



2017 DNSSEC KSK Rollover

edward.lewis@icann.org | NANOG 69 | February 7, 2017

What is the purpose of this talk?

1

To publicize the
new Root Zone
DNSSEC KSK

2

Provide status,
upcoming events,
and contact
information

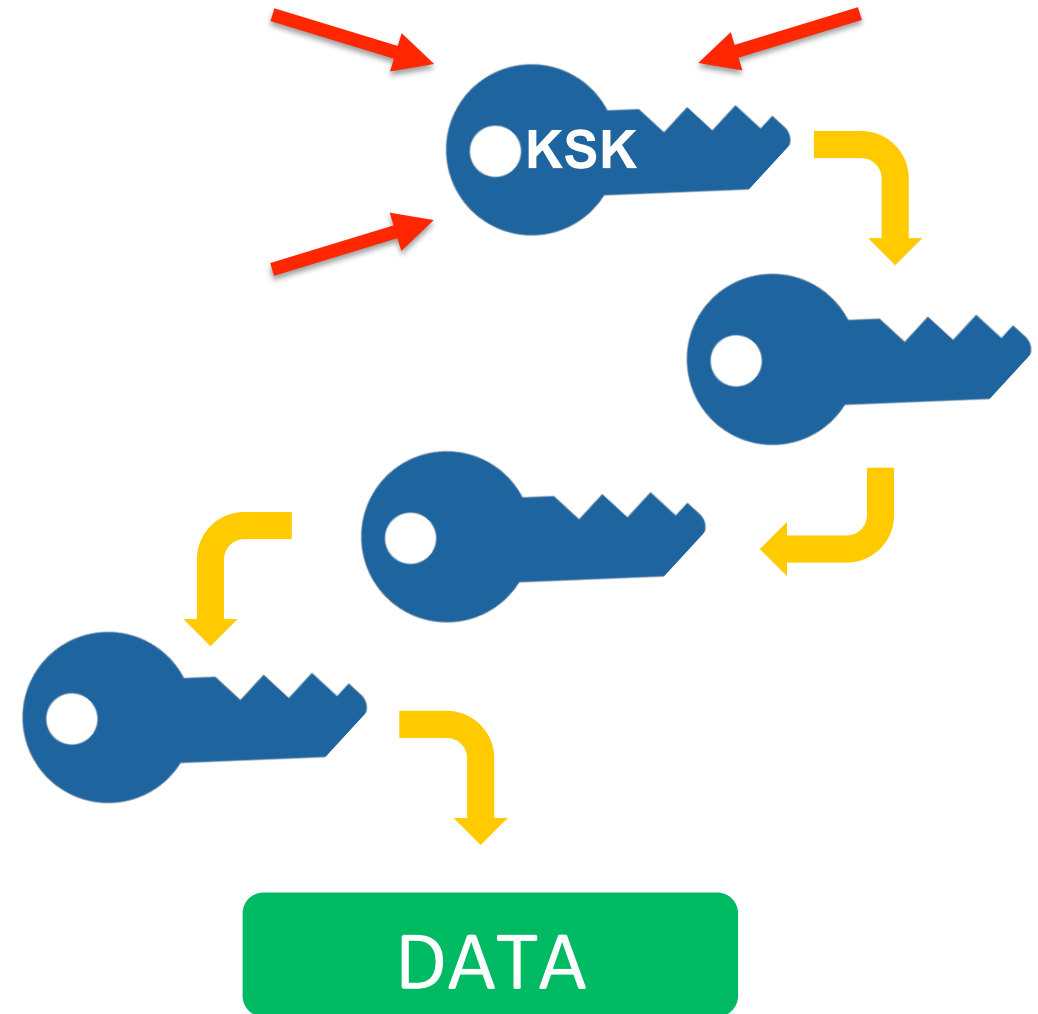
3

Provide helpful
resources on
the KSK roll



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
- ⦿ Public portion of the KSK is configuration parameter in DNS validating revolvers



What does it mean to rollover 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

What are the rollover's milestones?

