NIC ARGENTINA

ICANN

ICANN | 53

Buenos Aires

21-25 JUNE 2015

DNSSEC Workshop – ICANN 53 Buenos Aires

Luciano Minuchin – CIO

Nabil Saez de Arnedillo – Chief Technology

NIC.AR

A litle of History

DNSSEC - NIC ARGENTINA

- November 2013 – After ICANN 48 in Buenos Aires, we decided to implement DNSSEC. At that time, other priorities prevented us from moving ahead with the project.
- December 2014 – DNSSEC is established as a priority project for NIC.AR with a deployment due date of ICANN 53 in Buenos Aires.
- January 2015 – Servers were updated to support DNSSEC.
- Definitions of times, keys, architecture, equipment and algorithms.
- February 2015 - Creation of the DPS document
- March 2015 - ceremonies, failures, settings
- April 2015 - more ceremonies, more failures, more settings.
- May 2015 - New definition of dates, sizes, keys, architecture, equipment, algorithms.
- Ceremonies, ceremonies, ceremonies!!!
- June 8, 2015 - First Offline Keys Ceremony Generation
- June 18, 2015 - IANA approved the DS. Go-live!!!

Times

DNSSEC - NIC ARGENTINA

- Overall project time spent with part-time dedication: 5 months

- Overall project time spent with full dedication: 2 months

Technology

DNSSEC - NIC ARGENTINA

- **Offline Key Generation**
  - TPM technology
  - RSA256 algorithm
  - KSK 4096 BITS
  - ZSK 2048 BITS
  - RAM storage for action (TMFS)
  - Hard Disk Encryption
  - Copy of files from RAM to Pendrives with PGP

- **Automated signed zones.**
  - Dedicated and redundant equipment.
  - BIND 9.9.7
  - NSEC 3 OPT-OUT
  - Transfer to other servers with TSIG

Key Admin

DNSSEC - NIC ARGENTINA

ZSK signed with KSK

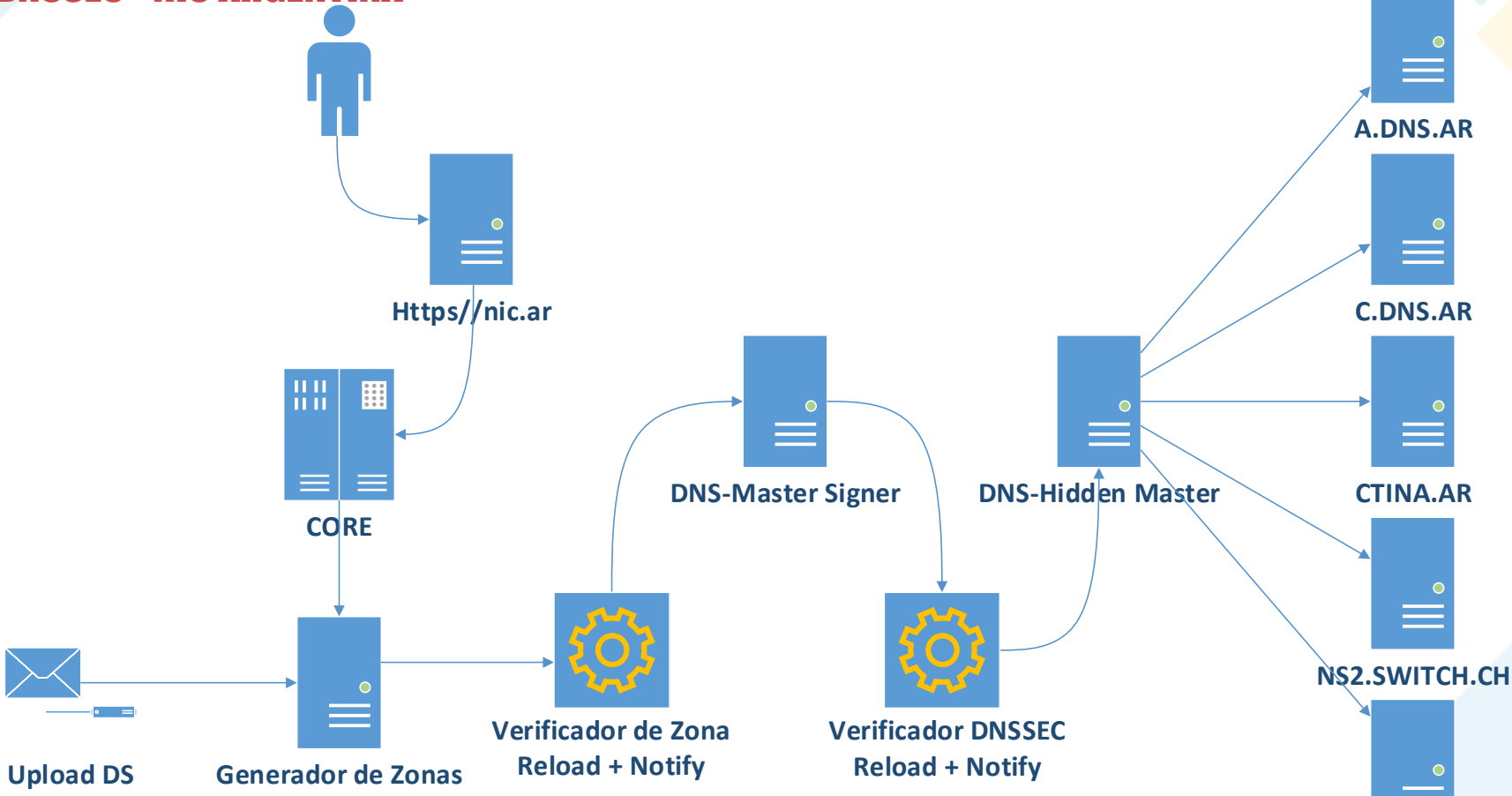
- Offline equipment ceremony
- Generation of KSK and ZSK
- AR Zone signed DNSKEY and RRsets generation
- KSK full offline archiving

Zone signed ZSK

- ZSK in Online computer with RRsets. Only operational keys
- Validation. Reload and Notify master zone DNS server
- Master to Slave transfer with TSIG

Architecture

DNSSEC - NIC ARGENTINA



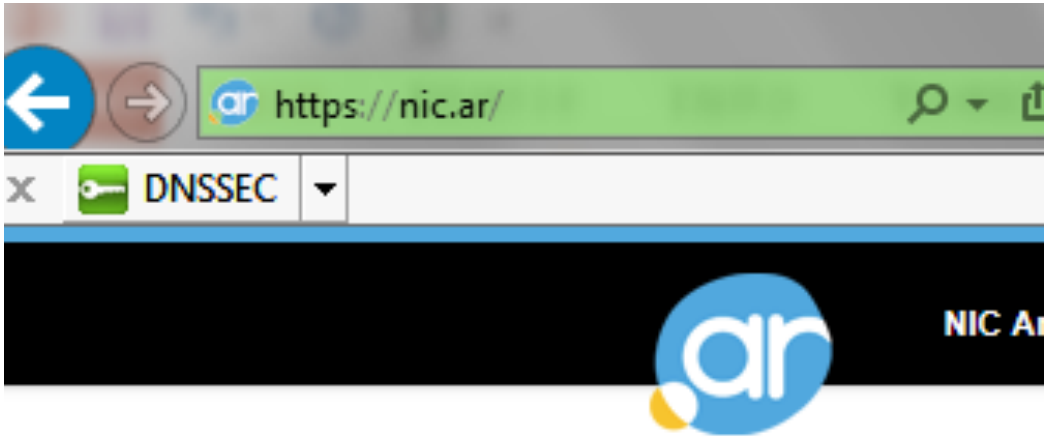
ICANN | 53
Buenos Aires
21-25 JUNE 2015

Physical KEY Security

DNSSEC - NIC ARGENTINA

- Pen Drives duplicated and encrypted with PGP
- Security bag with bank specifications
- Safe with double door and double security system
- Double closed circuit video
- Three access control with magnetic doors
- Federal police in access control and cameras

Mission Accomplished



ICANN | 53
Buenos Aires
21-25 JUNE 2015

New Challenges

- DNSSEC for government entities
- DNSSEC for financial institutions and transactional WEBs
- DNSSEC for small and medium ISPs
- Key monitoring tool
- New zones signature
- HSM Implementation???

Luciano Minuchin – minuchinl@nic.gob.ar

Nabil Saez – saezn@nic.gob.ar

MUCHAS GRACIAS

ICANN | 53
Buenos Aires
21-25 JUNE 2015