# 2017 DNSSEC KSK Rollover


Edward Lewis

**APNIC 44**

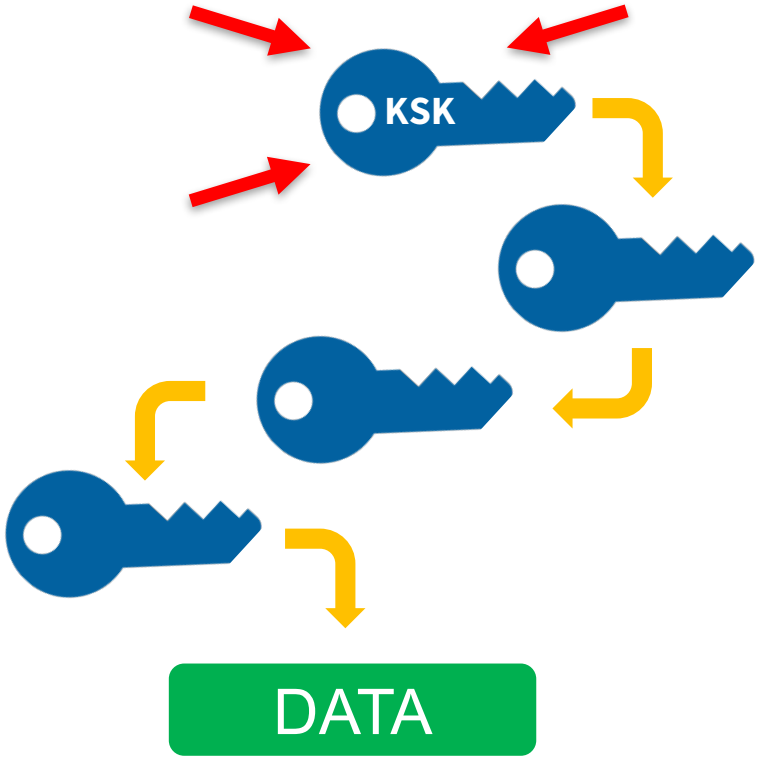
13 September 2017

# DNSSEC – Signing vs. Validation

- **DNS Security Extensions**
  - Digital signature is the basic element of work
- **Signing**
  - Zone Administrators add digital signatures
- **Validation**
  - DNS Caches, DNS Stubs check the signatures in a few ways, cryptographic and other (time, etc.)
- **Impact of DNSSEC root KSK rollover**
  - DNSSEC validators (e.g., some ISPs) need to prepare, new "root" of trust

# The Root Zone DNSSEC KSK

- The Root Zone DNSSEC Key Signing Key "**KSK**" is the top most cryptographic key in the DNSSEC hierarchy
- Public portion of the KSK is a configuration parameter in DNS validating revolvers
- The other "role" is a ZSK, zone signing key



# Rollover of the Root Zone DNSSEC KSK

- **There has been one functional, operational Root Zone DNSSEC KSK**
  - Called "KSK-2010"
  - Since 2010, nothing before that
- **A new KSK will be put into production later this year**
  - Call it "KSK-2017"
  - An orderly succession for continued smooth operations
- **Operators of DNSSEC recursive servers may have some work**
  - As little as review configurations
  - As much as install KSK-2017

# Important Milestones

| Event | Date |
|---|---|
| Creation of KSK-2017 | ~~October 27, 2016~~ |
| Production Qualified | ~~February 2, 2017~~ |
| Out-of-DNS-band Publication | ~~Now,~~ onwards |
| In-band (*Automated Updates*) Publication | ~~July 11, 2017 and~~ onwards |
| Sign (Production Use) | **October 11, 2017** and onwards |
| Revoke KSK-2010 | January 11, 2018 |
| Remove KSK-2010 from systems | Dates TBD, 2018 |

