

DNSSEC at .br update Perspectives on a Signed Root

LACNIC XIII - 19/05/2010 - Curaçao

Frederico A C Neves <fneves@registro.br>

Who we are?

- . Not for Profit executive arm of the .BR Internet Steering committee
 - . Internet Infrastructure Provider
 - . Registry for .br
 - . NIR for Brazil (~650 ASN)
 - . IX promoter and operator at 12 major cities
 - . Brazilian CERT (CERT.br)
 - . ICT statistics provider (5 year series)
 - . Internet quality measurement program
- . 2.1 million domain names
- . 66 second level zones
- . <http://nic.br/>

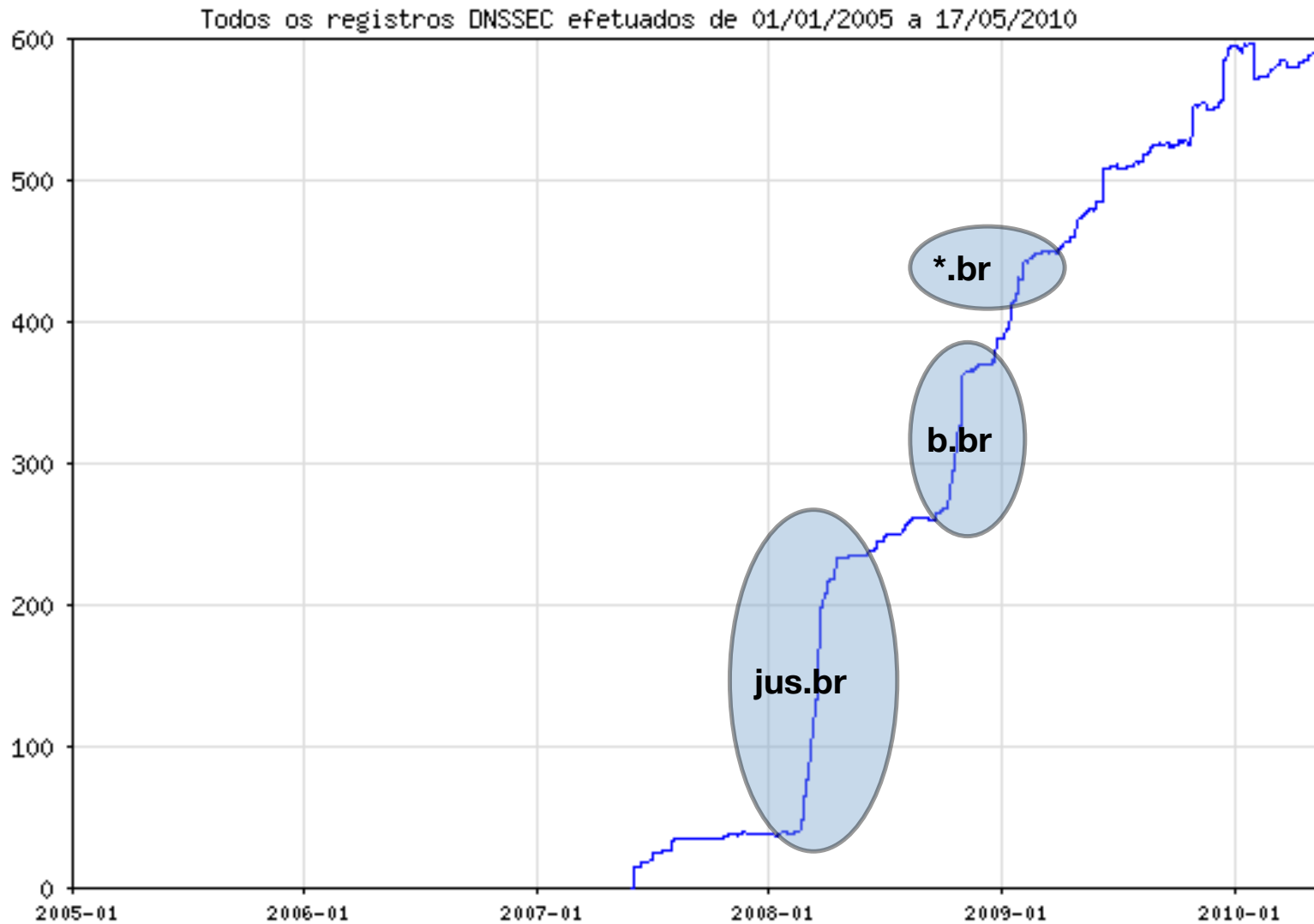
DNSSEC history at .br

- . Started with firm plans Dec/2006
- . Initial deployment 4/6/2007
 - . 5 small zones
