Root Zone KSK ceremony

CSNOG 2023

Ondřej Filip • 17.5.2023

CZ.NIC | SPRÁVCE DOMÉNY CZ

DNS, DNSSEC, root zone

- Many TLDs signed before DNS root zone
- DNSSEC Lookaside Validation (DLV) – the most used one by ISC
- Long discussion about a process of signing root zone – roles KSK, ZSK, …
- DNS Root zone signed in 2010 – KSK managed by ICANN/IANA (PTI), ZSK managed by Verisign (a.root-servers.net)
- IANA chose two locations – Culpeper, VA (Washington DC) and El Segundo, CA (Los Angeles)
- 27 volunteers from technical community – TCRs – 3 teams

People involved in KSK ceremonies

- 2x 7 COs, 7 RKSHs - https://www.iana.org/dnssec/tcrs
- 4 ceremonies a year – East coast / West coast alternation
- At least 3 COs per ceremony
- All video recorded

Abbreviations

AUD	= Third Party Auditor	**CA**	= Ceremony Administrator	**CO**	= Crypto Officer
EW	= External Witness	**FD**	= Flash Drive	**HSM**	= Hardware Security Module
IW	= Internal Witness	**KMF**	= Key Management Facility	**KSR**	= Key Signing Request
OP	= Operator	**PTI**	= Public Technical Identifiers	**RKSH**	= Recovery Key Share Holder
RKOS	= RZ KSK Operations Security	**RZM**	= Root Zone Maintainer	**SA**	= System Administrator
SKR	= Signed Key Response	**SMK**	= Storage Master Key	**SO**	= Security Officer
SSC	= Safe Security Controller	**SW**	= Staff Witness	**TCR**	= Trusted Community Representative

TEB = Tamper Evident Bag (AMPAC: #GCS1013, #GCS0912, #GCS1216 or MMF Industries: #2362010N20, #2362011N20)

Title / Roles	Printed Name	Signature	Date	Time
CA	Matthew Larson / ICANN			
IW	Patrick Jones / ICANN			
SSC1	Fernanda Iunes / ICANN			
SSC2	Carlos Reyes / ICANN			
CO1	Frederico Neves			
CO3	Ondrej Filip			
~~CO4~~	~~Robert Seastrom~~			
CO6 Current	Gaurab Upadhaya			
CO6 Successor	Hugo Salgado			
CO7	Dileepa Lathsara			
RZM	Trevor Davis / Verisign			
AUD	John Leonard / RSM		2023 Apr 27	
AUD	Emmanuel Nkereuwem / RSM			
~~SA~~	~~Moises Cirilo / ICANN~~			
SA	Darren Kara / ICANN			
RKOS / CA Backup	Andres Pavez / PTI			
RKOS / IW Backup	Aaron Foley / PTI			
SW	Danielle Rutherford / ICANN			
SW	Isabella Reber / ICANN			
EW	Mimi Rauschendorf			
EW	Bob Arasmith			

