Root KSK Management in 2020

Kim Davies
VP, IANA Services, ICANN; President, PTI

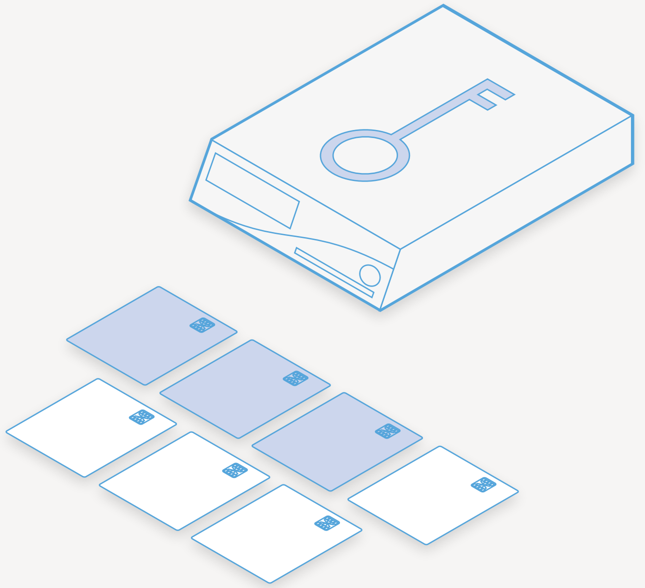
22 June 2020

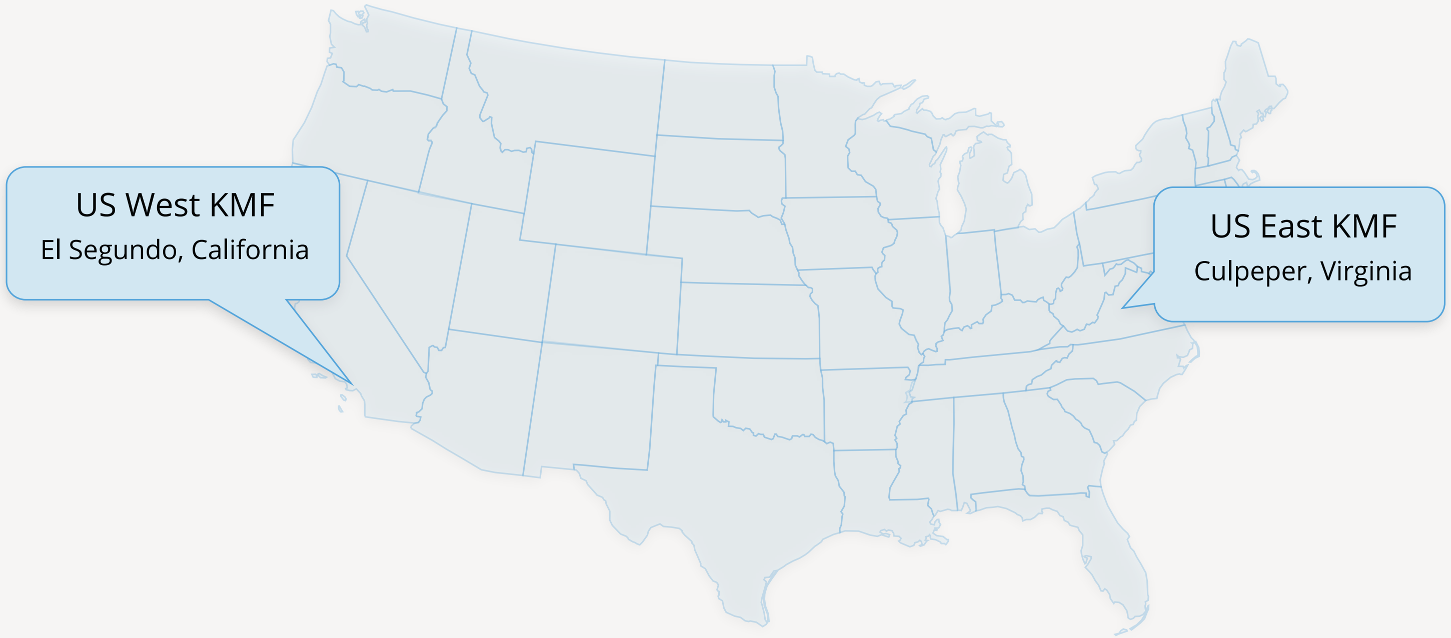
Our agenda

- An overview of normal KSK ceremony operations
- A review of the challenges we’ve faced this year
- The future

