.br Algorithm Rollover Report
Frederico Neves <fneves@registro.br>
ICANN 63 - Barcelona - 20181024
Executive Summary

- 10 months preparation
- From RSA/SHA1 to ECDSAP256
- Executed from Aug/20th to 23rd/2018
- Went smoothly no issues reported or detected
Introduction

- .br signed since 2007
- 128+ child zones (com.br, net.br, org.br, …)
- RSA-SHA1
- 2 KSK rollovers (2010, 2015)
  - Conservative Key Size increases
    - KSK (1280 to 1536 bits)
    - CSK (1024 to 1280 bits)
Motivation

- Improve security
  - Be prepared for an Algorithm Rollover
  - ECDSA (Elliptic Curve Digital Signature Algorithm)
- Reduce DNS response size
  - RRSIGs and DNSKEYS: 60% smaller
  - Less network usage
  - Less TCP fallback
Motivation

• Complete renovation of DNS provisioning system
  ○ Previous one dates back from 2004
  ○ C++
    ■ Maintainability issues
    ■ Deficiencies in memory management
  ○ Moving to Go
Dilemma: Conservative vs Liberal

Conservative

- RFC 4035, section 2.2:
  “There MUST be an RRSIG for each RRset using at least one DNSKEY of each algorithm in the zone apex DNSKEY RRset”

- Cache taken into consideration

- 5 steps:
  1. Add New RRSIGs
  2. Add New DNSKEY
  3. Change DS
  4. Remove Old DNSKEY
  5. Remove Old RRSIGS
Dilemma: Conservative vs Liberal

Conservative
- RFC 4035, section 2.2:
  "There MUST be an RRSIG for each RRset using at least one DNSKEY of each algorithm in the zone apex DNSKEY RRset"
- Cache taken into consideration
- 5 steps:
  1. Add New RRSIGs
  2. Add New DNSKEY
  3. Change DS
  4. Remove Old DNSKEY
  5. Remove Old RRSIGS

Liberal
- RFC 6840, section 5.11
  "This requirement applies to servers, not validators. Validators SHOULD accept any single valid path."
- 3 steps (double-signing scheme)
  1. Add New DNSKEY/RRSIGs
  2. Change DS
  3. Remove Old DNSKEY/RRSIGs
Dilemma: Conservative vs Liberal

Conservative
- RFC 4035, section 2.2:
  "There MUST be an RRSIG for each RRset using at least one DNSKEY of each algorithm in the zone apex DNSKEY RRset"
- Cache taken into consideration
- 5 steps:
  1. Add New RRSIGs
  2. Add New DNSKEY
  3. Change DS
  4. Remove Old DNSKEY
  5. Remove Old RRSIGS

Liberal
- RFC 6840, section 5.11
  "This requirement applies to servers, not validators. Validators SHOULD accept any single valid path."
- 3 steps (double-signing scheme)
  1. Add New DNSKEY/RRSIGs
  2. Change DS
  3. Remove Old DNSKEY/RRSIGs
Liberal ✓

- Much simpler process
Liberal ✓

- Much simpler process
- Only Unbound prior to 1.4.8 (Jan 2011) known to be too strict
- Tested rollover in both cases (ecdsa-l.br vs ecdsa-c.br)
  - Probes with RIPE Atlas
  - No significant measurement difference between both
  - 2 tests, one to decide method and one to fully test the provisioning system [1]
Algorithm Rollover

- RSASHA1
- KSK 1536bit
- ZSK 1280bit

- RSASHA1 and RSASHA1NSEC3
- CSK 1280bit
Algorithm Rollover

- RSASHA1
- KSK 1536bit
- ZSK 1280bit
- RSASHA1 and RSASHA1NSEC3
- CSK 1280bit

- ECDSA-P256-SHA256
- KSK
- ZSK
- ECDSA-P256-SHA256
- CSK
Execution
Preliminaries

- New KSK had to be created on HSM (Hardware Security Module)
  - HSM software update (support for ECDSA)
  - All 4 HSMs had to be synchronised
  - 2 different sites
- Reduce TTL to 3600 (1h) to speed up the process
  - CSK rollover concluded in 7 hours
CSK Rollover (*.br)

• 20/Aug/2018
  ○ 12:00 - New CSK added on all child zones
    ■ Double-signing
      (Wait 5 TTLs (5h) for new key to propagate)
  ○ 17:00 - DS changed on .br for all child zones
  ○ 19:00 - Old CSK removed from all child zones

(All times in UTC)
KSK and ZSK Rollover (.br)

- 20/Aug/2018
  ○ 12:00 - New KSK and ZSK added on .br
    ■ Double-signing
  ○ 17:00 - Request DS change at IANA
  ○ 22:00 - DS changed at IANA
  *(Wait for new DS to propagate)*
- 23/Aug/2018
  ○ 13:00 - Old KSK and ZSK removed from .br

(All times in UTC)
Results
Trustchain - CSK Rollover

Key added
DS changed
Key removed

[Graph showing percentage over time with Secure and Insecure markers]

- Secure
- Insecure
Algorithm Rollover

IN    DNSKEY

br.    21600 IN DNSKEY 257 3 5 AwEAAZvox2cw9B9DxfpSDg0uSDEXhutJxVfF79Gwb06VNBs1PaSi6qC 5UDG6GyGwv1LtNFi5rnazYps9aJNL2s5j13g7lKwZmncsXd0SWQIVp6 P7fc4ULGqRyzn0a4z678q69wYc/bYIo+dAjv/20/Cbk+syRmeRYwoNT Vyk03o6sKLRsj/b7QRLogxa8Psbg+wujFkkX0bSM7XqKhP4dsDDp9Pq meXL8097rxcLPV8h0bvdmcld Ap/r5I2w9rPbz0==

br.    21600 IN DNSKEY 256 3 5 AwEAAgdq9z+k2ZBZhy03laVDL+78dG5EMsE9PyAY0uy5wq27Y70NJBi zPexJSF5wtPa7gWgRYjEwFJ5xPx1adM+Z53jdum0hmW1WicZsYNQ3vJ IUpoKb l00GoPizfuBoHJFRGhv0HtBen0vzoQ5VllX6M+HrYLZXrEDXJq IIZnfj9503sXwL4zYjFmxe7Wi5ia8pGwyFGZD j0V76rnFknChem=

br.    21600 IN RRSIG DNSKEY 5 1 21600 20180903000000 20180812
000000 802 br. gnRbp06Uf1KewXffD7t7Umb4trmIslbRoKQst0tjxZx5TLapvU+ssaK 8A+ZasayomCh+scs DXFoHDpcyUut1WgL7fDWH6AE1uJ9f1ALDplGx64X 7km6ZoSyfoKMChwOGbhze/q+2BBOL7iyRuw462zZf57TaJBI 6UdbcQfBx jZ37Y9iF22TUyoXPxExtSr1+qiVoRrnX09CPJxEVRzfNu8d7MxdqJS qNvAuGSxyq7NMTv1RwdwXfAze5MADGVQ

; MSG SIZE rcvd: 638
Algorithm Rollover

ECDSA

289 bytes (55% less)
Response size - CDF

- ECDSA: 99% < 850 bytes
- RSA: 99% < 1200 bytes
- 65% < 512 bytes
- 42% < 512 bytes
Test Rollovers Raw Measurement Data

** ecdsa-c.br:
https://atlas.ripe.net/measurements/144609[94-97]/
** ecdsa-l.br:
https://atlas.ripe.net/measurements/144609[90-93]/

2018-07-11 – Second Liberal test
https://atlas.ripe.net/measurements/151011[60-63]/
https://atlas.ripe.net/measurements/151011[83-84]/
https://atlas.ripe.net/measurements/151011[88-89]/
https://atlas.ripe.net/measurements/151011[93-94]/
Rollover Raw Measurement Data

[2]
** br: 2018-08-20 - 2018-08-27
- trustchain
  https://atlas.ripe.net/measurements/157403[77-80]/
- propagation delay dnskey/ds/rrsig
  https://atlas.ripe.net/measurements/157403[81-86]/
  https://atlas.ripe.net/measurements/157626[29-34]/

** com.br: 2018-08-20 - 2018-08-21
https://atlas.ripe.net/measurements/157401[44-53]/
Questions?
Thank You

Cesar Kuroiwa / Hugo Kobayashi / Frederico Neves
<fneves@registro.br>