KSK Sentinel

draft-ietf-dnsop-kskroll-sentinel

Geoff Huston
Joao Silva Damas
Warren Kumari
### Major changes

<table>
<thead>
<tr>
<th>Status</th>
<th>Title</th>
<th>Details</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Clarifications regarding caching and SERVFAIL responses</strong></td>
<td>#14 by pspacek was merged 15 minutes ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Fix editorial nits</strong></td>
<td>#13 by pspacek was merged 2 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Clarify situation with multiple resolvers</strong></td>
<td>#12 by paulehoffman was merged 16 minutes ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Editorial changes to Section 3</strong></td>
<td>#11 by paulehoffman was merged 15 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Update Privacy Concerns, deprecate Key ID</strong></td>
<td>#10 by wessels was merged 19 days ago • Approved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Added Duane’s privacy concerns</strong></td>
<td>#8 by paulehoffman was merged 20 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Makes the use cases clearer</strong></td>
<td>#7 by paulehoffman was merged 20 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Fixed some A/AAAA stuff</strong></td>
<td>#6 by paulehoffman was merged 20 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Changed the example numbers</strong></td>
<td>#5 by paulehoffman was merged 20 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Made it clear that names and addresses must be real</strong></td>
<td>#4 by paulehoffman was merged 20 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Used key-tag and Key Tag consistently throughout</strong></td>
<td>#3 by paulehoffman was merged 20 days ago</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Lots of editorial fixes</strong></td>
<td>#2 by paulehoffman was merged 20 days ago • Approved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✅ 13 Closed</td>
<td><strong>Make the protocol apply to all zones, not just the root</strong></td>
<td>#1 by paulehoffman was closed 20 days ago</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Major changes

- Conversational description of how this works.
- This is for the **active** root TA.
- Many many readability fixes (thanks all!)
- Make examples FQDN.
- Some privacy clarifications.
- SERVFAIL vs NXDOMAIN...
Major changes

Names!

- _is-ta-<key-tag>
- kskroll-sentinel-is-ta-<hex key-tag>
- kskroll-sentinel-is-ta-<dec key-tag>
Demo

Demo: http://www.ksk-test.net:

Sentinel KSK Test

tl;dr: **You are using a legacy resolver, we cannot determine your fate**!

This page uses the methods described in [A Sentinel for Detecting Trusted Keys in DNSSEC](#) to determine if the resolvers that you are using will survive the upcoming KSK roll. You should really read the document, but the 50’000ft view is that it attempts to load resources from 3 names:

- "http://invalid.ksk-test.net/invalid.gif"
- "http://kskroll-sentinel-is-ta-20236.ksk-test.net/is-ta.gif"
- "http://kskroll-sentinel-not-ta-20236.ksk-test.net/not-ta.gif"

It then uses some simple logic to tell what your fate will be after the KSK roll:

1. If you are **not** using a validating resolver, you will be able to load the *invalid* record.
2. If you are using a validating resolver which *does not* understand this new mechanism you will be able to load both of the sentinel records: *kskroll-sentinel-is-ta-20236* and *kskroll-sentinel-not-ta-20236*.
3. If you are using a resolver that supports this mechanism you will only be able to load one of the two sentinel records - which one tells you how you will fare in the rollover.

When running the above test, you:

- were **NOT** able to fetch the "invalid" record
- were able to fetch the "kskroll-sentinel-is-ta-20236" record
- were able to fetch the "kskroll-sentinel-not-ta-20236" record
Questions?
Backup Slides
What's the problem?

- We need to roll the DNSSEC trust-anchor (KSK).
- Have no way to measure the impact.
RFC8145!

Internet Engineering Task Force (IETF)
Request for Comments: 8145
Category: Standards Track
ISSN: 2070-1721

PROPOSED STANDARD

D. Wessels
Verisign
W. Kumari
Google
P. Hoffman
ICANN
April 2017

Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)

Abstract

The DNS Security Extensions (DNSSEC) were developed to provide origin authentication and integrity protection for DNS data by using digital signatures. These digital signatures can be verified by building a chain of trust starting from a trust anchor and proceeding down to a
Pretty graphs!
Prettier graphs!

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

Graph showing trends over time from 01-Sep-17 to 01-Feb-18.
Sentinel
1. Requires a (simple) resolver update
2. Allows anyone to set up a measurement service
3. Exposes the result to the users

The change
Just before sending the response (after resolution, validation):

- kskroll-sentinel-is-ta-[key].something?
  - If have the key, reply normally, else SERVFAIL
- kskroll-sentinel-not-ta-[key].something?
  - If do NOT have the key, reply normally, else SERVFAIL
Example

- I'm a validating resolver. I support sentinel.
- I have the new KSK (20326)
- I get a query for invalid.example.com
  - It fails DNSSEC validation - SERVFAIL
- I get a query for
  kskroll-sentinel-is-ta-20326.example.com
- I resolve it and get 192.0.2.23
  - I have (and am using) KeyID 20326
    - answer with 192.0.2.23
- I get a query for
  kskroll-sentinel-not-ta-20326.example.com
  - I do have (and am using) KeyID 20326
    - send SERVFAIL
Yawn. So what?!

```
<html>
  <body>
    <h1>KSK Roll Test</h1>
    <p>
      Fish: <img src="invalid.example.com/fish.jpg">
      Kitten: <img src="kskroll-sentinel-is-ta-20326.example.com/kitten.jpg">
      Puppy: <img src="kskroll-sentinel-not-ta-20326.example.com/puppy.jpg">
    </p>
  </body>
</html>
```

Do you see:

- Fish? Not validating, key-roll doesn't affect you.
- Kitten and Puppy? Legacy, we cannot tell.
- Kitten? You have the new key, you'll be fine.
- Puppy? **DANGER!** You only have the old key.
Srsly? Kittens?! Sadly, no...
...but kittens!!!
Sorry, still no... :-(

Demo: http://www.ksk-test.net:

Sentinel KSK Test

tl;dr: You are using a legacy resolver, we cannot determine your fate!

This page uses the methods described in A Sentinel for Detecting Trusted Keys in DNSSEC to determine if the resolvers that you are using will survive the upcoming KSK roll. You should really read the document, but the 50'000ft view is that it attempts to load resources from 3 names:

- "http://invalid.ksk-test.net/invalid.gif"
- "http://kskroll-sentinel-is-ta-20236.ksk-test.net/is-ta.gif"
- "http://kskroll-sentinel-not-ta-20236.ksk-test.net/not-ta.gif"

It then uses some simple logic to tell what your fate will be after the KSK roll:

1. If you are not using a validating resolver, you will be able to load the invalid record.
2. If you are using a validating resolver which does not understand this new mechanism you will be able to load both of the sentinel records: kskroll-sentinel-is-ta-20236 and kskroll-sentinel-not-ta-20236.
3. If you are using a resolver that supports this mechanism you will only be able to load one of the two sentinel records - which one tells you how you will fare in the rollover.

When running the above test, you:

- were NOT able to fetch the "invalid" record
- were able to fetch the "kskroll-sentinel-is-ta-20236" record
- were able to fetch the "kskroll-sentinel-not-ta-20236" record
Questions?