



DNSSEC Implementation at .CR

ccNSO TechDay

Luis Espinoza S.

CTO – NIC Costa Rica



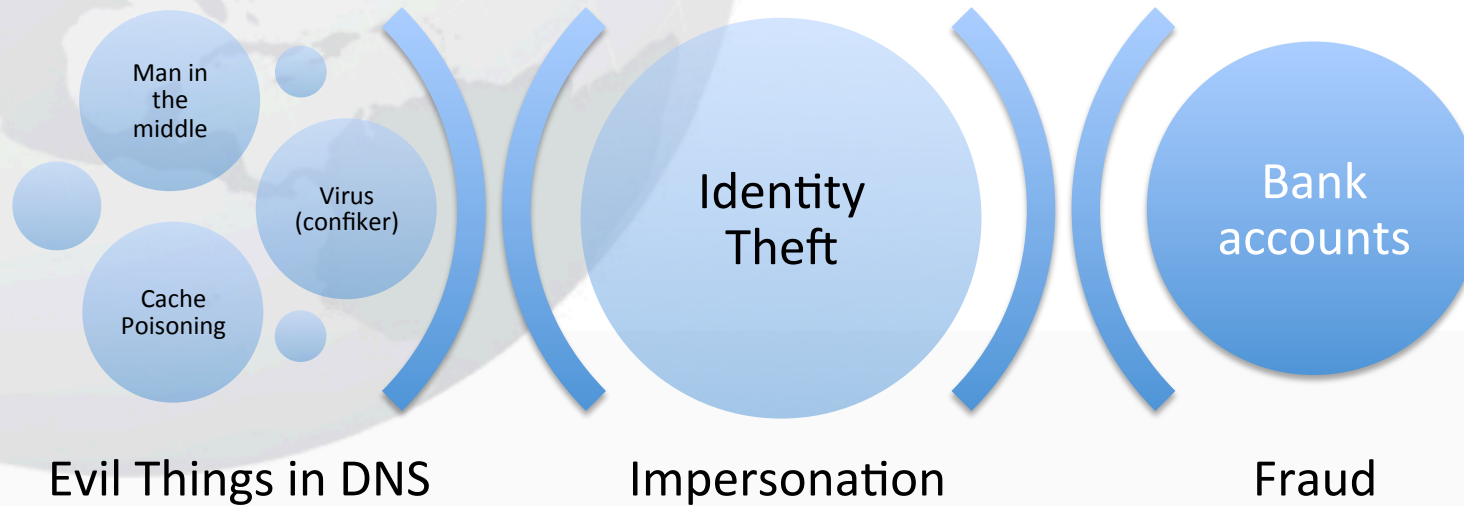
Agenda

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

