A BRIEF PRIMER ON MANAGING THE KEYS TO THE INTERNET

DAVID HUBERMAN

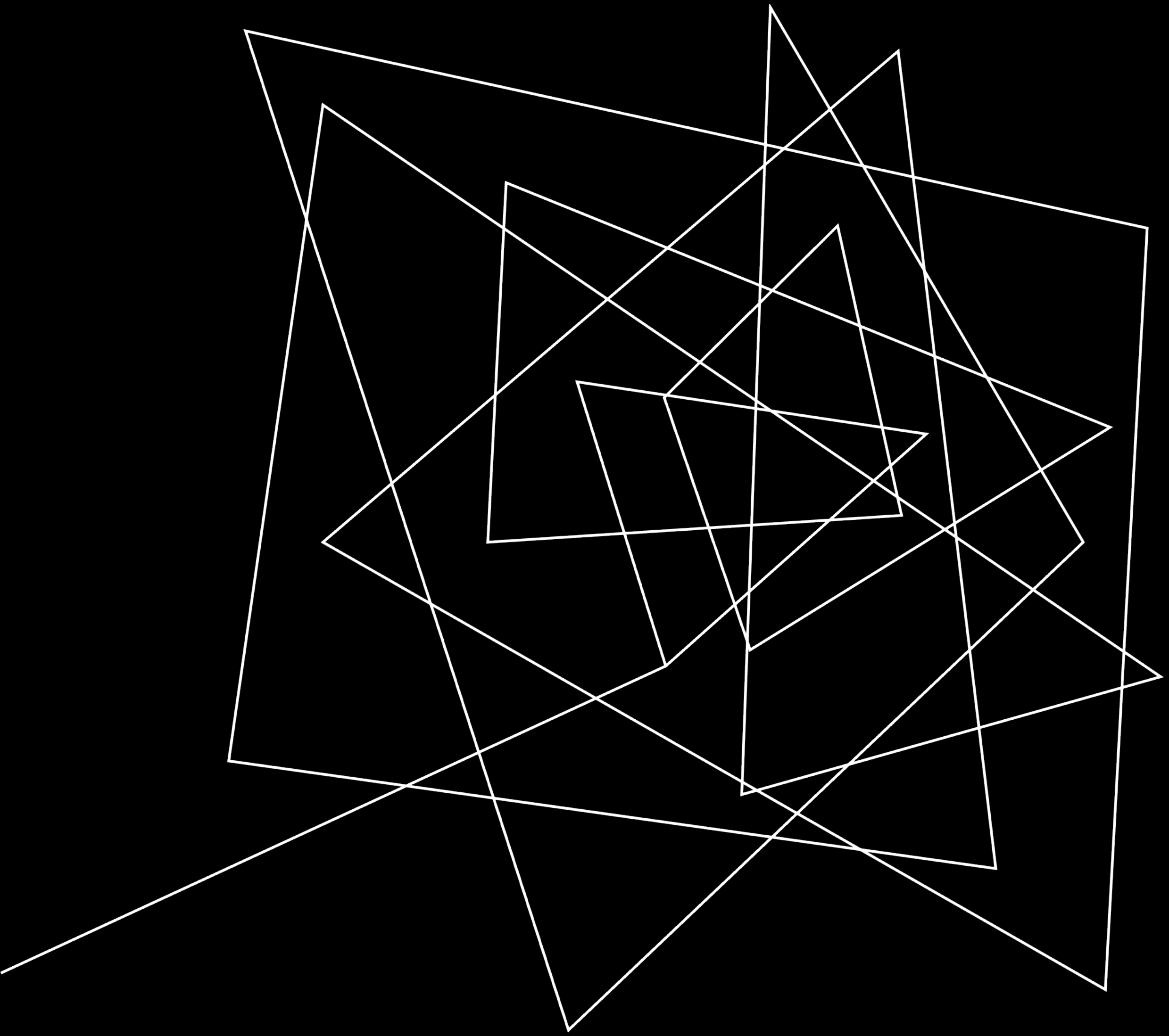
ICANN’s OFFICE OF THE CTO

INTRODUCTION

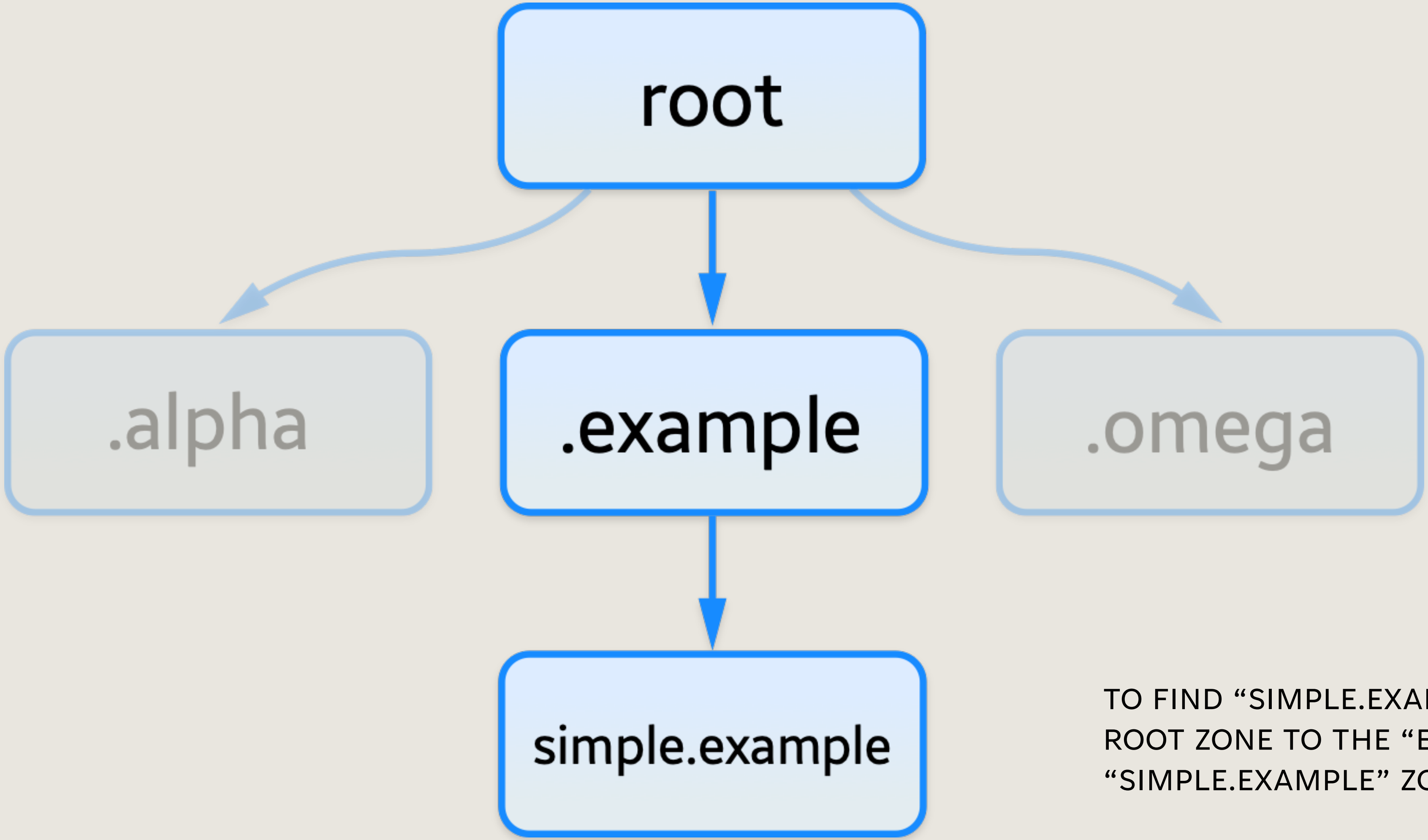
There aren't really 7 keys to the Internet. That's just marketing.

There are 7 people who each hold one physical safety deposit box key. Inside each safety deposit box are credentials which, when used together, enable the operation of a hardware device which generates key signatures.

