.BO DNSSEC Deployment

Agenda

1. About ccTLD .bo
2. DNSSEC
3. Initial plan to deploying
4. Development
5. Plan adjustments
6. Conclusions

About ccTLD .bo

- The Agency for the Development of the Society of the Information in Bolivia is the entity that manages the ccTLD .bo, ADSIB is the registry and its registrar.

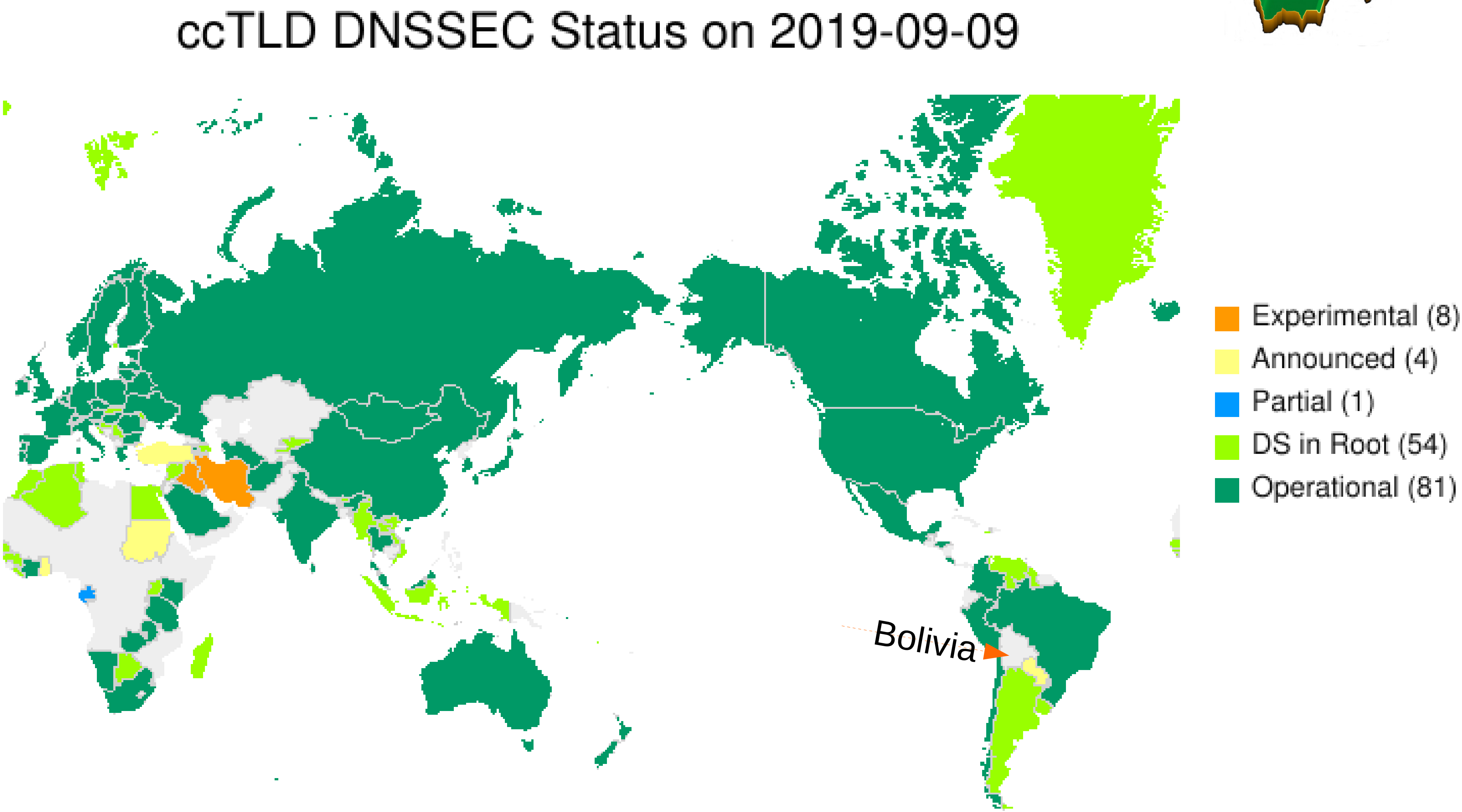
adsib
agencia para el desarrollo de la
sociedad de la información en Bolivia

- ADSIB is an governmental entity that depends of the Vice Presidency of the Plurinational State of Bolivia.

More about ccTLD .bo

- To may 2020 it has more than 13.800 domain names registered and actives.
- 62% of the domain names are third level and 26% second level domains.
- ADSIB decided to deploy DNSSEC and invited different entities that provide digital services, its objective is to decreases the vulnerability to attacks to the domain names .bo.

DNSSEC



ccTLD DNSSEC Status on 2019-09-09

https://www.internetsociety.org/deploy360/dnssec/maps/

DNSSEC

- “DNSSEC is a set of extension to the DNS, and it does not fundamentally change the DNS. A zone administrator adds digital signatures to the contents of a zone file by adding additional information into the zone through the use of DNSSEC-related Resource Record types (RRTypes).”

- “The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) cryptographic authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.”

Initial plan to deploying

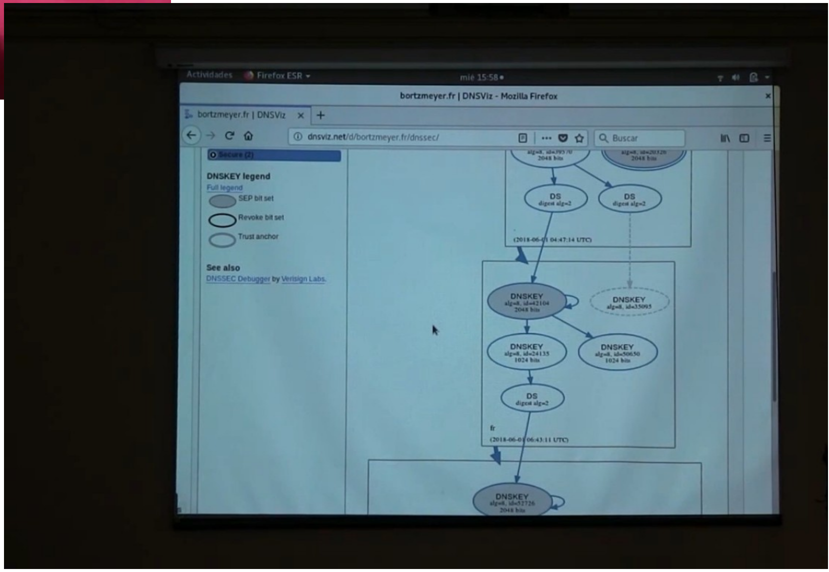
- Training DNSSEC
  - Internal ADSIB (2018)
  - Other entities (2019)
  - Monitoring – new entities (2020 - ...)
- Experimental environment and operation
  - Internal test (2018)
  - Register dnssec.bo and test (January 2019)
  - Test with users (July 2019 - ...)
- Documentation (October 2019)
  - Policy, Practice Statement and Procedures
- Deploy
  - Key generation and zone signing .BO   (November 2019)
  - Publish DS record DNS ROOT (December 2019)
  - Recive DS records from registrants (December 2019 - ...)
- Evaluation and monitoring DNSSEC (December 2019 - ...)

4. Development

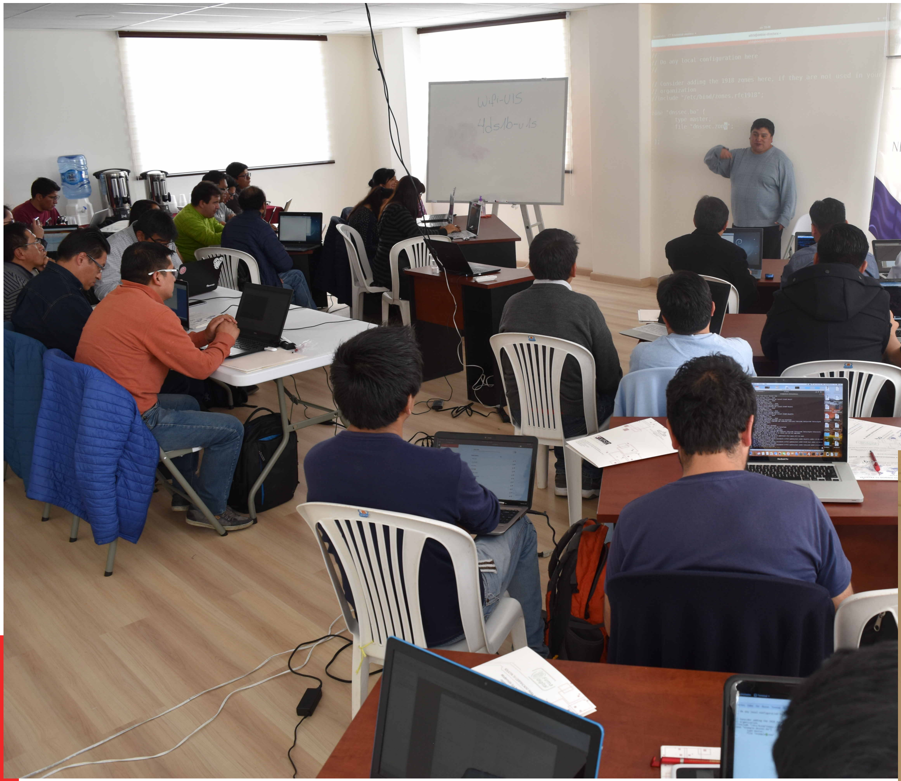
Trainning

ADSIB staff and public entities staff

Stéphane Bortzmeyer
AFNIC
Octubre 2018



Trainning



Jose Machicado
ADSIB
May and July 2019

Entities involucred

Vicepresidencia del Estado
Presidencia de la Asamblea Legislativa Plurinaci
BOLIVIA

fndr
Fondo Nacional de Desarrollo Regional

BANCO CENTRAL DE BOLIVIA

ASP-B
ADMINISTRACIÓN DE SERVICIOS PORTUARIOS - BOLIVIA

Aduana Nacional

SENASAG
BOLIVIA
Servicio Nacional de Sanidad Agropecuaria e Inocuidad Alimentaria

AGETIC
agencia de gobierno electrónico y tecnologías de información y comunicación

entel
Líder en telecomunicaciones

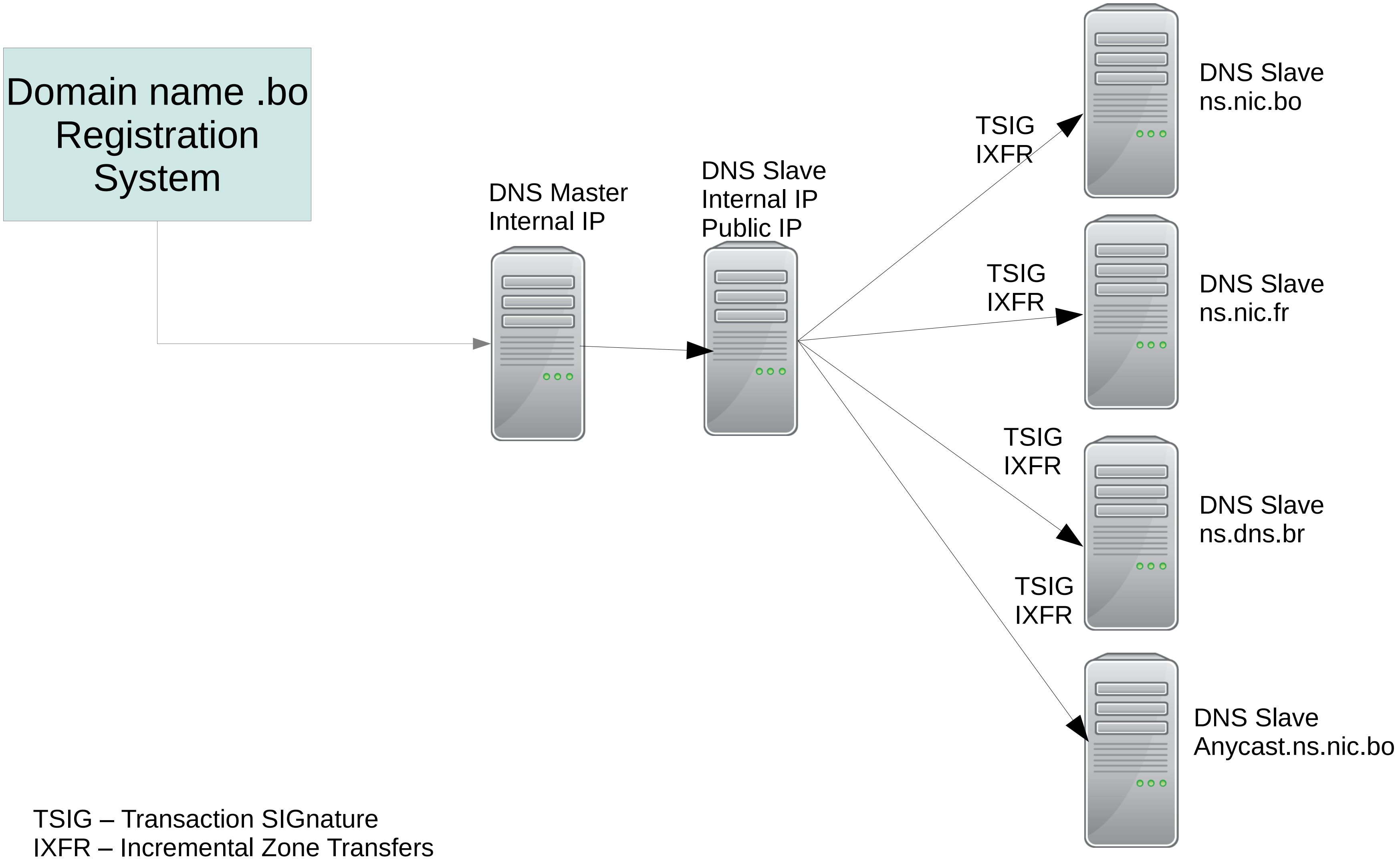
ATT
AUTORIDAD DE REGULACIÓN Y FISCALIZACIÓN DE TELECOMUNICACIONES Y TRANSPORTES

Contraloría General del Estado
BOLIVIA

Obras
MINISTERIO DE OBRAS PÚBLICAS, SERVIC

Datacom

Infraestructure DNS



Domain name .bo Registration System

DNS Master
Internal IP

DNS Slave
Internal IP
Public IP

TSIG
IXFR

DNS Slave
ns.nic.bo

TSIG
IXFR

DNS Slave
ns.nic.fr

TSIG
IXFR

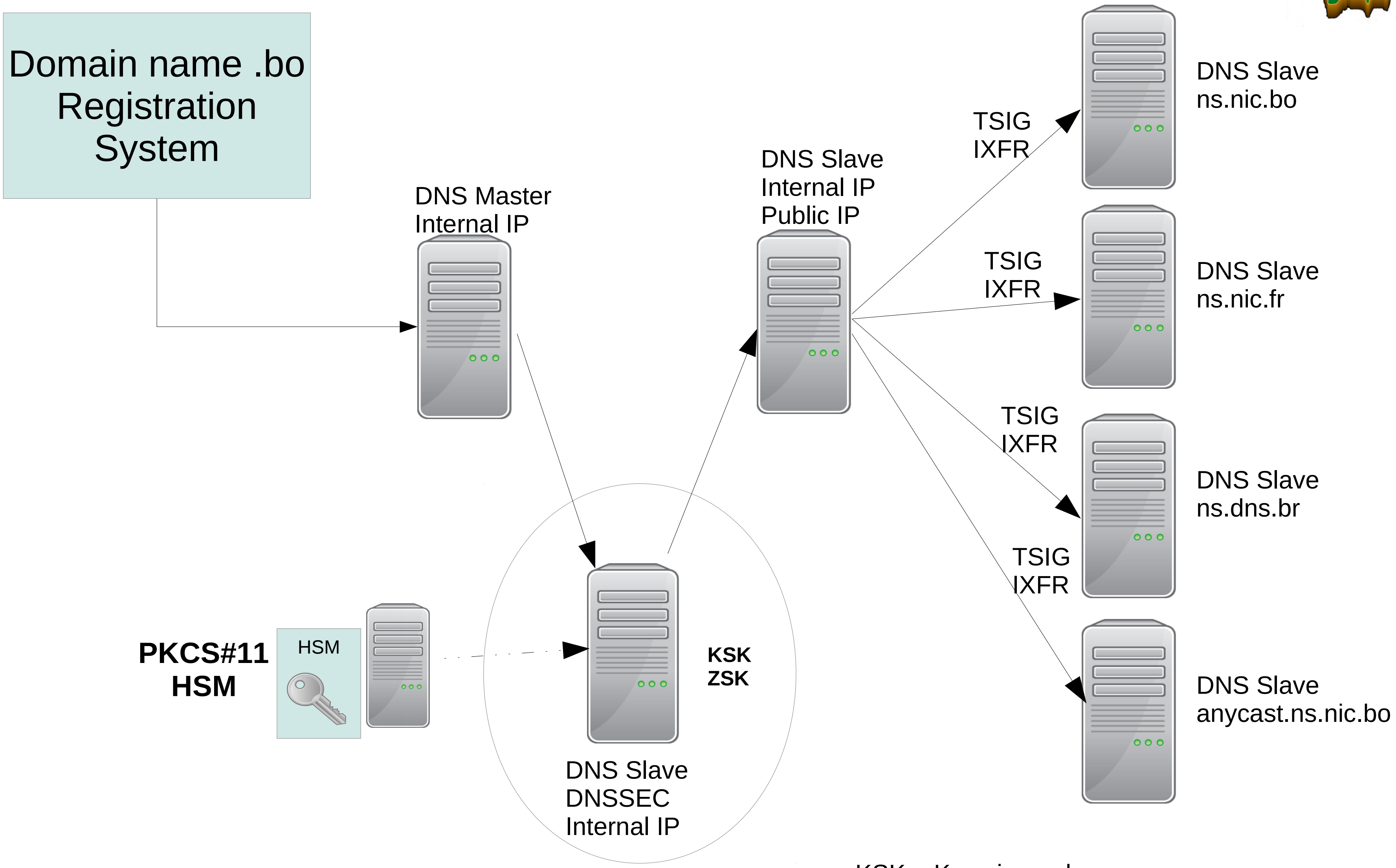
DNS Slave
ns.dns.br

TSIG
IXFR

DNS Slave
Anycast.ns.nic.bo

TSIG – Transaction SIGnature
IXFR – Incremental Zone Transfers

Infraestructure DNSSEC



Domain name .bo Registration System

DNS Master
Internal IP

DNS Slave
Internal IP
Public IP

TSIG
