2017 KSK Rollover Operational Implementation Plan

Version: 2016-07-22

Contents

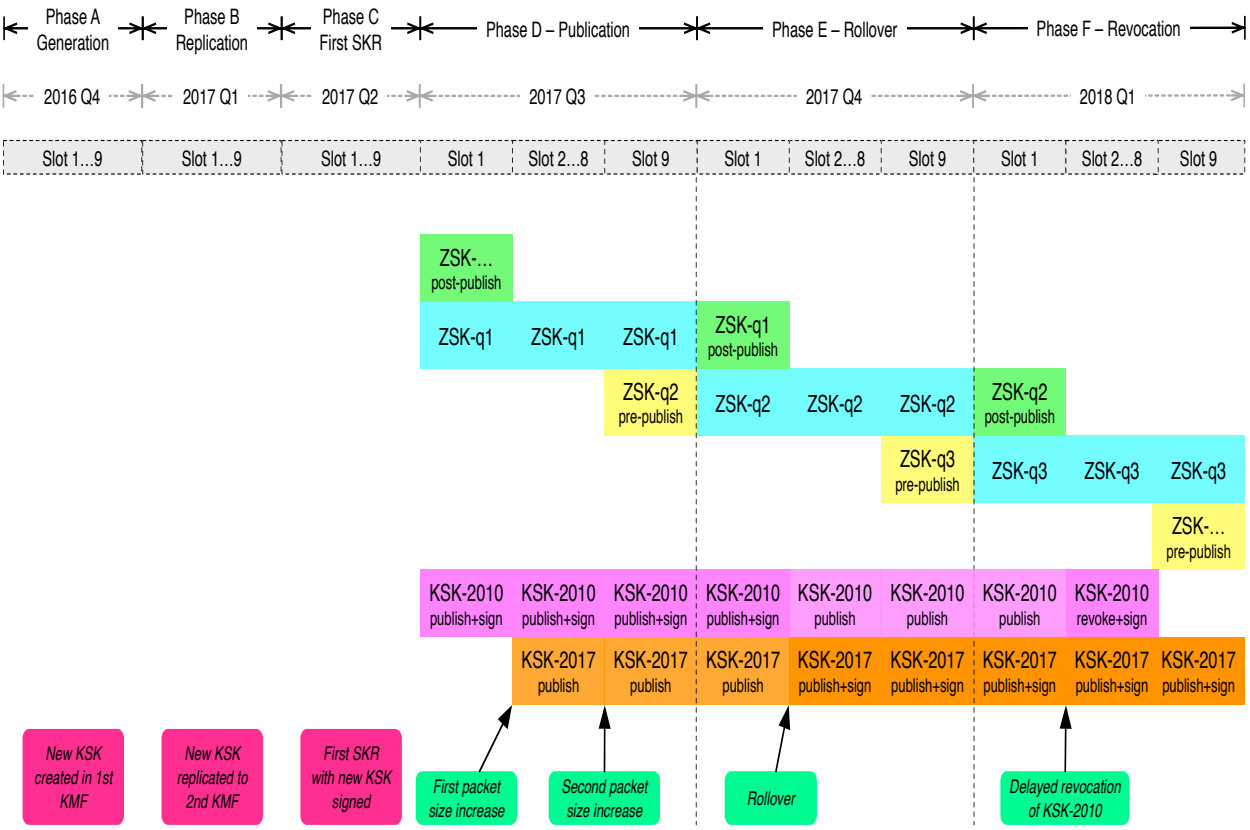
Introduction

This document describes in detail the operational steps to accomplish the 2017 KSK rollover project. The steps will be those performed by the IANA Functions Operator and the Root Zone Maintainer. The steps to be performed are based on the processes documented in the **Root Zone KSK Rollover Plan** developed by the Design Team, and internal documents and meetings of the IANA Functions Operator and Root Zone Maintainer.

Phases

The KSK rollover process updates the root zone trust anchor, introduces a new Key Signing Key (KSK-2017) in the root zone, and retires the current Key Signing Key (KSK-2010). The full process, from generating KSK-2017 to deleting KSK-2010 from key management facilities, is done in eight phases (A to H).

