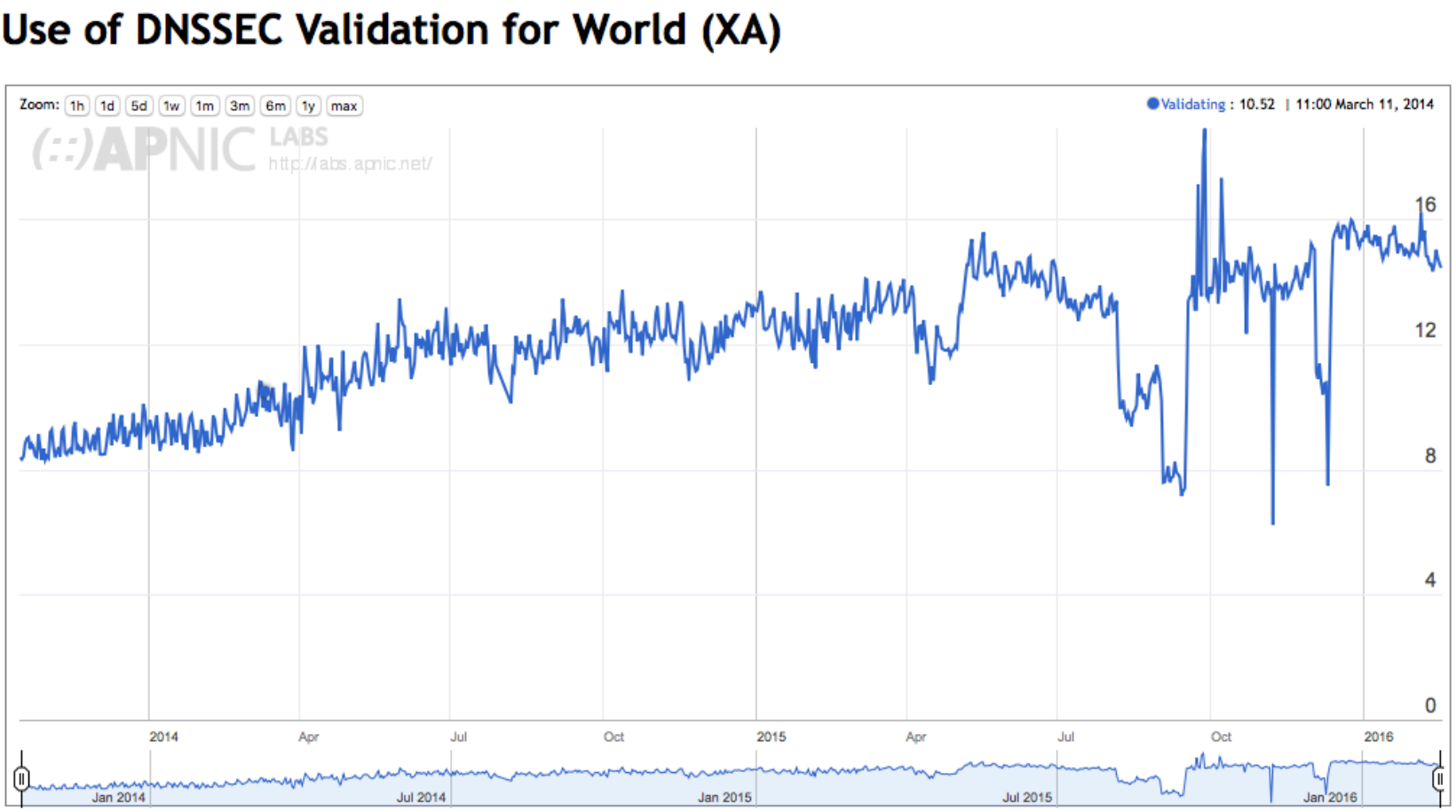
Rolling the Root

Geoff Huston
APNIC Labs
March 2016

Use of DNSSEC Validation in Today's Internet



Why is this relevant?

Because…

the root zone managers are preparing to roll the DNS Root Zone Key Signing Key

(and this may break your DNS service!)

and 9 months

Five Years Ago…

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.

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.

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.