A quick primer

- The Root Zone KSK is administered as part of the IANA functions, and serves as the trust anchor for DNSSEC.
- Changing the KSK, a “rollover”, is uniquely complex as it requires updating the trust anchor configuration in validating resolvers globally.
- The KSK is kept safe in two geographically distinct secured facilities
- Secure storage (HSMs) activated through an m-of-n scheme involving trusted community representatives from around the world





US West KMF
El Segundo, California

US East KMF
Culpeper, Virginia

Some security objectives of this design

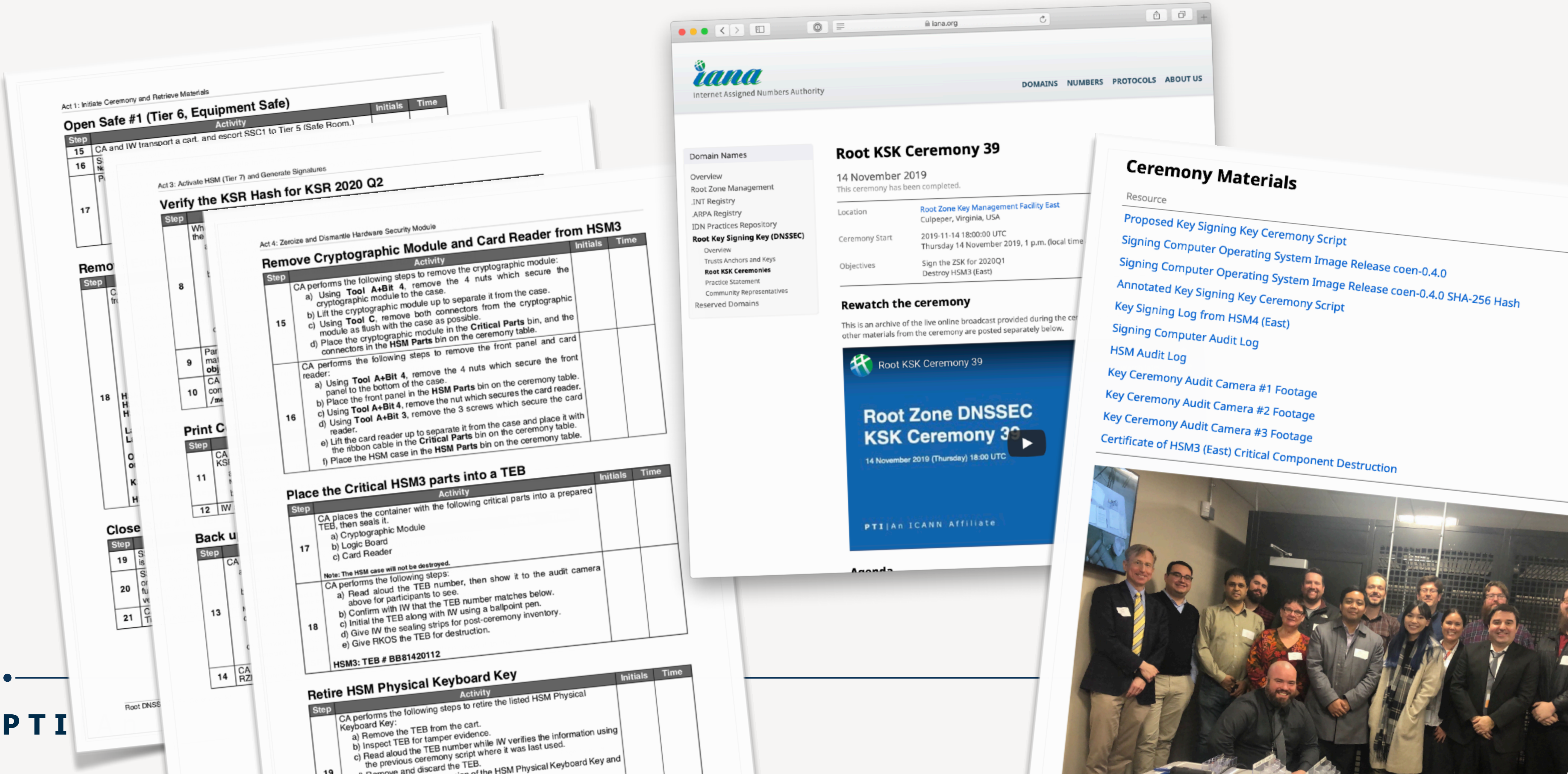
- **Overlapping layers of security**
  - If any one layer of protection is inadequate, the many layers of protection ensure the safety of the KSK
- **Protect the chain of custody**
  - Sensitive materials are guarded their entire life through tamper evident enclosures, and strict management each time they are used
- **Minimize collusion risk**
  - Many different personnel need to coordinate, including non staff members, to successfully conduct a ceremony
- **Redundancy to ensure successful operations**
  - Duplicate locations, duplicate HSMs, recovery options
- **Guard against surreptitious entry**
  - While any unauthorized access is not desirable, undetected access is what we are primarily designing against
  - If we detect unauthorized access, we can replace the KSK
- **Open design**
  - All software and associated materials is open source and published