- **Phase A: Generation**
- **Phase B: Replication**
- **Phase C: First SKR**
- **Phase D: Publication**
- **Phase E: Rollover**
- **Phase F: Revocation**
- **Phase G: Delete 1**
- **Phase H: Delete 2**



For operators who implement *Automated Updates of DNS Security Trust Anchors* (RFC 5011) for the root zone, the rollover process will involve the three phases D, E and F. KSK-2017 is published in the root zone in phase D and begins its use for signing in phase E. KSK-2010 will stop being used in phase E and is then revoked in phase F.

For operators who manage trust anchors out of band, the root zone trust anchors file is needed. The process for obtaining and authenticating this file is out of scope of this document. The trust anchors file will be updated after KSK-2017 is successfully replicated and when KSK-2010 is revoked.

Changes to the keyset in the root zone and the trust anchors might lead to complications. Software may not be able to cope with the changes in the trust anchors file or the changed keyset in the root zone, while networks might not be able to handle an increased DNS response size. If these complications are widespread and severe, the Root Zone Management Partners may decide that these changes need to be undone to bring the system back to a stable state. This is referred to as a **back out** scenario.

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.

Impact of a Back Out or Extension

Backing out of the rollover process is a significant step. There is no contingency planned after a back out, other than to keep the stable back out state indefinitely. If there is a back out situation, the causes that led to a back out will be studied and the results will be used as input for a new KSK rollover process. In short, once a back out is performed, the process is essentially reversed back to the end of the previous phase. The only exception is once KSK-2010 is revoked in phase F, the back out is to go to phase G instead of going back to phase E, since a revoked key must not reappear unrevoked in the keyset data.

Extending the current phase means that the next phase of the KSK rollover process is postponed by at least one calendar quarter.

Assumptions and Design Requirements

- During the KSK rollover process, the ZSK is rolled regularly. The KSK rollover process is designed to work independently of the regular ZSK roll. A back out scenario should not hamper a regular ZSK roll. Hence, if the KSK roll process is brought back to a stable state, it will appear as if the latest step of the KSK roll did not happen while the ZSK has actually rolled forward.
- The plan is based on phases which currently match consecutive calendar quarters. However, phases may be extended to cover several quarters if required.
- It is assumed that a situation requiring the backing out of any phase is unlikely, but needs nevertheless to be fully planned for. ICANN has identified steps where a back out may be needed, and has developed plans for how to execute such a back out.
- The response sizes for a signed DNSKEY RRset response are, if possible, to be kept below 1500 bytes for a UDP query.

Terminology

- **HSM:** Hardware Security Module
- **KMF:** Key Management Facility
- **KSR:** Key Signing Request
- **SKR:** Signed Key Response
- **KSK-2010:** The key signing key (KSK) that has been used for signing the root zone since 2010.
- **KSK-2017:** The key signing key (KSK) that will be used for signing the root zone starting in 2017. This key will eventually replace KSK-2010.

Tentative Milestones

Date	Event
2016-07-22	The KSK roll project plan made public for review and discussion
2016-10-27	KSK-2017 KSK is generated
2017-02	KSK-2017 KSK is operationally ready
2017-03	KSK-2017 KSK is published on the IANA web site
2017-07-11	KSK-2017 KSK is published in the root zone
2017-09-19	Response size increase due to ZSK rollover
2017-10-11	KSK-2017 KSK is used for signing the root zone keyset
2018-01-11	KSK-2010 KSK is published as revoked
2018-03-22	KSK-2010 KSK is removed from the root zone
2018-08	KSK-2010 deleted from all HSMs
2018-08-31	The KSK rollover process concludes

Key Ceremonies

Month	Events related to KSK roll
2016-10	Generate KSK-2017 at the 1st KMF
2017-02	Replicate KSK-2017 to the 2nd KMF
2017-05	Produce phase D SKRs
2017-08	Produce phase E SKRs
2017-11	Produce phase F SKRs
2018-02	Normal key ceremony
2018-05	Delete KSK-2010 at 1st KMF
2018-08	Delete KSK-2010 at 2nd KMF

Quarters, Phases and Slots

The KSK rollover process is divided into eight phases (lettered as A to H). Each phase is aligned to a calendar quarter (starting January 1, April 1, July 1, and October 1), and contains nine slots of ten days (with the length of the last slot varying depending on how many days are left in the quarter). As per the *Root Zone DNSSEC Key Management* document, slots 9 and 1 are reserved for the ZSK roll, and slots 2 to 8 are reserved for the KSK roll. This means that changes to the KSK portion of the keyset will appear on the first day of slot 2 unless a back out is needed.

