

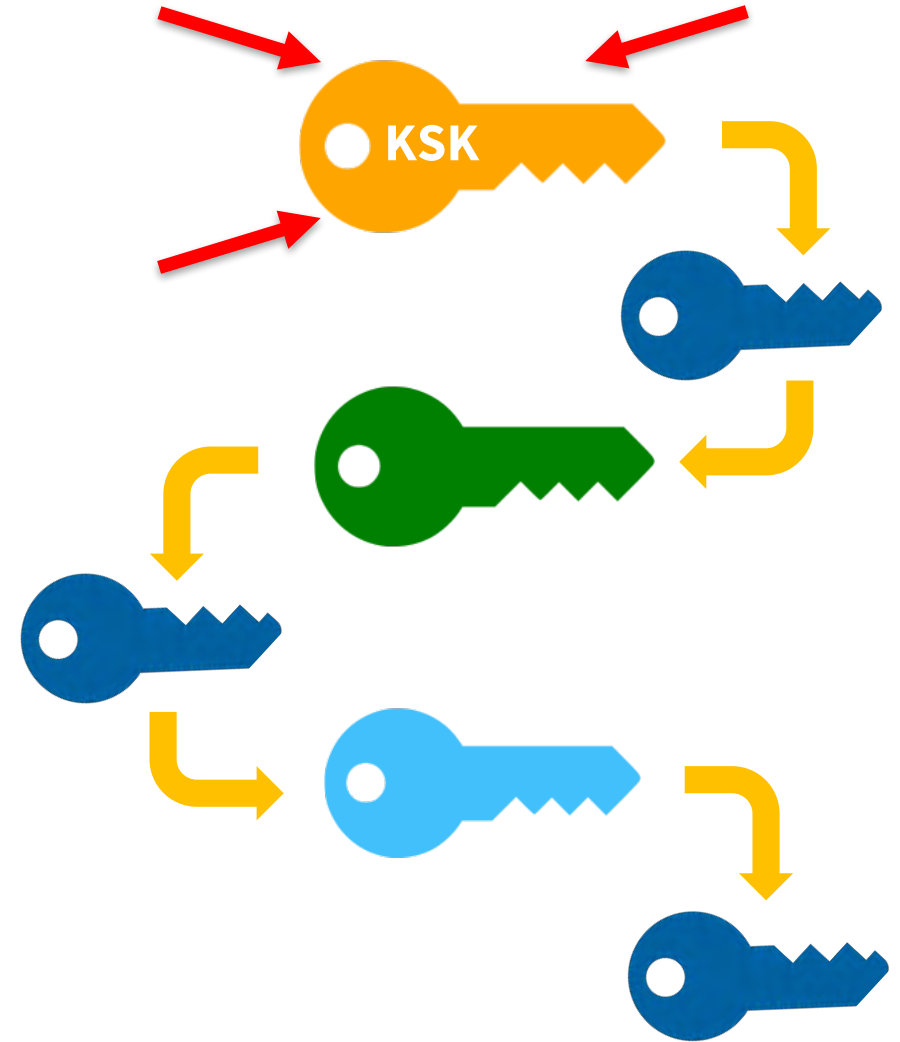


2017 Root DNSSEC KSK Rollover

Punky.Duero@iana.org | NANOG 70 | June 6, 2017

What is the Root Zone DNSSEC KSK?

- © The Root Zone DNSSEC Key Signing Key “**KSK**” is the top most cryptographic key in the DNSSEC hierarchy





- ⦿ Functional and Operational since 2010
- ⦿ Called **KSK-2010**



- ⦿ Functional and Operational since 2010
- ⦿ Called **KSK-2010**



- ⦿ New Key called **KSK-2017**

Next Milestone: JULY 11, 2017

- ◉ **KSK-2017** shows up on the DNS Resource Record
- ◉ RFC 5011 – Automated Updates of DNSSEC Trust Anchor
- ◉ **Operators of DNSSEC recursive servers may have some work**
 - ◉ As little as review configurations
 - ◉ As much as install KSK-2017

◎ The DNSKEY resource record will be:

. IN DNSKEY 257 3 8

AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxexF3
+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
R1AkUTV74bU=

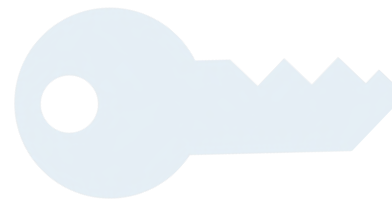
"Root"

Note: liberties taken with formatting for presentation purposes

- ⦿ A tool that retrieves the trust anchor from **<https://data.iana.org/root-anchors/root-anchors.xml>** and validates all active root KSK records

