Root Zone DNSSEC KSK Rollover

Edward Lewis

ENOG 15

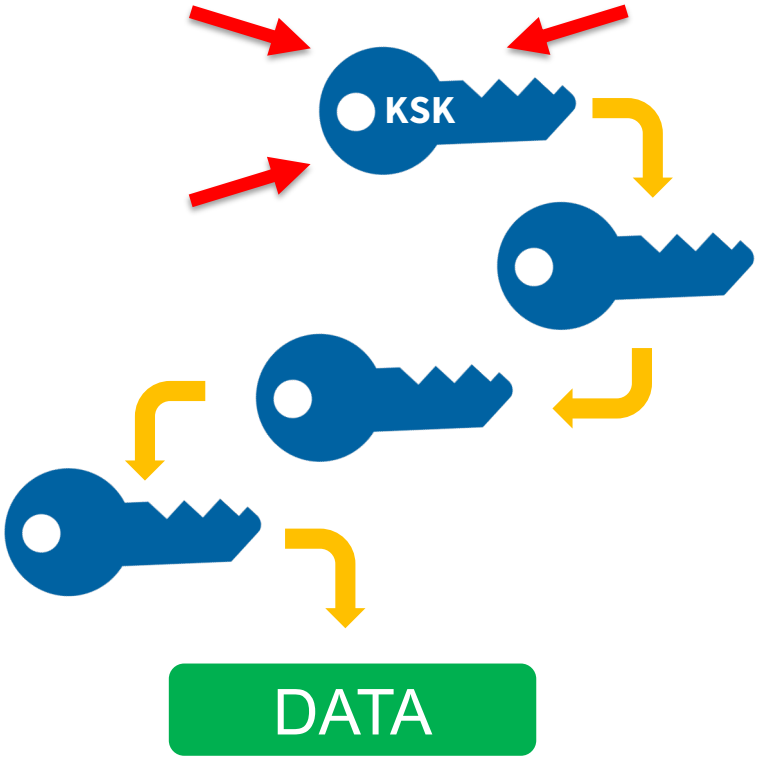
5 June 2018

The Basics

- **This talk is related to the Domain Name System, in particular, the security extensions made to it**
  - DNSSEC – DNS Security Extensions
  - The addition of *digital signatures* to data, using a hierarchy of asymmetric cryptographic keys to achieve massive scale
    - Signing – generate signatures
    - Validation – checking signatures
  - Two of the *cryptographic roles* defined for keys
    - Key Signing Key – a key that signs a bundle of other keys
    - Zone Signing Key – a key that is used to sign data

The Root Zone DNSSEC KSK

- The Root Zone DNSSEC KSK is the top most cryptographic key in the DNSSEC validation hierarchy
- Public portion of the KSK is a configuration parameter in DNS validating revolvers



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

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 product**
  - Call it "KSK-2017"
  - An orderly succession for continued
- **Operators of DNSSEC recursive servers may have some work**
  - As little as review configurations
  - As much as install KSK-2017

Not a Typo

A result of the delay

The Approach to the KSK Rollover

- **The rollover process emerged from plans developed in 2015**

- ***Automated Updates of DNSSEC Trust Anchors***
  - RFC-Editor STD 74, also known as RFC 5011

- **Recommendations are for operators to rely on "RFC 5011"**
  - Some crucial milestones *have already passed*
  - We are still adhering to it for the final phases
  - In the future, we will likely rely on it again

Important Milestones

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

The "Was To Be"

Important Milestones - Updated

Event	Date
Creation of KSK-2017	October 27, 2016
Production Qualified	February 2, 2017
Out-of-DNS-band Publication	February 2, 2017, onwards
Automated Updates Publication	July 11, 2017, onwards
Sign (Production Use)	***October 11, 2018, tentative***
Revoke KSK-2010	***TBD***
Remove KSK-2010	***TBD***