If a phase is extended, or if there is a situation which requires the process to be backed out to the previous phase, all actions associated with the next phase are postponed until the Root Zone Management Partners decide to transition to the next phase. If the process during phase F is backed out to phase G (since phase F cannot back out to phase E), there will still be a planned, full quarter phase G planned for the next quarter.

Phase A: Key Generation

Key ceremony tentatively scheduled for October 27, 2016, East Coast KMF.

- KSK-2017 generated at the first KMF
- Key backup transported to the second KMF

- Certificate Signing Request (CSR) of KSK-2017 is published as part of the audit records

Phase A is successful when KSK-2017 has been successfully generated at the first KMF and successfully stored in the Tier 6 security level of the second KMF.

Phase B: Key Replication

Key ceremony tentatively scheduled for February 2017, West Coast KMF.

- Key backup restored into production HSMs at the second KMF
- KSK-2017 now present at all four production HSMs at the two KMFs and thus operationally ready
- After the ceremony, update TA XML to include KSK-2017 (validFrom set to ceremony date)
- Deprecated validation methods for TA XML removed (see *Publication Changes*)

Phase B is successful when KSK-2017 has been successfully restored at the second KMF, and the TA XML update has been published.

Phase C: First SKR

Key ceremony tentatively scheduled for May 2017.

- First set of KSRs containing KSK-2017 are signed

Phase C is successful when the first set of KSRs have been successfully signed and tested.

Phase D: Publication

Publication of new key tentatively scheduled for July 11, 2017.

- KSK-2017 published the root zone as part of the DNSKEY RRset that is signed by KSK-2010

Phase D is successful when tested configurations have successfully configured a trust anchor based on the new key, and when there is no identifiable systemic failure impacting DNSSEC validating servers in numbers greater than the threshold set by the design team.

Phase E: Rollover

Key rollover tentatively scheduled for October 11, 2017.

- KSK-2017 used for signing the root DNSKEY RRset (which contains both KSK-2010 and KSK-2017)

Phase E is successful when no operational issues remain after rollover from KSK-2010 to KSK-2017.

Phase F: Revocation

Revocation tentatively scheduled for January 11, 2018.

- The DNSKEY RRset has both KSK-2010 with the revoked bit set and KSK-2017
- In slot 2, update TA XML to change the validUntil for KSK-2010 to be the start of slot

Phase F is successful when no operational issues remain after revocation of KSK-2010.

Phase G: Delete 1

Key ceremony tentatively scheduled for May 2018, East Coast KMF.

- KSK-2010 deleted from all HSMs at the first KMF
- Encrypted backups of KSK-2010 for first KMF are destroyed

Phase G is successful when KSK-2010 is no longer present in any HSM at the first KMF, and all backups have been destroyed.

Phase H: Delete 2

Key ceremony tentatively scheduled for August 2018, West Coast KMF.

- KSK-2010 deleted from all HSMs at the second KMF
- Encrypted backups of KSK-2010 for second KMF are destroyed

Phase H is successful when KSK-2010 is no longer present in any HSM at the second KMF, and all backups have been destroyed.

Key Signing Ceremonies

A KSK signs the DNSKEY RRset in the root zone. These signatures are generated during a key signing ceremony and become part of Signed Key Responses (SKR). An SKR contains the DNSKEY RRsets and signatures that are valid for each slot in the following quarter. Ceremonies are held once per quarter.

During a quarter, the rollover process can be in one of four different states. When all is well, the rollover process will go *forward* from the current phase to the next phase, starting the next quarter (phase C-to-D, D-to-E, etc.). If the Root Zone Management Partners decide to *extend* the current phase, the next quarter will be an extended phase (phase C-to-C, D-to-D, etc.). Additionally, the next quarter might need a *back out* (phase D-to-C, E-to-D, etc., with the exception of phase F, which can't go back to E as the key has already been revoked). Lastly, if the current phase has a back out, the next quarter is a *prolonged back out* phase (phase D-to-D, E-to-E, etc.).