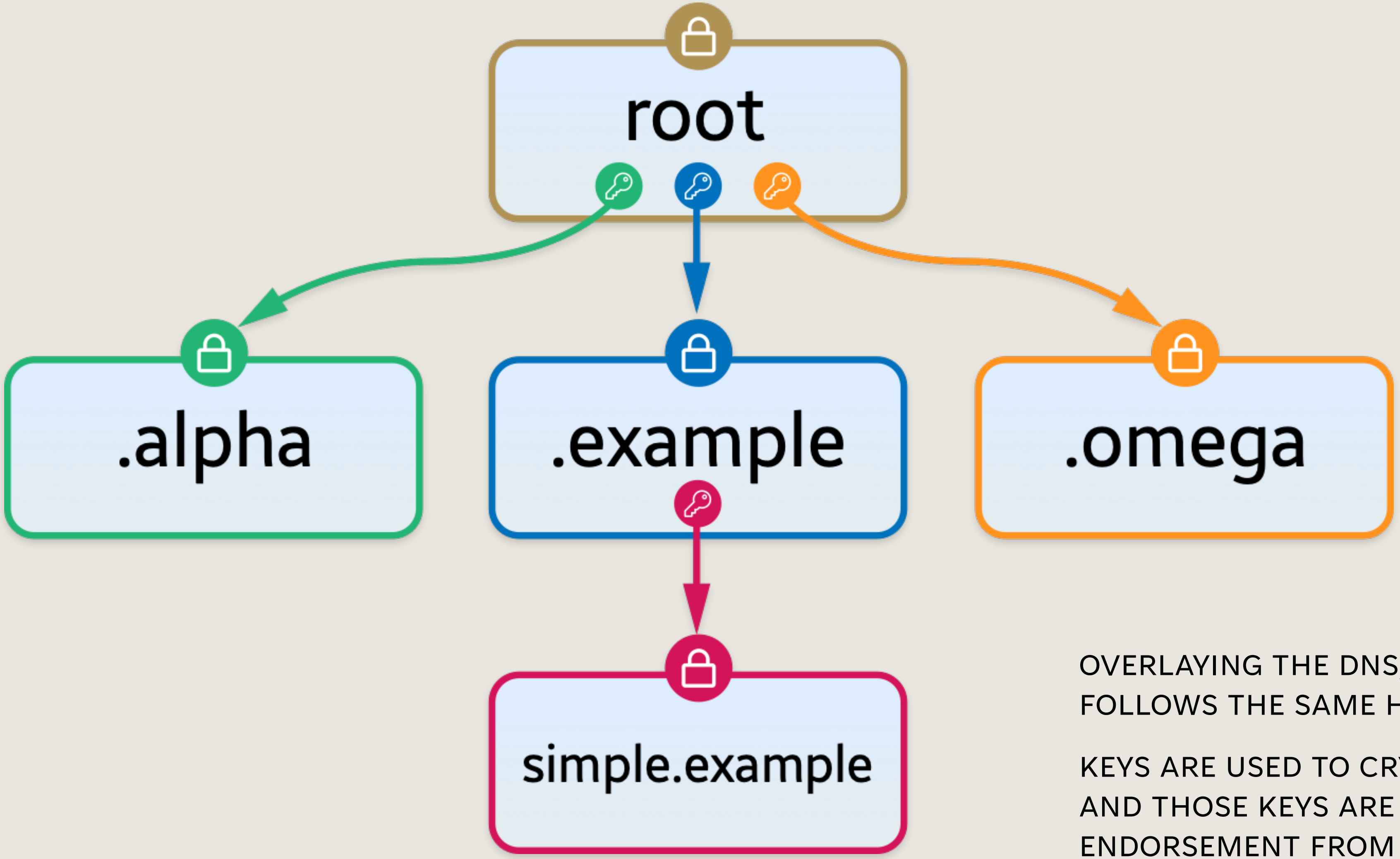
Let me explain . . .



WHAT IS A KEY SIGNING KEY?

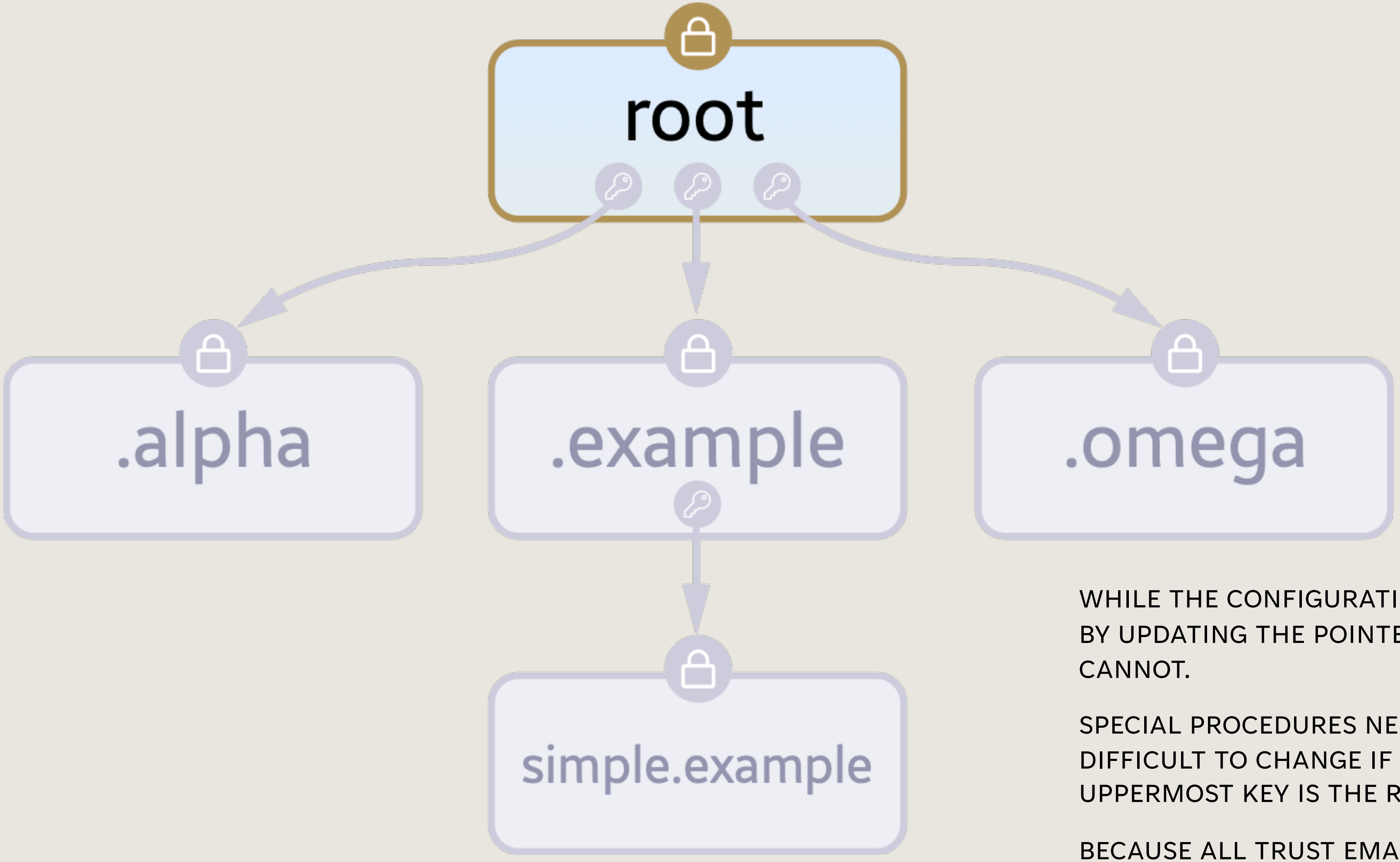


TO FIND “SIMPLE.EXAMPLE”, YOU TRAVERSE FROM THE ROOT ZONE TO THE “EXAMPLE” ZONE TO THE “SIMPLE.EXAMPLE” ZONE.



OVERLAYING THE DNS, THE SECURITY TRUST MODEL FOLLOWS THE SAME HIERARCHY.

KEYS ARE USED TO CRYPTOGRAPHICALLY SIGN ZONES, AND THOSE KEYS ARE TRUSTED BASED ON ENDORSEMENT FROM THE ZONE ABOVE.



WHILE THE CONFIGURATION OF OTHER ZONES CAN EASILY BE CHANGED BY UPDATING THE POINTERS IN THEIR PARENT ZONE, THE ROOT ZONE CANNOT.

