Rolling the Root

APNIC Labs
Goff Huston
Use of DNSSEC in Today's Internet
Use of DNSSEC Validation for Northern America (xG)
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!)

Because the root zone managers are preparing to roll the DNS Root Zone Key Signing Key.
Five Years Ago...

The DNSSEC root key has been divided among seven people:

Schneier on Security

ICANN’s First DNSSEC Key Ceremony For the Root Zone
Five Years Ago…

Section 5.2.10.

At time the privilege component will be destroyed in accordance with
after the operation perant until the n"st 4 years. Key copyman
After a key has been removed from the key server, it will be removed
resoures from the key server. (RC 1211) [REC 321]

An XSK roll-over is scheduled to occur automatically on a
cessionary as required, or after 5 years of operation.

each RX XSK will be scheduled to be rotated over through a Key

6.3. Key Rotating Key Roll-over

DS.

RXK operator's system as described in the root zone RXK operator's
RXK Roll-over. The root zone RXK operator's

6.4. Zone Signing Key Roll-over

when RXK (R2C572) / The RXK signature will be generated by encrypting SHA-256 hashes

The RXK signature will be generated by encrypting SHA-256 hashes


Roost Zone RXK Operator DS

with the specific requirements of the U.S. Department of Commerce.
Licensing, Managing, Chaining and Distributing DNS Keys in accordance
these notices, but are not limited to distribution.

This document is the DNSSEC Practice Statement (PDS) for the Root

Abstract

DNSSEC Practice Statement for the Root Zone RXK Operator

May 21, 2010

Key
Signature
DS
IN
T. Oxbog

F. Juggard

FIVE YEARS AGO...
Five Years Ago…

When the plate is removed, the cryozone is removed from the storage station. Each cryozone will be scheduled to be rotated over through a key.

Abstract

This document is the DSSC Practitioner's Statement (DPS) for the root DSSC Operator.

Project Design Team

Five Years Ago
Zone Signing Key

- The DNSKEY record for the ZSK is signed by the KSK.
- The ZSK is rolled regularly every quarter.
- Zone Signed Keying Key is used to generate the digital signature RRSIG records in the root.
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

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

- It is copied everywhere as "configuration data"
Secure data center in Culpeper, VA - Location of first DNSSEC Key Signing Ceremony

The Eastern KSK Repository
KSK spotting by George Michelson

The Ultra Secret Third KSK Repository in Amsterdam
KSK spotting by George Michaelson

The Uruguay Mobile KSK

Uruguay
SAL. 6621
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

• October – Prepare Final Report

  (comment close 5th October 2015)


• October – Pass to the Root Zone Management Partners who then will develop an operational plan and execute

• January – June:
Rolling the KSK?

- All DNS resolvers that perform validation of DNS responses do not load the new KSK.
- This key roll could have a public impact, particularly if DNSSEC-validating resolvers do not load a new KSK public key and replace the existing trust anchor with this new value at the appropriate time.
- They will need to load a new KSK public key and replace a local copy of the KSK.
- All DNS resolvers that perform validation of DNS responses.
Easy, Right?

- 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
- Revoking the old KSK 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

Easy, Right!
The RFC5011 Approach
Just Like Last Time?

What could possibly go wrong?

Just Like Last Time?

What could possibly go wrong?

Just Like Last Time?

What could possibly go wrong?

Just Like Last Time?

What could possibly go wrong?

Just Like Last Time?

What could possibly go wrong?

Just Like Last Time?

What could possibly go wrong?

Just Like Last Time?

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)

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

- Everybody can cope with large DNS responses.

- And now we all support RFC5011 key roll processes.

So all this will go without a hitch.

Nobody will even notice the KSK roll at the root.

Truly truly!

And this is now:
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 validates when validation fails)

– Everyone can cope with large DNS responses

– And now we all support RFC5011 key roll processes

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

So all this will go without a hitch.

Nobody will even notice the KSK roll at the root.

Not!

Truly Ruly!
What we all should be concerned about...

That resolvers who validate DNS responses will fail to pick up the new DNS root key automatically during the dual signature phase of the rollover. The resolvers will be unable to receive the larger DNS responses that will occur during the dual signature phase of the rollover.

That resolvers who validate DNS responses will fail to pick up introduction of a new KSK — i.e., they do not have code that follows RFC5011 procedures for the new DNS root key automatically.

...concerned about...

What we all should be...
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 may be affected?
- What will the resolvers do when validation fails?
- Will they perform lookup 'thrashing'?
- What will users do when resolvers return SERVFAIL?
- Really hard to test this in the wild with recursive resolvers

RFC5011

How many users will redirect their query to a non-validating resolver if resolvers return SERVFAIL?

Some DNSSEC validating resolvers do not support RFC5011.
There is a LOT of DNSSEC validation out there:

- 30% of all queries have DNSSEC-OK set
- 87% of all queries have DNSSEC-OK set
- 25% of end users are using DNS resolvers that will validate the response
- 12% of end users don’t believe bad validation news and turn to other non-validating resolvers when validation fails.

Some Observations – 1
Some Observations - 2

There is very little IPv6 being used out there - 1% of queries use IPv6 as the transport protocol when given a dual stack name server.

It seems that when given a choice:

- Browsers prefer IPv6
- Resolvers prefer IPv4
Some Observations

ECDSA is viable—sort of

1 in 5 clients who use resolvers that validate RSA-signed responses are unable to validate the same response when signed using ECDSA.

But they fail to "unsigned" rather than "invalid" so it's a (sort of) safe fail.
Some Observations - 4

- So it will probably work
- 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 1,350 octets
- And the DNS failure rate appears to rise by around 1 - 2%
- BUT .org currently runs at 1,650 octets and nobody is screaming
- The larger DNS responses will probably work
We can't measure automated key take up – we can't see how many resolvers fail to use RFC5011 notices to pick up the new KSK as a Trust Anchor in advance – we will only see it via failure on key roll.

Some Observations - 5
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 to use a non-validating resolver. A small pool of users will be affected with no DNS.
Public comment:
draft report for ICANN Public Comment

Comments close 5th October 2015

Please read & comment
What can I do?

Check your recursive resolver config!
Good Dog!
trusted-keys {
  257 3 5 "AWEAEATdGy" 
} 

bind {
  ! "=
...

JmMrzxppbUinm0OPWCgN4x9dpg

37
Questions?
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 signaling options in resolvers to expose RFC5011 capability?

Comments - I
What measurements are planned to be undertaken during the key roll process? What is the threshold metric for proceeding to the next phase? What are the threshold metrics for proceeding with the revocation of the old KSK?
Algorithm Change

Comments - 3

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

Comments - 5
Why do all root zones flip to use the new KSK all at once? Why is there not a period of dual signatures 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. All together all at once?