Increasing the Zone Signing Key Size for the Root Zone

Duane Wessels

NANOG 67, DNS Track

June 14, 2016

Presentation Outline

- Current root zone DNSSEC parameters
- Schedule
- Change details
- Consequences of a 2048-bit ZSK
- Fallback plan

Initialisms

KSK	Key Signing Key	Operated by IANA/ICANN
ZSK	Zone Signing Key	Operated by Verisign
KSR	Key Signing Request	XML-formatted bundle of keys to be signed
SKR	Signed Key Response	XML-formatted bundle of signatures

This is not the KSK Rollover

- You may have recently heard about work underway to roll the root zone Key Signing Key (aka Trust Anchor).

- That's **not** what this is.

- Verisign is working closely with the other Root Zone Management partners to ensure that the ZSK length change does not coincide with other activity that would increase the root zone DNSKEY response size.

Current DNSSEC parameters

Parameter	KSK	ZSK
Algorithm	8	8
Size	2048-bits	1024-bits
Rolled	(not yet*)	quarterly
Re-sign period	10 days	12 hours
Signature validity	15 days	10 days
Signs	DNSKEYs	everything else

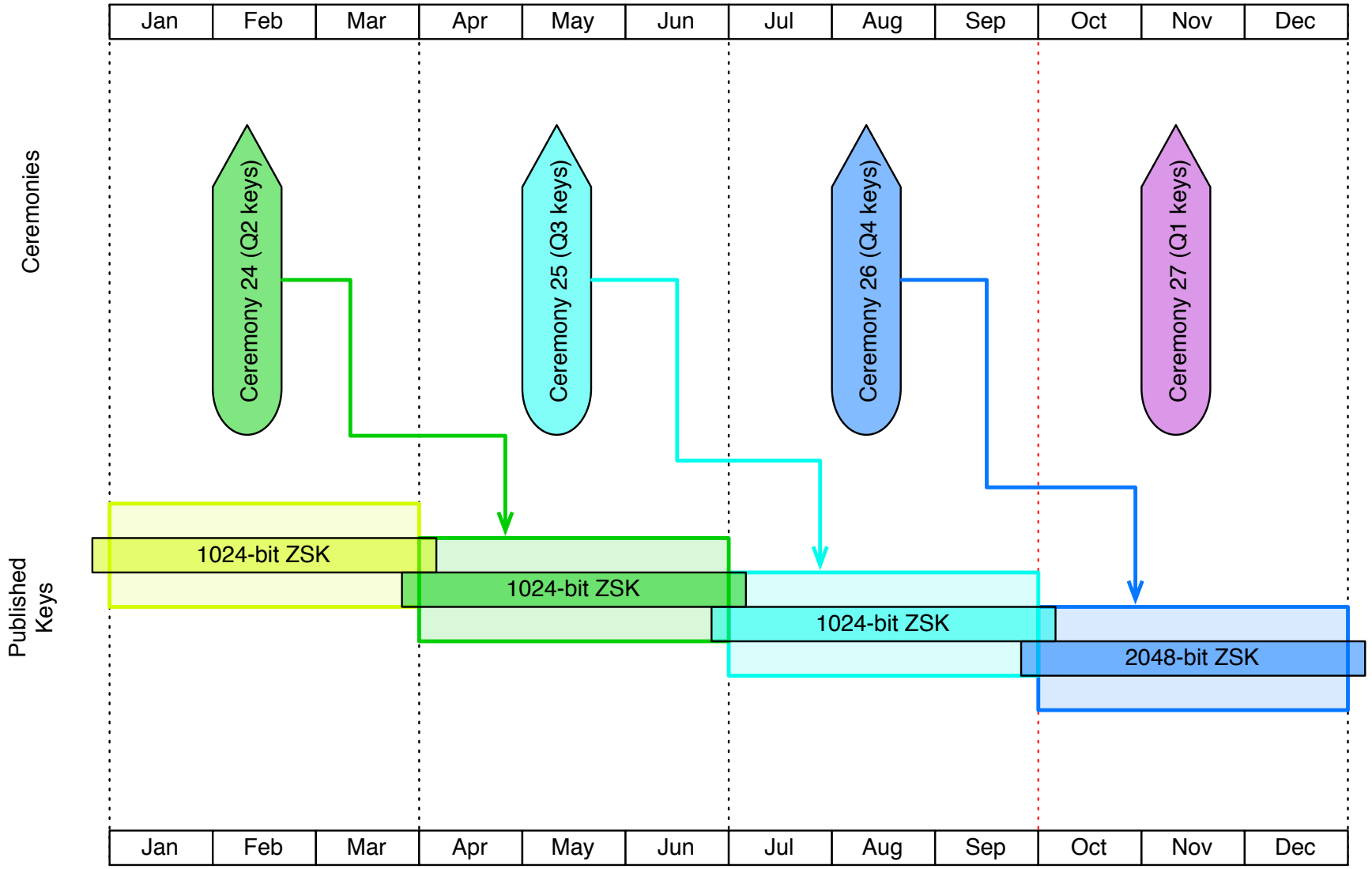
- ZSK size will be increased to 2048-bits
- No other parameters will be changed

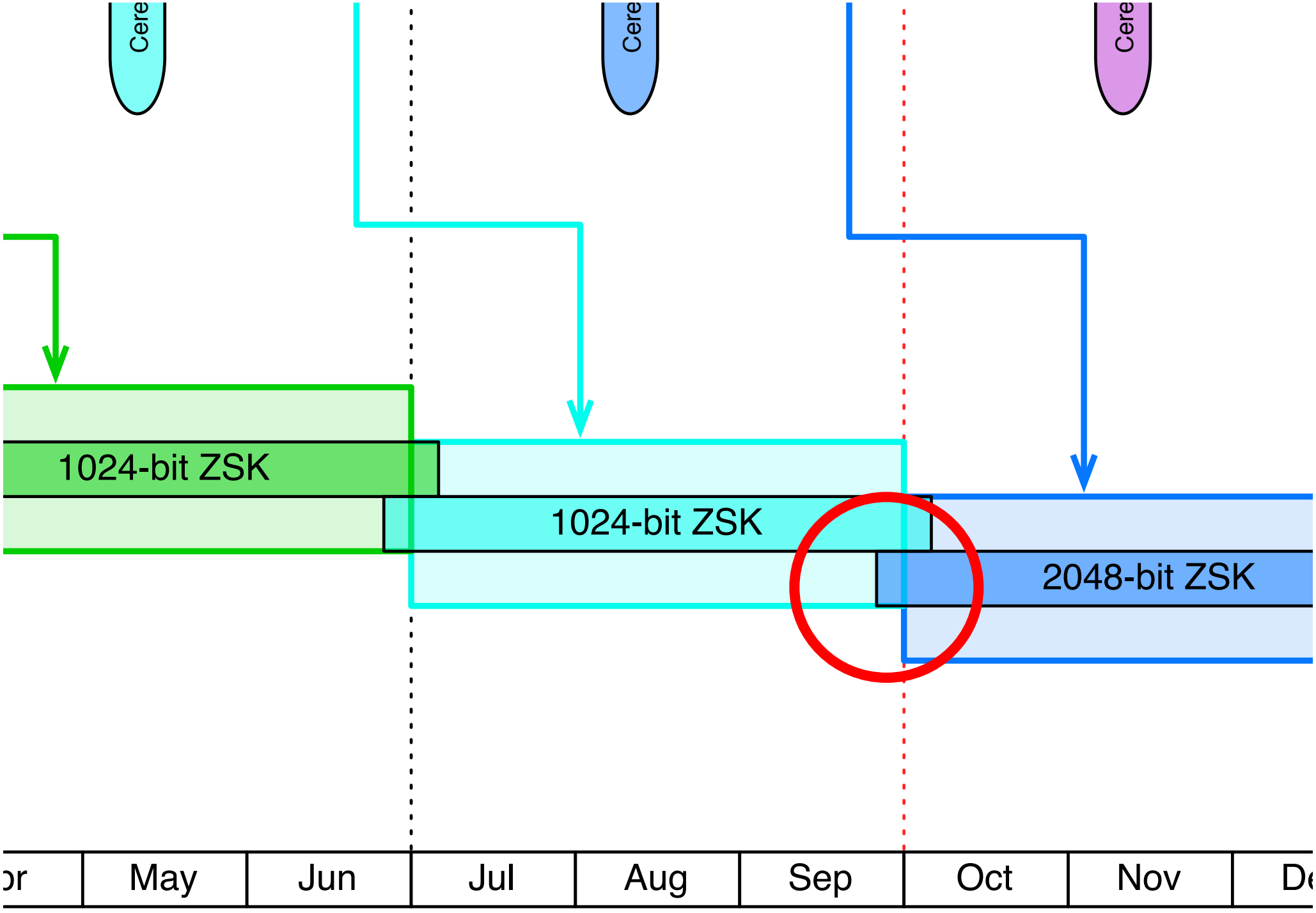
*Sticklers (Hi Roy!) will bring up the DURZ transition in 2010

Schedule

Date		Milestone
2016-04-15	✓	Testing between ICANN and Verisign
2016-05-12	✓	KSK ceremony #25; sign 2016Q3 ZSKs
2016-08-11		KSK ceremony #26; sign 2016Q4 ZSKs
2016-09-20		First 2048-bit ZSK pre-published in root zone
2016-10-01		Root zone signed with 2048-bit ZSK

Schedule


Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Ceremonies
Ceremony 24 (Q2 keys)
Ceremony 25 (Q3 keys)
Ceremony 26 (Q4 keys)
Ceremony 27 (Q1 keys)
Published Keys
1024-bit ZSK
1024-bit ZSK
1024-bit ZSK
2048-bit ZSK
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec

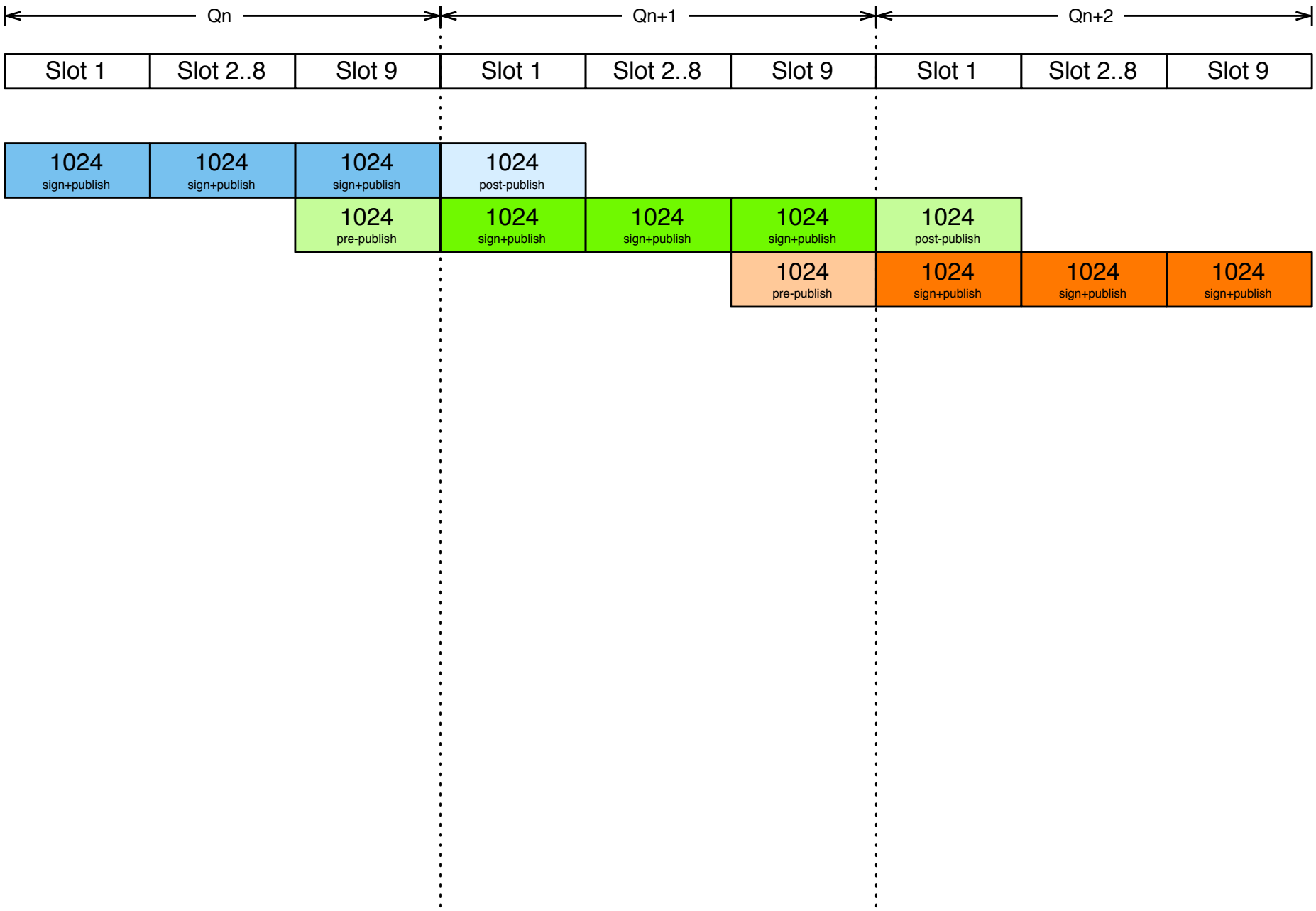

Cere
Cere
Cere
1024-bit ZSK
1024-bit ZSK
2048-bit ZSK
or
May
Jun
Jul
Aug
Sep
Oct
Nov
De

Rollover Details

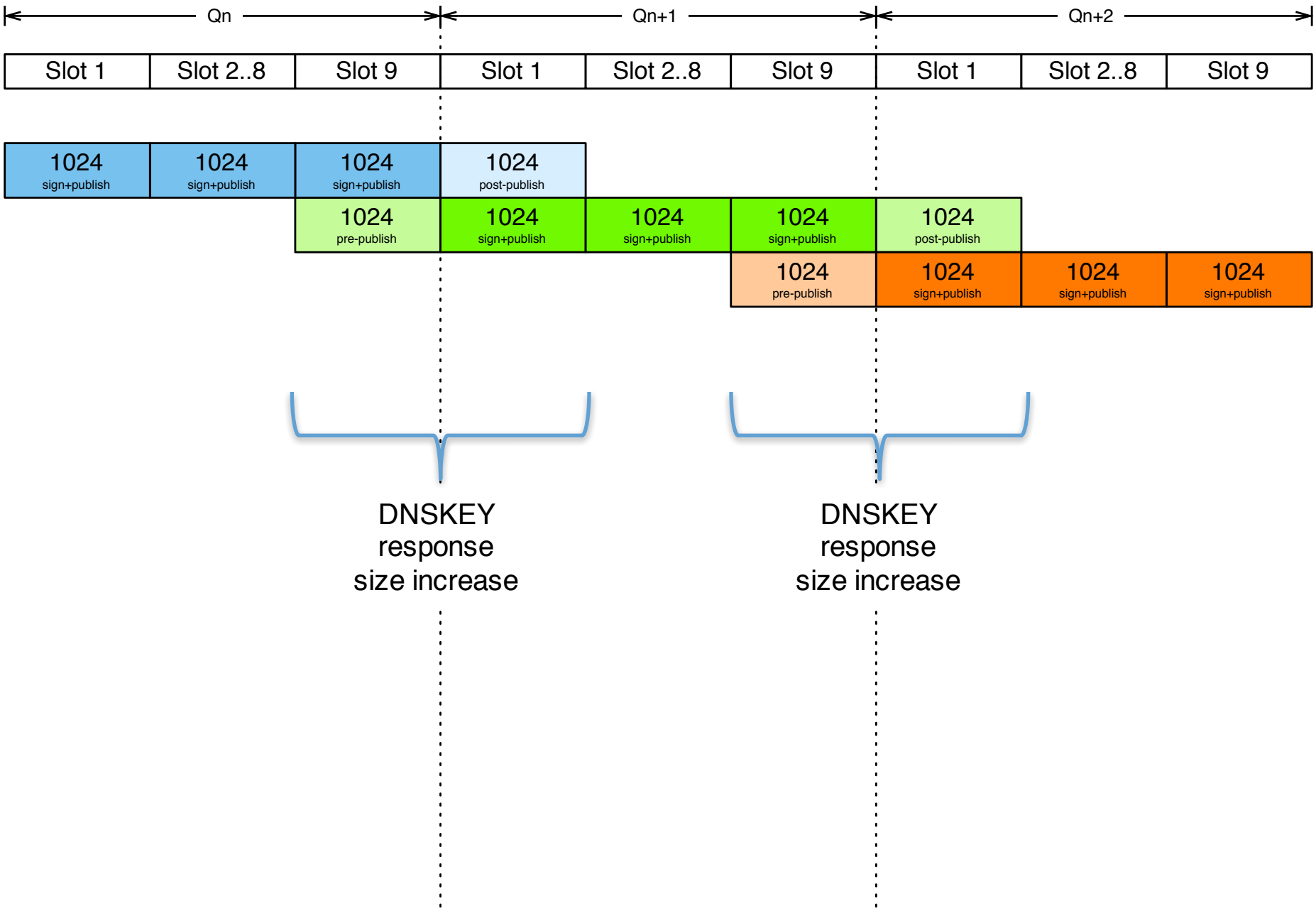
The ZSK Rollover Process

- ZSK is Rolled quarterly
- Quarter is divided into 9 slots of 10 days each
  - Sometimes the 9th slot is longer
- The DNSKEY RRSIG record changes in each slot
- Uses pre-publish technique
  - Incoming ZSKs pre-published for one slot (9th slot)
  - Outgoing ZSKs post-published for one slot (1st slot)
- Size of DNSKEY response message increased due to pre-/post-publish

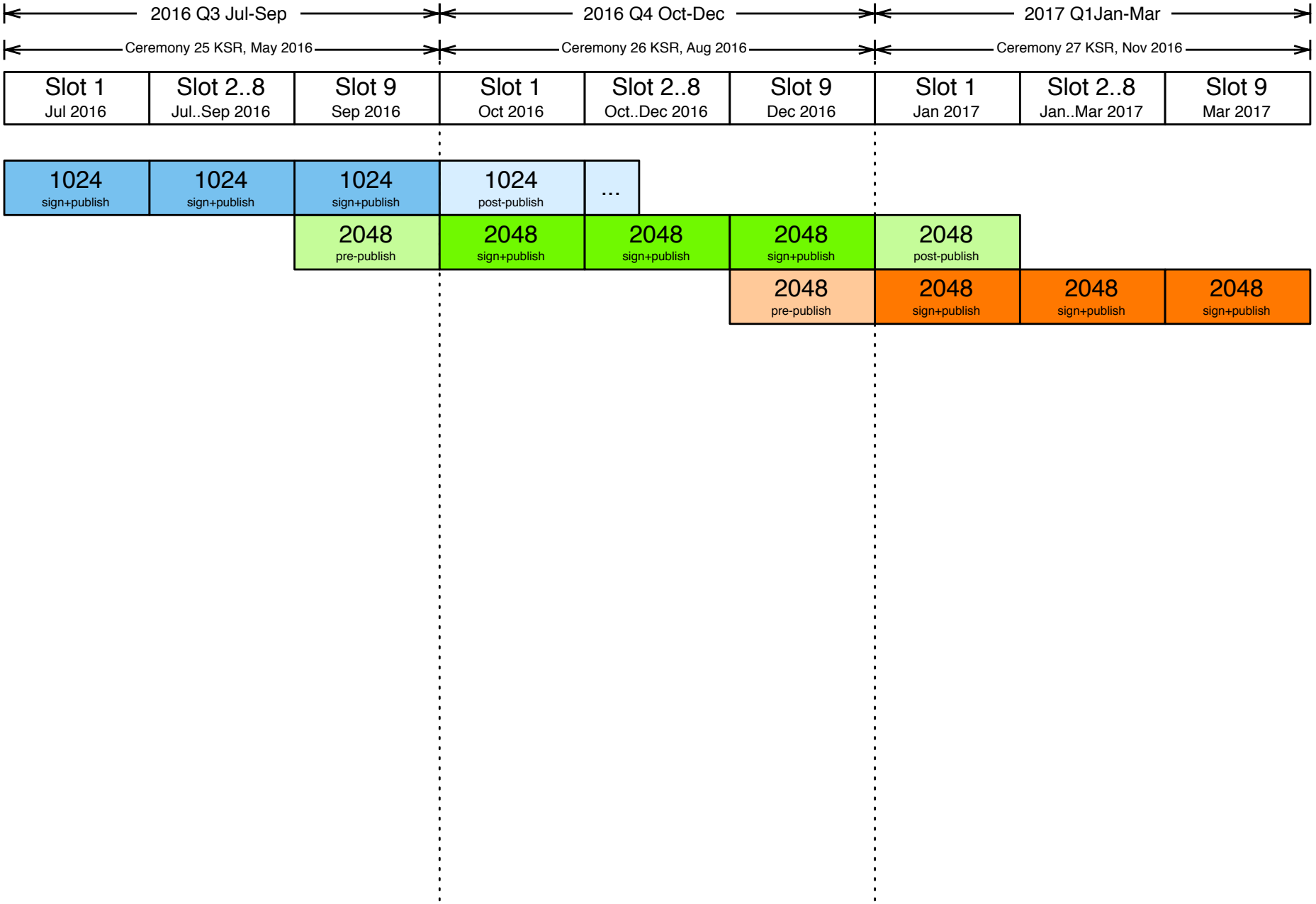
ZSK 1024→1024 Normal Rollover



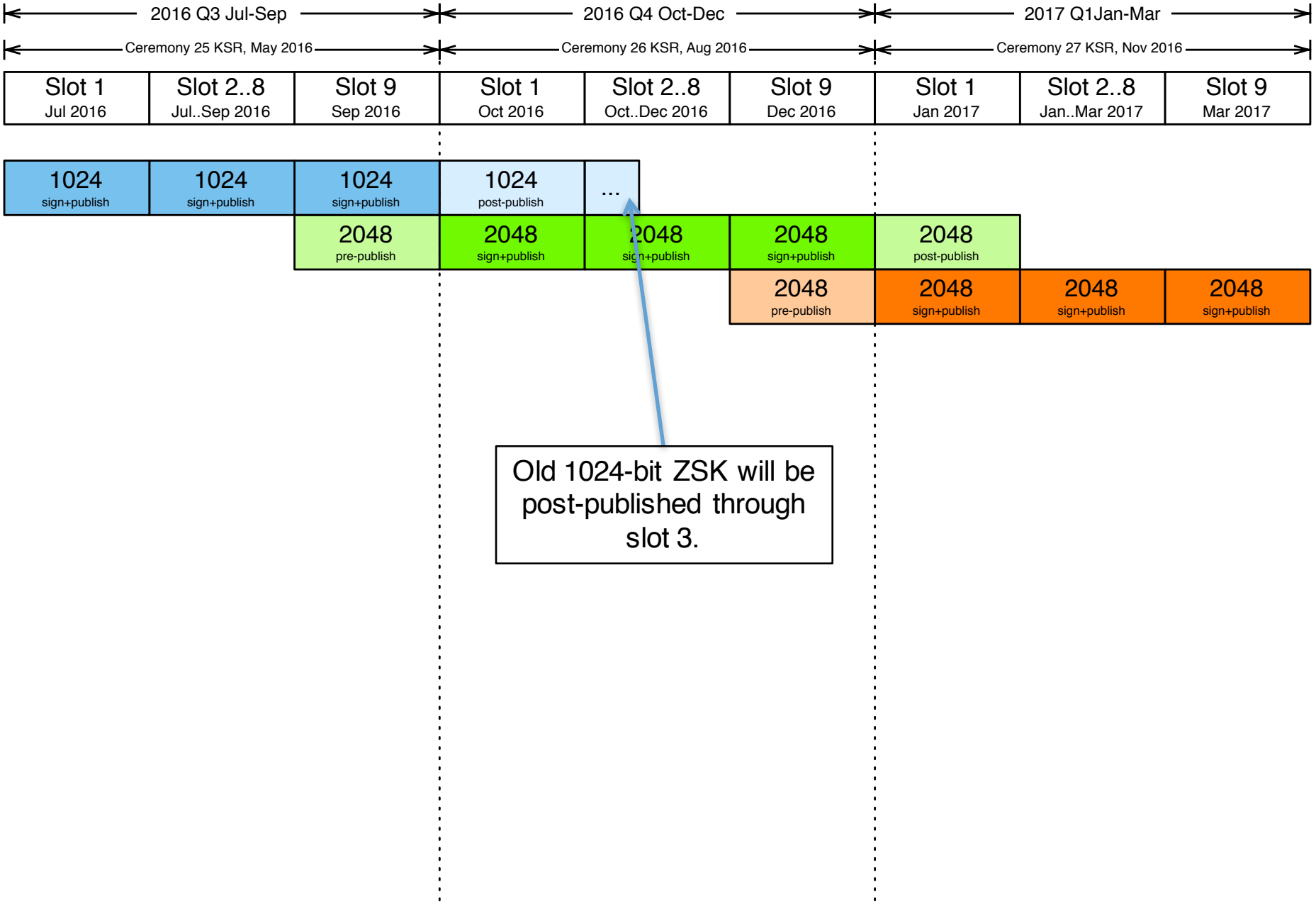
ZSK 1024→1024 Normal Rollover



ZSK 1024→2048 Rollover



ZSK 1024→2048 Rollover

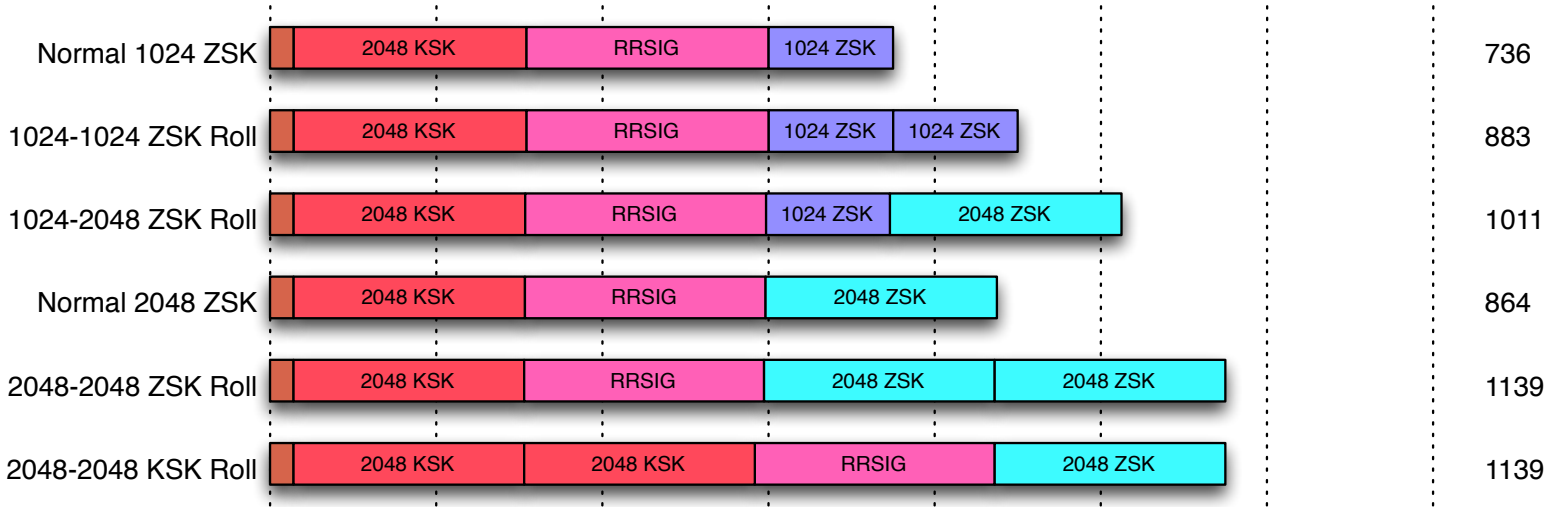


1024-2048 Rollover

- Much like normal 1024 rollover
- Except longer post-publish period for outgoing 1024-bit key
  - ...just in case

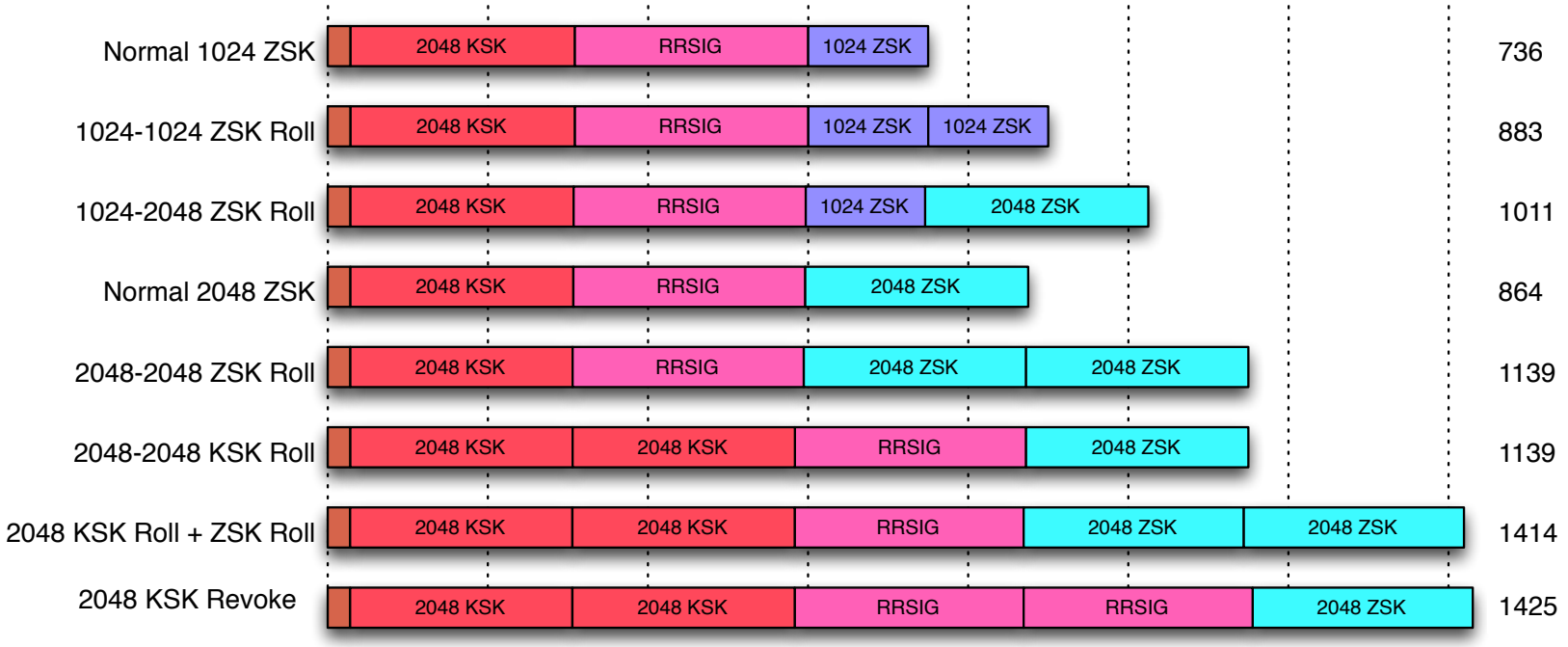
Consequences of a 2048-bit ZSK

Size of Signed DNSKEY Response



- DNSKEY response size changes throughout this process
- Normal (non-roll) size increases from 736 to 864 octets
- ZSK rollover size increases from 883 to 1138 octets

Size of Signed DNSKEY Response



- DNSKEY response size changes throughout this process
- Normal (non-roll) size increases from 736 to 864 octets
- ZSK rollover size increases from 883 to 1138 octets
- Future KSK revoke size would be 1425 octets

Size of Other Signed Responses

- All non-DNSKEY RRSets are signed by the ZSK
- DO=1 responses will be larger
- 1024-bit ZSK signature (RRSIG) : 159 octets
- 2048-bit ZSK signature (RRSIG) : 287 octets
- But its not that simple....
- We replayed real query logs to various DNSSEC configurations to understand traffic impacts

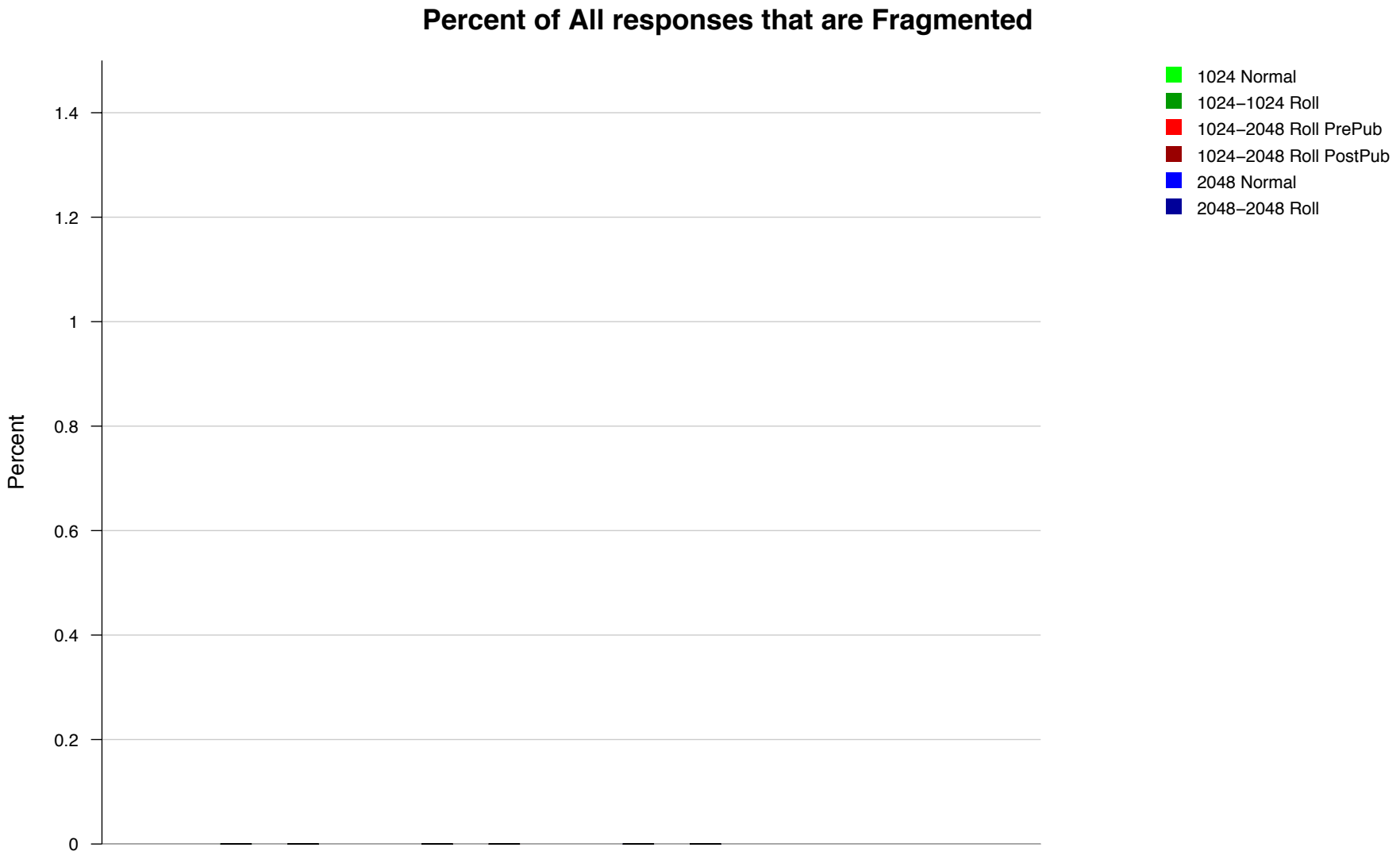
Measurement Methodology

- Captured 10 minutes of queries sent to a.root-servers.net
- Signed a root zone with various DNSSEC configurations
- Replayed traffic over both UDP and TCP
  - Including client EDNS0 UDP message sizes and DO flag values
- Recorded the response size, TC flag, etc.

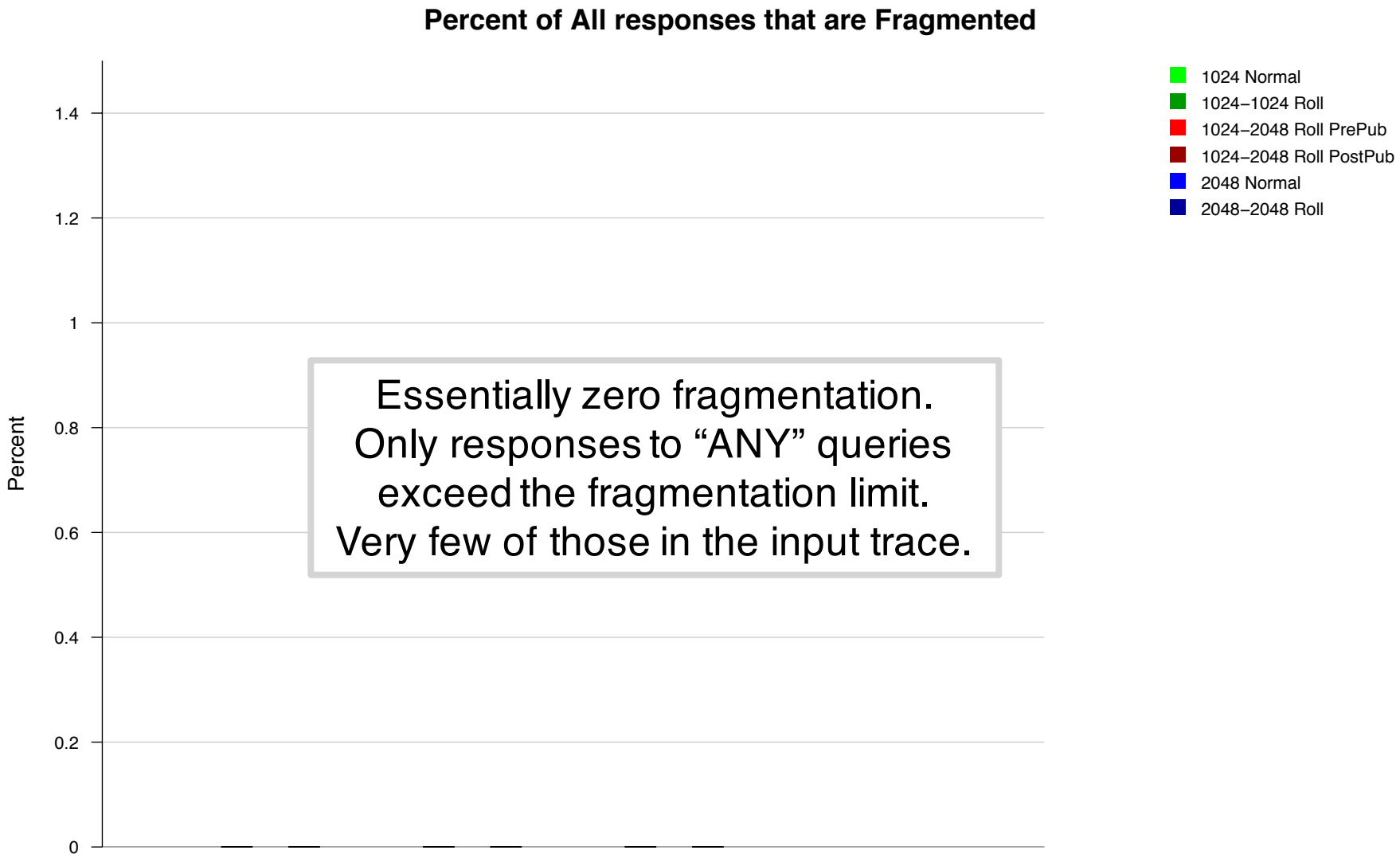
Quick Stats

- Zone File
  - SOA Serial 2016022401
- Input Trace:
  - February 24, 2016
  - 22:00:00 -- 22:10:00 UTC (10 minutes duration)
  - 40,993,338 IP packets captured
  - 37,494,153 DNS UDP queries captured
    - 62,490 queries/second
  - A-root sites: NYC3, LON3, LAX2, FRA1, HKG5

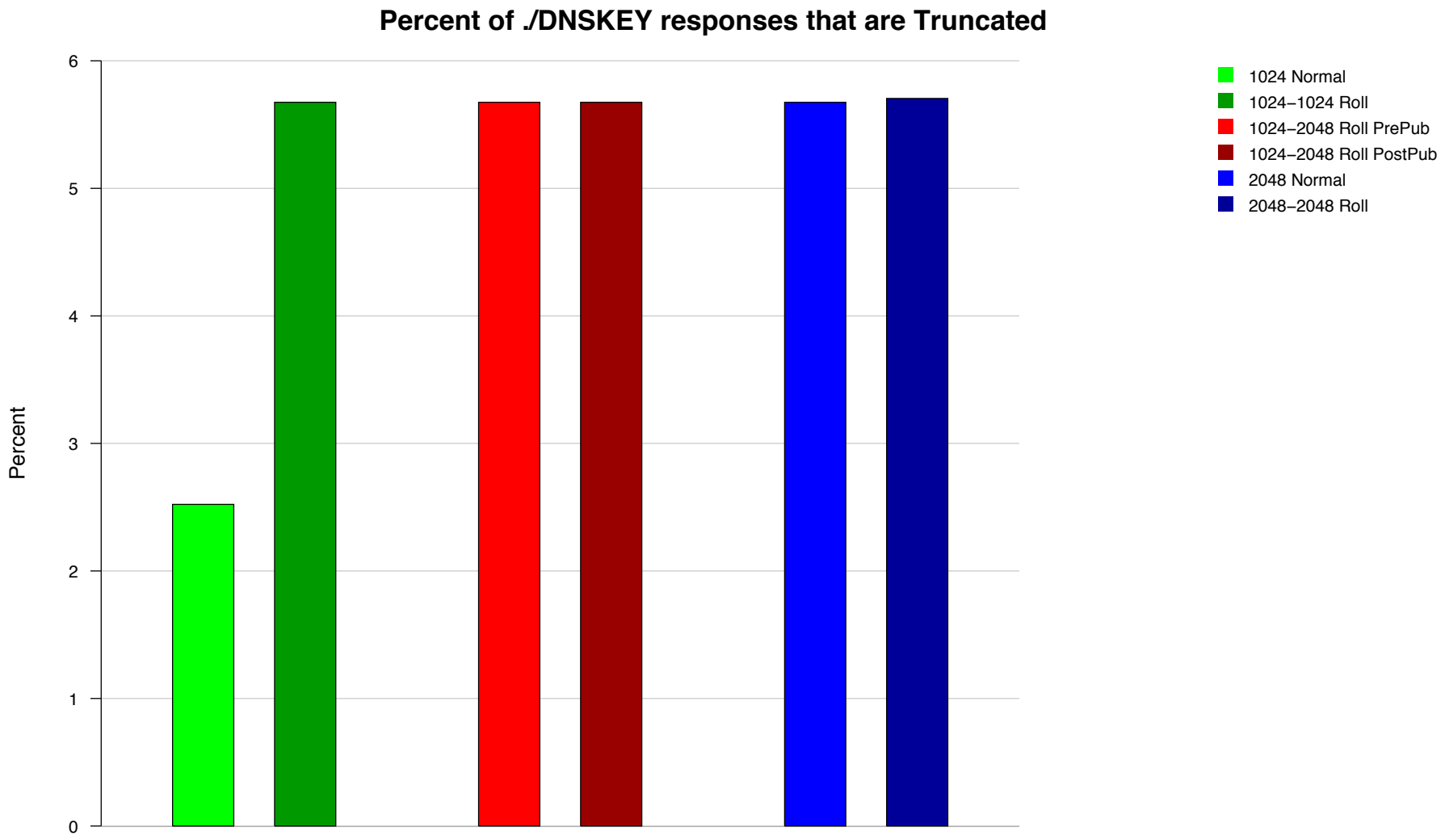
Fragmentation



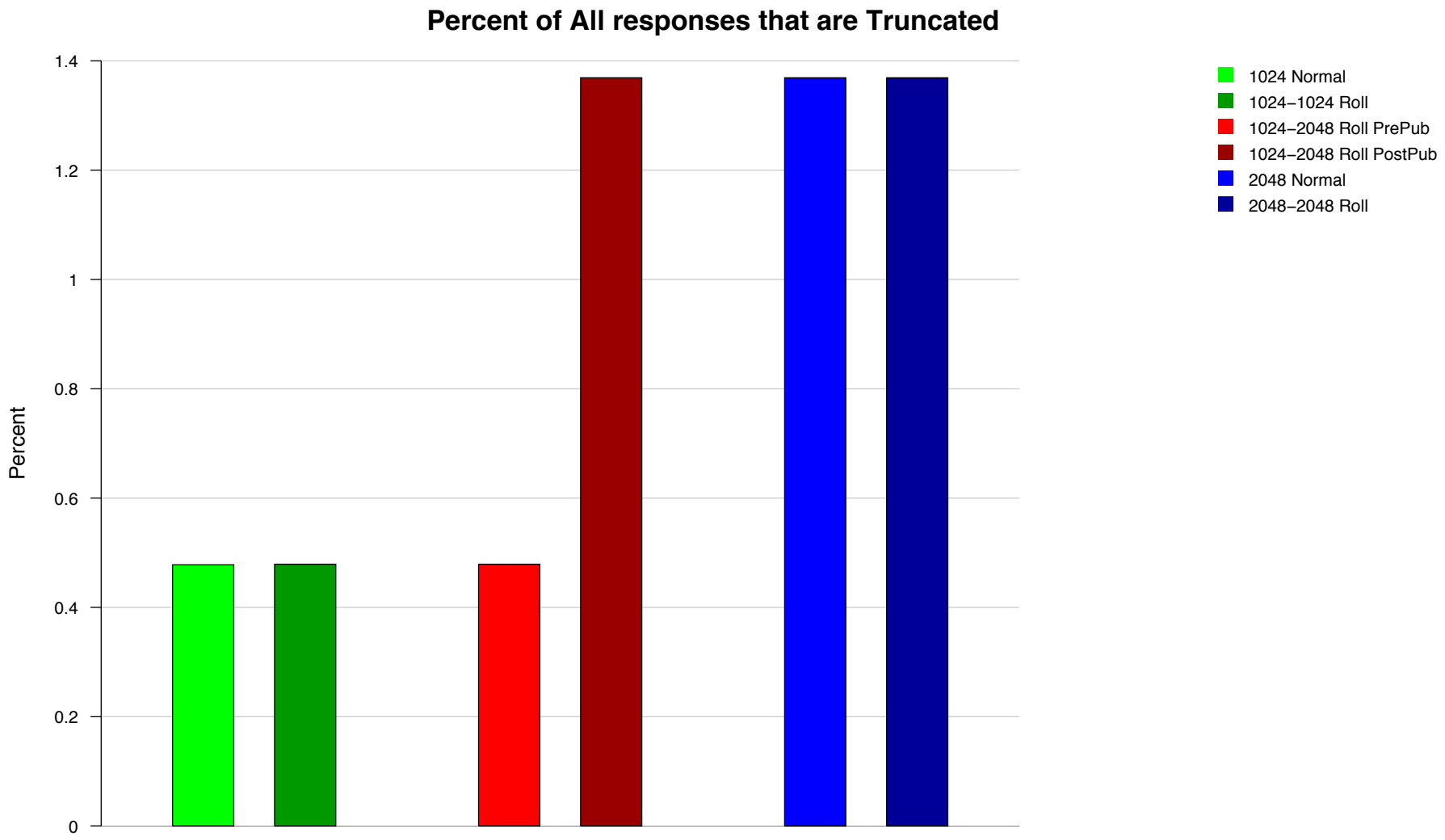
Fragmentation



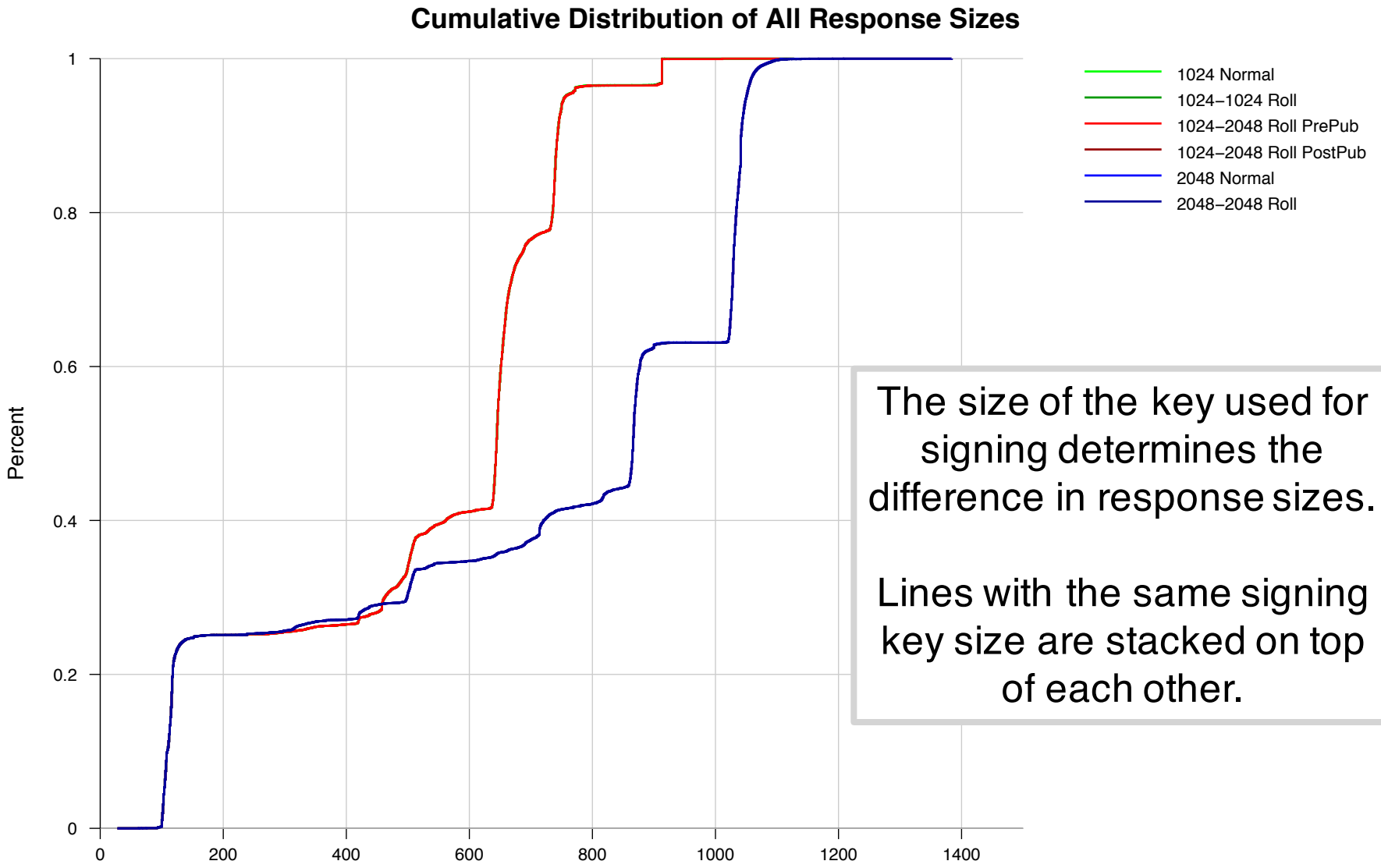
Truncation -- DNSKEY



Truncation -- All



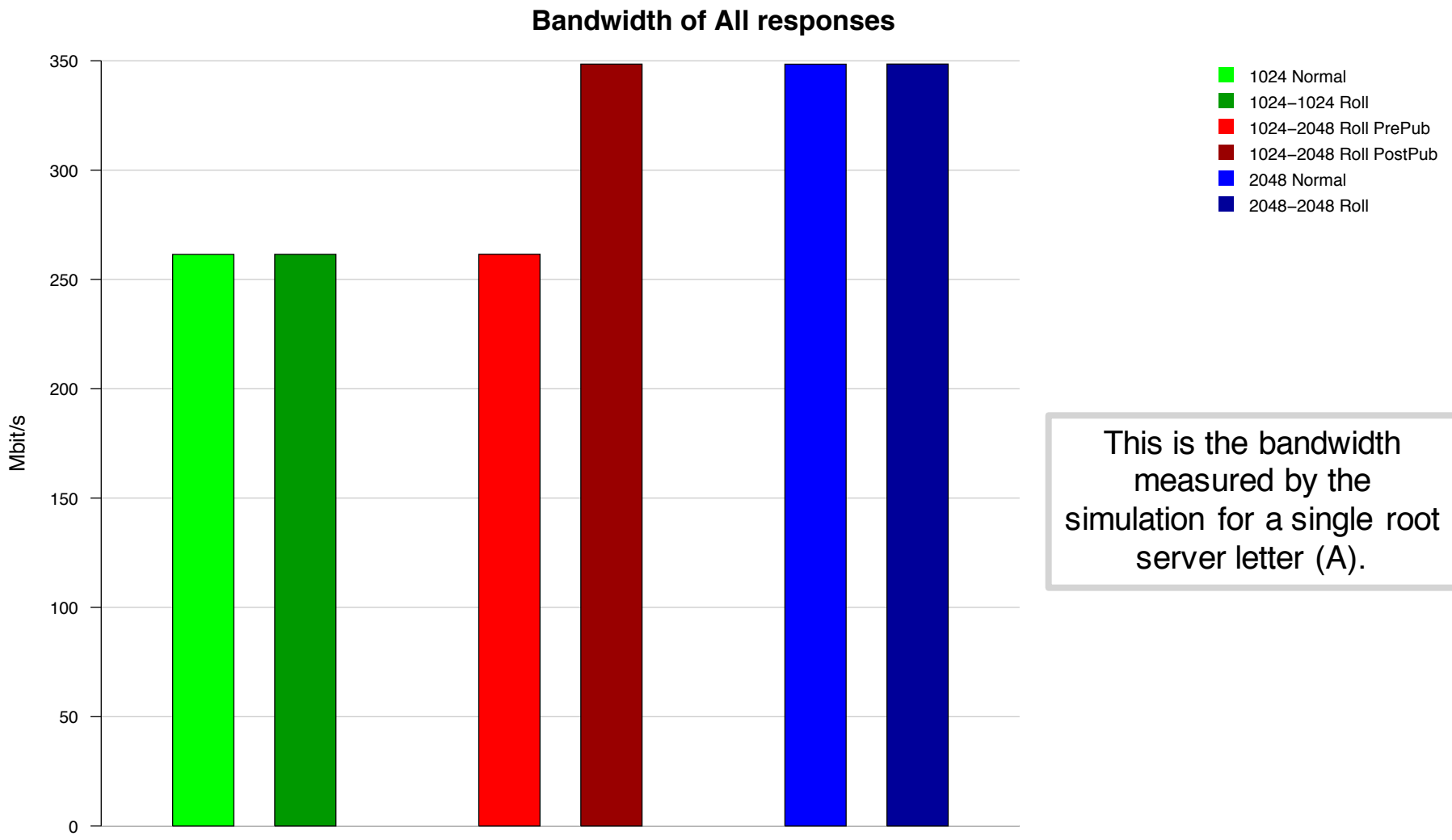
Response Size Distribution



The size of the key used for signing determines the difference in response sizes.

Lines with the same signing key size are stacked on top of each other.

Bandwidth



This is the bandwidth measured by the simulation for a single root server letter (A).

Fallback Plan

Need for Fallback

- We fully expect the length change to occur without incident
- However, unforeseen problems may be beyond our control