<https://github.com/iana-org/get-trust-anchor>

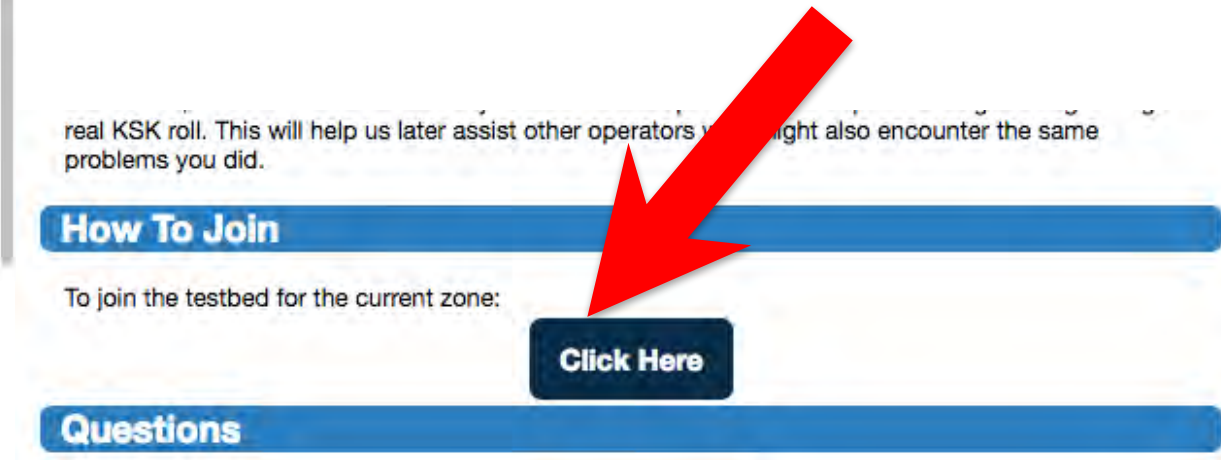
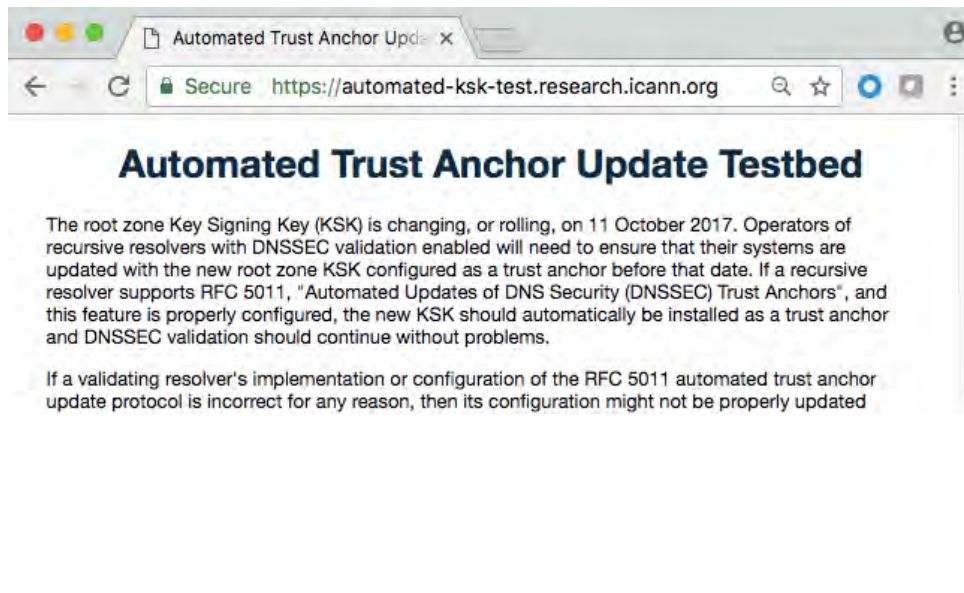
- ⦿ Writes DS and DNSKEY records to files that can be used to configure DNSSEC validators



Tools and Resources Provided by ICANN

- ◉ Designed to allow operators to test whether production resolver configurations follow *Automated Updates*

<https://go.icann.org/KSKtest>

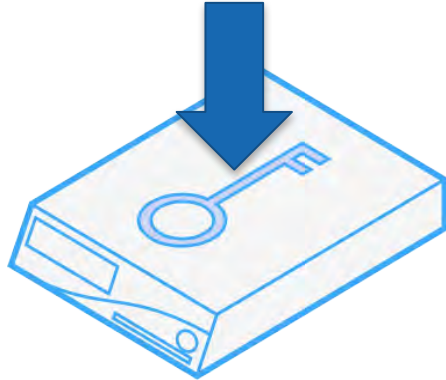


How is the Root Zone DNSSEC KSK Secured?
Why are ***Trusted Community Representatives***
being recruited?