Key signing ceremonies

- Authorized use of the KSK is managed through planned events known as **key signing ceremonies**
- Approximately four times a year, the TCRs and others meet to use the HSMs to sign keys to be used for the root zone.
- Ceremonies convene a quorum of participants needed to activate the KSK in its secure enclosure, with sufficient controls to satisfy observers it is being used in a legitimate way and there is no risk of inadvertent use.
- The ceremony is conducted in a highly transparent manner, with the opportunity for interjection if anyone is concerned.
- The purpose is to ensure **trust in the process**. DNSSEC only provides security if the community is confident the KSK has not been compromised.

Key signing ceremonies

- Each ceremony is orchestrated using a comprehensive script that identifies each individual step that needs to be undertaken.
- The process is streamed and recorded, with external witnesses watching every step. All materials (videos, code, scripts, etc.) are posted online.



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.)		

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

Verify the KSR Hash for KSR 2020 Q2

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 **Tool A+Bit 4**, 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 **Tool C**, remove both connectors from the cryptographic module as flush with the case as possible. d) Place the cryptographic module in the **Critical Parts** bin, and the connectors in the **HSM Parts** bin on the ceremony table.		
16	CA performs the following steps to remove the front panel and card reader: a) Using **Tool A+Bit 4**, remove the 4 nuts which secure the front panel to the bottom of the case. b) Place the front panel in the **HSM Parts** bin on the ceremony table. c) Using **Tool A+Bit 4**, remove the nut which secures the card reader. d) Using **Tool A+Bit 3**, 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 **Critical Parts** bin on the ceremony table. f) Place the HSM case in the **HSM Parts** 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 **Note: The HSM case will not be destroyed.**		
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. … of the HSM Physical Keyboard Key and		

Root KSK Ceremony 39

14 November 2019

This ceremony has been completed.

Location	Root Zone Key Management Facility East Culpeper, Virginia, USA
Ceremony Start	2019-11-14 18:00:00 UTC Thursday 14 November 2019, 1 p.m. (local time
Objectives	Sign the ZSK for 2020Q1 Destroy HSM3 (East)

Rewatch the ceremony

This is an archive of the live online broadcast provided during the ce other materials from the ceremony are posted separately below.

Ceremony Materials

Resource

- 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

A good ceremony

- Fundamental objectives need to be performed with no improper disclosure of sensitive materials, and meeting all security controls and passing our control audit.
- There can be deviations from the script, called “exceptions”, so long as it is properly witnessed and accounted for
  - Most issues can be solved on the fly with no loss of confidence in the system and with ceremony objectives accomplished
  - Redundant design of the ceremony allows multiple ways to accomplish objective in the live ceremony context
- Ultimately, we need to retain ongoing community trust in how they are conducted.

Bigger problems

- In 10 years of ceremony operations we’ve been able to recover every issue on the day of the ceremony without any challenges.
  - We’ve always held the following day as a ‘standby day’, but never had to use it
- However, 2020 has been a unique year.

