DNSSEC Implementation at .CR

ccNSO TechDay March 2012

Luis Espinoza S.

CTO – NIC Costa Rica

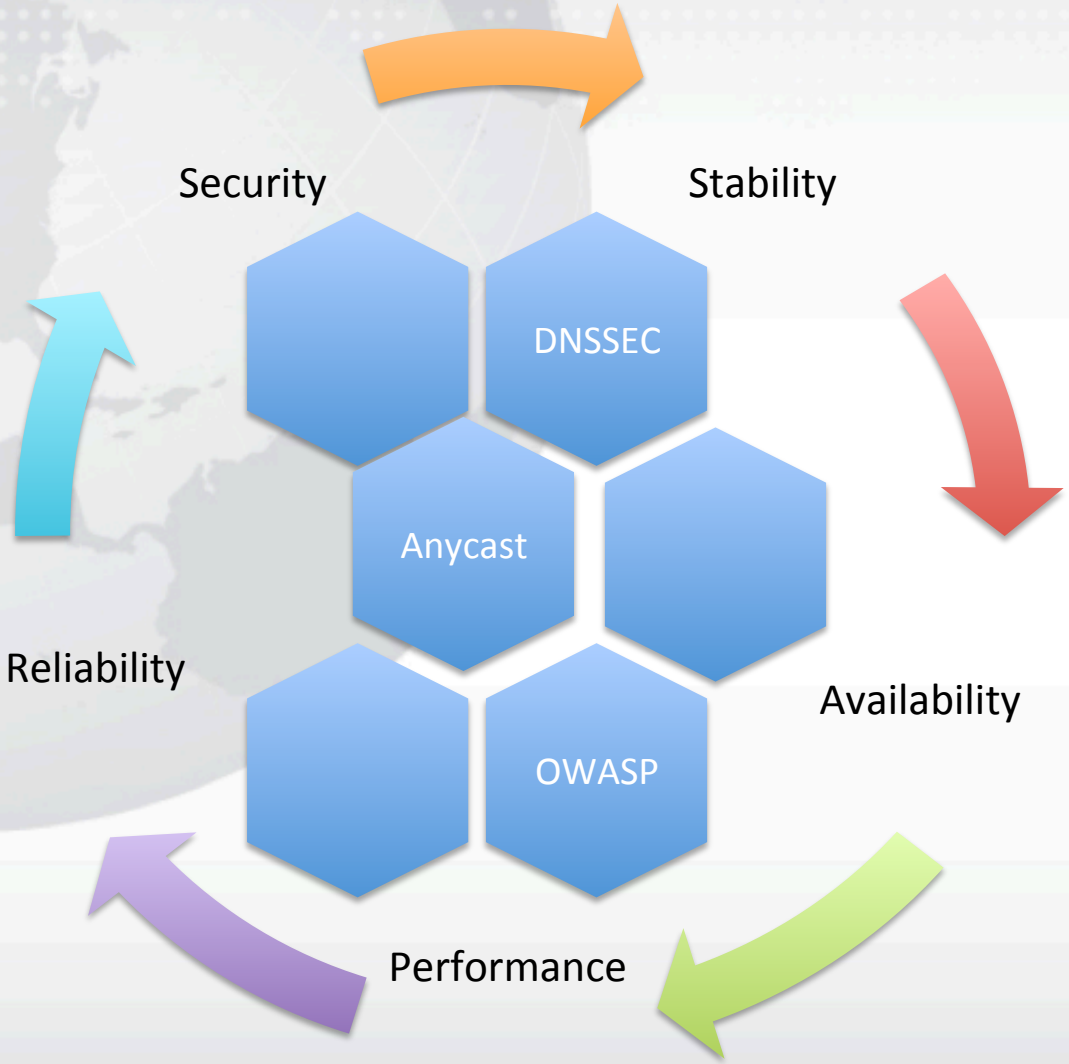
NIC-Internet Costa Rica

Academia Nacional de Ciencias

