Rolling the Root Zone DNSSEC Key Signing Key

Edward Lewis | AFRINIC25 | November 2016
edward.lewis@icann.org

Motivation for this talk

- ICANN is about to change an important configuration parameter in DNSSEC

- For a network operator, this may create a need for action

- This discussion is meant to inform: Why this is happening, what is happening, and when
  - Highlighting: the availability of project plan documents
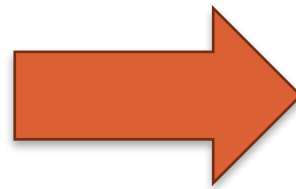
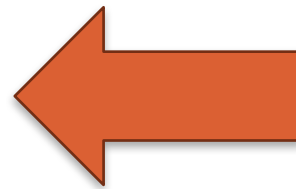**1** Trust Anchors & Root KSK

2 Root Zone DNSSEC

3 KSK Roll Project

DNS for Those Who Don't Like Protocols

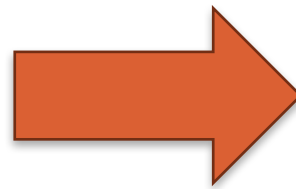What is the IPv6 address for www.example.com.?

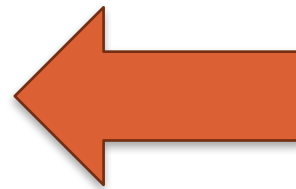www.example.com. is 2001:db8::

DNSSEC for Those Who Don't Like Protocols

What is the IPv6 address for www.example.com.?

www.example.com. is 2001:db8::

Digital signature by example.com.

What is DNSSEC Validation?

- Validation includes the process of inspecting the digital signature and the data to verify the answer is the appropriate one
  - The signature and data need a public key, a chain of keys, and a trust anchor
  - Software tools today can do this when configured

- Validation is more than a cryptographic check
  - Is the answer related to the question?
  - Is the answer "fresh", replayed, and so on?

Why Bother?

- Why bother?
  - The DNS protocol is gullible, easily fooled
  - Forged answers in DNS can result in misdirected traffic
  - Protect your DNS service, protect customers

- Validation is "self-protection"

- With DNSSEC as a base
  - Extensions to secure email transfer (stop spam)
  - Supplement to X.509 Certificate operations

Roles of Keys in DNSSEC

- DNSSEC has three kinds of records that, in some loose definition, hold cryptographic key data. The records exist because of the use of the data or "role"/"job"

  - KSK – Key Signing Key, produce signatures of keys
  - ZSK – Zone Signing Key, produces all other signatures
  - DS – Delegation Signer, a "pointer" to a key

- *This was supposed to simplify DNS operations!*

Crypto-checking a Signature

www.example.com. is 2001:db8::

Digital signature by example.com.

example.com. ZSK

?