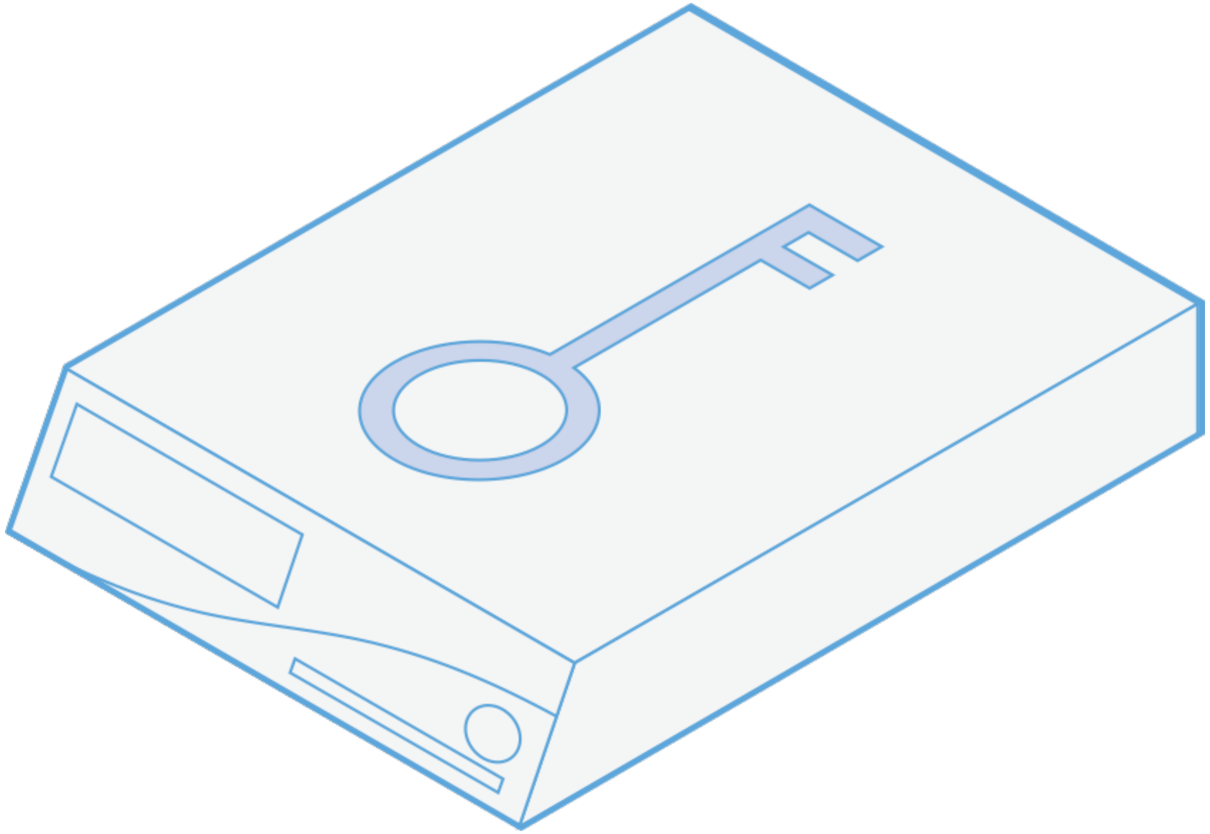
SPECIAL PROCEDURES NEED TO BE IN PLACE BECAUSE IT IS VERY DIFFICULT TO CHANGE IF IT IS BROKEN OR COMPROMISED. THE UPPERMOST KEY IS THE ROOT ZONE “KEY SIGNING KEY” OR KSK.

BECAUSE ALL TRUST EMANATES FROM THE TOP, IT IS ALSO KNOWN AS THE TRUST ANCHOR.

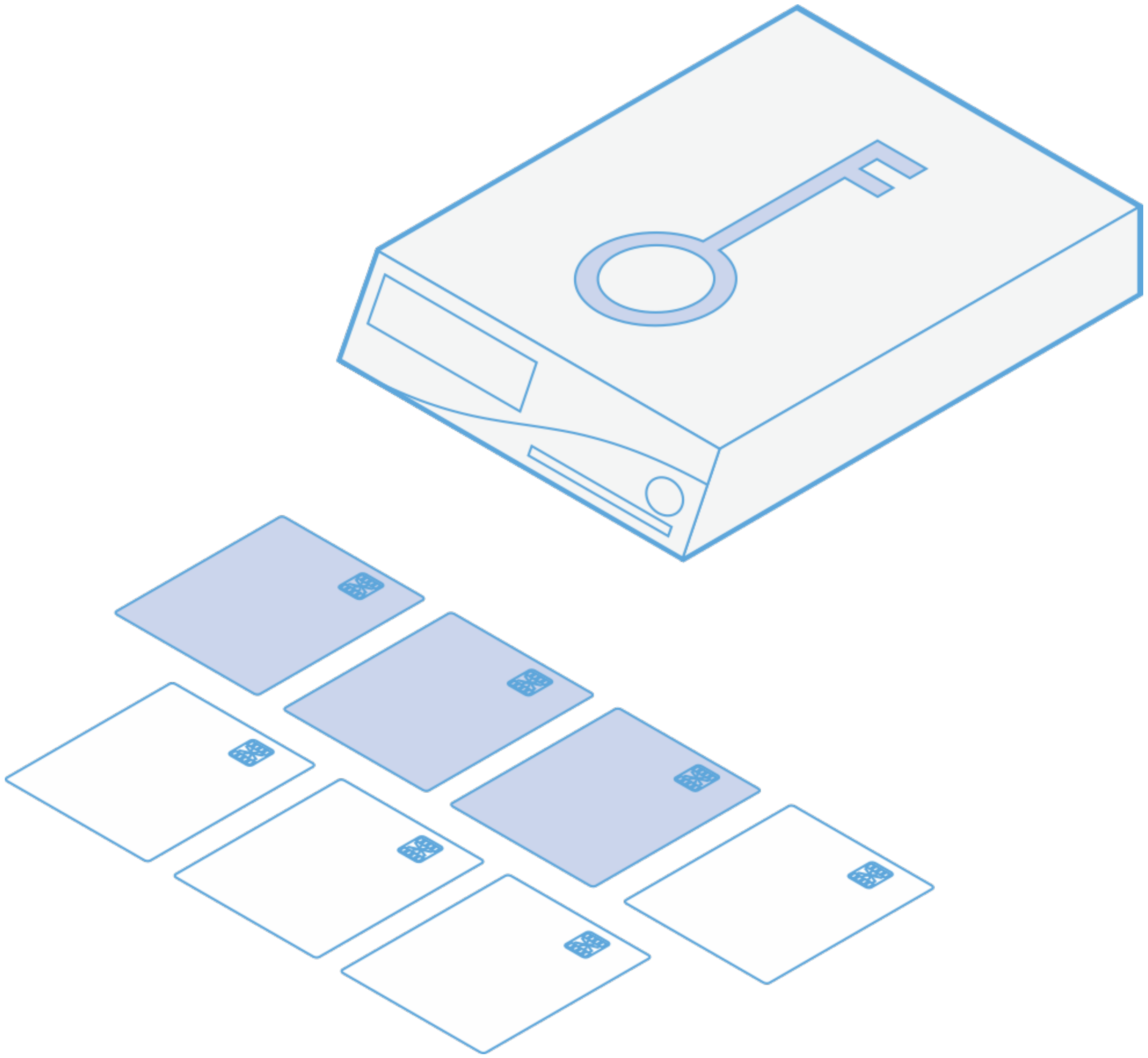
SO HOW DO WE SECURE THE ROOT SIGNING KEY?

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.



