

Root KSK Roll Delay Update

PacNOG 21

Patrick Jones, Sr. Director, Global Stakeholder Engagement

4 December 2017



Background

- ⦿ When you validate DNSSEC signed DNS records, you need a Trust Anchor.
 - A Trust Anchor is a Public Key.
- ⦿ Public Keys should not live forever.
- ⦿ These Trust Anchors probably should be periodically renewed (rolled).
 - You can do this automatically or manually.
- ⦿ However, there was no way for us (ICANN) to check if you have the right key configured.
- ⦿ Therefore, a multi-year design and outreach effort ensued:
 - Design-team, blogs, outreach, presentations in various venues, plans, vendors and governments were contacted, etc., etc.

The Process

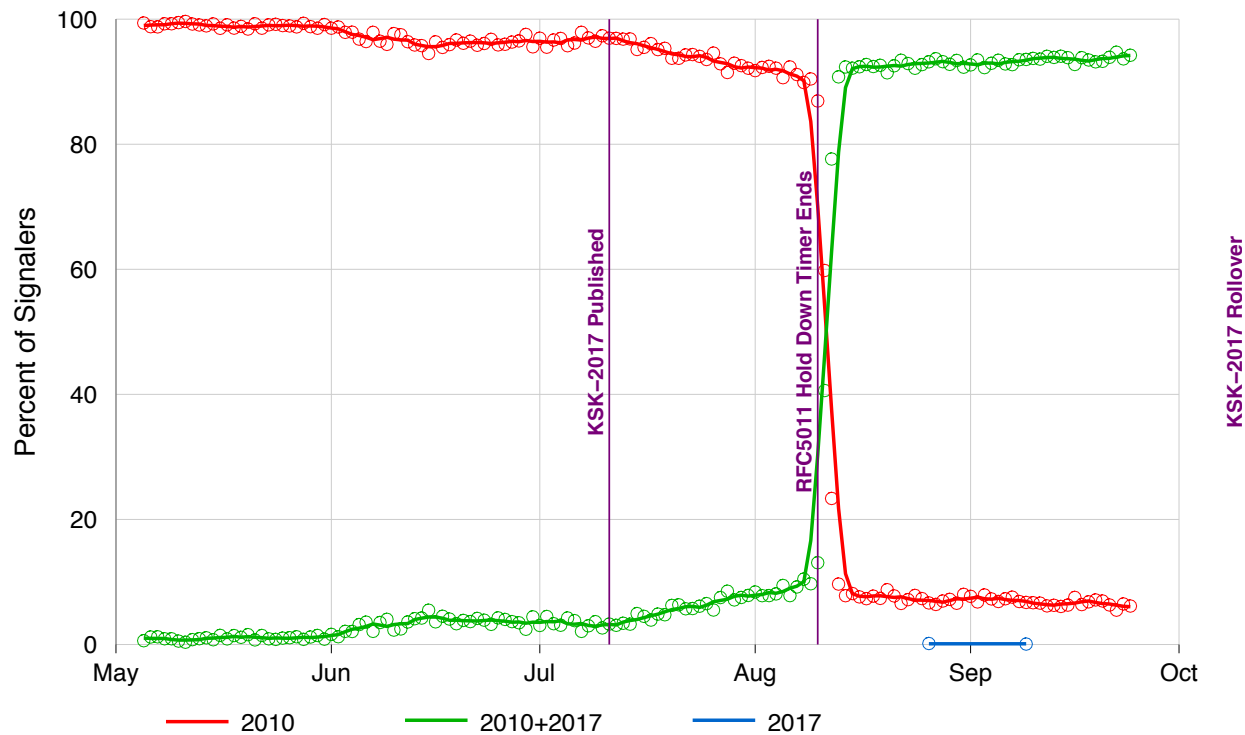
- ⦿ **11 July 2017:** Introduce the new KSK-2017.
 - Monitor if there are fundamental changes in root-server traffic
 - If not, continue, else fall back.