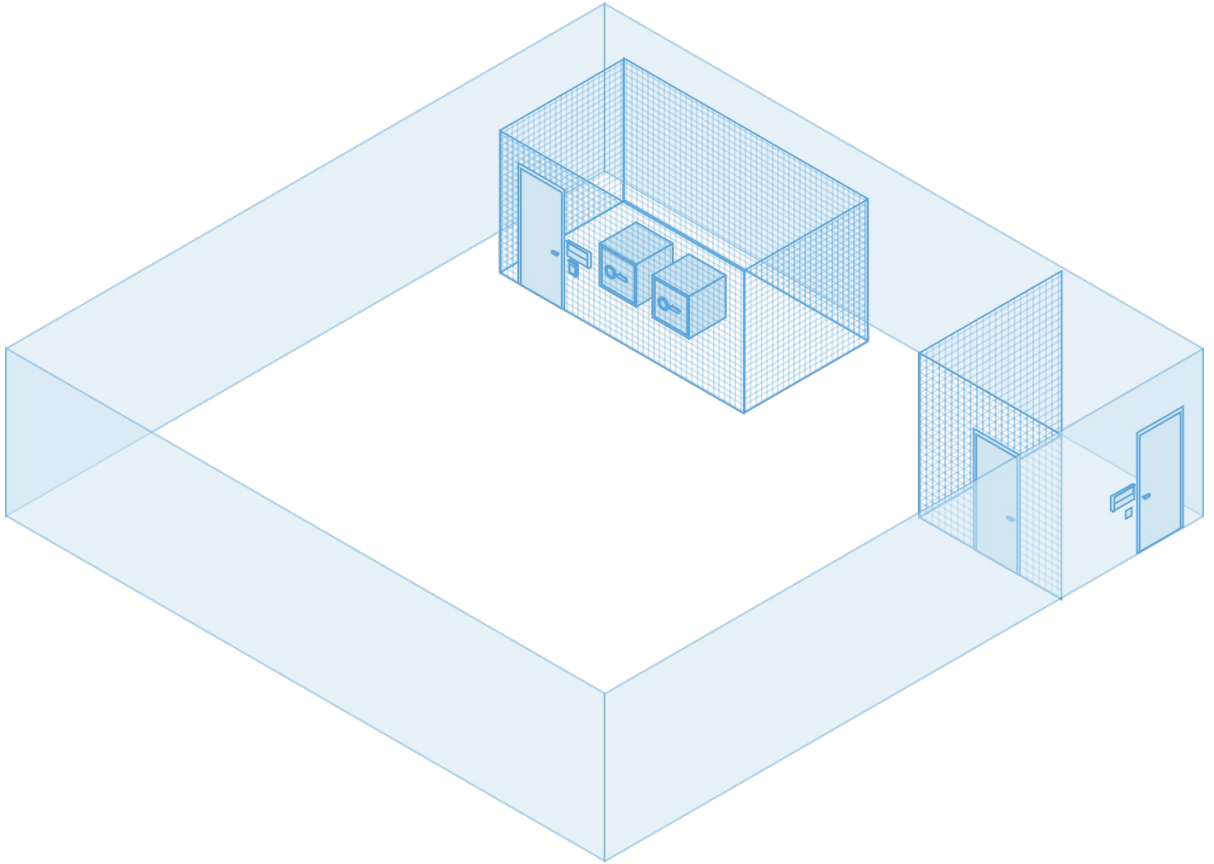
Ceremony room

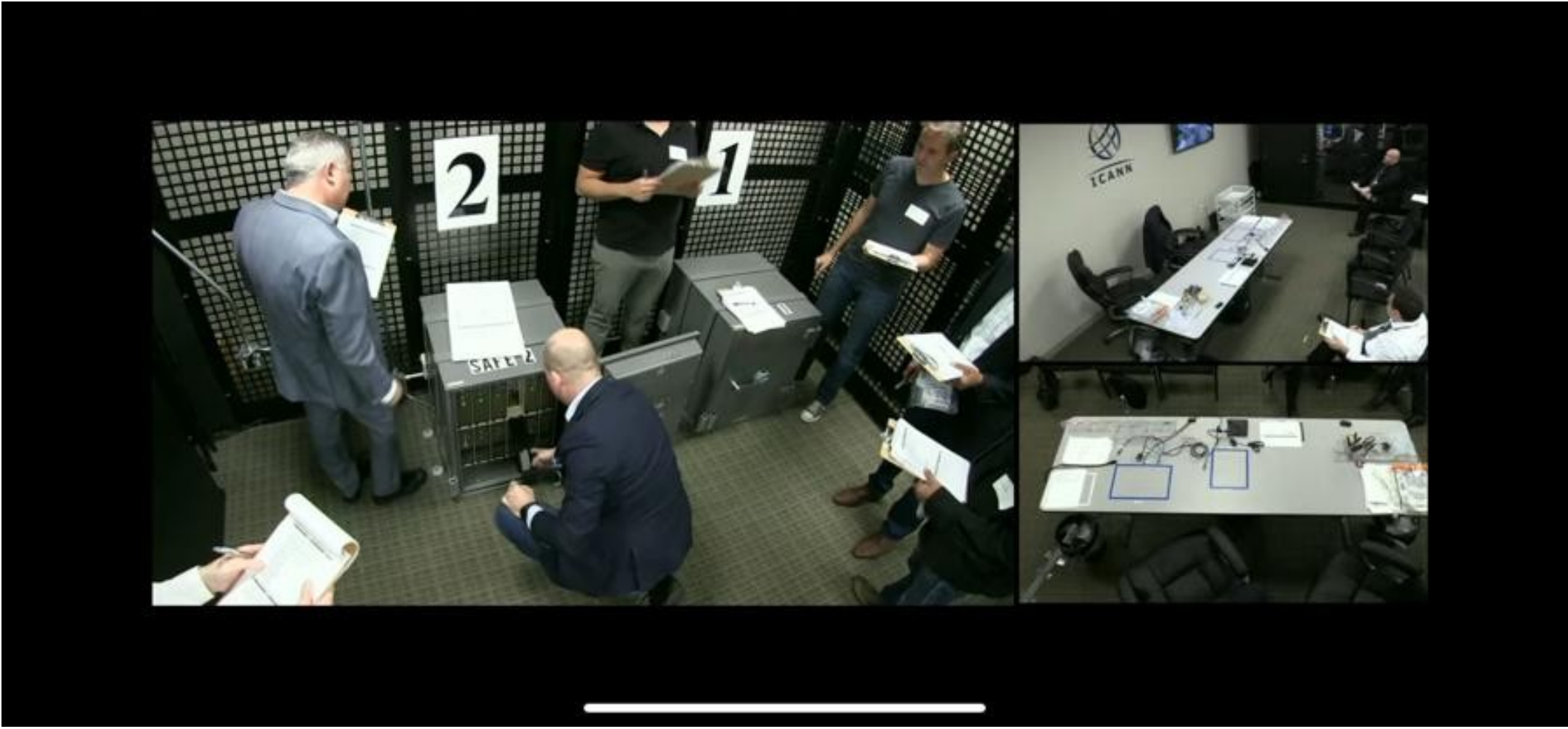
Key ceremony room – Tier – 4

