



# Rolling the Root Zone DNSSEC Key Signing Key

Dr. Richard Lamb | November 2016 [richard.lamb@icann.org](mailto:richard.lamb@icann.org)

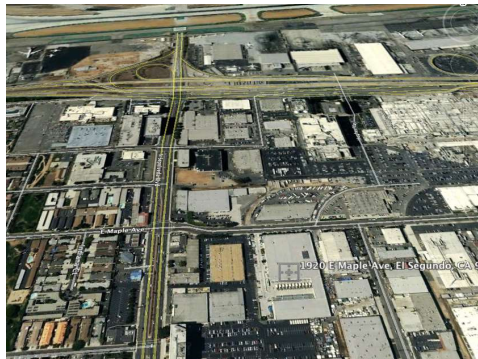
# Motivation for this talk

- ICANN is about to change an important configuration parameter in DNSSEC
- For a network operator, this may create a need for action
- This discussion is meant to inform: Why this is happening, what is happening, and when
  - Highlighting: the availability of project plan documents

Do Class Exercise Here

# Current Root KSK

- The current root KSK was created in 2010
  - Stored in Hardware Security Modules in two Key Management Facilities
  - The operations surrounding the key is an entirely different talk (21 trusted community representatives, multi-person controls, key ceremonies, 3<sup>rd</sup> party audit.)





# Why change the current Root KSK?

- Good cryptographic hygiene
  - Secrets don't remain secret forever
- Good operational hygiene
  - Have a plan, complete enough to execute
  - Exercise the plan under normal circumstances
- Promised to do so in a policy statement\* in 2010
  - “Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation.”

\* <https://www.iana.org/dnssec/icann-dps.txt> Section 6.5

# Bottom Line

- Changing the root KSK will impact just about all DNSSEC validations (15% worldwide)
  - If the trust anchor is "misconfigured" (i.e., the wrong key) DNSSEC will reject legitimate responses
  - To anyone or any process relying on DNS, it will appear that the desired data is unavailable, website is unreachable, "the Internet is down"

- The KSK Rollover Plan Documents

- Available at: *<https://www.icann.org/kskroll>*
  - 2017 KSK Rollover Operational Implementation Plan
  - 2017 KSK Rollover Systems Test Plan
  - 2017 KSK Rollover Monitoring Plan
  - 2017 KSK Rollover External Test Plan
  - 2017 KSK Rollover Back Out Plan
- We encourage interested folks to given them a read



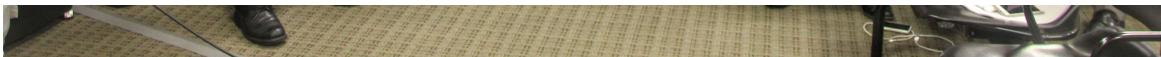
# Overview of Project Plans

- The new KSK was created on October 27, 2016
- Expect new KSK to be install on backup site Feb 2017



```
Starting: kekgen (at Thu Oct 27 18:49:20 2016 UTC)
Use HSM /opt/dnssec/sep.hsmconfig?
HSM /opt/dnssec/sep.hsmconfig activated.
setenv KEYSER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/keysper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/keysper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM Slot 0 included
Loaded /opt/keysper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
Label: 1CAHNR3K
ManufacturerID: AEP Networks
Model: Keyper 5860-2
Serial: H1403032
Generating 2048 bit RSA keypair...
Created keypair labeled "KlaJeys"
SHA256 DS resource records and hash:
. IN DS 20326 8 2 E04D448B08BF1D39A55C08D7C65D0845E8E80409B8C683457104237CF8EBCD
>> tapeworm hazardous crumpled provincial alone midsummer Belfast corporate revenge fan
cinote alone asteroid kiwi glossary aggregate Joplin endorse typewriter merit Dakota pu
pyr pyramid frighten confidence nightclub autograph root consensus soybean warranty t
umdr microscope <<
Created CSR file "KlaJeys.csr":
O: Public Technical Identifiers
OU: Cryptographic Business Operations
CN: Root Zone KSK 2016-10-2718:50:19+00:00
1.3.6.1.4.1.1000.53: . IN DS 20326 8 2 E04D448B08BF1D39A55C08D7C65D0845E8E80409B8C6834
57104237CF8EBCD
KlaJeys.csr SHA256 thumbprint and hash:
36740866E75997F4727302774636C31A6C43D81F5FA43D10A43DECB1C63755
>> Christmas hydraulic asleep hazardous transit examine freshunk Virginia lockup cele
brate chairlift: celebrate indoors Galveston ammo company rematch reproduce commence inv
entive vapor whimsical crucial scavenger ahead Pandora commence unicorn sailboat respon
sive clamshell equipment <<
Unloaded /opt/keysper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
```