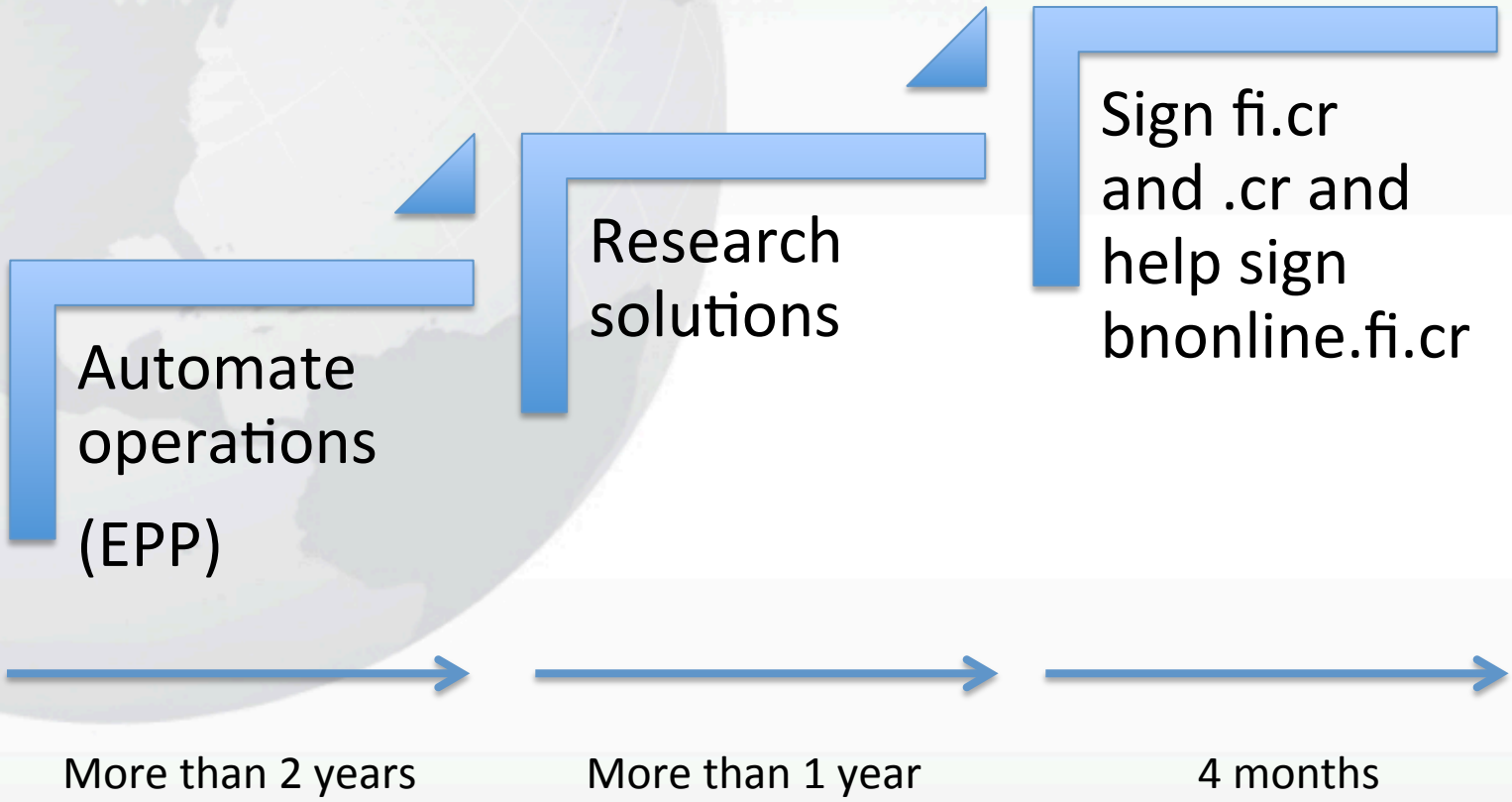
Agenda

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

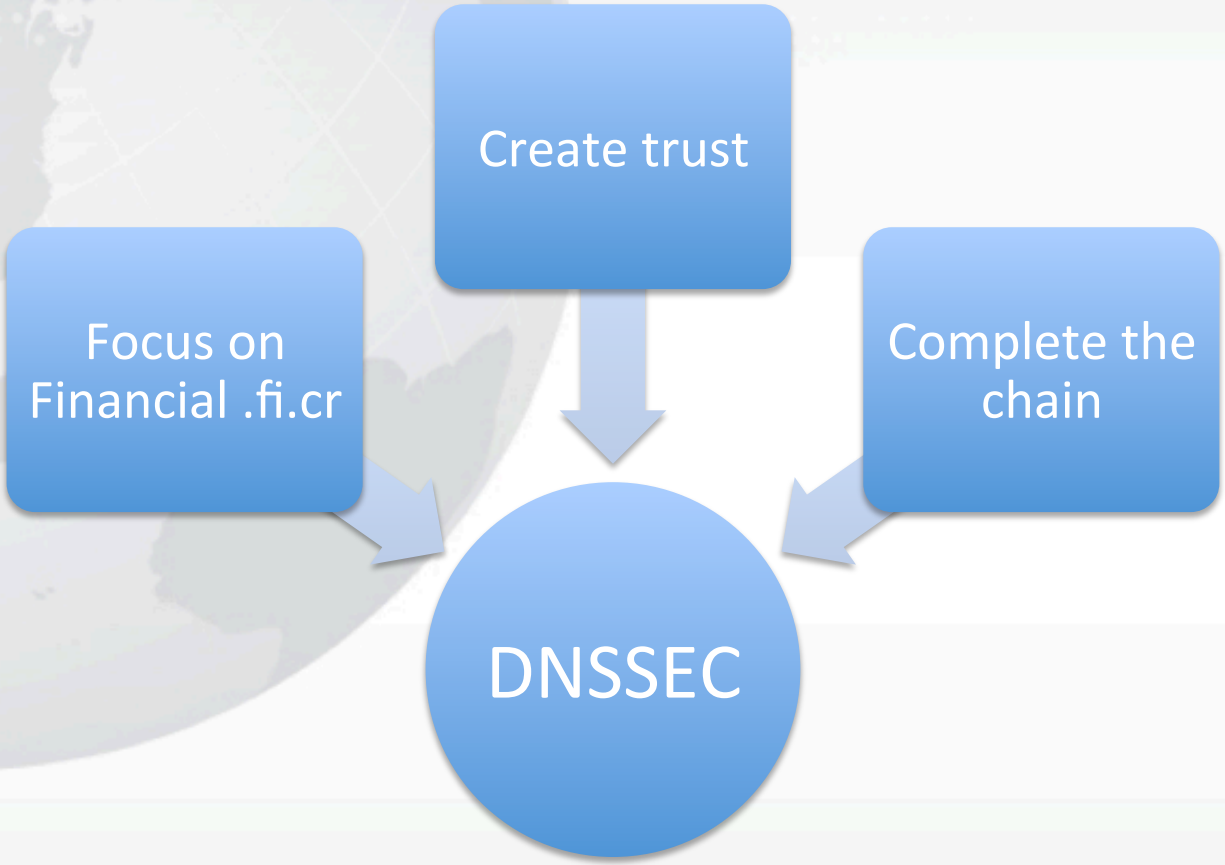
Introduction



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