KSK Ceremony 40

February 2020

Key Ceremony 40

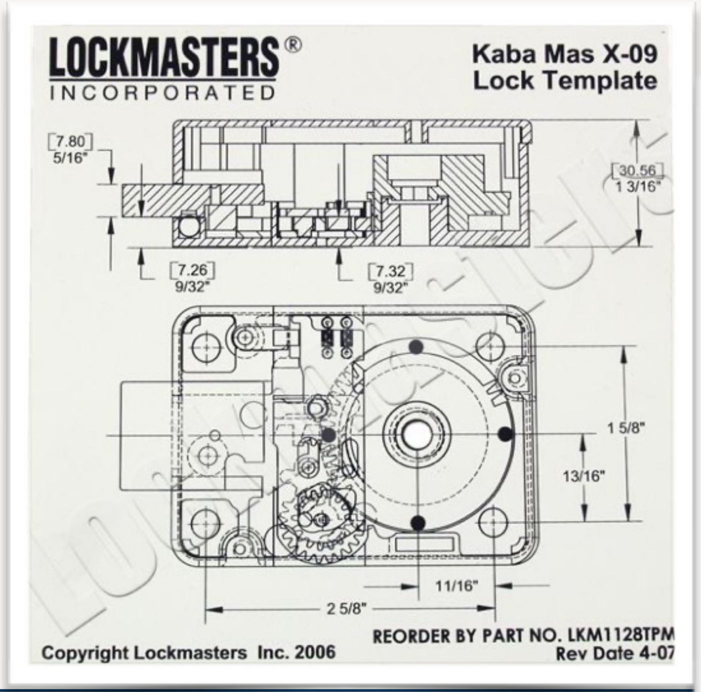
- Scheduled for 12 February 2020, objective to sign key material for April-June 2020, and decommission an old HSM
- Pre-ceremony activity included maintenance work to upgrade the lock assemblies within the safe
  - These are performed in administrative ceremonies that are audited to the same standard as the key signing ceremonies, but do not involve HSM activation
  - 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.

Key Ceremony 40

- 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



Considerations in the fog of war

- Did the SSC forget the combination or fumble the mechanism?
  - Not unprecedented, the mechanism is tricky
  - Locks are designed with exponential backoff style behavior
- What is broken?
  - Can’t see in the safe. Hypothesizing failure modes, safe construction
- How do we not break it more?
  - Both the lock and safe have tamper resistant features
- Stamina
  - A small group of people in a windowless room may lose their collegiality.
  - The locksmith is doing hard physical labour. Will he hold out?
- Maintaining quorum
  - Can we do all the necessary work before TCRs had to fly away, to reconvene at an undetermined time?

Some takeaways

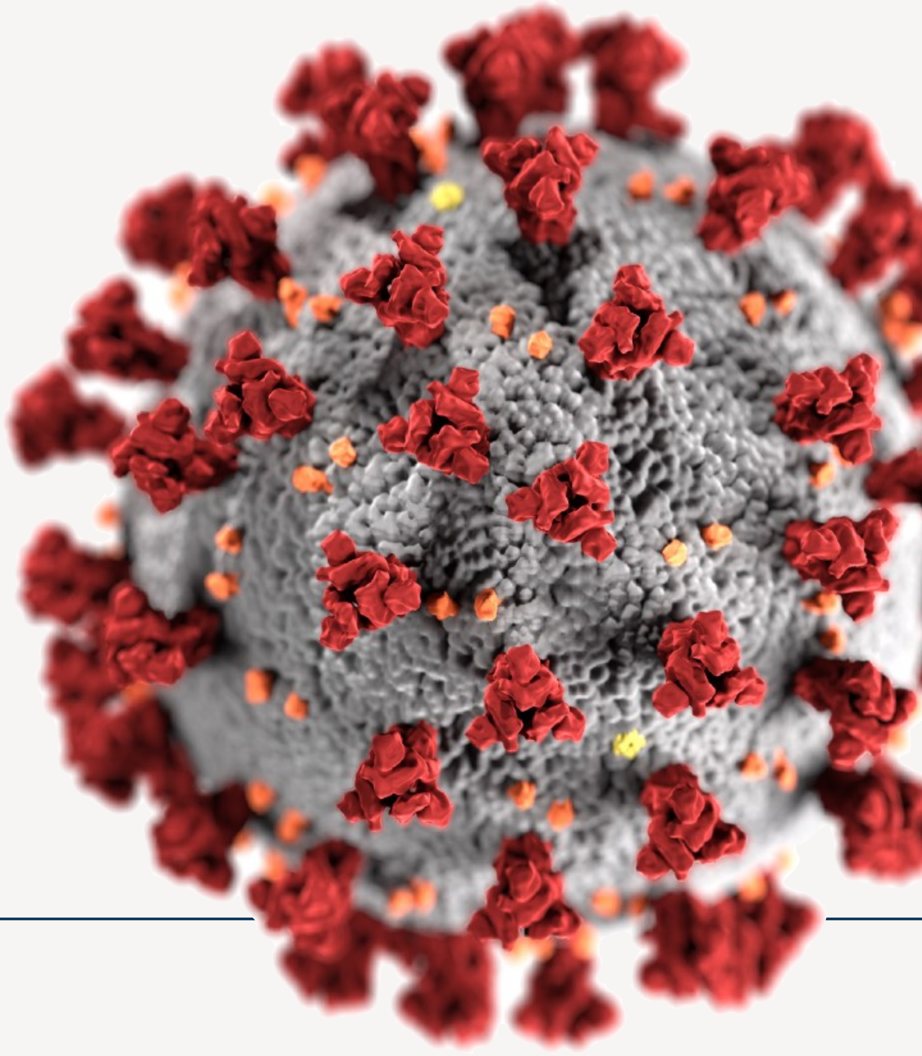
- Ceremony was successfully conducted with a 4 day delay
- Gained valuable experience that will inform our future plans for disaster recovery
- Community volunteers and staff alike supported us around the clock to bring the issue to conclusion and perform key ceremony
- Some revisions to administrative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

