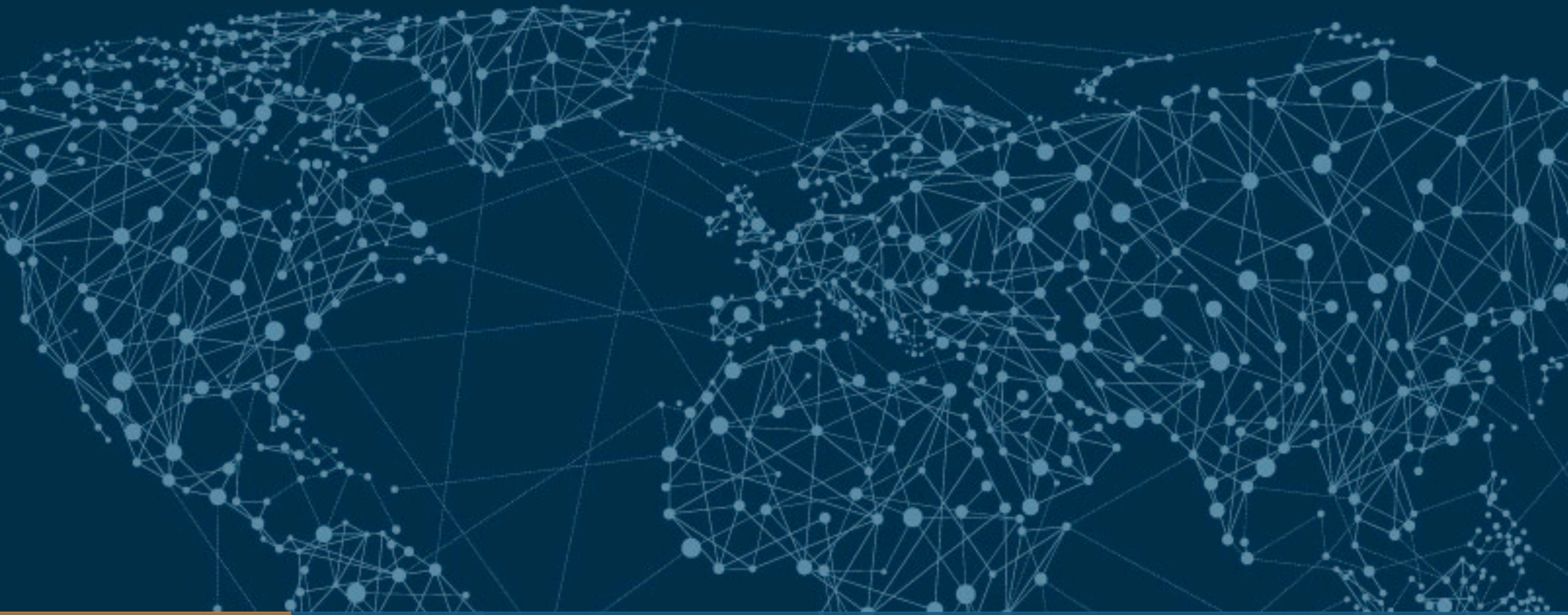


Rolling the Root Zone DNSSEC Key Signing Key

Motivation for the Talk

- ICANN is about to change an important configuration parameter in DNSSEC
- For a network 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), self-signs the key set
  - Zone Signing Key (ZSK), 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 operations began in 2010
    - The KSK signs the ZSK quarterly 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, 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 are available at: https://www.icann.org/kskroll

Communications Approach

- Target technical audiences performing DNSSEC validation (e.g., Network Operating Groups)
  - 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