Five Years and 9 months 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 and 9 months Ago…

Root DNSSEC Design Team

F. Ljunggren
Kirei
T. Okubo
VeriSign
R. Lamb
ICANN
J. Schlyter
Kirei

"after 5 years of operation"

The Root Zone Managers made a commitment to all those those users who are placing their trust in the integrity of this DNS Root Key that its management will entail a key roll "after 5 years of operation" – which in my view means that this should be happening more or less about NOW, if not sooner!

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.

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”
– Most of the time the KSK is kept offline in highly secure facilities

The Eastern KSK Repository

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

The Western KSK Repository

El Segundo, California *

The Ultra Secret Third KSK Repository in Amsterdam

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

2015 Design Team Milestones

- January – June:

  Study, discuss, measure, ponder, discuss some more

- August
  - Present a draft report for ICANN Public Comment

    https://www.icann.org/public-comments/root-ksk-2015-08-06-en

    (comment close 5th October 2015)

- October
  - Prepare final report

- December
  - Report passed to ICANN to work with the Root Zone Management Partners to develop an operational plan and execute

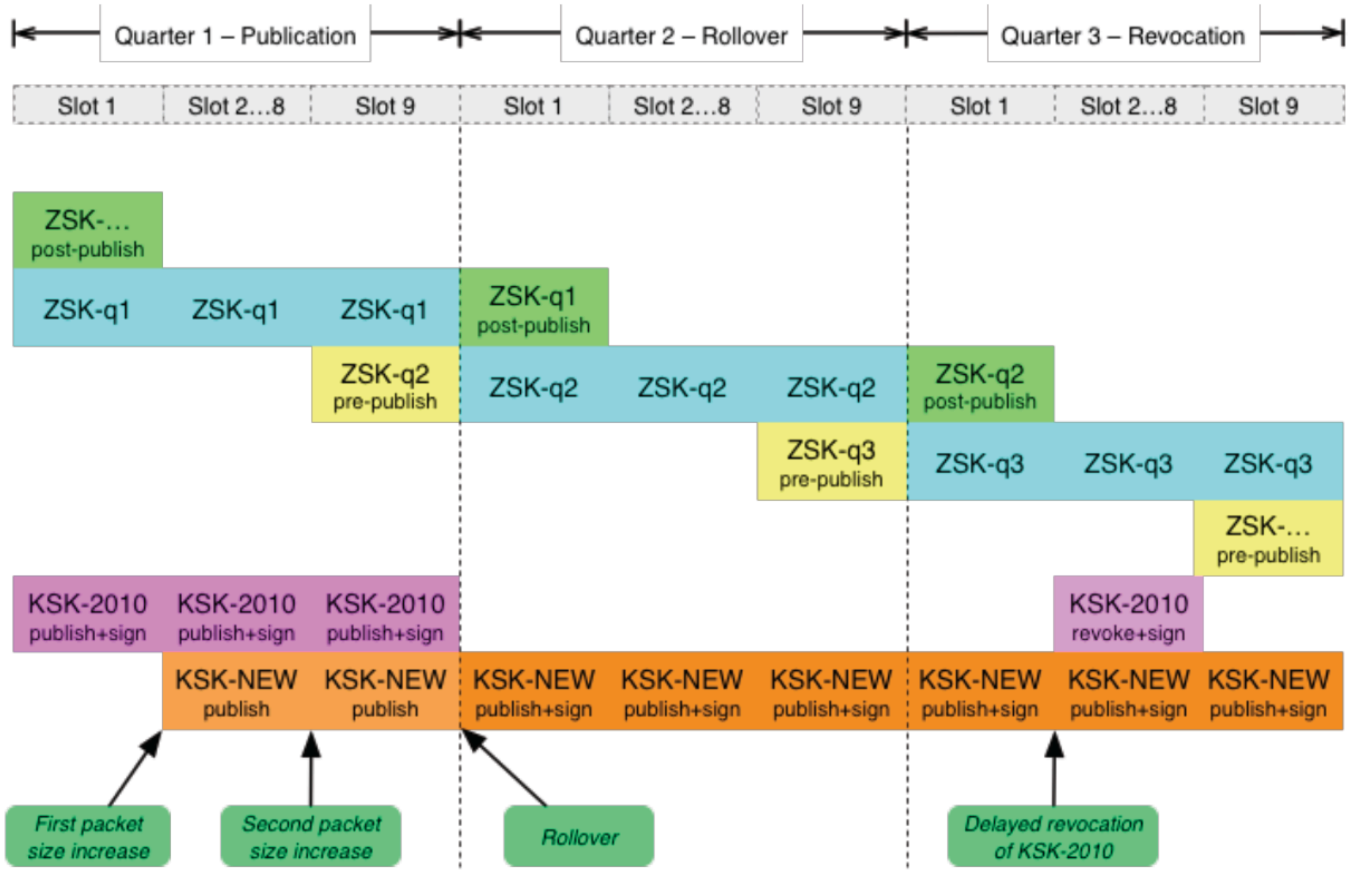
Rolling the KSK?

- 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, particularly if DNSSEC-validating resolvers do not load the new KSK

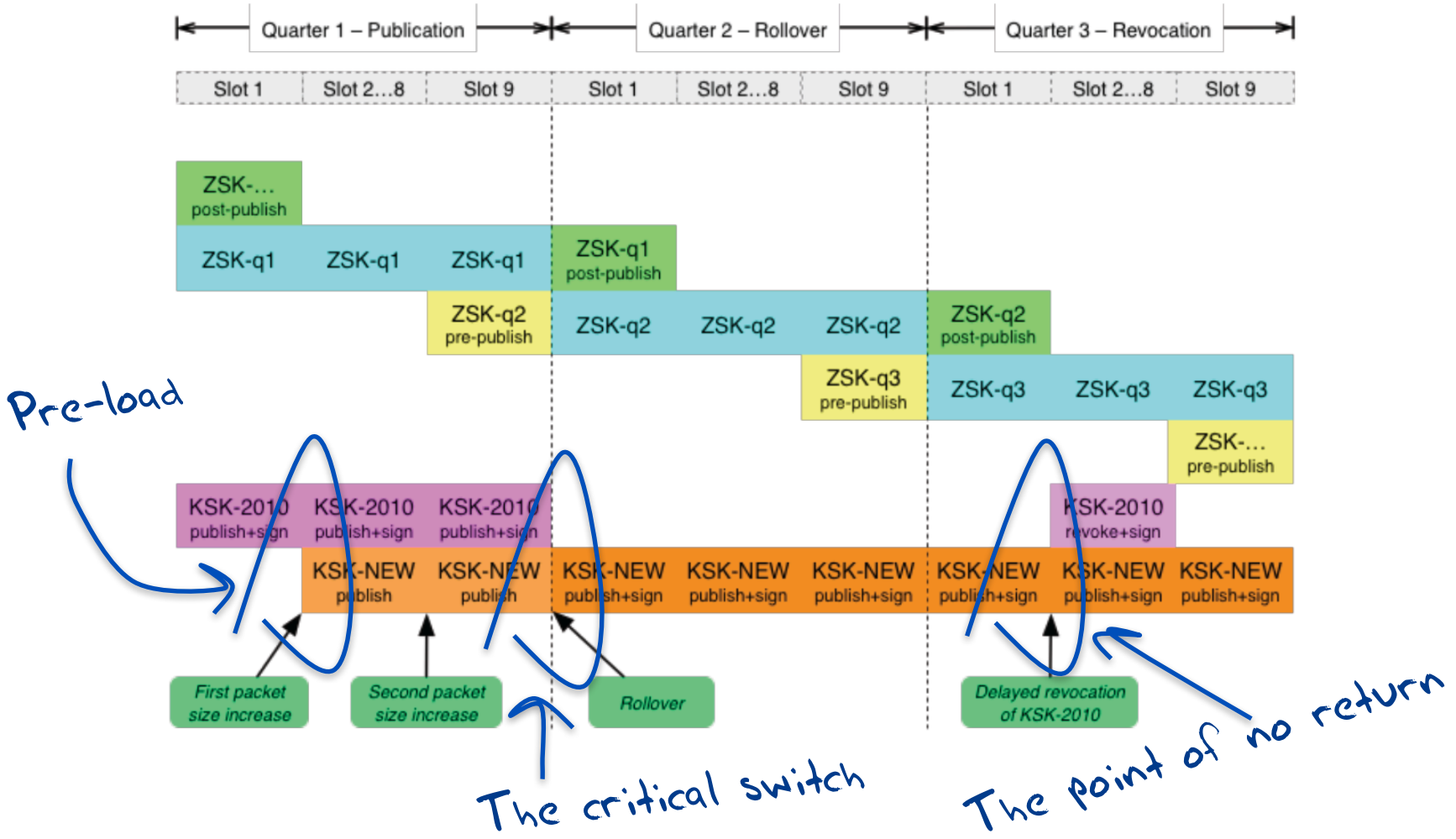
Easy, Right? Just follow RFC5011…

- Publish a new KSK and include it in DNSKEY responses, signed by the old KSK
  - Resolvers use old-signs-over-new to pick up the new KSK, validate it using the old KSK, and add the new KSK to the local cache of trust anchor material (i.e. this steps allows resolvers to “learn” the new KSK as a trust point)
- Wait
  - For at least 30 days
- Withdraw the old KSK
  - And sign the DNSKEY RR in the root zone with only the new KSK
- Wait
  - For a a while
- Revoke the old KSK
  - Because its never wise to keep old information in a trusted state

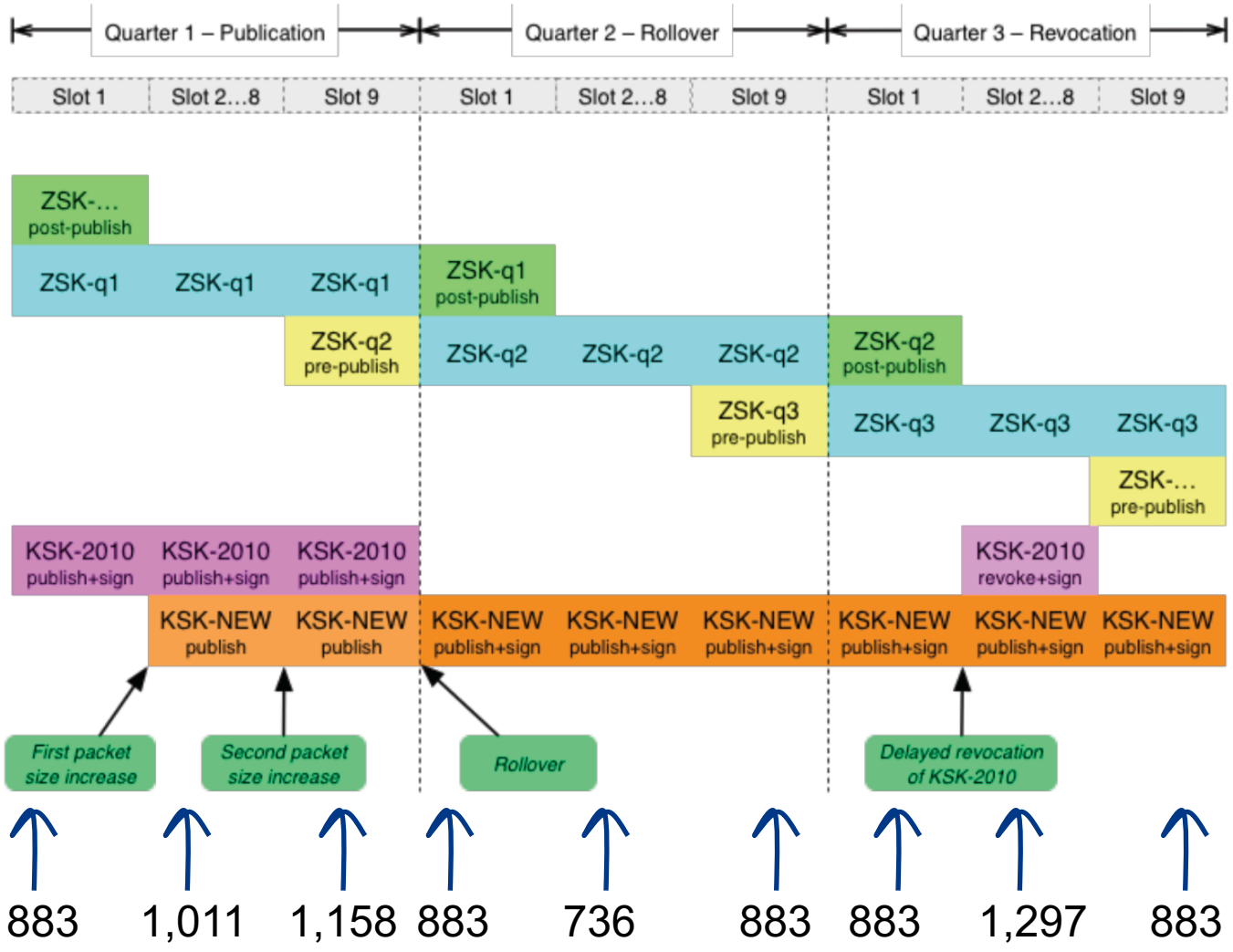
The RFC5011 Approach



The RFC5011 Approach



The RFC5011 Approach



Easy, Right?

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?

But that was then…

And this is now:

- Resolvers are now not so aggressive in searching for alternate validation paths when validation fails

  (as long as resolvers keep their code up to date, which everyone does – right?)
- And now we ***all*** support RFC5011 key roll processes
- And ***everyone*** can cope with large DNS responses

So all this will go without a hitch

Nobody will even notice the KSK roll at the root

But that was then…

And this is now:

- Resolvers are now not so aggressive in searching for alternate validation paths when validation fails
  - (as long as resolvers keep their code up to date, which everyone does)
- And now we only roll processes
- And ***everyone*** DNS responses

So all this will go w

Nobody will even notice the KSK roll at the root

Not!

What we all should be concerned about…

That resolvers who validate DNS responses will fail to pick up the new DNS root key automatically

- i.e. they do not have code that follows RFC5011 procedures for the introduction of a new KSK

The resolvers will be unable to receive the larger DNS responses that will occur during the dual signature phase of the rollover

Technical Concerns

- Some DNSSEC validating resolvers do not support RFC5011
  - How many resolvers may be affected in this way?
  - How many users may be affected?
  - What will the resolvers do when validation fails?
    - Will they perform lookup ‘thrashing’