Safe room – Tier – 5

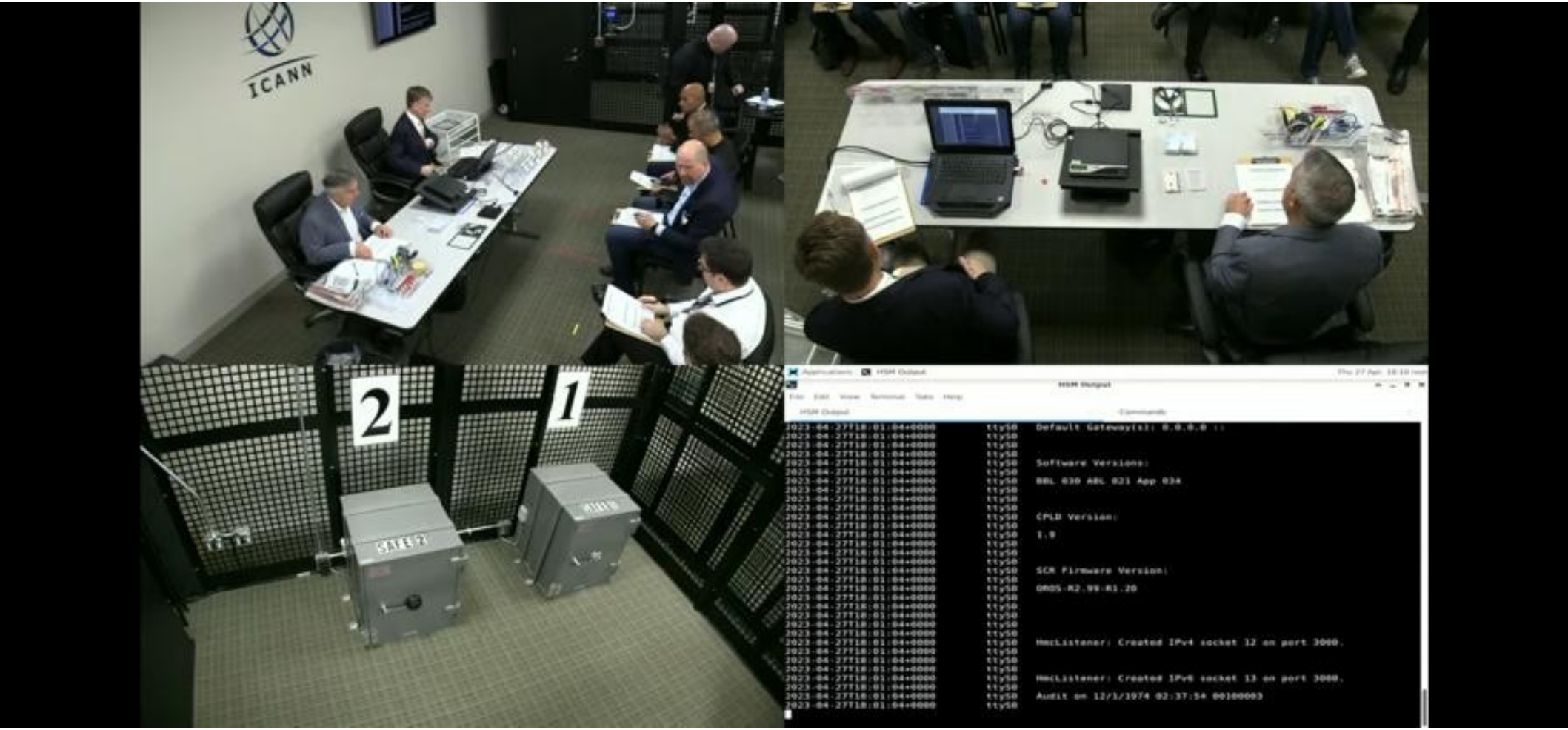
Equipment and credential safes – Tier – 6