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

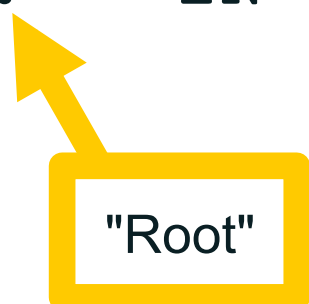
How can the new key be recognized?

- ◉ **The KSK-2017's Key Tag 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

What does the new DNSKEY Resource Record look like?

◎ For KSK-2017, 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

Why are there DS and DNSKEY forms of KSK-2017?

- ⦿ **Tools that you will use to manage DNSSEC trust anchor configurations work on either the DS form, the DNSKEY form or both**
 - ⦿ Per tool, historical reasons
 - ⦿ The DS record contains a hash of KSK-2017
 - ⦿ The DNSKEY record contains the public key of KSK-2017
- ⦿ **Consult your tool's documentation to know which is appropriate**



What is the 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
- ⊙ Recommended course of action – rely on RFC 5011’s *Automated Updates of DNSSEC Trust Anchors* protocol

- ⊙ **Why mention this?**

- ⊙ Alternative to *Automated Updates* is bootstrapping (or establishing an initial state of trust in) a trust anchor
- ⊙ That would be necessary in stormy (emergency) conditions



What is *Automated Updates of DNSSEC Trust Anchors*?

⦿ ***Automated Updates of DNSSEC Trust Anchors*** (RFC 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
- ⦿ Defined "add hold" time is 30 days



How does this look on a calendar?

July 2017						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

KSK-2017
appears
in DNS

August 2017						
S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

KSK-2017
should be
trusted

September 2017						
S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

October 2017						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

KSK-2017
starts
signing

What does it mean if you rely on *Automated Updates*?

⦿ **On 11 July 2017**

- ⦿ KSK-2017's DNSKEY record will appear in the DNS root key set
- ⦿ Tools following RFC 5011 will start counting days

⦿ **After 11 August 2017 (give or take a day)**

- ⦿ Your tool should see KSK-2017 in its trust anchor database
- ⦿ If not, debugging is needed, you have a few weeks to fix
- ⦿ (Don't panic if it's not immediate, remember time zone, etc.)

⦿ **On 11 October 2017**

- ⦿ KSK-2017 goes "live," validation ought to be confirmed



What is favorable about *Automatic Updates*?

- ⦿ **Many DNSSEC validation tools have RFC 5011 support built-in**
 - ⦿ The support needs to be configured properly, consult your administrator guide
 - ⦿ All in all, nothing an operator can't handle
- ⦿ **You can choose to "do it the hard way"**
 - ⦿ You do have options
 - ⦿ We are providing the keys in different ways to help



Is *Automated Updates* or a manual approach preferred?

- ⦿ **Mindful that the choice is a matter of local policy**
 - ⦿ DNSSEC validation is for the benefit of the receiver
 - ⦿ Not all operational environments are the same, not all validating tools implement *Automated Updates*
 - ⦿ We are doing our best to accommodate different approaches
- ⦿ ***Automated Updates* is likely the preferred approach**
 - ⦿ Relies only on what has been trusted before
 - ⦿ It's the most reliable/stable approach, simplest basis for trust



How can the new key be obtained and verified automatically?

- ⦿ **If you are DNSSEC validating with KSK-2010**

- ⦿ You can simply follow *Automated Updates of DNSSEC Trust Anchors* by configuring your tool of choice to do so



How can the new key be obtained and verified 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**
 - ⊙ If you trust the presentation copy you've seen here
- ⊙ **Obtain a copy from another operator, or other trusted source**
 - ⊙ How well do you trust "them"?
- ⊙ **Perhaps it will be on a trinket too**
 - ⊙ Not promising one, but...



What is get_trust_anchor.py?

