZKO0xA/dnssec/
Policy change

https://dnsviz.net/d/nl/ZKUx5g/dnssec/
Add algorithm 13 DS to root

https://dnsviz.net/d/各自/ZLDMUA/dnssec/
Remove algorithm 8 DS from root

https://dnsviz.net/d/nl/ZLdb4Q/dnssec/
Stop using algorithm 8

https://dnsviz.net/d/nl/ZLuFjA/dnssec/
Measurements with RIPE Atlas probes

- Rollover-mon
- Propagation delay for DNSKEY (1/h)
- Propagation delay for DS (1/d)
- DNSKEY @nsX.dns.nl (5 min)
- DS records @root servers (5 min)
- Trust chain (1/h)
- 17153 = EC KSK
Measurements

- Strange measurements
- Caused by
  - Small buffersize
  - Trying to get key ID from fragments
Response sizes in bytes*

<table>
<thead>
<tr>
<th>Type</th>
<th>Before</th>
<th>During</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXDOMAIN</td>
<td>1015</td>
<td>1402</td>
<td>759</td>
</tr>
<tr>
<td>DNSKEY</td>
<td>766</td>
<td>1024</td>
<td>310</td>
</tr>
<tr>
<td>NS</td>
<td>1214</td>
<td>1022</td>
<td>928</td>
</tr>
</tbody>
</table>

* Only showing sizes from ns1.dns.nl (v6 and v4), based on DNSviz data, other implementations differ
Change in TCP traffic

• Before: ~1% TCP queries (~359 qps)
• During: ~5% TCP queries (~2421 qps)
• After: ~1% TCP queries

Source: stats.sidnlabs.nl
Change in TCP traffic
Lack of TCP support

• Increase of 1.6 times
• 25% had an increase of 8 times
• Keep asking via UDP
• University measurements
• Impact unknown
• No failure reports
Measurements

• Removing the RSA KSK
No measured impact
Are there any questions?
Thank you for your attention!