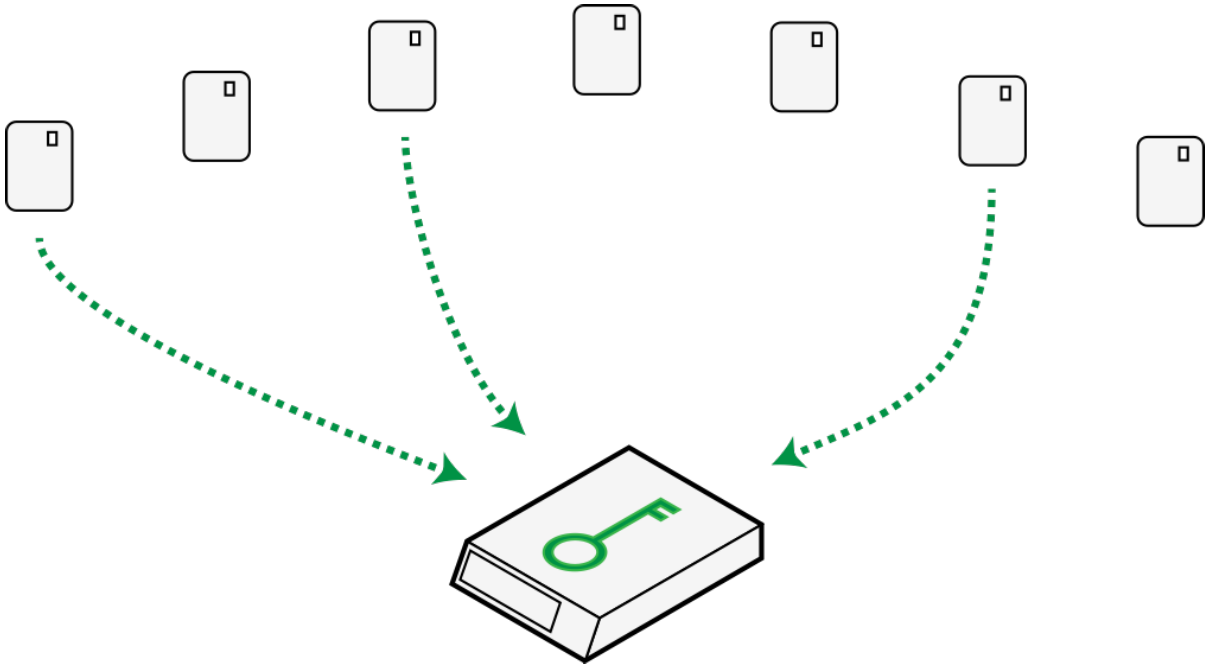
SEVEN SMART CARDS EXIST THAT CAN TURN ON EACH DEVICE. THE DEVICE IS CONFIGURED SUCH THAT 3 OF THE 7 SMART CARDS MUST BE PRESENT TO MAKE IT USEABLE.



EACH SMART CARD IS ASSIGNED TO A DIFFERENT ICANN COMMUNITY MEMBER, KNOWN AS A **TRUSTED COMMUNITY REPRESENTATIVE**.

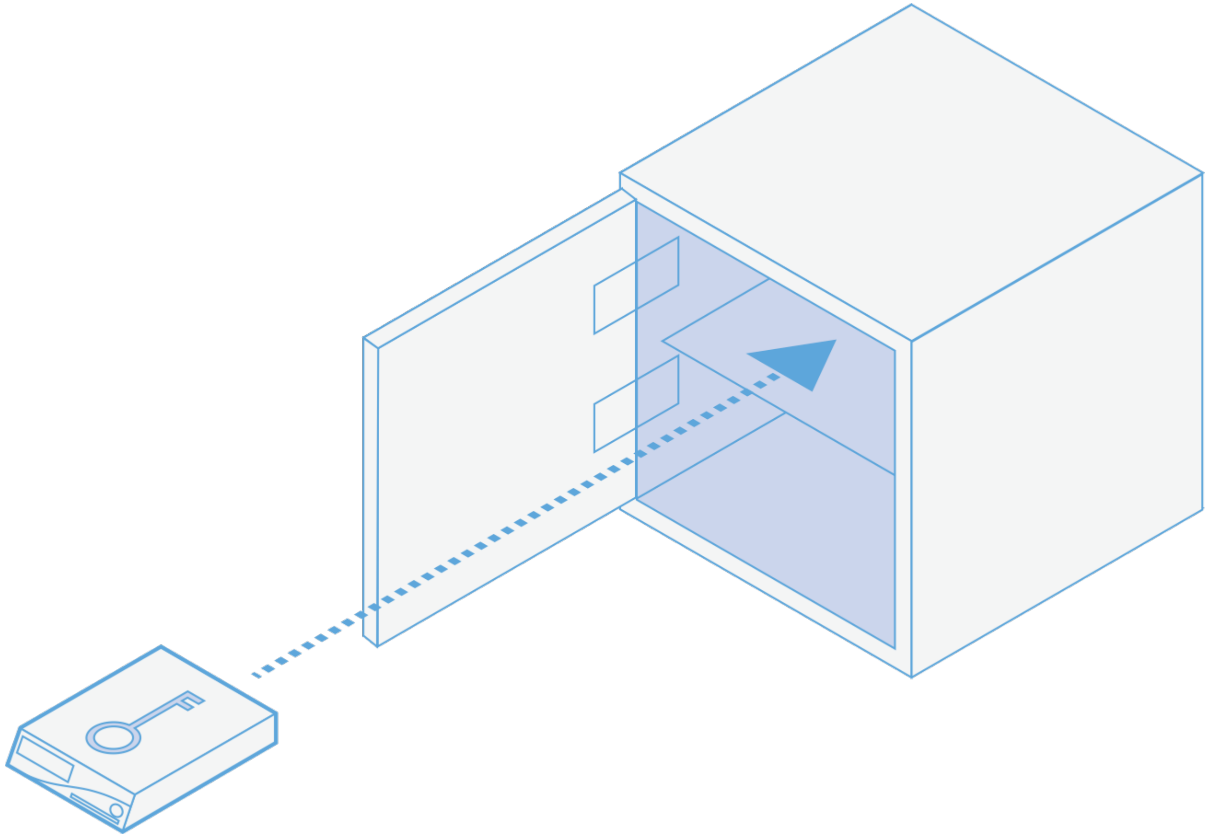
TO ACCESS THE KEY SIGNING KEY, THEREFORE, AT LEAST THREE OF THESE TCRS NEED TO CONVENE.

THESE PLANNED EVENTS ARE CALLED **KEY SIGNING CEREMONIES**.



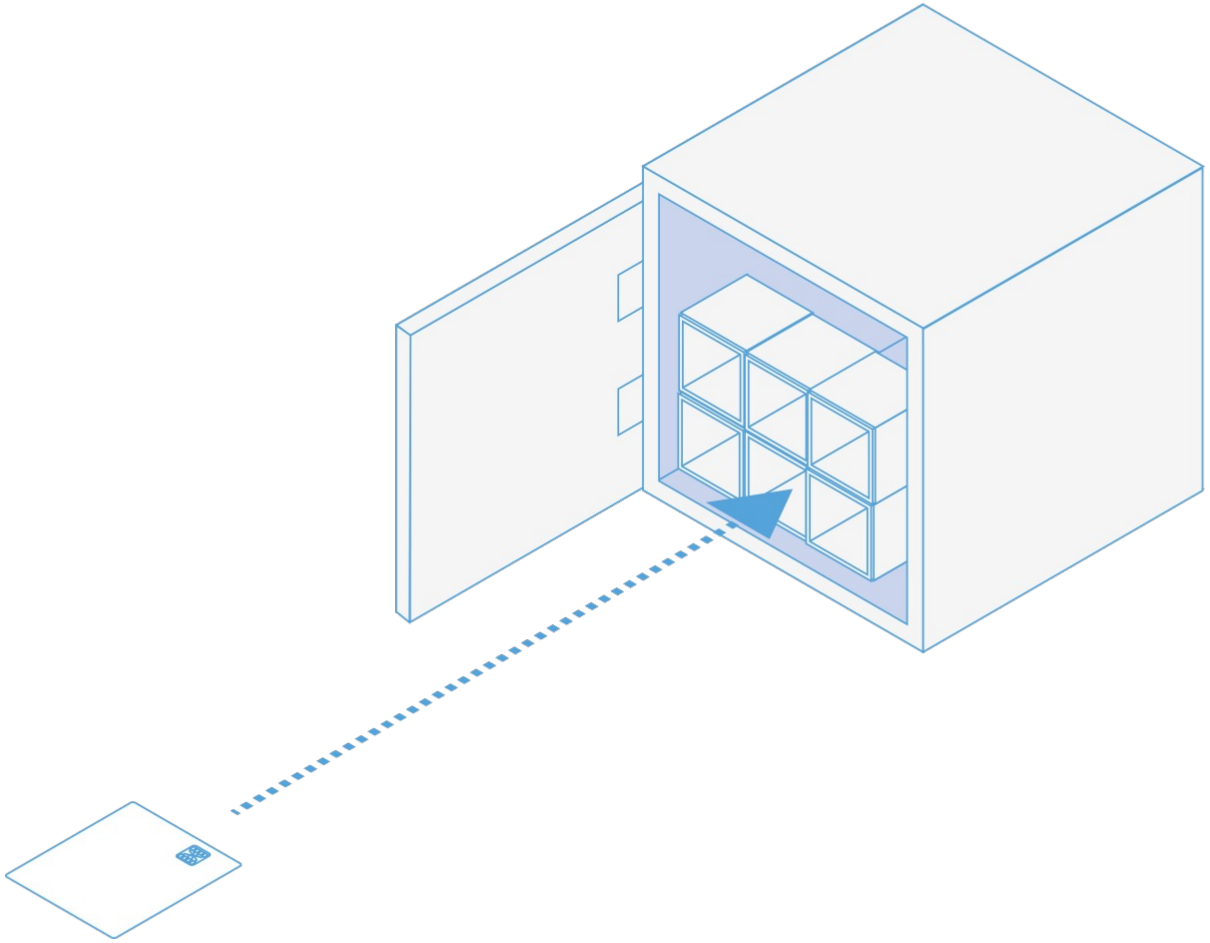
THE HSM IS STORED INSIDE A HIGH-SECURITY SAFE, WHICH CAN ONLY BE OPENED BY A DESIGNATED PERSON, THE SAFE SECURITY CONTROLLER.