 - . .br .blog.br .eng.br .eti.br .gov.br
- . DS collection since day one
 - . All registry interfaces
 - . WEB interface
 - . EPP (RFC4310)
- . Finished initial deployment 15/1/2009
 - . Signature with NSEC3 (RFC5155)
 - . 3 Large zones .org.br .net.br .com.br

Deployment Strategy

- Deploy DNSSEC as mandatory to new chartered SLD for high value domains
 - No functioning DS means no delegations
 - First one for the Judiciary Power (JUS.BR)
 - oct/2007
 - Second one for Banks (B.BR)
 - sep/2008
- Provided for Hosting Provider automation tools (<http://registro.br/dnsshim/>)
- Training
- Continue outreach to ISPs and Hosting Providers

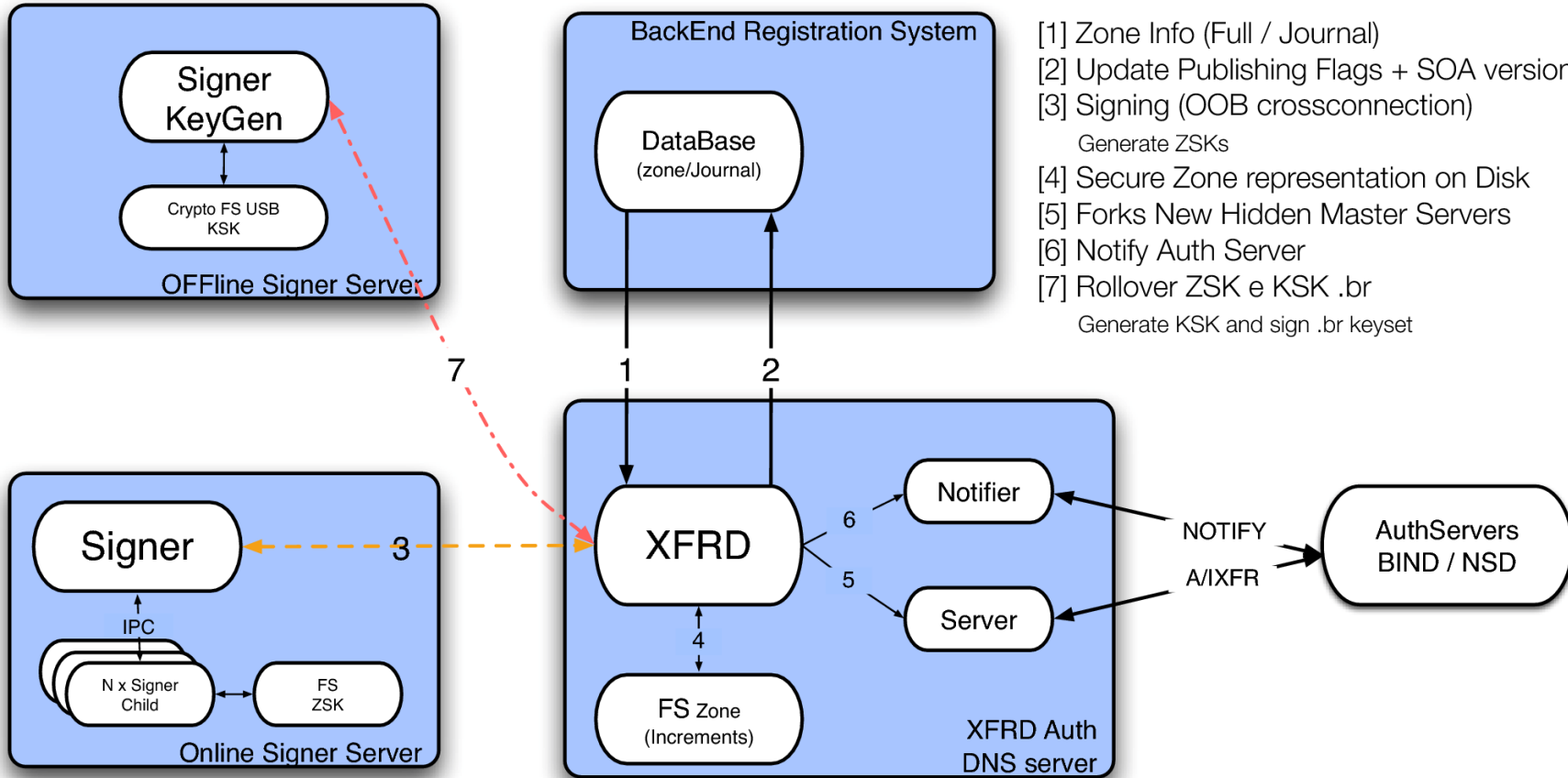
Growth - <http://registro.br/stat/dnssec.html>



Deficiências – XFRD 3.x

- Poor hardware and data redundancy
- Poor protection for the keys stored in online signer
- Manual rollovers
- Manipulation of KSK BR in offline signer

XFRD 3.x



DNSSEC Updates Keys Policy

- <http://registro.br/info/dnssec-policy.html>
- **KSK BR**
 - RSASHA1 1280 bits
 - Double-signing rollover: every 2 to 5 years (change)
 - Third week of May
- **ZSK BR**
 - RSASHA1 1152 bits
 - Pre-publishing rollover: every 3 months
 - First week of Feb/May/Aug/Nov
- **ZSK *.BR**
 - RSASHA1 1024 bits
 - Pre-publishing rollover: monthly
 - Second week of the month

Improvements – XFRD 4.x

- Redundancy (Backup site)
- Keys protection in online signer
- HSM – Hardware Security Module
- Automated Rollovers
- Pre-publishing zone validation

Redundancy

- Backup site
 - Production hardware, software and configuration
 - setup duplicated at backup site
- Online synchronization
 - IPsec tunnel keeps both sites securely connected
 - Rsync takes care of data replication

New Online Signer

- . ZSKs encrypted on disk
 - . PKCS#12
 - . AES-256
- . Smart Card Protection
 - . 2:8 scheme (Shamir Secret Sharing Scheme)
 - . Smart Cards necessary for Signer activation
(Decryption of ZSKs)

HSM – Hardware Security Module

- Cryptographic Hardware
- Substitutes the offline signer
- Responsible for manipulating the KSK BR
- Protected by Smart Cards (SSSS)
- Groups: Administrators, Auditors and Operators
- Manipulated only during ceremonies (2x/year)

