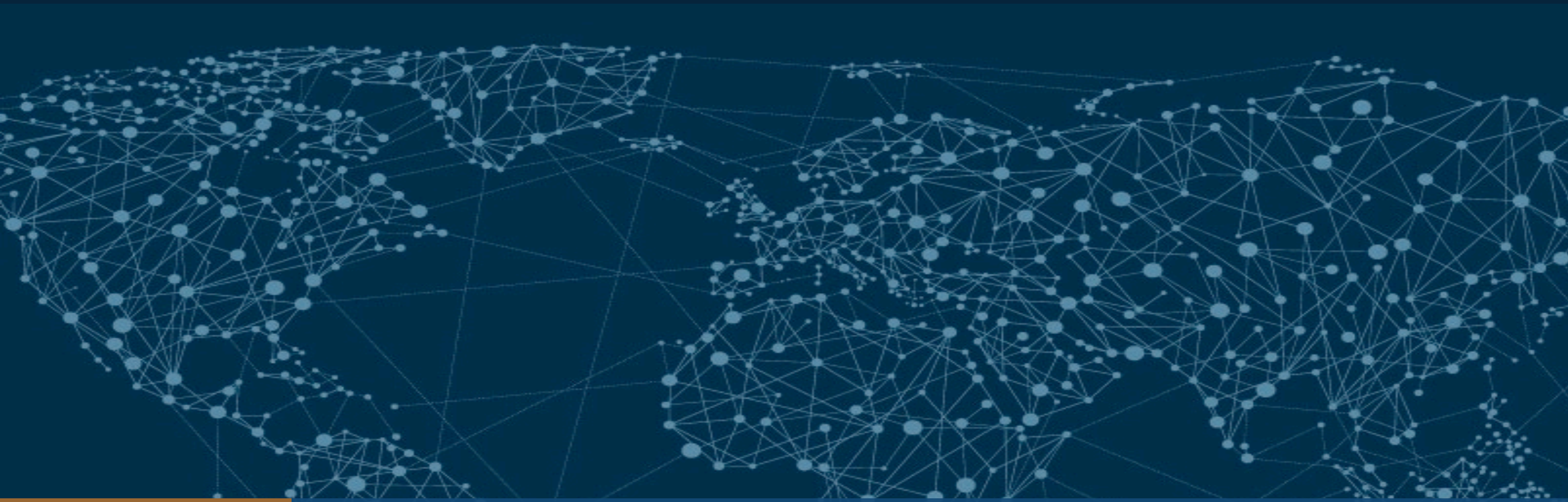


2017 DNSSEC KSK Rollover

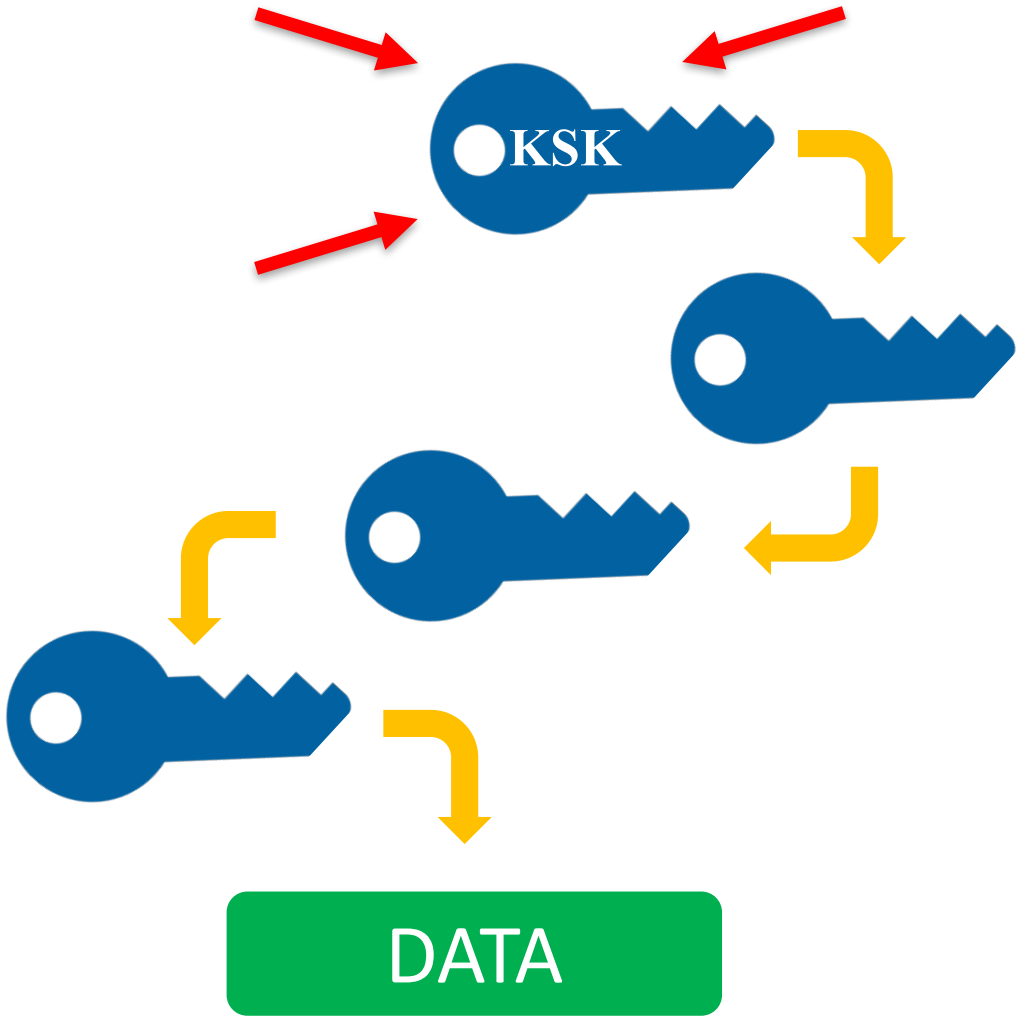
Carlos Martínez | LACNIC | *LACNIC 27, Foz Do Iguassú*

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	~~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

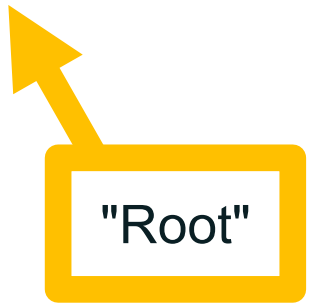
Recognizing KSK-2017

- **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
```



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

Automated Updates timetable

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 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?

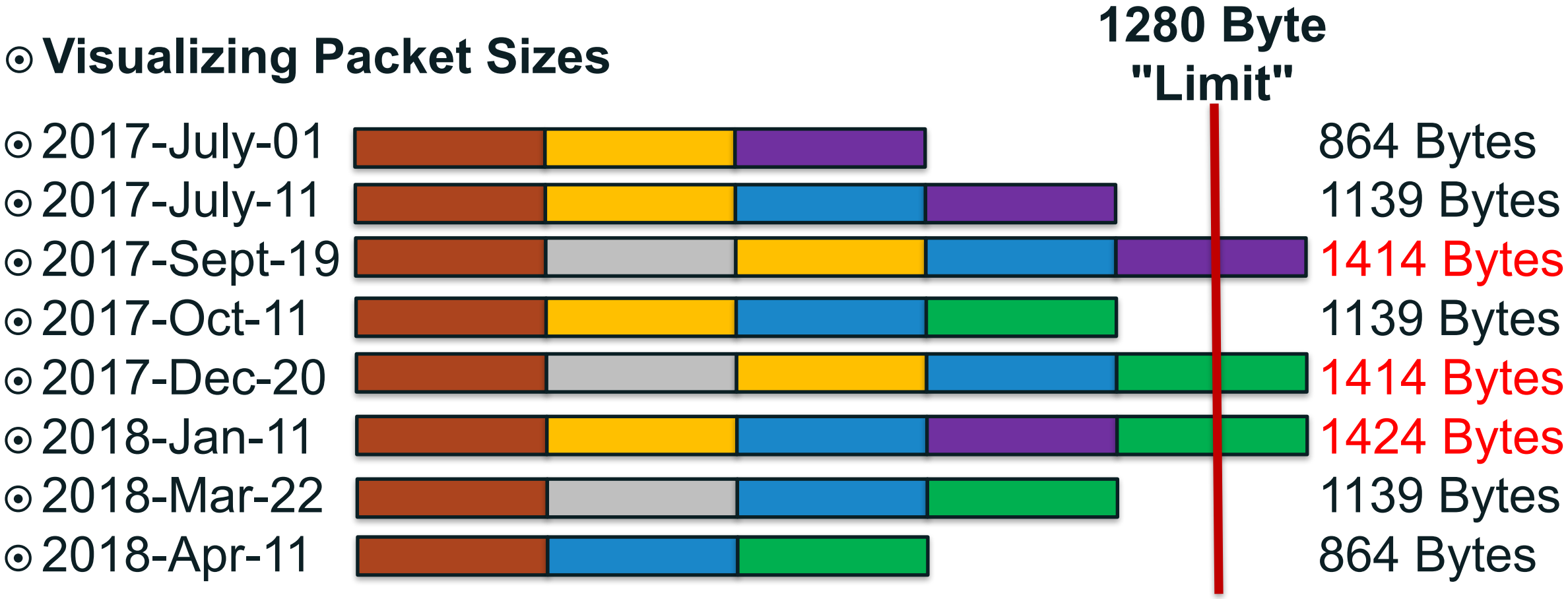
- **Many DNSSEC validation tools have RFC 5011 support built-in**
  - The support needs to be configured properly, consult your administrator guide
  - All in all, nothing an operator can't handle
- **You can choose to "do it the hard way"**
  - You do have options
  - ICANN is publishing KSK-2017 in 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

Impact on the KSK Rollover Process

- **Visualizing Packet Sizes**



Recommendation for IPv6

- **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
  - This is 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

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 *2017-03-05.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***

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

facebook.com/icannorg

youtube.com/user/icannnews

linkedin.com/company/icann

soundcloud.com/icann

weibo.com/ICANNorg

flickr.com/photos/icann

slideshare.net/icannpresentations