Normal key ceremonies sign a single KSR (*Key Signing Request*) from the Root Zone Maintainer and return a single SKR (*Signed Key Response*). During the key rollover, the key ceremonies will need to sign multiple KSRs and return multiple SKRs to prepare the next quarter.

Detailed information on the various SKR configuration schemas can be found in *Appendix: SKR Configuration Schemas*.

SKR Summary

A KSK roll has an impact on the Root Zone in three consecutive phases. The SKRs for each of these phases are generated during the ceremony in the previous quarter.

- **Phase D: Introducing KSK-2017 (ceremony occurs in phase C)**
  - forward from C to D
  - back out from D to C
  - extend C to C
- **Phase E: Start using KSK-2017 and stop using KSK-2010 (ceremony occurs in phase D)**
  - forward from D to E
  - back out from E to D
  - extend D to D
  - prolong back out from C to C

- **Phase F: Revoking KSK-2010 (ceremony occurs in phase E)**
  - forward from E to F
  - back out from F to G
  - extend E to E
  - prolong back out from D to D

KSR/SKR File Names

The KSR/SKR files are named '{ksr|skr}-root-YYYY-qQUARTER-STRING.xml', where YYYY/QUARTER indicates which year and quarter the SKR is to be used and STRING is a string identifying which phase transition the KSR/SKR corresponds to. In addition to the filename, each KSR/SKR pair is uniquely identified by an id tag and a serial number in the XML in the files.

During the KSK roll, the Root Zone maintainer is expected to provide up to four KSRs for each ceremony in preparation for phase D, E and F. In these KSRs, the generic string should contain the letters of the two phases the KSR/SKR spans, e.g. "c-to-c", "c-to-d", "d-to-c", etc.

Phase D Ceremony (occurs in phase C)

The ceremony in phase C, to prepare for phase D, is tentatively scheduled for the second quarter of 2017. The XML SKR files generated during this ceremony all contain the string "skr-root-2017-q3-" at the beginning of the filename. There will be three files generated:

- **C-to-D:** move forward to publication (skr-root-2017-q3-c-to-d.xml)
- **D-to-C:** back out from publication to normal (skr-root-2017-q3-d-to-c.xml)
- **C-to-C:** extend phase C, do not continue to publication (skr-root-2017-q3-c-to-c.xml)

Phase E Ceremony (occurs in phase D)

The ceremony in phase D, to prepare for phase E, is tentatively scheduled for the third quarter of 2017 (assuming that phase C was not extended). The XML SKR files generated during this ceremony all contain the string "skr-root-2017-q4-" at the beginning of the filename. There will be four files generated:

- **D-to-E:** move from publication to rollover (skr-root-2017-q4-d-to-e.xml)

- **E-to-D:** back out from rollover to publication (skr-root-2017-q4-e-to-d.xml)
- **D-to-D:** extend phase D, stay in publication (skr-root-2017-q4-d-to-d.xml)
- **C-to-C:** prolong backout from phase D (skr-root-2017-q4-c-to-c.xml)

Phase F Ceremony (occurs in phase E)

The ceremony in phase E, to prepare for phase F, is tentatively scheduled for the fourth quarter of 2017 (assuming that there were no previous extensions). The XML SKR files generated during this ceremony all contain the string "skr-root-2018-q1-" at the beginning of the filename. There will be four files generated:

- **E-to-F:** move from rollover to revocation (skr-root-2018-q1-e-to-f.xml)
- **F-to-G:** move from revocation to normal (skr-root-2018-q1-f-to-g.xml)
- **E-to-E:** extend phase E, stay in rollover (skr-root-2018-q1-e-to-e.xml)
- **D-to-D:** prolong back out from phase E (skr-root-2018-q1-d-to-d.xml)

Trust Anchor Publication

Publication of root zone trust anchors will occur in two streams. The streams have different contents and different mechanisms for verification of the authenticity of the trust anchor.

Publication Stream Trust Anchors

In this stream, the trust anchors are in an XML-formatted file that contains the equivalent of DS records corresponding to the DNSKEY records for KSKs visible in the DNS root zone as well as keys intended for eventual publication as root zone KSKs that have been created but not yet published in the DNS. The root zone trust anchors are distributed over HTTPS from the URL **https://data.iana.org/root-anchors/root-anchors.xml**.

