

# Root KSK Management

Briefing for the CSC, March 2020

Kim Davies

VP, IANA Services; President, PTI

**PTI** | An ICANN Affiliate

# 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

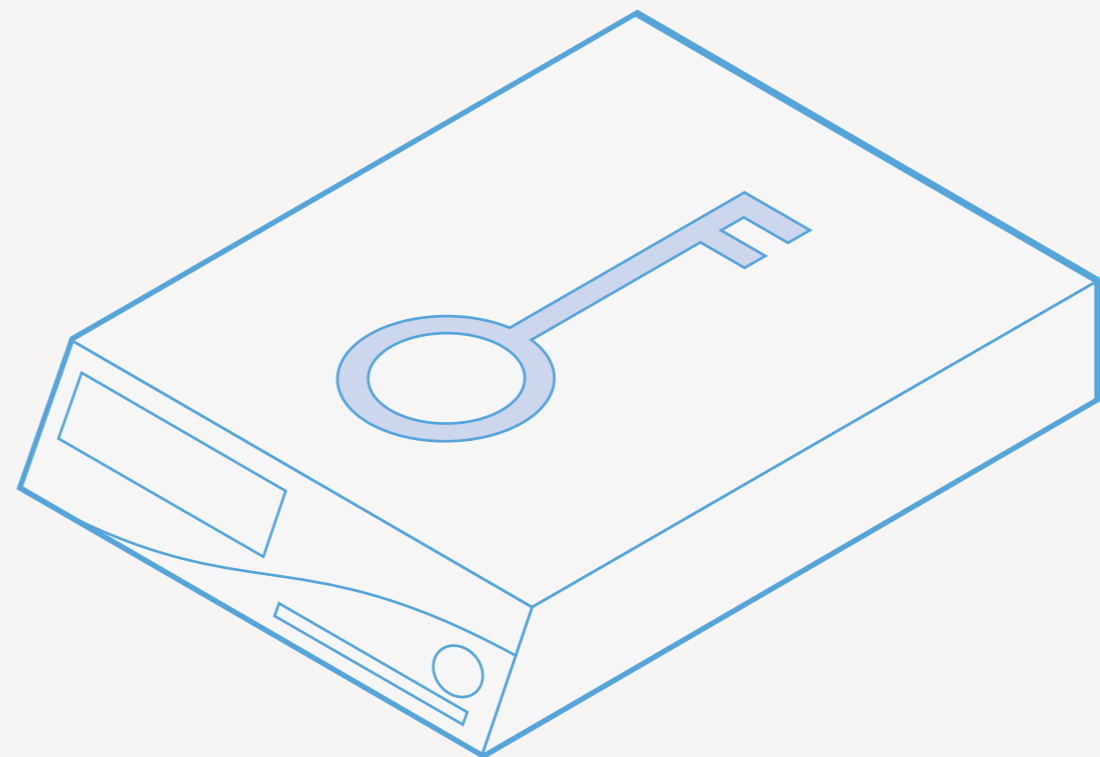
---

- 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

---

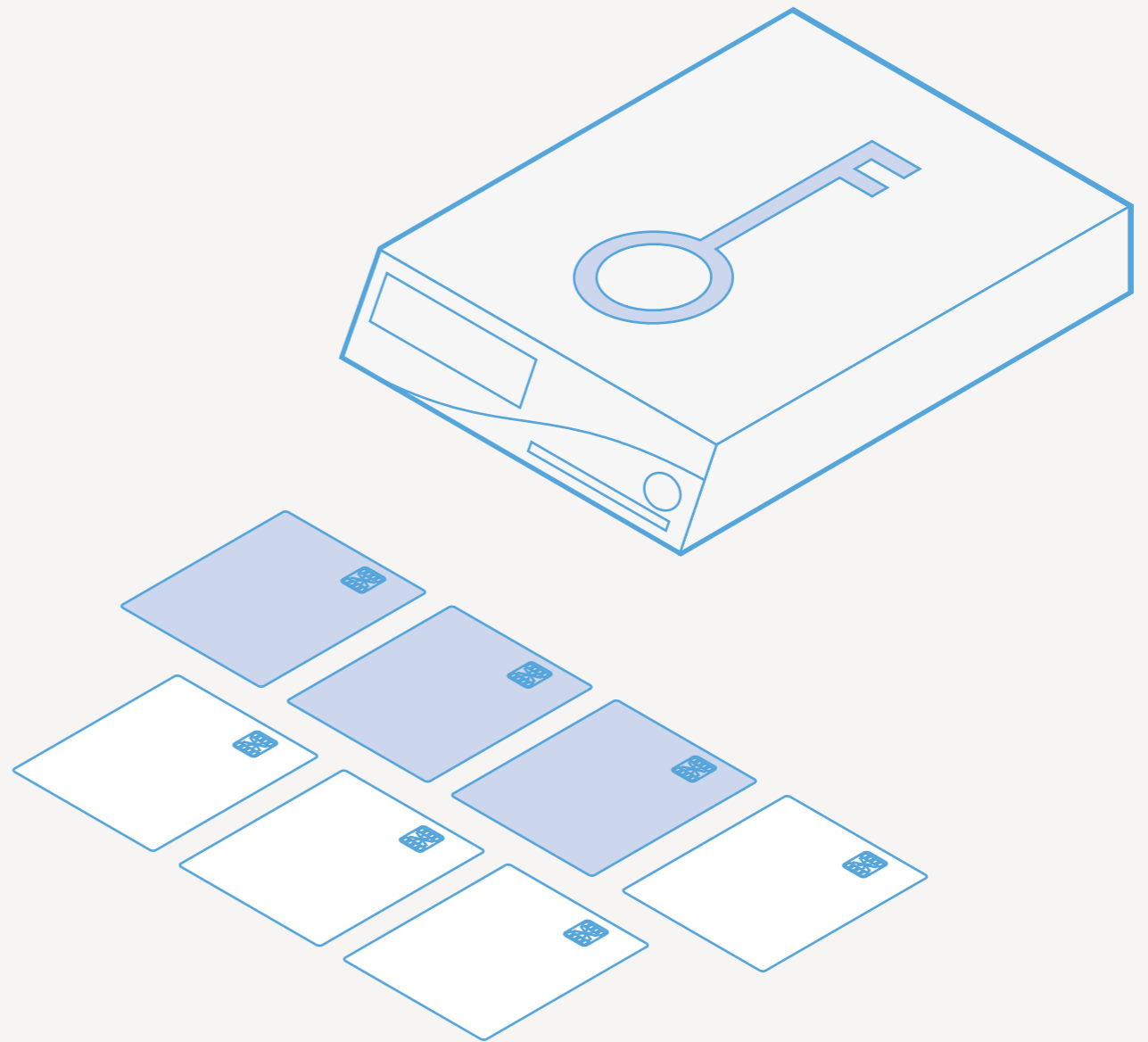
- The root KSK is stored in a device called a **hardware security module (HSM)** whose sole purpose is to securely store cryptographic keys. The device is designed to be tamper-proof. If there is an attempt to open it, the contents will self-destruct.