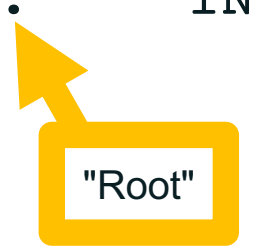
# Recognizing KSK-2017

- **The KSK-2017's Key Tag (defined protocol parameter) is**

  20326

- **The Delegation Signer (DS) Resource Record for KSK-2017 is**

```
.       IN   DS     20326 8 2
                    E06D44B80B8F1D39A95C0B0D7C65D084
                    58E880409BBC683457104237C7F8EC8D
```




*Note: liberties taken with formatting for presentation purposes*

# KSK-2017 in a DNSKEY Resource Record

- **The DNSKEY resource record is:**

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

"Root"

*Note: liberties taken with formatting for presentation purposes*

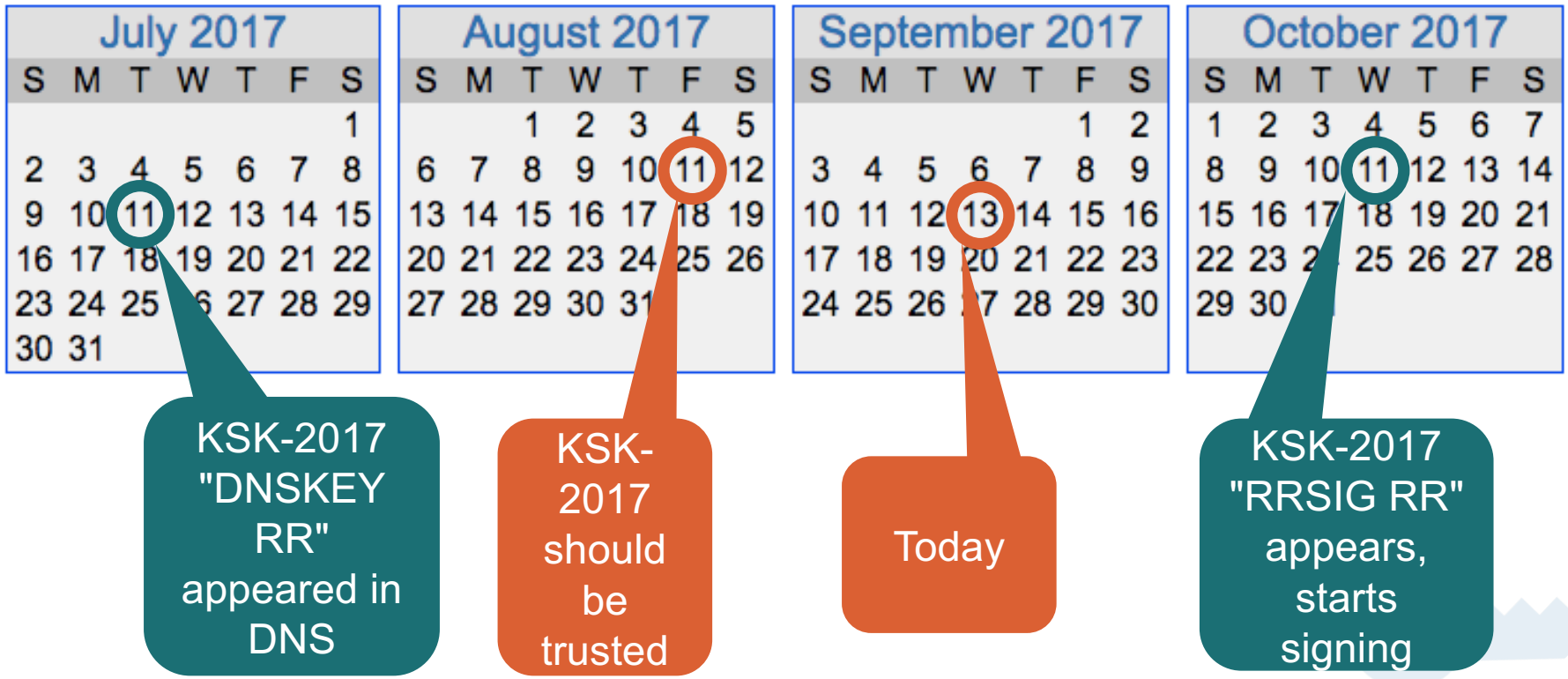
# Current "State of the System"