The authenticity of the contents of the publication stream trust anchor file can be verified with an S/MIME signature that is available from the URL **https://data.iana.org/root-anchors/root-anchors.p7s**. That signature chains to the ICANN Root CA.

For the upcoming KSK rollover, the publication stream trust anchor will change when the new KSK (KSK-2017) has been installed in the second KMF, and again when the old KSK (KSK-2010) is published with its revoked bit set.

KSK Creation Stream Trust Anchors

In this stream, a trust anchor is a certificate signing request (CSR) that was created during a KSK creation ceremony. The CSR is in PKCS#10 format (described in RFC 2986). The CSR contains a DS record in the *subject* field, and the public key in the *subjectPKInfo* field. The first trust anchor in this stream is the CSR that was created in the 2010 KSK creation ceremony.

The authenticity of a CSR can be verified by comparing the contents of the CSR with the contents of the CSR announced during the KSK generation ceremony. The log containing the CSR from the first KSK generation can be found at **https://data.iana.org/ksk-ceremony/1/kskgen-20100616-211906.log**.

Normal Use of Trust Anchors by Software Developers

Software developers who create or maintain DNSSEC validation software are encouraged to have their software conform to RFC 5011. For such software, a trust anchor is needed for initializing the trust anchor store but the software itself does not need to retrieve the root zone trust anchor after that because updating is done through the DNS itself.

Software developers who store trust anchors in configuration files are encouraged to retrieve the publication stream trust anchor file (the XML file) when the software distribution is being created, when the software is being installed by an operator, or at both events.

For software that does not conform to RFC 5011, or software that is configured to not use RFC 5011 for updating trust anchors using the DNS, the publication stream trust anchor file should be retrieved when the resolver starts up, and when the KSKs in the DNSKEY RRset in the DNS root zone are changed.

Whenever the publication stream trust anchor is used, it should be compared to the contents of the DNSKEY RRset in the DNS root zone. Only DNSKEY records that are associated with records in the trust anchor XML file should be trusted.

Other Use of Trust Anchors by Software Developers

Software developers can also use the KSK creation stream trust anchor files to configure trust anchors before the associated DNSKEY record appears in the DNS root zone. A developer can extract the DS record and the public key from those files.

Note, however, that the data in the CSR for a newly-created key that is not in the DNSKEY RRset in the root zone might never appear in the root zone, or might appear in the root zone and later be removed. Because of this, software that uses these trust anchors can easily have an incorrect view of the KSKs actually in use. This stream is made available mostly for operators who want to perform additional comparisons of the contents of the zone with the contents of the keys at the time of their creation.

Publication Changes

- A detached PGP signature of the Trust Anchor XML file was issued for KSK-2010. Such a PGP signature **will not be issued** for KSK-2017.
- A certificate containing the root KSK, signed by a certificate that chains to the ICANN Root CA, was issued for KSK-2010. Such a certificate **will not be issued** for KSK-2017.

These publication changes will occur during Phase B, which introduces changes to the Trust Anchor XML file to add KSK-2017.

Key Management

Key Generation & Replication

The new KSK will be generated during a key ceremony at one of two Key Management Facilities (KMF). The key will be created in one of two Hardware Security Modules (HSM) and immediately transferred to another HSM at the same KMF. Encrypted key backups and associated HSM database files will also be created and one of them transported to the other KMF. At next key ceremony, a key backup will be imported to two HSMs at the other KMF.

No software changes are required to create the new KSK.

Key Deletion

When the incumbent KSK has been revoked, the key is deleted from all HSMs.

No software changes are required to delete the old KSK.

KSR Signing

The existing KSR signer (*ksrsigner*) was not designed for the current key rollover scheme and needs to be updated in order to be able to produce the required SKRs.

The following configuration schemas (further explained in *Appendix: SKR Configuration Schemas*) must be implemented by *ksrsigner*:

- normal(2010)
- normal(2017)
- publish(2010,2017)
- publish+(2010,2017)
- rollover(2010,2017)
- rollover+(2010,2017)
- revoke(2010,2017)
- revoke+(2010,2017)

Coordination

RSSAC

ICANN will request that RSSAC coordinate a review of the detailed timetable for the KSK rollover period before it is published, and should accommodate reasonable requests to modify that timetable in the event that any root server operator identifies operational reasons to do so.

