DNSSEC Operational Practices: The Good, The Bad and The Ugly

Roland van Rijswijk-Deij
Nordic Domain Days

joint work with: Tho Le, Luca Allodi and Nicola Zannone of TU Eindhoven
DNSSEC in the second decade

- Mass deployment of DNSSEC took off in 2008, after "Kaminsky"
- We have just entered the second decade of DNSSEC
- Things seem to be going well:
  - Vast majority of top-level domains support DNSSEC
  - Number of validating resolvers still growing
- But also: many "important" domains still not signed (Google, Facebook, Amazon, ...)

DNSSEC in the Nordic region

- .no 58%
- .se 54%
- .is 3%
- .dk 2%
- .fi 1%

For comparison:

- .com 0.7%
- .net 1%
- .org 1%

But also:

- .nl 53%

What do these have in common?
Incentives, incentives, incentives, incentives!
Studying incentives

- **Both** .nl and .se **have financial incentives for registrars** to encourage DNSSEC deployment.

- These **incentives are modest** (a few percent discount on registration).

- This means that the incentives **only pay off financially if you deploy** DNSSEC **for 100,000s of domains**.

- While this **clearly** has **led to mass deployment** of DNSSEC, we wondered if it has **also led to secure deployments**?
Study goals

• We wanted to **study** the **quality** of DNSSEC deployments **in terms of security** as defined in DNSSEC best practices

• Our **assumption**: only large operators benefit economically from incentives, therefore **we expect small operators to deploy** DNSSEC with a different motivation

• **Hypothesis:**
  "Despite the presence of 'per-domain' economic incentives in .nl and .se, large DNS operators deploy DNSSEC with lower compliance to security guidelines than small DNS operators."
DNSSEC in two slides

**KSK**

**ZSK**

**DNSKEY set**

**signs**

**RRs**

**contains**

**DS**

**root zone**

**.com zone**

**KSK**

**ZSK**

**DNSKEY set**

**signs**

**RRs**

**contains**

**DS**

**hash of**

**example.com zone**

**KSK**

**ZSK**

**DNSKEY set**

**signs**

**RRs**

**contains**

**www**
DNSSEC in two slides

- "from" key
- "to" key
- zone signatures
- rollover moment

- active signing key
- pre-publication of new key
- post-publication of old key
- signatures with old key
- signatures with new key
## Best Current Practice

<table>
<thead>
<tr>
<th>Aspects</th>
<th>NIST recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key size</td>
<td>- ECDSA keys.</td>
</tr>
<tr>
<td></td>
<td>- RSA: KSKs $\geq$ 2048 bits and ZSKs $\geq$ 1024 bits.</td>
</tr>
<tr>
<td>Key algorithm</td>
<td>- Recommended: Algorithms 8 and 10.</td>
</tr>
<tr>
<td>Key rollover</td>
<td><strong>KSKs/CSKs:</strong></td>
</tr>
<tr>
<td></td>
<td>- ECDSA keys and RSA keys (with key size $\geq$2048 bits): rollover within 24 months.</td>
</tr>
<tr>
<td></td>
<td><strong>ZSKs:</strong></td>
</tr>
<tr>
<td></td>
<td>- 1024-bit RSA keys: rollover within 90 days.</td>
</tr>
<tr>
<td></td>
<td>- RSA keys’ size between 1024 - 2048 bits: rollover within 12 months.</td>
</tr>
<tr>
<td></td>
<td>- ECDSA keys and RSA keys (with key size $\geq$ 2048 bits): rollovers within 24 months.</td>
</tr>
</tbody>
</table>
For this study we used data from the OpenINTEL project

https://openintel.nl/
## Approach

<table>
<thead>
<tr>
<th>TLDs</th>
<th>Measurement Period</th>
<th>#Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>.net</td>
<td>2015-02-28 - 2017-07-31</td>
<td>13,011,428</td>
</tr>
<tr>
<td>.org</td>
<td>2015-02-28 - 2017-07-31</td>
<td>9,373,214</td>
</tr>
<tr>
<td>.nl</td>
<td>2016-02-09 - 2017-07-31</td>
<td>5,440,975</td>
</tr>
<tr>
<td>.se</td>
<td>2016-06-07 - 2017-07-31</td>
<td>1,440,244</td>
</tr>
</tbody>
</table>

- For comparison
- Focus of study

- Analyse RRSIG and DNSKEY records for **all signed domains every day**
  to check key sizes, algorithms and key rollovers
Rollover complexity

1. Monthly view

2. Merge via key tag

3. Validate duplicated key_tag keys

4. Add

5. Identify key effective period

6. Compare to the last day of a month

Active keys

Retired keys

Previous keys

Keys
Large versus Small

Just 14 operators responsible for over 80% of signed domains

Just 3 operators responsible for over 80% of signed domains
All the DNSSEC large and small

- To check if **large operators** are more likely to deploy DNSSEC under an incentive, we compared .com/.net/.org to .nl and .se

<table>
<thead>
<tr>
<th>TLD</th>
<th>#Domains</th>
<th>#Signed</th>
<th>%</th>
<th>#Domains</th>
<th>#Signed</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>.com</td>
<td>93,464,626</td>
<td>712,162</td>
<td>0.76%</td>
<td>23,349,922</td>
<td>224,251</td>
<td>0.96%</td>
</tr>
<tr>
<td>.net</td>
<td>10,412,605</td>
<td>114,687</td>
<td>1.10%</td>
<td>2,598,823</td>
<td>26,400</td>
<td>1.02%</td>
</tr>
<tr>
<td>.org</td>
<td>7,501,310</td>
<td>85,166</td>
<td>1.14%</td>
<td>1,871,904</td>
<td>20,342</td>
<td>1.09%</td>
</tr>
<tr>
<td>.nl</td>
<td>4,353,518</td>
<td>2,736,393</td>
<td>62.85%</td>
<td>1,087,457</td>
<td>92,791</td>
<td>8.53%</td>
</tr>
<tr>
<td>.se</td>
<td>1,153,129</td>
<td>723,532</td>
<td>62.75%</td>
<td>287,115</td>
<td>13,794</td>
<td>4.80%</td>
</tr>
</tbody>
</table>

