DNSSEC & KSK Rollover

Patrick Jones

Middle East DNS Forum
24 April 2018
What is DNSSEC?

- DNSSEC = “DNS Security Extensions”
- DNSSEC is a protocol that is currently being deployed to secure the Domain Name System (DNS)
- DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names
- Result of over a decade of community based, open standards development
DNS Security Extensions

- Provides origin authentication
- Integrity assurance for DNS data
- Authenticated denial of existence of DNS data

creates a chain of trust
DNSSEC

Benefits

- **End User** – gain confidence of reaching intended website
- **Registrant** – fraud mitigation & greater brand protection
- **Registrar** – Comply with industry standards & meet registrant demands for increased security
- **Registry** – Meet industry good practices & registrar demands for increased domain security
Benefits

- Attract and retain security & reputation-focused registrants
- Create new service offerings
- Adding to trust overall
State of DNSSEC Deployment

Over 90% of top-level domains are signed with DNSSEC

- 1543 TLDs in the root, 1407 are signed
- About 50% of ccTLDs are signed
- Recent adoption in Bhutan, Italy, Guinea-Bissau
- 2nd level DNSSEC deployment growing slow & steady
State of DNSSEC Deployment
KSK Rollover
ICANN is in the process of performing a Root Zone DNS Security Extensions (DNSSEC) Key Signing Key (KSK) rollover

- The Root Zone DNSSEC Key Signing Key “KSK” is the topmost cryptographic key in the DNSSEC hierarchy

- The KSK is a cryptographic public-private key pair:
  - Public part: trusted starting point for DNSSEC validation
  - Private part: signs the Zone Signing Key (ZSK)

- Builds a “chain of trust” of successive keys and signatures to validate the authenticity of any DNSSEC signed data
Why is ICANN Rolling the KSK?

- Because it’s not good for a cryptographic key to live forever. The cryptographic keys used in DNSSEC-signing DNS data should be changed periodically
  - Ensures infrastructure can support key change in case of emergency

- This type of change has never before occurred at the root level
  - There has been one functional, operational Root Zone DNSSEC KSK since 2010

- Because it’s better to make proactive changes during normal operations when things are running smoothly, rather than be reactive in an emergency. The KSK rollover must be widely and carefully coordinated to ensure that it does not interfere with normal operations
When Does the Rollover Take Place?

- The changing or "rolling" of the KSK Key was originally scheduled to occur on 11 October 2017, but it was delayed because some data obtained in September 2017 showed that a significant number of resolvers used by Internet Service Providers (ISPs) and Network Operators were not yet ready for the key rollover.

- There may be multiple reasons why operators do not have the new KSK installed in their systems: some may not have their resolver software properly configured.

- After a preliminary consultation with the community, ICANN posted a plan for starting the rollover process again. That plan was open for community comment at https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en. The comment period closed on 2 April 2018 and a summary was published on 23 April 2018.

- The plan calls for ICANN to roll the root KSK on 11 October 2018 while encouraging ISPs and Network operators to use this additional time period to be certain that their systems are ready for the key rollover.
What Do Operators Need to Do?

- Be aware whether DNSSEC is enabled in your servers
- Be aware of how trust is evaluated in your operations
- Test/verify your set ups
- Inspect configuration files, are they (also) up to date?
- If DNSSEC validation is enabled or planned in your system
  - Have a plan for participating in the KSK rollover
  - Know the dates, know the symptoms, solutions
How To Update Your System

If your software supports automated updates of DNSSEC trust anchors (RFC 5011):

- The KSK will be updated automatically at the appropriate time
- You do not need to take additional action
  - Devices that are offline during the rollover will have to be updated manually if they are brought online after the rollover is finished

If your software does not support automated updates of DNSSEC trust anchors (RFC 5011) or is not configured to use it:

- The software’s trust anchor file must be manually updated
- The new root zone KSK is now available here after March 2017:

  http://data.iana.org/root-anchors/
ICANN is offering a test bed for operators or any interested parties to confirm that their systems handle the automated update process correctly.

Check to make sure your systems are ready by visiting: go.icann.org/KSKtest
For More Information

1. Visit https://icann.org/kskroll

2. Join the conversation online
   - Use the hashtag #KeyRoll
   - Sign up to the mailing list https://mm.icann.org/listinfo/ksk-rollover

3. Ask a question to globalsupport@icann.org
   - Subject line: “KSK Rollover”

4. Attend an event
   - Visit https://features.icann.org/calendar to find upcoming KSK rollover presentations in your region
Engage with ICANN – Thank You and Questions

Visit us at icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann
linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann