2017 DNSSEC KSK Rollover

Edward.Lewis@icann.org | NLUUG | May 16, 2017

Purpose of this Talk

1

To publicize the new Root Zone DNSSEC KSK

2

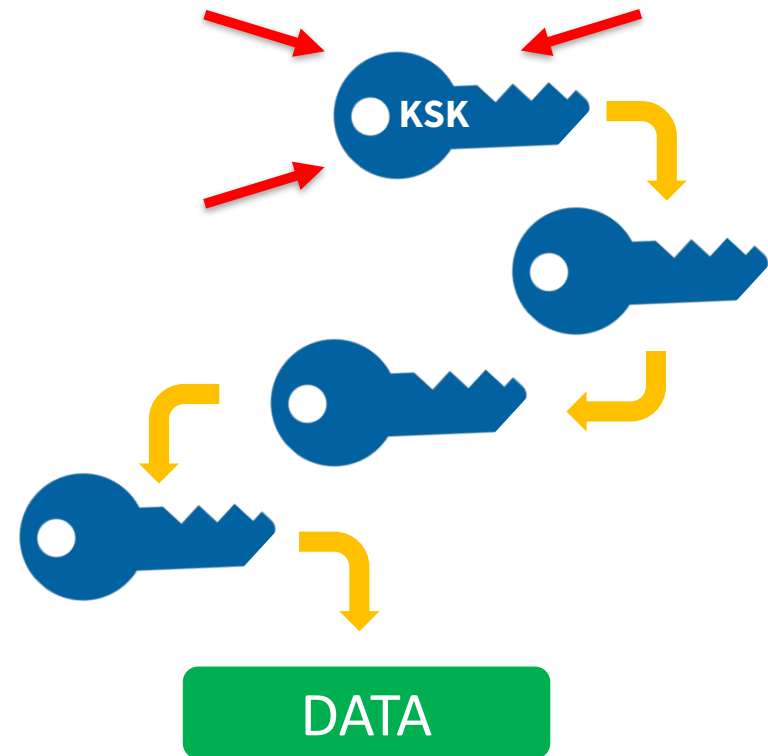Provide status, upcoming events, and contact information

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 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

Important Milestones

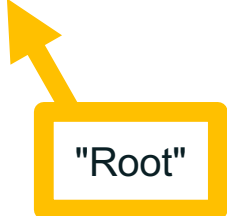| Event	Date
Creation of KSK-2017	~~October 27, 2016~~
Production Qualified	~~February 2, 2017~~
Out-of-DNS-band Publication	Now, onwards
In-band (*Automated Updates*) Publication	July 11, 2017 and onwards
Sign (Production Use)	**October 11, 2017** and onwards
Revoke KSK-2010	January 11, 2018
Remove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