Root Zone DNSSEC Key Signing Key

Private Key

Mfeh5eyIDdD5LKyWbRd2n9WGe2R8PzgCmr
3EgVLrjyBxWezFI96WSVexTBAvkMgJzkKTOi
W1vklbzxeF3+/4Rq7HrxRixHIFiExOLAgWOJr
5emLvN7SWX...+B5xOINVz8Og8kvArMt
NROxVQuCa...nA...Tn40jLHwVN
lGa8subX2Nn...1AkUTV74bU=8efS3rCj/
EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7
pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTld
sIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8H
B5qihyFRm+2hM8AnXGXws9555KrU



Hardware
Security Module

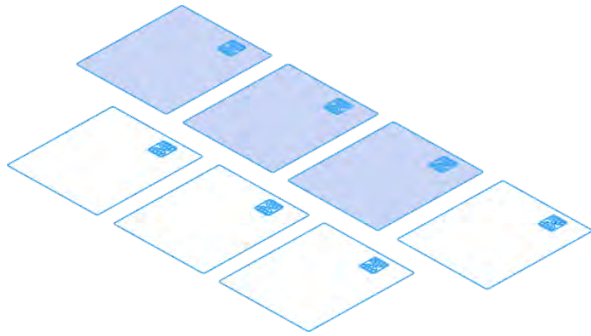
Public Key

AwEAAz/tAm8yTn4Mfeh5eyI96WSVexTBAv
kMgJzkKTOiW1vklbzxeF3+/4RgWOq7HrxRix
HIFiExOLAJr5emLvN7SWXgnLh4+B5xQINVz8
Og8kvArMtNR...CaSnIddD5LKyWbRd2n
9WGe2R8Pzg...m...F0jLHwVN8
efS3rCj/EWgv...arpVUDK/b58Da+sqqls3
eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjV
c1uTldslXuOLYA4/ilBmSVIzuDWfdRUfhHdY
6+cn8HFRm+2hM8AnXGXws9555KrUB5qihyl
Ga8subX2Nn6UwNR1AkUTV74bU=

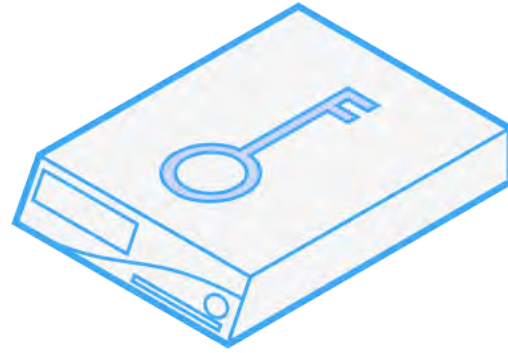


DNS Recursive
Server w/
DNSSEC

Root DNSSEC Key Signing Key



Smart Card
Credentials



Hardware
Security Module



- Stores Digital Keys
- FIPS 140-2 Level 4 Certified
- A lot of Sensors

Trusted Community Representatives (TCRs)