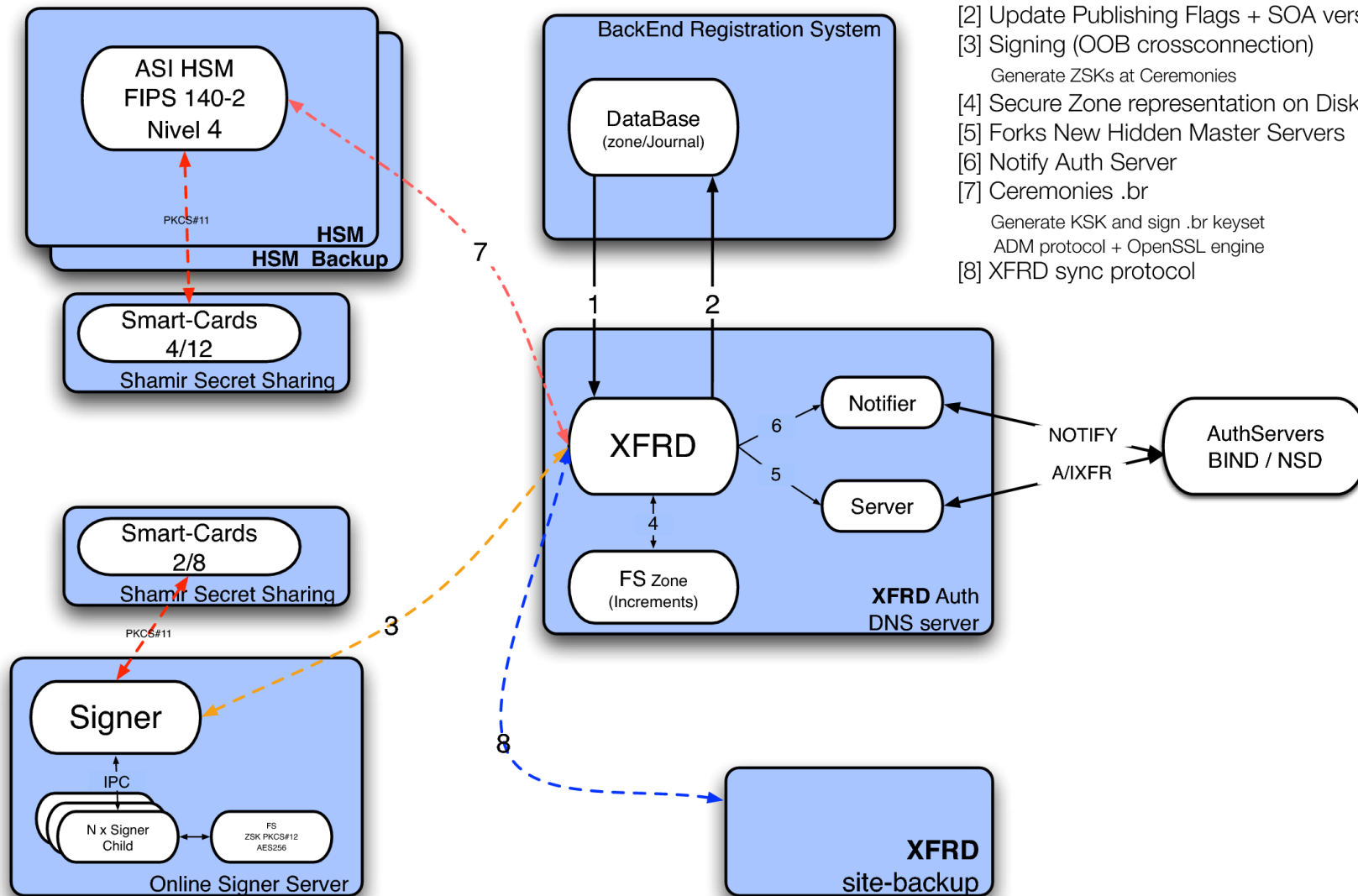
Automated Rollovers

- DNSKEY changes
- Biannual ceremonies
- Keys generation for a period of six months
- KSK BR signatures generation (HSM)
- Remote monitoring of key rollovers

Pre-publishing zone validation

- DNSSEC chain of trust validation
- Consistency of NSEC/NSEC3 records
- As usual default policy apply – Abort and notify on any inconsistency at publication time

XFRD 4.x



- [1] Zone Info (Full / Journal)
- [2] Update Publishing Flags + SOA version
- [3] Signing (OOB crossconnection)
Generate ZSKs at Ceremonies
- [4] Secure Zone representation on Disk
- [5] Forks New Hidden Master Servers
- [6] Notify Auth Server
- [7] Ceremonies .br
Generate KSK and sign .br keyset
ADM protocol + OpenSSL engine
- [8] XFRD sync protocol

Ceremony of 13/05/2010

- 1.HSM Activation
- 2.Ceremony 2010 – 01 (NIC.br)
- 3.Ceremony 2010 – 02 (Oi – Backup site)

First results will be observed on:
24/05/2010 ZSK .br rollover start
31/05/2010 KSK .br rollover start

Perspectives on a Signed Root

- Much easier deployment for TLDs
 - No need to care for Trust Anchor Distribution and the related rollover problems
 - It's simply a record update at IANA
- Much easier deployment for ISPs
 - A single TA to configure
 - No need for iTAR/DLV
 - Automatic rollover using 5011 enabled software
- More signed content available incentive more ISPs to start validating
- Secure DNS data means secure key distribution for the masses and a fertile environment for security innovation

Questions / Comments

Thanks