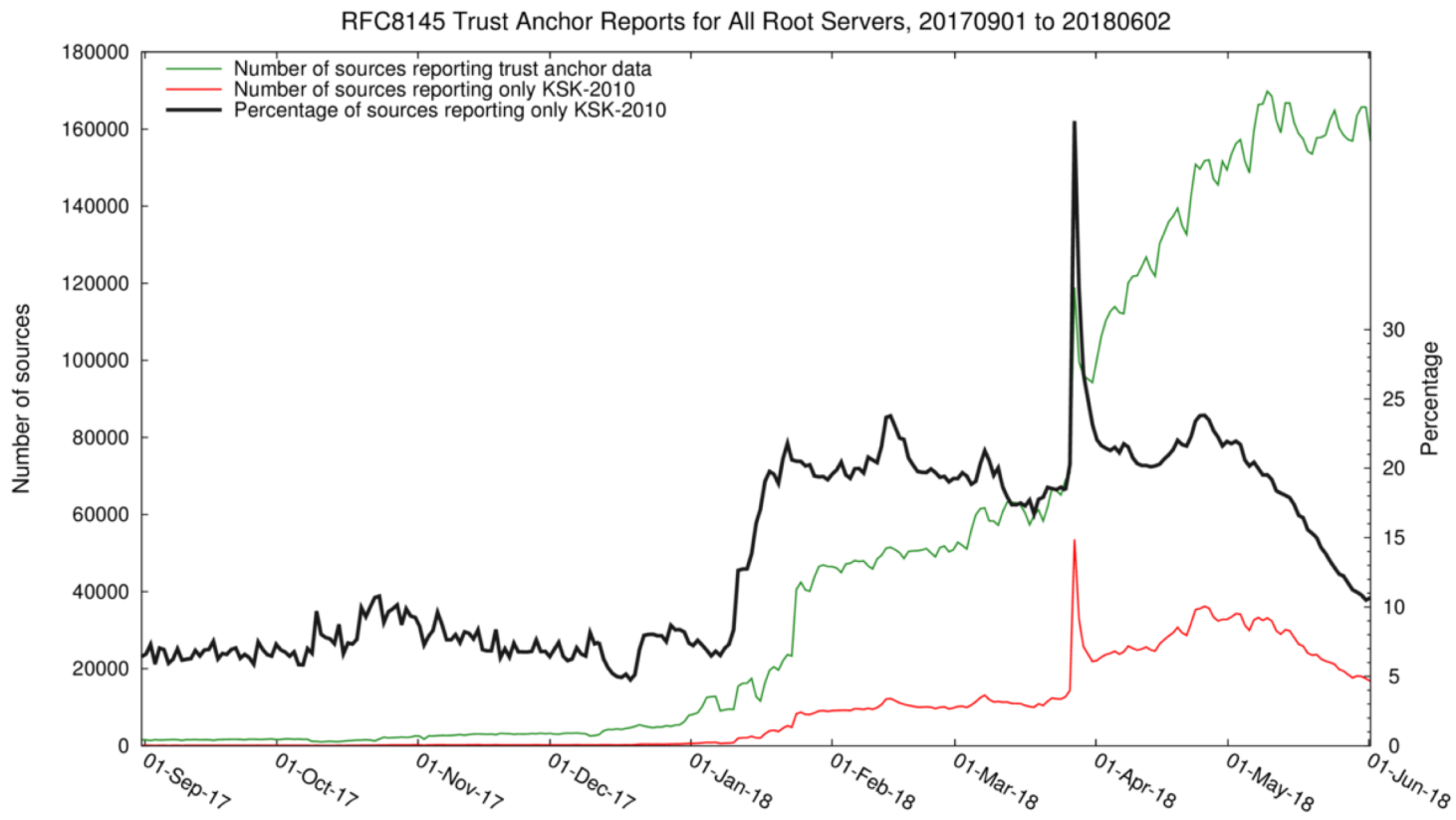
Why the Updated Milestones?

