Managing the trust anchor of the DNS against adversity

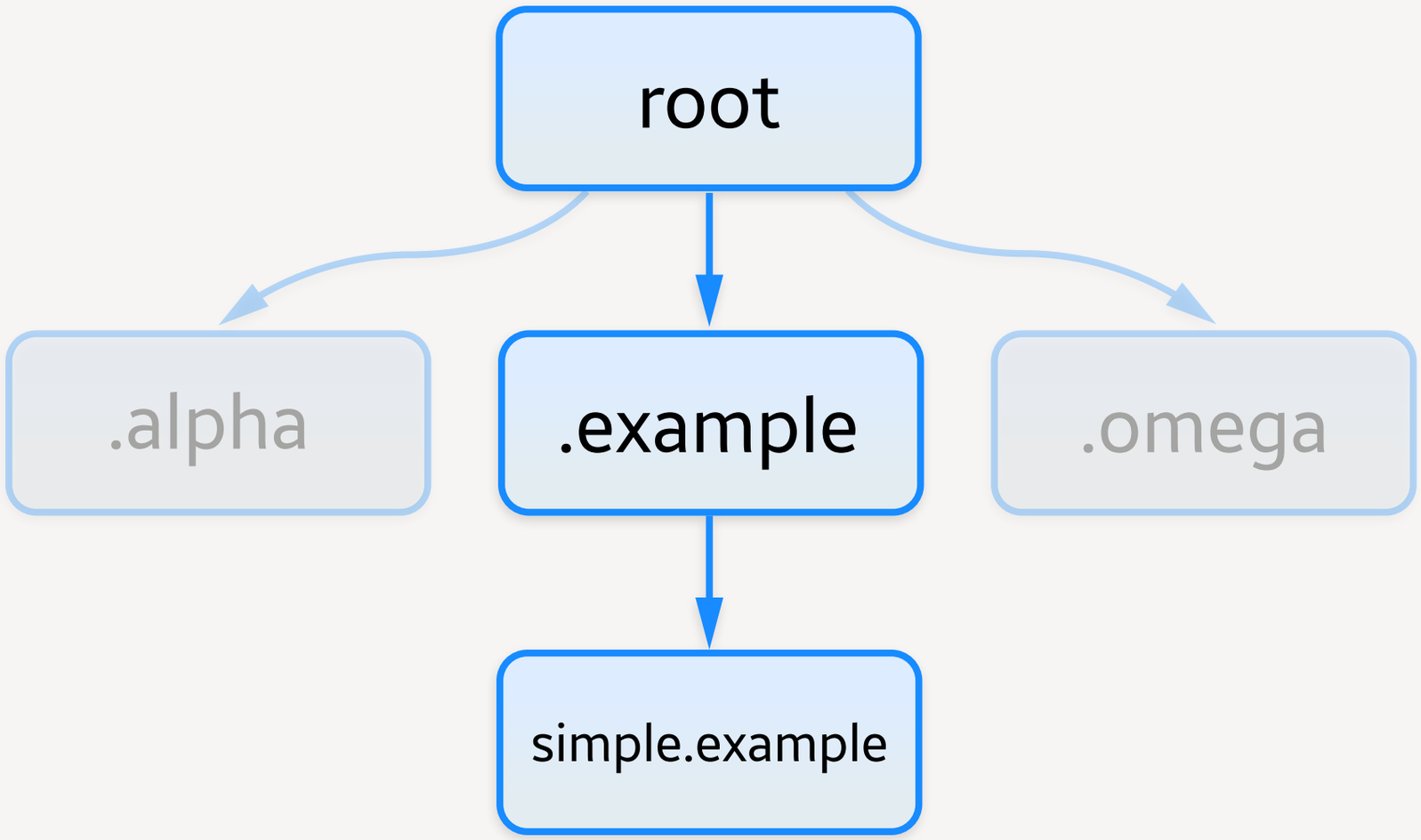
Kim Davies
VP, IANA Services, ICANN; President, PTI

15 April 2020

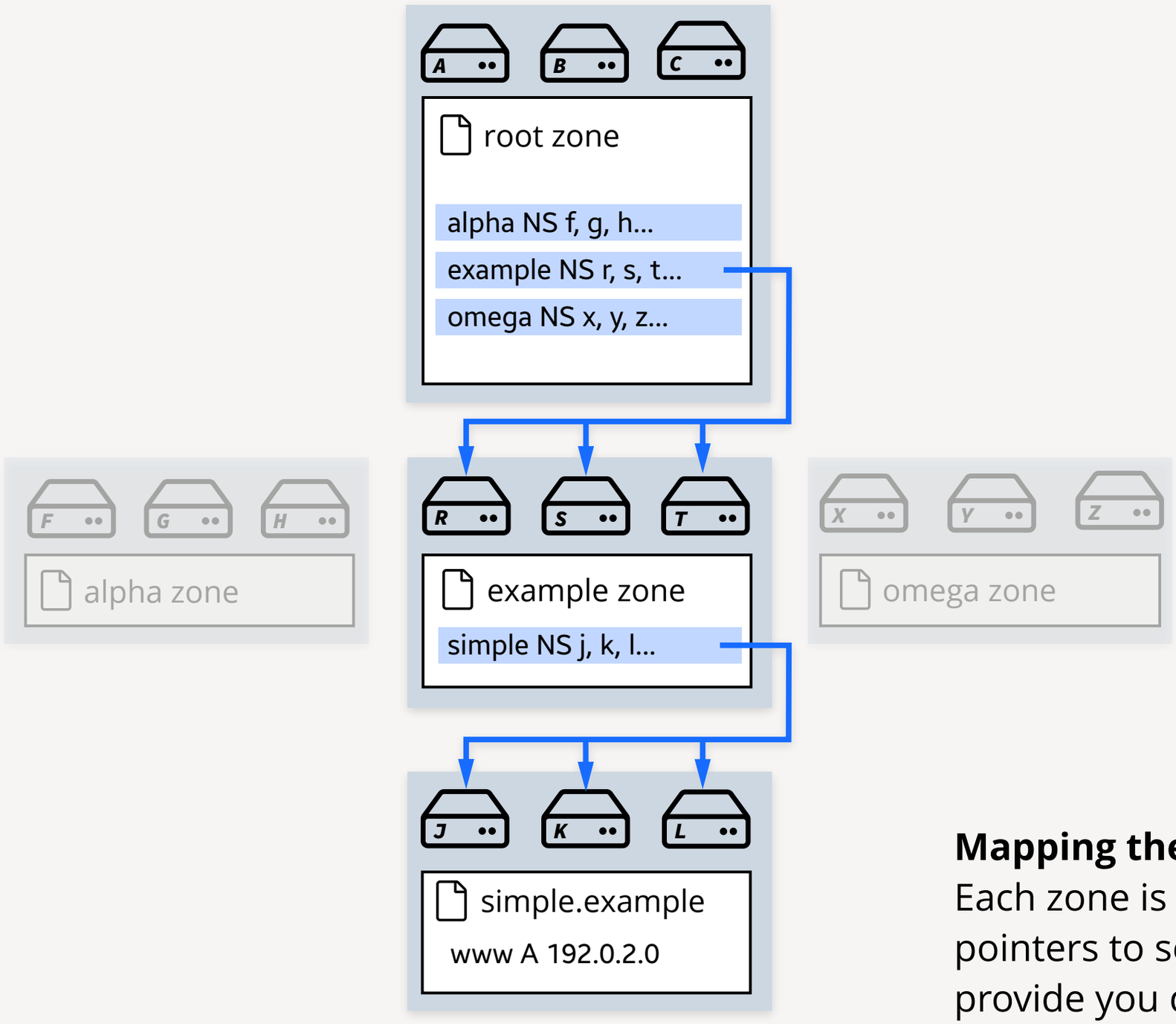
PTI | An ICANN Affiliate

Our agenda

- Introducing the concepts
  - The role of cryptographic keys in securing the DNS
  - How we safely store and use the trust anchor
- An overview of normal operations
- A review of the challenges we've faced
- The future

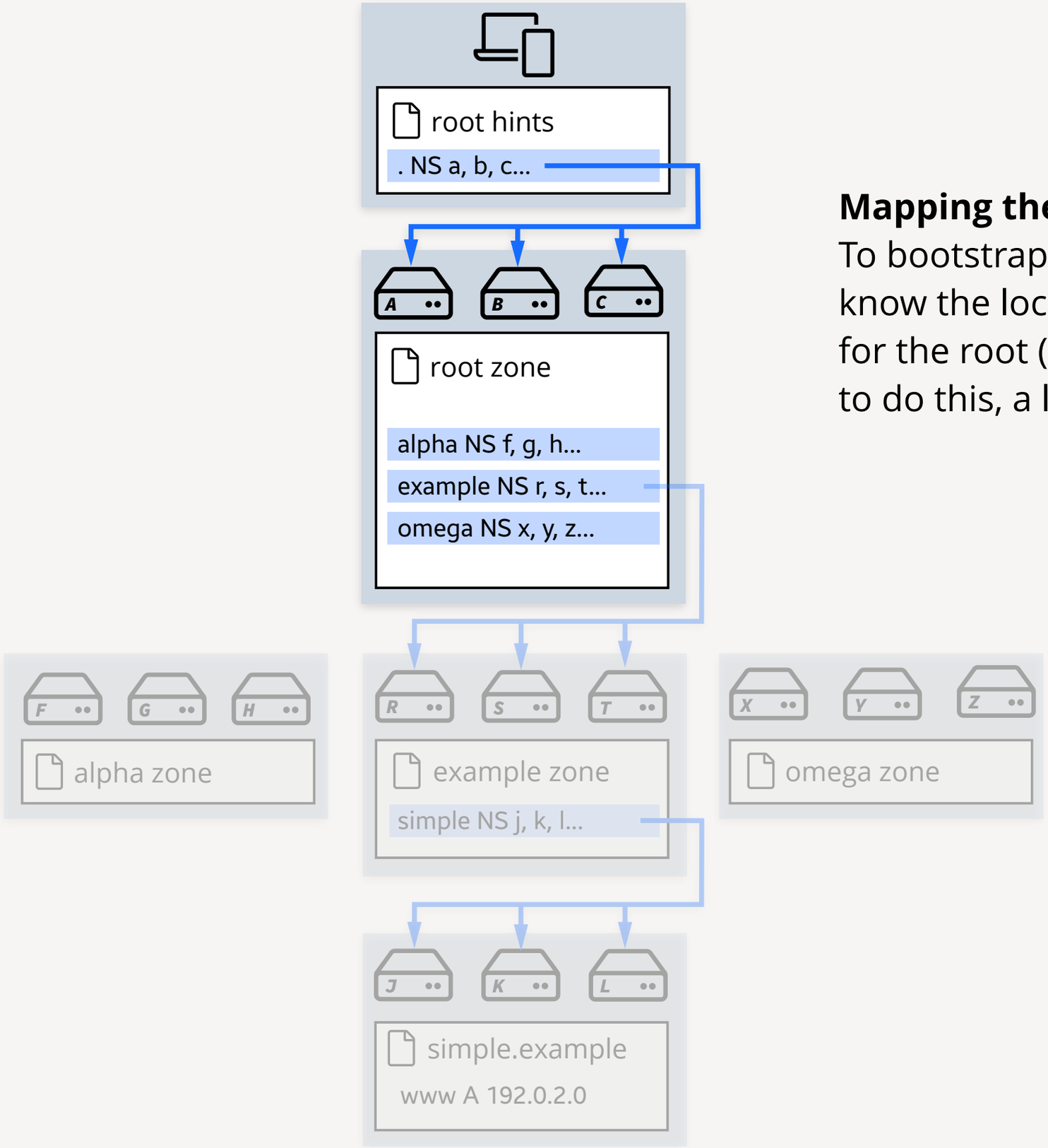


The DNS as a logical hierarchy
To find “simple.example”, you traverse from the root zone to the “example” zone to the “simple.example” zone.



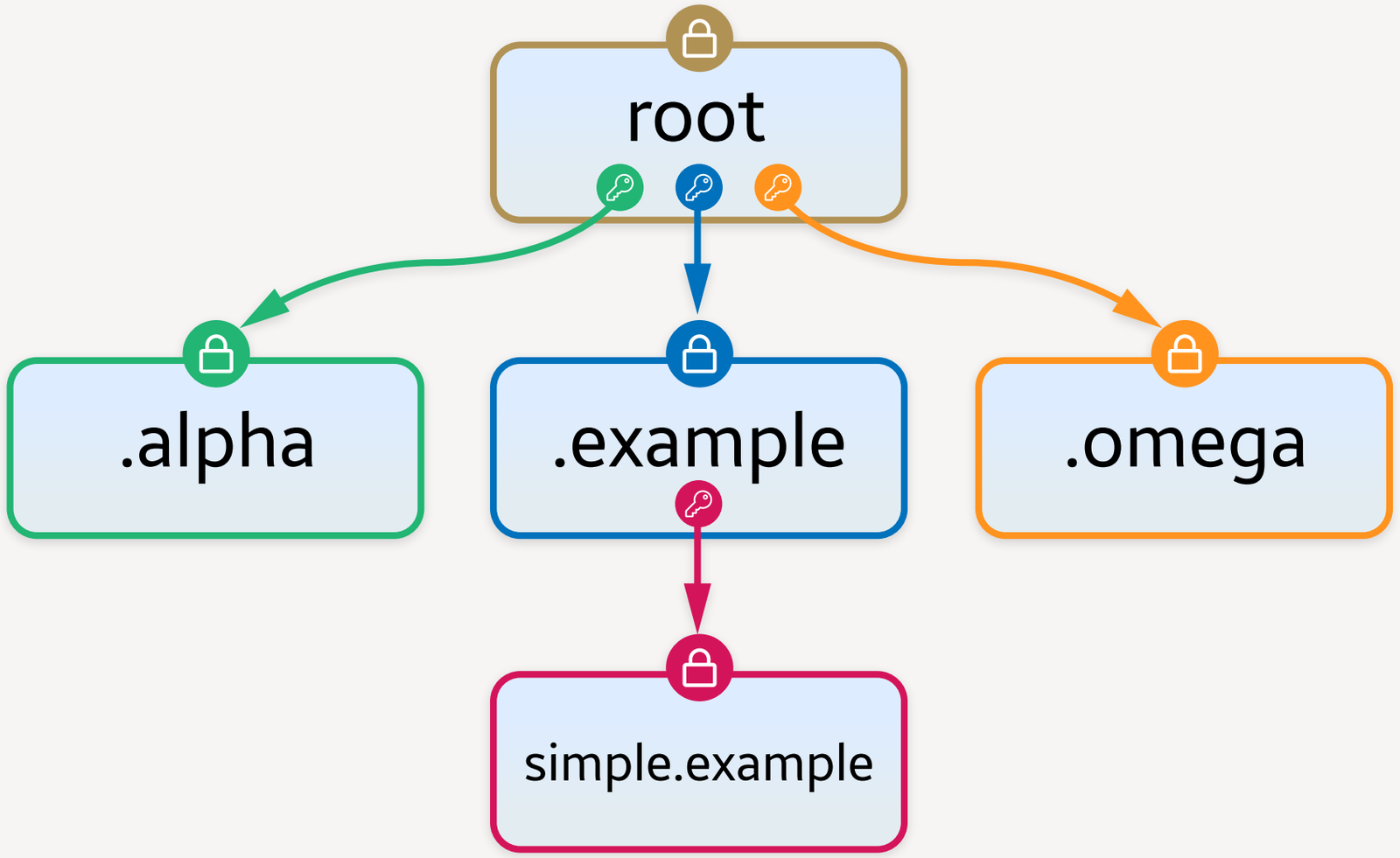
Mapping the logical to reality

Each zone is conceptually a file that contains pointers to servers that can authoritatively provide you data from another zone.



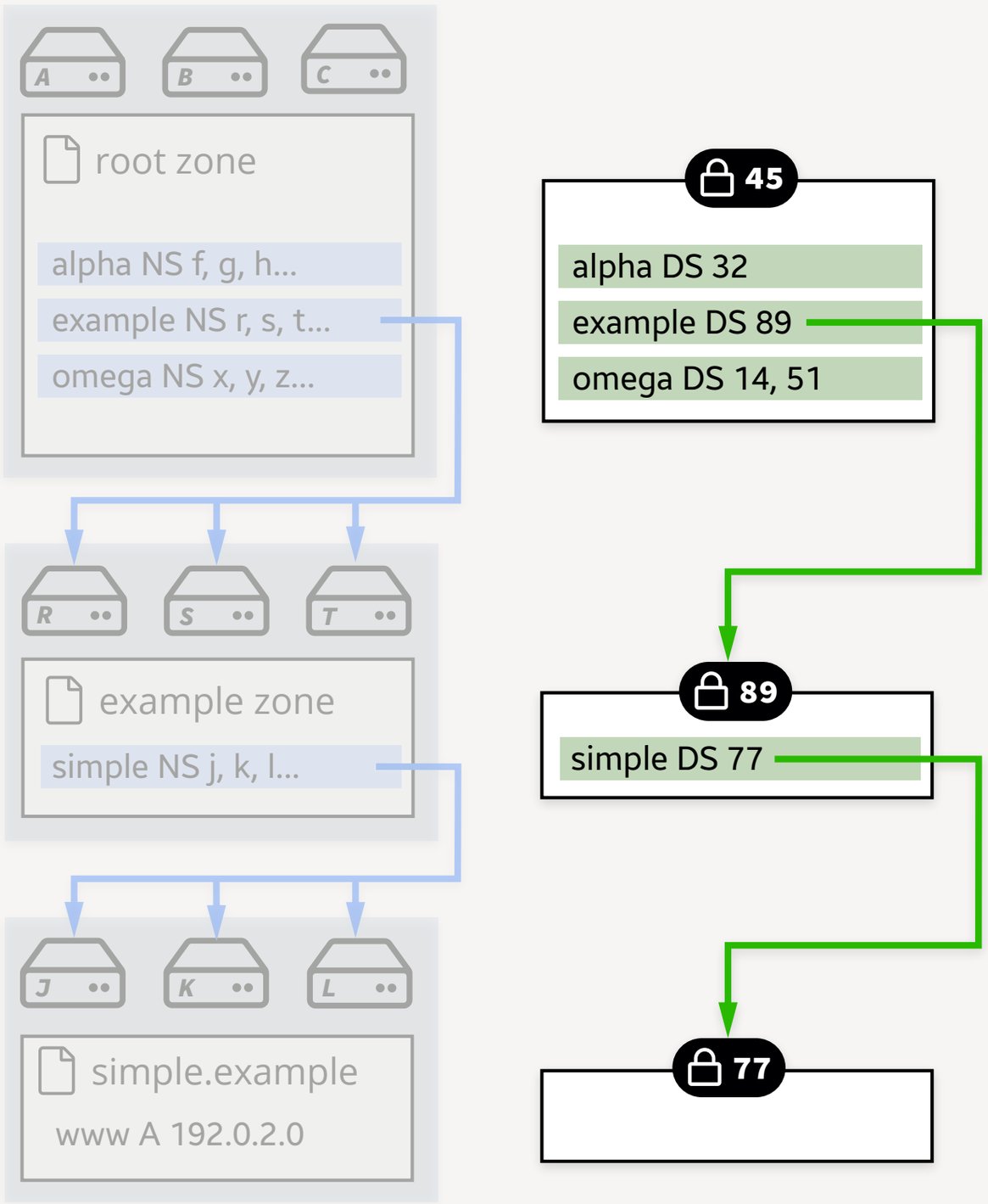
Mapping the logical to reality

To bootstrap the process, a resolver needs to know the locations of the servers authoritative for the root (root servers). They use “root hints” to do this, a local configuration setting.