ICANN will coordinate with RSSAC to request that the root server operators carry out data collection that will inform subsequent analysis and help characterize the operational impact of the KSK rollover, and that the plans and products of that data collection be made available for third-party analysis.

RZM Partners

The RZM Partners will use multiple real-time communications channels during critical changes to the root zone. This includes addition and removal of a KSK, as well as changes in priming queries response sizes.

The existing system (**Send Word Now**) used by the Root Zone Maintainer to alert root server operators in case of operational issues will be used to alert the RZM Partners in case out of schedule events need to be assessed and acted upon quickly.

Trusted Community Representatives

Trusted Community Representatives (TCRs) that attest to the proper conduct of key ceremonies, must be fully informed of the rollover program and understand the implications of each phase in order to properly oversee and attest the relevant key ceremonies. ICANN will perform outreach and information sharing throughout the process to aid proper oversight by this group.

Appendix: SKR Configuration Schemas

A number of different SKR configuration schemas will be needed for the KSK rollover. For each schema below, the following information is provided:

- ***schema*** -- the name of configuration schema (referred to elsewhere)
- ***publish*** -- what keys to published as the DNSKEY RRset
- ***sign*** -- what keys to use to sign the DNSKEY RRset

C-to-C & D-to-C

- ***schema:*** *normal(2010)*
- ***publish:*** *KSK-2010 during all slots*
- ***sign:*** *all slots with KSK-2010*

C-to-D

- ***schema:*** *publish(2010,2017)*
- ***publish:*** *KSK-2010 during slot 1*
- ***publish:*** *KSK-2010 & KSK-2017 during slot 2-9*
- ***sign:*** *all slots with KSK-2010*

D-to-D & E-to-D

- ***schema:*** *publish+(2010,2017)*
- ***publish:*** *KSK-2010 & KSK-2017 during slot 1-9*
- ***sign:*** *all slots with KSK-2010*

D-to-E

- ***schema:*** *rollover(2010,2017)*
- ***publish:*** *KSK-2010 & KSK-2017 during slot 1-9*
- ***sign:*** *slot 1 with KSK-2010*
- ***sign:*** *slot 2-9 with KSK-2017*

E-to-E

- ***schema:*** *rollover+(2010,2017)*
- ***publish:*** *KSK-2010 & KSK-2017 during slot 1-9*
- ***sign:*** *all slots with KSK-2017*

E-to-F

- ***schema:*** *revoke(2010,2017)*
- ***publish:*** *KSK-2010 & KSK-2017 during slot 1*
- ***publish:*** *revoked KSK-2010 & non-revoked KSK-2017 during slot 2-8*
- ***publish:*** *KSK-2017 during slot 9*
- ***sign:*** *slot 1 with KSK-2017*
- ***sign:*** *slot 2-8 with KSK-2010 and KSK-2017*
- ***sign:*** *slot 9 with KSK-2017*

F-to-G & G-to-G

- ***schema:*** *normal(2017)*
- ***publish:*** *KSK-2017 during all slots*
- ***sign:*** *all slots with KSK-2017*

F-to-F

- ***schema:*** *revoke+(2010,2017)*
- ***publish:*** *KSK-2017 during slot 1*
- ***publish:*** *revoked KSK-2010 & non-revoked KSK-2017 during slot 2-8*
- ***publish:*** *KSK-2017 during slot 9*
- ***sign:*** *slot 1 with KSK-2017*
- ***sign:*** *slot 2-8 with KSK-2010 and KSK-2017*
- ***sign:*** *slot 9 with KSK-2017*

Appendix: Design Team Recommendations

The **Root Zone KSK Rollover Plan** presents a number of recommendations. This appendix describes how the *Operational Implementation Plan* applies to these recommendations.

Recommendation 1: The Root Zone KSK rollover should follow the procedures described in RFC 5011 to update the trust anchors during KSK rollover.

> ICANN will use RFC 5011 to roll the root KSK.

