Root KSK Management

Briefing for the CSC, March 2020

Kim Davies
VP, IANA Services; President, PTI
Introduction

- Root zone is signed with DNSSEC since 2010
- Uses two layers of signatures, as is common:
  - A secure entry point, known as a **key signing key** (KSK)
  - Operational keys, rotated regularly, endorsed by the KSK, known as **zone signing keys** (ZSKs)
- What is less common is custody of these two layers is distinct:
  - KSK is managed by PTI
  - ZSK is managed by Verisign, as root zone maintainer
- The KSK for the root zone is also unique as it serves as the secure entry-point to the whole DNS (by virtue of being at the root), known as being a **trust anchor**.
  - Configured in resolution devices, so difficult to change.
  - Because changes can not be done rapidly, extra caution is required in its management.
KSK Management

• Highly transparent process was designed to manage the KSK
  • Opposite of similar practices for likeminded tasks, usually highly secret.
• Involvement includes the concept to ‘trusted community representatives’
  • Selected for geographical, skills and representation balance
  • Performs some of the multi-layers trusted roles for the KSK management
  • Builds confidence in KSK management by acting as a conduit to the communities they represent
• Constantly improving
  • Always take lessons learnt and build action plans to evolve our approach
Overview of KSK security

- The root KSK is stored in a device called a **hardware security module (HSM)** whose sole purpose is to securely store cryptographic keys. The device is designed to be tamper-proof. If there is an attempt to open it, the contents with self-destruct.
Overview of KSK security

- Seven smart cards exist that can turn on each device. The device is configured such that **3 of the 7 smart cards** must be present to make it useable.
Overview of KSK security

• Each smart card is assigned to a different ICANN community member, known as a trusted community representative. To access the key signing key, therefore, at least three of these TCRs need to be present*. 

*Note: The text indicates that accessing the key signing key requires the presence of at least three TCRs, but the specific number three is mentioned, suggesting it is a minimum requirement. The asterisk (*) implies additional context or a footnote that is not visible in the image.
Overview of KSK security

- The HSM is stored inside a high-security safe, which can only be opened by a designated person, the **safe security controller**. The safe is monitored with seismic and other sensors.
Overview of KSK security

- The safes are stored in a secure room which can only be opened jointly by two designated persons, the ceremony administrator and the internal witness. The room is monitored with intrusion and motion sensors.
Overview of KSK security

- The safe room is located within a larger room where ceremonies are performed involving the TCRs and other persons. Ceremonies are recorded on video, witnessed by the participants and others, and audited by a third-party audit firm. Access to the room needs to be granted by another designed person, the **physical access control manager**, who is not on-site.
Overview of KSK security

- The ceremony rooms, known as **key management facilities**, are located within two guarded facilities, one each on the US West and East costs.

US West KMF
El Segundo, California

US East KMF
Culpeper, Virginia
Selected Operational Tasks

- Coordinate and hold KSK ceremonies
- Manage TCR relationships
- Liaise with Verisign on ZSK issues (key exchange, DPS, logistics, evolution)
- Hardware lifecycle management
- Vendor management
- Enhancement projects, including associated R&D
- Audit management (engagement, control design, evidence)
- Policy and procedure lifecycle management

- Performed by two staff within the IANA team
Key ceremonies

- Approximately four times a year, the TCRs others meet to use the HSMs to sign keys to be used for the root zone.
- The ceremony is conducted in a highly transparent manner, the with opportunity for interjection if anyone is concerned.
- The purposes is to ensure **trust in the process**. DNSSEC only provides security if the community is confident the KSK has not been compromised.
Key ceremonies

- Each ceremony is orchestrated using a comprehensive script that identifies each individual step that needs to be undertaken.
Ceremony artefacts

- The process is streamed and recorded, with external witnesses watching every step. All materials (videos, code, scripts, etc.) are posted online.
Recent Operational Activity

- Consultation on Future KSK Rollovers
- Retrospective on Ceremony 40
- Planning for Ceremony 41
Consultation on Future KSK Rollovers

- First KSK was created in 2010 (“KSK-2010”)
- Design team was formed to develop a set of recommendations on how to perform a rollover
- Originally scheduled for 2017, the second KSK (“KSK-2017”) ultimately started signing the zone on 11 October 2018
  - One year pause in process to consider impact of anomalous telemetry data
- Rollover successfully occurred with minimal disruption
- **What do we want to do now?**
Initial feedback