- Should it be necessary, we are prepared to revert to a “known good state”
  - i.e. a 1024-bit ZSK
- In fact the exact same 1024-bit key just prior to the length change

Dual KSRs / SKRs

In support of this fallback plan, ICANN will sign two KSRs at two root KSK ceremonies:

- The 2048-bit ZSK
  - plus associated post-publish and pre-publish keys
- The fallback 1024-bit ZSK
  - plus associated post-publish and pre-publish keys

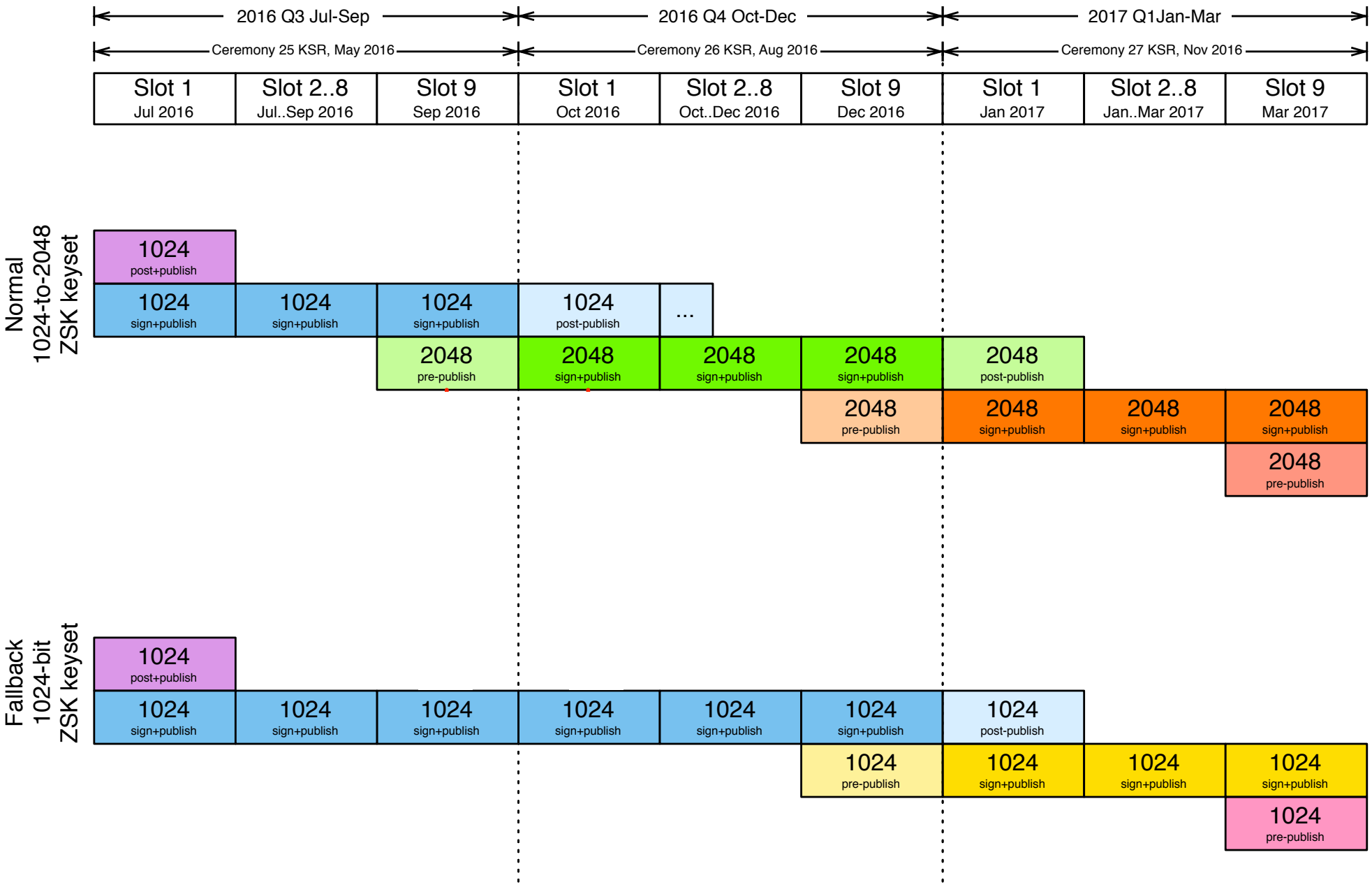
Fallback Criteria

- Something unforeseen
- Something very serious
- Something that can not be solved by (temporarily) disabling DNSSEC validation at a small number of recursive name servers.

