Rolling the Keys of the DNS Root Zone

Geoff Huston
Member of the KSK Roll Design Team

Five Years Ago

ICANN's First DNSSEC Key Ceremony for the Root Zone

The global deployment of Domain Name System Security Extensions (DNSSEC) will achieve an important milestone on June 16, 2010 as ICANN hosts the first production DNSSEC key ceremony in a high security data centre in Culpeper, VA, outside of Washington, DC.

ars technica

MAIN MENU · MY STORIES: 25 · FORUMS · SUBSCRIBE · JOBS · ARS CONSORTIUM

RISK ASSESSMENT / SECURITY & HACKTIVISM

DNS root zone finally signed, but security battle not over

The root of the DNS hierarchy is now protected with a cryptographic signature …

by **Iljitsch van Beijnum** - Jul 16, 2010 11:28pm CEST

Yesterday, the DNS root zone was signed. This is an important step in the deployment of DNSSEC, the mechanism that will finally secure the DNS against manipulation by malicious third parties.

, VA - location of first DNSSEC key signing ceremony

Schneier on Security

Blog · Newsletter · Books · Essays · News · Schedule · Crypto · About Me

← Pork-Filled Counter-Islamic Bomb Device

Security Vulnerabilities of Smart Electricity Meters →

DNSSEC Root Key Split Among Seven People

The DNSSEC root key has been divided among seven people:

> Part of ICANN's security scheme is the Domain Name System Security, a security protocol that ensures Web sites are registered and "signed" (this is the security measure built into the Web that ensures when you go to a URL you arrive at a real site and not an identical pirate site). Most major servers are a part of DNSSEC, as it's known, and during a major international attack, the system might sever connections between important servers to contain the damage.

The Eastern KSK Repository

Secure data center in Culpeper, VA - location of first DNSSEC key signing ceremony

The Western KSK Repository

El Segundo, California *

* No – that's not really a picture of the the El Segundo KSK repository facilitie

KSK?

- The Root Zone Key Signing Key signs the DNSKEY RR set of the root zone
  - The Zone Signing Key (ZSK) signs the individual root zone entries
- The KSK Public Key is used as the DNSSEC Validation trust anchor
  - It is copied everywhere as “configuration data”
- The KSK Private Key is stored inside an HSM

Five Years Ago…

Root DNSSEC Design Team

F. Ljunggren
Kirei
T. Okubo
VeriSign
R. Lamb
ICANN
J. Schlyter
Kirei
May 21, 2010

DNSSEC Practice Statement for the Root Zone KSK Operator

Abstract

This document is the DNSSEC Practice Statement (DPS) for the Root Zone Key Signing Key (KSK) Operator. It states the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. These include, but are not limited to: issuing, managing, changing and distributing DNS keys in accordance with the specific requirements of the U.S. Department of Commerce.

6.3. Signature format

The cryptographic hash function used in conjunction with the signing algorithm is required to be sufficiently resistant to preimage attacks during the time in which the signature is valid.

The RZ KSK signatures will be generated by encrypting SHA-256 hashes using RSA [RFC5702].

6.4. Zone signing key roll-over

ZSK rollover is carried out quarterly automatically by the Root Zone ZSK Operator's system as described in the Root Zone ZSK Operator's DPS.

6.5. Key signing key roll-over

Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation.

RZ KSK roll-over is scheduled to facilitate automatic updates of resolvers' Trust Anchors as described in RFC 5011 [RFC5011].

After a RZ KSK has been removed from the key set, it will be retained after its operational period until the next scheduled key ceremony, when the private component will be destroyed in accordance with section 5.2.10.

Five Years Ago…

Root DNSSEC Design Team

F. Ljunggren
Kirei
T. Okubo
VeriSign
R. Lamb
ICANN
J. Schlyter
Kirei
May 21, 2010

DNSSEC Practice Statement for the Root Zone KSK Operator

Abstract

This document is the DNSSEC Practice Statement (DPS) for the Root Zone Key Signing Key (KSK) Operator. It states the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. These include, but are not limited to: issuing, managing, changing and distributing DNS keys in accordance with the specific requirements of the U.S. Department of Commerce

6.3. Signature format

The cryptographic hash function used in conjunction with the signing algorithm is required to be sufficiently resistant to preimage attacks during the time in which the signature is valid.

The RZ KSK signatures will be generated by encrypting SHA-256 hashes using RSA [RFC5702].

6.4. Zone signing key roll-over

ZSK rollover is carried out quarterly automatically by the Root Zone ZSK Operator's system as described in the Root Zone ZSK Operator's DPS.

6.5. Key signing key roll-over

Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation.

RZ KSK roll-over is scheduled to facilitate automatic updates of resolvers' Trust Anchors as described in RFC 5011 [RFC5011].

After a RZ KSK has been removed from the key set, it will be retained after its operational period until the next scheduled key ceremony, when the private component will be destroyed in accordance with section 5.2.10.

It's Time!

The Cast of Actors

- Root Zone Management Partners:
  - Internet Corporation for Assigned Names and Numbers (ICANN)
  - National Telecommunications and Information Administration, US Department of Commerce (NTIA)
  - Verisign
- External Design Team for KSK Roll

Approach

- ICANN Public Consultation – 2012
- Detailed Engineering Study - 2013
- SSAC Study (SAC-063) - 2013
- KSK Roll Design Team - 2015

Design Team Members

- Joe Ably
- John Dickinson
- Ondrej Sury
- Toshiro Yoneya
- Jaap Akkerhuis
- Paul Wouters
- Geoff Huston

Plus the participation from the Root Zone Management Partners

2015 Design Team Milestones

- January – June:

  Study, discuss, measure, ponder, discuss some more

- June
  - Present a draft report for ICANN Public Comment
- July
  - Prepare final report
- Pass to the Root Zone Management Partners who then will develop an operational plan and execute

Rolling the KSK?

- All DNS resolvers that perform validation of DNS responses use a local copy of the KSK
- They will need to load a new KSK public key and replace the existing trust anchor with this new value at the appropriate time
- This key roll could have a public impact
- We have had some experience in the past on issues arising from rolling keys…

Roll Over and Die?

February 2010

George Michaelson
Patrik Wallström
Roy Arends
Geoff Huston

In this month's column I have the pleasure of being joined by George Michaelson, Patrik Wallström and Roy Arends to present some critical results following recent investigations on the behaviour of DNS resolvers with DNSSEC. It's a little longer than usual, but I trust that its well worth the read.
-- *Geoff*

It is considered good security practice to treat cryptographic keys with a healthy level of respect. The conventional wisdom appears to be that the more material you sign with a given private key the more clues you are leaving behind that could enable some form of effective key guessing. As RFC4641 states: "the longer a key is in use, the greater the probability that it will have been compromised through carelessness, accident, espionage, or cryptanalysis." Even though the risk is considered slight if you have chosen to use a decent key length, RFC 4641 recommends, as good operational practice, that you should "roll" your key at regular intervals. Evidently it's a popular view that fresh keys are better keys!

The standard practice for a "staged" key rollover is to generate a new key pair, and then have the two public keys co-exist at the publication point for a period of time, allowing relying parties, or clients, some period of time to pick up the new public key part. Where possible during this period, signing is performed twice, once with each key, so that the validation test can be performed using either key. After an appropriate interval of parallel operation the old key pair can be deprecated and the new key can be used for signing.

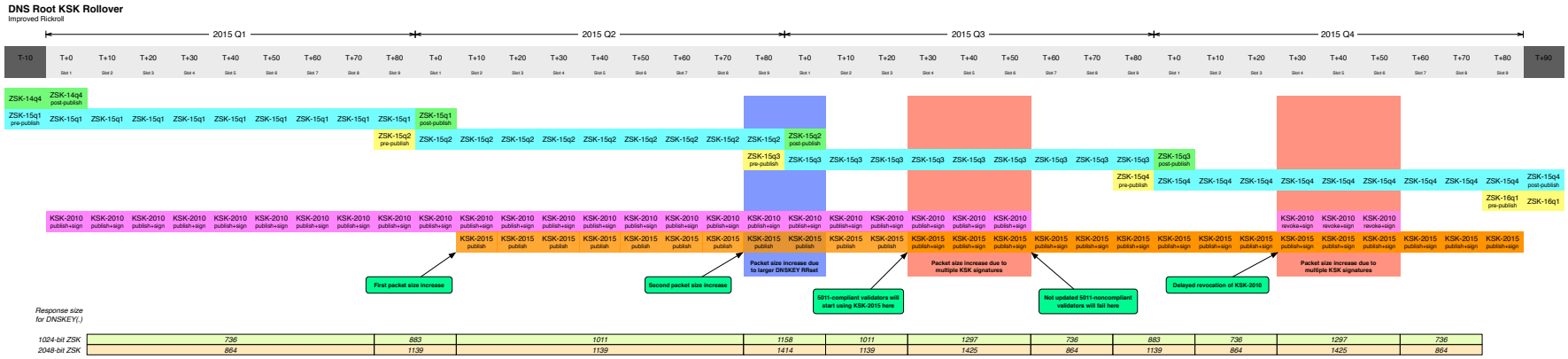
This practice of staged rollover as part of key management is used in X.509 certificates, and is also used in signing the DNS, using DNSSEC. A zone operator who wants to roll the DNSSEC key value would provide notice of a pending key change, publish the public key part of a new key pair, and then use the new and old private keys in parallel for a period. On the face of it, this process sounds quite straightforward.

What could possibly go wrong?

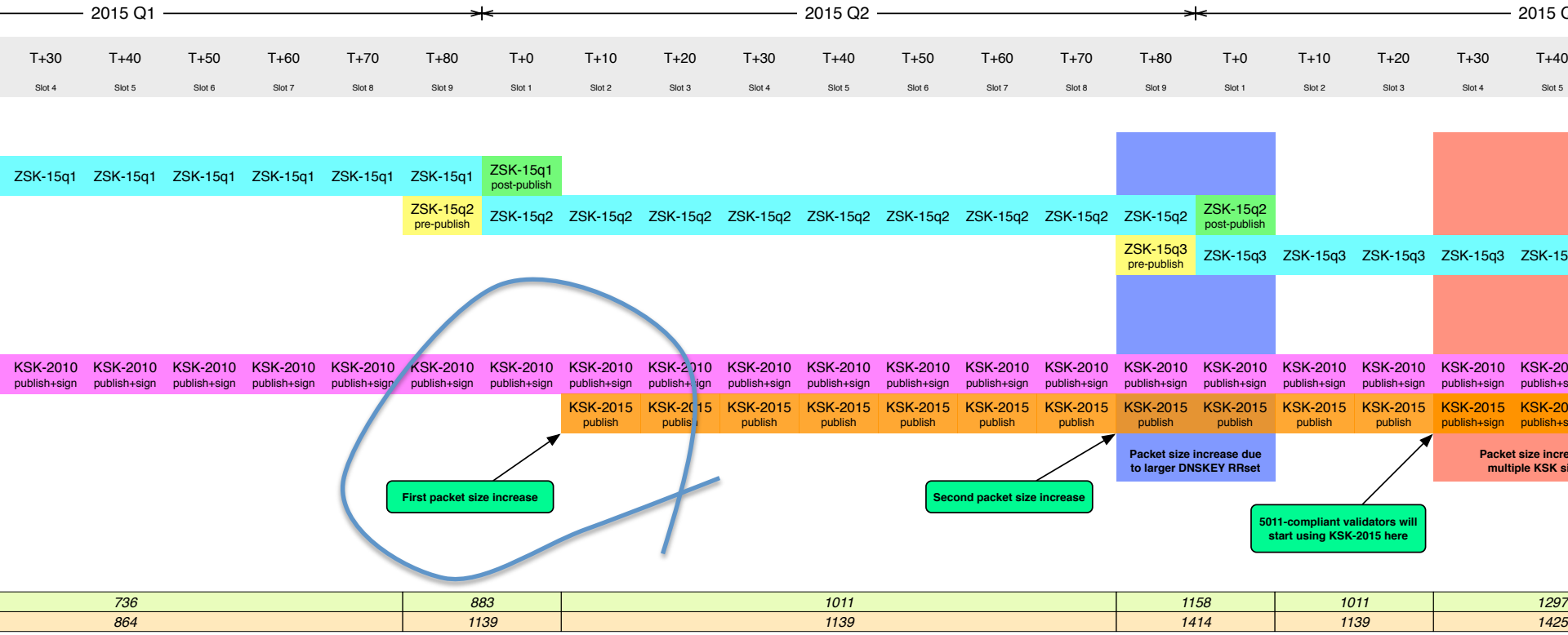
The RFC5011 Approach

- Publish a new KSK and include it in DNSKEY responses
- Use the new KSK to sign the ZSK, as well as the old KSK signature
  - Resolvers use old-signs-over-new to pick up the new KSK, validate it using the old KSK, and replace the local trust anchor material with the new KSK
- Withdraw the old signature signed via the old KSK
- Revoke the old KSK

The RFC5011 Approach

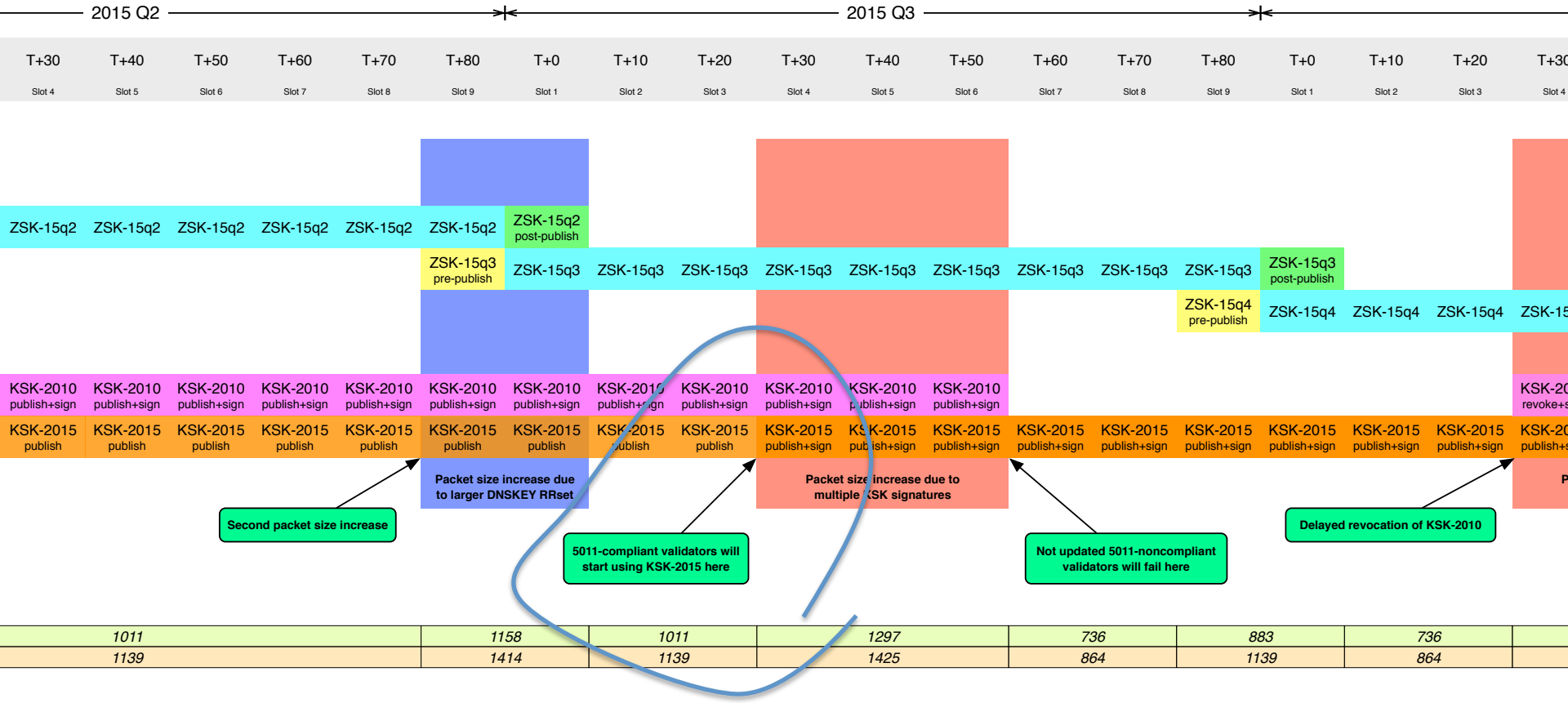


1. Introduce New KSK

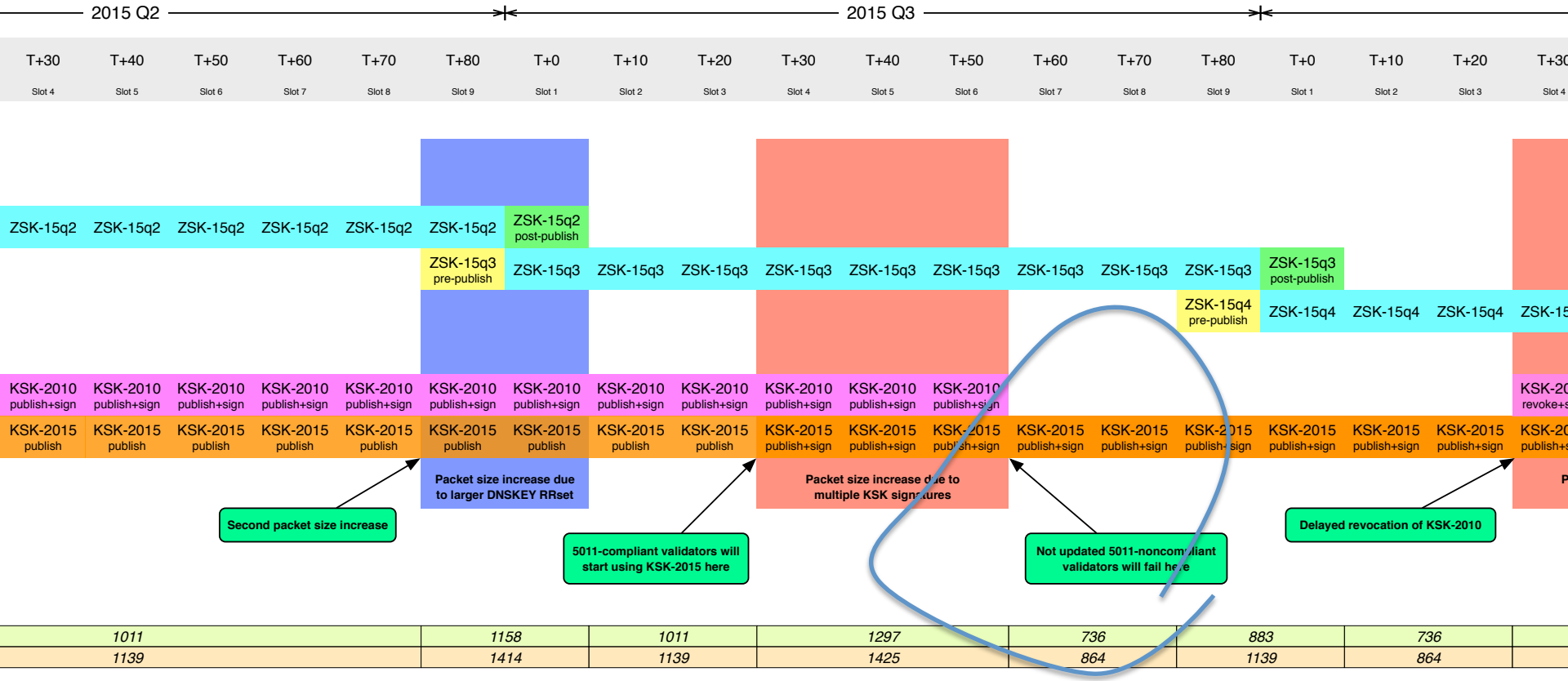


736	*883*	*1011*	*1158*	*1011*	*1297*
864	*1139*	*1139*	*1414*	*1139*	*1425*

2. New KSK signs

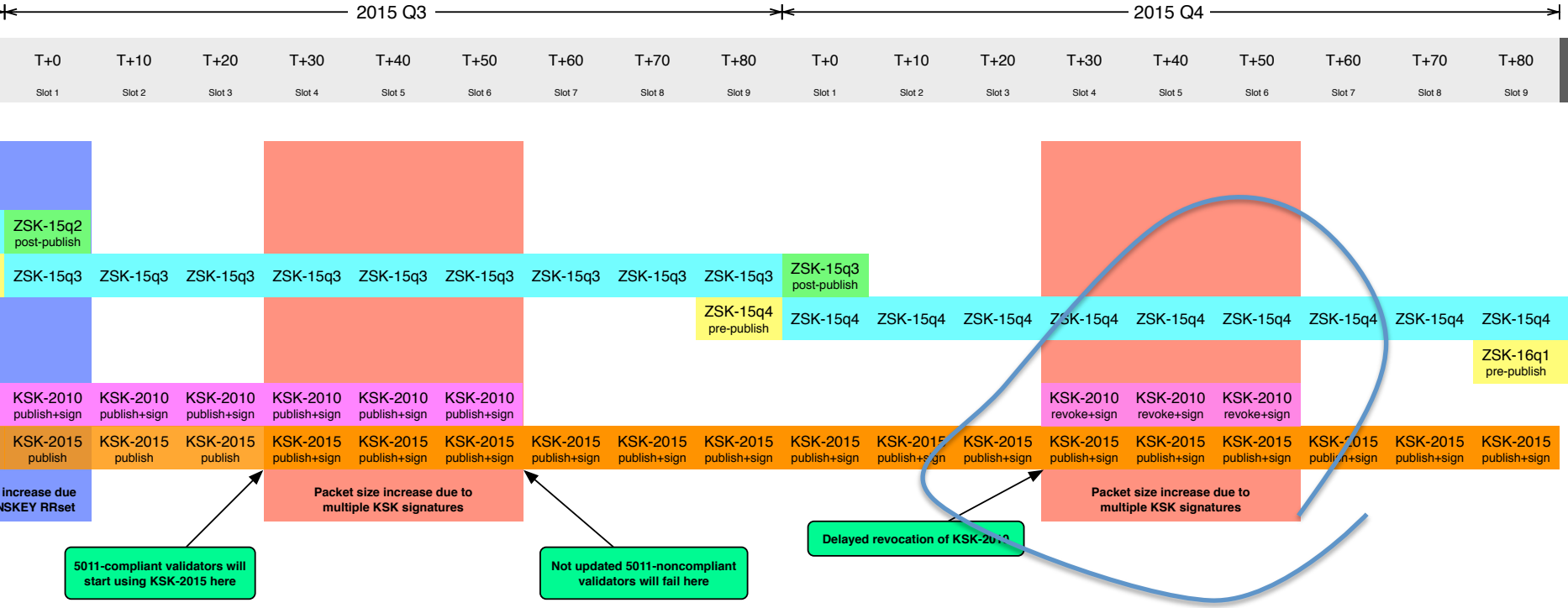


3. Remove old KSK



1011	*1158*	*1011*	*1297*	*736*	*883*	*736*	
1139	*1414*	*1139*	*1425*	*864*	*1139*	*864*	

4. Destroy old KSK



158	*1011*	*1297*	*736*	*883*	*736*	*1297*	*736*
414	*1139*	*1425*	*864*	*1139*	*864*	*1425*	*864*

Technical Concerns

- Some DNSSEC validating resolvers do not support RFC5011
  - How many?
  - What will they do when validation fails?
- During the Dual-Sign phase of the roll the RZ DNSKEY responses will be larger
  - Interaction with IPv6 and 1280 minimum MTU - UDP fragmentation?
  - Interaction with EDNS0 UDP Buffer Size and response truncation - Increased TCP query loads?
  - How many resolvers will be stranded by these larger responses?
- Can you bench test your DNS resolvers in a KSK roll?

Some Numbers

- Up to 90% of unique queries posed to authoritative name servers use EDNS0 and set DNSSEC OK
- Up to 24% of unique queries are followed by DNSSEC validation
- Up to 11% of unique queries will be followed by a non-validating query sequence if DNSSEC validation fails

Some More Numbers

- Some 8% of unique queries have an EDNS0 UDP buffer size < 1,500 octets
  - These queries would revert to TCP in the case of a large response

- What is not directly measureable by experimental sampling of resolver behaviors is the extent to which resolvers support RFC5011 key roll signalling

Community Concerns

- How can the Root Zone Partners keep you informed about the KSK Roll process?
  - What do you need to know?
  - How would you like to be informed?

Questions?