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.
Root Zone DNSSEC KSK

- Functional and Operational since 2010
- Called KSK-2010
Root Zone DNSSEC KSK

- 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/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiWlvkIbzxeF3+
/+4RgWOq7HrxRixH1FlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWFdRUFhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qiylGa8subX2Nn6UwNR1AkUTV74bU=
```

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

Mfeh5eyIDdD5LKyWbRd2n9We2R8PzgCmr3EgVLrjyBxWezF096WSVexTBAvkMyGzKTOiW1vkIbzxeF3+/4Rq7HnxRiHFIEvOLAgW0JrSelmwNT5WYx5xQVNZvOBqNkwArMtNROvVQyCA2pAf5x08LHwWNlGa8subX2Nn6UwNR1AkUTV74bU=8ef53rCj/EWgwlWzb3tarpVJDK/b58Da+sq63xeNbuw7pr+eoZGRf6K6n9L3c6H5Apxz7LjVC1uTIdSlXxlOYA4/lBmSVjzuzuDWeRfUffHdhY6+cn8HBSqhyFRm+2hMBAnXGxws9555KrU

Public Key

AwEAAaz/tm8yTr4Mfeh5eyI96WSVexTBAvkmGJzkkKQIWIvKvbzxeF3+/4Rg4W0q7HGrRiHIFIEvOAmL95Wxg9nlHv8BxQVNNZvOBqNkwArMtNROvVQyCA2pAf5x08LHwWNlGa8subX2Nn6UwNR1AkUTV74bU=8ef53rCj/EWgwlWzb3tarpVJDK/b58Da+sq63xeNbuw7pr+eoZGRf6K6n9L3c6H5Apxz7LjVC1uTIdSlXxlOYA4/lBmSVjzuzuDWeRfUffHdhY6+cn8HBSqhyFRm+2hMBAnXGxws9555KrU

Hardware Security Module

DNS Recursive Server w/ DNSSEC
Root DNSSEC Key Signing Key

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

Smart Card Credentials

Hardware Security Module
Trusted Community Representatives (TCRs)

 Crypto Officer (CO)

https://www.iana.org/help/tcr-roles
SAFE #2 – Credential Safe

Smart Card Credentials

Photo by Olaf Kolkman
SAFE #1 – Hardware Safe

Laptop

Hardware Security Module (HSM)
Safe Room

SAFE Room

Photo by Kim Davies

Photo by Duanne Wessels
Ceremony Room
Key Management Facility

KMF West
El Segundo, California

KMF East
Culpeper, Virginia
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

How can you engage with ICANN?

Follow #Keyroll

twitter.com/icann
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