KSK Rollover: Questions and Answers

What is the Key Signing Key?

- The Root Zone Key Signing Key (KSK) is a cryptographic public-private key pair that plays an important role in the Domain Name System Security Extensions (DNSSEC). The Root Zone KSK serves as the trusted starting point for DNSSEC validation, similar to how the root zone serves as the starting point for DNS resolution.
- Just as one starts at the root zone to resolve a domain name anywhere in DNS, software performing DNSSEC validation trusts the root zone KSK and builds a "chain of trust" of successive keys and signatures to validate the authenticity of any signed data in DNS.

What does the Key Signing Key (KSK) rollover involve?

- The KSK rollover process updates the root zone trust anchor by introducing a new KSK (KSK-2017) into the root zone.

Why roll the KSK?

- Because it's not good for a cryptographic key to live forever. Like any password, it needs to be changed sometimes.
- Because it's better to make proactive changes during normal operations when things are running smoothly, rather than be reactive in an emergency.
- When DNSSEC was first deployed in 2010, NTIA required that the KSK be rolled and the Root Zone Management Partners subsequently outlined requirements to change the key after five years of operations. The role of NTIA ended on 1 October 2016.

Who needs to know about the KSK rollover?

- Internet service providers, enterprise network operators and others who operate DNSSEC validation must update their systems with the public part of the new key signing key.

How will they know?

- ICANN is executing an extensive outreach campaign to ensure that those who currently use the KSK know about the change.
- Interested parties can view a schedule of events at which the rollover will be discussed on the ICANN website, where they can also follow KSK updates and join a special mailing list. They can also follow the hashtag #KeyRoll on social media to stay informed.

What's the impact on Internet users?

- If completed smoothly, there will be no visible change for the end user.

What could go wrong?

- It's possible that some software performing DNSSEC validation will not be updated with the new KSK, or that some software may not be able to cope with the changes in the trust anchors file published on the IANA website. If these complications are widespread, the Root Zone Management Partners may decide that the changes need to be reversed so the system can be brought back to a stable state. This is referred to as a "back out scenario." If necessary, the length of a given phase may also be extended to help

ensure stability, if for example new information indicates that the next phase may lead to complications.

What would the effect be of a "back out" or extension?

- The whole point of a back out or extension would be to maintain operational stability so the effect on end users would be minimal.

How long would a back out or extension last?

- It could last indefinitely or until the causes that led to a back out are studied and rectified. The fixes would then be folded into a new KSK rollover process.

Will network operators see a financial impact from the KSK rollover?

- In most cases, preparing for the KSK rollover will have a small associated cost. However, network operators with dedicated IT staffers can help prepare for the KSK rollover during routine network maintenance, without additional costs.
- After a network operator prepares for the rollover, there is minimal or no further financial impact. Network operators who verify their DNS resolution infrastructure can support the automated update of the key and will not need to make any changes to their infrastructure or modifications to their operational procedures.
- If network operators are unprepared for the rollover and they have enabled DNSSEC, they run the risk of a significant financial impact. If the trust anchor has not been updated to reflect the new key, DNS resolvers will treat responses signed under the new key as having been tampered with and will discard those responses. This will result in end users getting an error any time they look up a domain name, which could result in support calls from customers.

How exactly will the KSK be rolled?

- It will take place in eight phases, which are expected to take about two years. Each of the eight phases is associated with a scheduled key ceremony.
- A KSK signs the DNSKEY Resource Record Set (RRset), which is all the records for a given domain in the root zone. These signatures are generated during key signing ceremonies and become part of Signed Key Responses (SKRs).

What's the timing of the eight phases?

- **Phase A: Key generation (Oct 2016)**
  - KSK-2017 generated at the first key management facility
- **Phase B: Key replication (Feb 2017)**
  - KSK-2017 copied to the second key management facility. KSK now qualified for entering the production state.
- **Phase C: First data is signed with KSK-2017 for use in Phase D (May 2017)**
  - First set of key signing requests are signed.
- **Phase D: Publication (Aug 2017)**
  - KSK-2017 is published to the root zone.
  - Both KSK-2010 and KSK-2017 are used to sign the root zone.
- **Phase E: Rollover (Nov 2017)**
  - Only KSK-2017 is used to sign the root zone.
- **Phase F: Revocation (Feb 2018)**
  - KSK-2010 is removed from the root zone.
- **Phase G: Delete 1 (May 2018)**

    - KSK-2010 is deleted from the first key management facility.
- **Phase H: Delete 2 (Aug 2018)**
    - KSK-2010 is deleted from the second key management facility

What action can be taken now?

- Software developers who create or maintain DNSSEC validation software should make certain it conforms to RFC 5011.
- For software that does not conform to RFC 5011, or software that is configured to not use RFC 5011, a publication stream trust anchor file will be available here. The file should be retrieved when the resolver starts up, and when the KSKs in the DNSKEY RRset in the DNS root zone are changed.
- Software developers and operators of validating resolvers can access operational tests, developed by ICANN, to evaluate whether their systems properly implement RFC 5011 and will automatically update during the KSK roll.