✔

OR

✖

The Root

- root KSK
- root ZSK
- com. DS

.COM

- com. KSK
- com. ZSK
- example.com. DS

example

- example.com. KSK

example.com. ZSK
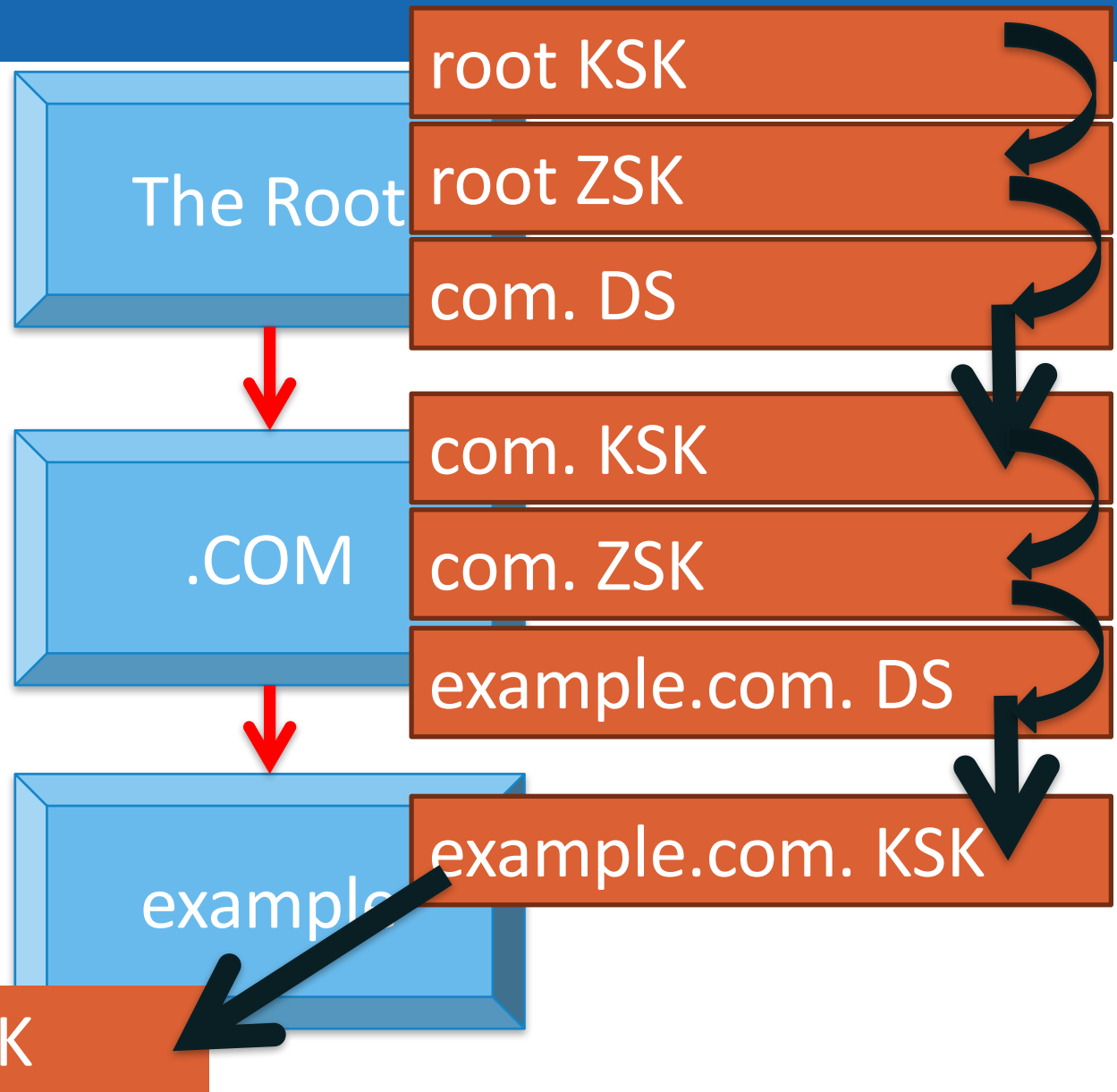
Over 1300 DNS - DNSSEC TLDs

The Root

.UK

.中国

.ORG

.COM

.NET

.INFO

.LK

.NL

root KSK

root ZSK

com. DS

net. DS

org. DS

lk. DS

uk. DS

Over 1300 DS sets!

+Over 500K in com...

Anchor of the Chain of Trust

The Root

.COM

example

root KSK

root ZSK

com. DS

com. KSK

com. ZSK

example.com. DS

example.com. KSK

example.com. ZSK
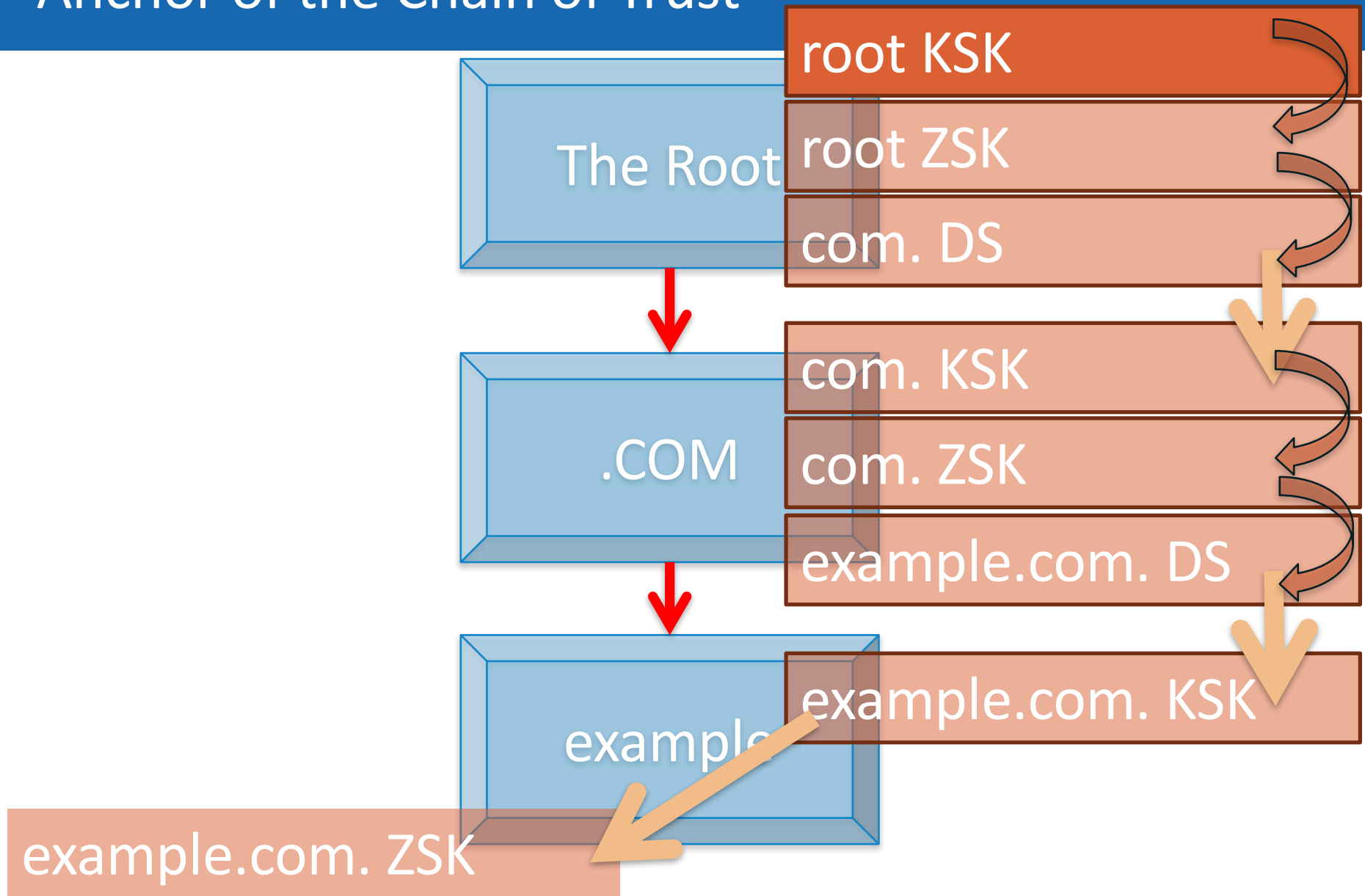
What is a Trust Anchor?

- Besides being the "top" of any DNSSEC validation process?

- A trust anchor is a key that an operator places full faith and trust into for the purposes of verifying responses
  - It could be implicitly trusted because it came with the software
  - It could be explicitly trusted via due diligence examination

Is the Root Zone KSK *the* Trust Anchor?

- Maybe
- It's really up to you

- By convention, there's a unique root zone, it has a KSK, for the global public Internet operated by ICANN
- By default, DNSSEC validation tools come configured with that KSK as *the* trust anchor

- But a user of the tools can add other trust anchors

1 Trust Anchors & Root KSK

2 Root Zone DNSSEC

3 KSK Roll Project

DNSSEC in the Root Zone

- DNSSEC in the Root Zone is managed by:
  - ICANN, responsible for operating the root KSK
  - Verisign, responsible for operating the root ZSK
- Operating the KSK
  - KSK lifecycle management, "sign the ZSK"
- Operating the ZSK
  - ZSK lifecycle management, "sign the root zone"

- Activities are coordinated but operated separately

Current Root KSK

- The current root KSK was created in 2010
    - Stored in Hardware Security Modules in two Key Management Facilities
    - The operations surrounding the key is an entirely different talk

Getting the Root KSK (Public portion only!)

- Via the DNS
  - As reliable as the data in unprotected DNS
  - (Works if you not subject to an "attack")
- Via the Web
  - https://data.iana.org/root-anchors/root-anchors.xml
  - Secured by an X.509 certificate and signature
- Via other means
  - Code
  - Presentations, t-shirts, friends
  - Always remember to check the legitimacy!

