DNSSEC Implementation at .CR

ccNSO TechDay

Luis Espinoza S.

CTO – NIC Costa Rica

NIC-Internet Costa Rica

Academia Nacional de Ciencias

Agenda

- Introduction
- Planning
- Research and development
- Implementation
- The results.

Introduction

- Evil things come up to DNS:
  - Man in the middle attacks (cache poisoning).
  - Virus (Conficker).
  - Provide: Identity theft (phishing)
  - Results: Bank fraud or worst!

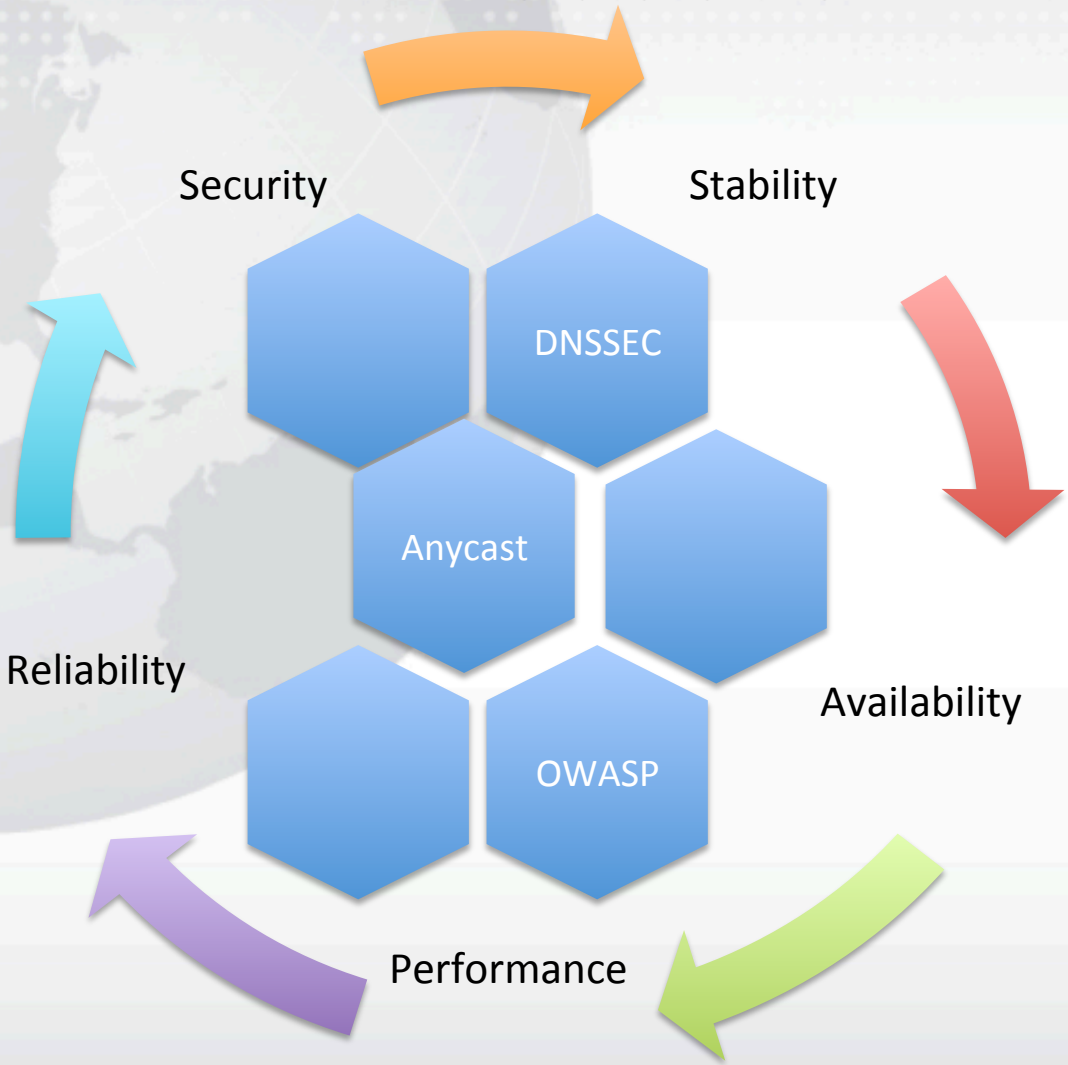
Introduction

Evil Things in DNS

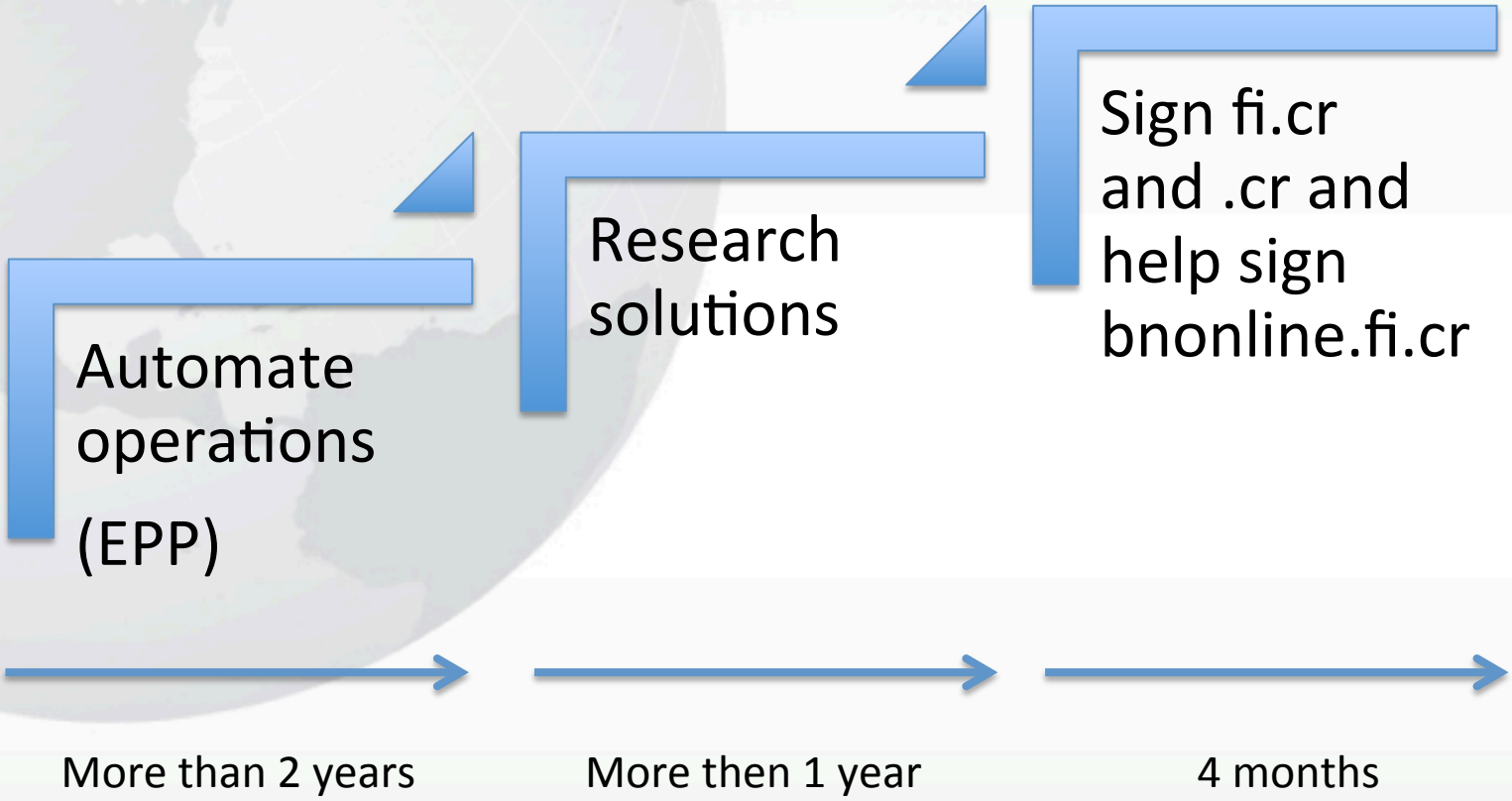
Impersonation

Fraud

Introduction

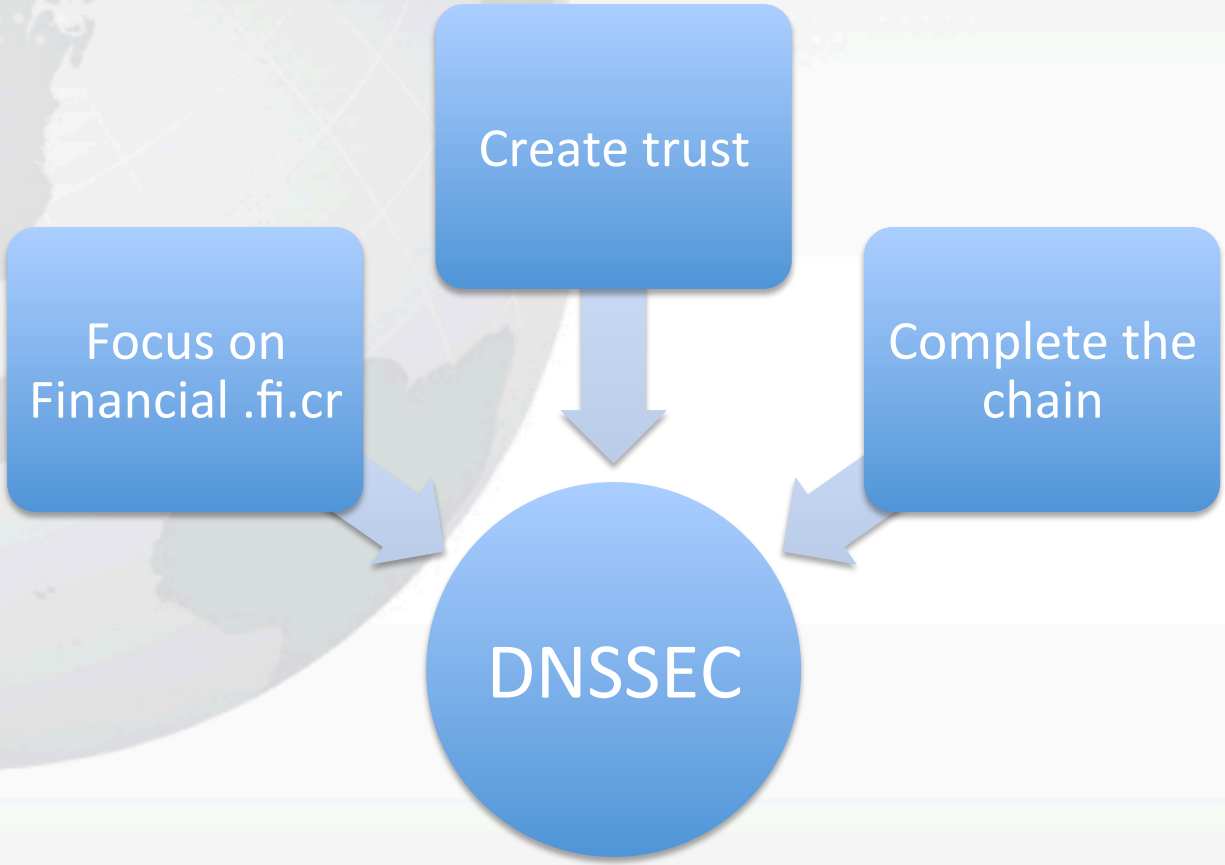


Planning DNSSEC Deploy



NIC-Internet Costa Rica
Academia Nacional de Ciencias

Implementation



Implementation details

- Look for an important Bank under .fi.cr to present a pilot project – Banco Nacional de Costa Rica.
- Implement DNSSEC for .fi.cr and chain with .cr, then chain with root-servers.
- Use hardware based solution (new low cost solution based on TPM).
- DNSSEC Policy Statement