  - What will users do when resolvers return SERVFAIL?
    - How many users will redirect their query to a non-validating resolver

Technical Concerns

- Some DNSSEC validating resolvers do not support RFC5011
  - How many resolvers may be affected
  - How many users
  - W
  - when resolvers return SERVFAIL?
    - How many users will redirect their query to a non-validating resolver

Really hard to test this in the wild with recursive resolvers

Some Observations - 1

There is a LOT of DNSSEC validation out there

- 87% of all queries to authoritative name servers have EDNS0+DNSSEC-OK set
- 33% of all DNSSEC-OK queries attempt to validate the response
- 30% of end users are using DNS resolvers that will validate what they are told
- 15% of end users don't believe bad validation news and turn to other non-validating resolvers when validation fails.
- The other 15% validate the answers and will accept bad news as the final word.

Some Observations - 2

The larger DNS responses will probably work

- The “fall back to TCP” will rise to 6% of queries when the response size get to around 1,300 octets
- And the DNS failure rate appears to rise by around 1 - 2 %

- BUT .org has been running its DNSKEY response at 1,650 octets and nobody screamed failure!
  - So it will probably work?

Some Observations - 3

We can't measure automated key take up

- We can't see how many validating resolvers fail to use RFC5011 to pick up the new KSK as a Trust Anchor in advance
- We will not know how many "new' validating resolvers appear in the 30 day holddown period with the old key pre-loaded

