Proposal for Future Root Zone KSK Rollovers

This proposal describes the considerations and an anticipated framework under which future changes to the Root Zone Key Signing Key (KSK) are made. The Root Zone KSK serves as the trust anchor for DNSSEC and is managed as part of the IANA functions, performed by ICANN through its affiliate Public Technical Identifiers (PTI). We seek feedback from the community to refine and finalize our approach prior to implementation through operational and procedural updates.

This proposal has been created based upon initial outreach and engagement with those involved directly in the first KSK rollover in 2018, including comments received through the ICANN KSK Rollover discussion list[1].

1. Executive Summary

We seek to create a predictable approach to managing the Root Zone KSK's lifecycle by establishing a standard KSK rollover interval. Predictable rollovers will help the overall implementation of DNSSEC in a number of ways:

- Exercising the associated procedures routinely will better ensure the various actors involved are suitably prepared for key rollovers, particularly in the event of the need to make an unscheduled (emergency) change to the KSK; and

- Being well practiced in rolling the key will make additional potential changes less challenging — such as changing cryptographic signing algorithms.

Specifically, a three-year rollover interval strikes a responsible balance between ensuring that procedures and software remain sufficiently agile to adopt new keys as they are commissioned, while not introducing too much operational complexity through overly-frequent changes to the KSK. A three-year rollover interval will also assist in developing institutional memory of all participants in the process.

We also propose that each new KSK be generated well before it signs the zone. This will allow a longer period of pre-publication, and consequently allow for the new KSK's earlier use if there is a need to perform an emergency rollover. As a result, the overall lifespan of future KSKs is anticipated to be about six years — two years of which will be in a standby state (published, but not yet actively used),

[1] https://mm.icann.org/listinfo/ksk-rollover

three years in an active state, and the final year being revoked and then deleted from the key management facilities.

When DNSSEC was first introduced into the DNS root zone in 2010, it was decided that the KSK should be rolled over as required, or after five years of operation. This is documented in section 6.5 of the DNSSEC Practice Statement for the Root Zone KSK Operator[2]. One of the anticipated benefits was to ensure resolver software was able to adopt new trust anchors predictably. Proving the capability to use new trust anchors in resolver software is considered particularly crucial if an emergency necessitates an unscheduled KSK rollover.

The first KSK rollover was performed through a multi-year process, based on an approach created by a multi-disciplinary community design team[3]. This culminated in the new KSK being used to sign the root zone starting on 11 October 2018. In general, this first rollover was seen as a success, with a minimal amount of disruption visible to Internet users. This was due in part to ICANN providing significant resources to perform outreach to the community beforehand to ensure global preparedness.

2. Root Zone KSK Lifecycle

The KSK lifecycle defines three key statuses of the KSK:

- Creation
- Signing
- Destruction

A KSK rollover refers to the process of switching the active KSK from one key to another, and includes pre-publication of the new key in a manner that allows it to be trusted, processing updates to the root zone trust anchor, introducing a new KSK in the root zone, and retiring the previous KSK.

Our current approach, which we propose be retained, defines eight distinct phases (A-H), with each phase aligned with a calendar quarter and an associated KSK ceremony being conducted in that time period. While it would be possible to compress the timing of some phases, in retaining the current approach we avoid additional complexity of the KSK ceremonies that take place in the Key Management Facilities (KMFs).

If a phase is extended, or if there is a situation which requires the process to be reverted to the previous phase, all actions associated with the next phase are postponed by at least one calendar

[2] https://www.iana.org/dnssec/dps/ksk-operator/ksk-dps.txt
[3] https://www.icann.org/news/announcement-2-2015-02-04-en