- When the rollover started there was no way to measure resolver configurations
- During the project, a new measure was invented, implemented and rolled out
- The new measure's results were at best confusing and concerning
- So the rollover was paused to have a look

The Measure

- **A readiness measure invented in the IETF**
  - *Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)*, aka RFC 8145
  - Quickly turned into code
  - Combined with a noticeable "tech refresh"

A Quick Look at Data



A Longer Look at The Data

- **Verisign researcher, looking at two root servers**
  - Noticed that the number of DNSSEC Validators having only the KSK-2010 was uncomfortably high (7%)

- **Results were confirmed by ICANN**
  - Feed of data from nearly all of the root servers
  - Rates of "only KSK-2010" seemed to rise over time or as more reporters came on-line

- **But data is not always informative!**

The Early Analysis

- **Brute force investigation**
  - Contact IP sources of the "alarm"
    - Proved difficult
  - When there were responses, no significant systemic reason
  - Many dynamic addresses, raising questions about known use cases (running a DNS server on a dynamic address?)
- **Is the data clean?**
  - Doubt about the measurement accuracy
- **Look for some systematic cause**
  - No identifiable fault in popular DNS code

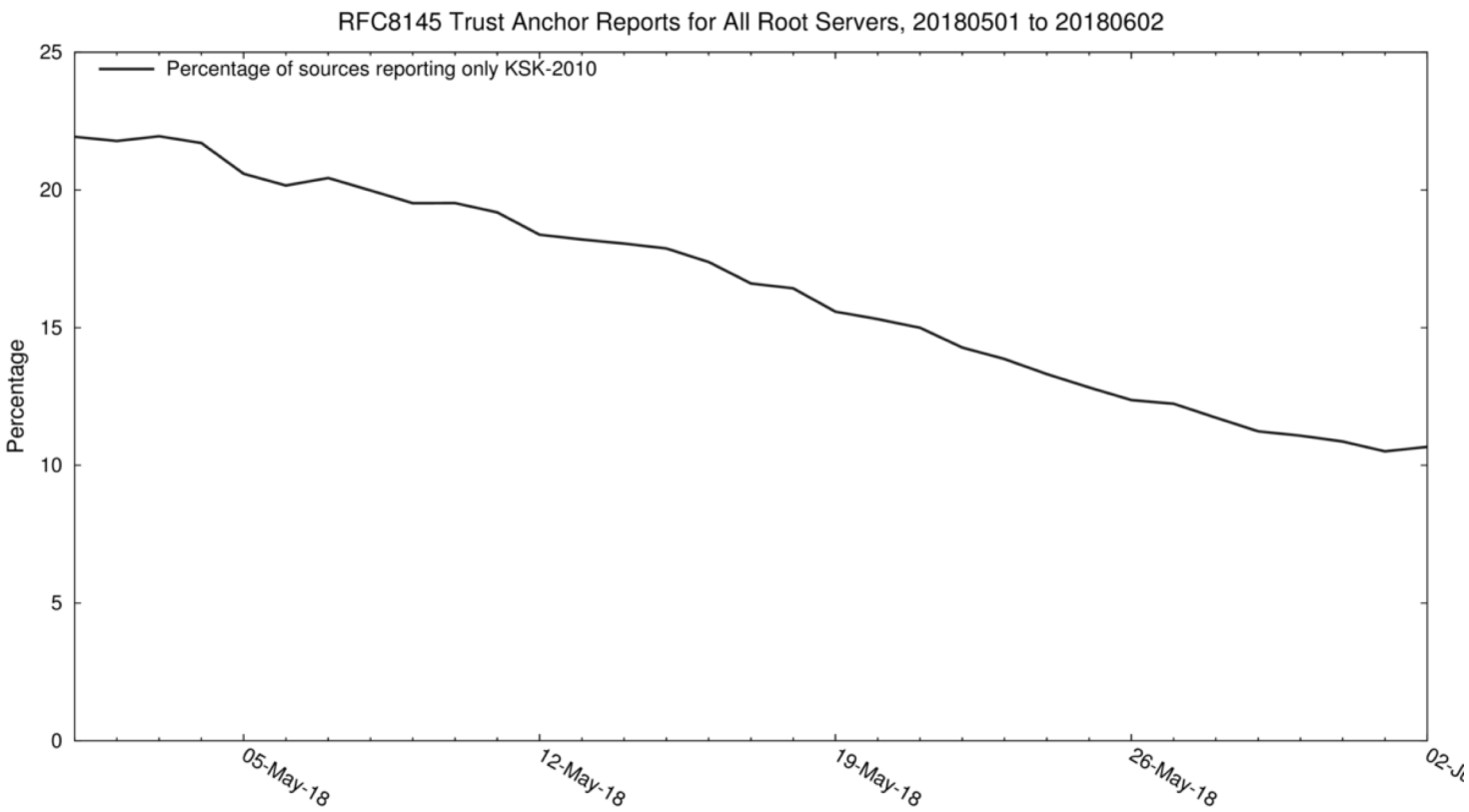
Decision to Pause the Rollover

- **September 2017, paused due to uncertainty**

- **No fault in the project plan or execution**
  - (Which would have made this easier to fix)
  - Found that the plan's "backout/fallback" plans worked, no work was needed to enter the pause state