# Overview of KSK security

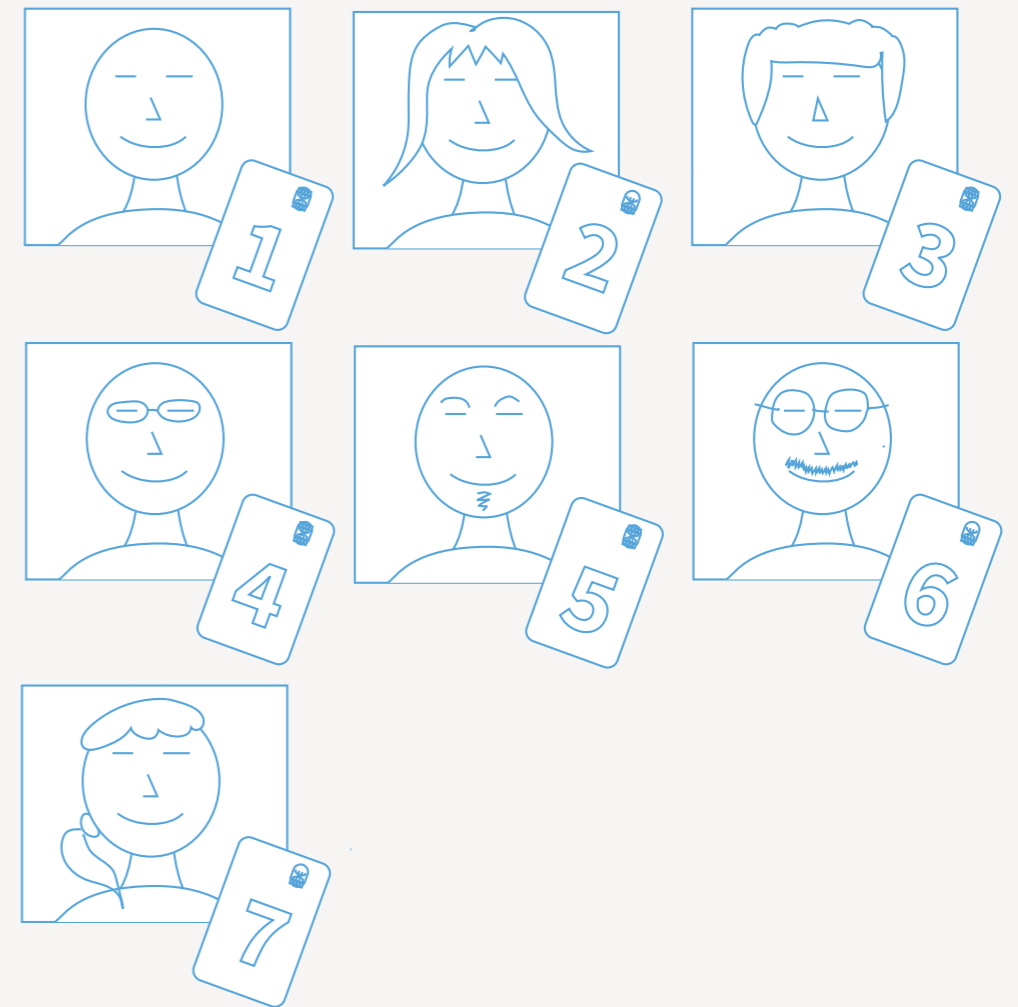
---

- 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

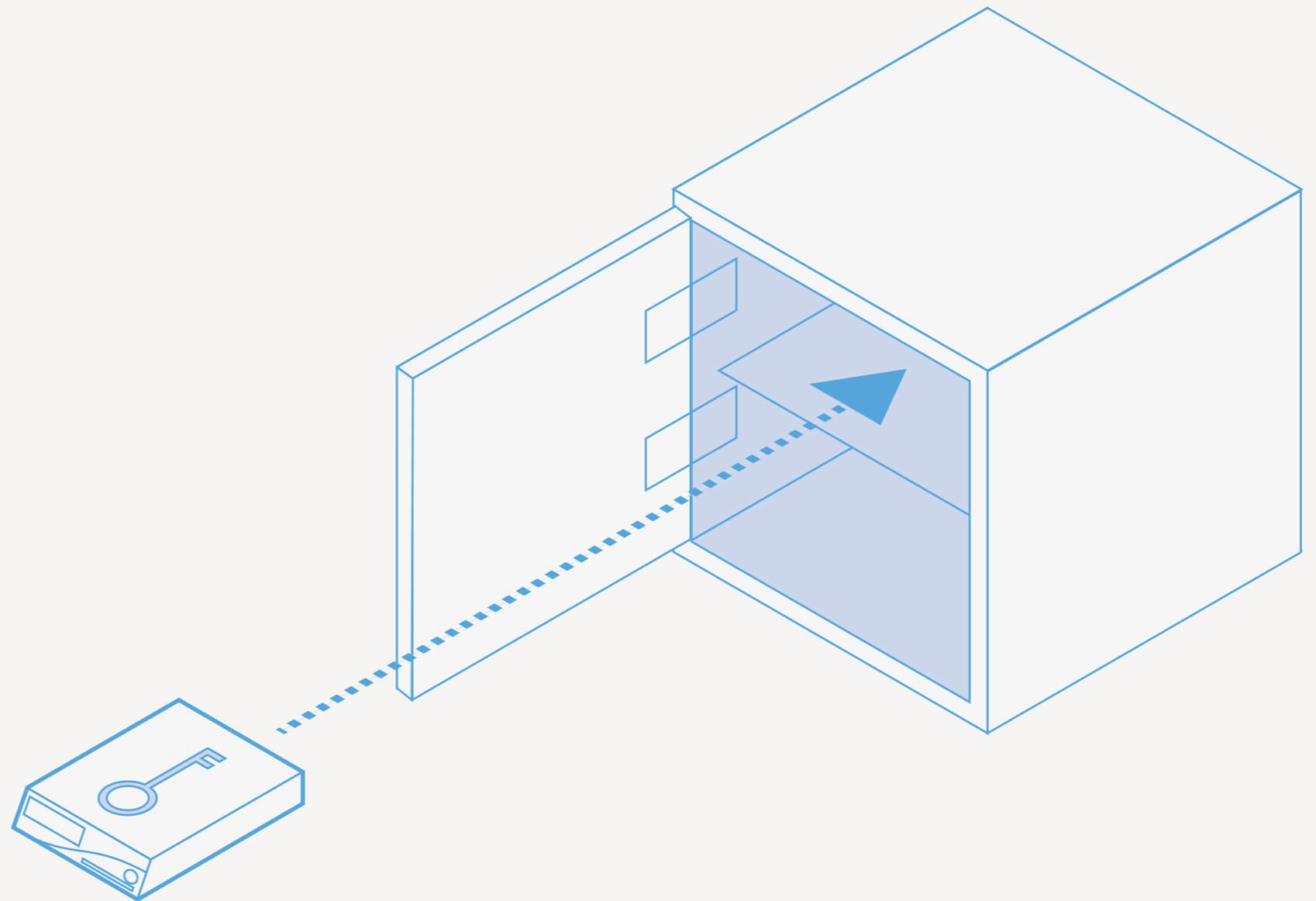
- Each smart card is assigned to a different ICANN community member, known as a trusted community representative. To access the key signing key, therefore, at least three of these TCRs need to be present\*.