THE SAFE IS MONITORED WITH SEISMIC AND OTHER SENSORS.



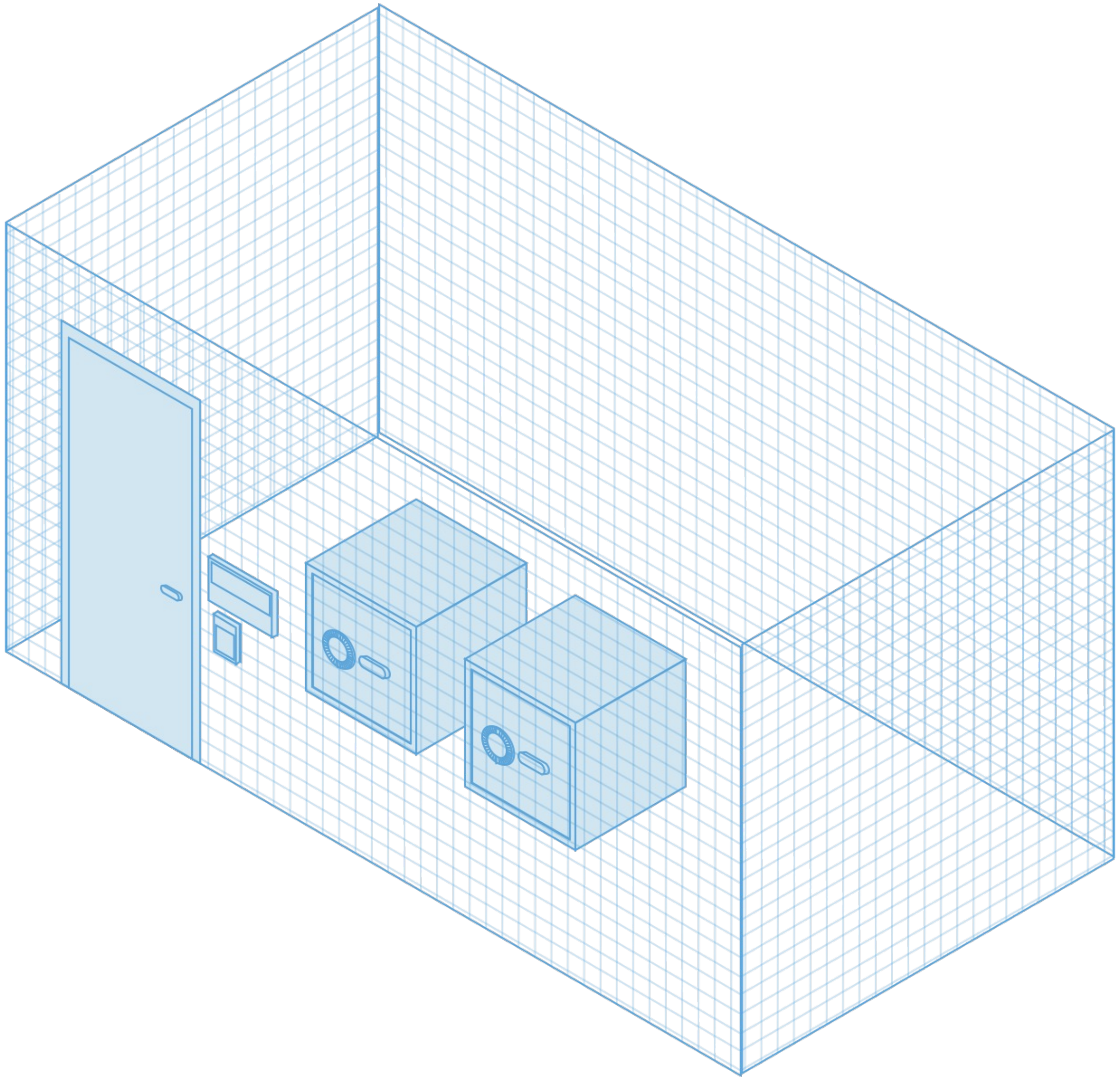
EACH TCR'S SMART CARD IS STORED IN A SECOND **CREDENTIAL SAFE** CONTAINING A SERIES OF SAFE DEPOSIT BOXES.

EACH SAFE DEPOSIT BOX IS ACCESSED USING A MECHANICAL KEY THAT THE TCR TAKES WITH THEM AND KEEPS SAFE BETWEEN CEREMONIES.



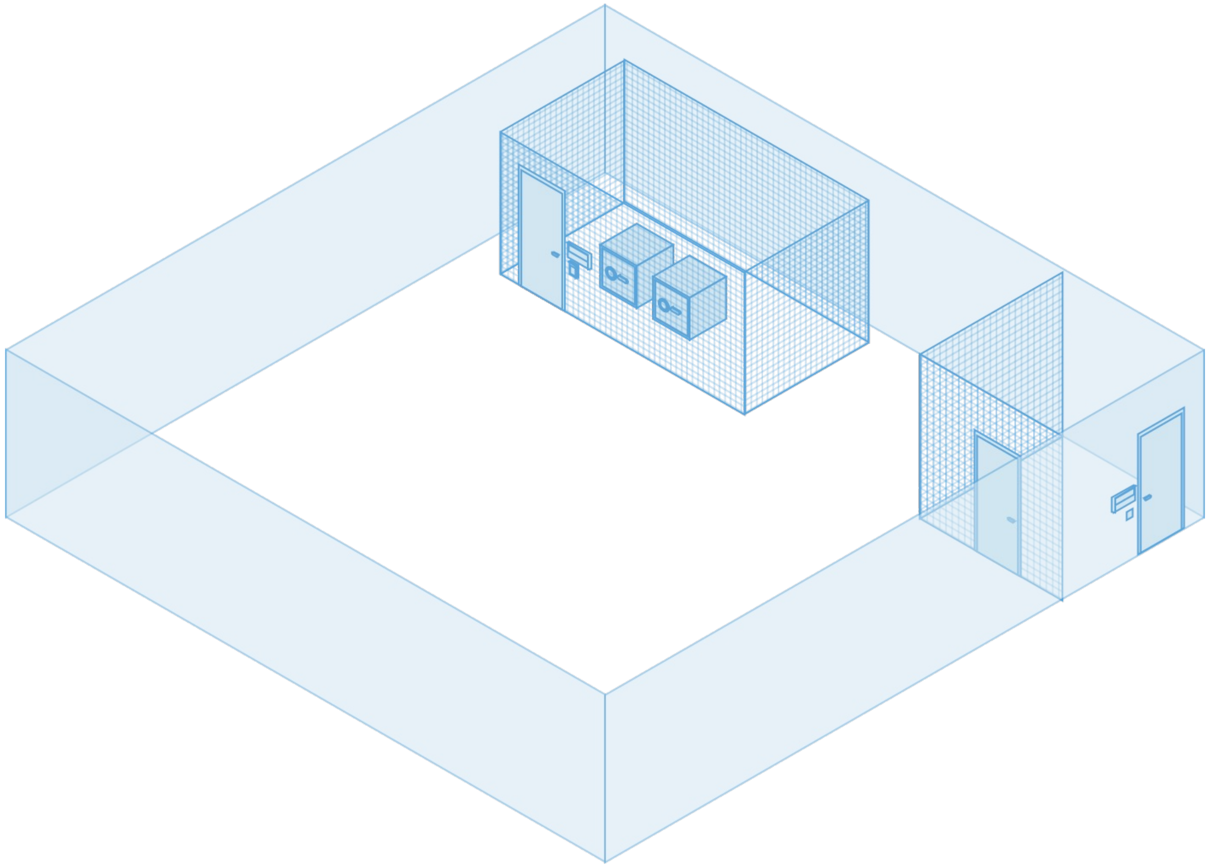
THE TWO SAFES ARE STORED IN A SECURE ROOM WHICH CAN ONLY BE OPENED JOINTLY BY TWO DESIGNATED PERSONS: THE CEREMONY ADMINISTRATOR AND THE INTERNAL WITNESS.