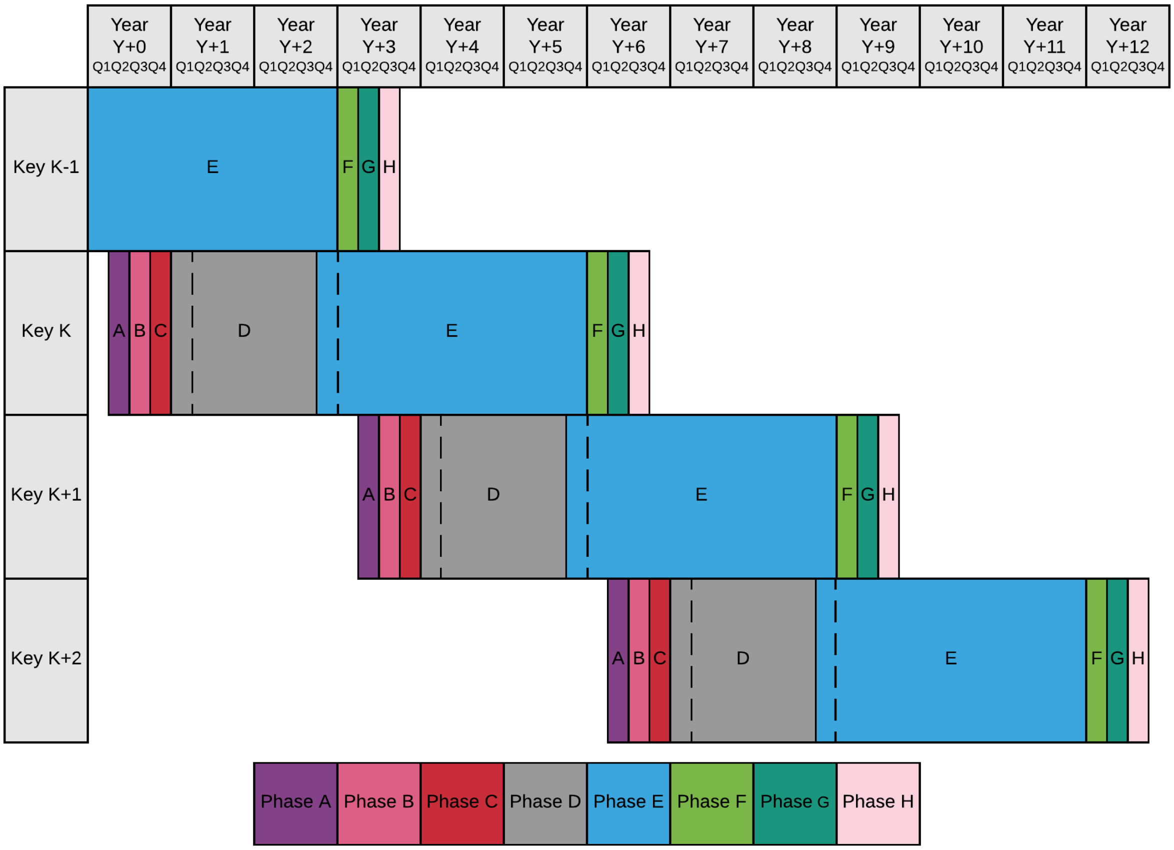
quarter or until the RZM Partners[4] decide to transition to the next phase. Details of the steps needed to perform the rollover are described in the *2017 KSK Rollover Operational Implementation Plan*[5]. The phases from the 2017 plan remain the same, but the duration of the keys' usage is lengthened.

[4] ICANN, PTI and Verisign. Verisign manages the Root Zone Zone Signing Key (ZSK) for ICANN under the Root Zone Maintainer contract.

[5] https://www.icann.org/en/system/files/files/ksk-rollover-operational-implementation-plan-22jul16-en.pdf

2.1. Phases and Rollover Cycle

Phase	Description
A: Generation	The new KSK is generated, and instantiated in the first KMF
B: Replication	The new KSK is replicated to the second KMF
C: First Keyset Signing	The first keysets containing the new KSK public key are signed to prepare for publication
D: Publication and Standby	The new KSK is published in the Root Zone as part of the DNSKEY RRset that is signed by the current KSK, to trigger RFC 5011 adoption. It remains in standby state until the rollover.
E: Rollover and Active	The new KSK is used for signing the root DNSKEY RRset.
F: Revocation	The previous KSK continues to be published in the root zone, but the revoked bit is set during this phase, and the revoked key is later removed during the phase
G: First Deletion	The previous KSK is deleted from the first KMF
H: Final Deletion	The previous KSK is deleted from the second KMF. No more copies exist.



In summary, early in the lifespan of the active KSK, its successor KSK is generated and published. This provides more than two years for adoption of the successor key as a trust anchor for the root zone before it is placed into production usage. Each KSK has an anticipated period of active usage of three years before the next rollover.

2.2. Timeline considerations

The current DNSSEC trust anchors for the root zone are published in a way that accommodates the retirement of an active KSK and the promotion of a newly-published KSK to active. Retired trust anchors will continue to be published after they are no longer active, but will be specified as having a validity period that is only in the past.

There are two principal methods in which the trust anchor is communicated — through publishing a trust anchor file[6], and using the RFC 5011 mechanism by signaling keys in the root zone data.

Changes to the trust anchor file occur:

[6] https://www.iana.org/dnssec/files

- during phase B, adding the new KSK
- during phase F, using a new validUntil field of the retired KSK that indicates that the key's validity has expired.