- ⦿ **10 August 2017:** “30 day hold-down period ends”
 - Monitor if there are fundamental changes in root-server traffic.
 - If not, continue, else fall back.

- ⦿ **19 September 2017:** DNSKEY Response size increased due to standard ZSK roll
 - Monitor if there are fundamental changes in root-server traffic.
 - If not, continue, else fall back.

The timeline in a graph

Root Zone Key Tag Signaling -- TA Update Evidence



Verisign Public

powered by VERISIGN

17

Who has KSK-2017 configured as a trust anchor?

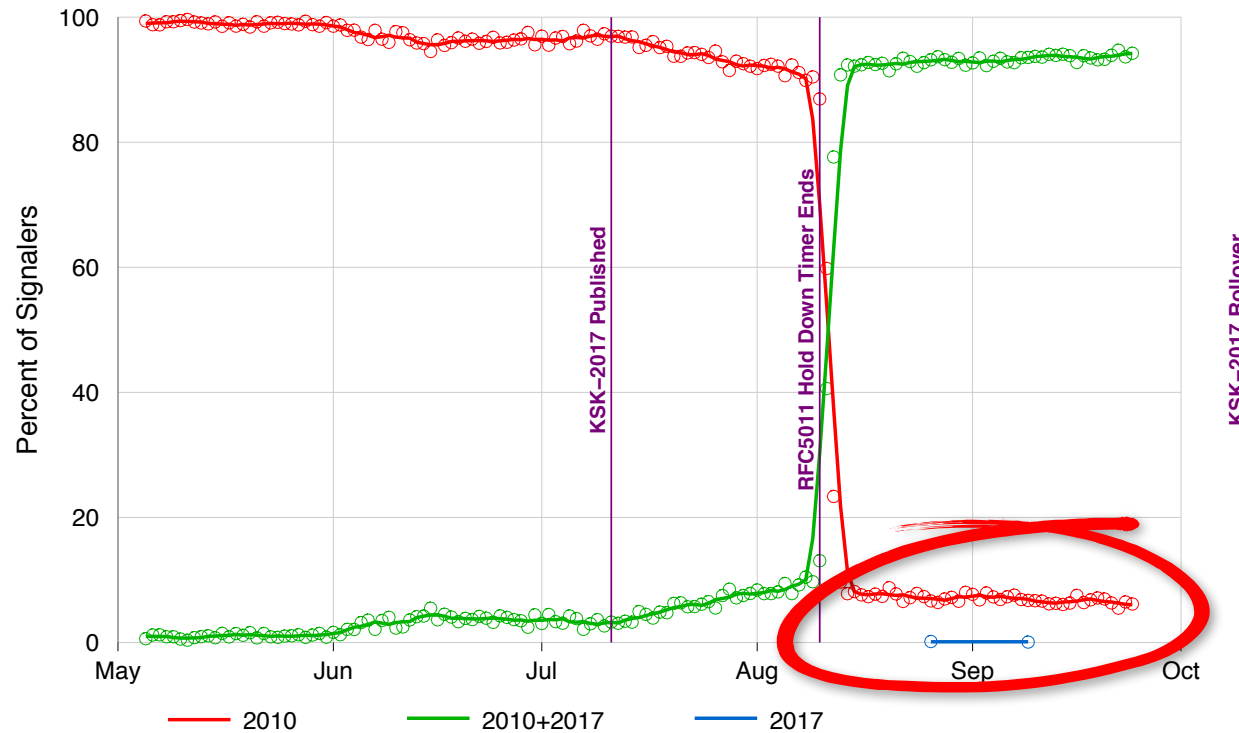
- ⦿ Until very recently, there was no way to know which trust anchors validators have configured
- ⦿ *Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)* is a recent protocol extension that can provide that information
 - Reports trust anchor key tags via EDNS option or DNS query
 - Published as RFC 8145 (April 2017)
- ⦿ Implementations
 - BIND 9.11 starting with 9.11.0b3 (28 July 2016)
 - BIND 9.10 starting with 9.10.5b1 (11 January 2017)
 - Unbound 1.6.4 (27 June 2017)
 - On by default in BIND (since 28 July 2016) and in Unbound since version 1.6.7 (10 October 2017)
 - No other known implementations