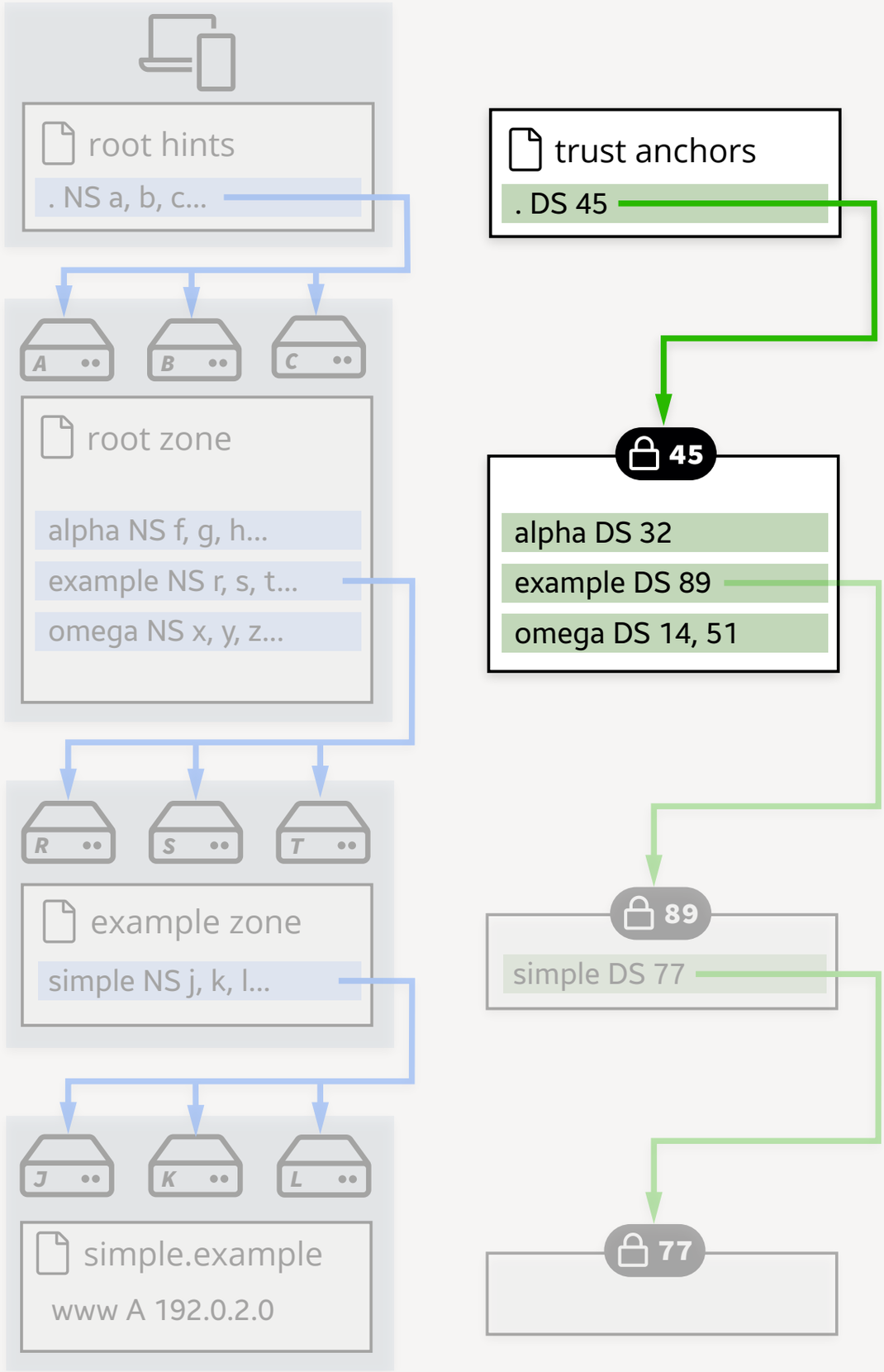
DNSSEC in the logical hierarchy

Similar to the DNS, trust follows the hierarchical model, where keys are used to cryptographically sign zones, and keys are trusted based on endorsement from the zone above.



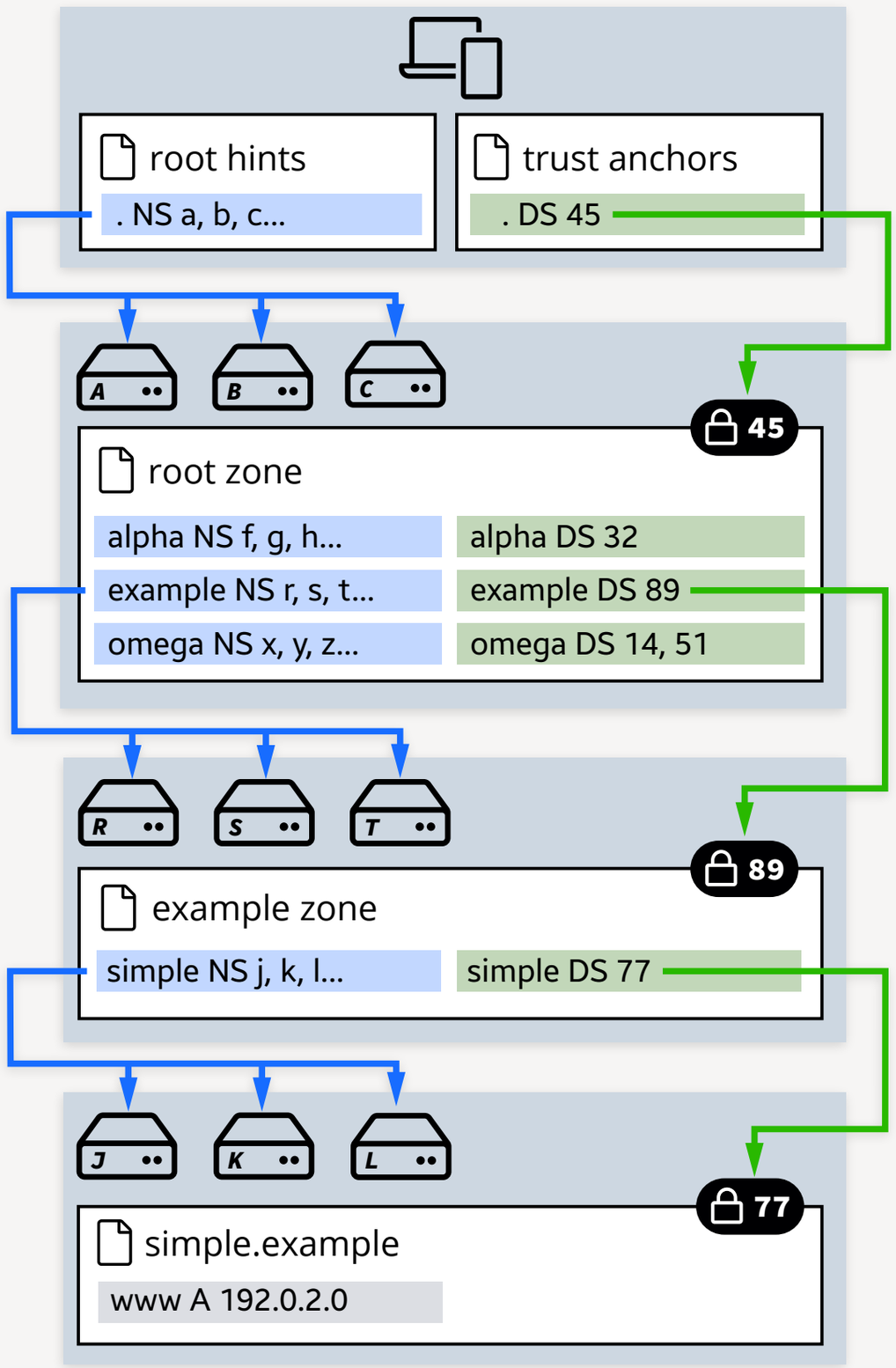
Mapping the logical to reality

As with delegations, there is a chain from the root zone down of "delegation signer" records that denote which key is expected to protect a particular zone.



Mapping the logical to reality

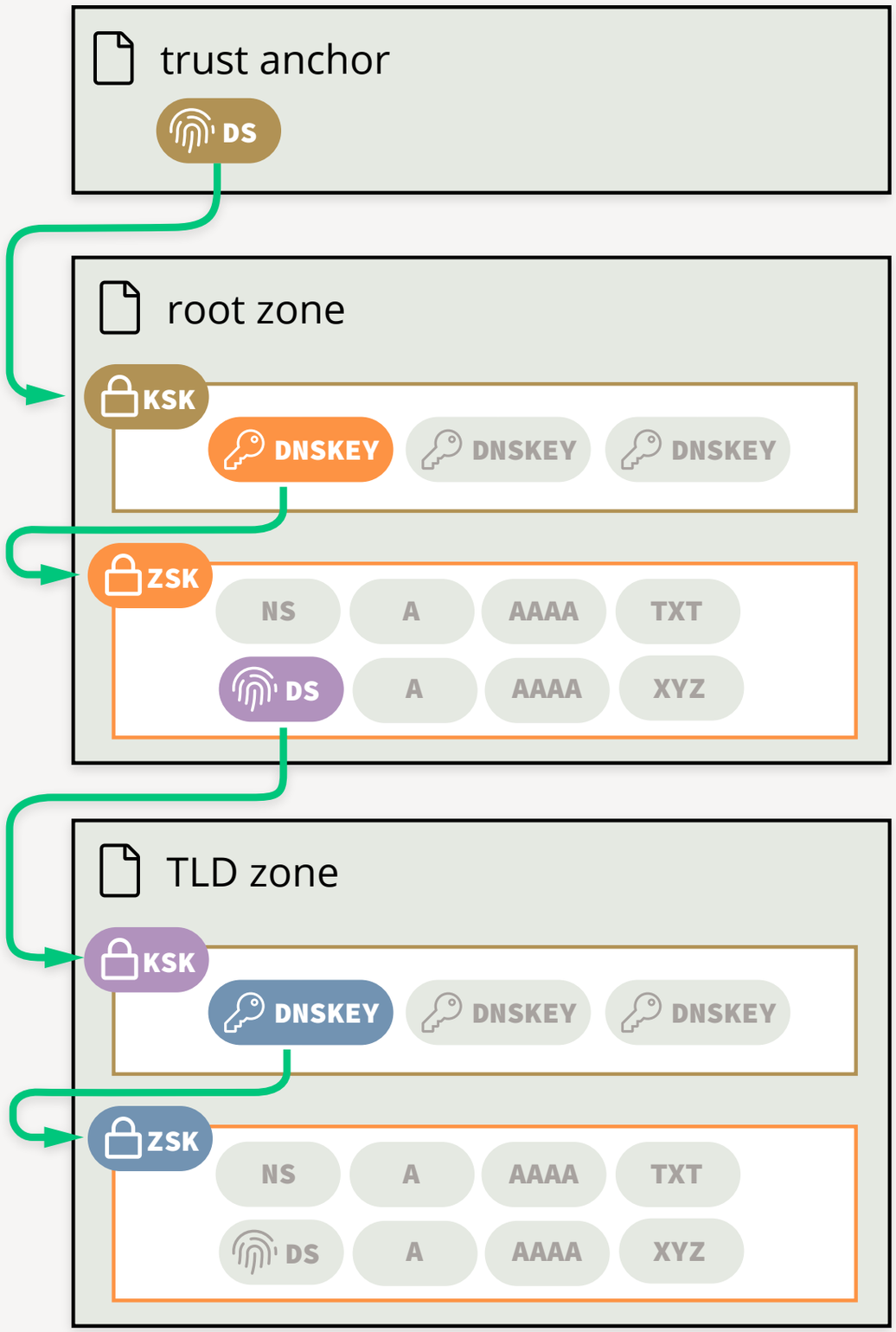
And to bootstrap, we need to configure the start of the process with which key to trust to sign the root zone, known as the “trust anchor”



Bringing it all together

Resolvers have two types of local configuration, root hints (to find the root servers) and trust anchors (what keys to trust for the root zone).

Down the hierarchy, NS records tell you where to find the next zone, and DS records tell you which keys you should trust to sign the next zone.



Additional keys for easier management

It is common configuration for each zone to have two layers of keys for signing their zone:

1. the secure entry point which the DS record points to, known as the **key signing key** (KSK)
2. a key that is used to sign the contents of the zone, known as the **zone signing key** (ZSK)

Why do this?

Allows you to change the ZSK regularly, improving security outcomes. Changing the KSK is complex as you need to update the associated DS record in another location.

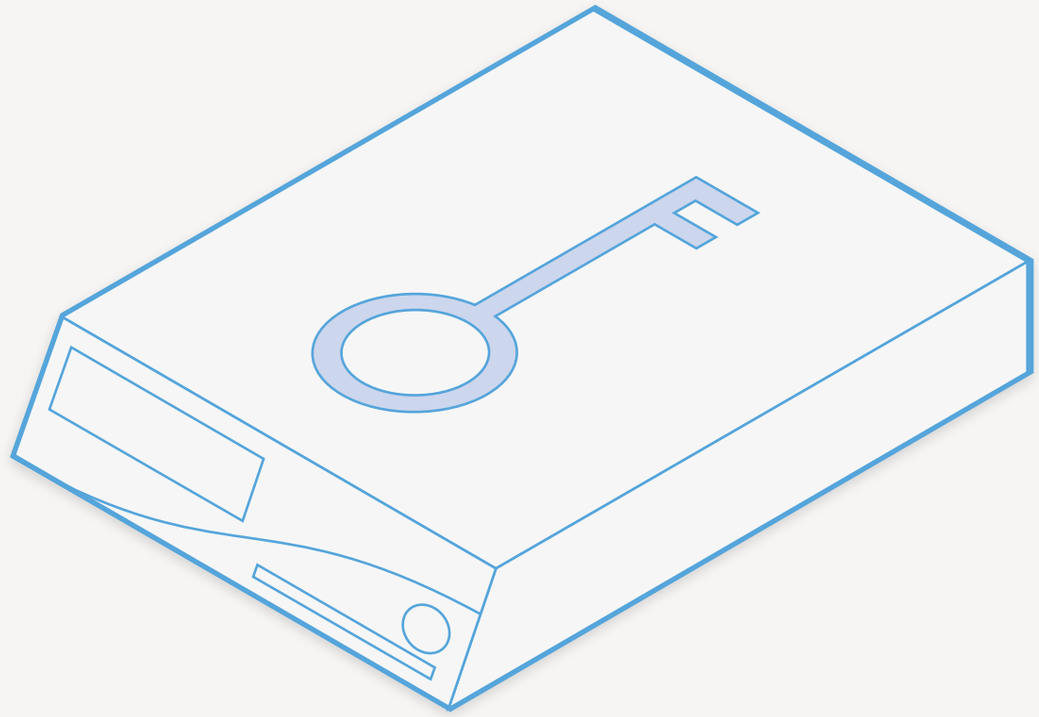
You can also protect the KSK to a higher level, allowing ZSKs to have short lifetimes but be more practical (for example, online signing).

The unique life of the trust anchor

- In the trust hierarchy, changing most keys are no big deal
  - Changing the ZSK? Just needs to be signed by the KSK. Usually the same operator in the same zone, straightforward.
  - Changing the KSK? Just notify your parent zone of a new KSK with a revised set of DS records.
- The root zone has no parent, so KSK changes to the root zone need to be made in the trust anchor configuration
  - Configured locally in resolvers
  - Therefore, very difficult to change, so we:
    - Use long update cycles for planned changes
    - Use update mechanisms (RFC 5011, software updates)
    - Minimize the need for unplanned changes
      - Keep the KSK safe!

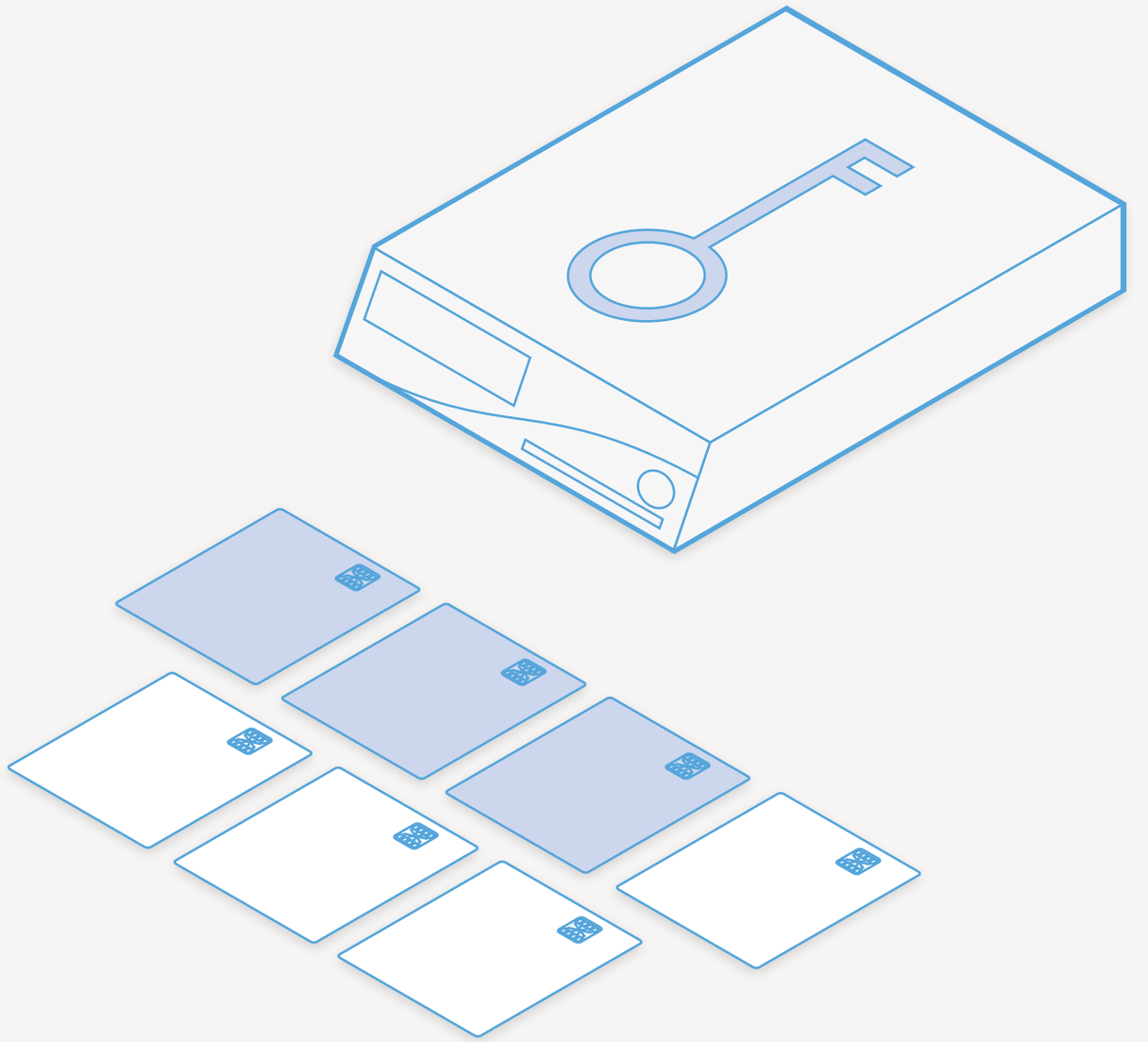
How do we keep the KSK safe?

- 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.



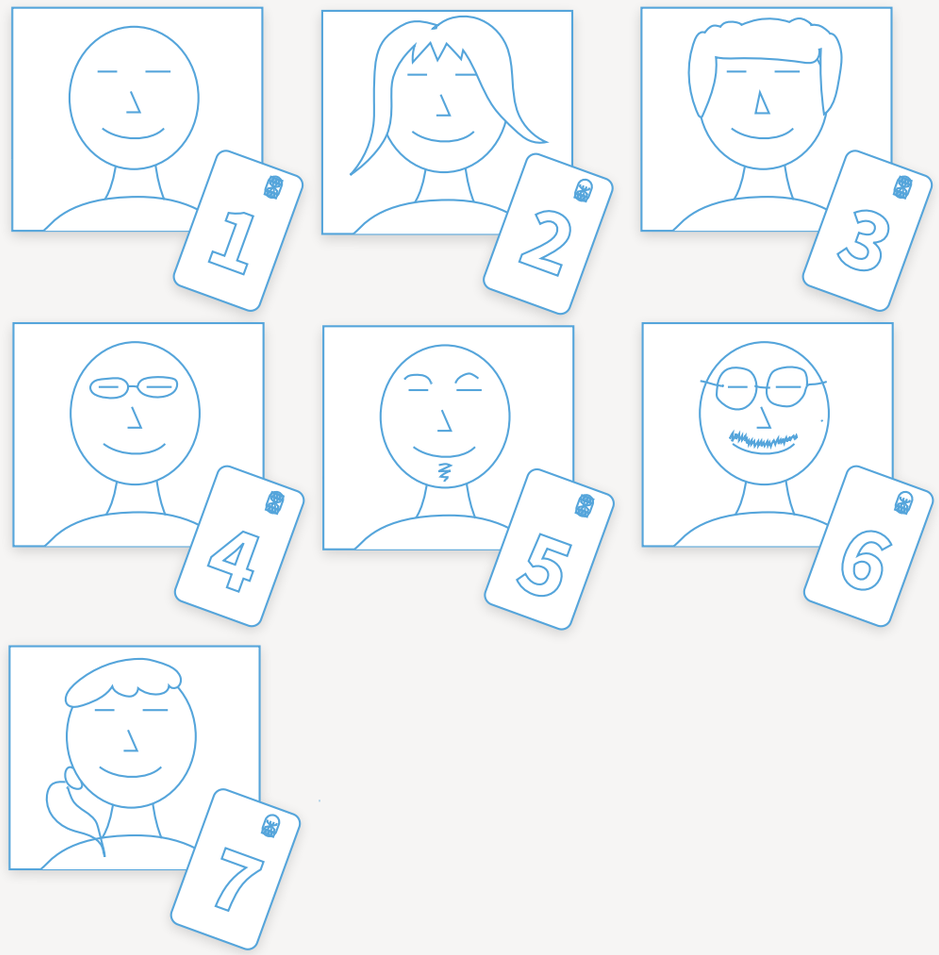
Overview of KSK security

- 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.



