ALGORITHM ROLLOVER ON .BR

registro.br   nic.br   cgi.br

# Introduction

Introduction

- .br signed since 2007
- 128 child zones (com.br, net.br, org.br, …)
- RSA-SHA1
- 2 KSK rollovers (2010, 2015)
  - Key size increased (1536bit)

Motivation

- Improve security
  - 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
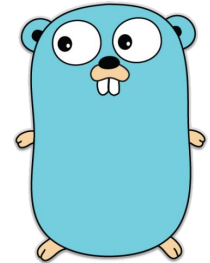
Dilemma: Conservative vs Liberal

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)
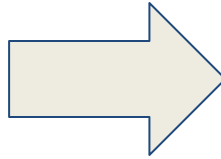 - Probes with RIPE Atlas
  - No significant change between both

Algorithm Rollover

- .br
  - RSASHA1
  - KSK 1536bit
  - ZSK 1280bit
- *.br
  - RSASHA1 and RSASHA1NSEC3
  - CSK 1280bit

  *CSK = Combined Signing Key

Algorithm Rollover

- .br
  - RSASHA1
  - KSK 1536bit
  - ZSK 1280bit
- *.br
  - RSASHA1 and RSASHA1NSEC3
  - CSK 1280bit

  *CSK = Combined Signing Key

- .br
  - ECDSA-P256-SHA256
  - KSK
  - ZSK
- *.br
  - ECDSA-P256-SHA256
  - CSK

registro.br nic.br cgi.br

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)
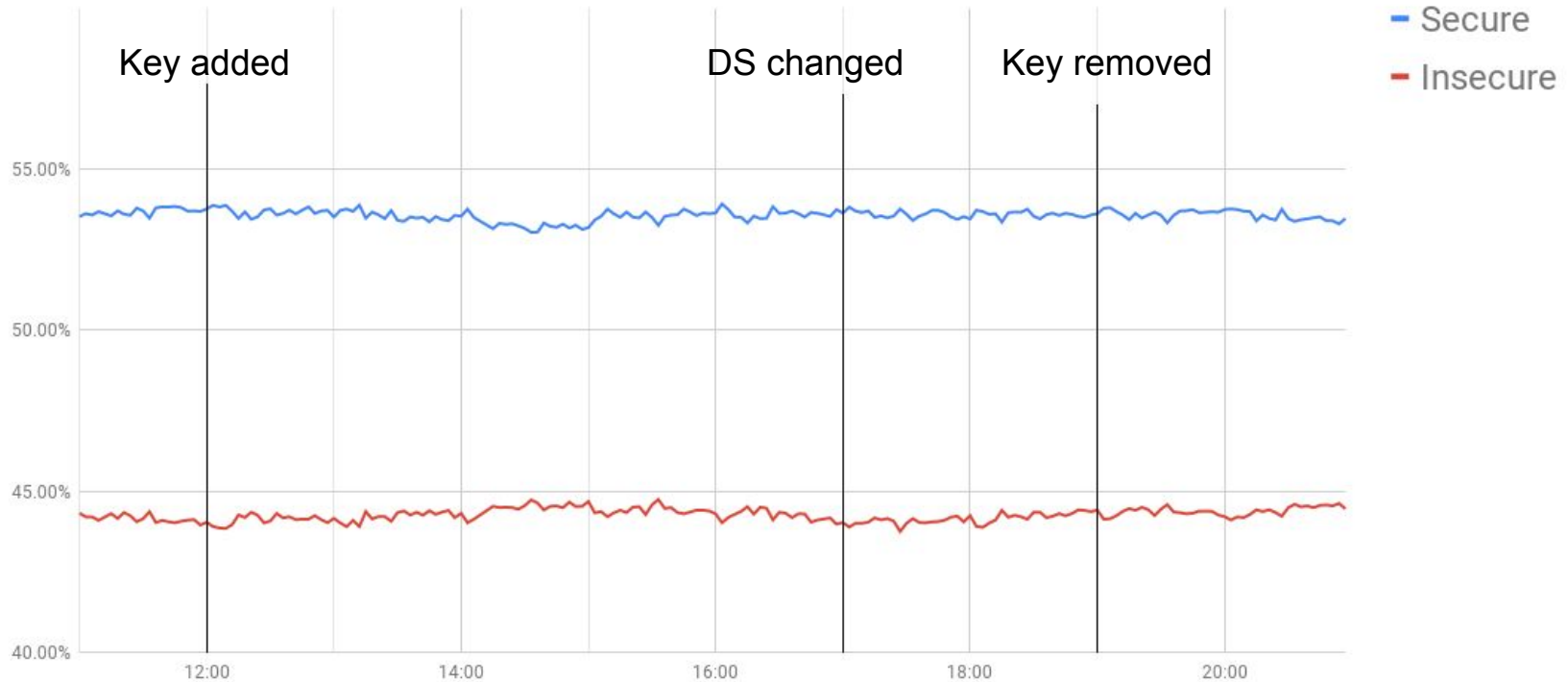
KSK and ZSK Rollover (.br)