Looking for key tag signaling

- RFC 8145 is so new and validator support so limited that the root KSK roll project team did not expect to get enough data to help with the first root KSK Roll.
 - On average, there are 4.2 Million unique addresses sending queries to root-servers.
 - Given typical deployment curves, it was assumed the dataset would be too small to statistically represent all validating resolvers.
- However...
 - Before the introduction of KSK-2017, RFC8145-able resolvers would send KSK-2010 only.
 - After the hold down period of 30 days, RFC8145-able resolvers would send both KSK-2010 and KSK-2017.
 - Duane Wessels (Verisign, co-author of 8145) started looking at A & J root traffic for this signaling

Hey! There's data! Wait. What?

Root Zone Key Tag Signaling -- TA Update Evidence



Verisign Public

powered by VERISIGN

17

Further analysis by OCTO Research

- ICANN OCTO Research did an analysis similar to Duane's
 - Analyzed query data from B, D, F and L root servers
 - For the entire month of September and October (until the 24th)
- Results:
 - Total number of unique addresses reporting key tag data: **27,084** (out of 4.2 million, 0.57%)
 - Total number that only ever reports KSK-2010: **1631**
 - **6.02% of reporting validators were not ready for the KSK roll on 11 October 2017**
 - Non-zero percentage of reporting validators were announcing **only** KSK-2017 (?!)
- Analysis is complicated
 - Dynamic resolver IPs make the situation look worse by inflating true number of sources
 - Resolvers behind forwarders make the situation look better as they obscure multiple validators behind the forwarder

Why do validators report just KSK-2010?

- ⊙ Multiple reasons suspected or confirmed:
 1. BIND reports trust anchors even if not validating
 2. Old configurations pre-dating automatic update support
 - E.g., BIND's *trusted-keys* instead of *managed-keys* or *dnssec-validation auto*
 3. Bugs in automatic update or key tag signaling support
 - E.g., announce key tags even if DNSSEC not enabled (DO=0)
 4. Operator error
 - E.g., Docker container keeps booting up with only KSK-2010 and starts 5011 all over again
- ⊙ We always knew old configurations would be an issue but never had objective data until now
- ⊙ We worried bugs and operator error were possible but didn't have evidence until now
- ⊙ Analysis is ongoing
 - Hired a contractor to try to figure out reasons for misconfiguration

Back to the plan and process

- ⦿ 19 September 2017: DNSKEY Response size increased due to standard ZSK roll
 - Monitor if there are fundamental changes in root-server traffic.
 - If not, continue, else fall back.
- ⦿ We had received Verisign's report and corroborated it with our own data.
- ⦿ From the Operational Plan:
 - “The Root Zone Management Partners might also decide to extend any phase for additional quarters. For example, if new information indicates that the next phase may lead to complications, the current phase would be prolonged. This is referred to as an extend scenario.”*
- ⦿ 27 September 2017: “Extend” scenario kicks in
 - ICANN Announces that the root KSK Rollover is delayed

Issues

- ⦿ We do not know how representative the set of validators reporting key tag data is compared to the set of all validators
- ⦿ Validators != end users (or “end systems”), and the impact on end users is what is most important
 - The design team recognized this
- ⦿ Determining number of end users/systems for a given resolver is hard
 - APNIC’s Google Ad experiment platform-based data will help
- ⦿ Mitigation is hard
 - We’ve already had a multi-year campaign to reach operators
 - Implementation-specific problems don’t make the problem easier

Next Steps

- ⦿ We postponed the root KSK roll until we can gather more information and understand the situation better
 - The delay will be at least one quarter
 - We have not yet determined how many quarters to delay
- ⦿ We will at least partially mitigate
 - Contractor hired to try to track down the 500 resolvers based on IP addresses and understand why misconfiguration is occurring
 - Data collection continues
- ⦿ We'll need to re-engage/re-tune the communications plan
 - Maybe “PLEASE DO **NOT** REMOVE KSK-2017!!”?