Recognizing KSK-2017

- ⊙ **The KSK-2017's Key Tag 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 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
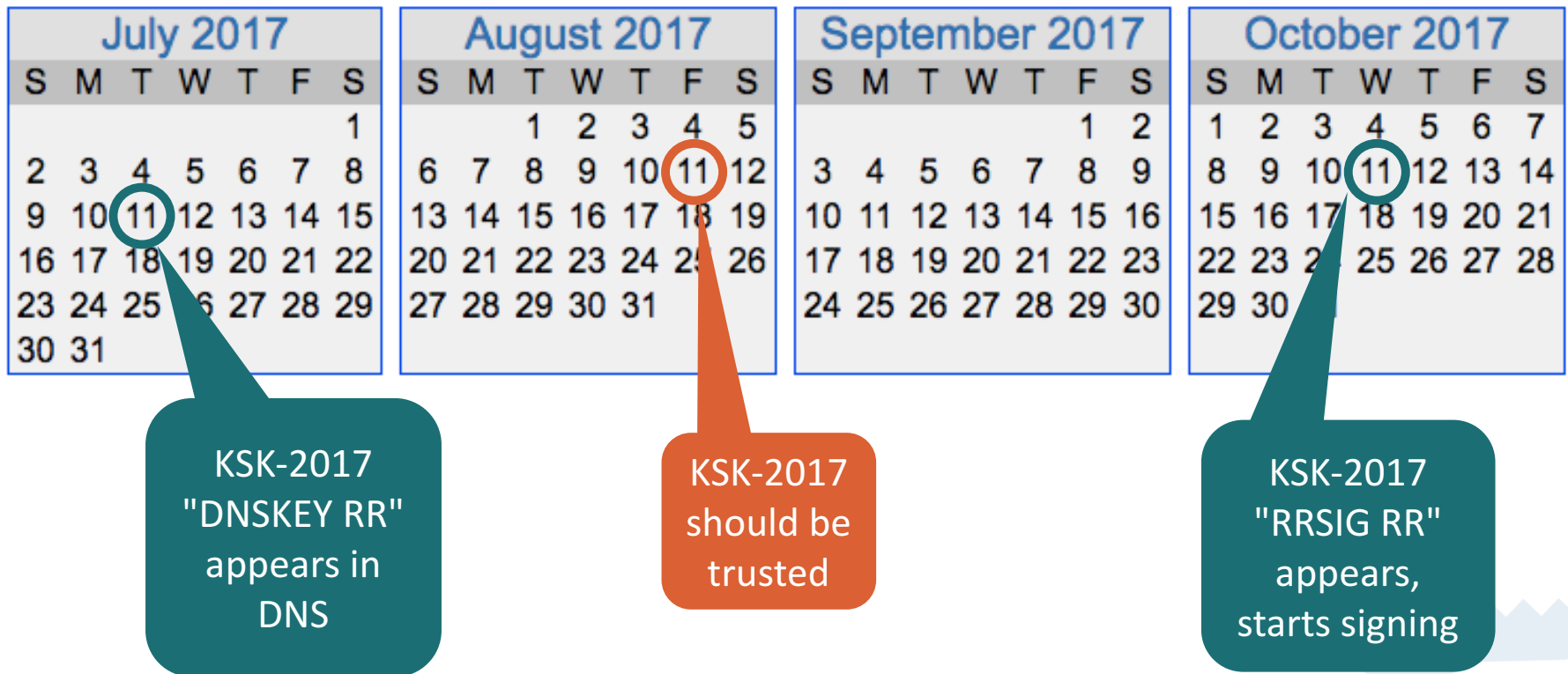⦿ That would be necessary in stormy (emergency) conditions

Automated Updates of DNSSEC Trust Anchors

⊙ **Defined in 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

Important dates when following *Automated Updates*

July 2017 — KSK-2017 "DNSKEY RR" appears in DNS (July 11)

August 2017 — KSK-2017 should be trusted (August 11)

October 2017 — KSK-2017 "RRSIG RR" appears, starts signing (October 11)

What if KSK-2017 isn't trusted on that day in August?

⊙ **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**
  - Consult your administrator guides/documentation

- **Under "good" conditions, safest way to transfer trust**
  - Only trust in KSK-2010 is "needed" to trust KSK-2017

- **For the root zone DNSSEC operator, most scalable way to reach the unknown operators using DNSSEC**
  - Entirely standards-based method

- **Still, establishing trust is subject to local (operator) policy**

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**
  - 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"?