Recommendation 2: ICANN should identify key DNS software vendors and work closely with them to formalize processes to ensure that trust anchor distribution using vendor-specific channels is robust and secure.
Recommendation 3: ICANN should identify key DNS systems integrators and work closely with them to formalize processes to ensure that trust anchor distribution using integrator-specific channels is robust and secure.

> ICANN has identified DNS software vendors and systems integrators, and will work closely with them to formalize processes to ensure that trust anchor distribution using integrator-specific channels are robust and secure.

Recommendation 4: ICANN should take an active role in promoting proper root zone trust anchor authentication, including highlighting the information posted on ICANN's IANA website.

> Revised trust anchor publication methods are part of the Operational Implementation Plan and will be promoted on the IANA website. ICANN is also working with authors of Internet Draft **draft-jabley-dnssec-trust-anchor** to describe the current trust anchor format and publication mechanisms.

Recommendation 5: Root Zone KSK rollover should require no substantive changes to existing KSK management and usage processes to retain the high standards of transparency associated with them.

> ICANN will not make any substantive changes to existing KSK management and usage processes.

Recommendation 6: All changes to the root zone DNSKEY RRsets must be aligned with the 10-day slots described in the KSK Operator's DPS.

The KSK rollover will be aligned with the 10-day slots described in the KSK Operator's DPS.

Recommendation 7: The existing algorithm and key size for the incoming KSK for the first Root Zone KSK rollover should be maintained.

Recommendation 8: The choice of algorithm and key size should be reviewed in the future for subsequent Root Zone KSK rollovers.

ICANN will not change the algorithm nor the key size for the new KSK.

Recommendation 9: ICANN, in cooperation with the RZM Partners, should design and execute a communications plan to raise awareness of the Root Zone KSK rollover, including outreach to the global technical community through appropriate technical meetings and to "Channel Partners" such as those identified in this document.

ICANN will develop and execute a communications plan in cooperation with the RZM Partners.

Recommendation 10: ICANN should request that RSSAC coordinate a review of the detailed timetable for the KSK rollover period before it is published, and should accommodate reasonable requests to modify that timetable in the event that any root server operator identifies operational reasons to do so.

ICANN has requested that RSSAC coordinate a review of the detailed timetable.

Recommendation 11: ICANN should coordinate with RSSAC and the RZM Partners to ensure that real-time communications channels are used to ensure good operational awareness of the root server system for each change in the root zone that involves the addition or removal of a KSK.

The RZM Partners will use multiple real-time communications channels during critical changes to the root zone. Such changes include addition and removal of a KSK in the root zone as well as changes in priming query response sizes.

Recommendation 12: ICANN should coordinate with RSSAC to request that the root server operators carry out data collection that will inform subsequent analysis and help characterize the operational impact of the KSK rollover, and that the plans and products of that data collection be made available for third-party analysis.

ICANN will coordinate with RSSAC to request that the root server operators carry out data collection that will inform analysis. The plans and results of that data collection will be made available to the public.

Recommendation 13: The RZM Partners should ensure that any future increase in ZSK size is carefully coordinated with KSK rollovers, such that the two exercises are not carried out concurrently.

The length of ZSK will be changed from 1024 to 2048 bits during 2016, and the KSK will be rolled after this change has been implemented.

Recommendation 14: To support a number of potential operational contingencies that may require rollback of changes to the root zone during each phase of the KSK key roll, SKRs using the incumbent KSK, SKRs using both the incumbent and the incoming KSK, and SKRs using the incoming KSK should be generated. The Design Team also recommends that the double-signing approach is the preferred mechanism to respond to a requirement to perform a rollback in Quarter 2 of the key roll procedure.

ICANN has developed a *Back Out Plan* to handle anticipated deviations from the *Operational Implementation Plan*. ICANN has chosen to not double-sign the back out of the key rollover phase, as further analysis has shown that this might put operations in an even more dangerous state due to packet size increase.

A double-signed approach would increase the size of the priming query at the time of back out from 1139 bytes to 1425 bytes. This would possibly create the need to back out once more to the increased response size.

In order for a resolver to be negatively affected by such a back out, it would had to have updated its trust anchor set by replacing KSK-2010 with KSK-2017, instead of just adding KSK-2017. However, the trust anchors distributed by IANA will include both trust anchors. ICANN does not believe that protecting against such a misconfiguration warrants an increase in back out complexity.