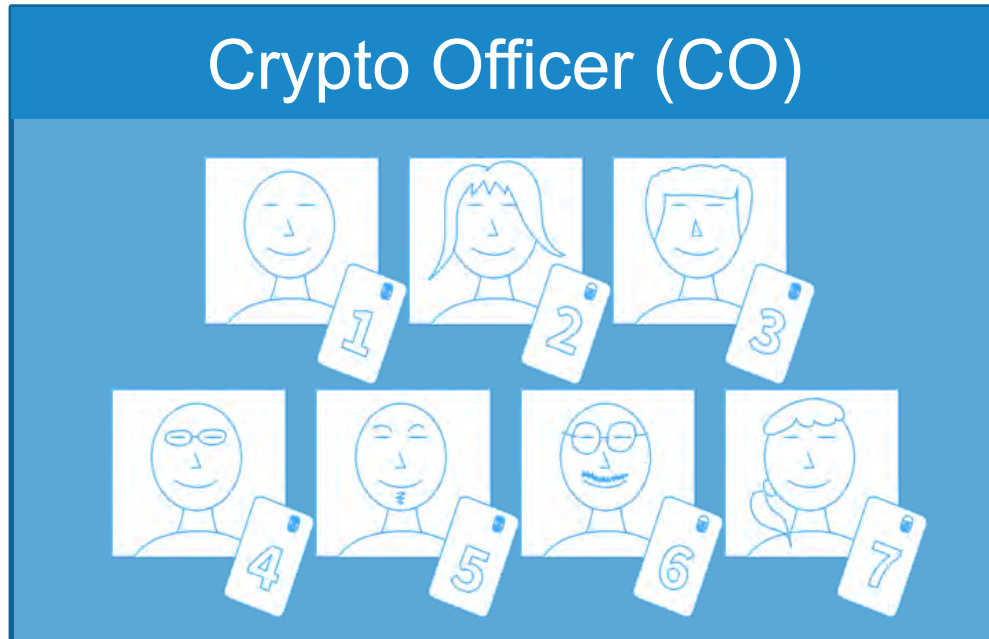
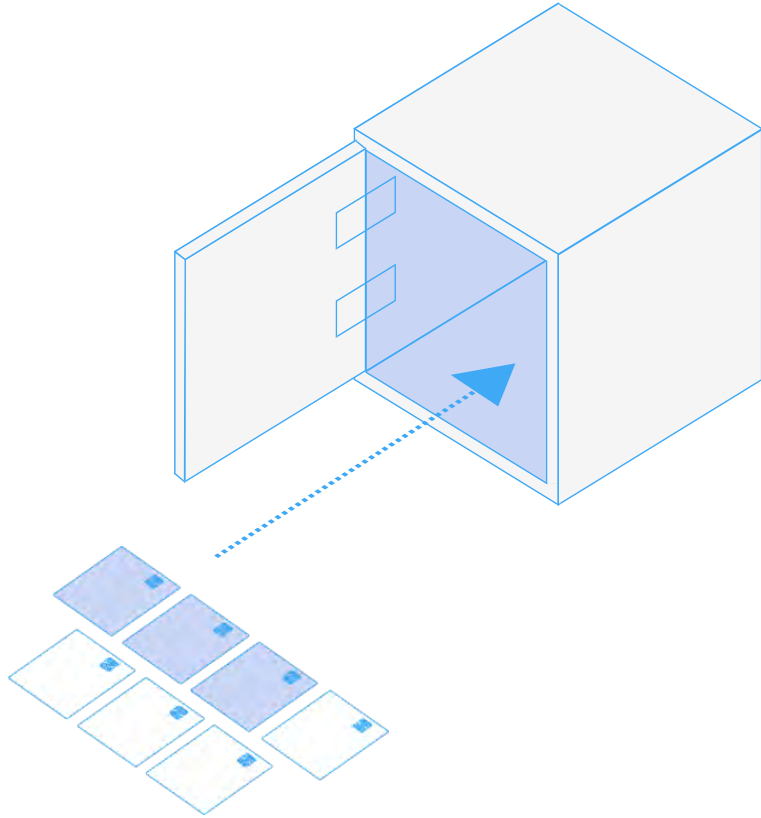