Deposit boxes – Tier - 7




2
1
ICANN


2
1
SAFE 2
ICANN


ICANN
2
1
HSM Output
Default Gateway(s): 0.0.0.0
Software Versions:
BBL 030 ABL 021 App 034
CPLD Version:
1.9
SCR Firmware Version:
OMOS-R2.99-R1.20
HmcListener: Created IPv4 socket 12 on port 3000.
HmcListener: Created IPv6 socket 13 on port 3000.
Audit on 12/1/1974 02:37:54 00100003

KSKs

- KSK-45
  - May 22 2022, 14 people, 6 hrs, Script 54 (131) pages
  - Reissue CO Cards, Destroy HSM4 (East), Replace 2 TCRs (CO3 – me and RKSH7)
- KSK-49
  - April 27, 2023, 19, people, 3.5 hrs, Sript 44 (83) pages
  - Replace TCR (CO6), Generate new KSK, OS media change DVD->SD)

KSK ceremonies

- Very robust process
- Very detailed planning (script in advance)
- Every small detail minuted – exceptions etc.
- Extreme level of transparency – cameras, software images, logs, … - check https://www.iana.org/dnssec/ceremonies

- Trust

My journey to CO3 East

- Call for volunteers (2010)
- Invited to ceremony #2 (West Coast) as External Witness

After „a while“

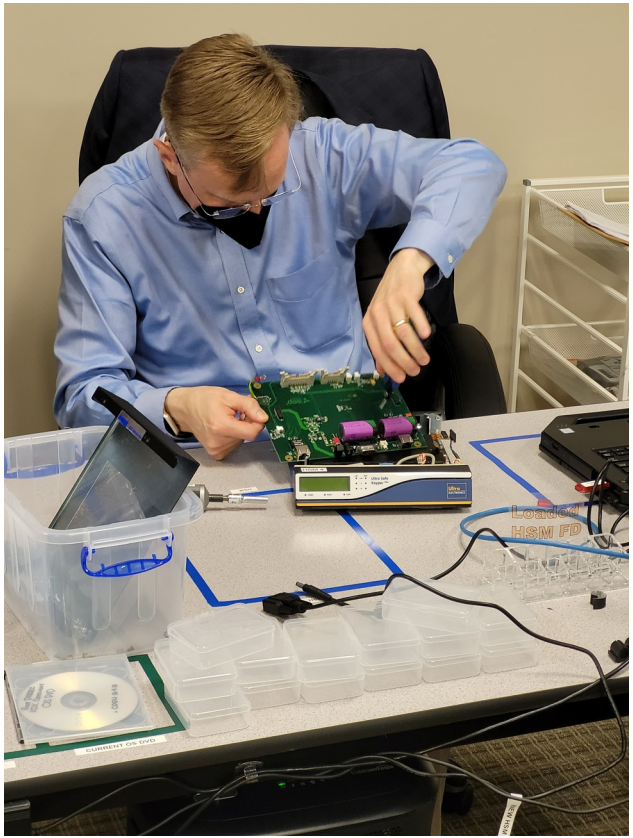
- November 2018 – informed that I am one of candidates for Backup TCR – background check
- September 2019 – selected as Backup TCR
- February 2020 – informed to be selected as a replacement of one TCR – planned for KSK-41 (April) – didn’t happen due to pandemic
- May 2022 – KSK-45 - Culpeper, Virginia, USA – finally possible to travel

