Comments on ICANN's "Plan to Restart the Root Key Signing Key (KSK) Rollover Process"

Burt Kaliski, Danny McPherson, Eric Osterweil, Matt Thomas, Brad Verd and Duane Wessels
VeriSign, Inc.
March 30, 2018

(These comments are provided in response to ICANN's call for public comments on the document "Plan to Restart the Root Key Signing Key (KSK) Rollover Process."[1])

For nearly a decade now, Internet users have had the ability to authenticate and validate the integrity of Domain Name System (DNS) records directly, thanks to the DNS Security Extensions (DNSSEC).

A public-key infrastructure (PKI) specially designed for DNS records, DNSSEC provides public/private digital signature key pairs at each level of the DNS hierarchy. These digital signatures provide a chain of trust from a DNS record back to a **root key signing key (Key Signing Key, KSK)**. The KSK is configured in a **trust anchor list** maintained by **validating resolvers**, which can thereby validate authenticity of the DNS record by verifying the chain of digital signatures.

Until recently, the root zone trust anchor list has contained just one root KSK, a 2048-bit RSA key referred to as **KSK-2010**.

Public/private key pairs in a PKI are changed periodically to mitigate the risk of future compromise, whether due to advances in cryptanalysis or failures in key management (algorithm changes may also sometimes be made to improve performance). Such proactive replacements occur at various places in the DNS hierarchy. One component that hasn't changed yet, however, is the root KSK.

In 2017, ICANN initiated such a transition, from KSK-2010 to another 2048-bit RSA key, **KSK-2017**. ICANN's plan[2] for the change consists of three main phases:

- **Publication**: KSK-2017, the new or "incoming" KSK, is added to the DNSKEY resource record set (RRset) for the root zone, where it is marked as a trust anchor. The RRset continues to be signed with KSK-2010, the old or "incumbent" KSK. A validating resolver that observes KSK-2017 in the RRset for a sufficient period (e.g. 30 days per the RFC 5011 "hold-down" period[3]) or obtains it by

[1] ICANN. *Plan to Restart the Root Key Signing Key (KSK) Rollover Process.* February 1, 2018. https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en
[2] ICANN. *2017 KSK Rollover Operational Implementation Plan.* July 22, 2016. https://www.icann.org/en/system/files/files/ksk-rollover-operational-implementation-plan-22jul16-en.pdf
[3] StJohns, M. *Automated Updates of DNS Security (DNSSEC) Trust Anchors.* IETF RFC 5011, September 2007. https://www.rfc-editor.org/rfc/rfc5011.txt

other means (e.g., from the DNS Root Zone Trust Anchors file published by IANA)[4] is expected to install the key as a new trust anchor.

- **Rollover:** The DNSKEY RRset — still including both KSK-2010 and KSK-2017 — is signed with KSK-2017. Validating resolvers that have installed KSK-2017 as a trust anchor can verify the signature and subsequently, successfully resolve DNSSEC-enabled names; those that haven't, cannot.
- **Revocation:** KSK-2010 is marked for removal. At this point, a validating resolver is expected to remove KSK-2010 from its trust anchor list. KSK-2010 does not appear thereafter in the RRset.

The publication phase of the plan began in July 2017, preceded by the addition of KSK-2017 to IANA's Root Zone Trust Anchors file in February 2017 (at which point some resolvers began adding the key to their configuration). The rollover phase was to begin in October 2017, but ICANN postponed it in September 2017[5,6] due to concerns that not enough validating resolvers had installed KSK-2017. Per the plan, revocation would occur three months after the start of the rollover phase.

How many resolvers don't yet have KSK-2017, and thus how many users might be impacted by the pending rollover, is still unknown. Statistics[7] published by ICANN based on one reporting mechanism, RFC 8145 trust anchor signaling,[8] indicate that as of the end of February 2018, more than 35% of the cumulative total of reporting resolvers did not have the KSK-2017 trust anchor. The fraction appeared to be increasing as more resolvers reported their status.

The extent to which these numbers are a cause for concern is unknown. It may well be that the validating resolvers that have so far been upgraded to support RFC 8145 (a relatively recent specification) are not as effective in managing their trust anchor lists for some reason, and that a higher fraction of non-reporting resolvers do indeed have KSK-2017. Moreover, if a validating resolver has a dynamic IP address, then it may be counted multiple times in the total, even though it is not generating much traffic from any one address. But the fact that there's no clear explanation, as ICANN acknowledged in December 2017 update,[9] suggests, first, that the reported shortcomings should be considered a potential *lower bound* of potential breakage, and, second, that publication of KSK-2017 cannot be considered complete.