IXFR

DNS Slave
ns.nic.bo

TSIG
IXFR

DNS Slave
ns.nic.fr

TSIG
IXFR

DNS Slave
ns.dns.br

TSIG
IXFR

DNS Slave
anycast.ns.nic.bo

PKCS#11
HSM

HSM

KSK
ZSK

DNS Slave
DNSSEC
Internal IP

TSIG – Transaction SIGnature
IXFR – Incremental Zone Transfers

KSK – Key signng key
ZSK – Zone signing key

Keys

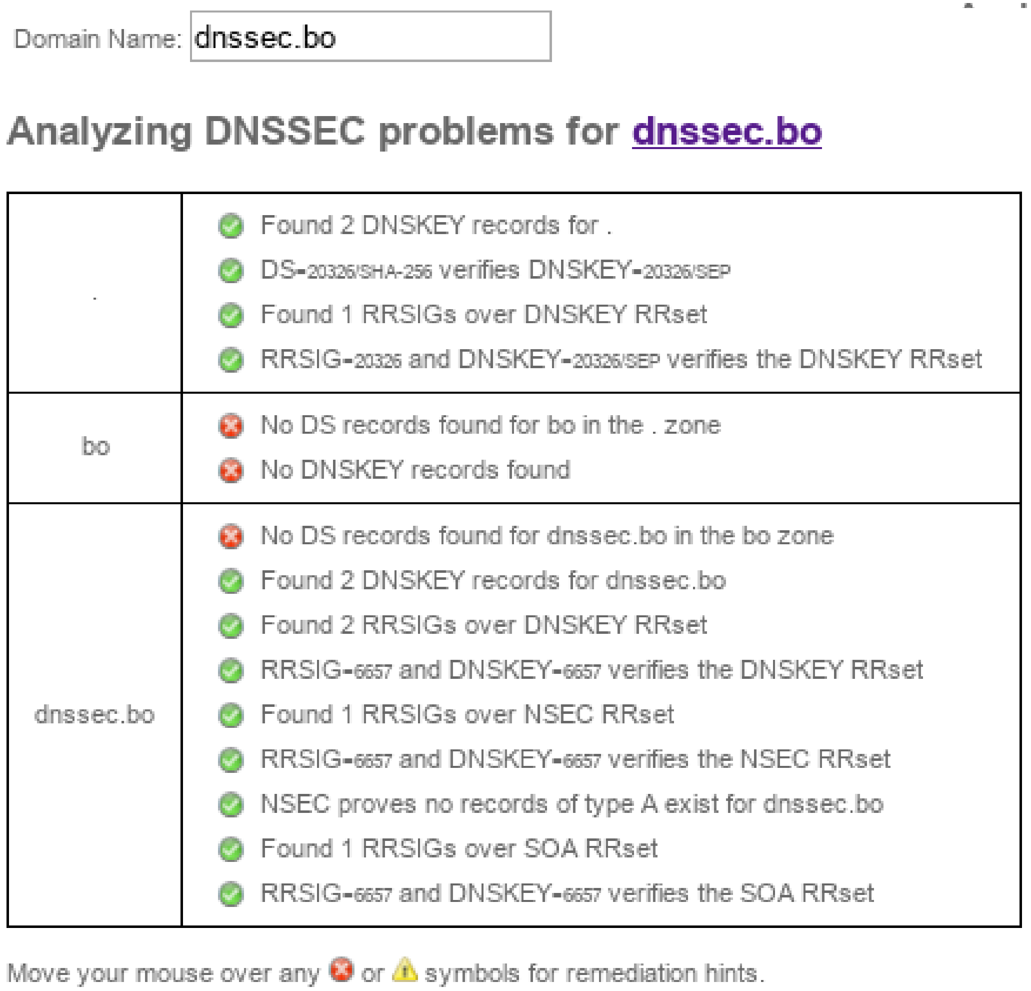
KSK (Key Signing Key):