# Overview of KSK security

---

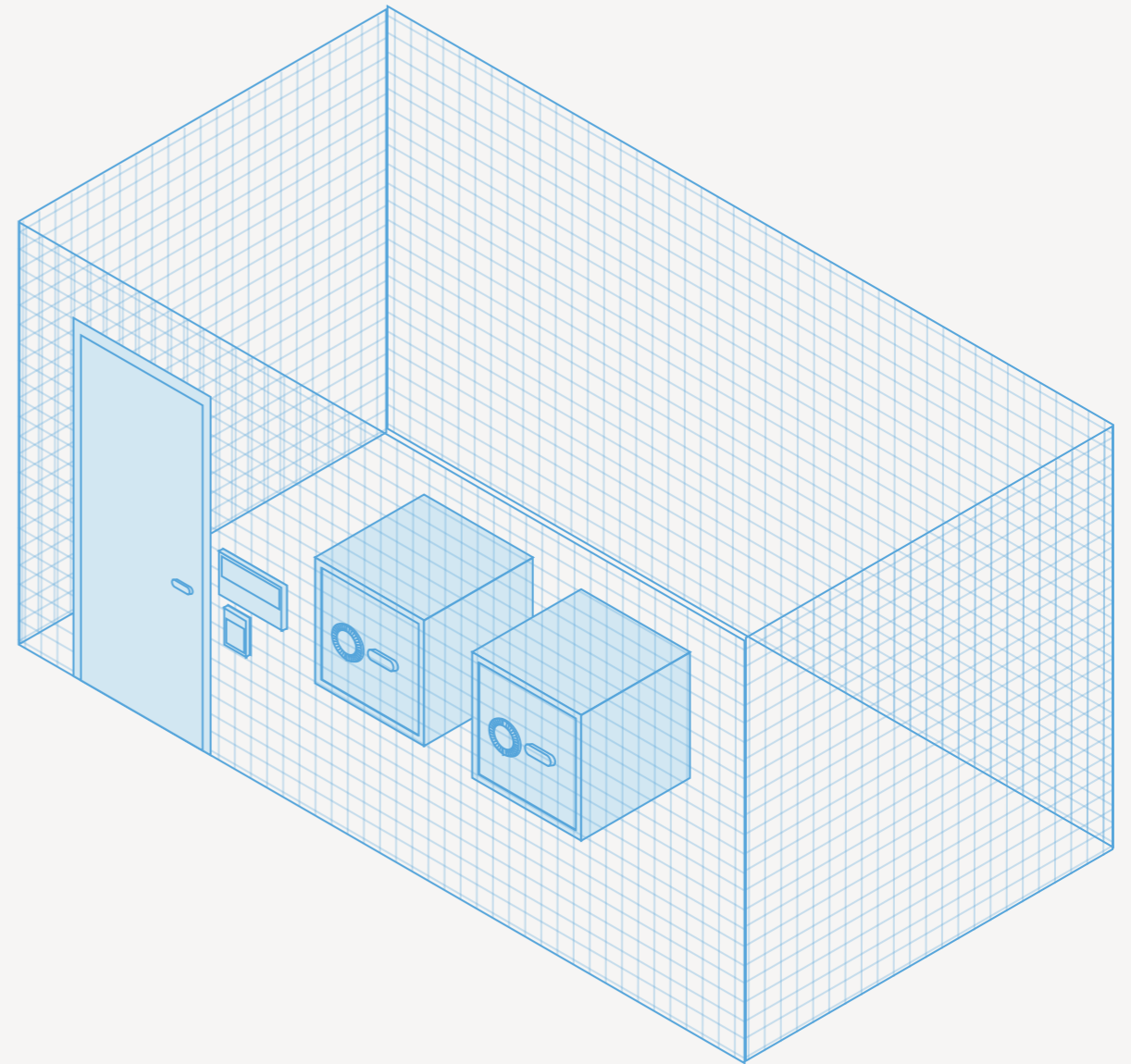
- The HSM is stored inside a high-security safe, which can only be opened by a designated person, the **safe security controller**. The safe is monitored with seismic and other sensors.