Verisign has performed some additional analysis from its perspective as root server and registry operator, and in support of its role, as ICANN's partner under the Root Zone Maintainer Service Agreement (RZMA),[10] in responsibly effectuating changes to the root zone. This analysis provides

---

[4] https://data.iana.org/root-anchors/

[5] Larson, M., and Hoffman, P. *Postponing the Root KSK Roll.* ICANN, October 17, 2017. https://www.icann.org/en/system/files/files/root-ksk-roll-postponed-17oct17-en.pdf

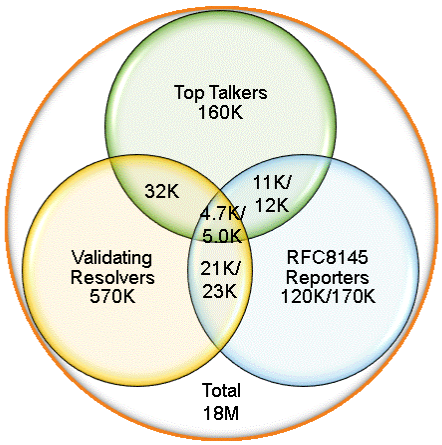
[6] Wessels, D. *A Closer Look at Postponing of the Root Zone KSK Rollover Decision.* CircleID, September 29, 2017. http://www.circleid.com/posts/20170929_a_closer_look_at_postponing_of_root_zone_ksk_rollover_decision/

[7] Larson, M. *Update on root KSK rollover (or, We're really doing it this time).* OARC 28, March 8-9, 2018. https://indico.dns-oarc.net/event/28/session/11/contribution/52

[8] Wessels, D., Kumari, W., and Hoffman, P. *Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC).* IETF RFC 8145, April 2017. https://www.rfc-editor.org/rfc/rfc8145.txt

[9] Larson, M. *Update on the Root KSK Rollover Project.* ICANN blog, December 18, 2017. https://www.icann.org/news/blog/update-on-the-root-ksk-rollover-project

[10] ICANN. *Root Zone Maintainer Agreement.* September 28, 2016. https://www.icann.org/en/stewardship-implementation/root-zone-maintainer-agreement-rzma



- **Top Talker** = Source appearing on at least two days AND ranked in top 1% of all sources based on number of DNS requests
- **Validating Resolver** = Source requesting at least one DNSKEY and one DS record
- **RFC8145 Reporter** = Source sending at least one RFC8145 trust anchor signal
  Notation: Sources consistently reporting KSK2017 / Total sources reporting
- **Observation Period** = March 1-15, 2018
- **Observation Space** = A and J Root Server Traffic
- All figures to two significant digits

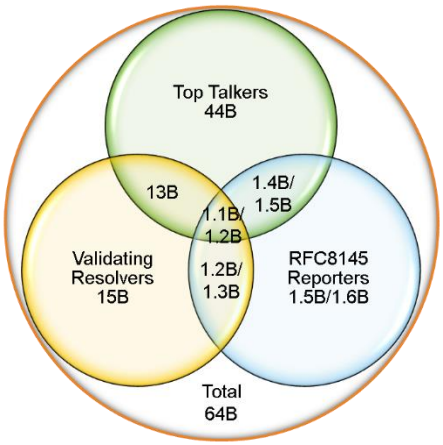
Figure 1: Observations on data related to validating resolver reporting of the new KSK, indicating number of DNS sources of each type.

further segmentation among the RFC 8145 reporters to focus on "top talkers" (high-traffic sources) and validating resolvers. Verisign's observations are inconclusive about the rollout of KSK-2017 in the full population of validating resolvers. Similar to ICANN's data, Verisign's analysis of DNS requests to the A and J root servers between March 1 and 15, 2018 indicates that a large fraction of RFC 8145 sources is not reporting knowledge of KSK-2017. This holds both across the cumulative total number of RFC 8145 sources, and the sources that are among the top talkers, the ones that generate the most traffic. Furthermore, a **large fraction of validating resolvers** (identified based on requesting at least one DNSKEY and one DS record during the period) **are not even reporting RFC 8145 data at all**. For example, as shown in Figure 1, only about 23,000 of 570,000 validating resolvers reported RFC 8145 data during the observation period — and only 21,000 of these consistently reported KSK-2017. In terms of query volume, as shown in Figure 2, RFC 8145 reporters represented about 1.3 billion DNS requests out of the 15 billion requests from validating resolvers. Taken together, the sources that are reporting RFC 8145 represent less than 3 percent of all DNS requests observed.

Adding to the uncertainty about how many validating resolvers have KSK-2017, is the clarity about what will happen to a validating resolver and to the users that rely only on that validating resolver if it doesn't have KSK-2017 when the rollover occurs.