Changing the Root KSK

- There is a plan in place to change the root KSK
  - For the first time

- This plan is precedent setting
  - Because it involves an uncountable roster of participants and impacted parties
  - When ICANN changes the KSK on our end -
  - Anyone who (anonymously) relies on it has to change a configuration on their end
  - No one can list all those involved – unless something goes wrong

Why (rock the boat)?

- Good cryptographic hygiene
  - Secrets don't remain secret forever

- Good operational hygiene
  - Have a plan, complete enough to execute
  - Exercise the plan under normal circumstances

- Why not a private test?
  - The change of the KSK involves everyone doing DNSSEC validation on the Internet, service operators, software producers

Bottom Line

- Changing the root KSK will impact just about all DNSSEC validations
  - If the trust anchor is "misconfigured" (i.e., the wrong key) DNSSEC will reject legitimate responses
  - To anyone or any process relying on DNS, it will appear that the desired data is unavailable, website is unreachable, "the Internet is down"

- There's a broader topic of trust anchor maintenance, but that is for another time

1
Trust Anchors
& Root KSK

2
Root Zone
DNSSEC

3
KSK Roll
Project

The KSK Rollover Project and Network Operators

- The project is meaningful to you if you are performing DNSSEC validation
  - Geoff Huston stats: steady 15% world wide
  - DNSSEC signing is not affected

- If you are validating it's time to revisit configurations and processes
  - A root KSK roll hasn't happened before, it's new to all of us

The KSK Rollover Plan Documents

- Available at: https://www.icann.org/kskroll
  - 2017 KSK Rollover Operational Implementation Plan
  - 2017 KSK Rollover Systems Test Plan
  - 2017 KSK Rollover Monitoring Plan
  - 2017 KSK Rollover External Test Plan
  - 2017 KSK Rollover Back Out Plan

- We encourage interested folks to given them a read

Overview of Project Plans

- Plans say - On October 11, 2017 a new KSK will go into use and the current KSK retired
  - On this day, if preparations haven't been made, trouble will ensue

- Plans include
  - Retaining the current cryptography settings
  - Following *Automated Updates of DNSSEC Trust Anchors*
  - Fitting the roll into normal maintenance events
  - Testing and monitoring

The Project's DNS Response Size Concerns

- Significant DNS responses will grow to 1425 bytes during the project

- Experimentation, especially in IPv6, suggests this might be a concern despite empirical evidence to the contrary

- How to avoid potential problems
  - Where UDP is allowed to port 53, also allow TCP
  - Refrain from filtering DNS messages based on size

IPv6 fragmentation and DNS

- IPv6 fragmentation is done by the sender with intermediate nodes using ICMP to indicate a fragment as being "too big"
  - By the time the DNS sender gets the ICMP, DNS has forgotten what it had sent

- From Geoff Huston experiments and analysis
  - http://www.potaroo.net/ispcol/2016-05/v6frags.html
  - TCP over IPv6 use an MTU of 1,280 bytes
  - UDP has marginal advantages with using larger MTU, "but"

Dates to Watch

- September 19, 2017
  - The root zone DNSKEY set will increase to 1414 bytes for 20 days, prior to that date 1139 bytes has been the high water mark

- October 11, 2017
  - On this date the root zone DNSKEY set will be signed only by the new KSK

- January 11, 2018
  - The root zone DNSKEY set will increase to 1425 bytes for 20 days

Trust Anchor Management

- How do you trust and configure?
  - Are trust anchors subject to configuration control?
  - Rely on embedded data in software?
  - Are DNSSEC validation failures monitored?

- Automated Updates of DNSSEC Trust Anchors
  - Most direct, reliable means for getting the key

- Negative Trust Anchor management – RFC 7646
  - Protects against errors made by others

Tools & Testbeds

- We are working with DNS software and tool developers and distributors
  - Management/troubleshooting aids
  - Updates of bundled keys

- Testbeds for Code Developers
  - Automated updates: http://keyroll.systems/
  - Root zone model: https://www.toot-servers.net/

- Testbeds for Service Operators
  - I.e., using "off-the-shelf" parameters
  - Planned for end-of-2016

For More Information

- Join the ksk-rollover@icann.org mailing list:
  - https://mm.icann.org/listinfo/ksk-rollover

- Follow on Twitter
  - @ICANN
  - Hashtag: #KeyRoll

- Visit the web page:
  - https://www.icann.org/kskroll

Engage with ICANN

Thank You and Questions

Reach me at:
Email: ksk-rollover@icann.org
Website: icann.org/kskroll

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations