



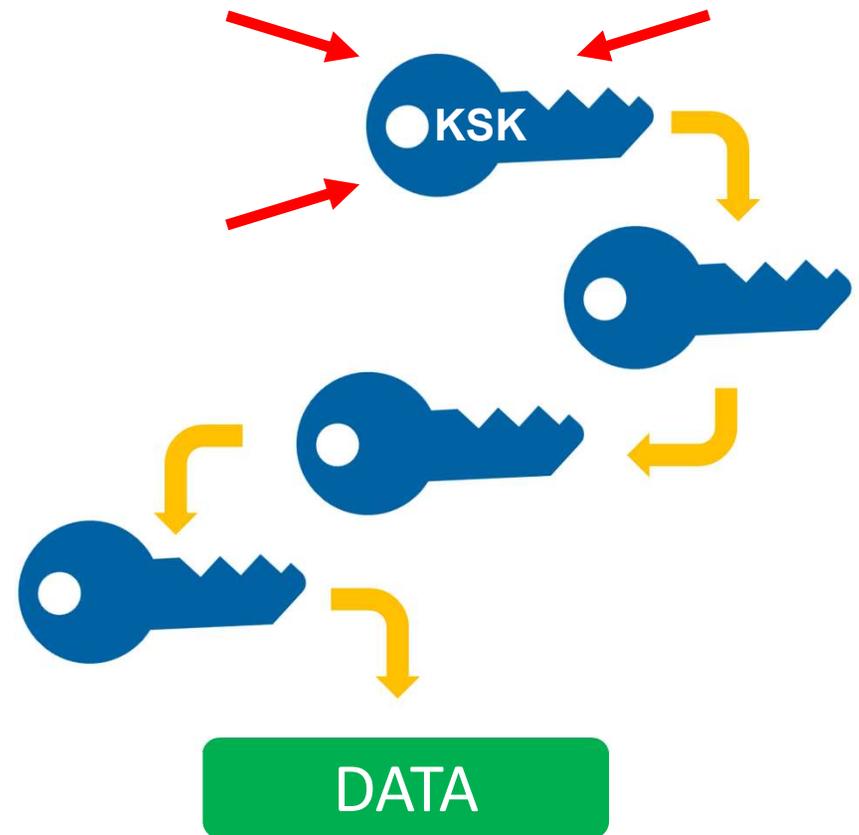
Root Zone KSK Rollover Update

Dr. Richard Lamb

richard.lamb@icann.org | ENOG 13 | May 24, 2017

Root zone KSK

- ⦿ The root zone key-signing key (KSK) is the topmost cryptographic key in the DNSSEC hierarchy
- ⦿ The public portion of the KSK is a configuration parameter (*trust anchor*) in DNS validating revolvers



Root zone KSK rollover

- ⊙ **There has been one root zone KSK**
 - ⊙ Since the root was first signed in 2010
 - ⊙ Called “KSK-2010”
- ⊙ **A new KSK will be used starting on 11 October 2017**
 - ⊙ An orderly succession for continued smooth operations
 - ⊙ Called “KSK-2017”
- ⊙ **Operators of DNSSEC validating resolvers may have some work**
 - ⊙ As little as review configurations
 - ⊙ As much as install KSK-2017

Root KSK rollover milestones

Event	Date
Creation of KSK-2017	27 October 2016
Operationally Ready	2 February 2017
Out-of-DNS-band Publication	Now (and onward)
In-band Publication	11 July 2017 (onward)
Sign the root key set (the actual rollover)	11 October 2017 (onward)
Revoke KSK-2010	11 January 2018
Remove KSK-2010 from ICANN facilities	Dates TBD, 2018

DNSKEY resource record for KSK-2017

. IN DNSKEY 257 3 8

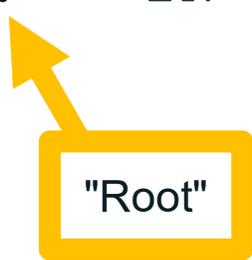
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
+/4RgWOq7HrxRixH1F1ExOLAJr5emLvN7SWXgnLh4+B5xQ1NVz8Og8kv
ArMtNROxVQuCaSnIDdd5LKyWbRd2n9WGe2R8PzgCmr3EgVLRjyBxWezF
0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqq1s3eNbuv7pr+e
oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
R1AkUTV74bU=

"Root"

Note: liberties taken with formatting for presentation purposes

Delegation Signer (DS) resource record for KSK-2017

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



Note: liberties taken with formatting for presentation purposes

Configuring KSK-2017 as a trust anchor

- ⊙ Any software doing DNSSEC validation must be configured with KSK-2017 as a trust anchor by **11 October 2017**
- ⊙ We are changing the KSK under good operational conditions
- ⊙ Leverage trust in KSK-2010 to distribute KSK-2017
- ⊙ Recommended course of action for operators – rely on RFC 5011's *Automated Updates of DNSSEC Trust Anchors* protocol
- ⊙ Alternative to *Automated Updates* is bootstrapping (i.e., establishing an initial state of trust in) a trust anchor



Automated Updates of DNSSEC Trust Anchors (RFC 5011)

- ⦿ Uses the current trust anchor(s) to trust a new KSK as a trust anchor
- ⦿ Allows for unattended DNSSEC validator operations
- ⦿ Requires time – if a new KSK appears and remains visible continuously for some specified time, it can be trusted
- ⦿ Defined “add hold-down” time is 30 days



Automated Updates timetable

- ⦿ **On 11 July 2017**

- ⦿ KSK-2017's DNSKEY record will appear in the root key set
- ⦿ DNS software following RFC 5011 will start the 30-day add hold-down timer

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

- ⦿ DNS software should have added KSK-2017 to trust anchor databases

- ⦿ **On 11 October 2017**

- ⦿ KSK-2017 used for signing the root key set
- ⦿ Must be configured in DNS software as a trust anchor for successful validation to continue



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

ICANN's automatic updates testbed

- ⊙ **On 13 March 2017, ICANN released a testbed to allow operators to test whether 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 *2017-03-05.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>***



ICANN's accelerated testbed

- ⦿ **Since 2015, ICANN has operated a testbed to allow software developers and other interested parties to test whether a product will follow *all phases of the KSK rollover***
 - ⦿ The goal is to test resolver software with a live test zone continually executing a KSK rollover in accelerated time
 - ⦿ A full test of all rollover phases lasts 27 minutes
 - ⦿ Using the testbed involves:
 - ⦿ Specially configuring your resolver software to operate in accelerated mode
 - ⦿ Configuring the current trust anchor at:
 - ⦿ ***<https://www.toot-servers.net>***



Call to action

- ⦿ All the work here is for operators, developers and distributors of software that performs DNSSEC validation
- ⦿ 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



Educational and informational resources

- ⦿ **Check out ICANN's main page for root KSK rollover information:**

<https://www.icann.org/kskroll>

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



Engaging 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



facebook.com/icannorg



youtube.com/user/icannnews



linkedin.com/company/icann



soundcloud.com/icann



weibo.com/ICANNorg



flickr.com/photos/icann



slideshare.net/icannpresentations

