The Key Management Facility of the Root Zone DNSSEC Key Signing Key (KSK)

Punky Duero

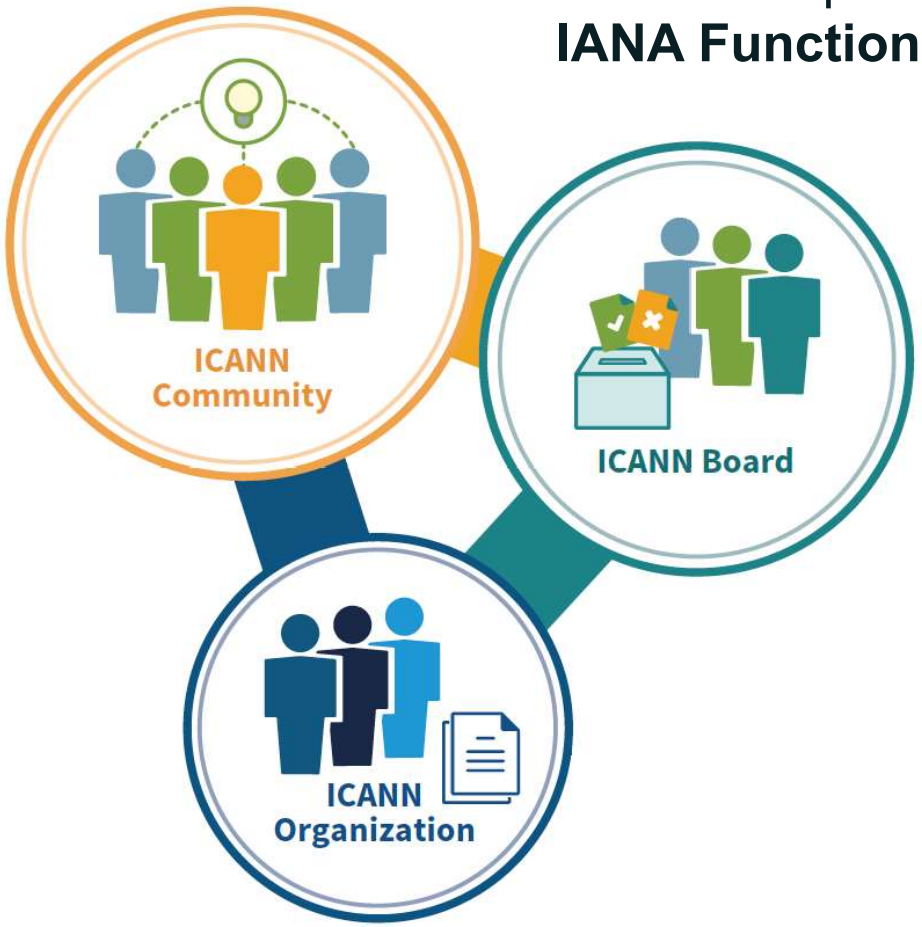
DEF CON 25 – CRYPTO & PRIVACY VILLAGE

30 July 2017

ICANN | IANA Functions

What is ICANN?

Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the top-level of the Internet's system of unique identifiers via global, multistakeholder, bottom-up consensus policy process, which is implemented via the **IANA Functions**



Internet Assigned Numbers Authority (**IANA**) **Functions**

- Protocol Parameters
- Number Resources
- Domain Name

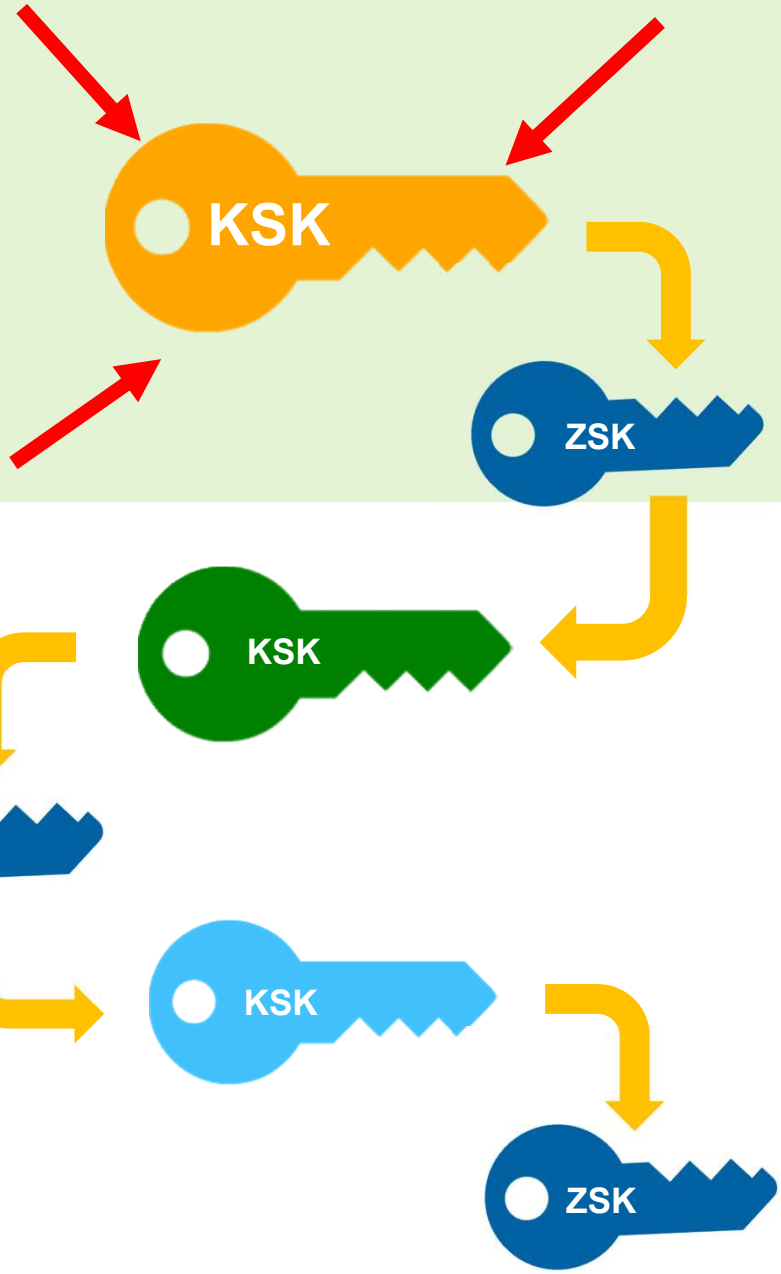
Agenda

1. Root Zone DNSSEC KSK Rollover
2. Key Management Facility
3. **The Key Ceremony**

Root Zone DNSSEC KSK Rollover

Root Zone DNSSEC KSK

The Root Zone DNSSEC Key Signing Key "**KSK**" is the top most cryptographic key in the DNSSEC hierarchy



DNSSEC = **"DNS Security Extensions"**

DNSSEC is a protocol that is currently being deployed to secure the Domain Name System (DNS)

Root Zone DNSSEC KSK Rollover

RSA-2048

Old Key called **KSK-2017**
(Operational)

RSA-2048

New Key called **KSK-2017**

Root Zone DNSSEC KSK – KSK-2017

```
. IN DNSKEY  257 3 8
     AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
     +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
     ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
     0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
     oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
     RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
     R1AkUTV74bU=
```

How To Update Your System

If your software supports automated updates of DNSSEC trust anchors (RFC 5011):

- The KSK will be updated automatically at the appropriate time
- You do not need to take additional action
  - Devices that are offline during the rollover will have to be updated manually if they are brought online after the rollover is finished

If your software does <u>not</u> support automated updates of DNSSEC trust anchors (RFC 5011) or is not configured to use it:

- The software's trust anchor file must be manually updated
- The new root zone KSK is now available here after March 2017:

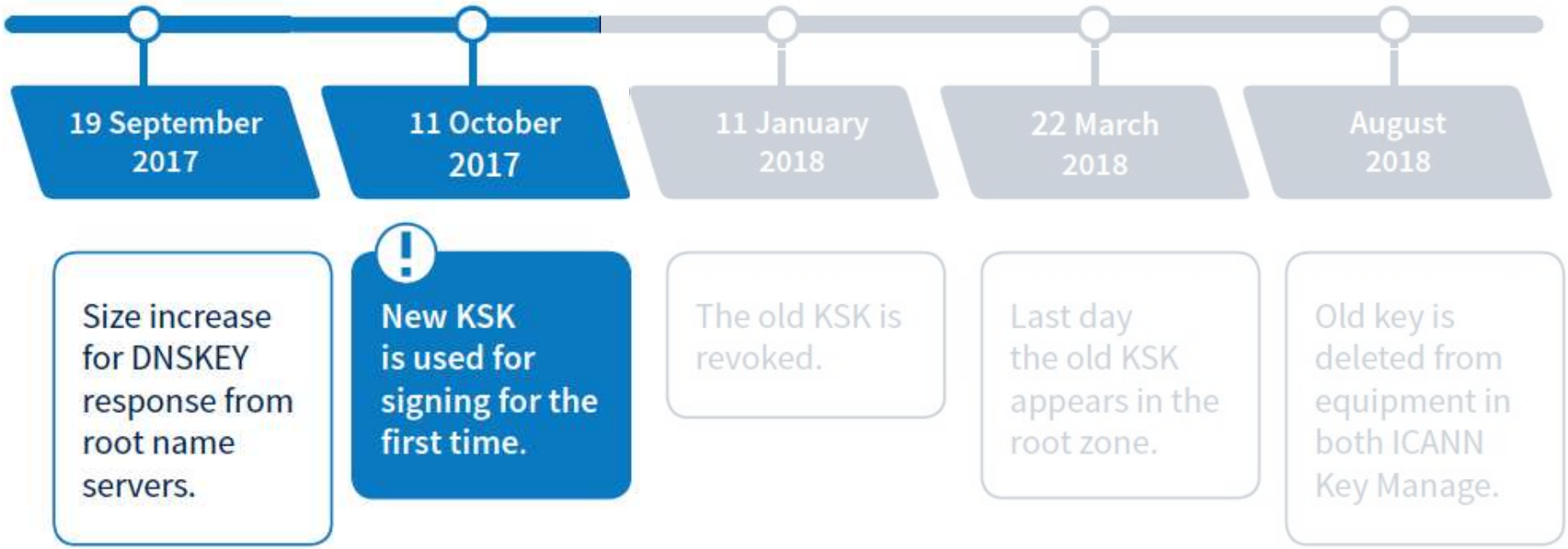
Root Anchors ▶

data.iana.org/root-anchors

When Does the Rollover Take Place?