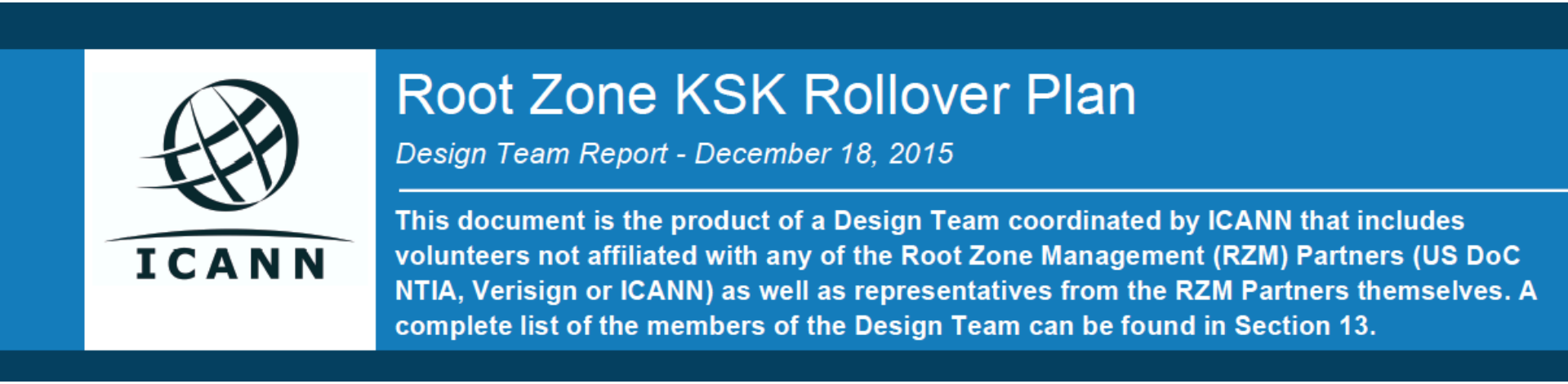
- We will only see these cases via failure on key roll

Where are we?

- A key roll of the Root Zone KSK will cause some resolvers to fail:
  - Resolvers who do not pick up the new key in the manner described by RFC5011
  - Resolvers who cannot receive a DNS response of ~1,300 octets
- Many users who use these failing resolvers will just switch over to use a non-validating resolver
- A small pool of users will be affected with no DNS

KSK Design Team

A report from the design team that was completed in December 2015…



This was published by ICANN on the 7th March 2016

https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf

Design Team Recommendations

Recommendation 1: The Root Zone KSK Rollover should follow the procedures described in RFC 5011 to update the Trust Anchors during Key Signing Key Rollover.

Recommendation 2: ICANN should identify key DNS software vendors and work closely with them to formalize processes to ensure that trust anchor distribution using vendor-specific channels is robust and secure.

Recommendation 3: ICANN should identify key DNS systems integrators and work closely with them to formalize processes to ensure that trust anchor distribution using integrator-specific channels is robust and secure.

Recommendation 4: ICANN should take an active role in promoting proper Root Zone Trust Anchor authentication, including highlighting the information posted on ICANN's IANA website.

Recommendations (cont)

Recommendation 5: Root Zone KSK Rollover should require no substantive changes to existing KSK management and usage processes in order to retain the high standards of transparency associated with them.

Recommendation 6: All changes to the Root Zone DNSKEY RRsets must be aligned with the 10-day slots described in the KSK Operator's DPS.

Recommendation 7: The existing algorithm and key size for the incoming KSK for the first Root Zone KSK rollover should be maintained.

Recommendation 8: The choice of algorithm and key size should be reviewed in the future, for subsequent Root Zone KSK rollovers.

Recommendation 9: ICANN, in cooperation with the RZM partners, should design and execute a communications plan to raise awareness of the Root Zone KSK rollover, including outreach to the global technical community through appropriate technical meetings and to "channel partners" such as those identified in this document.

Recommendations (cont)

Recommendation 10: ICANN should request that RSSAC coordinate a review of the detailed timetable for the KSK rollover period before it is published, and should accommodate reasonable requests to modify that timetable in the event that any root server operator identifies operational reasons to do so.

Recommendation 11: ICANN should coordinate with RSSAC and the RZM Partners to ensure that real-time communications channels are used to ensure good operational awareness of the root server system for each change in the Root Zone that involves the addition or removal of a KSK.

Recommendation 12: ICANN should coordinate with RSSAC to request that the root server operators carry out data collection that will inform subsequent analysis and help characterize the operational impact of the KSK rollover, and that the plans and products of that data collection be made available for third-party analysis.

Recommendation 13: The RZM partners should ensure that any future increase in ZSK size is carefully coordinated with KSK rollovers, such that the two exercises are not carried out concurrently.

Recommendations

Recommendation 14: In order to support a number of potential operational contingencies that may require rollback of changes to the root zone during each phase of the KSK keyroll, SKRs generated using the incumbent KSK, SKRs generated using both the incumbent and the incoming KSK, and SKRs generated using the incoming KSK should be generated. The

Design Team also recommends that the dual signing approach is the preferred mechanism to respond to a requirement to perform a rollback in Quarter 2 of the key roll procedure.