KSK Ceremony 41

April 2020

Key Ceremony 41

- Schedule for 23 April 2020, planning to:
  - Sign the 2020Q3 key material (covering July-September 2020)
  - Induct a new HSM (part of our normal hardware refresh cycle)
  - Replace two Trusted Community Representatives
- The evolving Coronavirus situation caused us to focus on developing contingencies for this ceremony as the situation deteriorated
- Initial 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, had not been well defined.



Some thoughts that crossed our mind

- Can folks still attend?
  - Ability to fly increasingly encumbered. Will anyone get sick?
- Can we continue to access our facility?
  - Government restrictions, corporate restrictions
- Do we drill the safe deposit boxes if we can't get TCRs?
  - We have precedent — 2 resigning TCRs' boxes were drilled out in the past
- Will we be able to hold another ceremony 3 months later?
  - What if things get worse? Can staff self-isolate indefinitely?
- What if we can't hold a ceremony at all?
  - Do we revert the root zone to unsigned state as a last resort?
- Dispersal of roles around the world to avoid collusion risk is basically your worst enemy when recovering from this kind of threat.
- How do we retain the confidence of everyone?

Contingency ideas

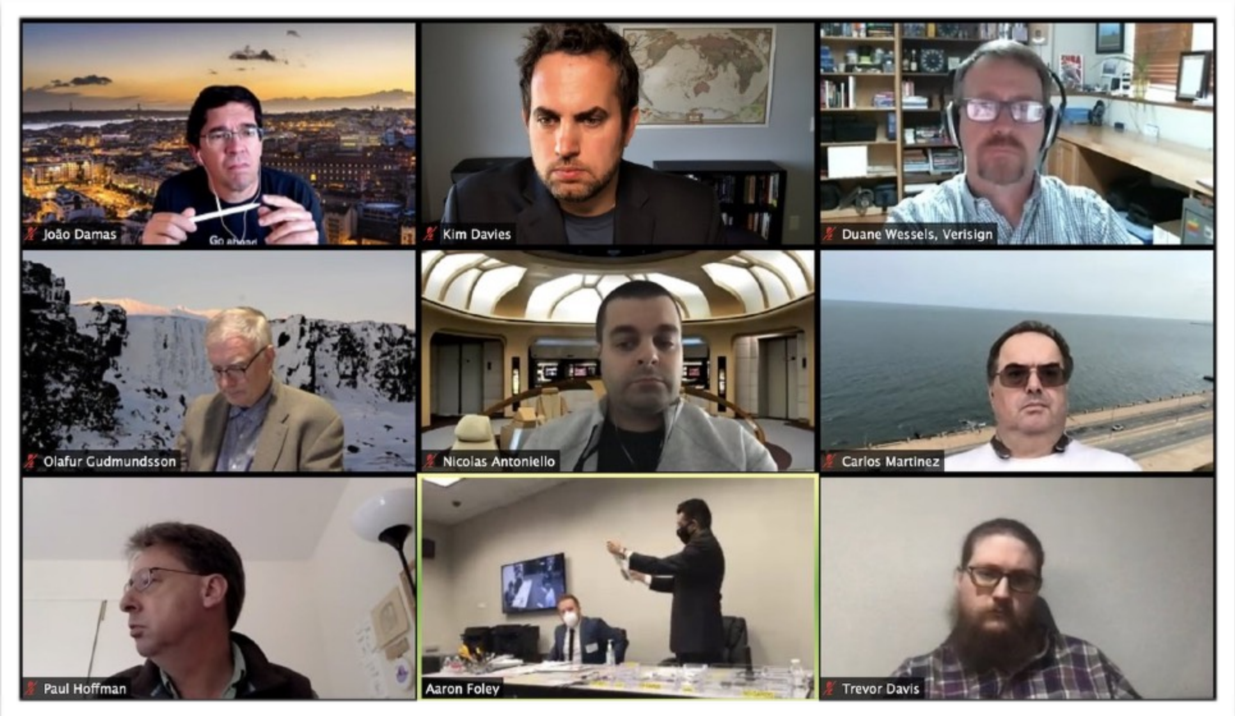
- Roughly in increasing order of severity:
  - Hold the ceremony with less than ideal number of people present
  - Advance the ceremony date
  - Postpone the ceremony date
  - Hold the ceremony in the alternative facility
  - Induct new TCRs to replace those unable to travel
  - Sign key material beyond 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.
- Graduated decision process
  - Triggering conditions mapped out in advance for contingency scenarios