Prior to the rollover, a validating resolver would verify the signature on the root DNSKEY RRset with KSK-2010, a KSK presumably long established in its trust anchor list. Following the rollover, when the resolver next obtains a fresh version of the DNSKEY RRset from the root server, the resolver would need to verify the signature with KSK-2017, but it won't have the key in its trust anchor list. This means that **DNSSEC validation** (i.e. name resolution for DNSSEC-enabled domains) **at a non-updated resolver will begin to fail**[11] as soon as the last RRset signed with KSK-2010 in its cache expires. This could be **as early as a moment after the rollover, and in any case no later than 48 hours afterwards** based on the time-to-live (TTL) for the signature record.

[11] DNSSEC is designed to "fail hard"; anything else would lead to "downgrade attacks."



- **Top Talker** = Source appearing on at least two days AND ranked in top 1% of all sources based on number of DNS requests
- **Validating Resolver** = Source requesting at least one DNSKEY and one DS record
- **RFC8145 Reporter** = Source sending at least one RFC8145 trust anchor signal
  Notation: Requests from sources consistently reporting KSK2017 / Total requests from sources reporting
- **Observation Period** = March 1-15, 2018
- **Observation Space** = A and J Root Server Traffic
- All figures to two significant digits

Figure 2: Observations on data related to validating resolver reporting of the new KSK, indicating number of DNS requests from each type of source.

In terms of the timetable, if ICANN rolls over from KSK-2010 to KSK-2017 on October 11, 2018, a Thursday, then at various points that day, as well as on the Friday and Saturday, **validating resolvers that have not installed KSK-2017 will no longer be able to authenticate or even resolve DNS responses**. Any clients of these validating resolvers that require DNSSEC validation prior to connecting to a web site will no longer be able to connect. Their **users will find such web sites suddenly "unavailable."**

The reason for the unavailability is not that the rollover failed in and of itself but that the **root KSK publication failed**: the resolver the user is relying on did not install the new KSK.

We therefore encourage ICANN and the community more broadly to **reframe root KSK publication as a standalone activity with its own success criteria**, rather than as just a step in the rollover plan. Before proceeding with the root KSK rollover, ICANN should publish measurable goals for the KSK rollout, including monthly or more frequent metrics for:

- how many operators have been notified of the new KSK (and what level of notification is "good enough");
- how many have acknowledged awareness of the new KSK;
- how many have installed the new KSK;
- how much root server traffic these operators represent;
- how many Internet users they serve;
- how many Internet properties risk becoming unreachable if KSK rollover were to occur the time the metrics are reported.

The rollover should not start until the rollout consistently meets these documented goals.

Separating rollout and rollover is important because it recognizes explicitly that **rollout is a community activity,** not a step that can be taken by one party.[12] While the technical mechanisms involved in both are similar from an operational perspective — just a change in RRset content and/or signing keys — the implications are quite different from an ecosystem perspective. Rollout requires a change in trust anchor sets among millions of validating resolvers. Rollover, once that change is in place, is just another routine signed RRset.[13]

One of the arguments made against delaying rollover until published rollout goals are met is that such criteria can be difficult to measure. Another is that the possibility of a delay rather than a deadline can reduce a community's incentive to take action. Both are valid points. But neither minimizes the importance of the party making a change engaging continuously with the parties that may be affected by the change — especially when that change can impact user experience.

ICANN CTO office's February 2018 plan[14] recognizes the importance of such outreach but lacks specific measurement goals. For example, regarding the October 11 date, the plan states that the date "gives ICANN org plenty of time to publicize the new date and attempt to get more validating resolvers ready for the roll over." ICANN should be specific about its publication goals for each month, the number of resolvers it will attempt to contact, and the number that should be ready as a result of its outreach.

The plan also states, "ICANN org will increase its efforts to reach the operators of validating recursive resolvers." These efforts should be planned to meet measurable geographic and user population criteria. "Attempts to minimize," "additional mitigating steps," and "new reasons" should also be tracked and reported by ICANN on a real-time basis – as they may well be more informative than the RFC 8145 trust anchor data.[15]

In approving a plan with such benchmarks, **the ICANN Board should also make it clear that if any of the benchmarks is missed, then the October date will be reconsidered**. In other words, the date should be considered provisional; "conditions on the ground" should drive the actual rollover, not the date.

---

[12] Separating the activities also has the advantage that in the future, ICANN could invoke a rollout independently of a rollover. For instance, ICANN could periodically roll out new backup keys, perhaps with a larger key size or a different algorithm, and then decide later which ones to roll to. Rollover would then be an ongoing background activity that manages the trust anchor lists, while rollover would be a foreground activity that transitions to a new trust anchor that's already been installed. This approach may need further improvements in trust anchor management, but underscores a further benefit of considering rollout separately from rollover.