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**

A Special Note About ISC's 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!**

Notes on 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

Information About Other Tools

⊙ **Unbound**
   https://schd.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)

Symptoms of a Problem 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

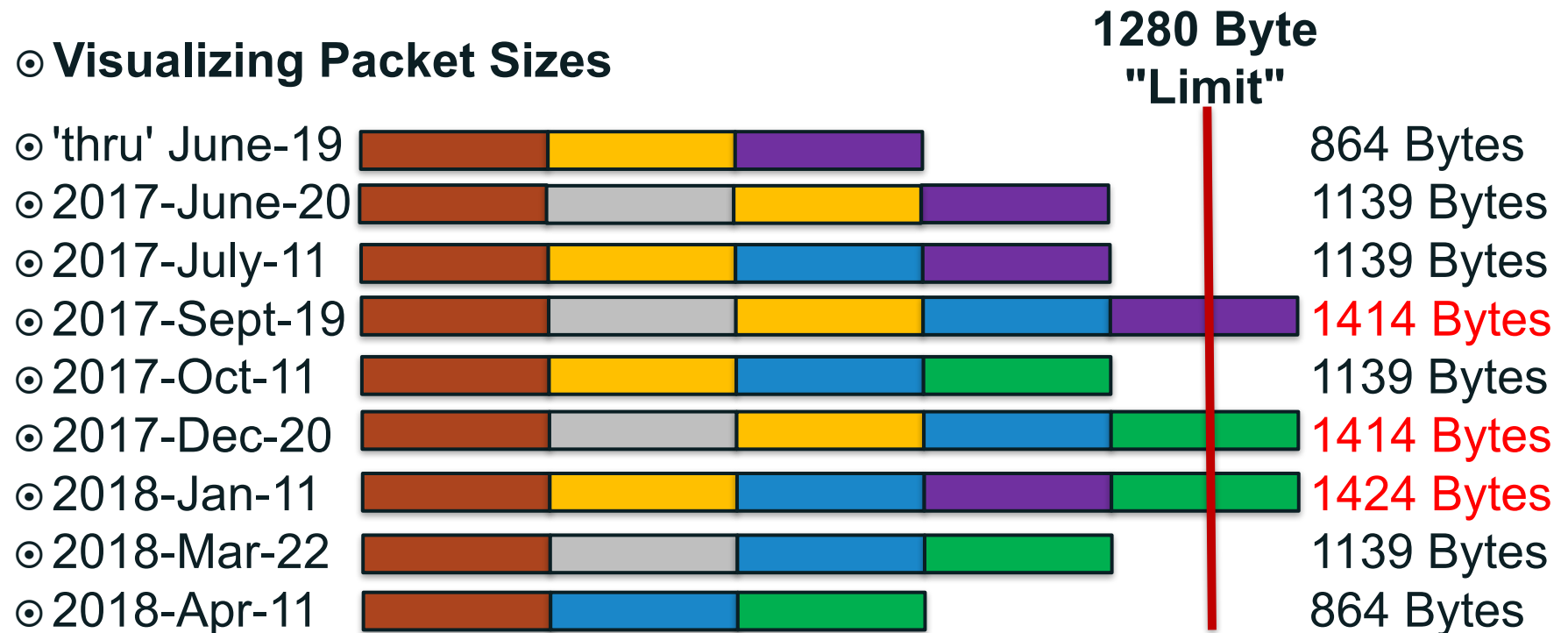◉ **IPv6's fragmentation feedback does not help DNS' use of UDP**
  ◉ No recollection (memory) of what was sent, can't resend

◉ **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**

1280 Byte "Limit"

⊙ 'thru' June-19	864 Bytes
⊙ 2017-June-20	1139 Bytes
⊙ 2017-July-11	1139 Bytes
⊙ 2017-Sept-19	1414 Bytes
⊙ 2017-Oct-11	1139 Bytes
⊙ 2017-Dec-20	1414 Bytes
⊙ 2018-Jan-11	1424 Bytes
⊙ 2018-Mar-22	1139 Bytes
⊙ 2018-Apr-11	864 Bytes