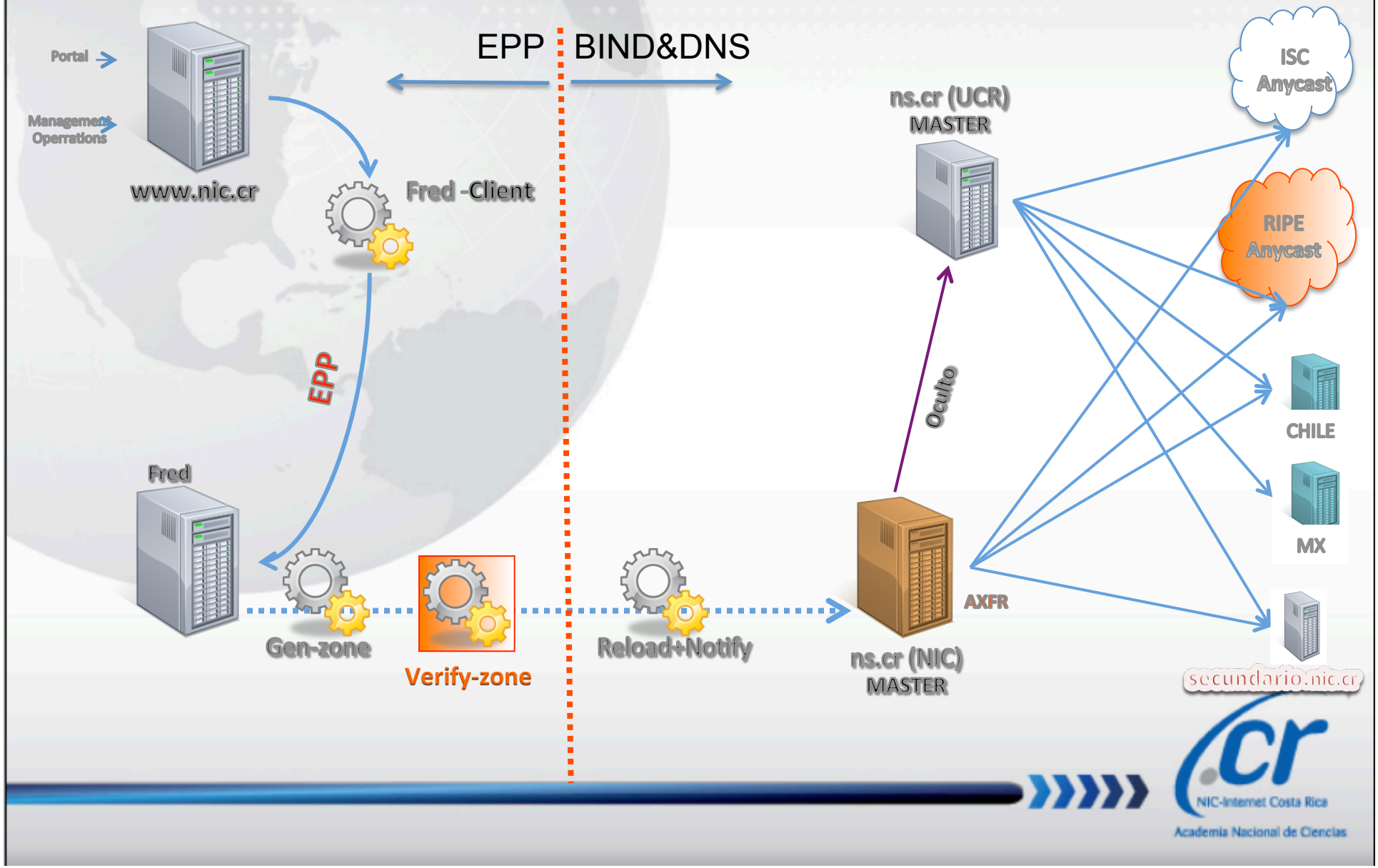
- Banco Nacional embrace DNSSEC

Implement

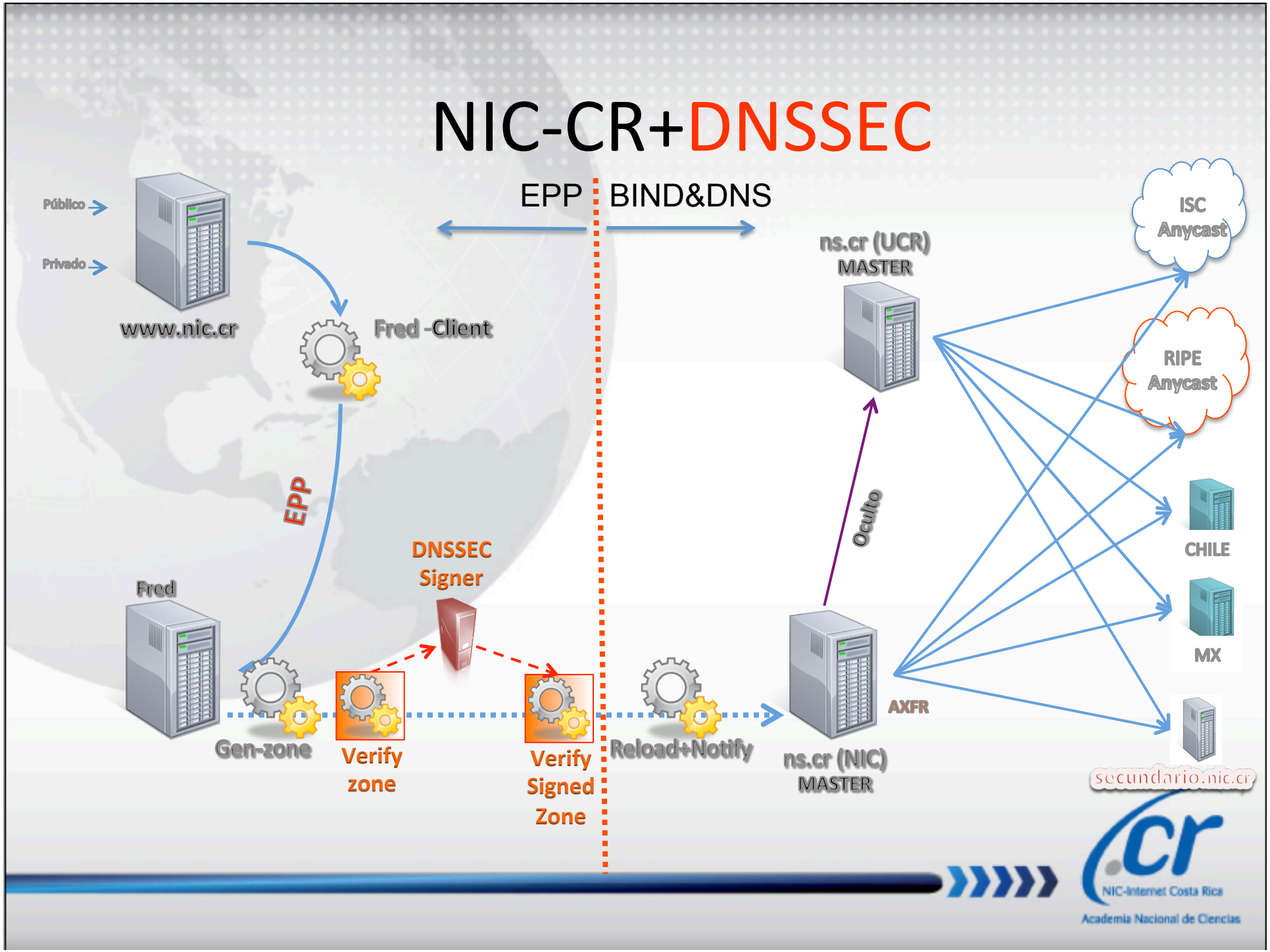
- Signer using TPM
- Signing and re-signing integrated within flow
- DPS in Spanish

NIC-Internet Costa Rica
Academia Nacional de Ciencias

EPP - Architecture NIC-CR



NIC-CR+DNSSEC



DNSSEC Signer


```
/etc/init.d/bind9 reload
```

```
export PKCS11_LIBRARY_PATH=/usr/lib/opencryptoki/libopencryptoki.so.0
export PKCS11_LIBRARY_PIN="$zpin"
# Generate salt for NSEC3 (do rarely)
salt=`printf %04x
/usr/local/dnssec
-e +1446000 -o $1
```

