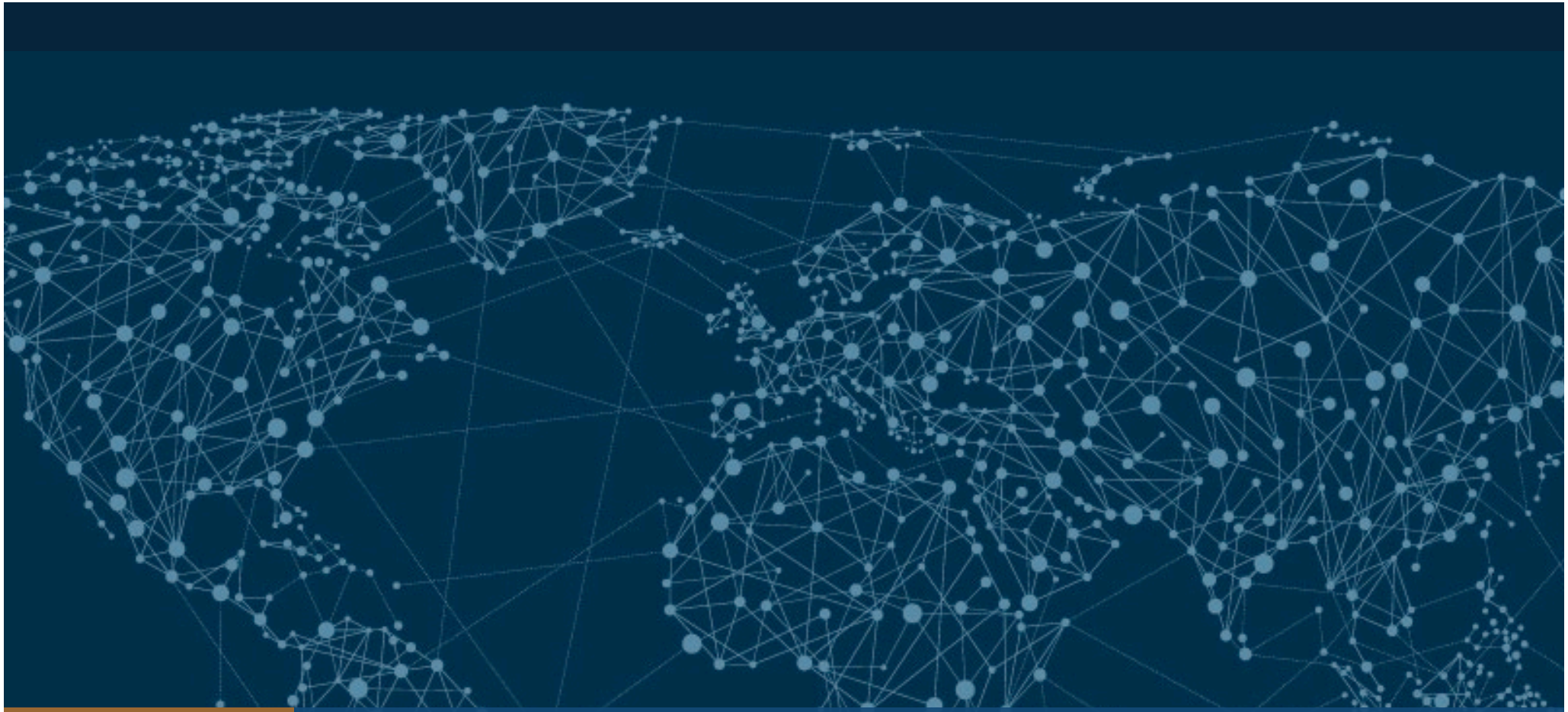


Rolling the Root Zone KSK

Matt Larson, VP of Research

Motivation for the Talk

- ICANN is about to change an important configuration parameter in DNSSEC
- For a DNS operator, this may create a need for action
- This discussion is meant to inform: What is happening, when, and what to do if troubleshooting is needed

DNSSEC in the Root Zone

- DNSSEC in the Root Zone is managed by:
  - ICANN, as the IANA Functions Operator
  - Verisign, as the Root Zone Maintainer (RZM)

- Some changes to the naming of the functions may happen in the future

DNSSEC Key Management in the Root Zone

- DNSSEC key management is divided into:
  - Key Signing Key (KSK), which signs just the keys
  - Zone Signing Key (ZSK), which signs other zone data

- These roles are meaningful to the operators of signed zones
  - The significance is that the roles are separated

KSK and ZSK

- ICANN, as IANA Functions Operator, manages the KSK
  - Same KSK since the root zone was signed in 2010
  - The KSK signs a new ZSK every quarter in a ceremony

- Verisign, as Root Zone Maintainer, manages the ZSK
  - ZSK is changed quarterly

Why Change the KSK?

- Primary reason – operational preparedness
  - KSK has no expiration date and currently no weakness
  - No key should live forever: bad crypto practice
  - DNSSEC Practice Statement states the key will be rolled
  - Prefer to exercise process in normal conditions
    - As opposed to abnormal, such as key compromise
- Big challenge
  - Involves countless/uncountable participants
  - No test environment can cover all possibilities

The KSK Roll Plan Documents

- The plan consists of five documents:
  - 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

- The documents were published in July, 2016, and are available at: https://www.icann.org/kskroll

Communications Approach

- Target technical audiences performing DNSSEC validation (e.g., Network Operating Groups)
  - Explain how to participate in the KSK rollover
- Broader communication
  - General awareness, resources available
- Integrated communications approach
  - Traditional channel (email, presentations)
  - Social media (#KeyRoll)
  - Leverage ICANN staff and stakeholder groups

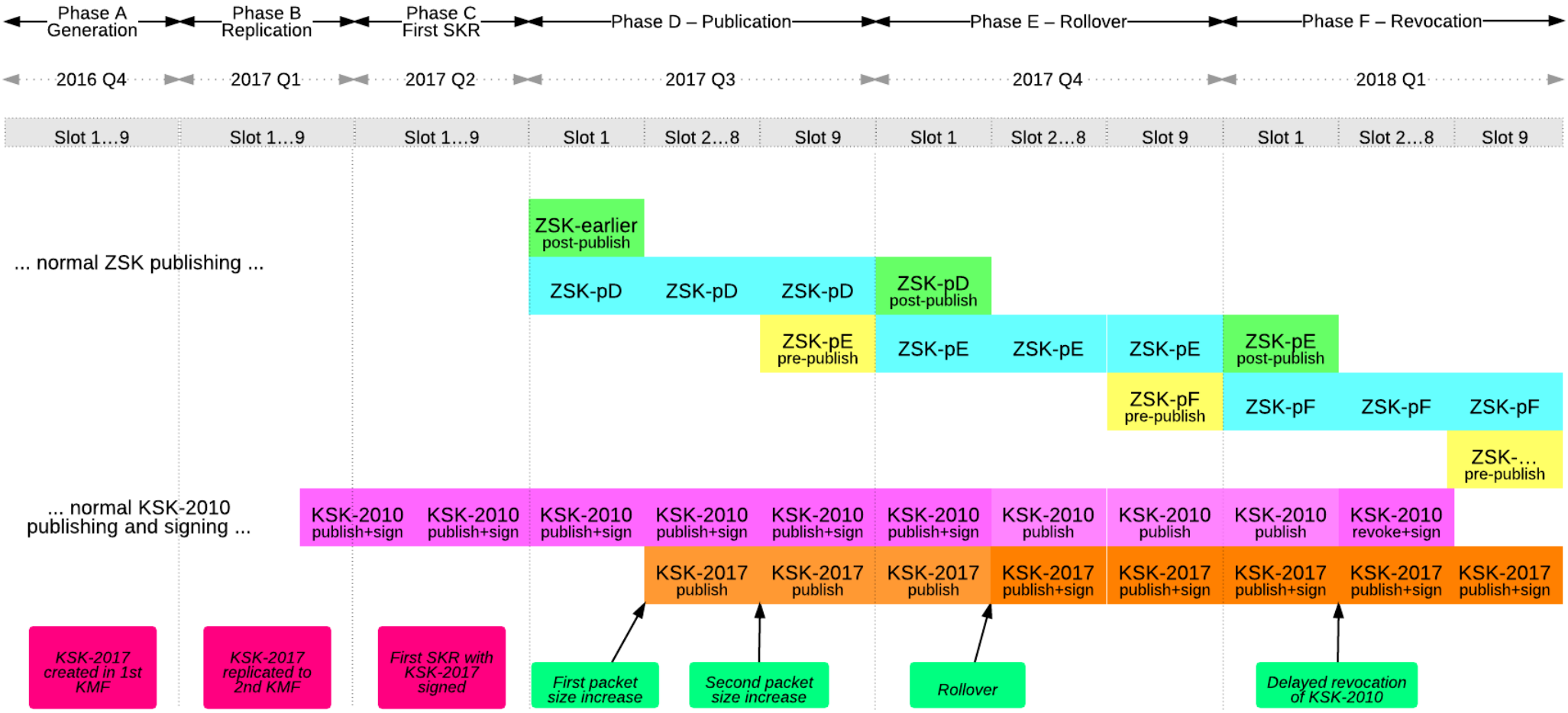
Operational Implementation Plan Phases

- Preparation Phases
  - System engineering, KSK creation and replication
  - Little to no operational impact on Internet
- Automated Updates (RFC 5011) Phases
  - KSK-2017 (new) pre-published, signed by KSK-2010 (current)
  - KSK-2010 is revoked
- Post Rollover Phases
  - Deletion of KSK-2010 from key management facilities
  - Project experiences documented

Operational Implementation Plan Dates

- Plans publicly available since July 22, 2016
- Key signing ceremonies
  - Q4 2016 ceremony (October 27): generate KSK-2017
  - Q1 2017 ceremony (February): KSK-2017 operationally ready
- DNS changes
  - KSK-2017 to be added to root zone on July 11, 2017 (with KSK-2010 still there)
  - **KSK-2017 signs DNSKEY RRset (instead of KSK-2010) beginning October 11, 2017**
  - KSK-2010 revoked on January 11, 2018, but is still in the root zone

Operational Implementation Plan Timeline



Systems Test Plan

- Key Management
  - Lifecycle
- Key Processing
  - Key Signing Request to Signed Key Response
- Trust Anchor Publication
  - Generation of the trust anchor file as formatted in eXtensible Markup Language (XML)