- **Sunny, as in “sunny day scenario”**
  - We are changing the KSK under good conditions
  - Leverage trust in KSK-2010 to distribute KSK-2017
  - Following the *Automated Updates of DNSSEC Trust Anchors* protocol (also known as "RFC 5011")

# *Automated Updates of DNSSEC Trust Anchors*

- **Defined in Request For Comments 5011**
  - Use the current trust anchor(s) to learn new
  - To allow for unattended DNSSEC validator operations
  - Based on "time" – if a new one appears and no one complains for some specified time, it can be trusted
  - Highlight: defined "add hold" time is 30 days
  - In months we will use Automated Updates to revoke KSK-2010
  - Operators are not required to follow Automated Updates

# Important Dates



# Rollover Process (Validator view)

- **Assumes DNSSEC is operating/configured to run**
  - ICANN is following the Automated Updates process
    - We are less than the "add holddown" time until the rollover event
  - (All) validators ***SHOULD ALREADY*** list the new KSK as trusted
    - Whether automatically updated or manually added
  - If KSK-2017 is not there now, manual updating is needed
- **Questions: How can one tell? How does one fix?**

# September 13 to October 11 is under 30 days!

- **Starting a DNSSEC Validator Today**
  - Not enough time to complete Automated Update's add hold-down
  - But that's not a problem
  - New DNS code ships with the new trust anchor
  - Older DNS code will bootstrap upon a clean start
  - But older DNS code with older configuration files need to be given a clean start

# How Can one Tell (if DNS Cache Validates)?

- **Send query for "dnssec-failed.org A" with DNSSEC flags**
  - If the response holds a return code of SERVFAIL, DNSSEC validation is in place
  - If the response holds an IPv4 address, DNSSEC validation is not in place

# Testing for DNSSEC

```
$ dig @$server dnssec-failed.org a +dnssec

; <<>> DiG 9.8.3-P1 <<>> dnssec-failed.org a +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 10492
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnssec-failed.org. IN A

;; Query time: 756 msec
;; SERVER: 10.47.11.34#53(10.47.11.34)
;; WHEN: Tue Sep  5 19:04:04 2017
;; MSG SIZE  rcvd: 46
```

**DNSSEC is on!**

# Testing for DNSSEC

```
$ dig @$server dnssec-failed.org a +dnssec

; <<>> DiG 9.8.3-P1 <<>> dnssec-failed.org a +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5832
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;dnssec-failed.org. IN A

;; ANSWER SECTION:
dnssec-failed.org. 7200 IN 69.252.80.75

;; Query time: 76 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Tue Sep  5 18:58:57 2017
;; MSG SIZE  rcvd: 62
```

**DNSSEC is off!**

# How Can one Tell (if KSK-2017 is Trusted)?

- **BIND**
  - 9.11.x "rndc managed-keys status"
  - 9.9.x and 9.10.x "rndc secroots"
- **Unbound**
  - Inspect the configured root.key file
- **PowerDNS**
  - "rec_control get-tas"
- **Knot Resolver**
  - Inspect the configured root.keys file
- **Microsoft Server**
  - "Administrative Tools"->"DNS"->"Trust Points"