Photo by Kim Davies

<https://www.iana.org/help/tcr-roles>

SAFE #2 – Credential Safe



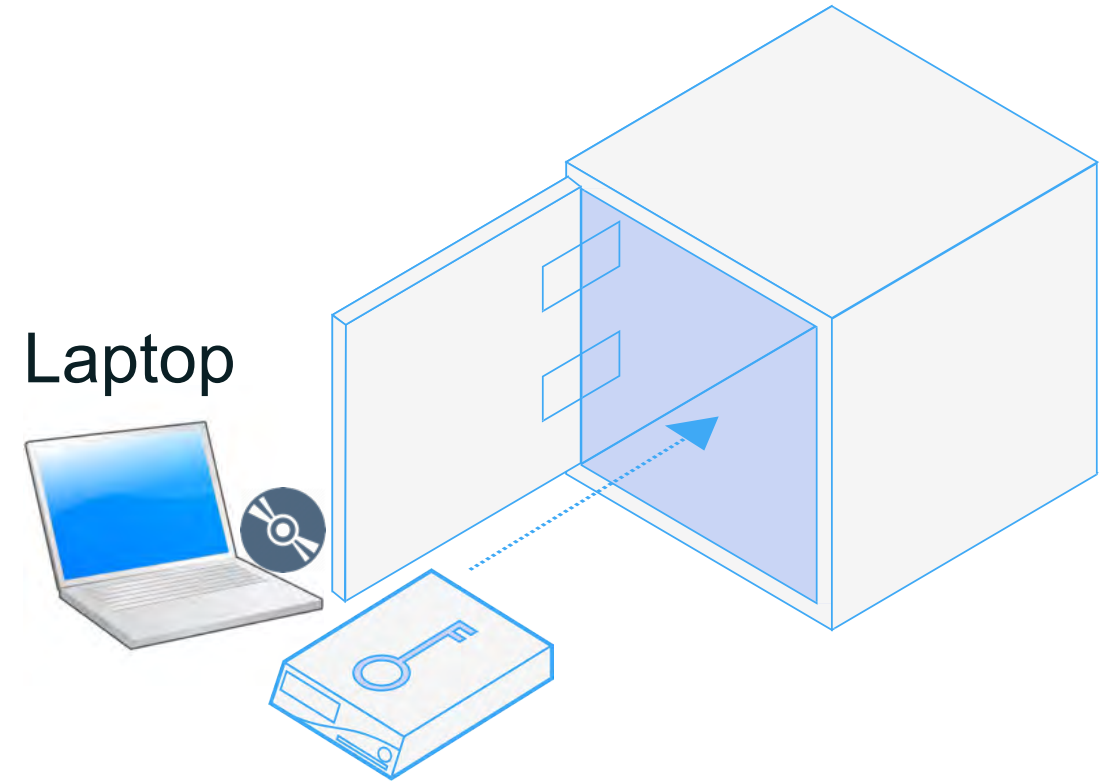
Smart Card
Credentials



Photo by Olaf Kolkman



SAFE #1 – Hardware Safe



Hardware Security
Module (HSM)