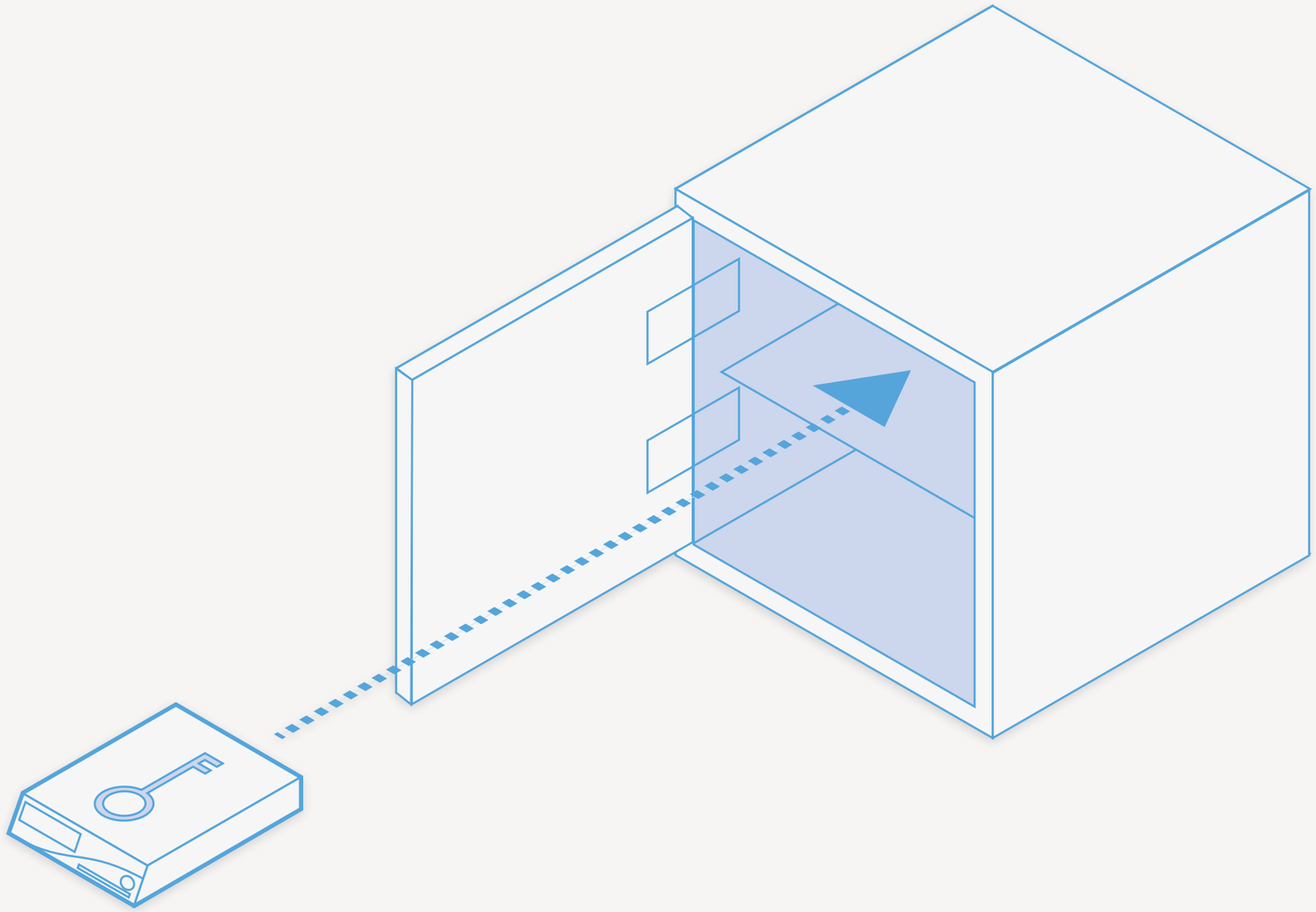
Overview of KSK security

- 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*.



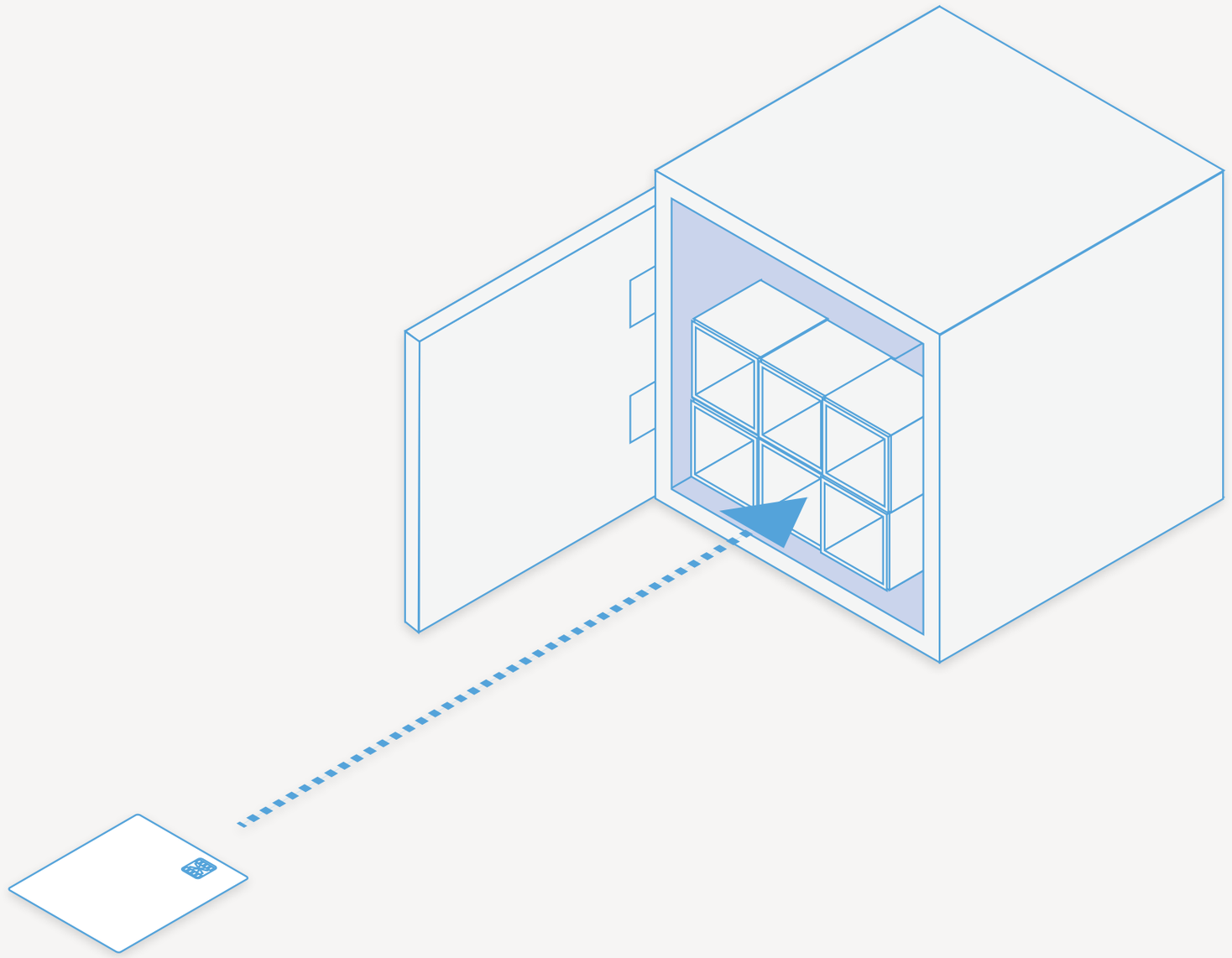
Overview of KSK security

- 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.



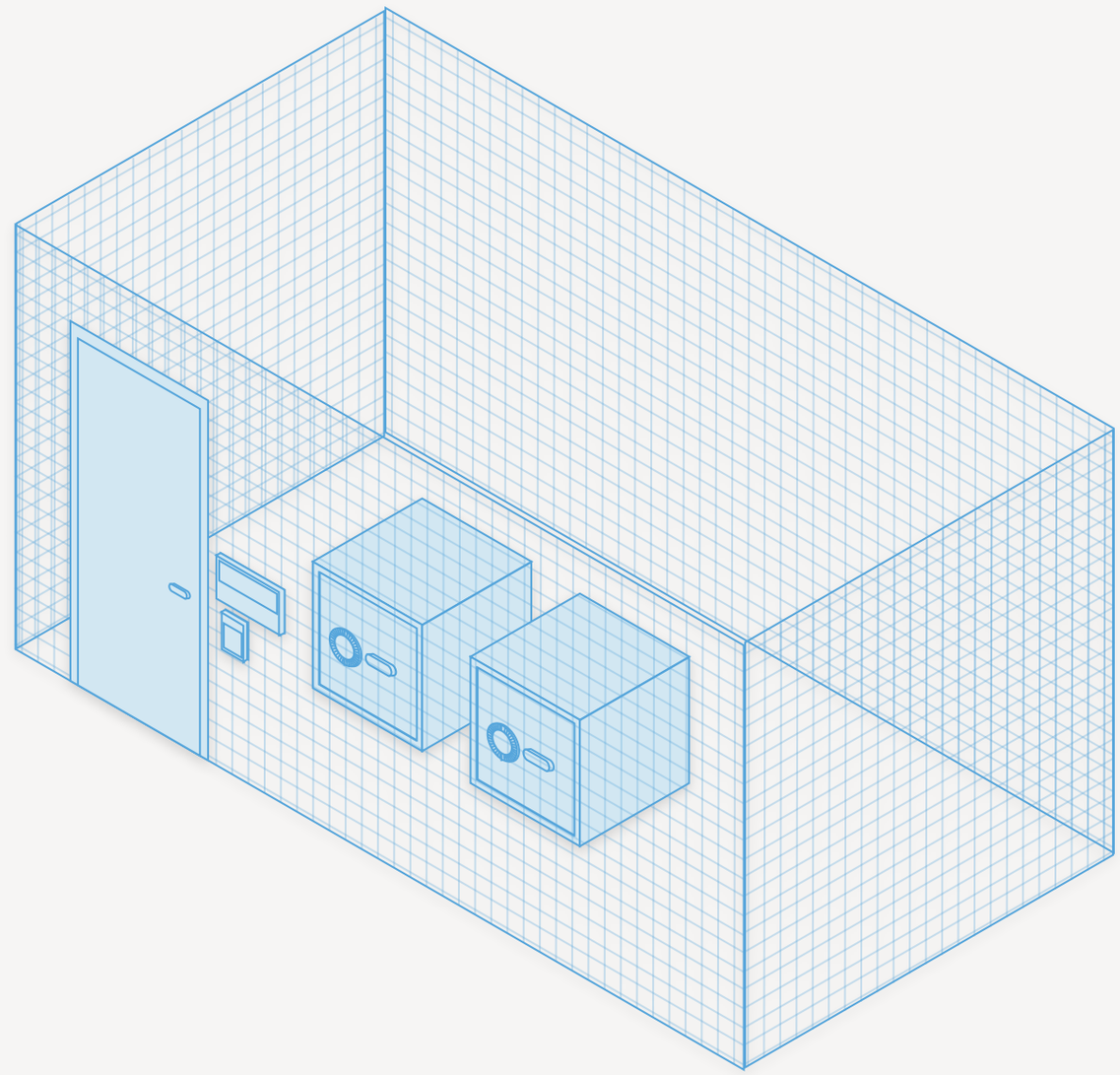
Overview of KSK security

- Each TCR's smart card is stored in a second **credential safe** containing a series of safe deposit boxes. Each safe deposit box is accessed using a mechanical key that the TCR takes with them and keeps safe between ceremonies.



