.br DNSSEC Algorithm Rollover

Frederico A. C. Neves
<fneves@registro.br>

ICANN 61 - Puerto Rico - 20180314

.br DNSSEC history

- 2007-05-04 .br initially signed
  - Using RSASHA1 1024 bits
- 2009-01-15 .[com|org].br signed
  - With the advent of nsec3/opt-out, all .br zones signed
- 2010-05-31 first KSK roll
  - Using RSASHA1 1280 bits
  - New Ceremony schema using HSMs
- 2010-06-23 .br DS hit the root
- 2015-06-18 second KSK roll
  - Using RSASHA1 1536 bits
- 2018-03-07 Currently with 3.9M delegations, 1M signed

Motivations

- ✓ Be prepared for an eventual emergency algorithm rollover
  - Exercise during regular times.
  - Current provisioning system lacks algorithm agility capabilities.
- ✓ Still using RSASHA1
  - Already rolled KSK twice and increased key lengths in 2010/2015
  - Substantially reduce response sizes (ECDSAP256SHA256)
  - Reduce the number of managed keys for second level zones as some uses NSEC3 proof of non existence requiring (RSASHA1-NSEC3-SHA1)
- ✓ Current DNS provisioning system originally written in 2004
  - Uses an old C++ dialect already showing its age.
  - Using a custom build DNS library.
  - Deficiencies at the memory management capabilities imposes operational restrictions requiring AXFR once a week for regular resigning.
- ✓ Architecture already largely “adapted” with the inclusion of DNSSEC in 2007 and signing ceremonies in 2010.
- ✓ Already porting registry system to newer architecture and technology.

Algorithm Rollover Approach

All the open source signers we are aware of, BIND "managed keys" and OpenDNSSEC, implements the “liberal” approach as described at 6781 4.1.4. But this document advices for a more “conservative" approach.

The public log around Oct/2016, on support mailing lists, reports that a validator following the “conservative” approach have being "convinced" to update and better behave with the “liberal" approach; Digging further, the starting version following the “liberal" approach is from Jan/2011, 7 years ago.

6840 in Feb/2013, 5 years ago, 5.11 clarifies the "confusing" 4035 language;

The difference from the “liberal”, that turns out to be a double-signature KSK, from the “conservative" approach is the addition of two extra steps. Only include the new key and withdraw the old one from the KEYSET, after the inclusion/withdraw of all the RRSIGs with the new/old algorithm.

We have our own signer and because of 6781 advice we were initially inclined to follow the conservative approach, but after all this findings and the recent report from a totally successful alg.roll of .SE, we’ll publicly exercise both approaches before taking a final decision. Hopefully this exercises and subsequent reports could consolidate the information and help to update current Operational Practices.

HSM Upgrades / Ceremony 2018-2

- ◇ **May 15** - HSM Upgrades
  - ✓ 4 HSMs currently in service at two ceremony facilities since May/2010. Substitute 2 of the 4 HSMs.
    - Substituted ones will be upgraded and commissioned at a third facility in Fortaleza/CE located 4000+ Km from the two current facilities that are located in São Paulo. This operation will be executed in Sep/2018 after the rollover is completed.
  - ✓ Upgrade software of the older HSMs.
  - ✓ Enrol a complete new set of HSMs Smart-cards credentials.
    - Current set is already missing 2 cards in a SSS 4 of 12. One lost, one broken.
- ◇ **May 16** - Ceremony 2018-2
  - ✓ This is a regular scheduled ceremony covering the period from Aug/18 to Jan/19.
  - ✓ This ceremony will still use our current KSK/Algorithm RSASHA1 that was rolled during ceremony 2015-1 20141208.