Safe Room

SAFE Room

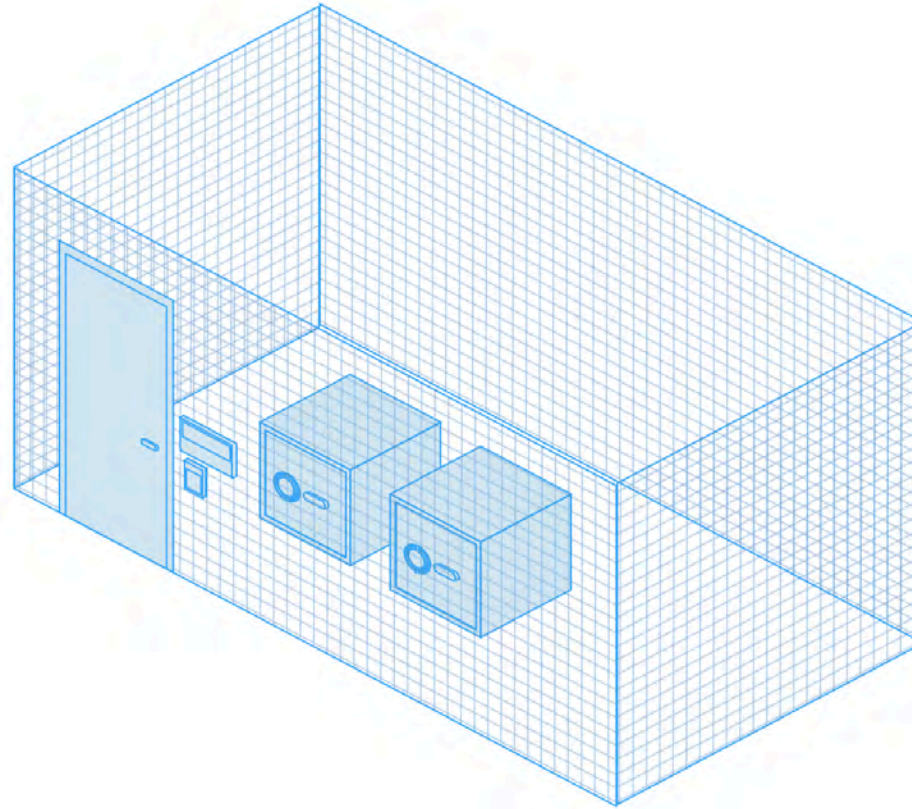


Photo by Duanne Wessels

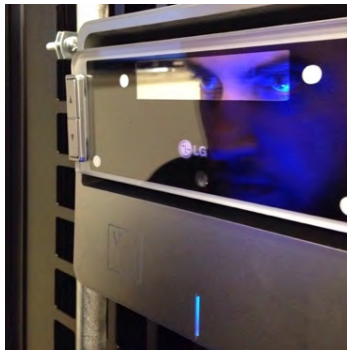