SSAC Update & Advice on Emoji Domain Names

Security and Stability Advisory Committee (SSAC)

Who We Are



⦿ 37 Members



⦿ Appointed by the ICANN Board

What We Do



Charter: Advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

What is Our Expertise

- Addressing and Routing
- Domain Name System (DNS)
- DNS Security Extensions (DNSSEC)
- Domain Registry/Registrar Operations
- DNS Abuse & Cybercrime
- Internationalization (Domain Names and Data)
- Internet Service/Access Provider
- ICANN Policy and Operations

How We Advise

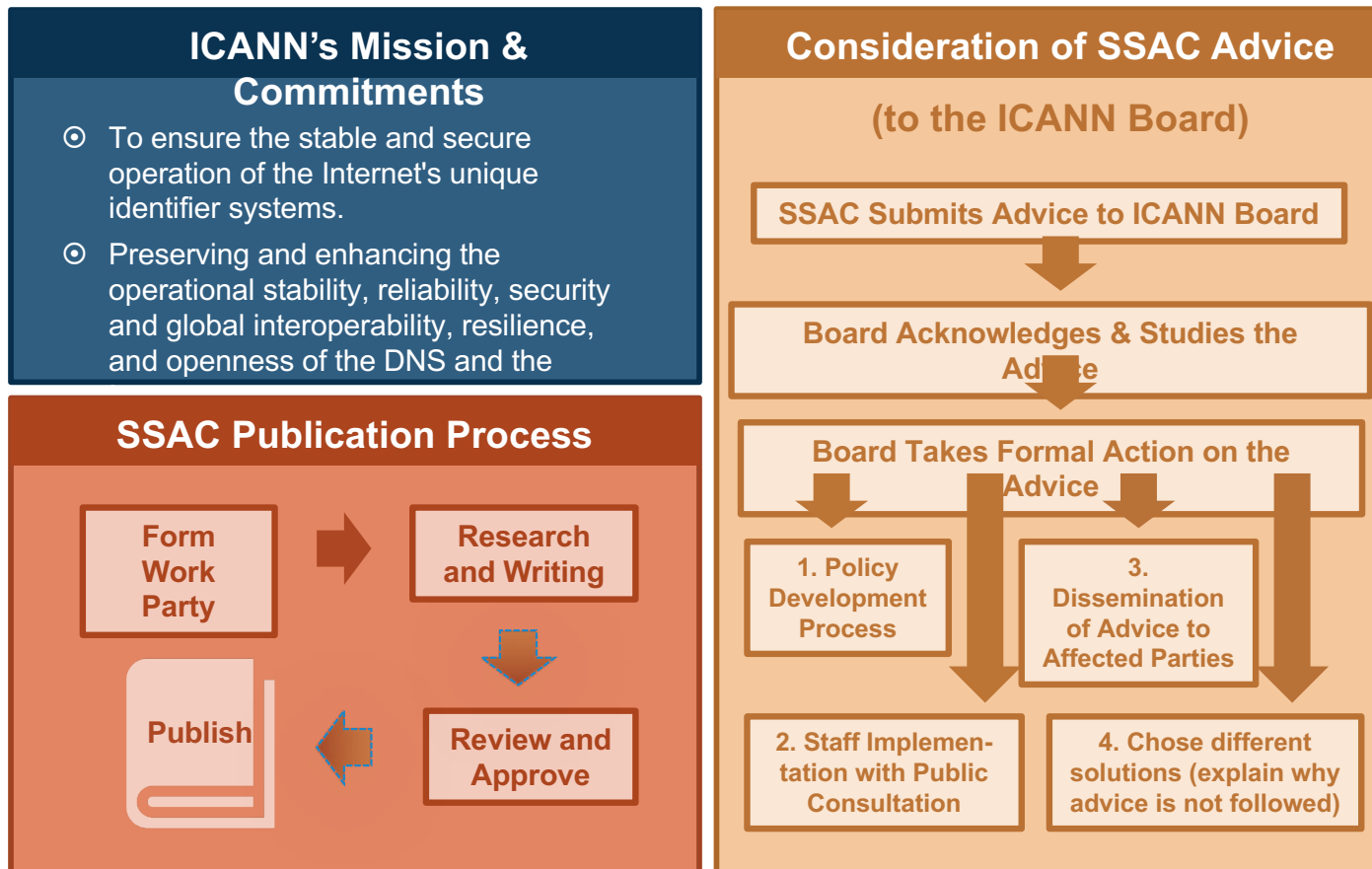


98
Publications
since 2002



⦿ REPORT ⦿ ADVISORIES ⦿ COMMENT

↓
OUTREACH

Security and Stability Advisory Committee (SSAC)



Security and Stability Advisory Committee (SSAC)

<h3>Current Work</h3> <h4>Parties</h4> <ul style="list-style-type: none">Management of the Namespace and Name CollisionsIDN HarmonizationSSAC Organizational ReviewWHOIS Rate LimitingInternet of ThingsDNSSEC Workshops (Ongoing)Membership Committee (Ongoing)	<h3>Recent Publications</h3> <p>[SAC098]: The Security, Stability, and Resiliency of the DNS Review (SSR2) (04 October 2017)</p> <p>[SAC097]: SSAC Advisory Regarding the Centralized Zone Data Service (CZDS) and Registry Operator Monthly Activity Reports (14 June 2017)</p> <p>[SAC096]: SSAC Comment on the CCWG-Accountability-WS2 Draft Framework of Interpretation for Human Rights (30 May 2017)</p> <p>[SAC095]: SSAC Advisory on the Use of Emoji in Domain Names (25 May 2017)</p>