[13] To be fair, the step following rollover – revocation – is also a change of state. For completeness, the process of changing from one root KSK to another involves rollout of a trust anchor list with the new key, rollover from the old key to the new, and rollout of a trust anchor list *without* the new key. Unlike the first activity, a failure in the third activity doesn't introduce operational risk, but neither does it mitigate the security risk of the compromise of the old key.

[14] ICANN. *Plan to Restart the Root Key Signing Key (KSK) Rollover Process.* Op. cit.

[15] More informative and influential still will be the ability for users and resolver operators to know if they're up to date, and to update themselves. Users should be able to detect if the resolver they're using is up to date and if not to have an easy way to switch to another one that is up to date. ICANN should apply what it learns from this experience and work with DNS standards and software developers to adopt new practices that help users and DNS operators do better next time. The recently proposed "sentinel" technique is a positive step in this direction (Huston, G., Damas, J., and Kumari, W., *A Sentinel for Detecting Trusted Keys in DNSSEC*. Internet-Draft, March 20, 2018. https://datatracker.ietf.org/doc/draft-ietf-dnsop-kskroll-sentinel/).

ICANN's outreach to validate the rollout of KSK-2017 will also help provide contacts for future rollouts and rollovers, so has benefits beyond just the present activities. It will give the community a framework for other updates that may occur in the future – whether rollouts of keys with new algorithms in response to long-term trends, emergency rollovers in response to short-term crises, or, more generally, mitigations to previously discussed risks such as name collisions. Recognizing that such outreach might involve unbudgeted resources, the community (including Verisign) can and should be engaged to help mitigate that impact if needed. Furthermore, a number of entities are experienced with similar outreach initiatives in the community already with well-exercised outreach capabilities.[16]

Thankfully, there's no urgency to change the root KSK. ICANN made the prudent choice of a 2048-bit RSA public key for the original trust anchor, consistent with NIST's recommendations for long-term security.[17] The management of the root KSK itself is performed in accordance with the carefully specified DNSSEC practice statement.[18] Advances in cryptanalysis and failures in key management are thus not immediate threats. The root KSK should still be changed proactively, but this should be done in a way that ensures that it really is changed — by both the publisher and the consumer — or otherwise the changes may introduce an operational threat to DNSSEC. All this means there's still time to get the rollout and rollover correct.

Changing the root KSK should not be taken as a goal in and of itself, but instead, rather, as another means of providing users the ability to authenticate and validate the integrity of DNS data — which in turn provides the Internet community a way to improve assurances for other kinds of data as well.[19] ICANN has provided a valuable service to the community in delaying the rollover phase when the success of the rollout of KSK-2017 became unclear. We would like to thank ICANN for coordinating this process and calling for comments from the community, and look forward to supporting ICANN in a prudent KSK rollout and rollover.

---

[16] Shadowserver Foundation, https://www.shadowserver.org/ is an example of such an organization.

[17] Based on generally accepted estimates for RSA key strength, 1024-bit RSA is roughly equivalent to an 80-bit symmetric key, and 2048-bit RSA to a 112-bit symmetric key (see, e.g., J.W. Bos et al., *On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography*, IACR ePrint 2009-389, https://eprint.iacr.org/2009/389.pdf). *NIST SP 800-57 Part 1 Recommendation for Key Management General* (Barker, E., NIST, January 2016, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf) disallows 80-bit security other than for "legacy processing," and allows 112-bit security through the year 2030. Moreover, the publicly reported record for RSA factorization is 768 bits, achieved in 2009 by T. Kleinjung *et al.* (*Factorization of a 768-bit RSA modulus*, IACR ePrint 2010-006, February 18, 2010, https://eprint.iacr.org/2010/006.pdf). The authors state: "Factoring a 1024-bit RSA modulus would be about a thousand times harder." Of course, this assumes only present methods, and neither cryptanalytic advances nor breakthroughs such as quantum computing, both of which are concerns for the long term. A prudent designer needs to accommodate the possibility of such threats, hence the need to transition periodically to larger key sizes and new algorithms.

[18] RZ KSK PMA. *DNSSEC Practice Statement.* October 1, 2016. https://www.iana.org/dnssec/icann-dps.txt

[19] The difficulty of rolling out a new KSK can be considered a testament to the strength of DNSSEC. Were it easier to add a root KSK to the list of trust anchors, operators might already be doing so inadvertently, much like the situation with web PKI and its ever-expanding trust list. The integrity of DNSSEC's trust anchor management further underscores the benefit of having a well-managed DNSSEC-based PKI as a complement to web PKI.