Photo by Kim Davies

Ceremony Room

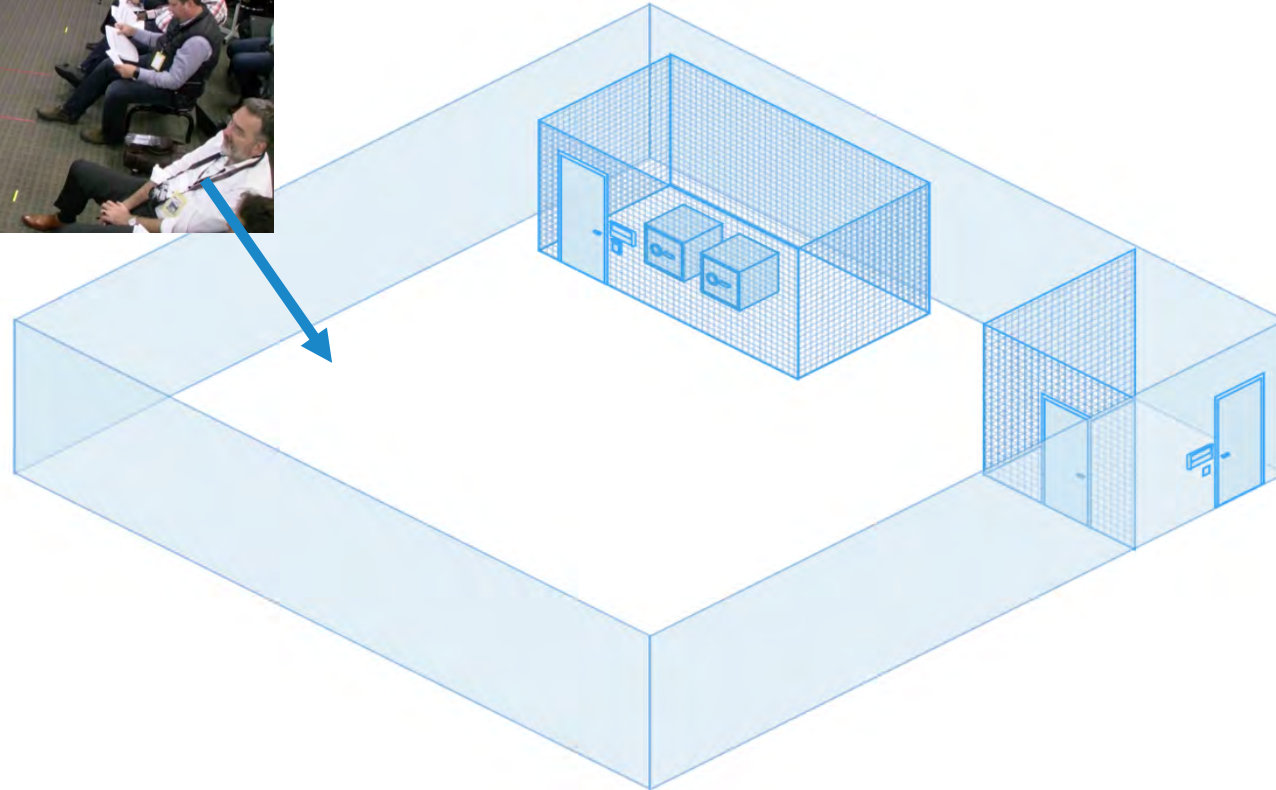
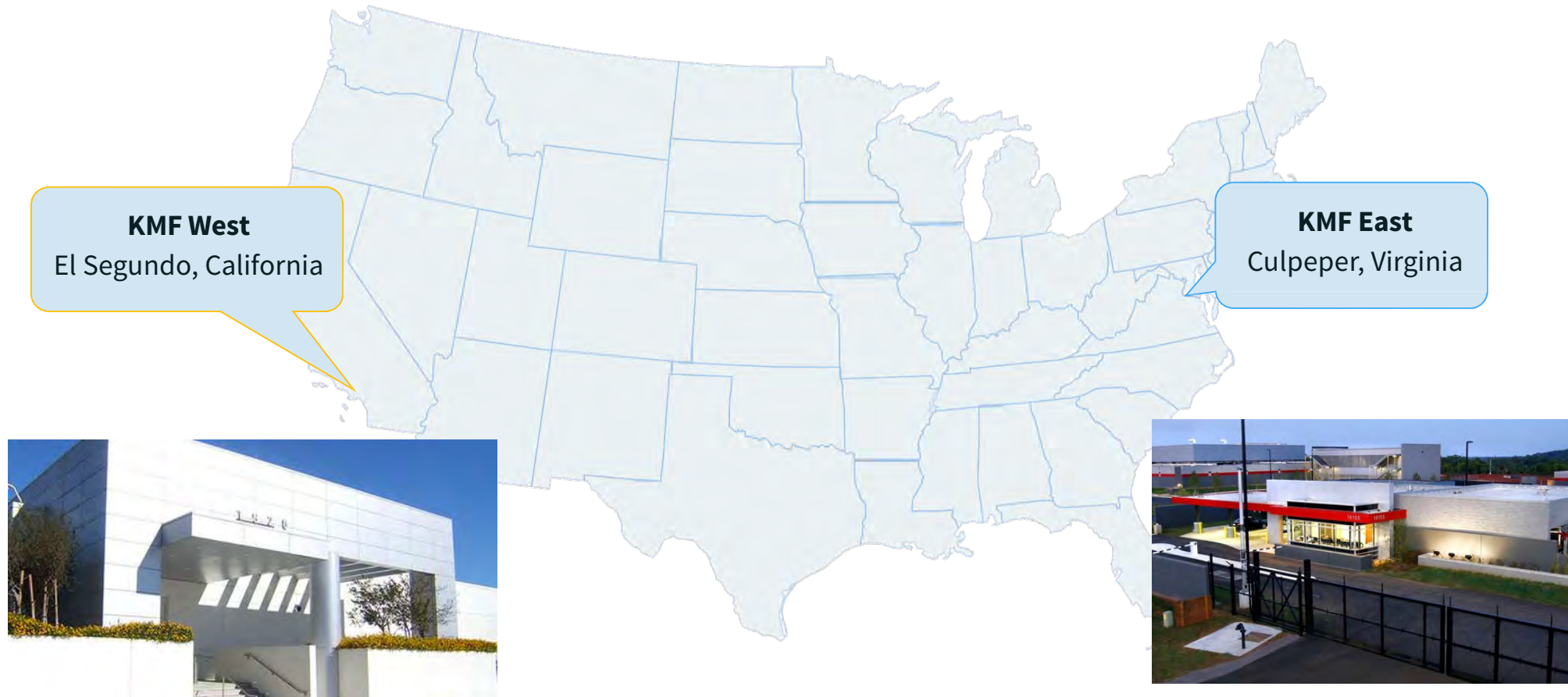