# 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.

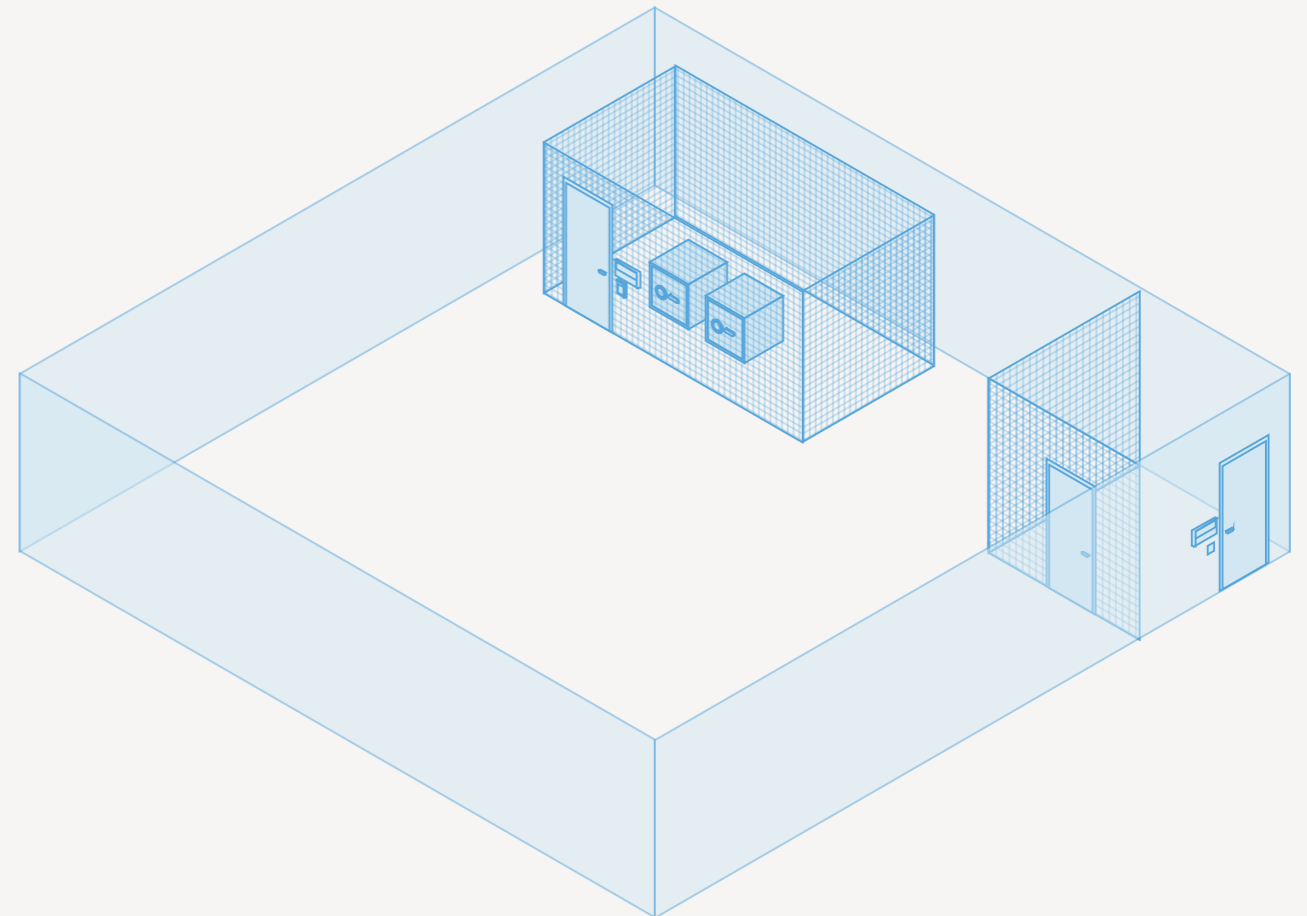




# Overview of KSK security

---

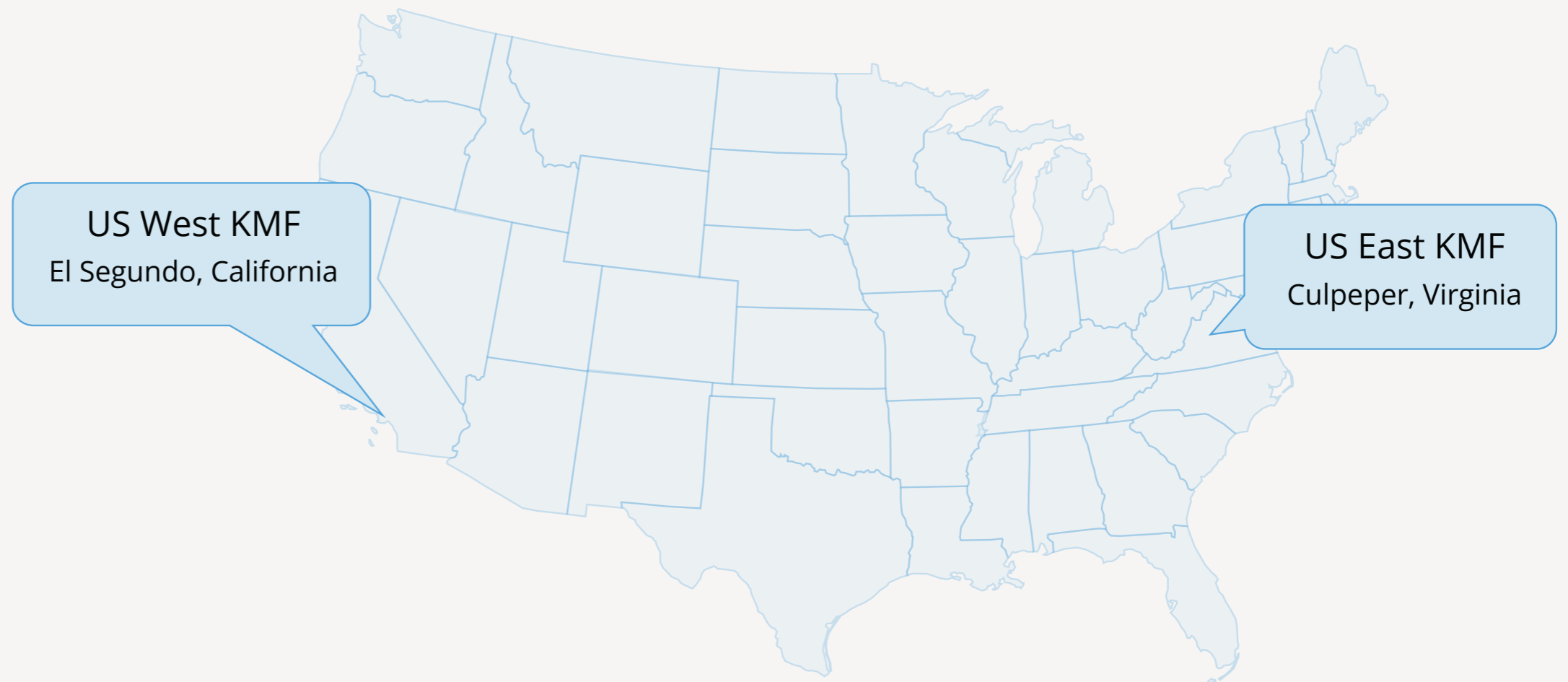
- The safe room is located within a larger room where ceremonies are performed involving the TCRs and other persons. Ceremonies are recorded on video, witnessed by the participants and others, and audited by a third-party audit firm. Access to the room needs to be granted by another designed person, 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 coasts.



# 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.

Act 1: Initiate Ceremony and Retrieve Materials

### Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
15	CA and IW transport a cart, and escort SSC1 to Tier 5 (Safe Room.)		
16	SSC1 opens Safe #1 while shielding the combination from the camera. <i>Note: SSC will begin by rapidly spinning the dial counter-clockwise in order to charge it.</i>		
17	Perform the following steps to complete the safe log: a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC1. c) SSC1 writes the date and time, then signs the safe log where "Open Safe" is indicated. d) IW verifies the entry then initials it.		

### Remove Equipment from Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
18	CA performs the following steps to extract each piece of equipment from the safe: a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera. c) Place each equipment TEB on the cart as specified on the list below. d) Write the date, time, and signature on the safe log where "Remove" is indicated. e) IW verifies the safe log entry, then initials it.  HSM3: TEB # BB51184512 (Place on Cart) HSM4: TEB # BB51184513 (Place on Cart) HSM5W: TEB # BB51184514 (Check and Return)  Laptop3: TEB # BB81420125 (Check and Return) Laptop4: TEB # BB81420103 (Place on Cart)  OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584386 (Place on Cart)  KSK-2017: TEB # BB46584387 (Check and Return)  HSM3 Physical Keyboard Key: TEB # BB21907221 (Place on Cart)		

### Close Safe #1 (Tier 6, Equipment Safe) Exit Tier 5 (Safe Room)

Step	Activity	Initials	Time
19	SSC1 writes the date and time, then signs the safe log where Close Safe is indicated. IW verifies the safe log entry then initials it.		
20	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.		
21	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).		