 <p>Security and Stability Advisory Committee</p>	<h3>Outreach</h3> <ul style="list-style-type: none"> ssac.icann.org and SSAC Intro: www.icann.org/news/multimedia/621 www.facebook.com/pages/SSAC/432173130235645 SAC067 SSAC Advisory on Maintaining the Security and Stability of the IANA Functions Through the Stewardship Transition and SAC068 SSAC Report on the IANA Functions Contract: www.icann.org/news/multimedia/729

SAC 95 Advisory on Use of Emoji in Domains

- ◎ SSAC advice adopted by ICANN Board 2 Nov 2017
- ◎ SSAC strongly recommends that emoji not be included in TLD labels or at any level in a domain name
- ◎ Emoji are symbols in Unicode, which are disallowed in IDNA 2008

SAC 95 Advisory on Use of Emoji in Domains

- ⦿ Emoji are not designed to be visually uniform or visually distinguishable.



- ⦿ Confusability issue for users and poses problems with universal acceptance of domain names.
- ⦿ Users can have accessibility problems due to inconsistent rendering.

SAC 95 Advisory on Use of Emoji in Domains

- ⦿ ICANN Board is requesting the ccNSO and GNSO integrate conformance with IDNA 2008 into policies so as to safeguard security, stability, resiliency & interoperability of domain names.
- ⦿ Emoji domains are currently being offered by 1 ccTLD in this region - .ws

Topics of Interest/Possible New Work

- ⊙ Signing root NS Sets Analysis
- ⊙ Are We Ready for an IPv6-Only Internet?
- ⊙ Analysis of WannaCry/Conficker
- ⊙ Challenges of Hosting Large Domain Portfolios
- ⊙ Proposal for .internal
- ⊙ SSAC Publication Review
- ⊙ SSAC Skills Survey
- ⊙ "Emerging Security Issues" Sessions at ICANN meetings

Engage with ICANN – Thank You and Questions



One World, One Internet

Visit us at icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann