.br DNSSEC Alg. Rollover 2018 Update

Frederico A. C. Neves
<fneves@registro.br>
ICANN 62 - Panamá - 20180625
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.
Ceremony Test / Rollover

◇ **Jun 18 - Exercise Ceremony**
  ✓ 3 public zones emulating .br rollover per rollover method. .br will act as parent registry

<table>
<thead>
<tr>
<th>Zone</th>
<th>Old Algorithm</th>
<th>New Algorithm</th>
<th>Keys</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecdsa-c.br</td>
<td>RSASHA1</td>
<td>ECDSASHA256</td>
<td>KSK/ZSK</td>
<td>conservative</td>
</tr>
<tr>
<td>com.ecdsa-c.br</td>
<td>RSASHA1-NSEC3-SHA1</td>
<td>ECDSASHA256</td>
<td>CSK</td>
<td>conservative</td>
</tr>
<tr>
<td>eng.ecdsa-c.br</td>
<td>RSASHA1</td>
<td>ECDSASHA256</td>
<td>CSK</td>
<td>conservative</td>
</tr>
<tr>
<td>ecdsa-l.br</td>
<td>RSASHA1</td>
<td>ECDSASHA256</td>
<td>KSK/ZSK</td>
<td>liberal</td>
</tr>
<tr>
<td>com.ecdsa-l.br</td>
<td>RSASHA1-NSEC3-SHA1</td>
<td>ECDSASHA256</td>
<td>CSK</td>
<td>liberal</td>
</tr>
<tr>
<td>eng.ecdsa-l.br</td>
<td>RSASHA1</td>
<td>ECDSASHA256</td>
<td>CSK</td>
<td>liberal</td>
</tr>
</tbody>
</table>

✓ Uses a test HSM / Same Script

◇ Using 1h TTLs at the Apex/DS records we could do the rollover test securely in 1 day.

◇ **Jun 19 to Jun 20 - Rollovers Test**
Rollover test - Monitoring

Using SIDN LABS monitoring technic we’ve monitored the test rollover with 1000 Ripe Atlas probes.

From a preliminary analysis of the data there is no perceived difference from each of the rollover methods.

Based on that analysis we’ve decided to follow the simpler, and slightly faster, liberal approach of algorithm rollover. This turns out to be a regular double signing rollover.
Visible Changes - Important Dates

**Jul 24** Julian SOA, 2nd level DS algorithm change (1 to 2) and increased publication frequency

**Jul 26** Announcements to operations mailing lists

**Aug 20 .br** Algorithm Rollover Begin (all times UTC)
- at 06:00 Zones double signed with old and new algorithm
- at 11:00 DS change for the second level zones
- at 13:00 Remove old algorithm keys/signatures. This is the end of the second level zones algorithm rollover
  - After 11:00 Update the .br DS at IANA

After the new DS is published at the Root zone we’ll wait 2 days and remove old algorithm keys/signatures from .br

We expect to completely finish the rollover during the first week but we’re prepared for longer periods of double signatures or a rollback if needed

**Sep 3** Apex/DS TTLs returned to regular values - 2 days / 6h
Questions / Comments?

Thank You