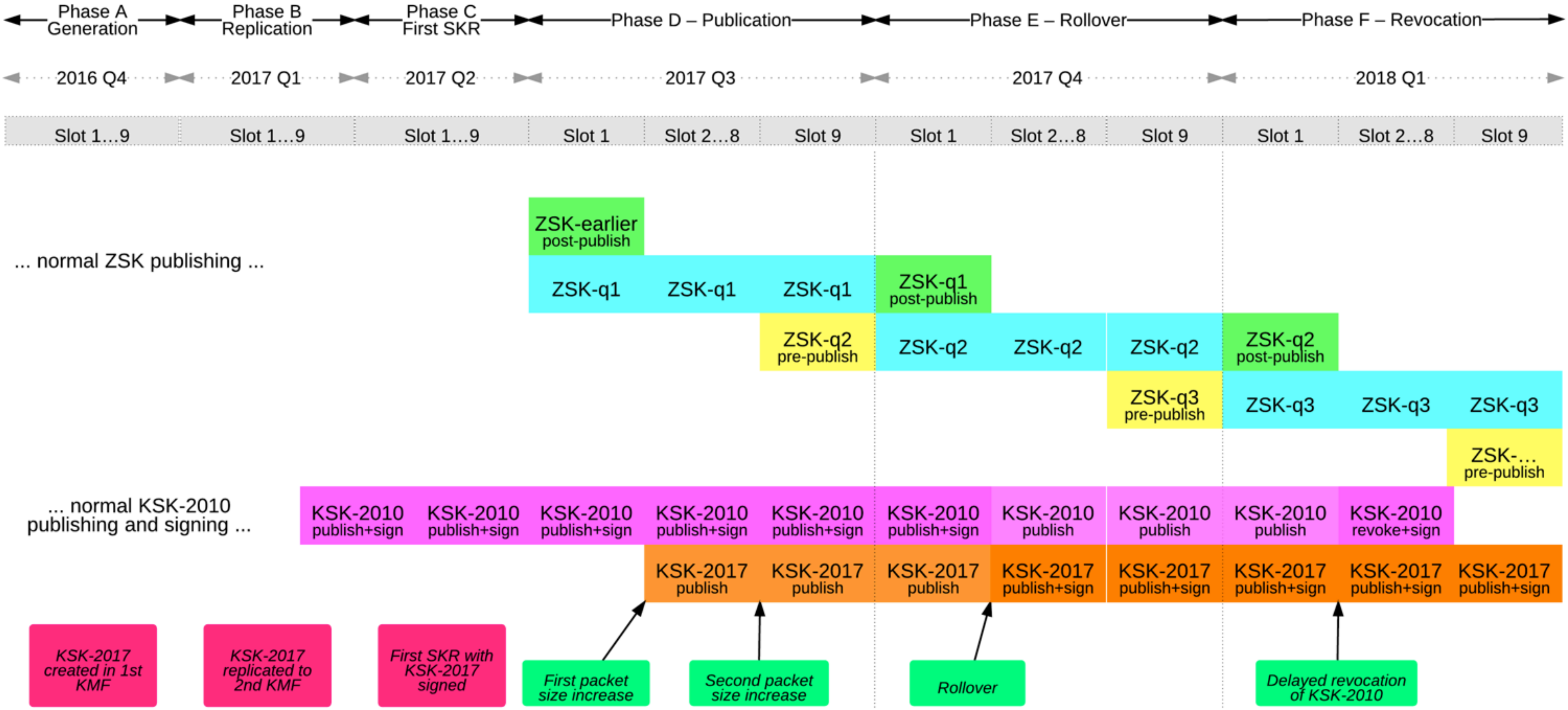
- Automated Updates (RFC 5011) Phases
  - KSK-2017 (new) pre-published, signs DNSKEY set
  - KSK-2010 (current) is revoked

- Post Rollover Phases
  - Deletion of KSK-2010 from system
  - Project experiences documented

Operational Implementation Plan Dates

- Plans publicly available from 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 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



	Phase A Generation	Phase B Replication	Phase C First SKR	Phase D – Publication			Phase E – Rollover			Phase F – Revocation		
	2016 Q4	2017 Q1	2017 Q2	2017 Q3			2017 Q4			2018 Q1		
	Slot 1…9	Slot 1…9	Slot 1…9	Slot 1	Slot 2…8	Slot 9	Slot 1	Slot 2…8	Slot 9	Slot 1	Slot 2…8	Slot 9
				ZSK-earlier post-publish								
... normal ZSK publishing ...				ZSK-q1	ZSK-q1	ZSK-q1	ZSK-q1 post-publish					
						ZSK-q2 pre-publish	ZSK-q2	ZSK-q2	ZSK-q2	ZSK-q2 post-publish		
									ZSK-q3 pre-publish	ZSK-q3	ZSK-q3	ZSK-q3
												ZSK-… pre-publish
... normal KSK-2010 publishing and signing ...		KSK-2010 publish+sign	KSK-2010 publish+sign	KSK-2010 publish+sign	KSK-2010 publish+sign	KSK-2010 publish+sign	KSK-2010 publish+sign	KSK-2010 publish	KSK-2010 publish	KSK-2010 publish	KSK-2010 revoke+sign	
					KSK-2017 publish	KSK-2017 publish	KSK-2017 publish	KSK-2017 publish+sign	KSK-2017 publish+sign	KSK-2017 publish+sign	KSK-2017 publish+sign	KSK-2017 publish+sign
	KSK-2017 created in 1st KMF	KSK-2017 replicated to 2nd KMF	First SKR with KSK-2017 signed	First packet size increase	Second packet size increase			Rollover			Delayed revocation of KSK-2010	

Systems Test Plan

- Testing internal systems for these components

- 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)

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

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

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 DNSKEY Resource Record Sets (RRsets) 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
  - Otherwise manual intervention is required
    - Add the KSK-2017 before October 11, 2017 (assuming all is on track)
    - Remove KSK-2010 at a later date

Planned KSK Rollover Dates

- Plans publicly available from 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 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