A Look at RFC 8145 Trust Anchor Signaling for the 2017 KSK Rollover – The Good Parts

ICANN 60 DNSSEC Workshop

Duane Wessels

November 1, 2017
RFC 8145 -- Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)
RFC 8145 – Key Tag Signaling

• Validators periodically report trust anchor key tags.

• What’s a key tag?

  • A 16-bit integer that identifies and enables efficient selection of DNSSEC public keys. Much like a ones’ complement checksum.

  • 19036 – key tag for KSK-2010

  • 20326 – key tag for KSK-2017

• Reported to a zone’s authoritative name servers.

• Should be transmitted about as frequently as DNSKEY expire.
Two Forms of Key Tag Signaling

• edns-key-tag option.
  • An appended option code in the ENDS0 / OPT record

• Separate key tag query.

• Key tag encoded in query name, using hexadecimal representation.
  • 19036 = hex 4a5c
  • 20326 = hex 4f66
# Timeline & Implementations

<table>
<thead>
<tr>
<th>When</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 December</td>
<td>draft-ietf-dnsop-edns-key-tag-00</td>
</tr>
<tr>
<td>2016 July</td>
<td>First implementation in BIND</td>
</tr>
<tr>
<td>2017 February</td>
<td>draft-ietf-dnsop-edns-key-tag-05</td>
</tr>
<tr>
<td>2017 April</td>
<td>RFC 8145</td>
</tr>
<tr>
<td>2017 April</td>
<td>First implementation in Unbound</td>
</tr>
<tr>
<td>2017 May</td>
<td>Start collecting data</td>
</tr>
</tbody>
</table>

BIND: ‘trust-anchor-telemetry’ defaults to ‘yes’

Unbound: initially ‘trust-anchor-signaling’ defaults to ‘no’, changed to ‘yes’ around October 1, 2017
Data
Data Sources

- Key Tag signals are sent to the name servers authoritative for the key they represent.
- In this case, the root zone.
- This data comes from A-root and J-root.
- Selection bias caveat: data provided by only relatively recent implementations.
### Data Sample

```sql
SELECT `timestamp`,lower(qname),dstip,srcip,year,month,day
FROM some_hadoop_hive_table
WHERE lower(qname) rlike '^_ta-'
AND qtype = 10
AND product = 'root';
```

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Qname</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Year</th>
<th>Month</th>
<th>Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>1500479443</td>
<td>_ta-4a5c</td>
<td>128.x.x.x</td>
<td>192.58.128.30</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500439539</td>
<td>_ta-4a5c</td>
<td>2a00:x:x::x</td>
<td>2001:503:ba3e::2:30</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500476401</td>
<td>_ta-4a5c</td>
<td>2001:x:x::x</td>
<td>2001:503:c27::2:30</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500476401</td>
<td>_ta-4a5c</td>
<td>2001:x:x::x</td>
<td>2001:503:c27::2:30</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500495841</td>
<td>_ta-4a5c-4f66</td>
<td>188.x.x.x</td>
<td>198.41.0.4</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500464521</td>
<td>_ta-4a5c</td>
<td>5.x.x.x</td>
<td>192.58.128.30</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500476401</td>
<td>_ta-4a5c</td>
<td>2001:x:x::x</td>
<td>2001:503:c27::2:30</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500476401</td>
<td>_ta-4a5c</td>
<td>194.x.x.x</td>
<td>198.41.0.4</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500476401</td>
<td>_ta-4a5c</td>
<td>2001:x:x::x</td>
<td>2001:503:c27::2:30</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500476401</td>
<td>_ta-4a5c</td>
<td>194.x.x.x</td>
<td>198.41.0.4</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>1500495841</td>
<td>_ta-4a5c-4f66</td>
<td>188.x.x.x</td>
<td>198.41.0.4</td>
<td>2017</td>
<td>7</td>
<td>19</td>
</tr>
</tbody>
</table>
Root Zone Key Tag Signaling — Number of Sources

Number of Signalers

May | Jun | Jul | Aug | Sep | Oct | Nov

KSK-2017 Published

RFC5011 Hold Down Timer Ends

Verisign Public
Number of Signalers

- Not-Updated
- Mixed
- Updated

KSK-2017 Published

RFC5011 Hold Down Timer Ends
Root Zone Key Tag Signaling — Number of Sources

Sources always signaling 2010 TA only.

Sources sometimes signaling 2010 TA and sometimes 2010+2017 TAs

Sources always signaling 2010+2017 TAs only

Number of Signers

May  Jun  Jul  Aug  Sep  Oct  Nov

Root Zone Key Tag Signaling — TA Update Evidence

Percent of Signalers

- 0%
- 20%
- 40%
- 60%
- 80%
- 100%

May  Jun  Jul  Aug  Sep  Oct  Nov

KSK-2017 Published

RFC5011 Hold Down Timer Ends

- 2010
- 2010+2017
- 2017
Non-IANA Key Tags

- How often do we see "unexpected" key tags?
- Observed 19 29 key tags for root other than 19036 and 20326.
- From less than 10 100 distinct source IPs per day.
Conclusions

• Signals from BIND (and Unbound?) appear to be of reasonably good quality.

• NATs, forwarding, dynamic IPs, and partial views complicate analysis.

• Something strange with new signalers on Oct 10.

• ISC, Thank you!
• NLnet Labs, thanks for changing trust-anchor-signaling to ‘yes’ by default.
• Other vendors, please consider implementing RFC 8145.