Current ZSK	Next ZSK	KSK-2010	KSK-2017	RRSIG-2010	RRSIG-2017

Experience with IPv6 Fragmentation and DNS

⊙ **Quantifying Concerns**

  ⊙ 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

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

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

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
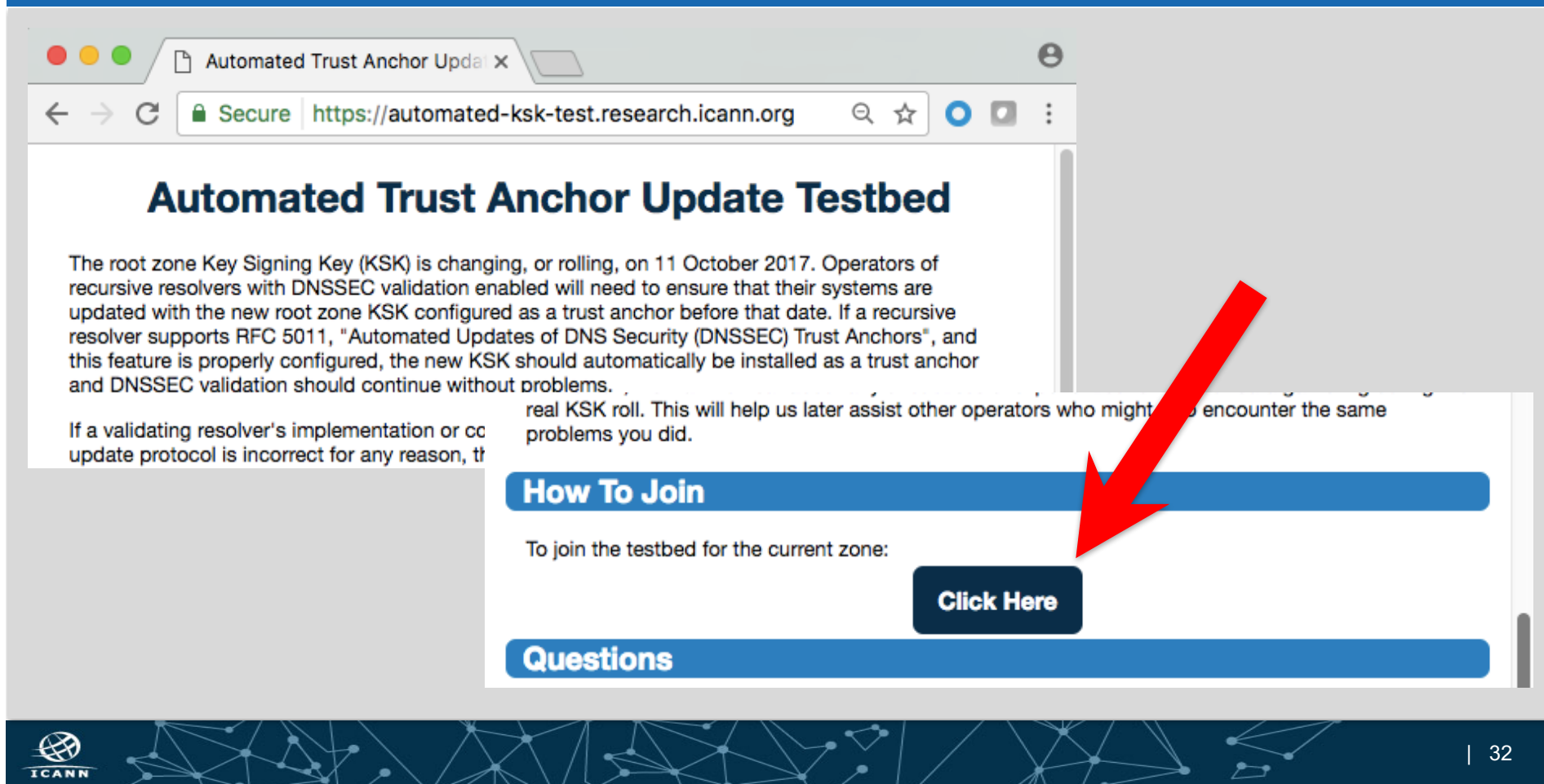
ICANN's *Automatic Updates* Testbed

- **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***

Signing Up For the Testbed

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

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