Root DNSSEC KSK Ceremony 40 Page 8 of 38

Act 3: Activate HSM (Tier 7) and Generate Signatures

### Verify the KSR Hash for KSR 2020 Q2

Step	Activity	Initials	Time
8	When the hash of the KSR is displayed on the terminal window, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves in front of the room and provide documents for IW to review off camera for the purpose of authentication. b) IW retains the hash and PGP word list for KSR 2020 Q2, and employment verification letter provided by the RZM representative and writes their name on the following line:  _____		
9	c) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used.		
9	Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks "are there any objections?"		
10	CA enters "y" in response to "Is this correct (y/N)?" to complete the KSR signing operation. The SKR is located in: <code>/media/KSR/KSR40/skr-root-2020-q2-0.xml</code>		

### Print Copies of the KSR Signer log

Step	Activity	Initials	Time
11	CA executes the commands below using the terminal window to print the KSR Signer log: a) <code>lpadmin -p HP -o copies-default=X</code> <i>Note: Replace "X" with the amount of copies needed for the participants.</i> b) <code>printlog<sup>[8]</sup> krsigner-202002*.log</code>		
12	IW attaches a copy of the required krsigner log to their script.		

### Back up the Newly Created SKR

Step	Activity	Initials	Time
13	CA executes the following commands using the terminal window: a) List the contents of the KSR FD by executing: <code>ls -ltrR /media/KSR</code> b) Copy the contents of the KSR FD to the HSMFD by executing: <code>cp -pR /media/KSR/*</code> <i>Note: Confirm overwrite by entering "y" if prompted.</i> c) List the contents of the HSMFD to verify it has been copied successfully by executing: <code>ls -ltrR</code> d) Unmount the KSR FD by executing: <code>umount /media/KSR</code>		
14	CA removes the KSR FD containing the SKR files, then gives it to the RZM representative.		

Root DNSSEC KSK Ceremony 40 Page 15 of 38

Act 4: Zeroize and Dismantle Hardware Security Module

### Remove Cryptographic Module and Card Reader from HSM3

Step	Activity	Initials	Time
15	CA performs the following steps to remove the cryptographic module: a) Using <b>Tool A+Bit 4</b> , remove the 4 nuts which secure the cryptographic module to the case. b) Lift the cryptographic module up to separate it from the case. c) Using <b>Tool C</b> , remove both connectors from the cryptographic module as flush with the case as possible. d) Place the cryptographic module in the <b>Critical Parts</b> bin, and the connectors in the <b>HSM Parts</b> bin on the ceremony table.		
16	CA performs the following steps to remove the front panel and card reader: a) Using <b>Tool A+Bit 4</b> , remove the 4 nuts which secure the front panel to the bottom of the case. b) Place the front panel in the <b>HSM Parts</b> bin on the ceremony table. c) Using <b>Tool A+Bit 4</b> , remove the nut which secures the card reader. d) Using <b>Tool A+Bit 3</b> , remove the 3 screws which secure the card reader. e) Lift the card reader up to separate it from the case and place it with the ribbon cable in the <b>Critical Parts</b> bin on the ceremony table. f) Place the HSM case in the <b>HSM Parts</b> bin on the ceremony table.		

### Place the Critical HSM3 parts into a TEB

Step	Activity	Initials	Time
17	CA places the container with the following critical parts into a prepared TEB, then seals it. a) Cryptographic Module b) Logic Board c) Card Reader  <i>Note: The HSM case will not be destroyed.</i>		
18	CA performs the following steps: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Give RKOS the TEB for destruction.  HSM3: TEB # BB81420112		