# Details on Checking Trust Anchors

- For further information, consult

https://www.icann.org/dns-resolvers-checking-current-trust-anchors

# What Should Be Seen

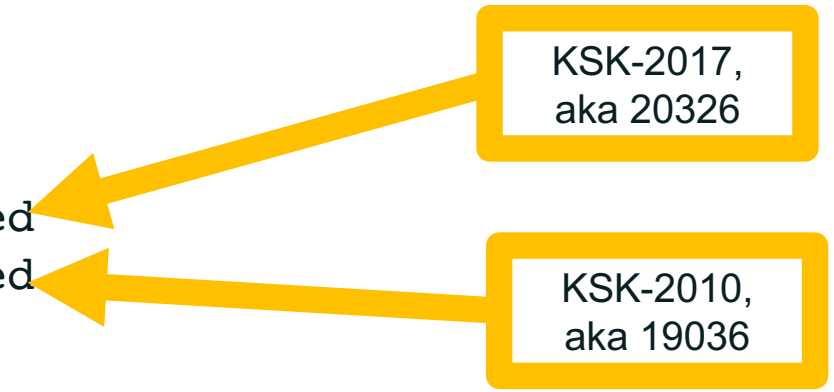
- **Two listed trust anchors for the root zone**
  - KSK-2017, key-id 20326
    - If you don't see this, the validator will fail beginning about October 11
  - KSK-2010, key-id 19036
    - If you don't see this, the validator is not working now!
- **Eventually KSK-2010 will "go away" - but not just yet**

# E.g., BIND

```
bind-9.9.5-testconfig $ rndc -c rndc.conf secroots
bind-9.9.5-testconfig $ cat named.secroots
05-Sep-2017 09:24:06.361

 Start view _default


./RSASHA256/20326 ; managed
./RSASHA256/19036 ; managed
```



# E.g., unbound

```
unbound $ cat root.key
; autotrust trust anchor file
;;id: . 1
;;last_queried: 1504239596 ;;Fri Sep  1 00:19:56 20
;;last_success: 1504239596 ;;Fri Sep  1 00:19:56 2017
;;next_probe_time: 1504281134 ;;Fri Sep  1 11:52:14 2017
;;query_failed: 0
;;query_interval: 43200
;;retry_time: 8640
. 172800 IN DNSKEY 257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAMgJzkKTOiW1vkIbzxeF/4RgWOq7HrxRixHlFlExOLAJr
mLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtROxVQuCaSnIDdD5LKyWd2n9WGe2R8PzgCmr3EgVLrjyBxW/zF
0jLHwVN8efS3rCj/EWgvIWgb9tavmDK/b58Da+sqqls3eNbw/pr+eoZG+SrDKWeL3c6H5Apxz7+jVc1
uTIdsIXxuOLYA4/ilBmSVIzuDWUfhHdY6+cn8HFRm+2G8AnXGXws9555KrlpihylGa8subXd/n6UwN
R1AkUTV74bU= ;{id = 20326 (ksk), size = 2048} ;;state=2 [  VALID  ] ;;count=0
;;lastchange=1502438004 ;;Fri Aug 11 03:53:24 2017
. 172800 IN DNSKEY 257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwcxQ0YI0EzrAcQqB
GCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QkkjF5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apDzN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMUPJ8LbqF6dsV6DoB
Qzgul0sGIcGOYl7OyQdXfZ57relDgeu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKiRblfdfwhYB4N7knNnulq
QxA+Uk1ihz0= ;{id = 19036 (ksk), size = 2048b} ;;state=2 [  VALID  ] ;;count=0
;;lastchange=1459820836 ;;Mon Apr  4 21:47:16 2016
```

KSK-2017, aka 20326

KSK-2010, aka 19036

Both are VALID

# If One Sees Both KSKs trusted

- Take a nap during the next few slides

# How does one fix?

- If one does not see both KSKs as trusted, then adjustments need to be made

- "How to's" are tool and environment dependent

https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

# Where to Get KSK-2017 Manually

- **Via the official IANA trust anchor XML file at https://data.iana.org/root-anchors/root-anchors.xml**
  - Contains the same information as a DS record for KSK-2017
  - Validate root-anchors.xml with the detached signature at https://data.iana.org/root-anchors/root-anchors.p7s
- **Via DNS (i.e., ask a root server for "./IN/DNSKEY")**
  - Validate the KSK-2017 by comparison with other trusted copies
- **Via "Other means" ...**

# What “other means” for a manual approach?

- **Most software/OS distributions of DNSSEC**
  - Embed copies of the KSK (now KSK-2010, later KSK-2017)
  - In contact with as many distributors as possible

- **Compare with the key from these slides**
  - Presuming you trust the contents of this presentation and the presenter :-)

- **Obtain a copy from another operator, or other trusted source**
  - How well do you trust "them"?