The KSK rollover is a process, not a single event

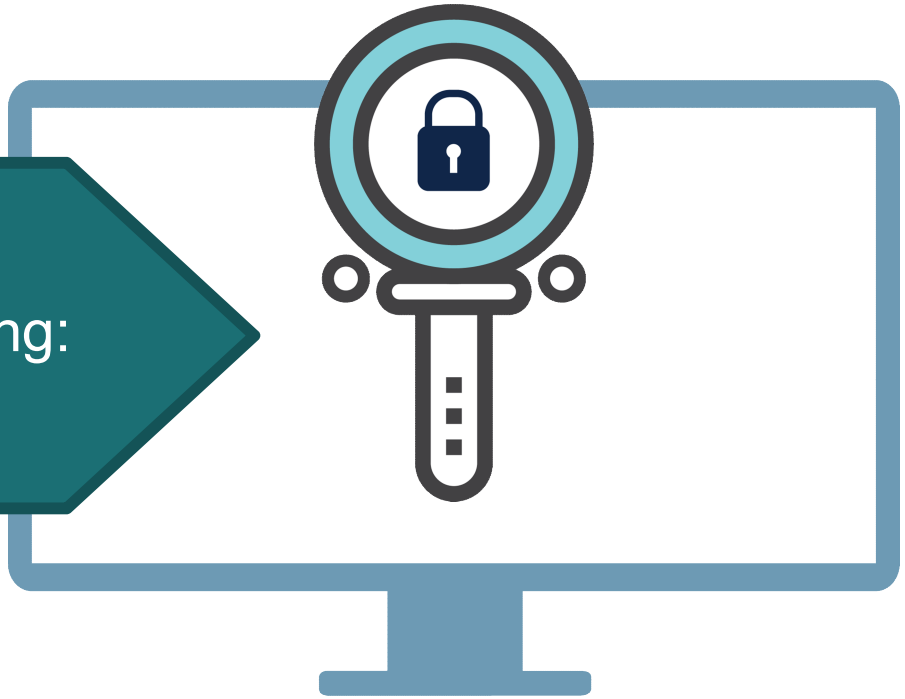
The following dates are key milestones in the process when end users may experience interruption in Internet services:



Check to See If Your Systems Are Ready

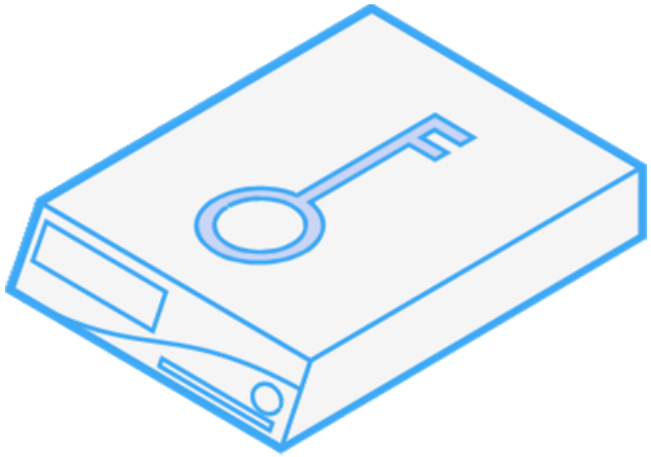
ICANN is offering a **test bed** for operators or any interested parties to confirm that their systems handle the automated update process correctly.

Check to make sure
your systems are ready by visiting:
go.icann.org/KSKtest



Where is the Root Zone DNSSEC KSK?

Hardware Security Module (HSM)