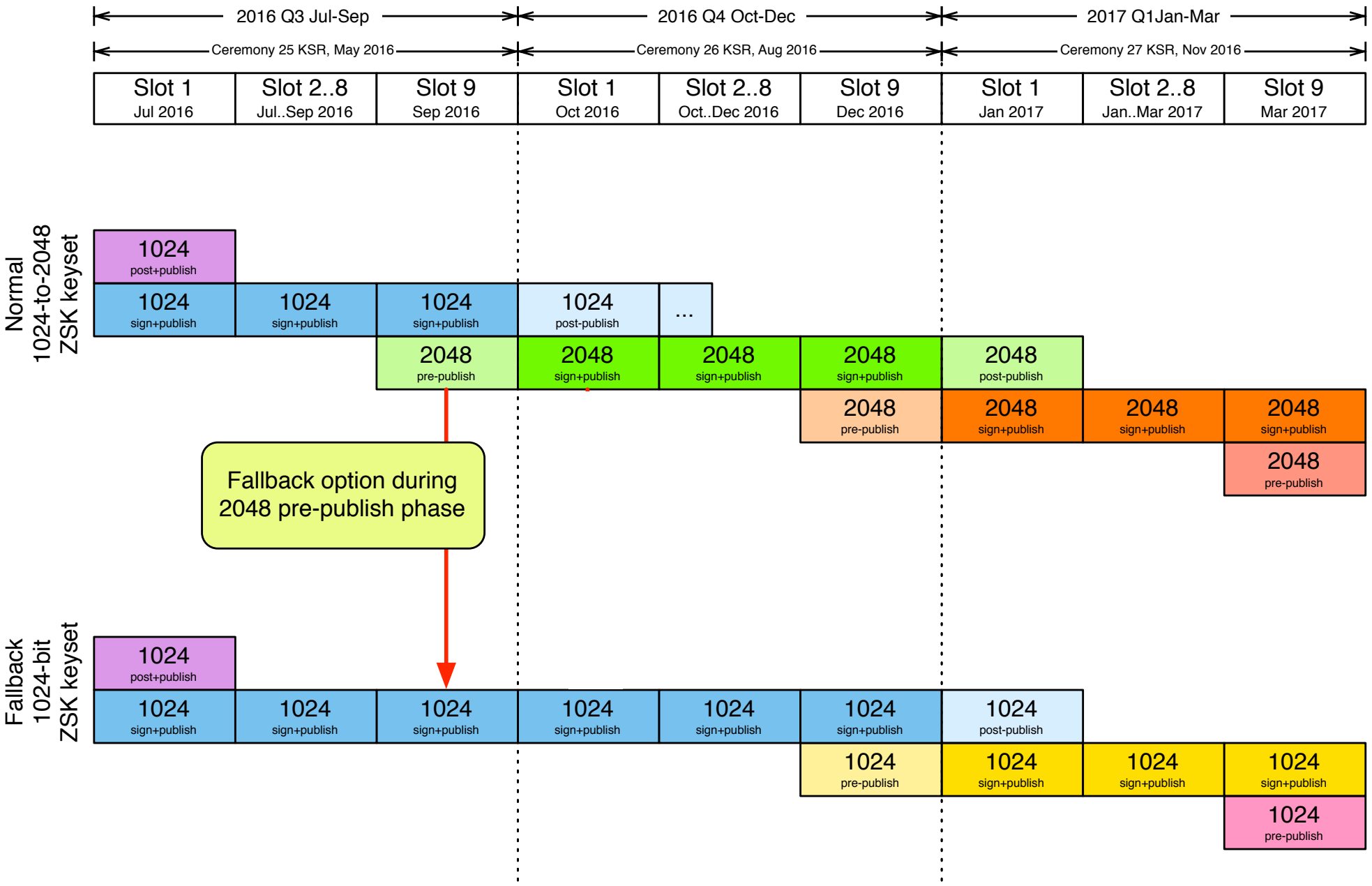
Important Milestones

- Introduction of 2048-bit ZSK to zone (pre-publish)
  - Slot 9 of Q3
- Zone signed by 2048-bit ZSK
  - Slot 1 of Q4
  - Cached RRSIGs will expire over the course of a few days
- Removal of old 1024-bit ZSK (end of post-publish)
  - Point of No Return

ZSK 1024→2048 Rollover



ZSK 1024→2048 Rollover

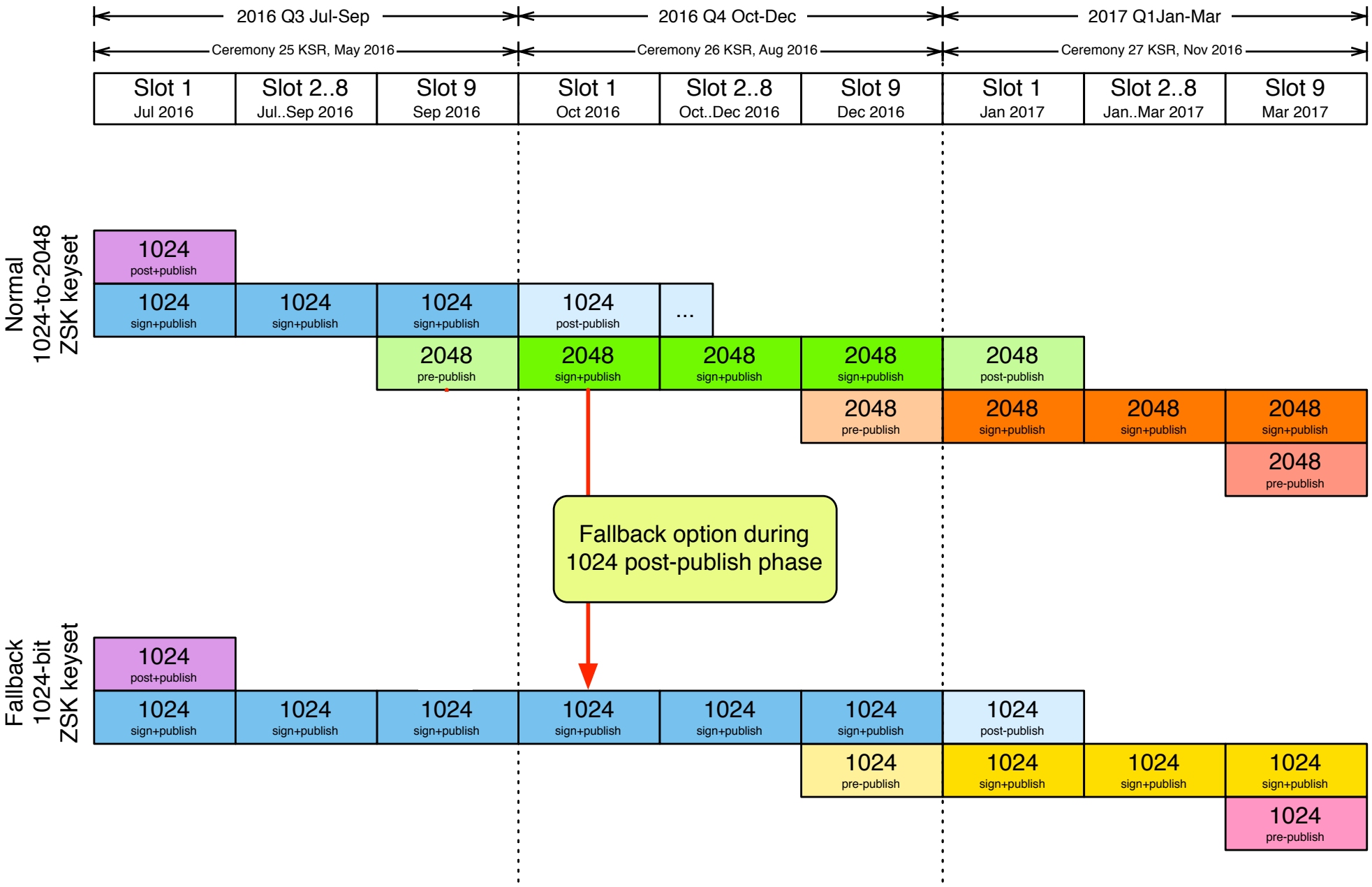


A “Slot 9” Fallback

If a problem arises during the slot 9 2048-bit pre-publish phase:

- Simply un-publish the 2048-bit ZSK from the root zone
- Publish only the current 1024-bit ZSK
- Continue signing with the current 1024-bit ZSK
- There will be no ZSK roll for the next calendar quarter

ZSK 1024→2048 Rollover



A “Slot 1” Fallback

If a problem arises during slot 1 after signing with the 2048-bit ZSK:

- Revert to signing with the old 1024-bit ZSK
  - It is still being published
- When to remove 2048-bit ZSK from zone depends on nature and severity of problem

Test Your Network

keysizetest.verisignlabs.com

keysizetest.verisignlabs.com

#	Description	KSKs	ZSKs	Signed DNSKEY Size	Result
1	1024 ZSK Normal	2048-bit RSASHA256 publish+sign	1024-bit RSASHA256 publish+sign	821	PASS
2	1024 ZSK Rollover	2048-bit RSASHA256 publish+sign	1024-bit RSASHA256 publish+sign 1024-bit RSASHA256 publish	981	PASS
3	1024-2048 ZSK pre-publish	2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish 1024-bit RSASHA256 publish+sign	1109	PASS
4	1024-2048 ZSK post-publish	2048-bit RSASHA256 publish+sign	1024-bit RSASHA256 publish 2048-bit RSASHA256 publish+sign	1109	PASS
5	2048 ZSK Normal	2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish+sign	949	PASS
6	2048 ZSK Rollover	2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish 2048-bit RSASHA256 publish+sign	1237	PASS
7	KSK Rollover with 1024 ZSK	2048-bit RSASHA256 publish+sign 2048-bit RSASHA256 publish+sign+revoke	1024-bit RSASHA256 publish+sign	1443	PASS
8	KSK Rollover with 2048 ZSK	2048-bit RSASHA256 publish+sign 2048-bit RSASHA256 publish+sign+revoke	2048-bit RSASHA256 publish+sign	1571	PASS
9	KSK Rollover with 2048 ZSK rollover	2048-bit RSASHA256 publish+sign+revoke 2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish+sign 2048-bit RSASHA256 publish	1865	PASS
10	This should fail			0	FAIL

Questions?

powered by

VERISIGN™

© 2016 VeriSign, Inc. All rights reserved. VERISIGN and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.