- **Takeaway:** uptake among large operators is an order of magnitude higher under an incentive!
Results for large operators in .nl

<table>
<thead>
<tr>
<th>DNS operator</th>
<th>Master NS†</th>
<th>#Signed</th>
<th>Algorithm</th>
<th>KSK size</th>
<th>ZSK size</th>
<th>ZSK Rollover</th>
</tr>
</thead>
<tbody>
<tr>
<td>TransIP</td>
<td>*.transip.net.</td>
<td>265,341</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Metaregistrar BV</td>
<td>*.metaregistrar.nl.</td>
<td>386,913</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Hostnet BV Network</td>
<td>*.hostnet.nl.</td>
<td>359,793</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Cyso Hosting</td>
<td>*.firstfind.nl.</td>
<td>246,385</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Argeweb BV</td>
<td>*.argewebhosting.eu.</td>
<td>101,993</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Openprovider</td>
<td>*.openprovider.nl.</td>
<td>79,367</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Village Media BV</td>
<td>*.webhostingserver.nl.</td>
<td>67,150</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Hosting2GO</td>
<td>*.hosting2go.nl.</td>
<td>64,568</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Flexwebhosting BV</td>
<td>*.flexwebhosting.nl.</td>
<td>60,753</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Internedservices</td>
<td>*.is.nl.</td>
<td>57,033</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>Neostrada</td>
<td>*.neostrada.nl.</td>
<td>56,295</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>One.com</td>
<td>*.one.com.</td>
<td>55,397</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>PCextreme</td>
<td>*.pcextreme.nl.</td>
<td>50,102</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
<tr>
<td>AXC B.V.</td>
<td>*.axc.nl.</td>
<td>47,861</td>
<td>x</td>
<td></td>
<td>+</td>
<td>x</td>
</tr>
</tbody>
</table>

- **Measured over 18 months** (so no KSK rollover)

**Takeaways:**

- **Algorithm and key sizes** mostly OK
- **ZSKs** are mostly 1024-bits (borderline secure) but are never rolled!
Results for large operators in .se

• **Measured over 14 months**
  (so no KSK rollover)

**Takeaways:**

• Story **similar to .nl**

• **Algorithm and key sizes**
  mostly **OK**

• **ZSKs** borderline secure
  but **never rolled!**

---

<table>
<thead>
<tr>
<th>DNS operator</th>
<th>Master NS†</th>
<th>#Signed</th>
<th>Algorithm</th>
<th>KSK size</th>
<th>ZSK size</th>
<th>ZSK Rollover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopia AB</td>
<td>*.loopia.se.</td>
<td>282,604</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>One.com</td>
<td>*.one.com.</td>
<td>221,372</td>
<td>✓</td>
<td>✰</td>
<td>✓+</td>
<td>✗</td>
</tr>
<tr>
<td>Binero AB</td>
<td>*.binero.se.</td>
<td>123,131</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

---

Measured over 14 months

Story similar to .nl

Algorithm and key sizes mostly OK

ZSKs borderline secure but never rolled!
What about the smaller operators?

Takeaways: Domains from **small operators** much more likely to roll their ZSKs properly

Compliance is **independent of size**
Why are large operators not rolling?

- Are you in the room? I'd love to hear from you!
- DNSSEC is complex; rollovers are arguably hard and potentially risky
- We know (from private communication) some large operators implement their own DNSSEC signer systems
- Rolling keys not a requirement to qualify for the DNSSEC incentive
- Smart operators know: reduce complexity -> reduce operational risk
- No one wants to be called out of bed at 3AM because of a DNSSEC problem
I have a theory about .se

• I had a quick look in OpenINTEL last week, for RSA keys in .se:

<table>
<thead>
<tr>
<th>key size</th>
<th>key type</th>
<th>#dns records</th>
<th>#unique keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>2048</td>
<td></td>
<td>651255</td>
<td>202802</td>
</tr>
<tr>
<td>2048</td>
<td></td>
<td>1841</td>
<td>1839</td>
</tr>
<tr>
<td>1024</td>
<td></td>
<td>257</td>
<td>1179</td>
</tr>
<tr>
<td>1024</td>
<td></td>
<td>256</td>
<td>1171742</td>
</tr>
</tbody>
</table>

Lots of key sharing

• Note: rollovers are even trickier when you're sharing keys
Conclusions

• Incentives got us massive DNSSEC deployment
• But not necessarily secure deployments!
• So perhaps it is time to tighten incentive requirements
• How to do this while keeping operators on board?
Recommendations

• Need to account for operational reality; operators want to minimise risk

• One way forward: use Elliptic Curve signing algorithms!
  • Smaller keys that are cryptographically much stronger (e.g. ECDSA P-256 roughly equivalent to 3072-bit RSA)
  • Not rolling a key is not a problem; according to current insights, these keys are good for 30+ years*
  • Widely supported by validating resolvers (source: rootcanary.org)
Thank you! Questions?

LinkedIn: nl.linkedin.com/in/rolandvanrijswijk

Twitter: @reseauxsansfil

Email: roland@nlnetlabs.nl