FIPS 140-2 Level 4 Certified

Photo: www.dj.cx

- Private Key for KSK-2010
- Private Key for KSK-2017

Smart Cards

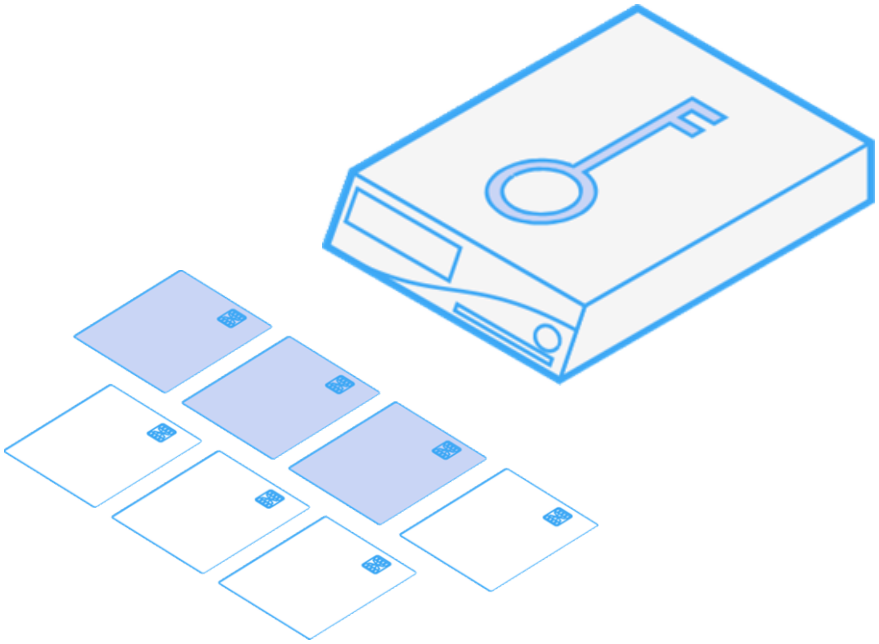
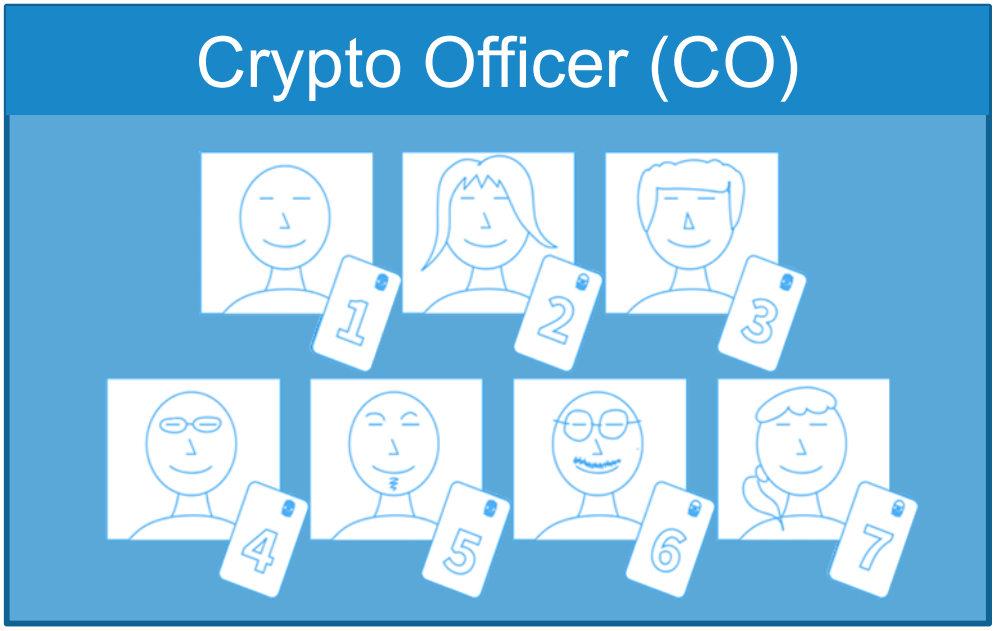


Photo: www.dj.cx

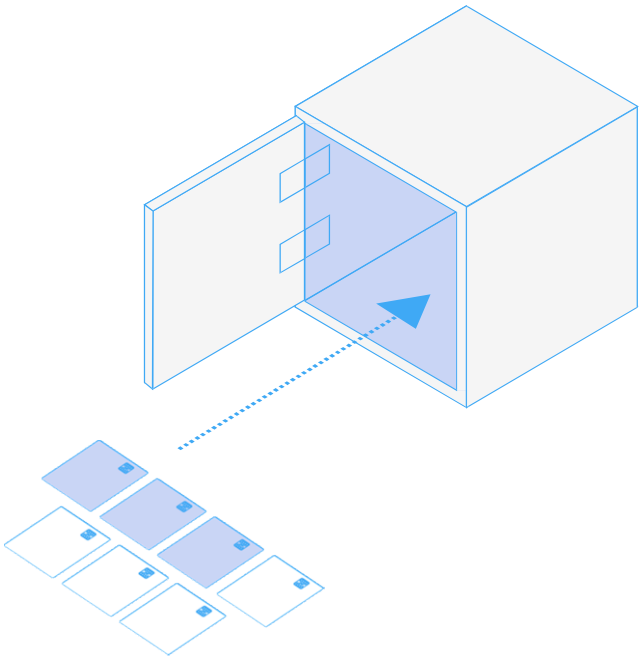
Trusted Community Representative (TCR)



Each smart card is assigned to different community members, known as **Trusted Community Representatives**