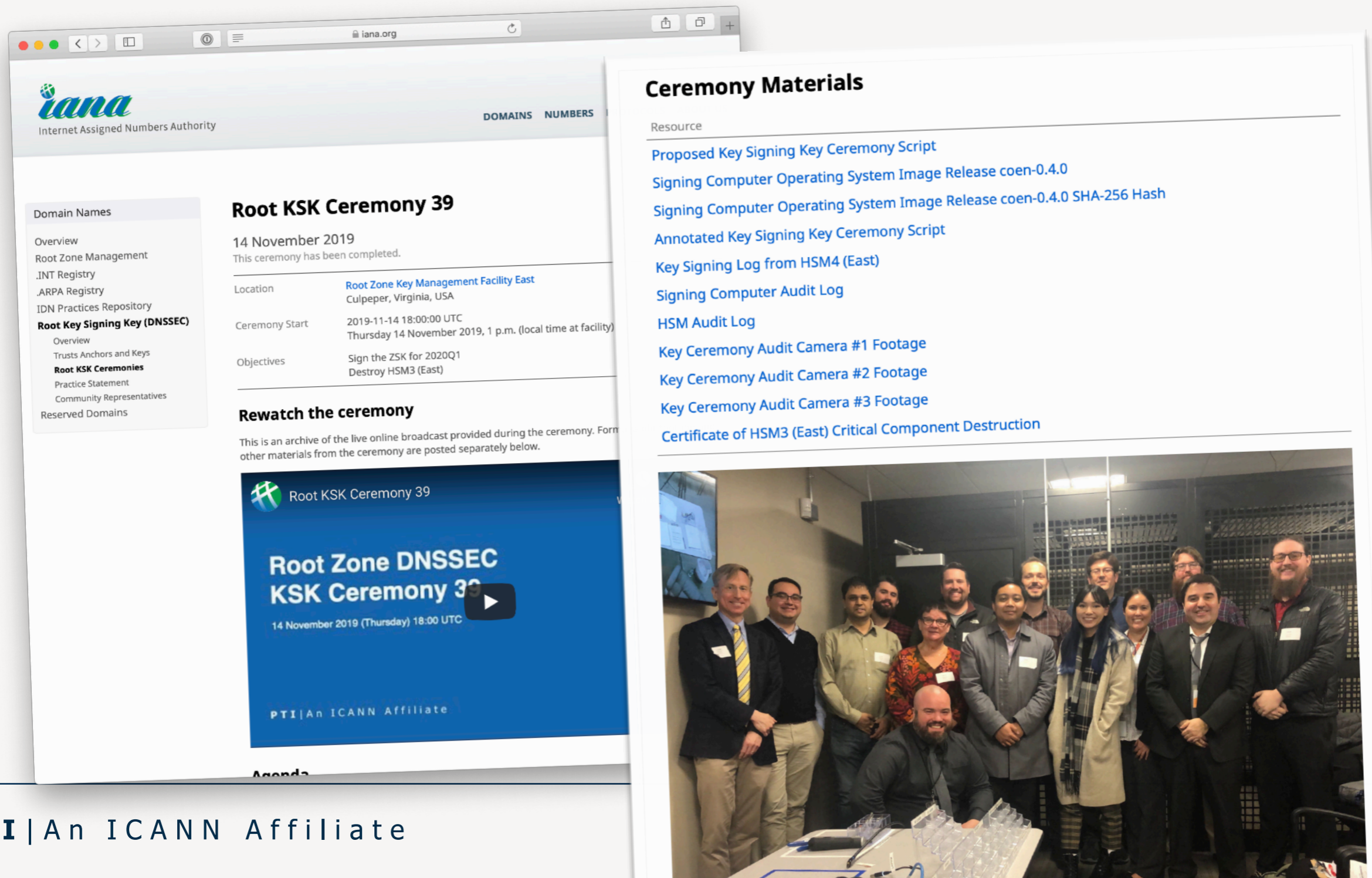
### Retire HSM Physical Keyboard Key

Step	Activity	Initials	Time
19	CA performs the following steps to retire the listed HSM Physical Keyboard Key: a) Remove the TEB from the cart. b) Inspect TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB. e) RKOS will take possession of the HSM Physical Keyboard Key and place in its designated area.  HSM3 Physical Keyboard Key: TEB # BB21907221 Last Verified: AT22 2015-07-20		

Root DNSSEC KSK Ceremony 40 Page 23 of 38

# Ceremony artefacts

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



The image shows a screenshot of the IANA website. The main content area displays information for the "Root KSK Ceremony 39" held on 14 November 2019. It includes details about the location (Root Zone Key Management Facility East, Culpeper, Virginia, USA), the start time (2019-11-14 18:00:00 UTC), and the objectives (Sign the ZSK for 2020Q1, Destroy HSM3 (East)). A "Rewatch the ceremony" section provides an archive of the live online broadcast. Below this is a video player thumbnail for the ceremony, featuring the PTI logo and the text "Root Zone DNSSEC KSK Ceremony 39" and "14 November 2019 (Thursday) 18:00 UTC".

On the right side of the screenshot, there is a "Ceremony Materials" section listing various resources:

- [Proposed Key Signing Key Ceremony Script](#)
- [Signing Computer Operating System Image Release coen-0.4.0](#)
- [Signing Computer Operating System Image Release coen-0.4.0 SHA-256 Hash](#)
- [Annotated Key Signing Key Ceremony Script](#)
- [Key Signing Log from HSM4 \(East\)](#)
- [Signing Computer Audit Log](#)
- [HSM Audit Log](#)
- [Key Ceremony Audit Camera #1 Footage](#)
- [Key Ceremony Audit Camera #2 Footage](#)
- [Key Ceremony Audit Camera #3 Footage](#)
- [Certificate of HSM3 \(East\) Critical Component Destruction](#)

At the bottom right of the screenshot is a group photograph of approximately 15 people, including men and women in business attire, standing in a room with server racks in the background.

# 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.
- <https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en>
- 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

# Key Ceremony 40

---

- 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](mailto:kim.davies@iana.org)**