



# 2017 DNSSEC KSK Rollover

[champika.wijayatunga@icann.org](mailto:champika.wijayatunga@icann.org) | MENOG17 | May 20, 2017

# Purpose of this Talk

1

To publicize the  
new Root Zone  
DNSSEC KSK

2

Provide status,  
upcoming events,  
and contact  
information

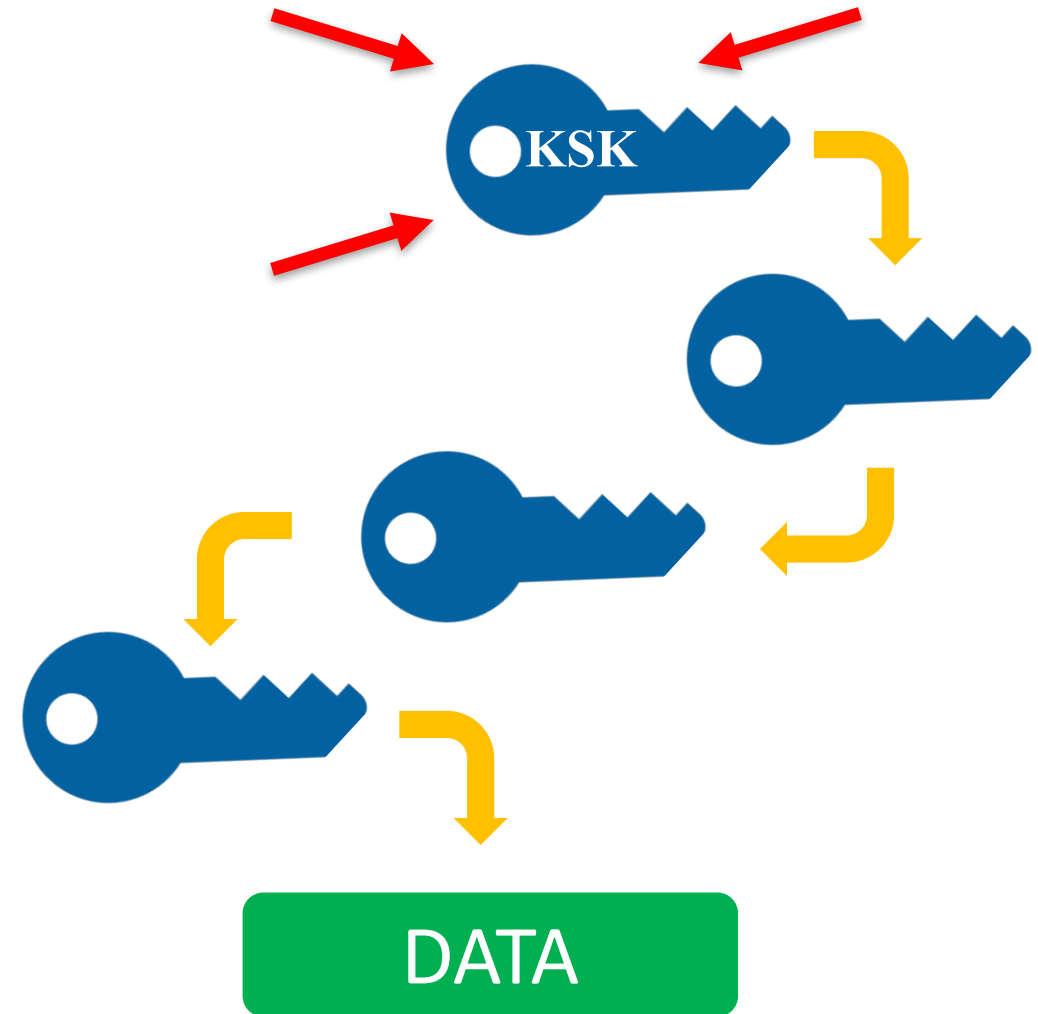
3

Provide helpful  
resources on  
the KSK roll



# 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



# 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	<del>October 27, 2016</del>
Production Qualified	<del>February 2, 2017</del>
Out-of-DNS-band Publication	Now, onwards
In-band ( <i>Automated Updates</i> ) 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

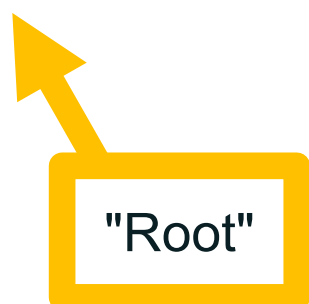
# Recognizing KSK-2017

## ◎ The KSK-2017's Key Tag 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*

## ◎ The DNSKEY resource record will be:

. 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**
  - ⦿ For each tool there are 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**





# 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
- ⊙ 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



# Automated Updates timetable

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

# Important dates when following *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 if KSK-2017 isn't trusted on August 11, 2017?

## ⦿ **Don't Panic!**

- ⦿ There are nearly two months to examine why, fix, and test before KSK-2017 "goes live"
- ⦿ Begin to investigate early but there is no need to rush a fix
- ⦿ Resources to consult are listed later in the slides

# Why is *Automatic Updates* in use?

- ⦿ **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
  - ⦿ ICANN is publishing KSK-2017 in different ways to help



# Preferred Approach

- ⦿ **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*
  - ⦿ ICANN is doing its 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



# Establishing Trust in KSK-2017 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



# Establishing Trust in 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**
  - ⊙ 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...



# Call to Action

- ⊙ All the work is for operators, developers and distributors of software that performs DNSSEC validation – keep reading/listening!
- ⊙ What if you're not one of them? What if you're an Internet user?
  - ⊙ Be aware that the root KSK rollover is happening on **11 October 2017**
  - ⊙ Do you know a DNS operator, software developer or software distributor?
    - ⊙ Ask them if they know about the root KSK rollover and if they're ready
    - ⊙ Direct them to ICANN's educational and information resources



# 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



# DNSSEC validation-enabled tools

⊙ **ISC's BIND**

⊙ **NLnet Lab's Unbound**

⊙ **Microsoft Windows**

⊙ **Nominum Vantio**

⊙ **CZnic's Knot Resolver**

⊙ **DNSMASQ**

⊙ **Secure64 DNS Cache**

⊙ **PowerDNS Recursor**



# Symptoms of a 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 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

# Three 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



- ⦿ **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>



# How can you engage with ICANN?



## Thank You and Questions

Join the [ksk-rollover@icann.org](mailto: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](https://twitter.com/icann)  
***Follow #Keyroll***



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



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



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



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



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



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



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