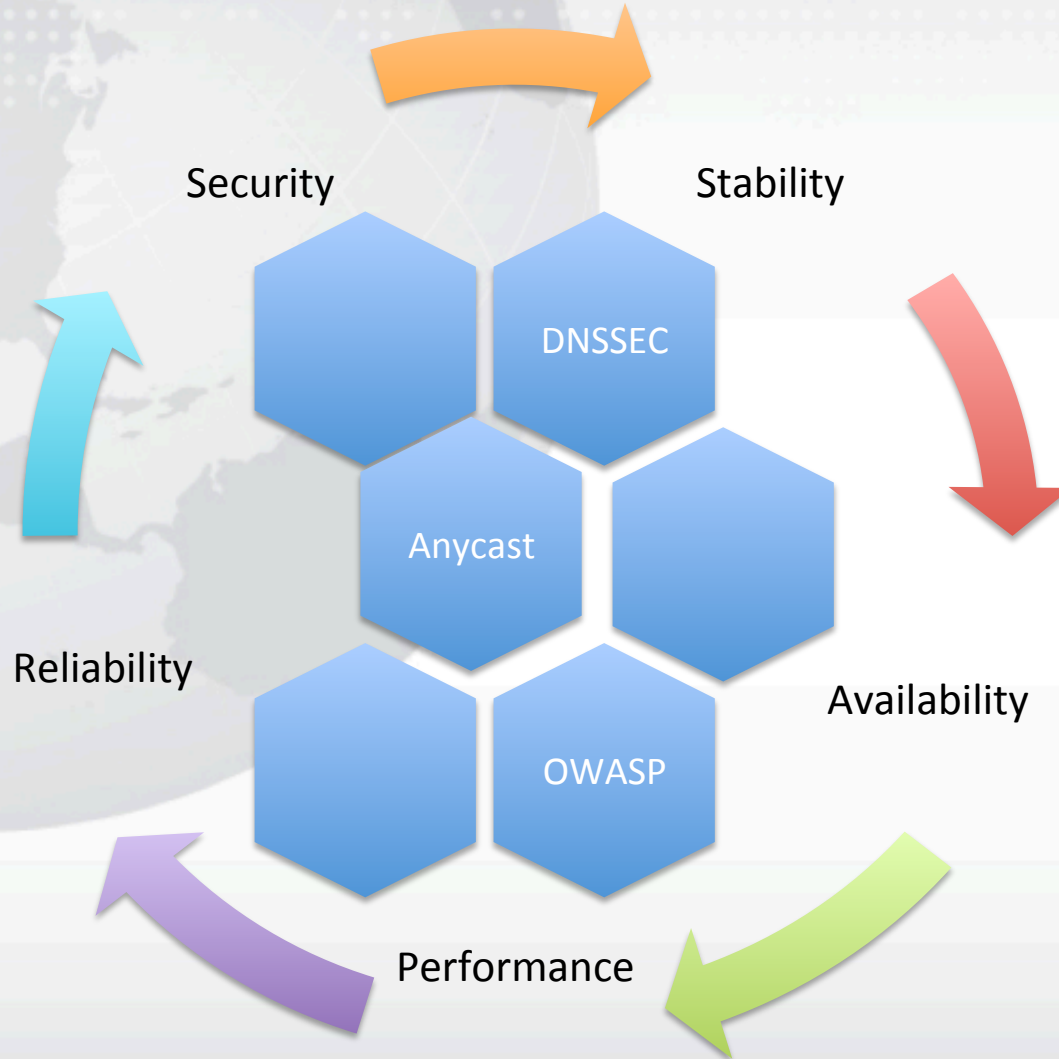
Introduction

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

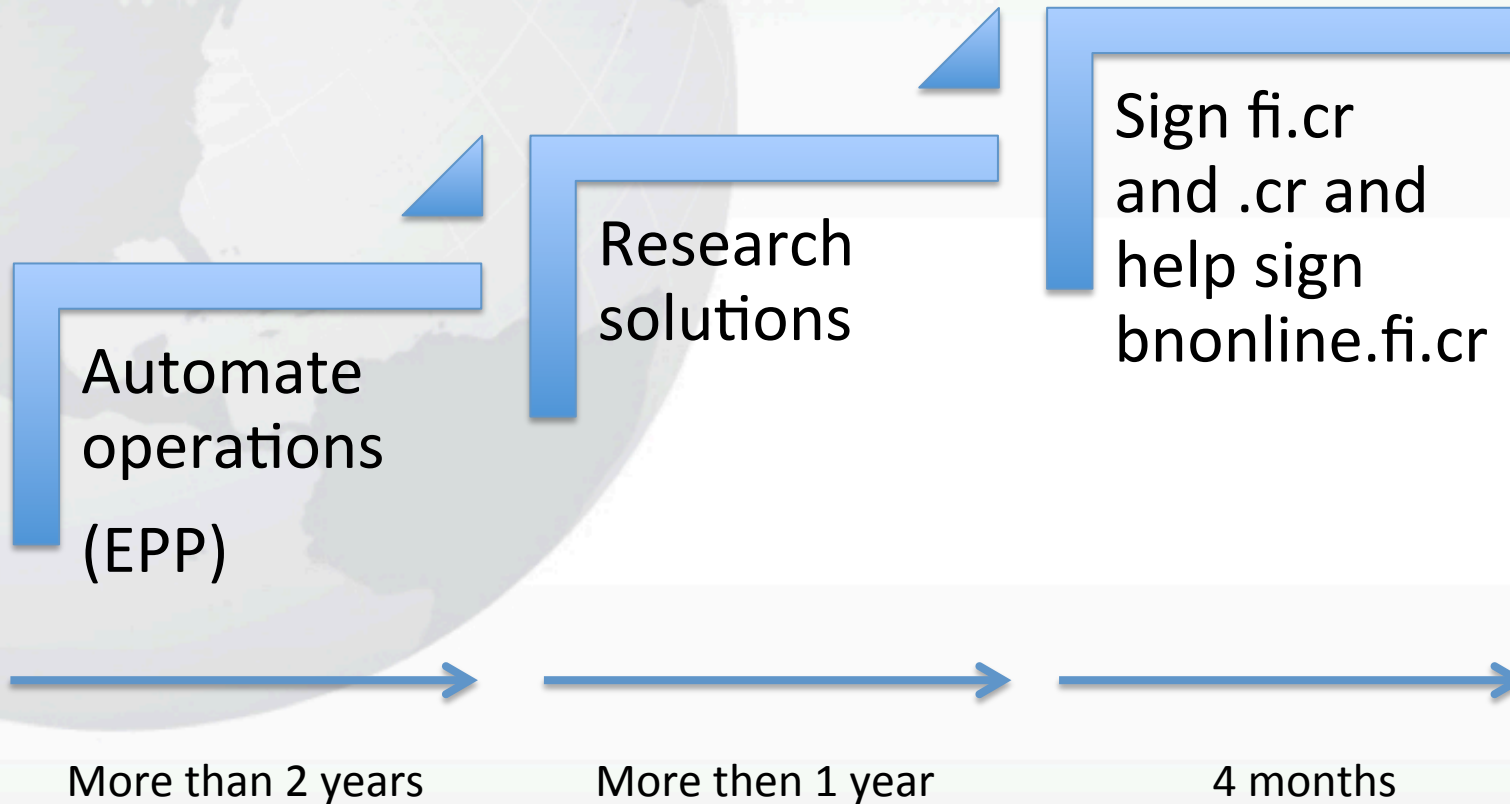
Introduction



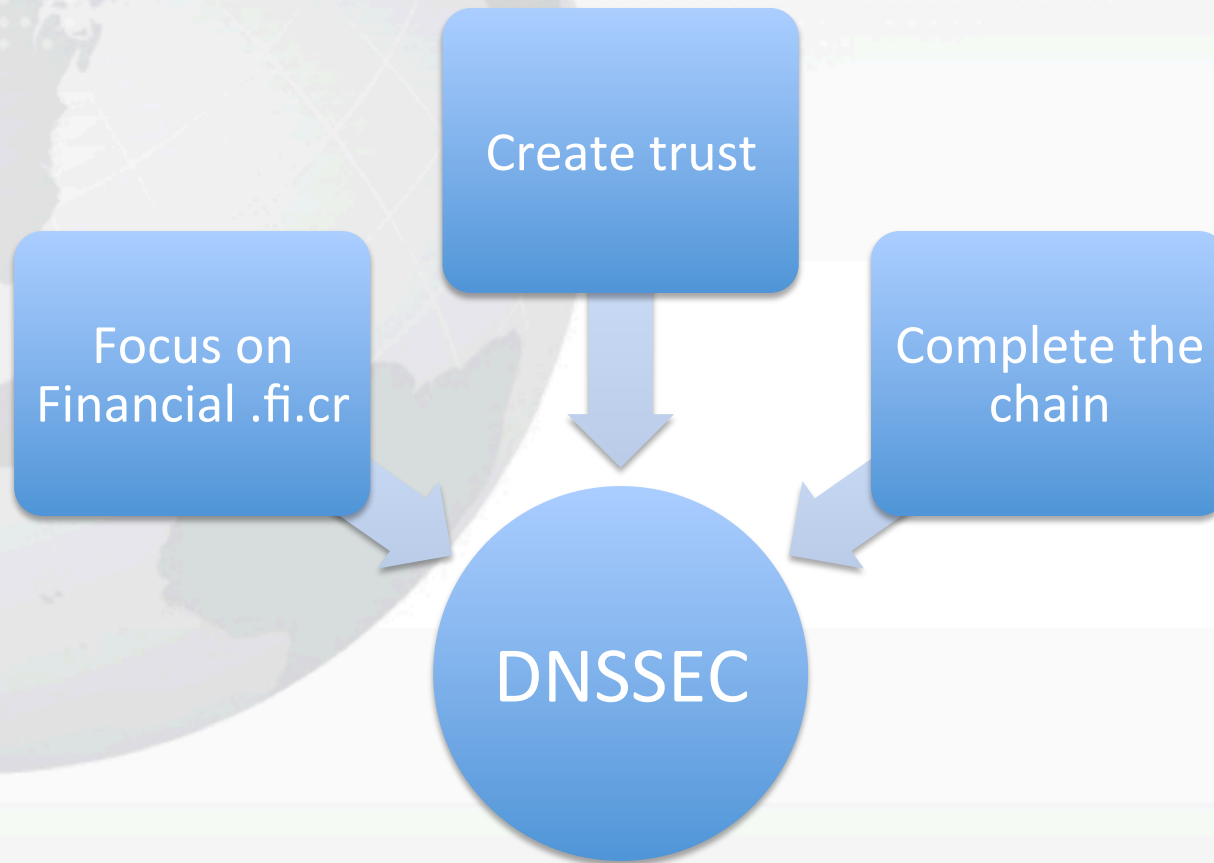
Introduction



Planning DNSSEC Deploy



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

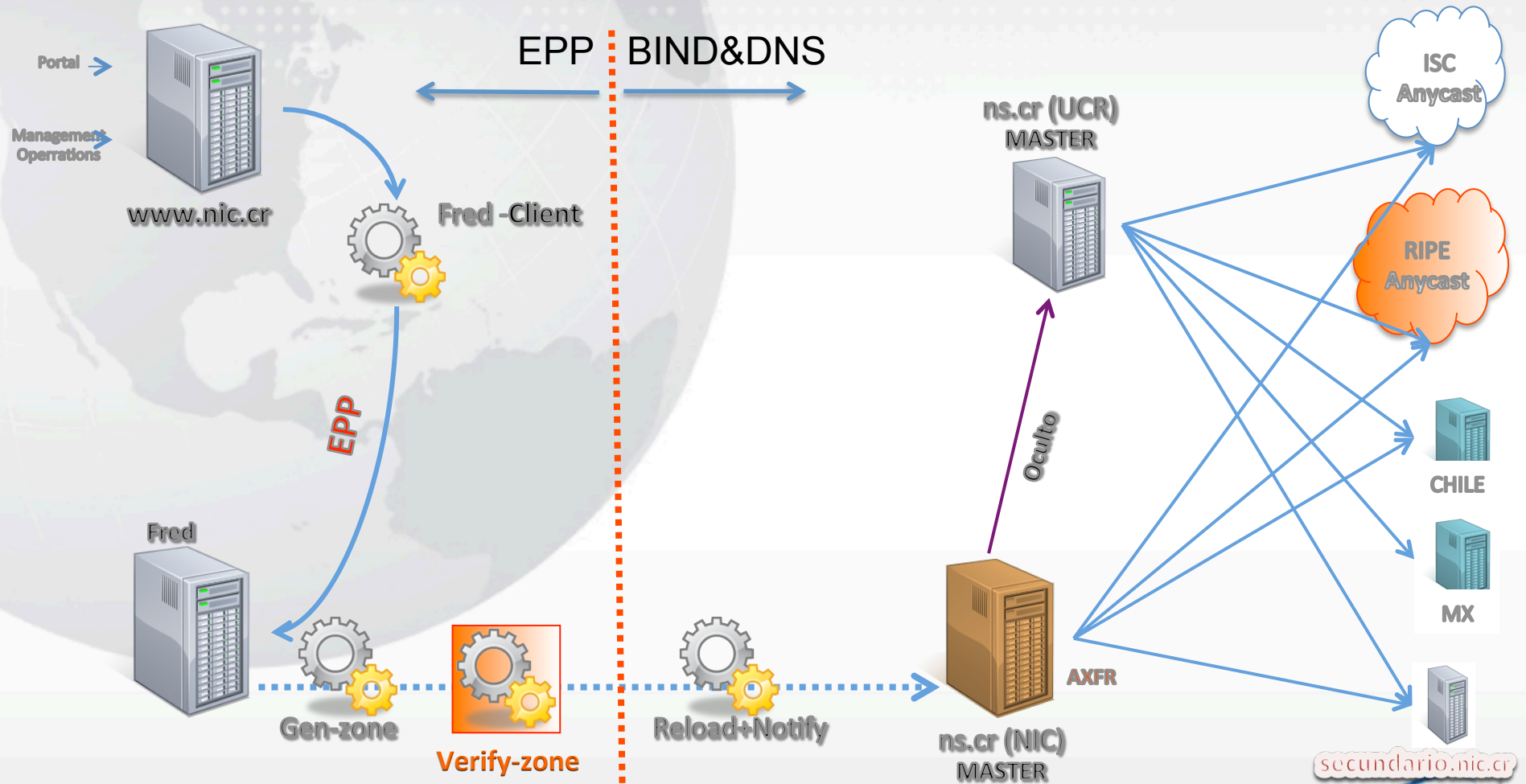
- Banco Nacional embrace DNSSEC

Implement

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



EPP - Architecture NIC-CR



Secondary Name Servers distribution for .cr



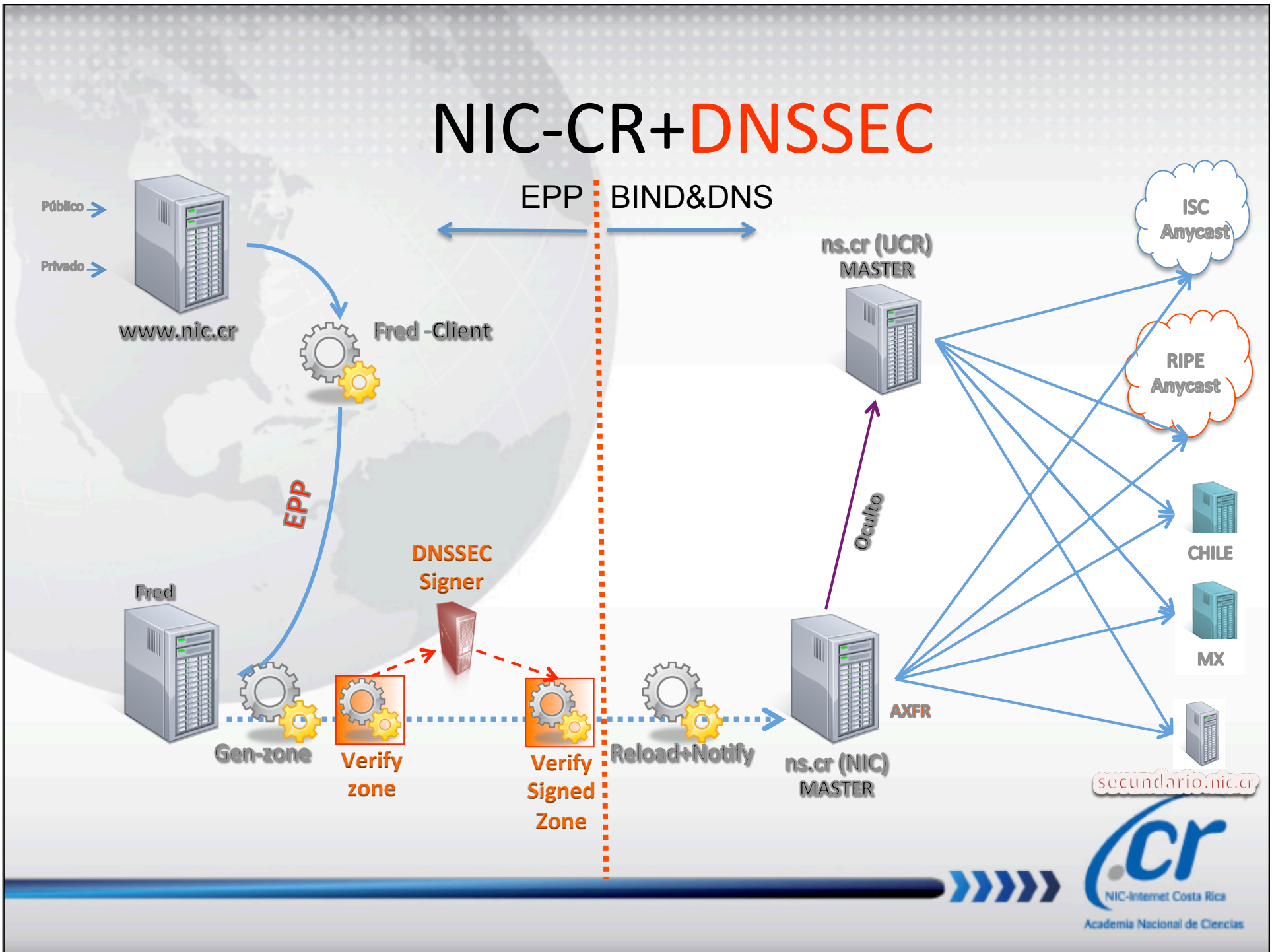
-  Basic Coverage: May 2011 - Mexico, USA, RIPE (EU), C.R.
-  New coverage: Chile
-  New coverage - Anycast: East Coast, West Coast, Asia, Europe.



www.nic.cr / domreg@nic.cr / Teléfono (506) 2280-4453 / Fax: (506) 2280-5261



NIC-CR+DNSSEC



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

Notices

RRset status

Secure (1)

- bnonline.fi.cr/SOA

DNSKEY/DS/NSEC status

Secure (11)

- ./DNSKEY (alg 8, id 19036)
- ./DNSKEY (alg 8, id 51201)
- bnonline.fi.cr/DNSKEY (alg 5, id 25080)
- bnonline.fi.cr/DNSKEY (alg 5, id 39938)
- bnonline.fi.cr/DS
- cr/DNSKEY (alg 8, id 29890)
- cr/DNSKEY (alg 8, id 30964)
- cr/DS
- fi.cr/DNSKEY (alg 8, id 40691)
- fi.cr/DNSKEY (alg 8, id 62674)
- fi.cr/DS

Delegation status

Secure (3)

- . to cr
- cr to fi.cr
- fi.cr to bnonline.fi.cr

DNSSEC Authentication Chain

Download: [png](#) | [svg](#) Mo

```
graph TD; A("DNSKEY  
alg=8, id=19036") --> B("DNSKEY  
alg=8, id=51201"); B --> C("DS  
digest alg=2"); C --> D("DNSKEY  
alg=8, id=29890"); D --> E("DNSKEY  
alg=8, id=30964");
```

(2012-03-11 19:11:59 UTC)

DNSSEC Verification

The screenshot shows a web browser window titled "BNCR - Internet Banking". The address bar displays "https://www.bnonline.fi.cr/Login/". A green "DNSSEC" popup is overlaid on the page, containing the following text:

DNSSEC Secured by DNSSEC

Domain name:
www.bnonline.fi.cr
is secured by DNSSEC.

Your computer is also secured by DNSSEC for this particular domain, so you are secured against domain name spoofing.

The background page is the BNCR Internet Banking login page, featuring the "BANCO NACIONAL" logo, a login form with an "INGRESAR" button, and a list of links such as "¿Dónde ingreso mi clave?", "Preguntas frecuentes", and "¿Olvidó su clave?". A "McAfee SECURE" badge is visible at the bottom left of the page. On the right side, there are promotional banners for "BN Pagos", "Nuevo Servicio BN Móvil", and "BN CUOTA UNICA".

Key management room



Security
Camera

Offline PC
with TPM

Key backup and custody

Tamper evidence bags labeled

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





Thanks!

lespinoz@nic.cr