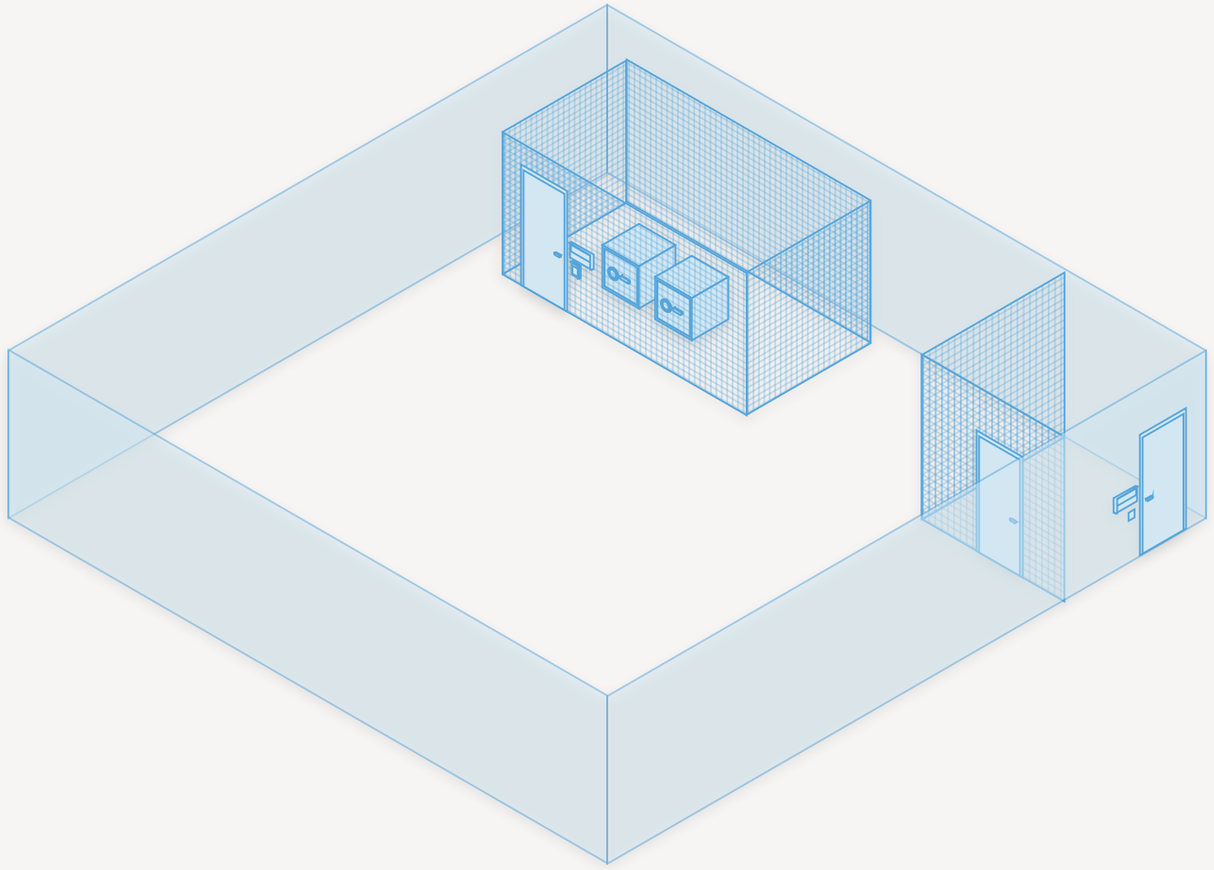
Overview of KSK security

- The two 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.



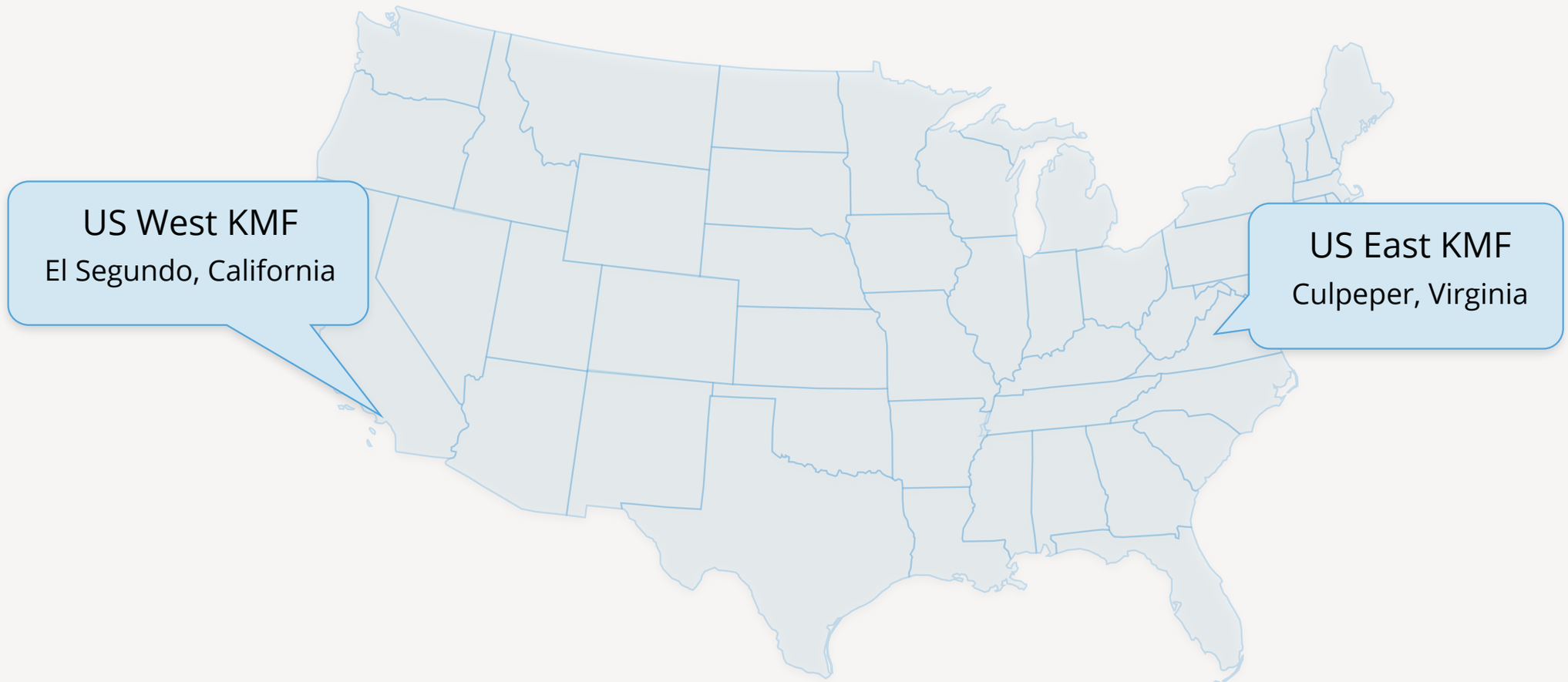
Overview of KSK security

- 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.



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

How do we use the KSK?

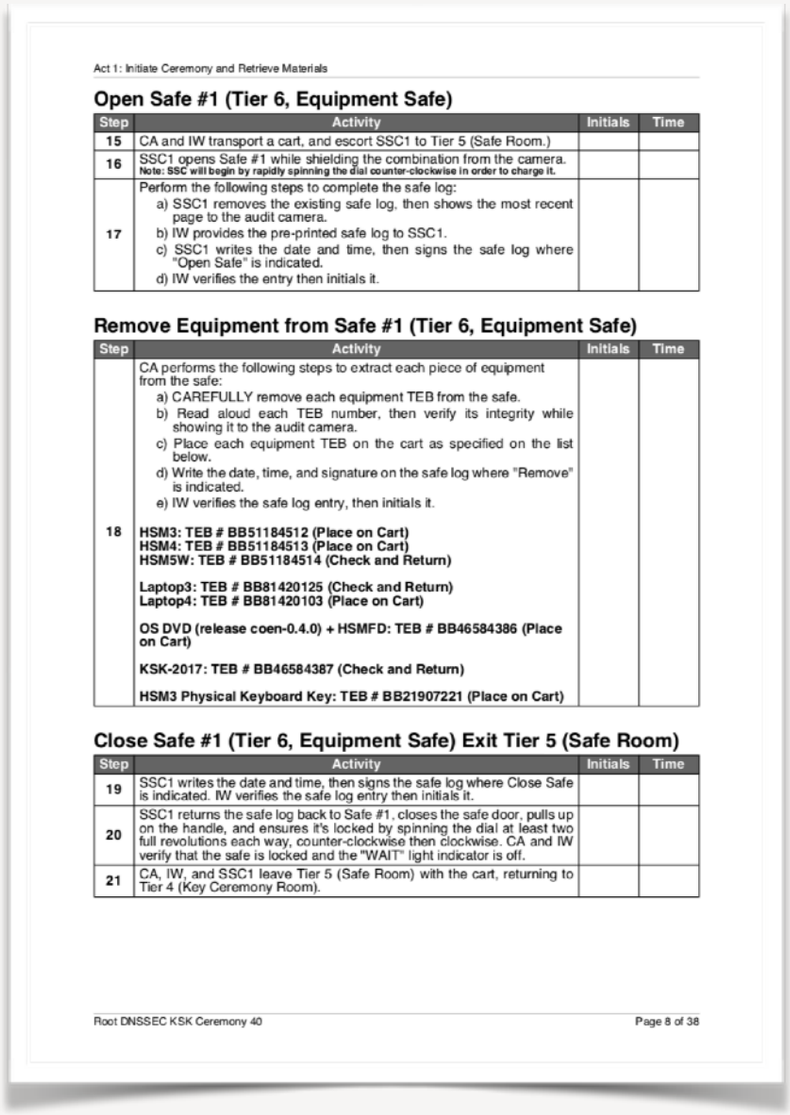
- KSK at rest is kept secure through the controls described
- Authorized use of the KSK is managed through planned events known as **key signing ceremonies,** or simply ceremonies
- Ceremonies convene a quorum of participants needed to activate the KSK in its secure enclosure, with sufficient controls to satisfy observers it is being used in a legitimate way and there is no risk of inadvertent use.