What was decided

- Settled on an approach to perform the ceremony with minimum personnel, with TCRs participating remotely.
  - DPS revised to clarify roles and responsibility and provide flexibility for disaster recovery
  - Obtained ICANN Board and executive approval, community buy-in
  - Minimized the scope of the ceremony by eliminating non-essential acts
  - 4 of 7 TCRs transmitted their secure credentials to 4 surrogates in Los Angeles
- Hold the ceremony on the time and date scheduled
  - … but in El Segundo, not Culpeper as originally planned
- Sign nine months of key material instead of the typical three
  - Release signatures in 3 month increments as usual
  - Balance the risk of being unable to hold a ceremony versus the risks of generating long period of signatures. No need to hold a ceremony earlier than February 2021 as a result.

Holding the ceremony

- Minimized attendees in person to bare minimum — all PTI and ICANN staff
- Bolstered normal remote participation to make it active rather than passive
    - Those that would have had trusted roles in-ceremony had a private Zoom conference. Allowed TCRs and others to play comparable role remotely, ability to interject and so on
- High level of interest during the public live stream
- Ceremony was a success



The future

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 others in the field
- Customer satisfaction (e.g. annual surveys) consistently high
- Events of 2020 have challenged us with several worst-case scenarios
  - Tested our ability to be adaptive
  - Allowed us to exercise scenarios that had only been hypotheticals to date
  - Stretched us to maintain high community trust as we navigate through

Longer term thinking about the model

- Key Management Facility locations
  - Do they need to be rethought? Would alternate or additional locations provide greater outcomes?
    - More resilient against threats to two existing facilities
    - More facilities increases the attack surface
    - Facilities are expensive, both build-out and ongoing, and need to be staffed
    - Rotating through more facilities means each one lays at rest longer, more opportunity for surreptitious activity or decay in operational environment
- Global mobility and physical-based security
  - In a post-pandemic 21st century, is a model founded on distributing trust around the world physically still appropriate?
  - Should we rely more on logical sharing of essential elements? Do fundamental aspects need a redesign?

Longer term thinking about the model

- Standby key
  - Do we generate and pre-populate an alternate trust anchor that can be put into action if needed via different mechanisms?
  - Benefits for recovery from force majeure events requires the standby key to avoid fate sharing with the production key
    - Store it via alternate mechanisms/different facilities to production key
    - How to secure it to a satisfactory level?
    - If it is scaled down, how do we perform ceremony operations?

Longer term thinking about the model

- KSK rollover consultation
  - As these issues were breaking, we were conducting a public consultation on future mechanisms for KSK rollovers, following the success of the first rollover in 2018.
  - These events provide new perspectives and stress tests to consider in future planning
  - Consciously paused work on evaluating feedback to focus operations around these two ceremonies. With that work completed, now refocusing efforts on long-term planning for KSK management.

Longer term thinking about the model

- Targeted outcomes in the draft PTI strategic plan for 2020-2024
  - “Adaptive to evolving requirements concerning the security of critical key materials (e.g. the Root Zone KSK), including evaluation of changes to cryptographic algorithms, reconfiguration of the secure facilities, and the role of recovery key shares as a viable disaster recovery method.”
  - “Policies and procedures are adapted to ensure successful engagement and future operations despite long-term limits on travel due to the COVID-19 pandemic and other similar events.“

Constant improvement is part of the DNA

- Constant renewal
  - Most aspects of the facility and ceremony procedures have been refined
  - Replacement cycle for most hardware in use
  - Debrief at the end of each ceremony with participants identifies areas for future improvement
- High transparency
  - As distinct from likeminded operations, we seek radical transparency to shine light on the process, as messy as it may be
  - New participants are always welcome through remote participation, guest witnesses, TCR renewal, etc. New perspective hones our approach.

Thank you!

kim.davies@iana.org