Photo by Kim Davies

Safe # 2 – Credential Safe



Smart Cards

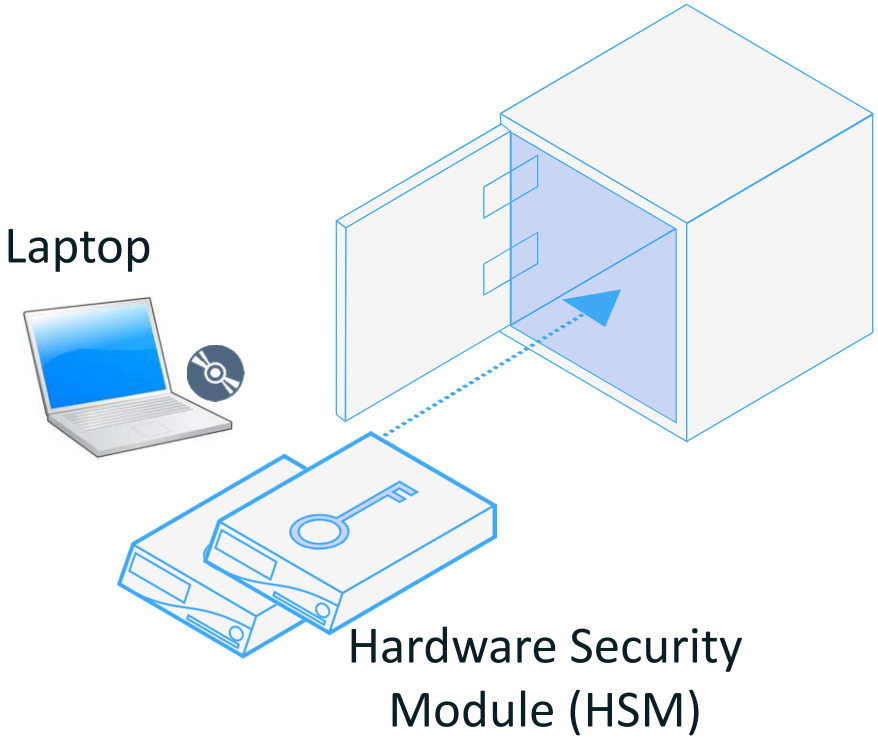
Photo: Olaf Kolkman

Photo: www.dj.cx

Can only be opened by a designated staff,
Credential Safe Controller

Safe #1 – Hardware Safe

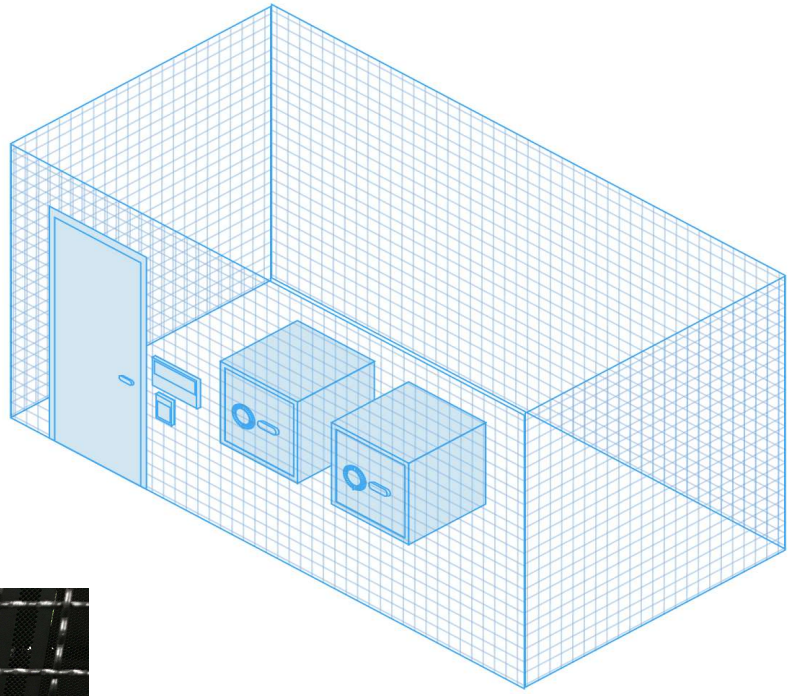
Photo: www.dj.cx



Can only be opened by a designated staff,
Hardware Safe Controller

Safe Room

Photo: www.dj.cx



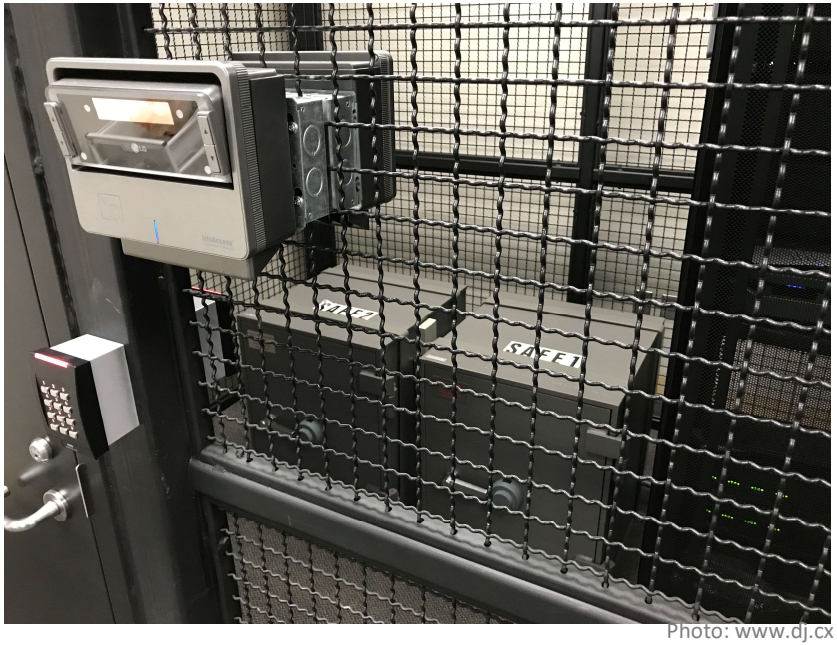
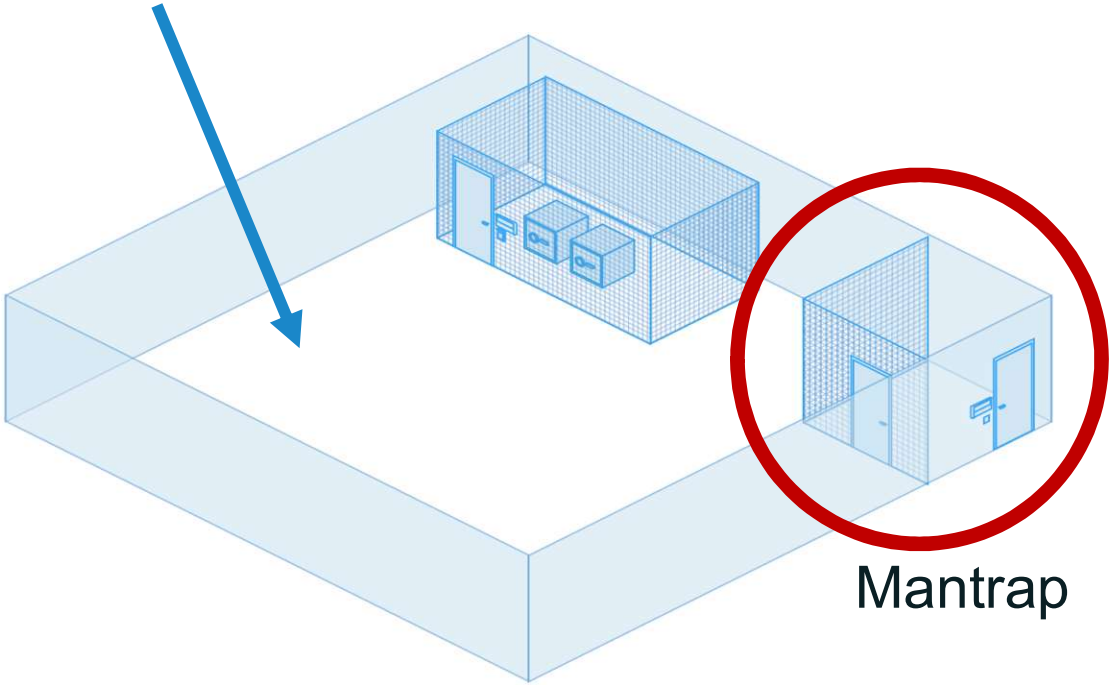


Photo: www.dj.cx

Photo: Kim Davies

Ceremony Room

Photo: www.dj.cx



Key Ceremonies

~~Team Ceremony~~ Key Ceremony

~~Tea Ceremony~~

Not like this Ceremony

Key Ceremony

Root DNSSEC KSK Ceremony 27

Act 1. Initiate Ceremony and Retrieve Equipments

Participants Arrive and Sign into Key Ceremony Room

Step	Activity	Initials	Time
1.	CA confirms with SA that all audit cameras are recording and online streaming is live.	PS	1702
2.	CA confirms that all participants are signed into the Ceremony Room and performs a roll call using the list of participants on Page 2.	PS	1704

Emergency Evacuation Procedures and Electronics Policy

Step	Activity	Initials	Time
3.	CA reviews emergency evacuation procedures with participants.	PS	1704
4.	CA explains the use of personal electronics devices during ceremony.	PS	1705
5.	CA briefly explains the purpose of the ceremony.	PS	1707

Verify Time and Date

Step	Activity	Initials	Time
6.	IW1 enters UTC date (year/month/day) and time using a reasonably accurate clock visible to all in the Ceremony Room: Date and time: 2016/10/27 1707:39 All entries into this script or any logs should follow this common source of time.	PS	17:07

Open Credential Safe #2

Step	Activity	Initials	Time
7.	CA and IW1 escorts SSC2, COs into the safe room together. CA brings a flashlight when entering the safe room.	PS	17:09
8.	SSC2, while shielding combination from camera, opens Safe #2.	PS	17:10
9.	SSC2 takes out the existing safe log and shows the most current page to the camera. IW1 provides a blank pre-printed safe log to the SSC2. SSC2 appends the new safe log then prints name, date, time, signature, and reason (i.e. "open safe") in the safe log. IW1 initials this entry. **Note: If log entry is pre-printed, verify the entry, record time of completion and sign.**	PS	17:11