Recommendation 15: The RZM Partners should undertake or commission a measurement program that is capable of measuring the impact of changes to resolvers' DNSSEC validation behavior, and also capable of estimating the population of endpoints that are negatively impacted by changes to resolvers' validation behavior.

ICANN will commission ongoing measurements of the rate of DNSSEC validation. These measurements will be able to detect statistically significant drops in the amount of validation when changes are made to the KSK.

Recommendation 16: Rollback of any step in the key roll process should be initiated if the measurement program indicated that a minimum of 0.5% of the estimated Internet end-user population has been negatively impacted by the change 72 hours after each change has been deployed into the root zone.

ICANN will consider back out of any step in the key roll process if the measurement program indicates a considerable amount of the estimated Internet end-user population has been negatively impacted by the change 72 hours after each change has been deployed into the root zone.

Recommendation 17: It is recommended that the KSK rollover process should begin on 1 April 2016, beginning with a nine-month period to generate the new KSK and use the existing scheduled KSK access ceremonies in the period from March to December 2016 to generate the new KSK, copy it to the secondary facility, and prepare the key material to be used in the key roll. The actions associated with changes to the root zone, using the steps and associated timetable as described in "Schedule for the Root Zone KSK Rollover" of this report will begin on 1 January 2017. The publication of the new KSK should be incorporated into the root zone on 11 January 2017, and the old KSK withdrawn and the new KSK to be used in its place on 1 April 2017. If the outcome of the process to evaluate acceptance of the new KSK meets the acceptance criteria described in "Rollback" of this report, then the old KSK should be revoked starting on 11 July 2017 and the revocation should be removed from the root zone 70 days thereafter, on 19 September 2017.

A detailed tentative schedule can be found in section *Tentative Milestones* of the *Operational Implementation Plan*.

Appendix: SSAC Recommendations

SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone presents a number of recommendations. This appendix describes how the *Operational Implementation Plan* assent to these recommendations.

Recommendation 1: Internet Corporation for Assigned Names and Numbers (ICANN) staff, in coordination with the other Root Zone Management Partners (United States Department of Commerce, National Telecommunications and Information Administration (NTIA), and Verisign), should immediately undertake a significant, worldwide communications effort to publicize the root zone KSK rollover motivation and process as widely as possible.

> ICANN has developed and will execute a communications plan in cooperation with the RZM Partners.
>
> ICANN has also identified DNS software vendors and systems integrators, and will work closely with them to formalize processes to ensure that trust anchor distribution using integrator-specific channels are robust and secure.

Recommendation 2: ICANN staff should lead, coordinate, or otherwise encourage the creation of a collaborative, representative testbed for the purpose of analyzing behaviors of various validating resolver implementations, their versions, and their network environments (e.g., middle boxes) that may affect or be affected by a root KSK rollover, such that potential problem areas can be identified, communicated, and addressed.

> ICANN will develop and deploy two external test environments, accessible by the general Internet public, to evaluate whether external systems are prepared to participate in the KSK roll. One test environment will provide multiple key rollovers in real time, whereas the other will provide continuous key rollovers using accelerated time.

Recommendation 3: ICANN staff should lead, coordinate, or otherwise encourage the creation of clear and objective metrics for acceptable levels of “breakage” resulting from a key rollover.

> ICANN staff will lead the creation of clear and objective metrics for acceptable levels of "breakage" resulting from a key rollover.

Recommendation 4: ICANN staff should lead, coordinate, or otherwise encourage the development of rollback procedures to be executed when a rollover has affected operational stability beyond a reasonable boundary.

> ICANN has developed a *Back Out Plan* that describes anticipated deviations from the *Operational Implementation Plan* based on anomalies occurring while executing the operational plan. The *Back Out Plan* describes the process to be followed, including data collection, applicable criteria, and the steps involved in changing the contents of the DNS.

Recommendation 5: ICANN staff should lead, coordinate, or otherwise encourage the collection of as much information as possible about the impact of a KSK rollover to provide input to planning for future rollovers.

> ICANN staff is already collecting root server traffic from two of the root server operators and collects RSSAC-002 statistics from every operator that is making them available to the public.

One World, One Internet

ICANN.ORG