THE ROOM IS MONITORED WITH INTRUSION AND MOTION SENSORS.

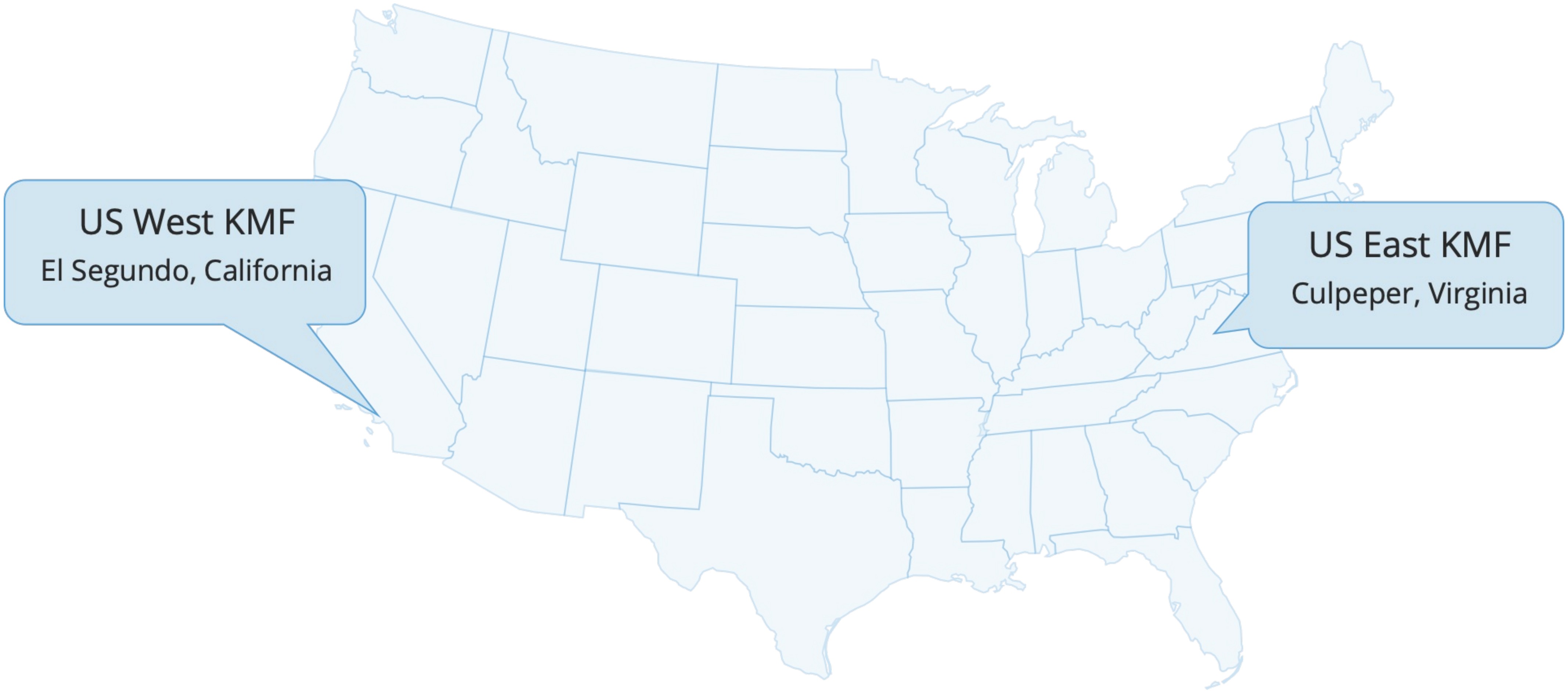


THE SAFE ROOM IS LOCATED WITHIN A LARGER ROOM WHERE CEREMONIES ARE PERFORMED INVOLVING THE TCRS AND OTHER PERSONS. CEREMONIES ARE RECORDED ON VIDEO, WITNESSED BY THE PARTICIPANTS AND OTHERS, AND AUDITED BY A THIRD-PARTY AUDIT FIRM.

ACCESS TO THE ROOM NEEDS TO BE GRANTED BY ANOTHER DESIGNED PERSON, THE **PHYSICAL ACCESS CONTROL MANAGER**, WHO IS NOT ON-SITE.



THE CEREMONY ROOMS, KNOWN AS KEY MANAGEMENT FACILITIES, ARE LOCATED WITHIN TWO GUARDED FACILITIES, ONE EACH ON THE US WEST AND EAST COASTS.

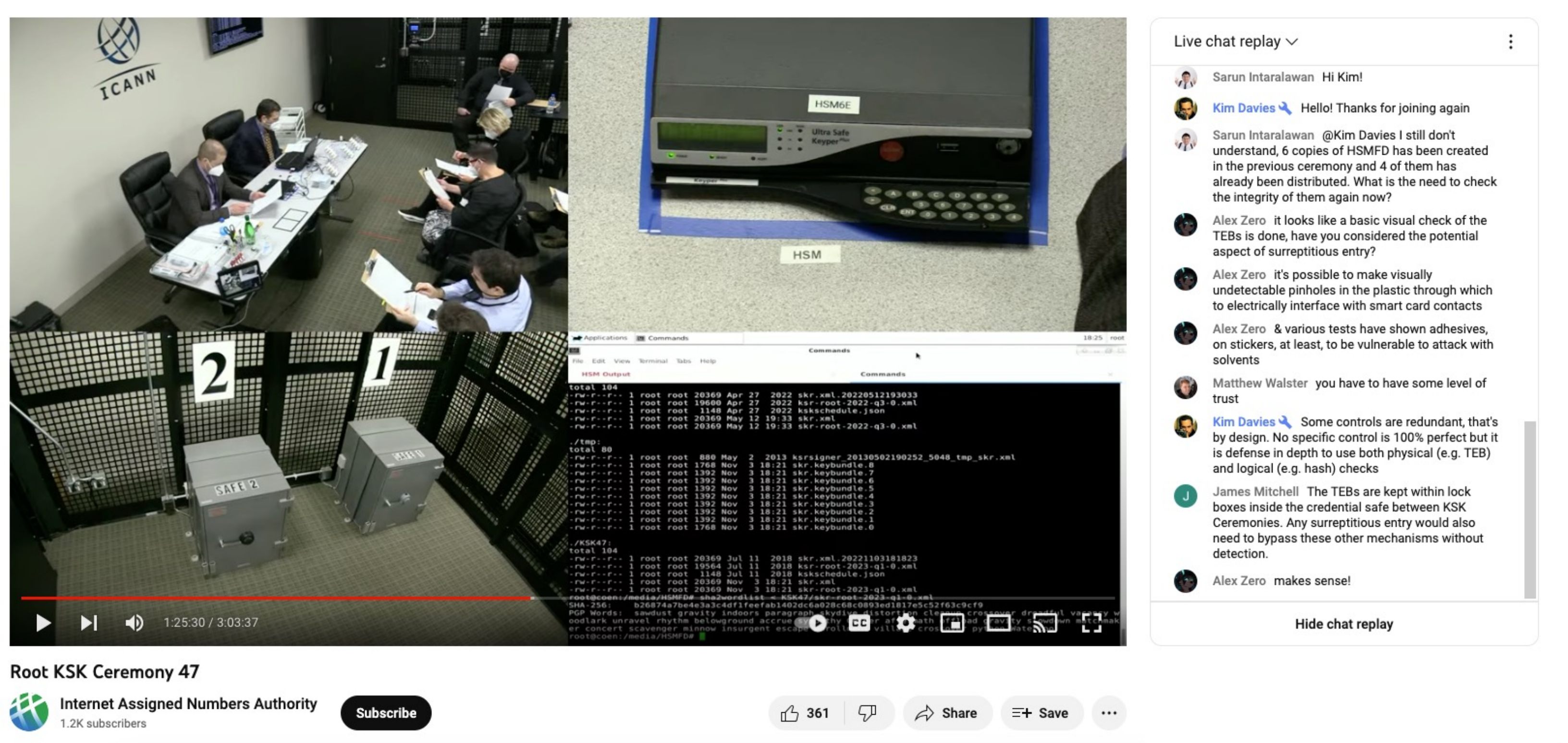


KEY CEREMONIES

APPROXIMATELY FOUR TIMES A YEAR, THE TCRS AND OTHERS MEET TO USE THE HSMS TO SIGN KEYS TO BE USED FOR THE ROOT ZONE.