Recommendation 15: The Root Zone Management partners should undertake or commission a measurement program that is capable of measuring the impact of changes to resolvers' DNSSEC validation behavior, and also capable of estimating the population of endpoints that are negatively impacted by changes to resolvers' validation behavior.

Recommendation 16: Rollback of any step in the key roll process should be initiated if the measurement program indicated that a minimum of 0.5% of the estimated Internet end user population has been negatively impacted by the change 72 hours after each change has been deployed into the root zone

Recommendations (cont)

Recommendation 17: It is recommended that the KSK Rollover process should commence on 1 April 2016, commencing with a nine-month period to generate the new KSK and use the existing scheduled KSK access ceremonies across the March to December 2016 period to generate the new KSK, copy it to the secondary facility and prepare the key material to be used in the keyroll. The actions associated with changes to the root zone, using the steps and associated timetable as described in Section 9 of this report will commence on 1 January 2017. The publication of the new KSK should be incorporated into the Root Zone on 11 January 2017, and the old KSK withdrawn and the new KSK to be used in its place on 1 April 2017. If the outcome of the process to evaluate acceptance of the new KSK meets the acceptance criteria described in Section 10 of this report, then the old KSK should be revoked starting on 11 July 2017 and the revocation should be removed from the root zone 70 days thereafter, on 19 September 2017.

it's already March so this proposed timetable may be a challenge to achieve☹

What can I do?

Check your recursive resolver config!

Good Dog!

```
# // recursive resolver configuration - Bind
…
managed-keys {
        . initial-key 257 3 5 "AwEAAfdqNV
          JMRMzrppU1WnNW0PWrGn4x9dPg
…
          =„; };
```

Bad Dog!

```
# // recursive resolver configuration - Bind
…
trusted-keys {
        . 257 3 5 "AwEAAfdqNV
          JMRMzrppU1WnNW0PWrGn4x9dPg
…
          =„; };
```

Update after the Verisign ZSK presentation …

- The ZSK is planned to shift to a 2048 bit key in the second half of 2016
- Its likely that the KSK roll would be delayed, to allow the ZSK key size change to be completed before embarking on the KSK roll
- Signed Root DNSKEY response sizes will increase:
  - 1 x ZSK, 1 x KSK, 1 x KSK signature: 864 octets
  - 2 x ZSK, 1 x KSK, 1 x KSK signature: 1,139 octets
  - 1 x ZSK , 2 x KSK, 1 x KSK signature: 1,139 octets
  - 2 x ZSK , 2 x KSK, 1 x KSK signature: 1,414 octets
  - 1 x ZSK , 2 x KSK, 2 x KSK signatures: 1,425 octets

Questions?

Comments/Discussion points - 1

Why Now?

What is the imperative to roll the key now? Could we use more time to improve preparedness for this roll? For example, could we use further time to introduce some explicit EDNS(0) signalling options in resolvers to expose RFC5011 capability?

Comments - 2

Measuring and Testing?

What measurements are planned to be undertaking during the key roll process? What are the threshold metrics for proceeding to the next phase? What is the threshold metric to proceed with the revocation of the old KSK?

Comments - 3

Algorithm Change

The report's language around the potential for algorithm change is unclear. There appears to be a strong bias to retention of RSA as the KSK algorithm, despite evidence that ECDSA is both shorter and potentially faster to compute. Whilst the report argues for a reduced risk of large packets, it doesn't clearly explain why larger RSA-based DNS response payloads would be preferable to smaller ECDSA DNS response payloads.

Comments - 4

Scheduling

The report notes as a constraint that a key roll must be aligned with existing Quarter and 10-day periods used in existing processes. This has the potential consequence of scheduling the critical change in the root zone on a weekend, or on a major public holiday. Why?

Comments - 5

Serialization

The report assumes a single new KSK. What are the issues of introducing 2 or even 3 new KSKs at this point?

Comments - 6

All together all at once?

Why do all root zones flip to use the new KSK all at the same time?

Why is there not a period of dual sigs over the root ZSK?

Why not allow each root server to switch from old to old+new to new using a staggered timetable?

There may be perfectly sound reasons why all together all at once is a better option than staggered introduction, but report does not appear to provide any such reasons.