Key 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.
- 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 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. **Note: SSC will begin by rapidly spinning the dial counter-clockwise in order to charge it.**		
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.		

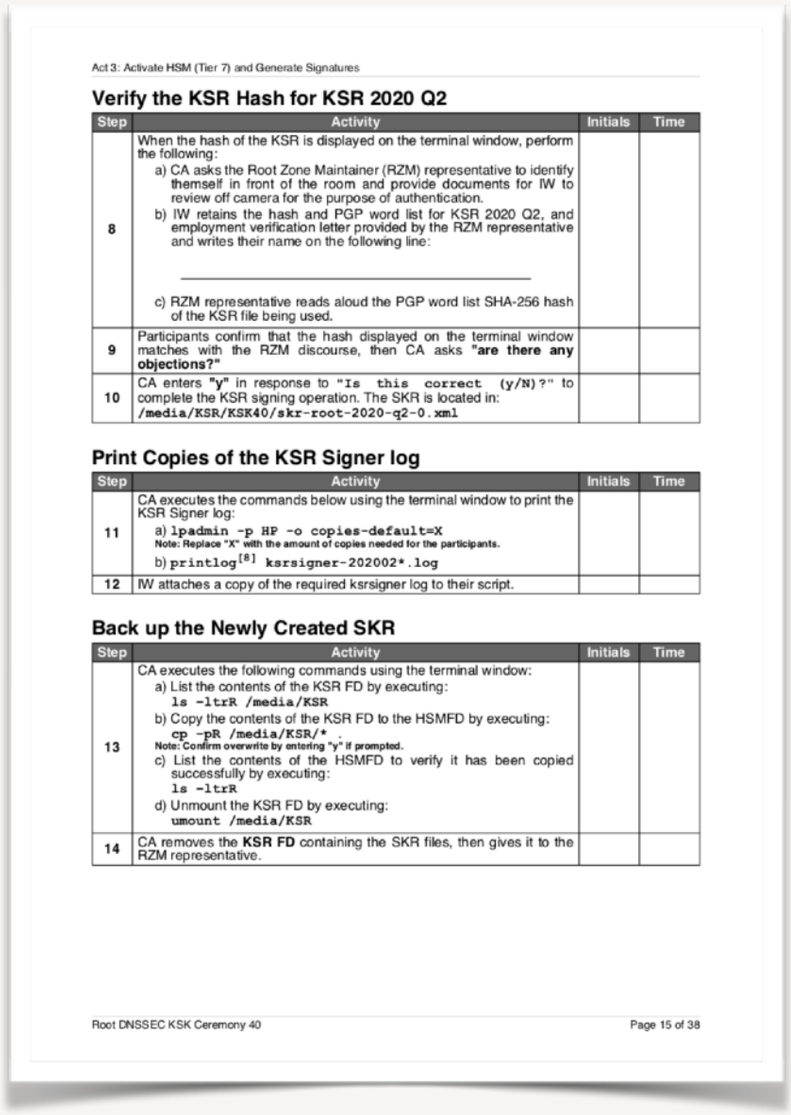
Remove Equipment from Safe #1 (Tier 6, Equipment Safe)

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 themself 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: _____ 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: `/media/KSR/KSK40/skr-root-2020-q2-0.xml`		

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) `lpadmin -p HP -o copies-default=X` **Note: Replace "X" with the amount of copies needed for the participants.** b) `printlog`[8] `ksrsigner-202002*.log`		
12	IW attaches a copy of the required ksrsigner log to their script.		

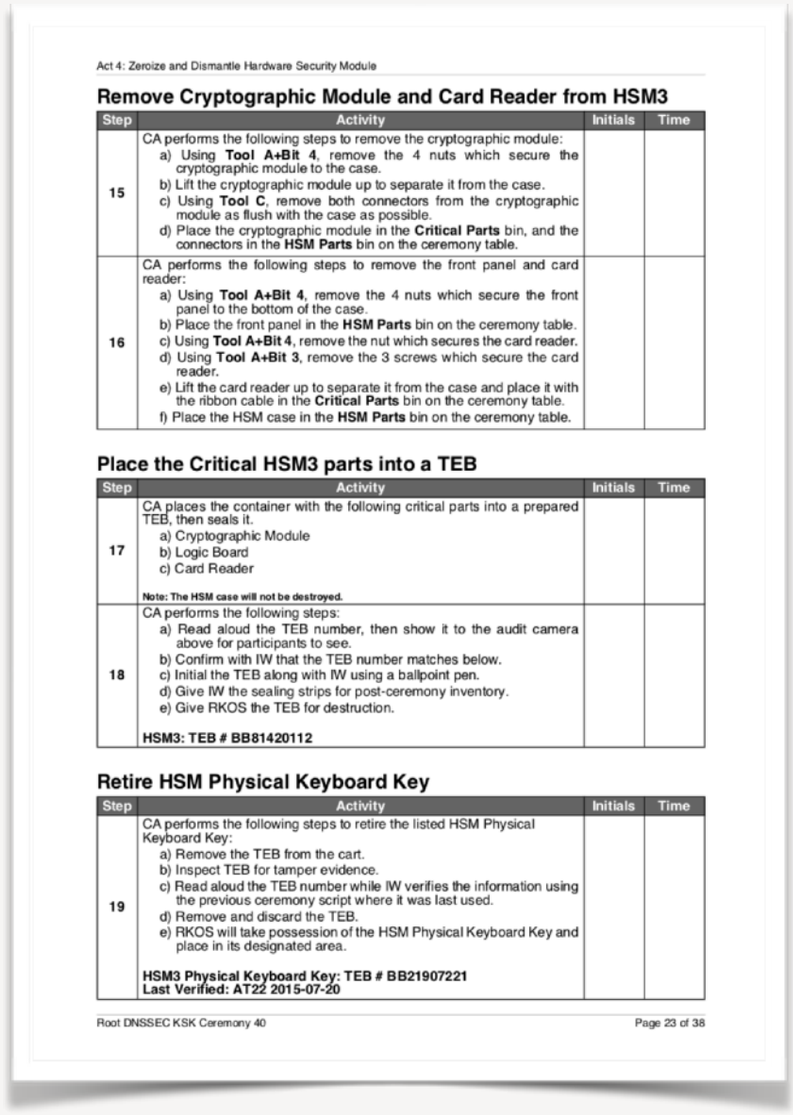
Back up the Newly Created SKR

Step	Activity	Initials	Time

13	CA executes the following commands using the terminal window:
	a) List the contents of the KSR FD by executing:
	`ls -ltrR /media/KSR`
	b) Copy the contents of the KSR FD to the HSMFD by executing:
	`cp -pR /media/KSR/* .`
	Note: Confirm overwrite by entering "y" if prompted.
	c) List the contents of the HSMFD to verify it has been copied successfully by executing:
	`ls -ltrR`
	d) Unmount the KSR FD by executing:
	`umount /media/KSR`		

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 **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**		