- **ICANN has engaged the community for ways forward**
  - Proposed an updated plan, asked for public comment
  - Open to external research on the issue
    - We don't have all the data, we can't/shouldn't in some cases

Progress in the Last Month



More Graphs

- **http://root-trust-anchor-reports.research.icann.org/**
  - Graphs for each reporting root server

- **Also a list of addresses that reported the KSK-2010 only**
  - For inspecting, tracking down the operators and hopefully fixing

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
```

"Root"

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” (despite the pause)**
  - The KSK is changed under good conditions
  - Slow and cautious approach
  - Following the *Automated Updates of DNSSEC Trust Anchors* protocol (also known as "RFC 5011")
- Most appropriate point regarding "Automated Updates"
  - Requires 30 days to adopt the new key, but the "required 30 days" has long since past

Rollover Process (Validator view)

- **Assumes DNSSEC is operating/configured to run**
  - The KSK rollover following the Automated Updates process
    - But the original add hold down time has expired
  - (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?**

How To See Whether a DNS Cache Validates?

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

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 validation is enabled!

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 validation is disabled!

How To See Whether KSK-2017 is Trusted?

- **Tool Dependent**
  - 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
```

KSK-2017, aka 20326

KSK-2010, aka 19036

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 11:5 14 2017
;;query_failed: 0
;;query_interval: 43200
;;retry_time: 8640
. 172800 IN DNSKEY 257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBA MgJzkKTOiW1vkIbzxe /4RgWOq7HrxRi 1FlExOLAJr
mLvN7SWXgnLh4+B5xQlNVz8Og8kvArM kOxVQuCaSnIDdD5LKyW d2n9WGe2R8PzgC 3EgVLrjyBxW zF
0jLHwVN8efS3rCj/EWgvIWgb9ta DK/b58Da+sqqls3eNb /pr+eoZG+SrD eL3c6H5Apxz7 jVc1
uTIdsIXxuOLYA4/ilBmSVIzuDW fhHdY6+cn8HFRm+2 AnXGXws9555Kr ihylGa8subX n6UwN
R1AkUTV74bU= ;{id = 20326 (ksk), size = 2048 ; ;;state=2 [  VALID  ] ;;count 0
;;lastchange=1502438004 ;;Fri Aug 11 03:5 .24 2017
. 172800 IN DNSKEY 257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29eu hVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjw 0YI0EzrAcQqB
GCzh/RStIoO8g0NfnfL2MTJRkxoXbfD VPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/Q kjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1a N9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCT PJ8LbqF6dsV6DoB
Qzgul0sGIcGOYl7OyQdXfZ57re ageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLK dfwhYB4N7knNnulq
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

What if KSK-2017 is not trusted?

- **Again, tool dependent**
  - https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

Symptoms of the Wrong Trust Anchor

- **DNSSEC validation fails for everything, resulting from an inability to build a chain of trust**
- **All DNS responses will "SERVFAIL"**
  - Even if the target zone is not DNSSEC signed
- **Look in logs for validation failures, implementation specific**

Where to Get KSK-2017 Manually

- **Via the official IANA trust anchor XML file at https://data.iana.org/root-anchors/root-anchors.xml**
- **Via DNS (i.e., ask a root server for "./IN/DNSKEY")**
- **Most software/OS distributions of DNSSEC**
  - When tech refreshing code, double-check configurations
- **Compare with the key from these slides**
- **Obtain a copy from another operator, or other trusted source**
  - How well do you trust "them"?

The Future

- **Revocation of KSK-2010 in ~~2018~~ the future**
  - 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

- **A python-language script to retrieve KSK-2010 and KSK-2017**
  https://github.com/iana-org/get-trust-anchor

- **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

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