Goals Achieved

DNSSEC awareness

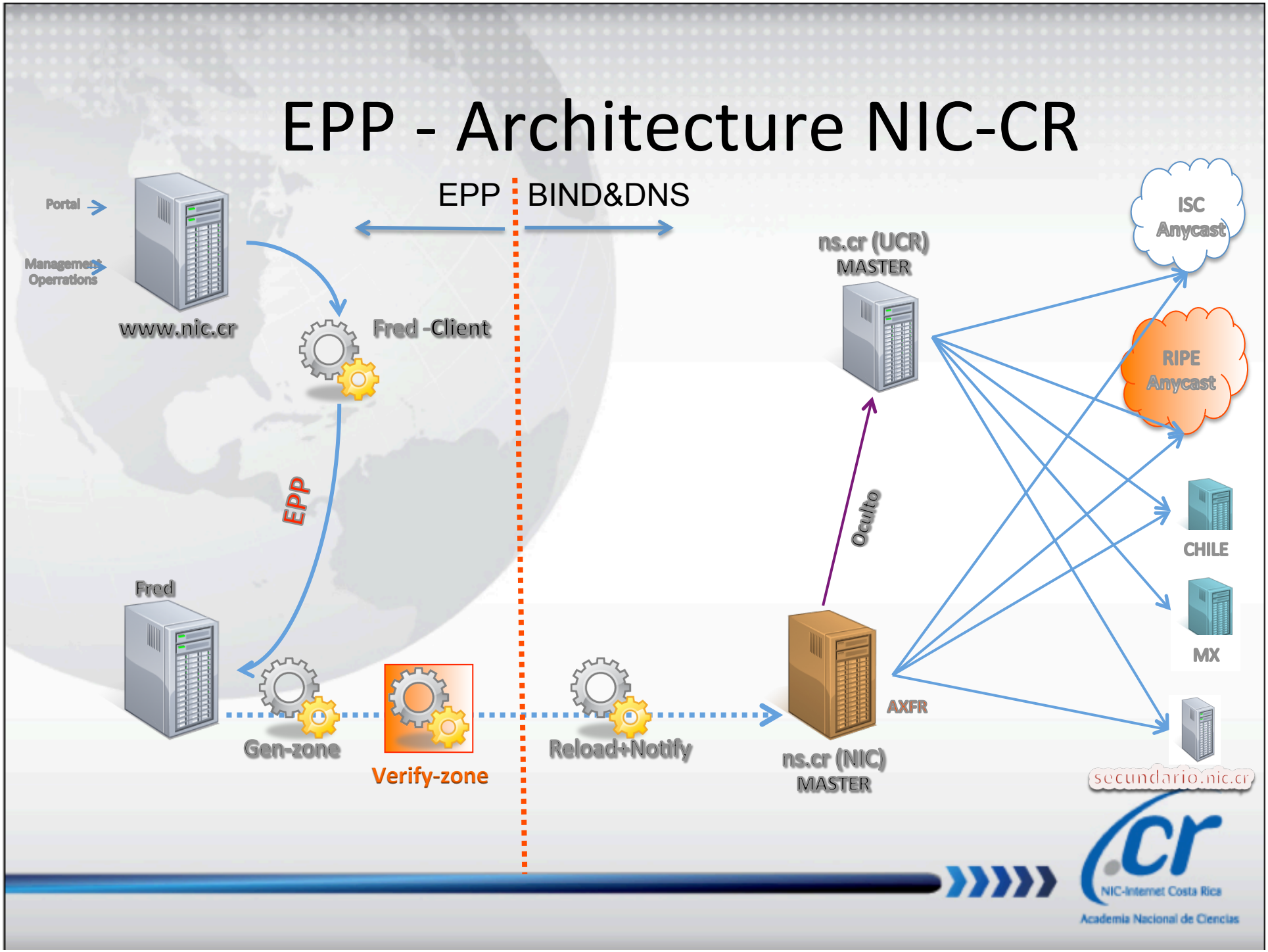
- Banco Nacional embrace DNSSEC

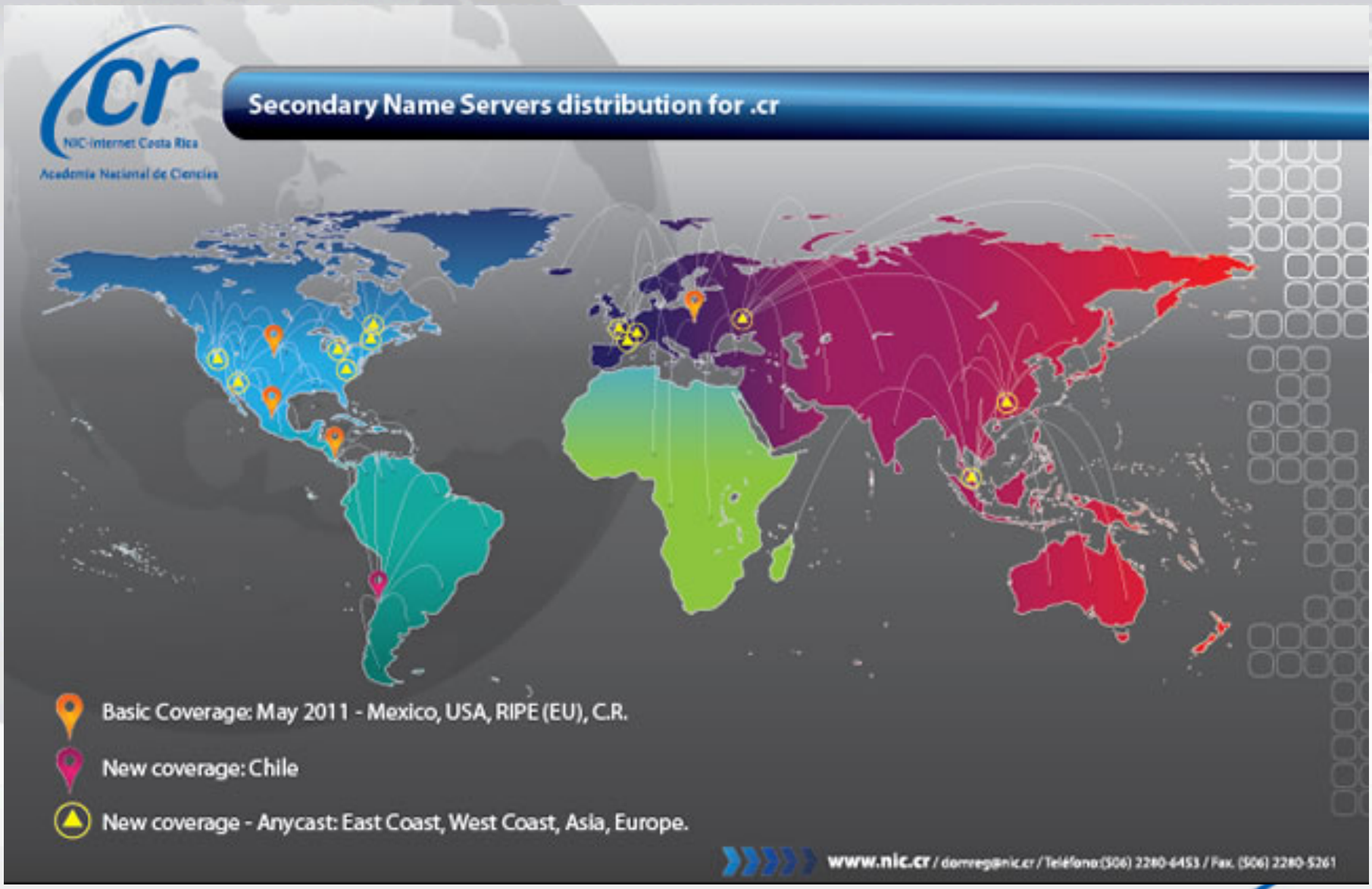
Implement

- Signer using TPM
- Signing and re-signing integrated within work flow
- DPS in Spanish

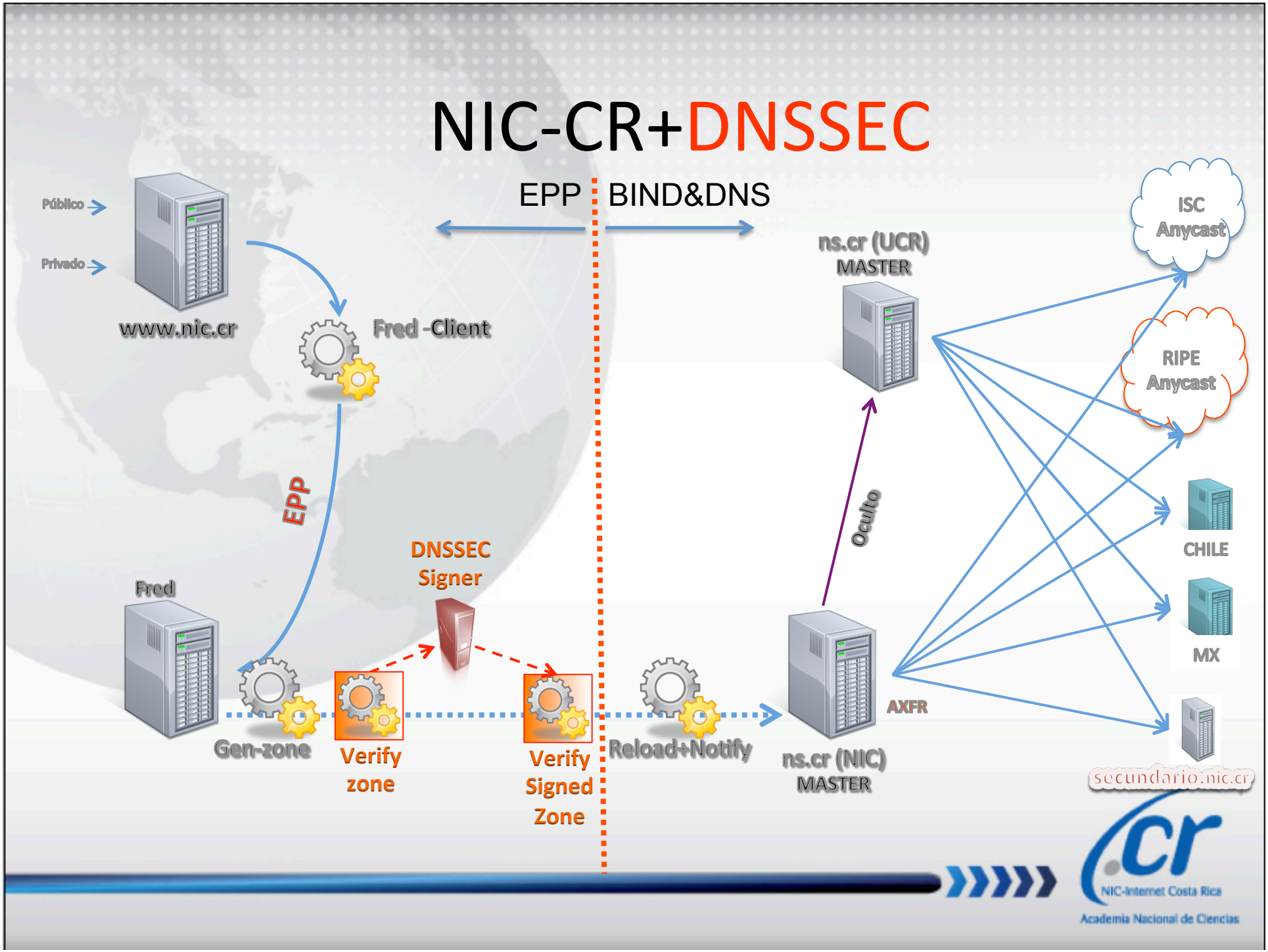
NIC-Internet Costa Rica
Academia Nacional de Ciencias

EPP - Architecture NIC-CR





.cr
NIC-Internet Costa Rica
Academia Nacional de Ciencias


NIC-CR+DNSSEC
EPP
BIND&DNS
Público
Privado
www.nic.cr
Fred -Client
EPP
Fred
DNSSEC
Signer
Gen-zone
Verify
zone
Verify
Signed
Zone
Reload+Notify
ns.cr (NIC)
MASTER
AXFR
Oculto
ns.cr (UCR)
MASTER
ISC
Anycast
RIPE
Anycast
CHILE
MX
secundario.nic.cr
.cr
NIC-Internet Costa Rica
Academia Nacional de Ciencias

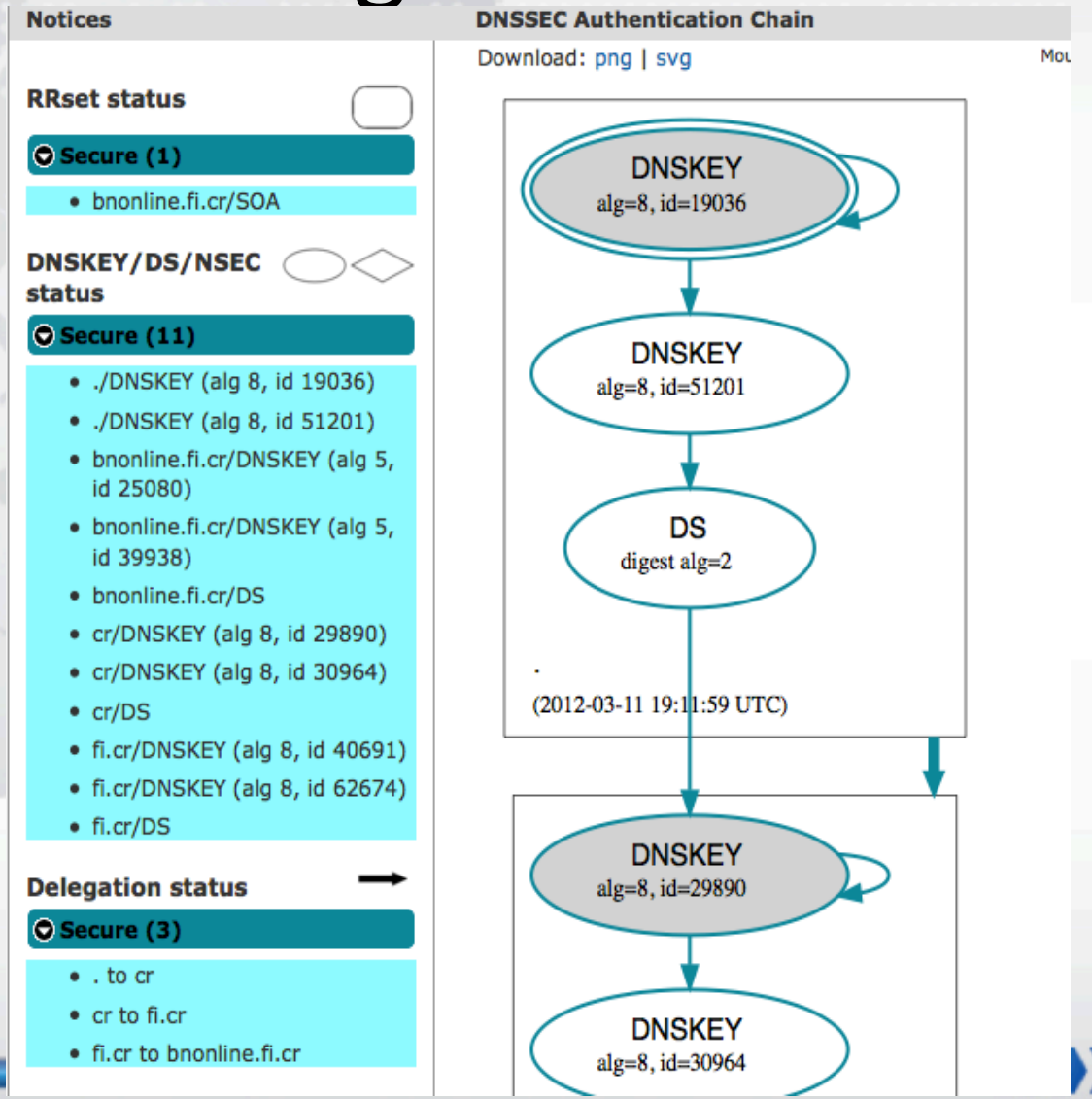
Main issues

- Cisco firewall:
  - policy-map type inspect dns preset_dns_map
    - Parameters
    - message-length maximum 4096.
- Find how to backup TPM keys before place sign in production environment.
- Process to approve and publish DPS.