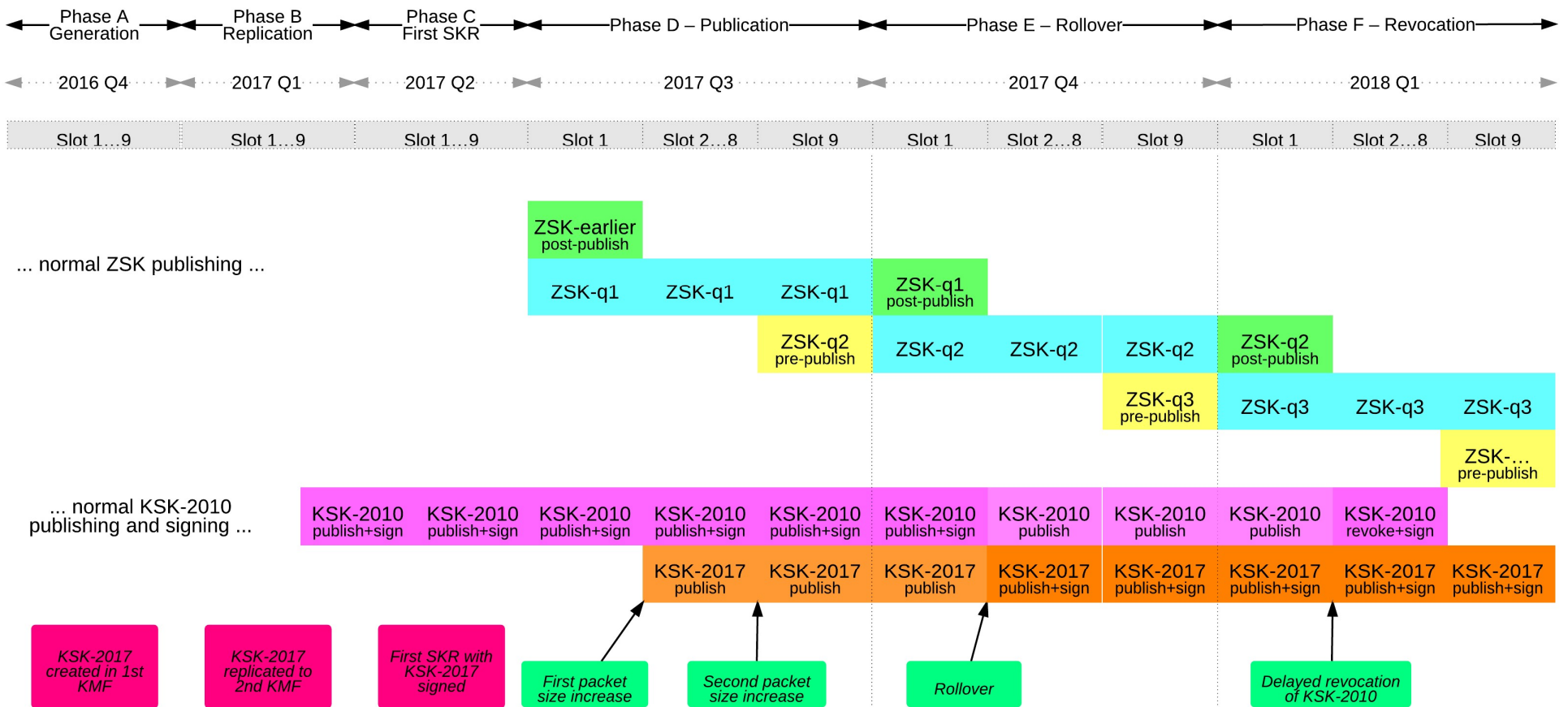
*Handwritten note:* Keyper 5860



# Upcoming Dates to Watch

- September 19, 2017
  - The root zone DNSKEY set will increase to 1414 bytes for 20 days, prior to that date 1139 bytes has been the high water mark
- **October 11, 2017**
  - On this date the root zone DNSKEY set will be signed only by the new KSK
- January 11, 2018
  - The root zone DNSKEY set will increase to 1425 bytes for 20 days

# Operational Implementation Plan Timeline



# Trust Anchor Management

- How do you trust and configure?
  - Are trust anchors subject to configuration control?
  - Rely on embedded data in software?
  - Are DNSSEC validation failures monitored?
- Automated Updates of DNSSEC Trust Anchors
  - Most direct, reliable means for getting the key
- Negative Trust Anchor management – RFC 7646
  - Protects against errors made by others

# Tools & Testbeds

- We are working with DNS software and tool developers and distributors
  - Management/troubleshooting aids
  - Updates of bundled keys
- Testbeds for Code Developers
  - Automated updates: *<http://keyroll.systems/>*
  - Root zone model: *<https://www.toot-servers.net/>*
- Testbeds for Service Operators
  - I.e., using "off-the-shelf" parameters
  - Planned for end-of-2016

# For More Information



- Join the `ksk-rollover@icann.org` mailing list:
  - <https://mm.icann.org/listinfo/ksk-rollover>



- Follow on Twitter
  - @ICANN
  - Hashtag: #KeyRoll



- Visit the web page:
  - <https://www.icann.org/kskroll>

# Engage with ICANN



## Thank You and Questions

Reach me at:

Email: [ksk-rollover@icann.org](mailto:ksk-rollover@icann.org)

Website: [icann.org/kskroll](http://icann.org/kskroll)



[twitter.com/icann](https://twitter.com/icann)



[gplus.to/icann](https://plus.google.com/icann)



[facebook.com/icannorg](https://facebook.com/icannorg)



[weibo.com/ICANNorg](https://weibo.com/ICANNorg)



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



[flickr.com/photos/icann](https://flickr.com/photos/icann)



[youtube.com/user/icannnews](https://youtube.com/user/icannnews)



[slideshare.net/icannpresentations](https://slideshare.net/icannpresentations)