External Test Plan

- Resources targeted for software developers
  - Two third-party “accelerated” RFC 5011 test environments with accelerated clocks
    - http://toot-servers.net
    - http://keyroll.systems
- Resources more suitable for operators
  - “Real time” RFC 5011 test environment being developed by ICANN
  - Roll a test zone trust anchor with actual 30-day Add Hold-Down timer

Monitoring Plan

- Automated monitoring involving
  - ICANN's L-root server
  - Information Science Institute's B-root server
- Looking for:
  - Low-level fragmentation issues, indicating responses are too large
  - Elevated query rates for the DNSKEY resource record set, indicating misconfigured trust anchors
- Plus a means for ad hoc reporting

Back Out Plan

- Plan includes back out capability
  - If necessary, can stay in current state or back out at every phase
  - Until KSK-2010 is revoked in Phase F
- Multiple back out sets of DNSKEY records signed at each ceremony
  - Back out can be immediate
  - No need for extra key ceremony

What You Need to Know

- Manage Your Trust Anchors
  - Be aware of your software tools for managing trust anchors
  - Be aware of the new KSK
- When Events Happen
  - Keep an eye on dates
  - Be mindful of when changes are scheduled and monitor appropriately

Managing Trust Anchors

- Trust anchors are configured data in DNSSEC validators
  - If Automated Updates of DNSSEC Trust Anchors (RFC 5011) is enabled and working, the rollover is automatic
    - “Trust but verify”
  - Otherwise manual intervention is required
    - Add KSK-2017 before October 11, 2017 (assuming all is on track)
    - Remove KSK-2010 at a later date

To recap: Planned KSK Rollover Dates

- Plans publicly available since July 22, 2016
- Key signing ceremonies
  - Q4 2016 ceremony (October 27): generate KSK-2017
  - Q1 2017 ceremony (February): KSK-2017 operationally ready
- DNS changes
  - KSK-2017 to be added to root zone on July 11, 2017 (with KSK-2010 still there)
  - **KSK-2017 signs DNSKEY RRset (instead of KSK-2010) beginning October 11, 2017**
  - KSK-2010 revoked on January 11, 2018, but is still in the root zone

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 us 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