- Key size: 2048
- Key rollover: 2 years
- Scheme of rollover: Pre-publish key
- Key Algorithm: RSA/SHA256

ZSK (Zone Signing Key):

- Key size: 1024
- Key rollover: 3 months
- Scheme of rollover: Double signature
- Key Algorithm: RSA/SHA256

Test zone

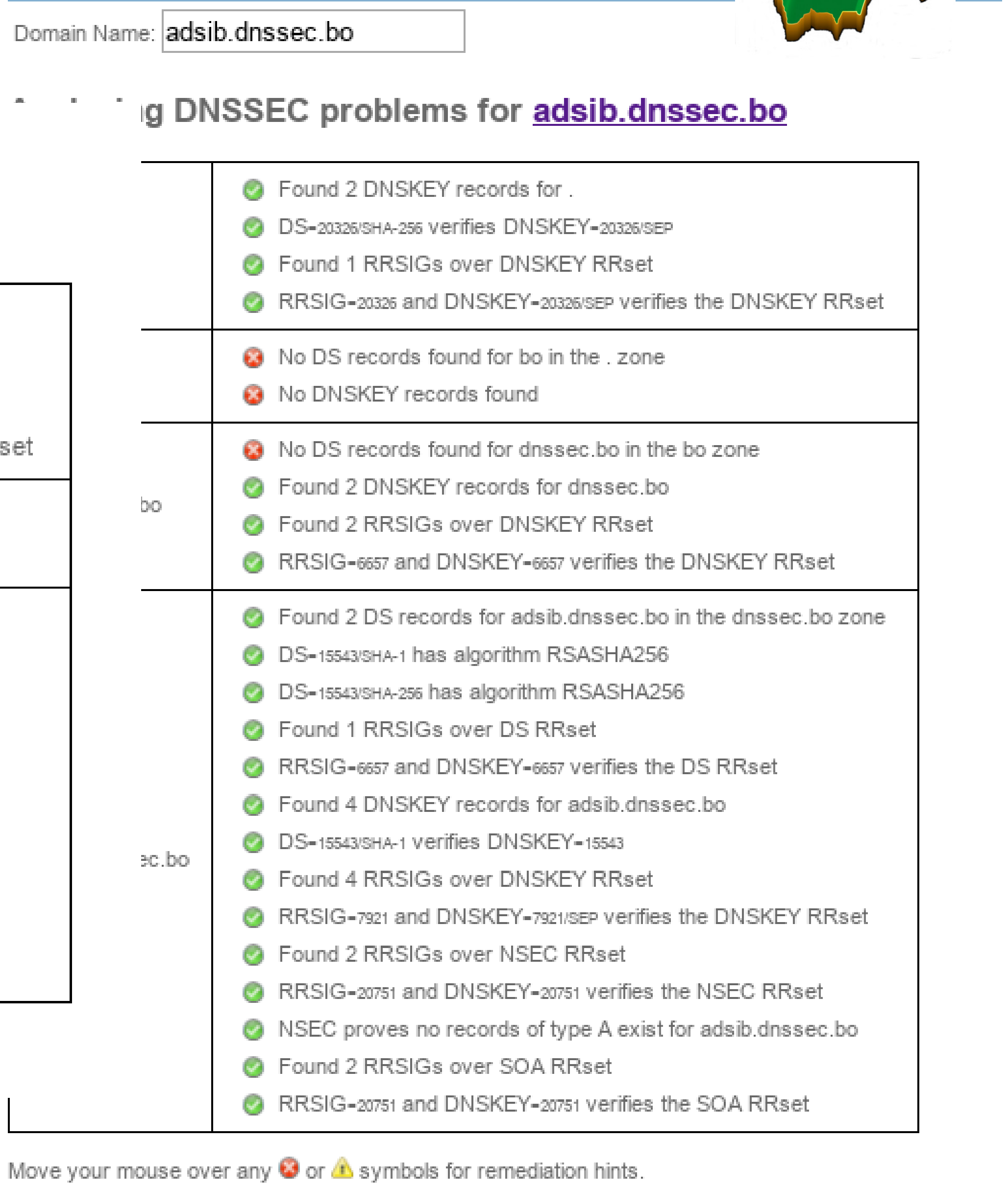


Domain Name: dnssec.bo

Analyzing DNSSEC problems for dnssec.bo

.	✓ Found 2 DNSKEY records for . ✓ DS-20326/SHA-256 verifies DNSKEY-20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG-20326 and DNSKEY-20326/SEP verifies the DNSKEY RRset
bo	✗ No DS records found for bo in the . zone ✗ No DNSKEY records found
dnssec.bo	✗ No DS records found for dnssec.bo in the bo zone ✓ Found 2 DNSKEY records for dnssec.bo ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the DNSKEY RRset ✓ Found 1 RRSIGs over NSEC RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the NSEC RRset ✓ NSEC proves no records of type A exist for dnssec.bo ✓ Found 1 RRSIGs over SOA RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the SOA RRset

Move your mouse over any ✗ or ⚠ symbols for remediation hints.



Domain Name: adsib.dnssec.bo

g DNSSEC problems for adsib.dnssec.bo

	✓ Found 2 DNSKEY records for . ✓ DS-20326/SHA-256 verifies DNSKEY-20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG-20326 and DNSKEY-20326/SEP verifies the DNSKEY RRset
	✗ No DS records found for bo in the . zone ✗ No DNSKEY records found
bo	✗ No DS records found for dnssec.bo in the bo zone ✓ Found 2 DNSKEY records for dnssec.bo ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the DNSKEY RRset
ec.bo	✓ Found 2 DS records for adsib.dnssec.bo in the dnssec.bo zone ✓ DS-15543/SHA-1 has algorithm RSASHA256 ✓ DS-15543/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG-6657 and DNSKEY-6657 verifies the DS RRset ✓ Found 4 DNSKEY records for adsib.dnssec.bo ✓ DS-15543/SHA-1 verifies DNSKEY-15543 ✓ Found 4 RRSIGs over DNSKEY RRset ✓ RRSIG-7921 and DNSKEY-7921/SEP verifies the DNSKEY RRset ✓ Found 2 RRSIGs over NSEC RRset ✓ RRSIG-20751 and DNSKEY-20751 verifies the NSEC RRset ✓ NSEC proves no records of type A exist for adsib.dnssec.bo ✓ Found 2 RRSIGs over SOA RRset ✓ RRSIG-20751 and DNSKEY-20751 verifies the SOA RRset

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Plan adjustments

- Training
  - Internal ADSIB DNSSEC (2018)
  - Other entities DNSSEC (2019)
  - Monitoring – new entities (2020 - ...)
- Experimental environment and operation
  - Internal test (2018)
  - Register dnssec.bo and test. (January 2019)
  - Test with users (July 2019 - ...)
- Documentation (October 2019)
  - Policy , Practice Statement and Procedures
- Deploy
  - Key generation and zone signing .BO
  - Publish DS record DNS ROOT
  - Receive DS records from registrants
- Evaluation and monitoring DNSSEC

Conclusions

- Measure forces prior to planning and defining how the DNSSEC deployment will be carried out helps to involucrate more people.
- Training and peer support is vital to reduce deployment time.
- It is crucial to have the support of the executives so that the technical part can carry out the deployment.
- Documentation of all processes is required to reduce risks.
- Defining roles and responsibilities can help that the rollover keys be carried out properly.
- After the deployment, the work has just begun.

Thanks

Jannett Ibañez Flores

jannettibanez@gmail.com
@Ibaezjannett