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

https://github.com/kirei/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



What does an operator need to do?

- ⦿ **Be aware whether DNSSEC is enabled in your servers**
- ⦿ **Be aware of how trust is evaluated in your operations**
- ⦿ **Test/verify your set ups**
- ⦿ **Inspect configuration files, are they (also) up to date?**
- ⦿ **If DNSSEC validation is enabled or planned in your system**
 - ⦿ Have a plan for participating in the KSK rollover
 - ⦿ Know the dates, know the symptoms, solutions



What tools are available for DNSSEC validation?

⊙ **ISC's BIND**

⊙ **NLnet Lab's Unbound**

⊙ **Microsoft Windows**

⊙ **Nominum Vantio**

⊙ **CZnic's Knot Resolver**

⊙ **DNSMASQ**

⊙ **Secure64 DNS Cache**

⊙ **PowerDNS Recursor**



What is special about BIND?

- ⦿ **Blog post from ISC**

<https://www.isc.org/blogs/2017-root-key-rollover-what-does-it-mean-for-bind-users/>

- ⦿ **Unique to BIND**

- ⦿ Because of BIND's long DNSSEC history, some "named.conf" files may have to be updated despite tech-refresh of BIND versions

- ⦿ Notably, the introduction of managed-keys in ***February 2010***, (ISC's version 9.7) an update to trusted-keys

- ⦿ **I.e., Check pre-February 2010 configurations!**



What about Microsoft Server?

- ◉ **Extensive Documentation**

- ◉ *DNSSEC and Windows: Get Ready, 'Cause Here It Comes! (2010)*

- <https://channel9.msdn.com/Events/TechEd/NorthAmerica/2010/WSV333>

- ◉ *DNSSEC in Windows Server 2012 (updated 2014)*

- <https://technet.microsoft.com/library/dn593694>



What about other tools?

◎ **Unbound**

https://sched.ws/hosted_files/icann572016/49/Jaap-Akkerhuis-Unbound-KSK-rollover.pdf

◎ **PowerDNS**

<https://doc.powerdns.com/md/recursor/dnssec/#trust-anchor-management>

◎ **Knot Resolver**

<https://knot-resolver.readthedocs.io/en/latest/daemon.html#enabling-dnssec>

◎ **DNSMASQ**

[http://www.thekelleys.org.uk/dnsmasq/CHANGELOG_\(see v2.69 notes\)](http://www.thekelleys.org.uk/dnsmasq/CHANGELOG_(see_v2.69_notes))



What are signs of a DNSSEC problem related to the rollover?

⦿ **Problems caused by IPv6 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

⦿ **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 check failures, implementation specific



What are the steps to recovery?

- 1. Stop the tickets!** It's OK to turn off DNSSEC validation while you fix (but do turn it back on!)
- 2. Debug.** If the problem is the trust anchor, find out why it isn't correct
 - ⦿ Did RFC 5011 fail? Did configuration tools fail to update the key?
 - ⦿ If the problem is fragmentation related, make sure TCP is enabled and/or make other transport adjustments
- 3. Test the recovery.** Make sure your fixes take hold



What educational/informational resources are available?

- ◎ **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



What ICANN's live test bed resources?

- ⦿ **ICANN is finalizing a test bed to allow operators to test whether configurations follow *Automated Updates***
 - ⦿ The goal is to use production settings with real-but-test DNS zones, running in real time
 - ⦿ A full test will need to run more than 30 days
- ⦿ Information on the test bed will appear on the ICANN KSK rollover page
 - <https://www.icann.org/resources/pages/ksk-rollover>



How can you engage with ICANN?



Thank You and Questions

Join the ksk-rollover@icann.org mailing list

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

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



twitter.com/icann
Follow #Keyroll



soundcloud.com/icann



facebook.com/icannorg



weibo.com/ICANNorg



youtube.com/user/icannnews



flickr.com/photos/icann



linkedin.com/company/icann



slideshare.net/icannpresentations