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.



```
total 104
-rw-r--r-- 1 root root 20369 Apr 27  2022 skr.xml.20220512193033
-rw-r--r-- 1 root root 19600 Apr 27  2022 ksr-root-2022-q3-0.xml
-rw-r--r-- 1 root root  1148 Apr 27  2022 kskschedule.json
-rw-r--r-- 1 root root 20369 May 12 19:33 skr.xml
-rw-r--r-- 1 root root 20369 May 12 19:33 skr-root-2022-q3-0.xml

./tmp:
total 80
-rw-r--r-- 1 root root  880 May  2  2013 ksrsigner_20130502190252_5048_tmp_skr.xml
-rw-r--r-- 1 root root 1768 Nov  3 18:21 skr.keybundle.8
-rw-r--r-- 1 root root 1392 Nov  3 18:21 skr.keybundle.7
-rw-r--r-- 1 root root 1392 Nov  3 18:21 skr.keybundle.6
-rw-r--r-- 1 root root 1392 Nov  3 18:21 skr.keybundle.5
-rw-r--r-- 1 root root 1392 Nov  3 18:21 skr.keybundle.4
-rw-r--r-- 1 root root 1392 Nov  3 18:21 skr.keybundle.3
-rw-r--r-- 1 root root 1392 Nov  3 18:21 skr.keybundle.2
-rw-r--r-- 1 root root 1392 Nov  3 18:21 skr.keybundle.1
-rw-r--r-- 1 root root 1768 Nov  3 18:21 skr.keybundle.0

./KSK47:
total 104
-rw-r--r-- 1 root root 20369 Jul 11  2018 skr.xml.20221103181823
-rw-r--r-- 1 root root 19564 Jul 11  2018 ksr-root-2023-q1-0.xml
-rw-r--r-- 1 root root  1148 Jul 11  2018 kskschedule.json
-rw-r--r-- 1 root root 20369 Nov  3 18:21 skr.xml
-rw-r--r-- 1 root root 20369 Nov  3 18:21 skr-root-2023-q1-0.xml
root@coen:/media/HSMFD# sha2wordlist < KSK47/skr-root-2023-q1-0.xml
SHA-256:    b26874a7be4e3a3c4df1feefab1402dc6a028c68c0893ed1817e5c52f63c9cf9
PGP Words:  sawdust gravity indoors paragraph skydive distortion cleanup crossover dreadful vacancy w
oodlark unravel rhythm belowground accrue [illegible] [illegible] aftermath offload gravity slowdown matchmak
er concert scavenger minnow insurgent escape [illegible] villa[illegible] crossover python Waterloo
root@coen:/media/HSMFD#
```

Sarun Intaralawan Hi Kim!

Kim Davies 🔧 Hello! Thanks for joining again

Sarun Intaralawan @Kim Davies I still don't understand, 6 copies of HSMFD has been created in the previous ceremony and 4 of them has already been distributed. What is the need to check the integrity of them again now?

Alex Zero it looks like a basic visual check of the TEBs is done, have you considered the potential aspect of surreptitious entry?

Alex Zero it's possible to make visually undetectable pinholes in the plastic through which to electrically interface with smart card contacts

Alex Zero & various tests have shown adhesives, on stickers, at least, to be vulnerable to attack with solvents

Matthew Walster you have to have some level of trust

Kim Davies 🔧 Some controls are redundant, that's by design. No specific control is 100% perfect but it is defense in depth to use both physical (e.g. TEB) and logical (e.g. hash) checks

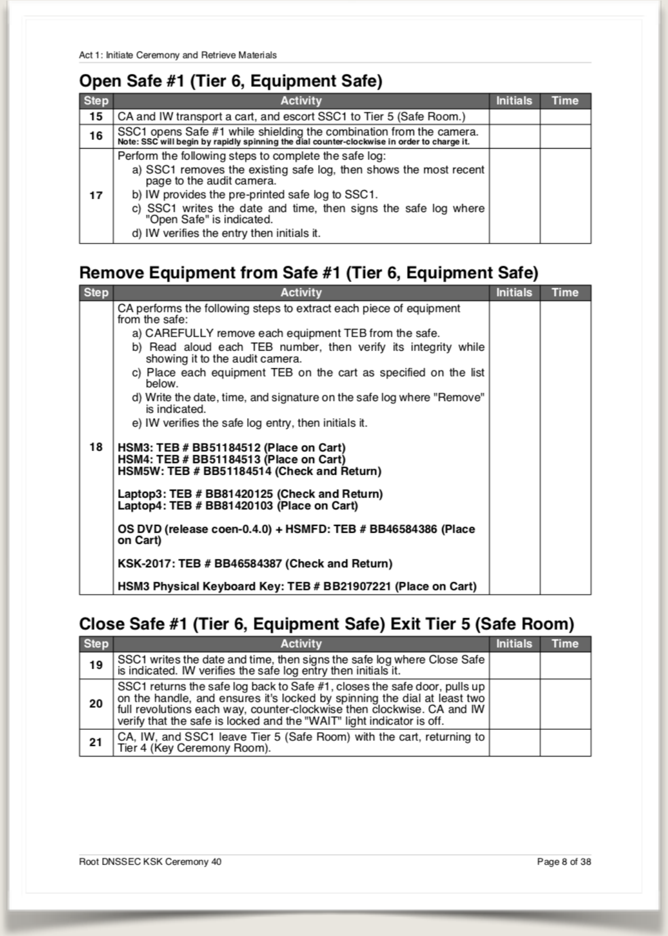
James Mitchell The TEBs are kept within lock boxes inside the credential safe between KSK Ceremonies. Any surreptitious entry would also need to bypass these other mechanisms without detection.

Alex Zero makes sense!

Root KSK Ceremony 47

Internet Assigned Numbers Authority
1.2K subscribers

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.		

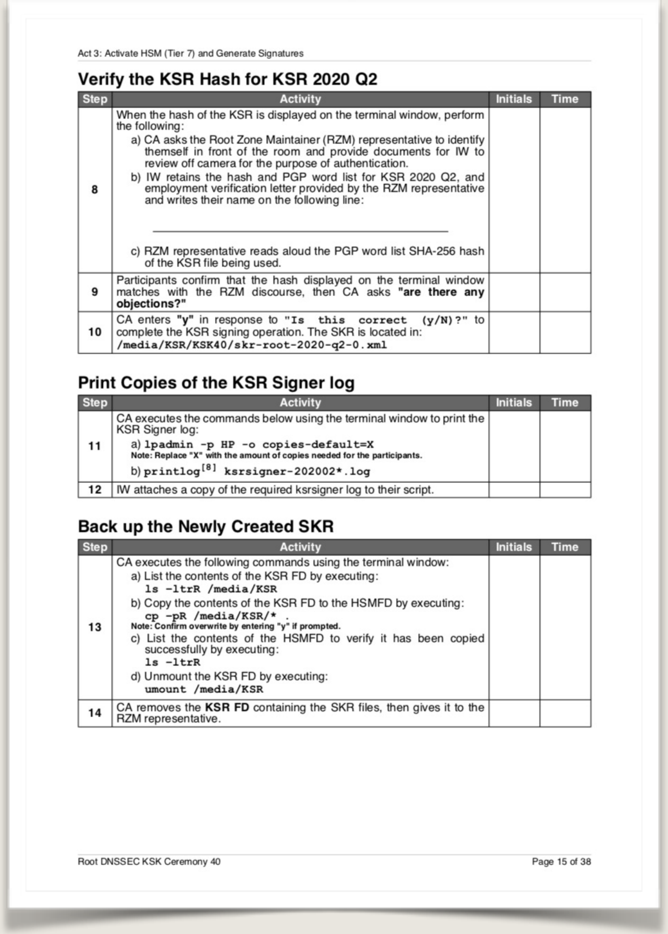
Remove Equipment from Safe #1 (Tier 6, Equipment Safe)

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.		