- Recognizing community interest in the rollover was at its peak during and shortly after the rollover, we solicited comments and directed responses to the ksk-rollover list for capture.
- We undertook to analyze those comments in 2019H2 and produce a recommendation for future rollovers.
- Common themes in this early commentary:
  - KSK rollover should be a routine event
  - KSK should be rolled over annually
  - Introduce backup and/or standby keys
  - Perform more monitoring of impacts of larger keysets
  - Consider alternate signing algorithms
Our proposal

• Create a predictable approach to future rollovers
• Plan for a three-year rollover interval to balance desire for more regular rollovers with the operational complexity involved
• At least two years for the new trust anchor to be published in advance, allowing greater propagation before the rollover
• Use similar phased approach aligned with the quarterly key ceremony schedules
Public Consultation

• We published an outline of the approach.
• Public comment period closed last month, in the process of distilling feedback received from 11 comments.
• Currently in the process of compiling staff report (delayed due to key ceremony issues we'll discuss next)
KSK Ceremony 40
(The last one)
Key Ceremony 40

• Scheduled for 12 February 2020
• Objectives
  • Sign the 2020Q2 key material (covering April-June 2020)
  • Decommission a HSM
• Pre-ceremony activity included maintenance work to upgrade the lock assemblies within the safe
  • These are performed in administrative ceremonies that are audited to the same standard as the key signing ceremonies, but do not involve HSM activation
  • Administrative ceremonies can also include when we induct new staff members into trusted roles
  • TCRs that are available are invited to witness these administrative ceremonies
On 11 February, the pre-ceremony work was being conducted to upgrade the lock assembly with a newer model.

The safe would not open.

- The device indicated the combination was dialed correctly, but the bolt did not retract to allow safe access.
- Electrical or mechanical failure of the lock.

The remedy exercised one of the worst-case disaster recovery scenarios that had been contemplated — “drilling the safe”.

- Approximately 20 hours across two days to drill into the lock assembly, remove the bolt, to allow the safe to open
- Followed by safe remediation and installation of new lock
- Complicated by triggering anti-defeat mechanisms in the lock due to novel materials in safe construction
Some takeaways

• Ceremony was successfully conducted with a 4 day delay
• Gained valuable experience that will inform our future plans for disaster recovery
• Community volunteers and staff alike supported us around the clock to bring the issue to conclusion and perform key ceremony
• Some revisions to administrative ceremonies moving forward to provide greater transparency.
KSK Ceremony 41
(The next one)
Key Ceremony 41

- Scheduled for 23 April 2020 (10 year anniversary!)

- Objectives
  - Sign the 2020Q3 key material (covering July-September 2020)
  - Replace two Trusted Community Representatives (COs)

- Currently expected to be held as planned, but the evolving Coronavirus situation has caused us to focus on developing contingencies in case the situation deteriorates

- Ongoing work
  - Periodic re-evaluation of participants ability to travel
  - Continuous monitoring of evolving threat situation
  - Building out contingency scenarios

- Notably, the design of the Key Management Facilities is designed to enable key operations to be performed in a disaster recovery scenario without the minimum number of TCRs present.
  - The exact triggering conditions, however, have not been well defined.
Contingency ideas

- Roughly in increasing order of severity:
  - Hold the ceremony with less than ideal number of people present
  - Advance the ceremony date
  - Postpone the ceremony date
  - Hold the ceremony in the alternative facility
  - Induct new TCRs to replace those unable to travel
  - Sign key material beyond a single quarter
  - Perform ceremony with less than 3 TCRs physically present, and/or below other staffing minimums

- Long-term mitigators for future ceremonies:
  - Re-evaluate alternate KMF locations
  - Reconfigure how many TCRs are needed, their geographic locations, can they overlap roles, etc.

- Areas we are exploring DPS updates
  - More precise triggering conditions mapped out in advance for contingency scenarios
General Observations
General Observations

- We feel the current KSK management is highly transparent and has a high level of accountability
  - Audited against an external framework, extensive use of third party auditors
  - TCRs play a key role in observing and critiquing the process, provides a feedback loop for continuous improvement
  - Materials are all made available to any third-party to apply scrutiny
- We provide thought leadership to those that manage CAs.
- Customer satisfaction (e.g. annual surveys) consistently high.
- As part of the naming functions, performance monitoring by the CSC is within its charter.
- Consider that transparency initiatives account for a large part of staff time already, should any changes be additive or substitute existing arrangements? What gaps are being filled? What resources are required to fulfill them?
Thank you!

kim.davies@iana.org