Changes to the root zone that trigger RFC 5011 adoption and revocation occur:

- during phase D, the new KSK is published in the root zone signed by the active KSK
- during phase F, the old KSK is published with the revoke bit set, indicating that it has been revoked, and the key is later removed from the root zone

One consequence of this timeline is the generation (phase A) and replication (phase B) of a new KSK is concurrent with the deletion of the former KSK in both KMFs (phases G and H).

2.3. Timing within a quarter

Historically, the changes described have been implemented in the root zone on the 11th day of the first month of a quarter (i.e. 11 January, 11 April, 11 July, and 11 October). We propose this be retained in accordance with the current language of the DNSSEC Practice Statement.

This timing is a consequence of aligning signatures that are signed at key ceremonies into 10-day slots. The first and last slot of a quarter are reserved for ZSK rollovers, leaving the second slot as the first opportunity in a quarter to perform KSK-related changes.

2.4. Rationale for rollover frequency

The proposed period of three years is frequent enough that the RZM Partners and DNS operators will be well-practiced in the KSK rollover process. Should a situation arise where an emergency rollover needs to take place, the rollover procedure is routine enough that we can anticipate minimal negative impact due to most validators already having the standby key.

The three year period is infrequent enough to reduce the operational complexity of managing multiple keys, yet allows for a lengthy pre-publication of a standby KSK allowing software and devices time to adopt and trust the standby KSK before the rollover to an active state.

The selection of a three year period also takes into account the KSK ceremonies and associated KMF activities. The length and complexity of the quarterly KSK ceremonies are impacted by factors such as the lifecycle of hardware security modules (HSMs), rotation of trusted community representatives (TCRs), lifecycle of TCR credentials, and maintenance and lifecycle of related IT and security hardware. Maintenance of these systems occur during ceremonies in addition to the basic activity of signing the ZSKs. Rollovers that are scheduled too often will result in a compressed timeline for the rollover process, or create additional overlap in the KSK lifecycle which would add undesirable complexity and length to the KSK ceremonies.

A regular KSK rollover will follow the process described in Figure 2, for twelve quarters or about a three year cycle, with the future KSK being a standby key for about two years before it becomes the KSK.

Note that the timelines given here are aspirational and not guaranteed. If an event occurs that warrants detailed study before proceeding, the rollover process can pause with the active KSK continuing to be used, even if doing so exceeds the nominal three-year period.

2.5. Rationale for having a standby key

This proposed lifecycle is different than the one that was used for the first KSK rollover in that it generates the next KSK earlier in the process, allowing for an extended period of publication to allow additional time for the adoption of the key as a trust anchor.

This provides two primary benefits:

- Longer lead times assist with the wide distribution and adoption of the next trust anchor. One of the main mechanisms of trust adoption is through the dissemination of the trust anchor data in operating system and DNS software updates, which can sometimes have a long lead time.

- Earlier trust in the generated key allows it to be more successfully used for an emergency KSK rollover. If the active KSK is compromised and the standby key remains secure, signing can be quickly switched to the new KSK and everyone who already trusts this standby key should be able to immediately validate with the new signatures. If a standby key is not yet trusted, an emergency KSK rollover has a greater potential for negative impact.

A potential risk of this approach is it disseminates the public key for a longer time window, thus providing additional opportunity for factoring or other attacks to derive the private key. However, 2048-bit RSA keys are widely assumed to be safe to use for the entire lifespan predicted in this proposal; for example, the 2048-bit RSA keys used in the web PKI are often used for a much longer period.

An emergency KSK rollover requires an unscheduled key ceremony to be conducted in response to an unanticipated security event, and thus needs to occur quickly. Accomplishing this while maintaining the chain of trust would be the most ideal scenario. The upcoming KSK could be used in a rollover while maintaining compliance with RFC 5011 as quickly as 33 days after the completion of phase D.

This has the potential to drastically reduce the waiting time required for an emergency rollover, which would be enacted in the event that the upcoming KSK had not yet reached that phase of its lifecycle.

While it’s possible to further overlap the lifecycle of the keys so that an RFC 5011 rollover could be accomplished at any time, it would require periods of time where 3 keys would be published in the root zone. This would have unknown and possibly detrimental effects in regard to the DNSKEY record size that outweigh the perceived benefits, as well as requiring changes to the DNSKEY key set more often that the proposed schedule described here.

2.6. Changes to key algorithm and strength

We do not propose changes in algorithm and/or key length at this time.

The current cryptographic algorithm employed for the KSK — 2048-bit RSA — has not been found to have any known exploitable vulnerabilities. Discussion of this topic is available in the previously published Root Zone KSK Rollover Plan[7] developed by a community design team.