Photo by Kim Davies

Key Signing Ceremony

Trusted Community Representatives
Enable the HSMs

Ceremony Administrator
Performs the Ceremony using scripts

Internal Witness
Attests the ceremony, signs affidavit

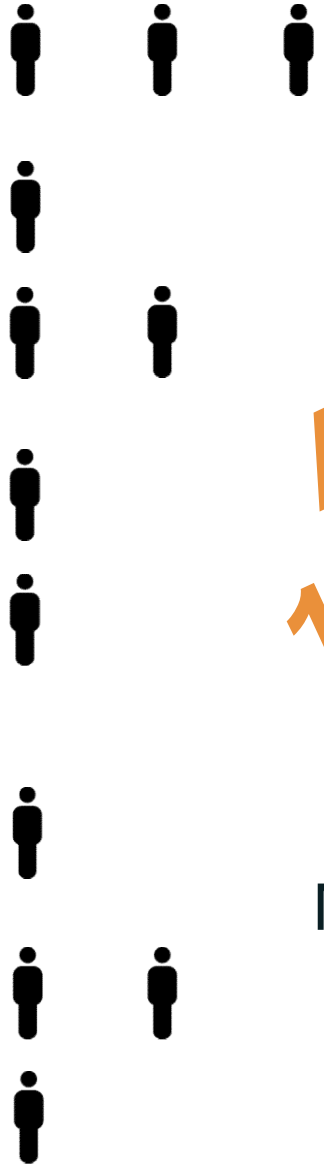
Hardware Safe Controller
Opens Safe #1

Credential Safe Controller
Opens Safe #2

System Administrator
Technical Support and Evidence Collection

Third-Party Auditors
Observe and Attest

Root Zone Management Partner
Bring Key Signing Request



At least 12 people!

Minimum Participants

Where is the Key Management Facility?

Key Management Facility (KMF)

US West KMF
El Segundo, California

US East KMF
Culpeper, Virginia

2016

January						
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Q1 February						
Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29					

March						
Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

April						
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Q2 May						
Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

June						
Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

July						
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Q3 August						
Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Septem						
Su	Mo	Tu	We	Th	Fr	Sa
				1	2	
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Q4 October						
Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

November						
Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

December						
Su	Mo	Tu	We	Th	Fr	Sa
					2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Trusted Community Representatives (TCRs)

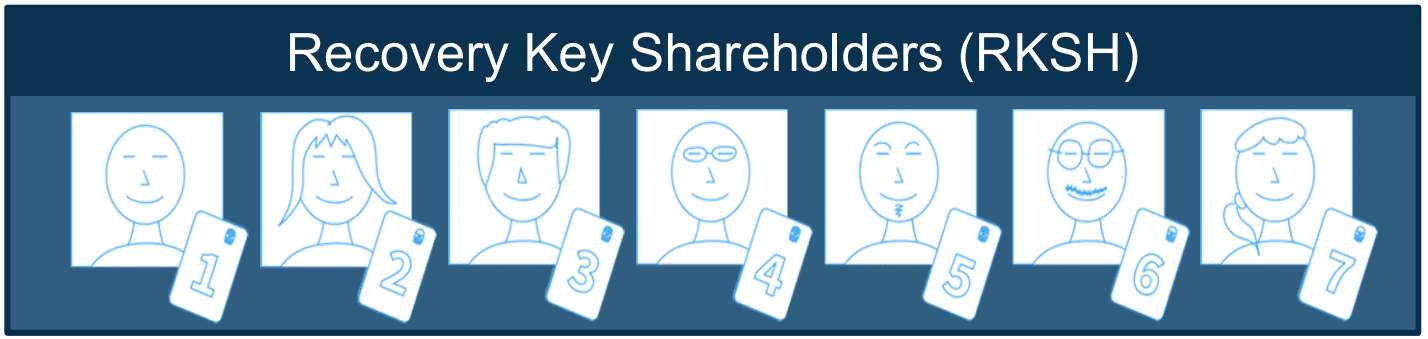
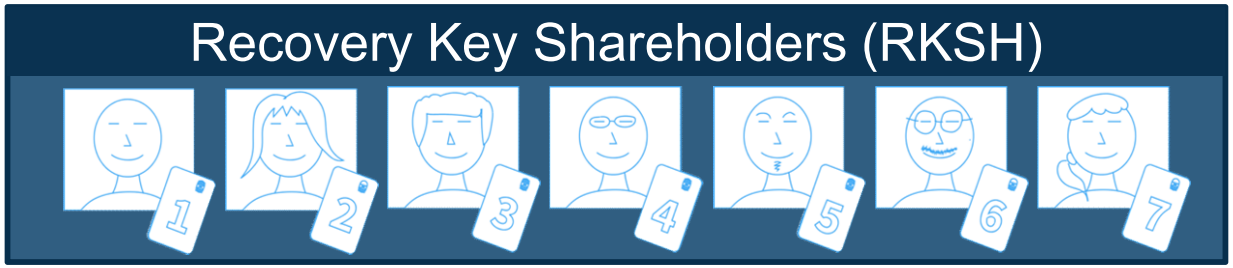
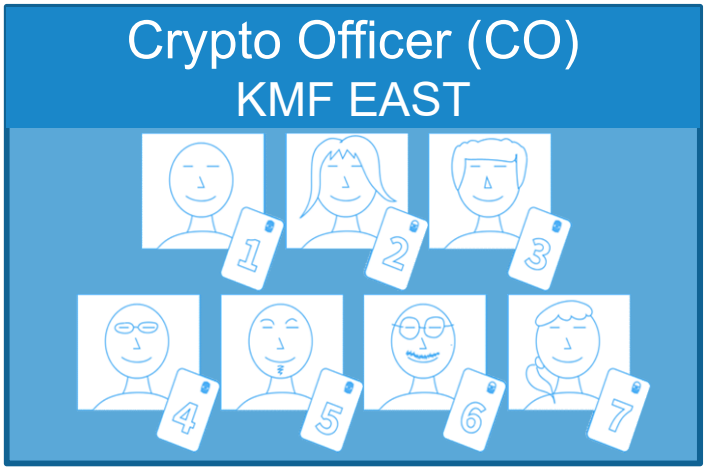