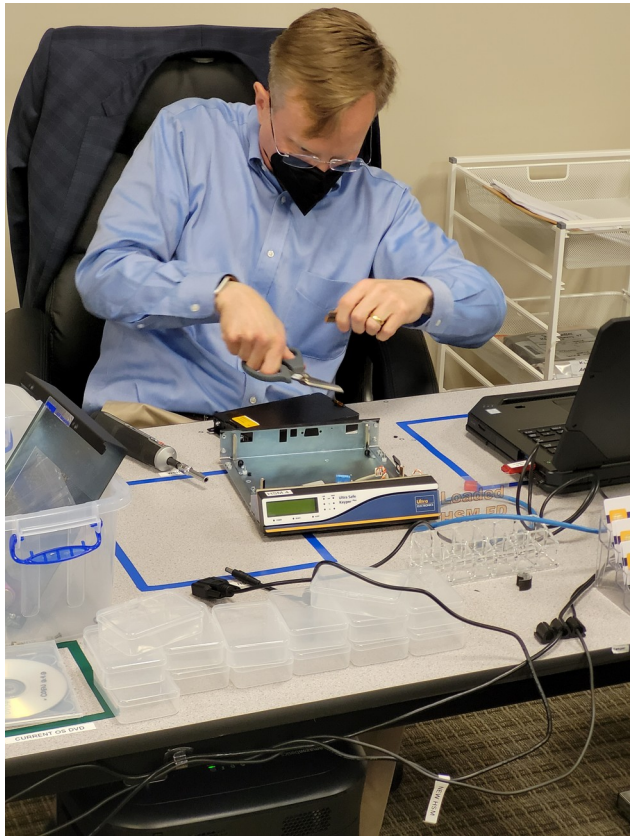
KSK-45

Do you wanna be TCR?

- Integrity, objectivity, reputation
- Understanding DNS and DNSSEC
- Represent the broadest cultural and geographic diversity
- Familiar with: the operation of TLD registries and registrars; IP address registries; Internet technical standards and protocols; policy development procedures, legal traditions and the public interest; and the broad range of business, individual, academic and non-commercial users of the Internet;
- Volunteer, English, No affiliation with PTI, ICANN or Verisign

And some fun :-)





Open the HSM Case and Remove the Logic Board from HSM4

Step	Activity	Initials	Time
20	IW reads steps 21 to 24 aloud while the CA dismantles **HSM4: Serial # H1411011**.		20:57
21	CA performs the following steps to access the HSM's critical components: a) Using **Tool A+Bit 2**, remove the two screws securing the serial port to the rear panel. b) Using **Tool A+Bit 1**, remove the four screws from the rear panel of the case securing the shell. c) Using **Tool A+Bit 1**, remove the four screws from the bottom of the case securing the shell. d) Using **Tool C**, slice the tamper stickers on the bottom of the case along the seam with the shell. e) Slide the shell toward the back of the case to remove it and place it in the **HSM Parts** bin on the ceremony table. f) Using **Tool A+Bit 3**, remove the two logic board screws nearest to the front panel securing the plastic logic board cover. g) Remove the plastic logic board cover and place it in the **HSM Parts** bin on the ceremony table. h) Using **Tool A+Bit 3**, remove the two remaining screws securing the logic board near the rear panel. i) Detach the four cables from the front of the logic board. Open the latches outward to release each of the ribbon cables. j) Using **Tool A+Bit 4**, remove the nut from the cryptographic module securing the ring terminal of the green/yellow wire and slide the ring terminal off of the threaded stud. k) Detach the cable from each side of the cryptographic module connecting it to the logic board.		21:00

Thank you!

Ondřej Filip

CZ.NIC | SPRÁVCE DOMÉNY CZ