A key rollover with an algorithm change has its own special considerations and would likely need specific study, review, and testing. While software under development for Root Zone KSK management has the capability to use the Elliptic Curve Digital Signature Algorithm (ECDSA), a comprehensive approach needs to consider the readiness and effects on all the other components in the ecosystem, including global resolver behavior.

2.7. Rollover Communications

Consistent communication with the community, including software vendors and resolver operators, about the new plan will be needed. This communication would include status updates and planned timing of future events so that appropriate monitoring can be performed.

We propose the continued use of the communications mechanisms previously used, including the root-dnssec-announce mailing list[8] and targeted announcements on the ICANN and IANA websites. When a predictable timeline is settled, it is anticipated the key dates can be shared earlier in advance with a greater level of confidence.

[7] https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf

[8] https://mm.icann.org/listinfo/root-dnssec-announce

3. Additional Considerations

The following is intended to provide background and context on the issues of scheduling and implementing a future KSK lifecycle. More extensive documentation on the processes and systems involved in the use of DNSSEC in the root zone have been published[9] and may provide further useful insight.

3.1. DNSSEC Deployment in the Root Zone

DNSSEC was first deployed in the root zone in 2010. ICANN and Verisign each published details of how their respective duties are performed in the documents *DNSSEC Practice Statement for the Root Zone KSK Operator* and *DNSSEC Practice Statement for the Root Zone ZSK Operator*, respectively[10].

The Root Zone KSK Operator stores the key material in HSMs that are kept in two different, highly secure KMFs.

The Root Zone Partners confer and take part in four ceremonies per year conducted at the KMFs in order to sign a set of operational Zone Signing Keys (ZSKs) that will be used to sign the root zone for the upcoming quarter. These ceremonies are scripted and performed using trusted roles from individuals within the ICANN Org and Trusted Community Representatives. The ceremonies are designed to be highly transparent and are audited by a third party.

3.2. Successful Completion of the First KSK Rollover

The *Review of the 2018 DNSSEC KSK Rollover*[11] describes the entire process of changing the KSK. The first change to the KSK became effective on 11 October 2018. This occurred after a thorough process of community consultations and technical steps needed to minimize unwanted side effects of the change.

Two companion conclusions are that it is impossible to predict how resolvers will react to KSK changes, and that an unduly long rollover process can have negative consequences for the community.

[9] https://www.icann.org/resources/pages/ksk-rollover
[10] https://www.iana.org/dnssec/dps
[11] https://www.icann.org/en/system/files/files/review-2018-dnssec-ksk-rollover-04mar19-en.pdf

4. Expected Changes to Processes

4.1. Scheduled Ceremonies

This approach to rollovers has no anticipated impact on the current schedule of key ceremonies conducted by ICANN. Currently, KSK ceremonies involving staff, contractors and community volunteers are scheduled four times per year.

4.2. Hardware Security Modules (HSMs)

The KSK Rollover has no anticipated impact on the HSMs effective operational lifetime. Currently, the HSMs are replaced approximately every five years, and the commissioning and decommissioning of HSMs are part of the normal ceremony routine. The entire set of keys is exported between devices when hardware renewal occurs and does not need to align with the logical key lifetimes.

4.3. KSK Management Software

The software used during KSK Ceremonies is capable of generating a new KSK and of managing a KSK rollover. The capabilities of the software were tested in the past KSK rollover. New software is currently in development and functionality will be thoroughly tested in relation to the capability of conducting a successful KSK rollover.

4.4. Key Management Facilities

This proposal uses the existing two key management facilities and does not propose any changes to their configuration.

5. Review of initial feedback

In early 2019, ICANN invited observers of the first KSK rollover to provide commentary for consideration in drafting this plan. These are comments on the key themes expressed in that initial feedback.

- The majority of commenters suggested that the KSK rollover should be a routine event
  - We propose a standard schedule for rollovers moving forward
- The majority of commenters suggested that the frequency of the KSK rollover should be yearly
  - We believe annual rollovers would incur too much complexity for key ceremony operations, and recommend a reduced schedule.
  - See section 2.4
- Commenters suggested the introduction of backup keys or standby keys
  - We propose an extended pre-publication period for future KSKs.
  - See section 2.5
- Commenters suggested that more investigation is needed for an unexpected increase to DNSKEY query results that may have a negative impact
  - ICANN will continue to monitor relevant DNS data as described in the *2017 KSK Rollover Monitoring Plan*[12]
- Commenters suggested that alternative signing algorithms should be investigated
  - While we do not propose a timeline for such investigations, we do envisage this as a parallel research activity. See section 2.6

[12] See https://www.icann.org/en/system/files/files/ksk-rollover-monitoring-plan-15sep16-en.pdf