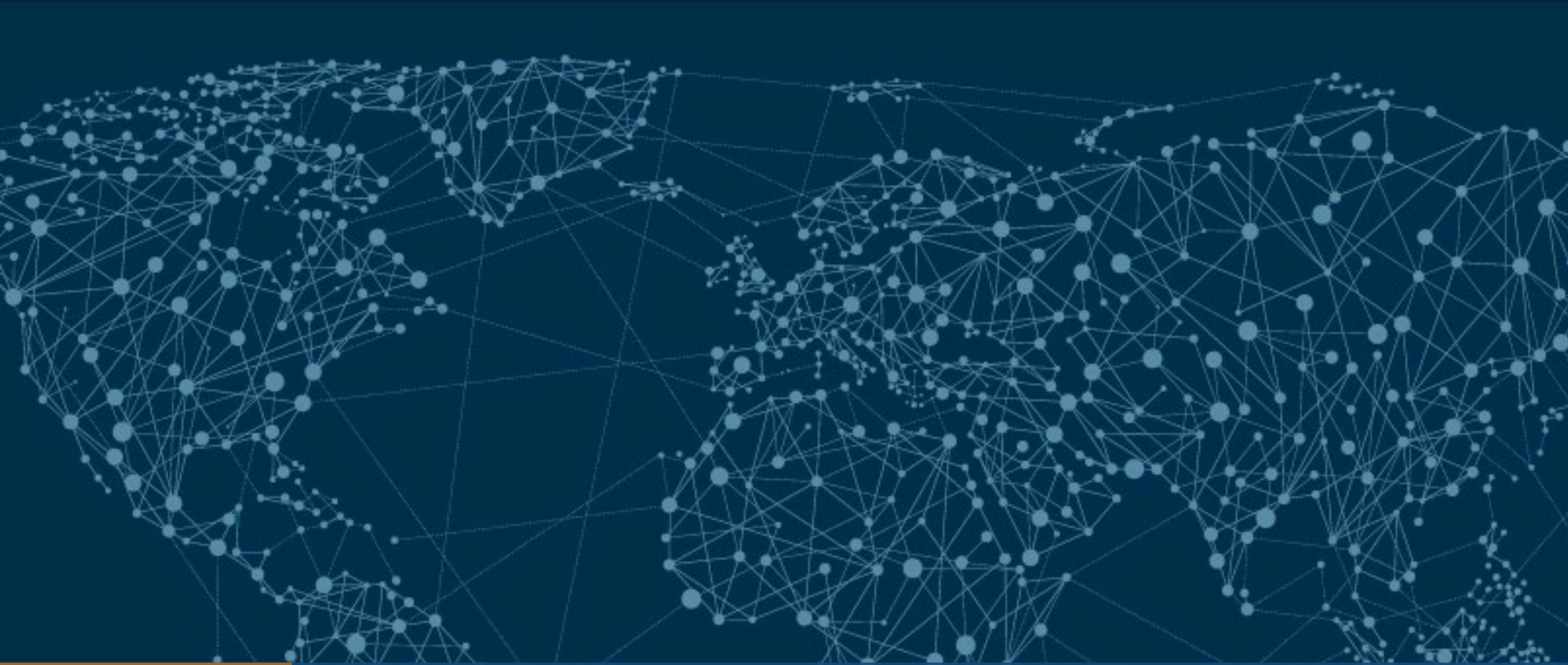


Rolling the Root Zone KSK

Matt Larson | ICANN56 (Helsinki) | June 2016
matt.larson@icann.org

DNSSEC in the Root Zone Managed Jointly

- ICANN (IANA Functions Operator)
  - Manages the KSK, same key since operations began in 2010
  - Quarterly the KSK signs the ZSK in a key ceremony
- Verisign (Root Zone Maintainer)
  - Manages the ZSK, key changed quarterly
  - The root DNSKEY RRset is managed in 10-day "slots"
- In coordination with US DoC NTIA per agreements

Activities Underway

- ZSK size increasing
  - Activity managed by Verisign, covered elsewhere
  - This activity will happen before...
- KSK changing (“rolling”)
- Separate but coordinated activities

Why Change the KSK?

- Primary reason: operational preparedness
  - KSK has no expiration date
  - Currently no weakness
  - But no key should live forever: bad cryptographic practice
  - Prefer to exercise rollover process under normal conditions
    - As opposed to abnormal, such as key compromise

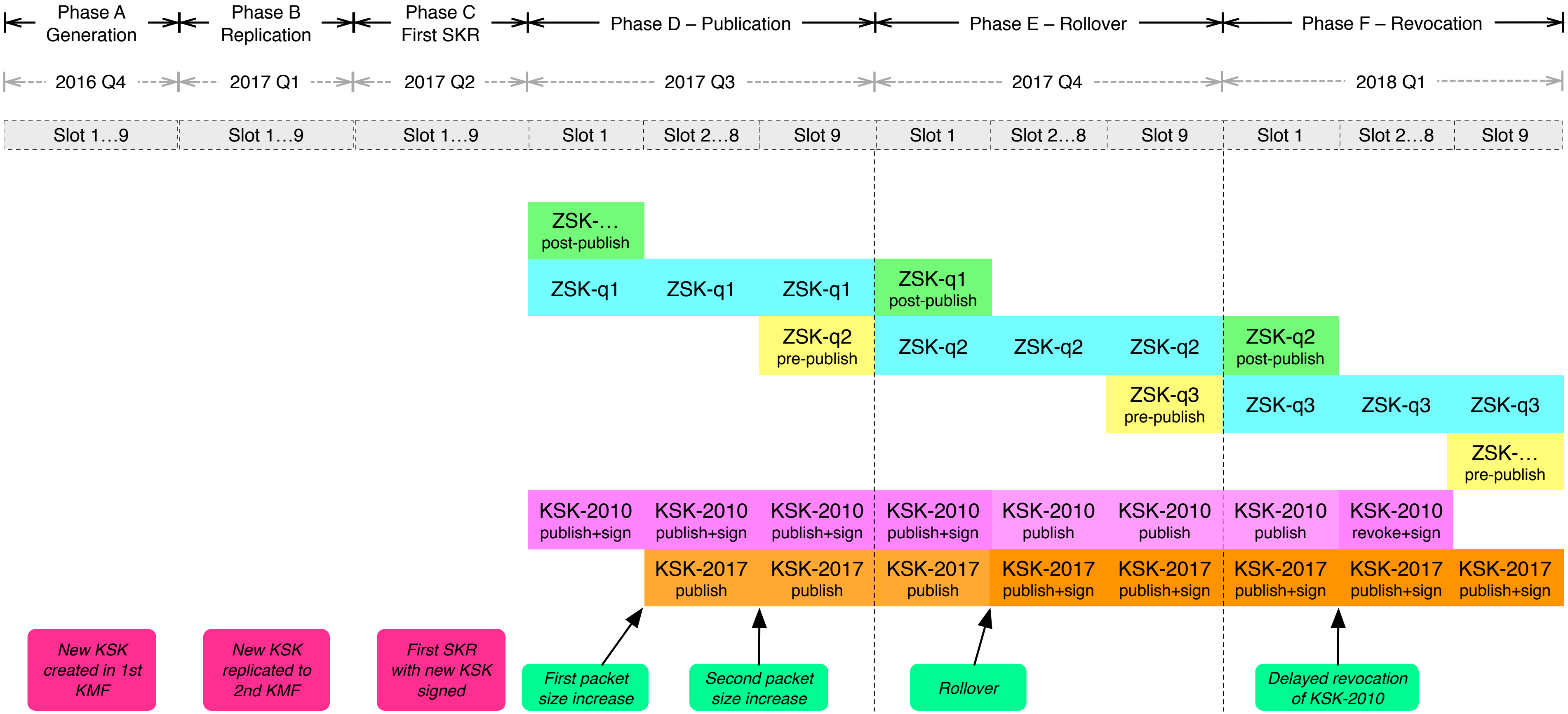
- Big challenge
  - Involves countless/uncountable participants
  - No test environment can cover all possibilities

Planned KSK Roll Dates

- Plans publically available mid-July, 2016
- Key ceremonies
  - Q4 2016 ceremony (November): generate new KSK
  - Q1 2017 ceremony (February): KSK operationally ready
- DNS changes
  - New KSK in root zone on July 11, 2017
  - New KSK signs DNSKEY RRset beginning October 11, 2017
  - Current KSK revoked on January 11, 2018

(Timing contingent on successful ZSK size increase)

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-… post-publish								
			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
			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
New KSK created in 1st KMF	*New KSK replicated to 2nd KMF*	*First SKR with new KSK signed*	*First packet size increase*	*Second packet size increase*		*Rollover*			*Delayed revocation of KSK-2010*		

If Issues Arise

- Plan includes back-out capability
  - If necessary, can stay in current state or roll back at every phase
    - Until old key revoked in Q1 2018
  - Multiple back-out DNSKEY RRsets signed at each ceremony
    - Back out can be immediate
    - No need for extra key ceremony

- Extensive monitoring during each phase
  - Near-real time analysis of root server traffic, observation of operational mailing lists and social media, etc.
  - Criteria for triggering back out under development
  - Will not be absolute but allow for operational discretion

Upcoming Activities

- Presenting the plan (July to December 2016)
  - Informal feedback
- Presenting the new KSK (January to July 2017)
  - New key will be introduced and publicized
- Follow *Automated Updates* (RFC 5011)
  - July 11, 2017 through early 2018

Changing Trust Anchors

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

Testing Resources

- Resources targeted for software developers
  - Two third-party “accelerated” RFC 5011 test environments with sped up 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

For More Information

- Join the 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: matt.larson@icann.org
Website: icann.org

twitter.com/icann

facebook.com/icannorg

linkedin.com/company/icann

youtube.com/user/icannnews

gplus.to/icann

weibo.com/ICANNorg

flickr.com/photos/icann

slideshare.net/icannpresentations