- 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
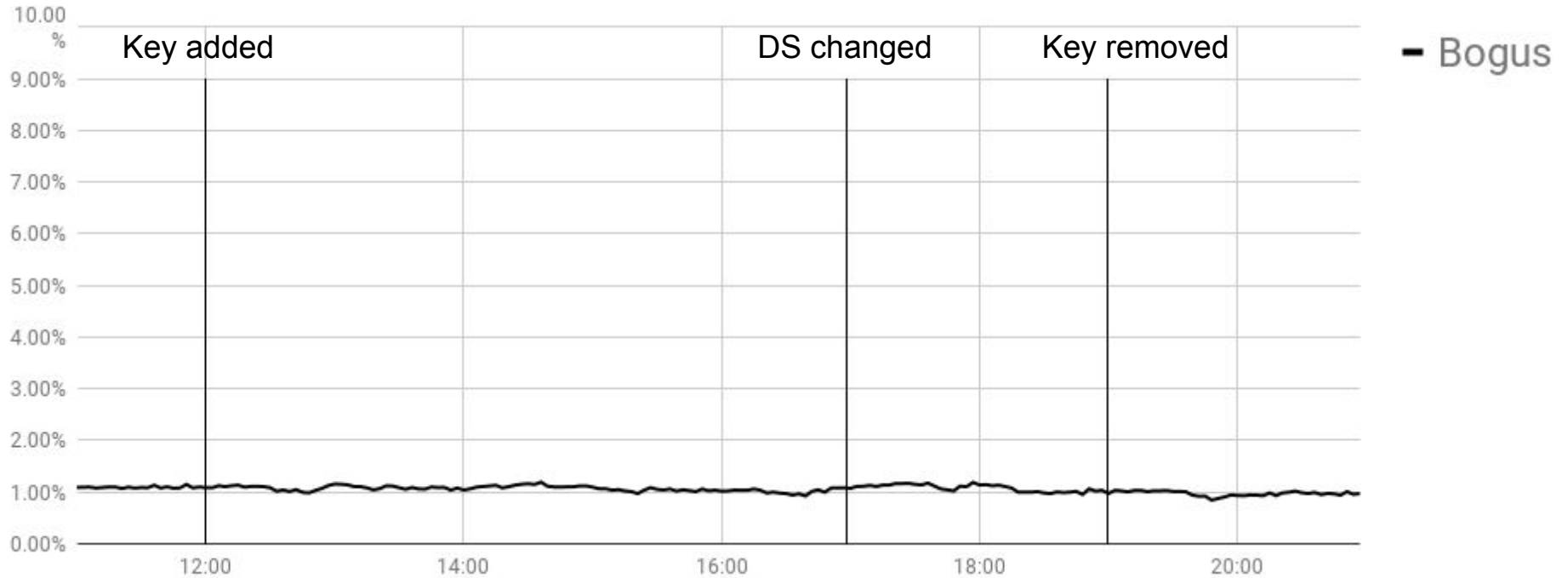 - 13:00 - Old KSK and ZSK removed from .br

(All times in UTC)

Results

Trustchain - CSK Rollover

Trustchain - CSK Rollover

Algorithm Rollover

RSA

```
;; QUESTION SECTION:
;br.                              IN       DNSKEY

;; ANSWER SECTION:
br.                    21600    IN       DNSKEY   257 3 5 AwEAAZvox2cw9B9DxfpSDgOuSDEXhutJ
xVfF79GwbO6VNBS1PaSio6qC 5UD6GyGwv1LtNFu5rnazYpS9aJNL2Sv5jl3gz7lKwZmncsXdOSWQIvP6 P7fc4U
LCgRyznOa4z678q69wYc/bYIio+dAjv/20/Cbk+syRmeRYwoNT VyfO3o6sKLrsj/b7QrLogxa8Psbg+wujFkkXO
bSM7XqKhP4dbsDDp9Pq meXL8097rxcLPV8hObvdmclDap/r5I2w9rPbzQ==
br.                    21600    IN       DNSKEY   256 3 5 AwEAAdzq9z+k2ZBZhyoO3laVDL+78dG5
EMsE9PyAYOuy5wq27Y7ONJBi zPexJSF5wtPa7gWgRYjEwFJ5xPxX1adM+Z53jdum0hmW1WicZsYNQ3vJ IUpoKb
l00GoPIzfuBoHJFRGhv0HtBen0vzoQ5VllX6M+HrYLZXrEDXJq IIZnf9J5O3sXwL4zYjfFmXe7Wi5Ia8pGwyFGZD
j0V76RnFknCheM=
br.                    21600    IN       RRSIG    DNSKEY 5 1 21600 20180903000000 20180812
000000 802 br. gNrbp06Uf1KewXXffD7t7Umb4trmIslbRoKQst0tjxZx5TLapvU+ssaK 8A+ZasayomCh+scs
DXFoHDpcyUut1WgL7fDWH6AEluJ9f1ALDplGx64X 7km6ZoSyfoKMChwOGbhze/q+2BBoL7iyRu462zZf57TaJBI
6UdbcQfBx jZ37Y9iF22TUYoXPxExtSr1+qiVoRrnXOr9CPJxEVRzfNu8d7MxkdqJS qNvAuGSxyq7NMTv1RwdwX
fAze5MADGVQ
;;
;; MSG SIZE  rcvd: 638
```

← 638 bytes

registro.br nic.br cgi.br

Algorithm Rollover

ECDSA

```
;; QUESTION SECTION:
;br.                                    IN        DNSKEY

;; ANSWER SECTION:
br.                     21600    IN        DNSKEY   256 3 13 lBbAHerLHCrYMnwHKdu0tnDOQx
T/Ppdzx5/iG/miOny2CWcf5LrtvU+y wRk+nKCSnzqczygJ3cFOzy+L1ZISzg==
br.                     21600    IN        DNSKEY   257 3 13 i9GgZ+/z2Y7VbG3AHrh7KD7FUH
GxmCKHfoVGv/zZ3DAcXTVnAywWTopC BxqZas4JkzaPdAGd0rVtRsKGRDhiFg==
br.                     21600    IN        RRSIG    DNSKEY 13 1 21600 20180909120000 20
180819120000 2471 br. Vesqhwm2LrGYmYoA+pSXBqnY3QVfkUVvU9ByH8segMvT/DSACQVBUwFx xTJl
Z5py8UGNJtaPmY+AcHu+epWuyg==
;; MSG SIZE  rcvd: 289
```
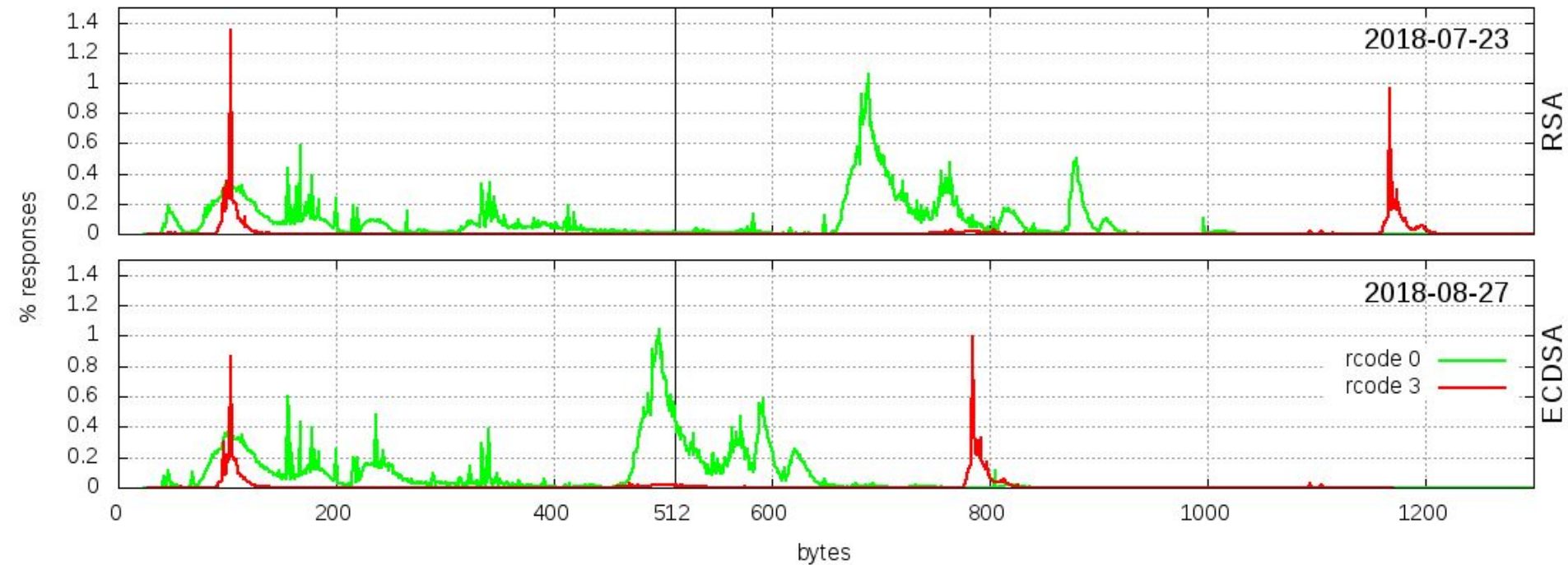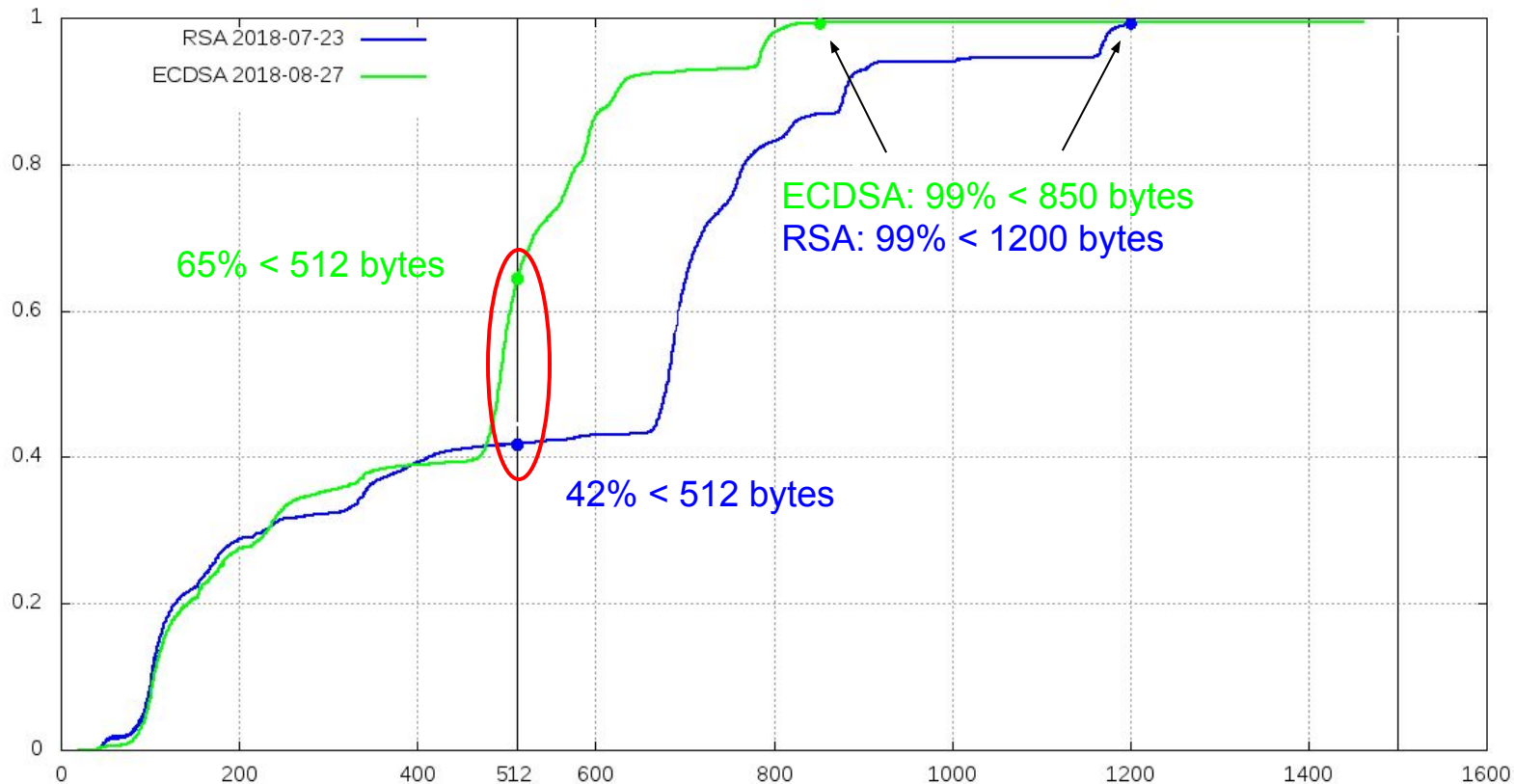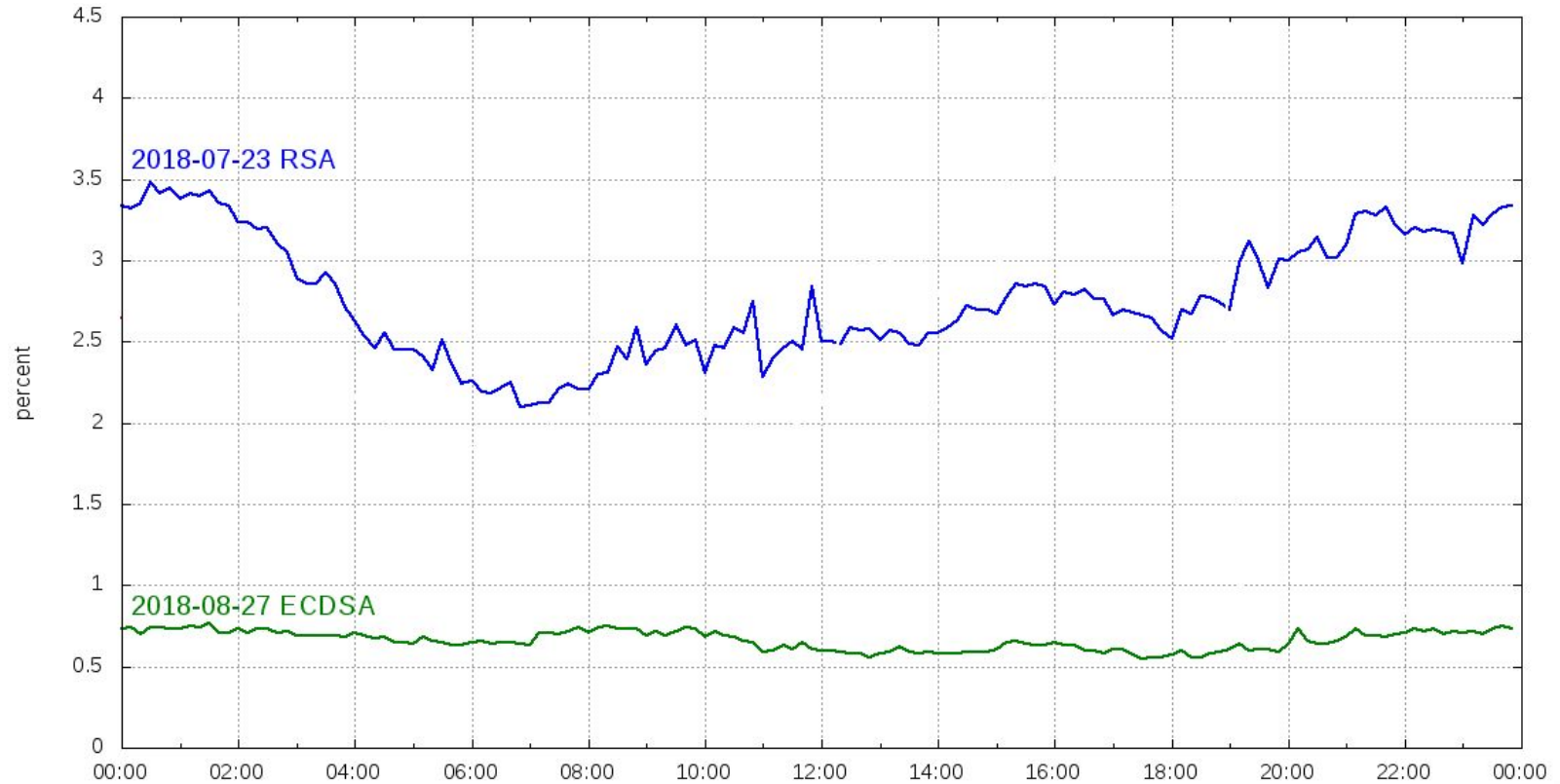
← 289 bytes (55% less)

Response size

Response size - CDF (cumulative distribution function)

TCP query %

Thank You

Cesar Kuroiwa
cesar@nic.br

registro.br nic.br cgi.br