bnonline.fi.cr

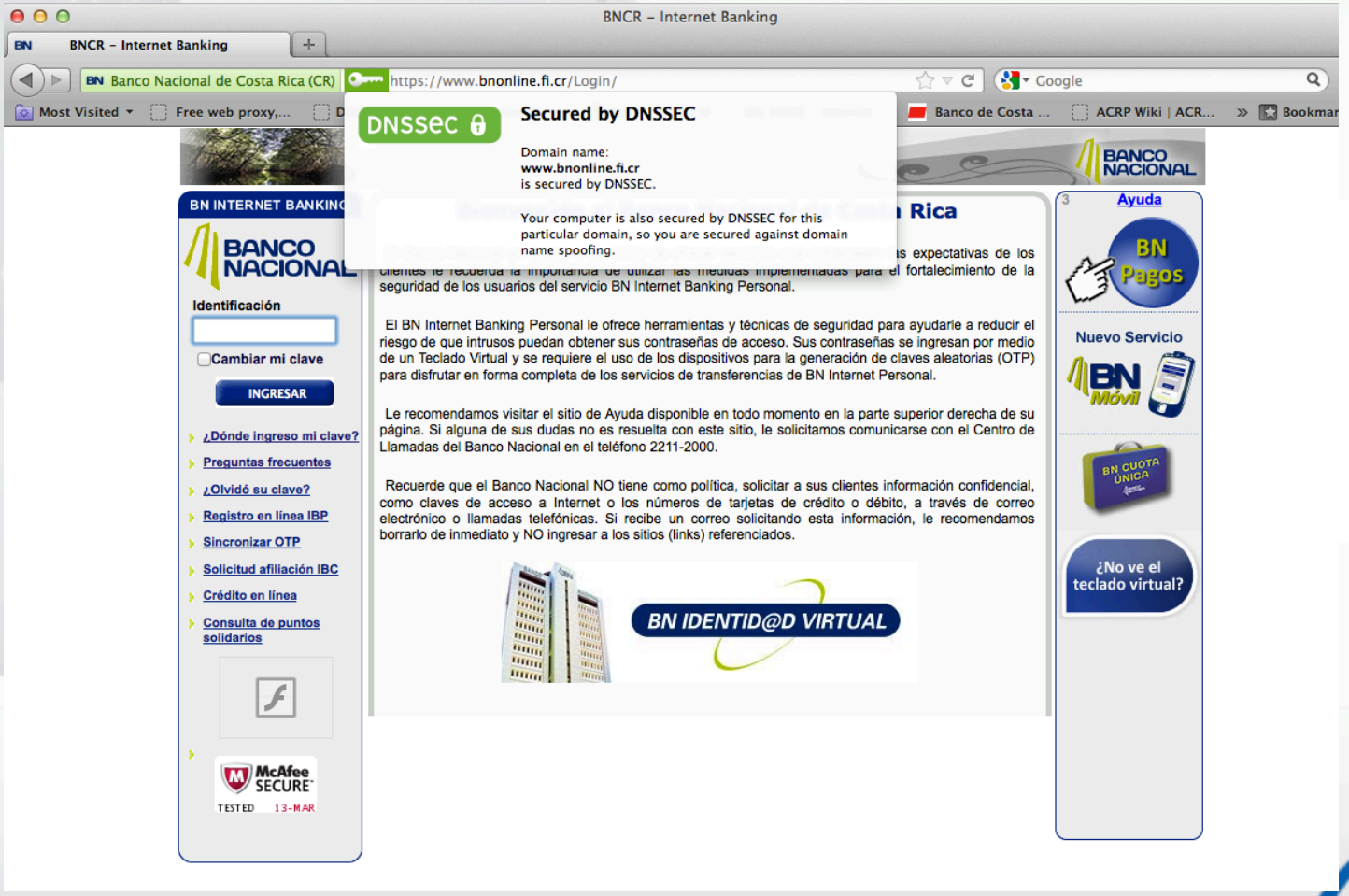
- Face to face meeting to awareness about the benefits of DNSSEC.
- Technical work session to explain concepts.
- Self signing process and email send of the DS.
- Incorporation of DS of bnonline.fi.cr within db..fi.cr via hourly script (don't use Fred for this yet).

Checking with dnsviz.net



NIC-Internet Costa Rica
Academia Nacional de Ciencias

DNSSEC Verification



Key management room

NIC-Internet Costa Rica
Academia Nacional de Ciencias

Key backup and custody

Tamper evidence bags labeled

3 USB flashdrives with copies of Keys. Local and remote (bank) in safeboxes

NIC-Internet Costa Rica

Academia Nacional de Ciencias

Thanks!

lespinoz@nic.cr

NIC-Internet Costa Rica

Academia Nacional de Ciencias