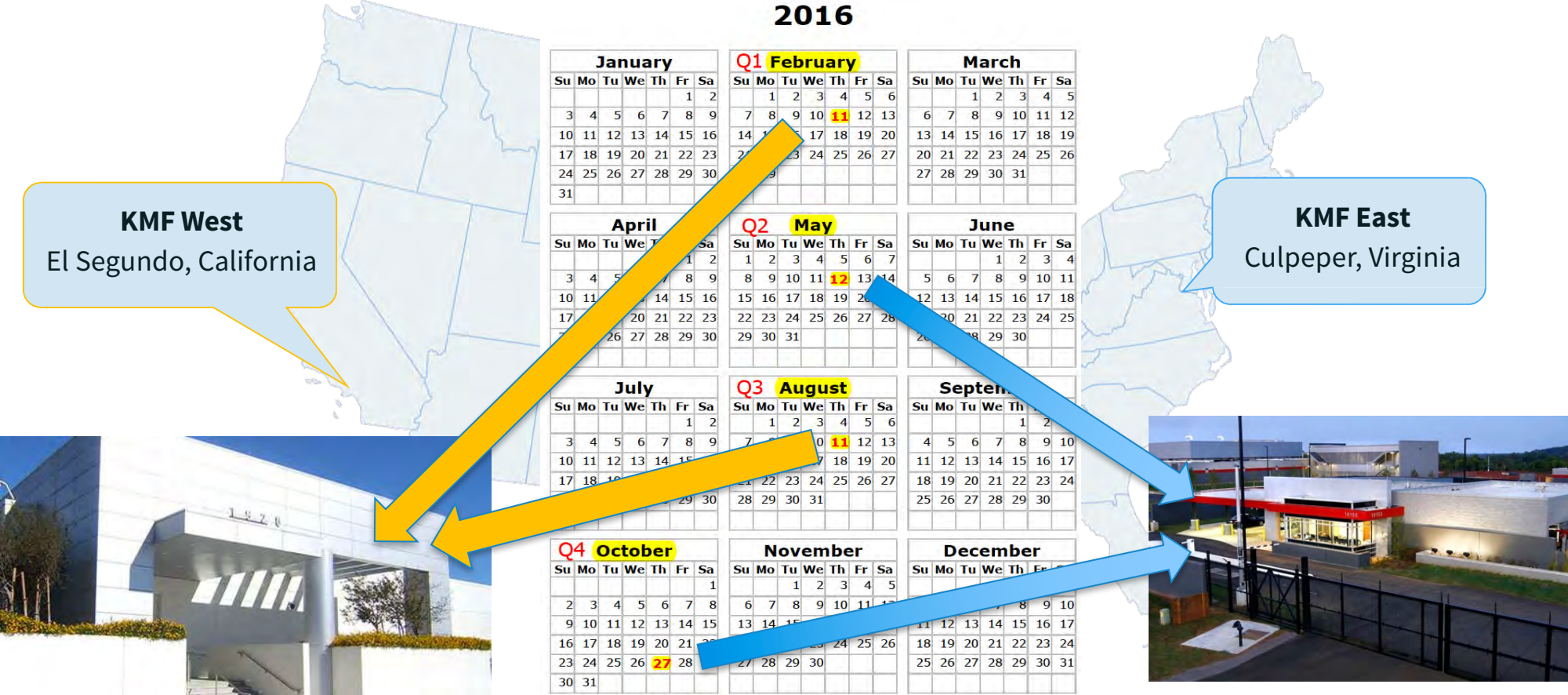
Photo: www.dj.cx



Key Management Facility



Key Management Facility



Trusted Community Representatives (TCRs)

Recovery Key Shareholders (RKSH)



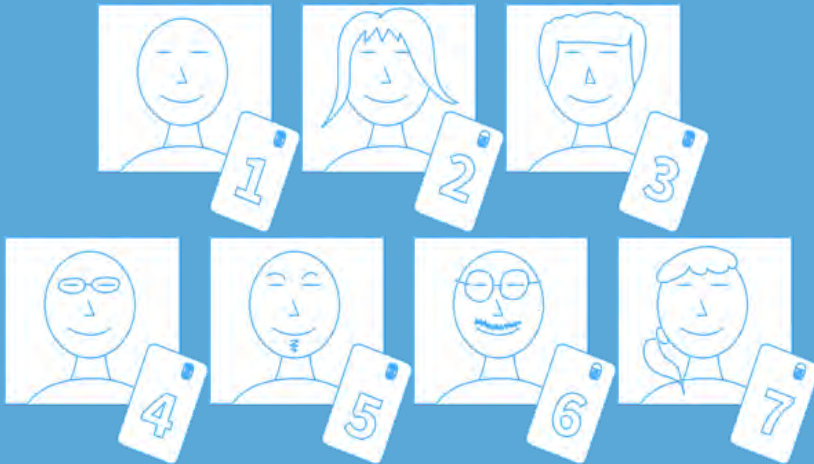
<https://www.iana.org/help/tcr-roles>

Trusted Community Representatives (TCRs)

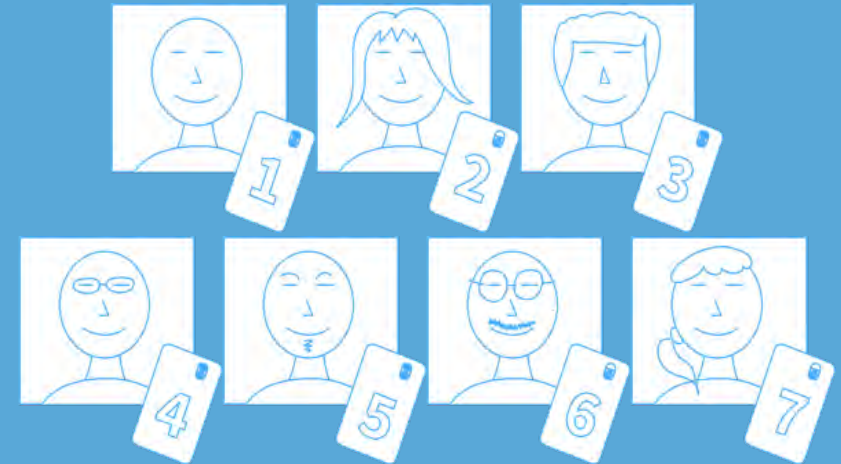
Recovery Key Shareholders (RKSH)



Crypto Officer (CO) KMF West



Crypto Officer (CO) KMF East



Call for Trusted Community Representatives (TCRs)



#ICANN seeking new volunteers to oversee key that protects the DNS Root Zone. Apply



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

How can you engage with ICANN?



Thank You and Questions

punky.duero@iana.org

Join the ksk-rollover@icann.org mailing list

KSK-Roll Website: <https://www.icann.org/kskroll>



twitter.com/icann

Follow #Keyroll



[linkedin.com/company/icann](https://www.linkedin.com/company/icann)

ICANN provided KSK Tools:

<https://github.com/iana-org/get-trust-anchor>

<https://go.icann.org/KSKtest>

Call for TCRs:

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