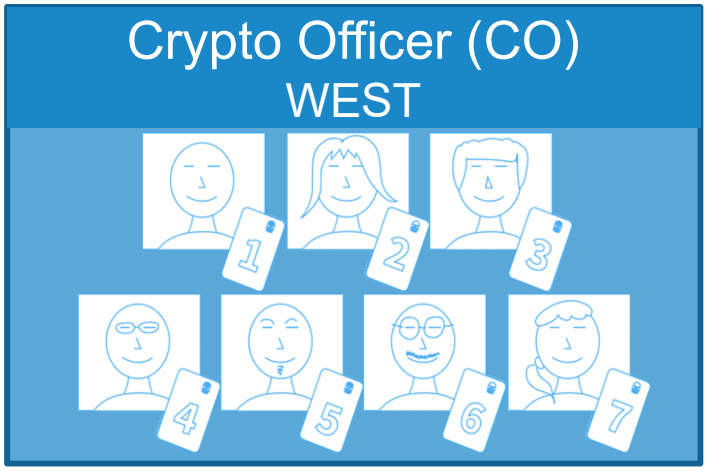
Photo: Kim Davies

Trusted Community Representatives (TCRs)





21 TCRs!



SOC 3 Certification

Photos

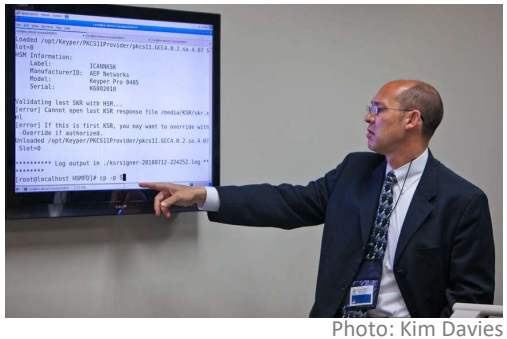


Photo: Kim Davies

Photo by Olaf Kolkman

Photo: www.dj.cx

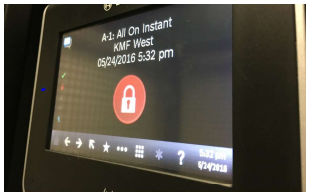


Photo: www.dj.cx

Photo: www.dj.cx

Photo: www.dj.cx

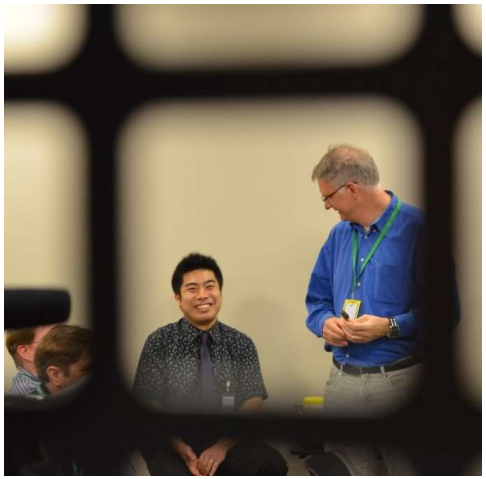


Photo: Kim Davies

Thank You

Email: punky.duero@icann.org


Punky Duero


@punkyduero


youtube.com/icannnews


linkedin/company/icann


www.icann.org

ICANN provided KSK Rollover Information and Tools:

https://www.icann.org/kskroll

https://github.com/iana-org/get-trust-anchor
https://go.icann.org/KSKtest

Root Zone DNSSEC Trust Anchor:

https://data.iana.org/root-anchors

Call for TCRs:

https://www.iana.org/help/tcr-application