IANA KSK Roll & Yeti

Shane Kerr / BII Labs
2016-03-24 / Yeti Virtual Meeting

天地互连

IANA KSK Roll Story

- Root KSK DPS: roll every 5 years
  - Signed 2010-07-15 (> 5.5 years ago... oops!)
- 2013-03-13 call for comments finished
- 2013-07 RZM partners met
- 2013-11 SSAC published advisory
- 2014-12 ICANN formed design committee
- 2015-08-06 comments on document
- 2016-03-07 ”final” KSK roll plan

https://www.iana.org/.../root-ksk-rollover-design-20160307.pdf

Main Challenge

- How can you roll the KSK safely?
  - Authority servers do not know when resolvers have updated their trust anchors
- RFC 5011 may help many resolvers
  - But not always implemented, or configured
  - Some operations *cannot* use RFC 5011
- Work in IETF to solve this
  - May help... 5 years from now

Recommendations

- 17 recommendations
  - Basically reasonable
- Use RFC 5011
- Don't change the crypto setup
- Tell everyone
- Monitor progress

The Plan

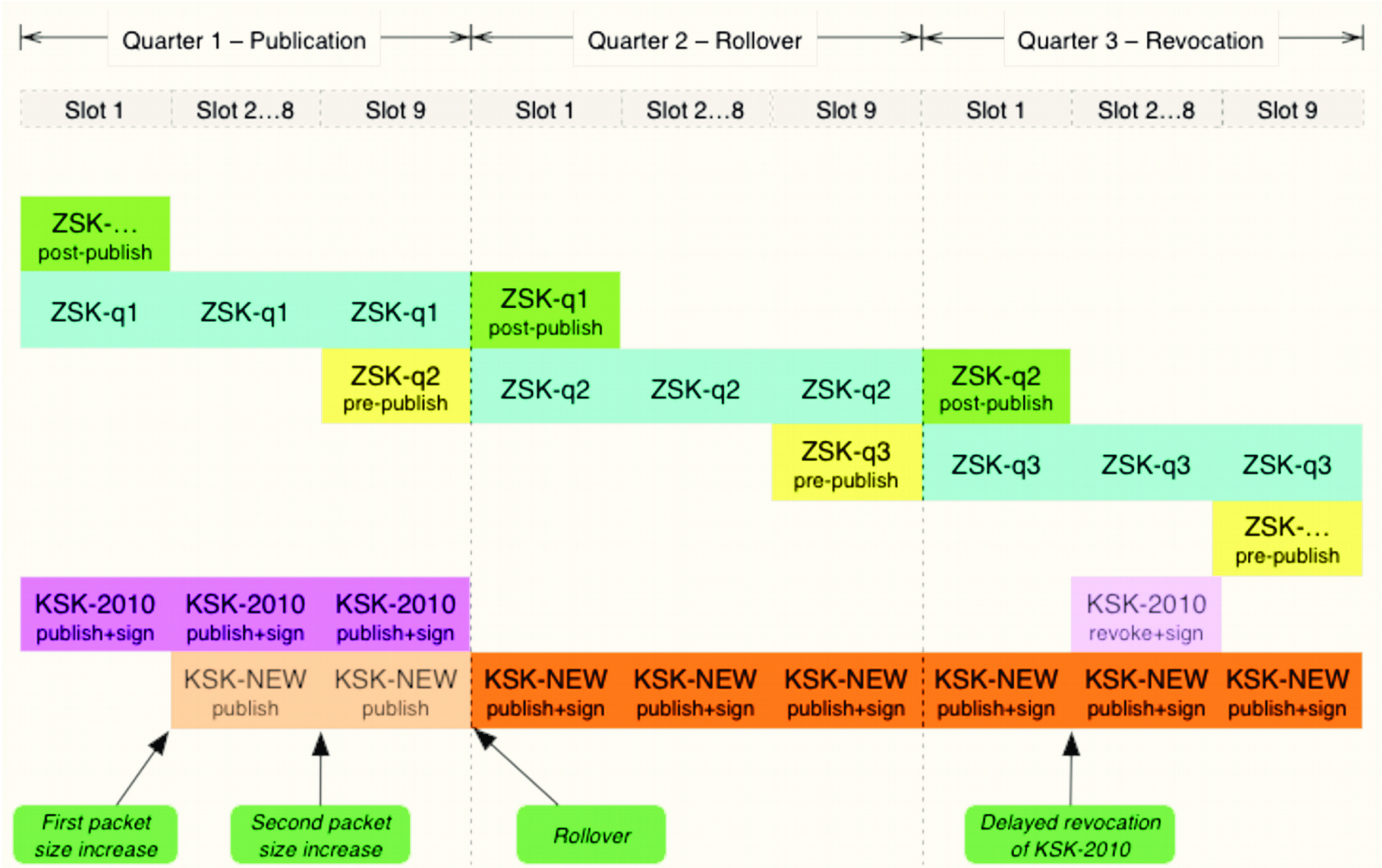

Figure 1. Rollover Scheduling

Bii 天地互连

What Can Yeti Do?

- Roll the Yeti KSK. :)
  - Takes at least 30 days, due to RFC 5011 hold-down timer
- Roll the Yeti KSK using the ICANN method
- Keep rolling, and devise a ”self-test”?
- What else?