Ceremony Test / Rollover

◇ **Jun 18** - Exercise Ceremony

✓ 3 public zones emulating .br rollover per rollover method. .br will act as parent registry

Zone	Old Algorithm	New Algorithm	Keys	Method
ecdsa-c.br	RSASHA1	ECDSASHA256	KSK/ZSK	conservative
com.ecdsa-c.br	RSASHA1-NSEC3-SHA1	ECDSASHA256	CSK	conservative
eng.ecdsa-c.br	RSASHA1	ECDSASHA256	CSK	conservative
ecdsa-l.br	RSASHA1	ECDSASHA256	KSK/ZSK	liberal
com.ecdsa-l.br	RSASHA1-NSEC3-SHA1	ECDSASHA256	CSK	liberal
eng.ecdsa-l.br	RSASHA1	ECDSASHA256	CSK	liberal

✓ Uses a test HSM / Same Script

◇ **Jun 19** - Rollover Begin (all times reported in UTC)

✓ 06:00 AM (new algorithm) ecdsa-c.br naZSK signatures included
ecdsa-l.br double-signed

◇ **Jun 21** - New Key

✓ 06:00 AM naKSK include on the KEYSET

✓ 12:00 PM 48h window with 2 24h completion exit paths to remove (old algorithm) oaKSK and include naKSK DS at the parent zone

◇ **Jun 22** - Old Key

✓ 12:00 PM oaKSK removed from the KEYSET

✓ 06:00 PM oaZSK signatures removed - Rollover End
ecdsa-l.br old algorithm removed

Rollover - Monitoring

Recent successful .SE algorithm rollover, following the liberal approach, was monitored by SIDN LABS. An excellent and detailed report is available at the address below.

https://www.sidnlabs.nl/a/weblog/keep-m-rolling-monitoring-ses-dnssec-algorithm-rollover

We plan to use their methodology and tool for monitoring the test rollovers. After analysing the results and generate a report we'll take a decision on what path to follow for the actual rollover.

Rollover Ceremony

- ◇ **Jul 23/24** - NIC-NU/JD OS/Software Upgrade / HSM Prepare
  - ✓ Upgrade on XFRD/Signer/HW Backup on both sites (NU/JD)
  - ✓ Prepare HSM1-JD for backup
  - ✓ Change SOA Serial to Julian format from YYYYMMDD## to YYYYDDD###
  - ✓ Increase the publishing frequency from 30' to 5’
- ◇ **Jul 25** - NIC-NU Rollover Ceremony
  - ✓ Starts at 12:00 Prepare HSM2-NU for backup
  - ✓ Generate/Validate new KSK-2018 at HSM1-NU
  - ✓ Export HSM1-NU for HSM2-NU and HSM1-JD
  - ✓ Import/Validate at HSM2-NU (expected end around 14:00)
  - ✓ Move ceremony to NIC-JD transporting wrapped backup for HSM1-JD and restarts at 17:00
  - ✓ Import/Validate at HSM1-JD
  - ✓ Prepare HSM2-JD for backup
  - ✓ Export HSM1-JD for HSM2-JD
  - ✓ Import/Validate at HSM2-JD
  - ✓ Run Ceremony 2018-3 using HSM2-JD
    - ✓ Parameters Algorithm Rollover begins Aug 20th with 8 weeks possible finish paths / rollbacks
    - ✓ Sign covering the period from Aug 20th to Jan/19

Visible Changes - Important Dates

Jun 19 Test Rollover Begin [com|eng].**ecdsa.br**

at 06:00 AM

Jun 22 Test Rollover Ends

at 06:00 PM

Jul 24 Julian SOA and increased publication frequency

Jul 26 Announcements to operations ml

Aug 20 .br Algorithm Rollover Begin (Schedule if Conservative Approach)

at 06:00 AM new algorithm ZSK signatures included

Aug 22 New algorithm KSK included at the KEYSET

at 06:00 AM

Aug 23-24* IANA DS update (*tentative finish during the first window)

Aug 27*

at 12:00 PM old algorithm KSK removed from the KEYSET

at 06:00 PM old algorithm ZSK signatures removed - Rollover Ends

Questions / Comments ?

Thank You