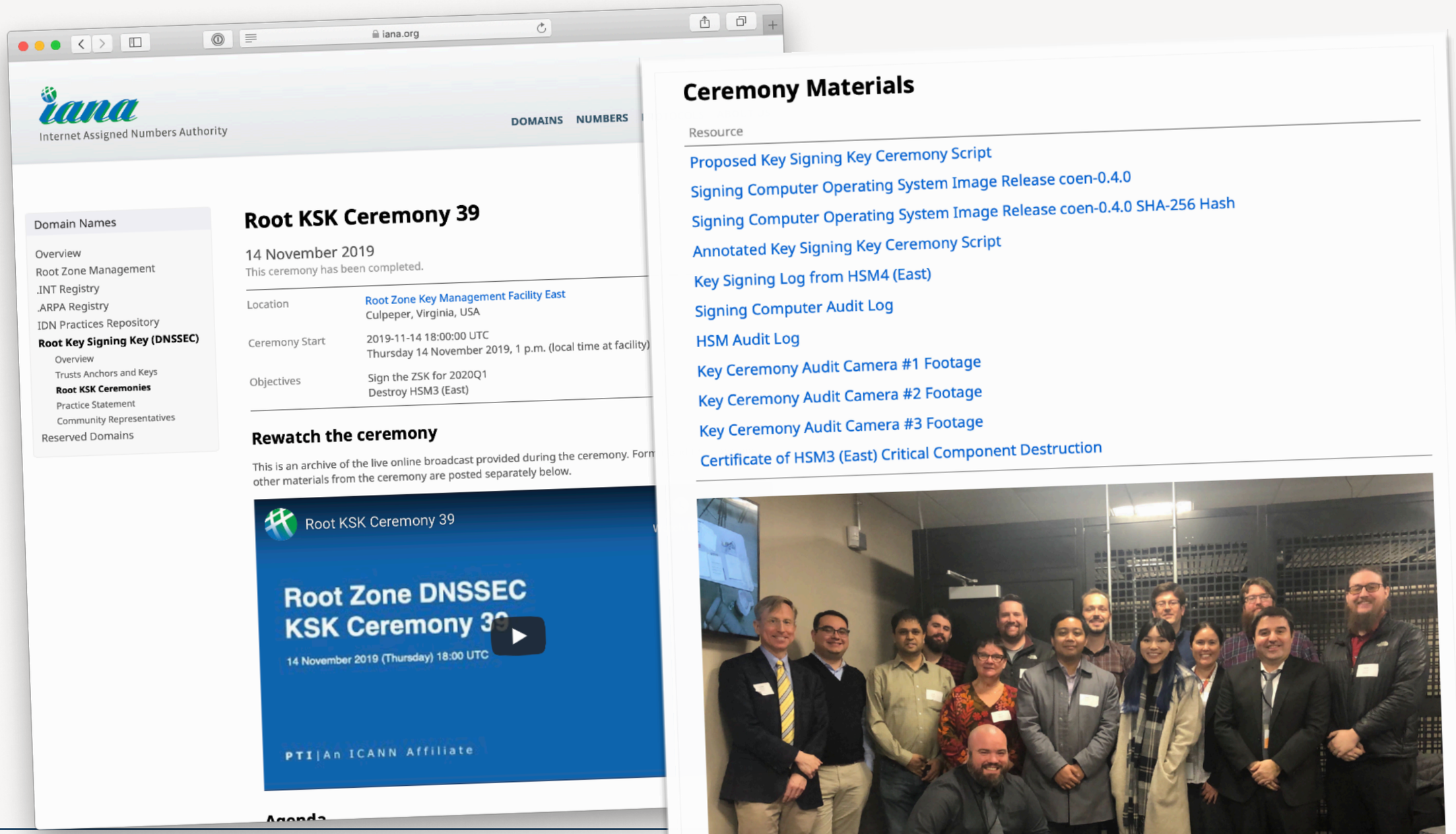
Retire HSM Physical Keyboard Key

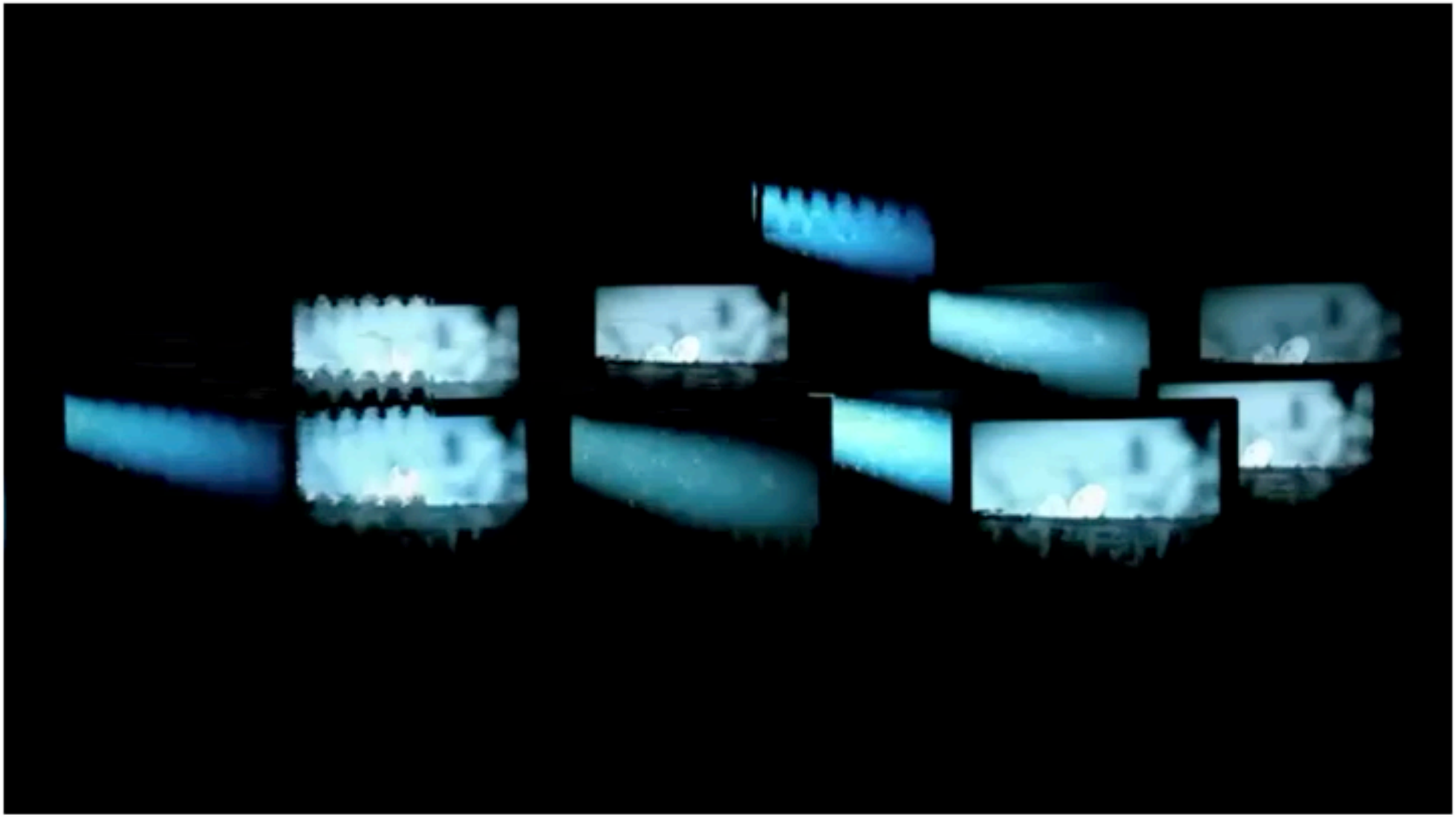
Step	Activity	Initials	Time
19	CA performs the following steps to retire the listed HSM Physical Keyboard Key: a) Remove the TEB from the cart. b) Inspect TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB. 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.





Media videos of key ceremonies
VICE News: *https://www.vice.com/en_us/article/zmwgwx/this-is-the-nerdy-ceremony-that-keeps-the-internet-running*
The Guardian: *https://www.theguardian.com/technology/2014/feb/28/seven-people-keys-worldwide-internet-security-web*
Others: *https://kimdavies.com/key-ceremony-primer/*

What does a perfect ceremony look like?

- Conducted exactly as prescribed in the script
- No improper disclosure of sensitive materials
- Meet all security controls, including satisfying control audit
- Comply with the DNSSEC Practice Statement (DPS), the formal policy governing KSK operations
- Everyone needed shows up on time, all equipment works exactly as it is meant to
- Doesn’t take unduly long to complete
- Managed lifecycles of the hardware and trusted personnel enrollment
- **Performed the necessary work of the ceremony (generating key signatures)**
- **Performed to the satisfaction of attendees and the broader community**

Ceremonies are never perfect

- Ceremonies are pre-scripted, but it is rare the ceremony goes exactly to script
  - It is okay to deviate from script.
  - CAs are empowered in the ceremony context to deviate to achieve the goal by improvising alternative solutions that meet the overall objective
  - Variances are written up as exceptions, which are documented to the satisfaction of participants
- 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

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 is a unique year.

KSK Ceremony 40

(The last one)

Key Ceremony 40

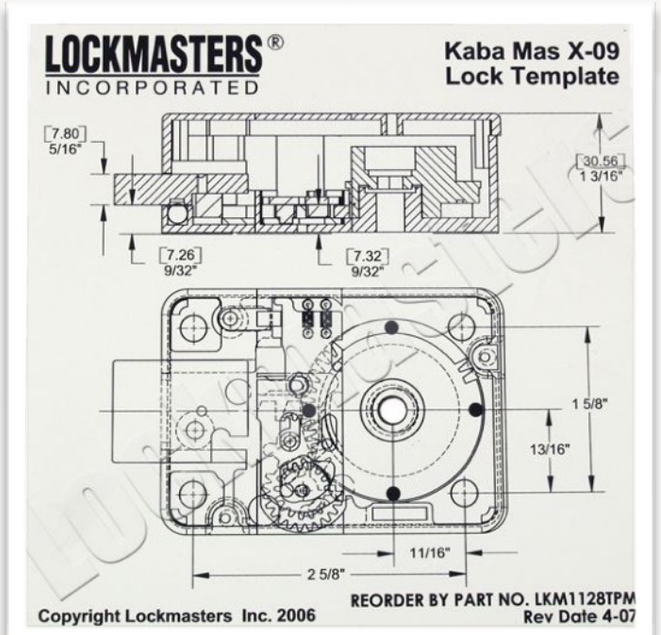
- Scheduled for 12 February 2020
- Objectives
  - Sign the 2020Q2 key material (covering April-June 2020)
  - Decommission a HSM
- Pre-ceremony activity included maintenance work to upgrade the lock assemblies within the safe
  - These are performed in administrative ceremonies that are audited to the 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

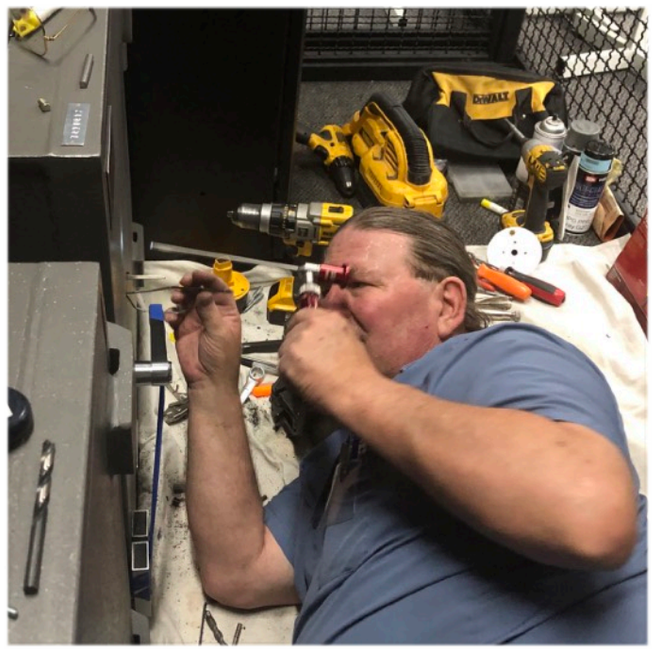
Key Ceremony 40

- 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.

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

(The next one)

Key Ceremony 41

- Scheduled for 23 April 2020 (10 year anniversary!)
- Planned objectives
  - 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 has caused us to focus on developing contingencies for this ceremony as the situation deteriorates
- 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, have 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
- 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.
- Areas we are exploring DPS updates
  - More precise triggering conditions mapped out in advance for contingency scenarios

Where are we now?

- We are advanced in planning to perform the ceremony with minimum personnel, with TCRs participating remotely.
  - DPS revised to clarify roles and responsibility and provide flexibility for disaster recovery
  - 4 of 7 TCRs are transmitting their secure credentials to 4 surrogates in Los Angeles
- We expect to hold the ceremony on the time and date scheduled
  - … but in El Segundo, not Culpeper as originally planned
- On April 6, we convened our Policy Management Authority (PMA) to approve changes to the DPS to better prescribe disaster recovery options.

Where are we now?

- Proceeding with this revised approach is contingent on executive and ICANN Board approval (expected tomorrow)
  - Normal rescheduling and tailoring of ceremonies is performed by staff, but there is recognition this warrants additional review and scrutiny
- Bolster normal remote participation to make it active rather than passive
  - Allow trusted roles in particular (TCRs etc.) to play comparable role remotely, ability to interject and so on
- Minimize the scope of the ceremony
  - Eliminate non-essential acts
- Sign an extended period (specifically, 9 months)
  - Eliminate the need for future ceremonies this year until circumstances improve
  - Withhold signature disclosure until the normal time window

In conclusion

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
  - Tests our ability to be adaptive
  - Allows us to exercise scenarios that had only been hypotheticals to date
  - Stretches 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
    - However, 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
  - Flagged in the forthcoming PTI Strategic Plan draft.
- 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?

Constant improvement is part of the DNA

- Constant renewal
  - Most aspects of the facility and ceremony procedures has 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