# Symptoms of Issues Related to the Rollover

- **If there are problems caused by fragmentation-related issues**
  - DNSSEC validation fails for everything, resulting from an inability to get the Root Zone DNSKEY set with KSK-2017
  - Look for a large number of queries leaving a recursive server "retrying" the question

- **If there are problems caused by using the wrong trust anchor**
  - DNSSEC validation fails for everything, resulting from an inability to build a chain of trust
  - Look in logs for validation failures, implementation specific

# Fragmentation, IPv6 and DNS

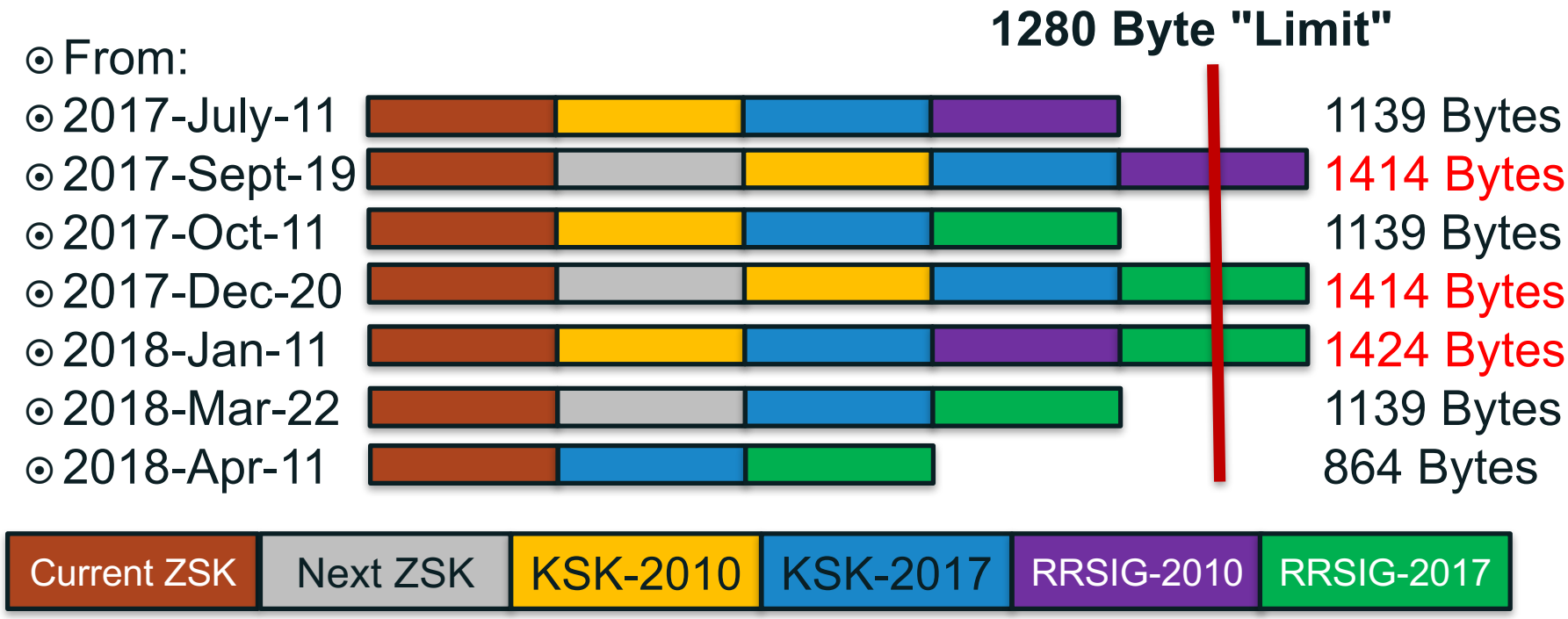
- **Fragmentation in IPv6**
  - Fragments created at source, reassembled at destination
  - Unlike IPv4, fragmentation not done in middle of network
  - Instead a notice is sent back to source