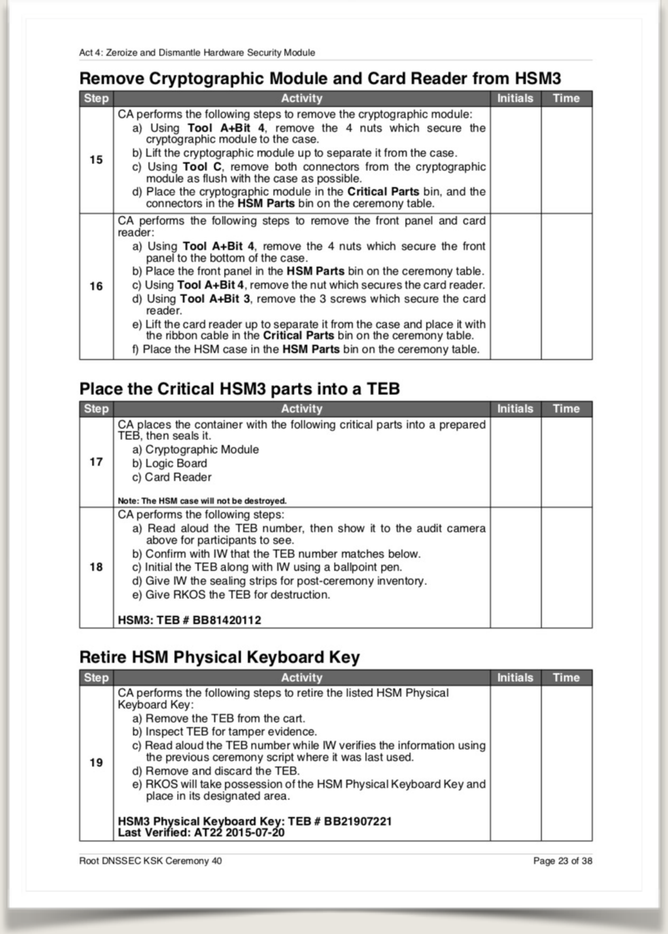
Back up the Newly Created SKR

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

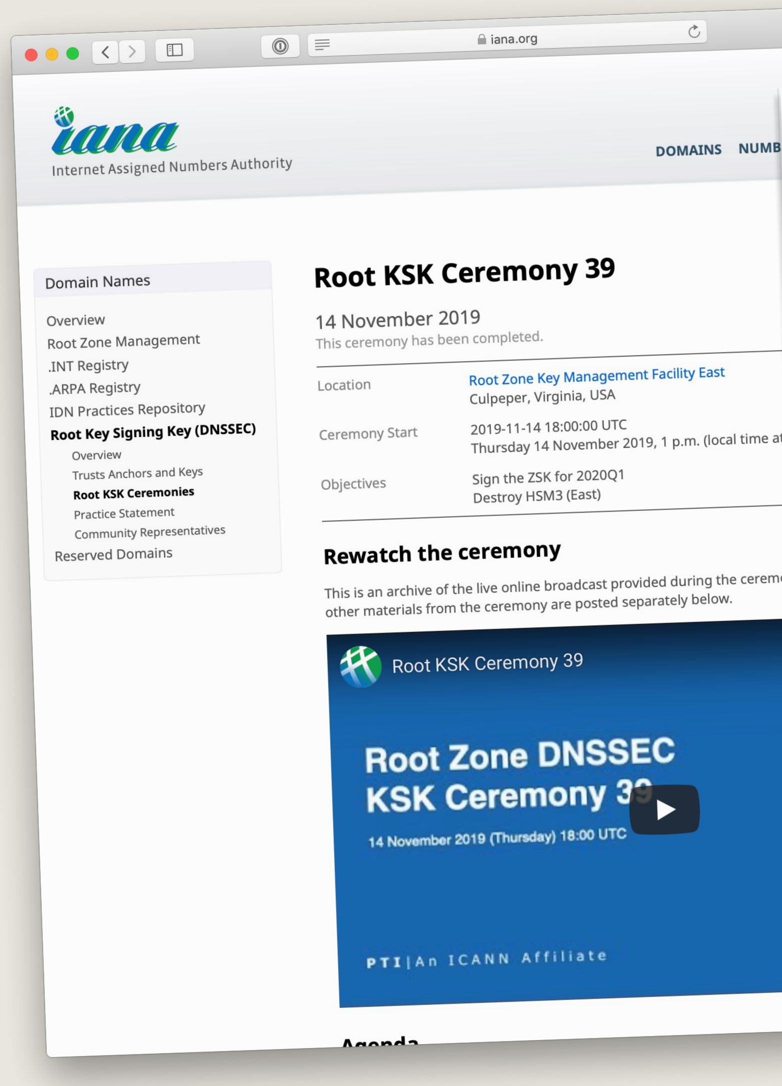
Step	Activity	Initials	Time
17	CA places the container with the following critical parts into a prepared TEB, then seals it. a) Cryptographic Module b) Logic Board c) Card Reader **Note: The HSM case will not be destroyed.**		
18	CA performs the following steps: a) Read aloud the TEB number, then show 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

THE PROCESS IS STREAMED AND RECORDED, WITH EXTERNAL WITNESSES WATCHING EVERY STEP. ALL MATERIALS (VIDEOS, CODE, SCRIPTS, ETC.) ARE POSTED ONLINE.



Root KSK Ceremony 39

14 November 2019

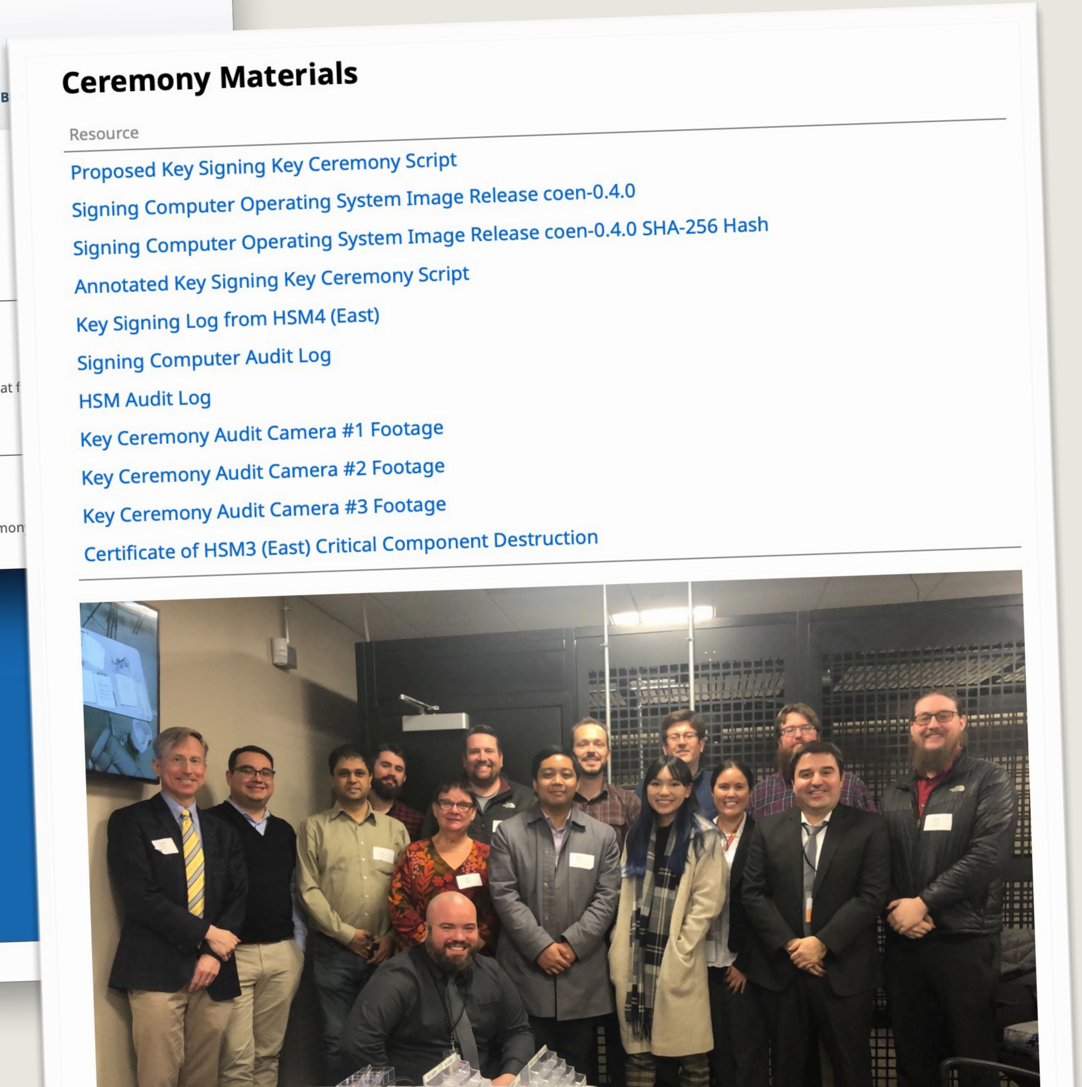
This ceremony has been completed.

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 at f
Objectives	Sign the ZSK for 2020Q1 Destroy HSM3 (East)

Rewatch the ceremony

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

Agenda



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

THANK YOU

David.Huberman@icann.org