- **IPv6's fragmentation feedback does not help DNS' use of UDP**
  - No recollection (memory) of what was sent, can't resend

- **At a high-level, there have been concerns about DNS responses over 1280 bytes**
  - The KSK Rollover process will peak over 1280 three times

# Impact on the KSK Rollover Process

- **Visualizing Packet Sizes (response to root DNSKEY query)**



# Experience with IPv6 Fragmentation and DNS

- **An Experiment was Run**
  - Examining responses from TLD zones, some with large keysets, has been helpful
    - From one vantage point (residential cable ISP), some large DNSKEY sets were not retrieved over IPv6 in UDP
    - From hosted virtual machines, almost no errors observed
    - Perhaps it is just paranoia!
  - Nevertheless, TCP over IPv6, worked for all sampled zones

# Recommendation for IPv6 (and for IPv4 too)

- **What you should do**
  - Make sure your servers can query over TCP (especially in IPv6)
  - Test and verify that you can receive large DNSKEY sets
    http://keysizetest.verisignlabs.com/
    https://www.dns-oarc.net/oarc/services/replysizetest
  - This should be a "permanent fix", not just for the KSK key rollover, TCP is an important piece of DNS operations

# The Future

- **Revocation of KSK-2010 in 2018**
  - Automated Updates will be used

- **There will be more KSK rollovers**
  - When, we don't know (yet)

  - What to do – consider and configure Automated Updates capabilities
    - Whether it fits operational architectures

# Tools and Resources Provided by ICANN

- **Following slides will describe these further**
- **A python-language script to retrieve KSK-2010 and KSK-2017**
  - get_trust_anchor.py
- **An *Automated Updates* testbed for production (test) servers**
  - https://automated-ksk-test.research.icann.org
- **Documentation**
  - https://www.icann.org/resources/pages/ksk-rollover
  - plus what was mentioned earlier

# get_trust_anchor.py

- **A tool that retrieves "https://data.iana.org/root-anchors/root-anchors.xml" and validates all active root KSK records**

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

  - Contains extensive in-code comments/documentation
  - Download & run in python v2.7, v3 or newer

    $ python get_trust_anchor.py

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

# ICANN's *Automatic Updates* Testbed

- **Designed to allow operators to test whether production resolver configurations follow *Automated Updates***
  - The goal is to test production resolvers with live test zones executing a KSK rollover in real time
    - A full test lasts several weeks
  - Joining the testbed involves:
    - Configuring a trust anchor for a test zone such as *2017-05-14.automated-ksk-test.research.icann.org*
    - Receiving periodic emails with instructions for what to do and what to watch for
  - ***https://automated-ksk-test.research.icann.org***

# Educational/informational Resources

- **ICANN organizes KSK rollover information here:**

  https://www.icann.org/resources/pages/ksk-rollover

  - Link to that page can be found on ICANN's main web page under "Quicklinks"

  - Contains links to what's been covered in this presentation, the get_trust_anchor.py script and information on ICANN's live testbeds

# Those Reference URLs, once again

https://www.icann.org/dns-resolvers-checking-current-trust-anchors

https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

# Engage with ICANN

**Join the ksk-rollover@icann.org mailing list**

Archives: https://mm.icann.org/listinfo/ksk-rollover

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


@icann | **Follow #KeyRoll**


facebook.com/icannorg


youtube.com/icannnews


flickr.com/icann


linkedin/company/icann


slideshare/icannpresentations


soundcloud/icann