db..go.c
db..ed.c
db..ac.c

firma-zona.cr

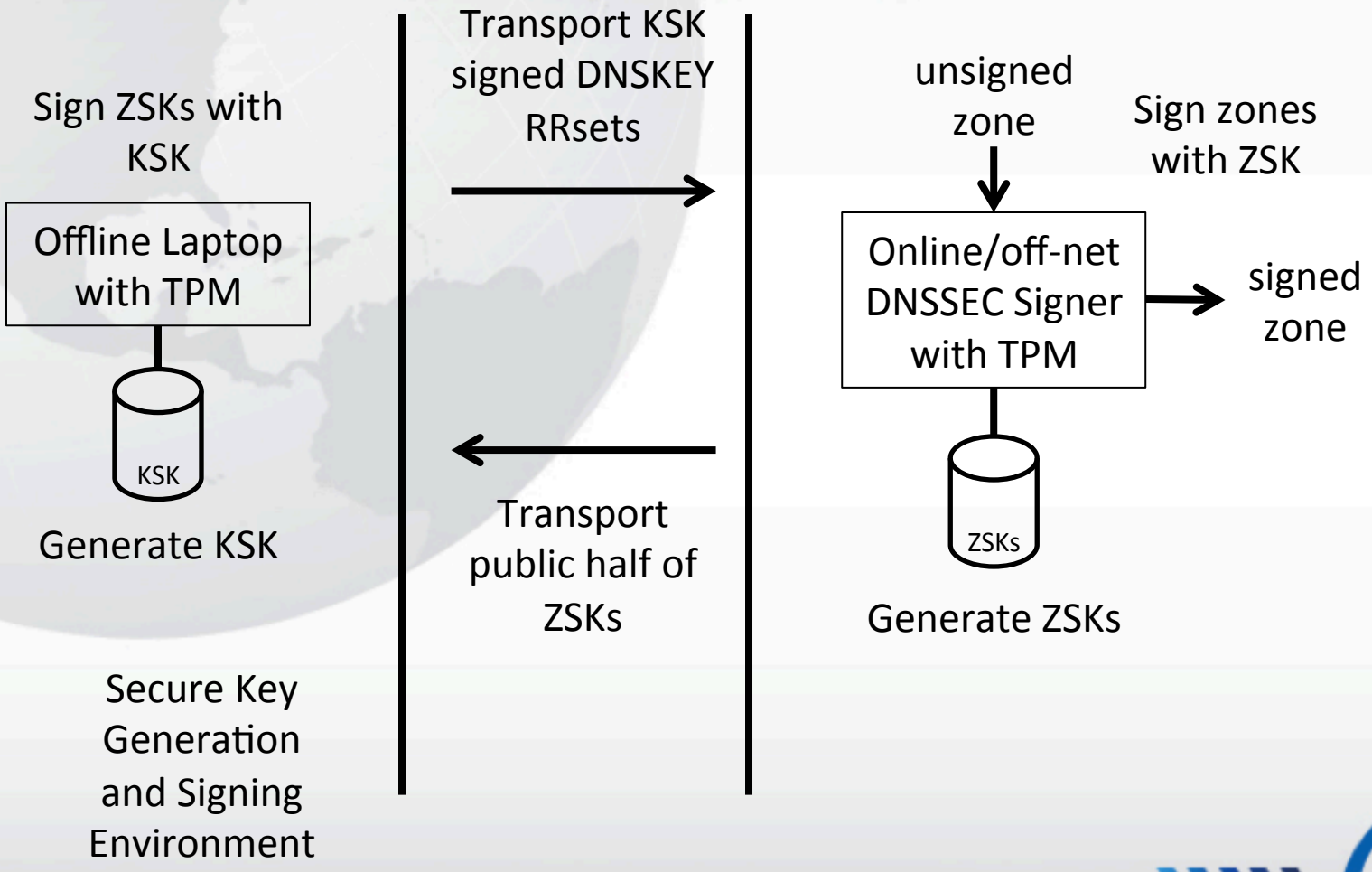
db.cr.signed

```
# p. ej.: ./firma.zona co.cr db..co.cr dnskeyrrset.co.cr
cat /etc/bind/db.cr /etc/bind/dsset-??.cr. /etc/bind/dsset-nic.cr. /etc/bind/dsset
-crnet.cr. /usr/local/dnssec/dnskeyrrset > $tmpfile
# Sign it with ZSK
export PKCS11_LIBRARY_PATH=/usr/lib/opencryptoki/libopencryptoki.so.0
export PKCS11_LIBRARY_PIN="$zpin"
# Generate salt for NSEC3 (do rarely)
salt=`printf %04x%04x $RANDOM $RANDOM`
/usr/local/dnssec/dnssec-signzone -K /usr/local/dnssec -v 3 -A -3 $salt -x -s now
-e +1446000 -o cr $tmpfile
```

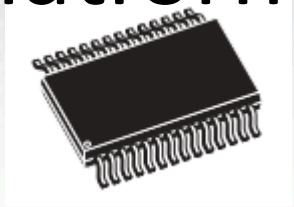
57 /usr/local/bin/integridad.zonas.2
31 /usr/local/dnssec/firma.zona.cr
31 /usr/local/dnssec/firma.zona.sub

NIC-Internet Costa Rica
Academia Nacional de Ciencias

Key Management



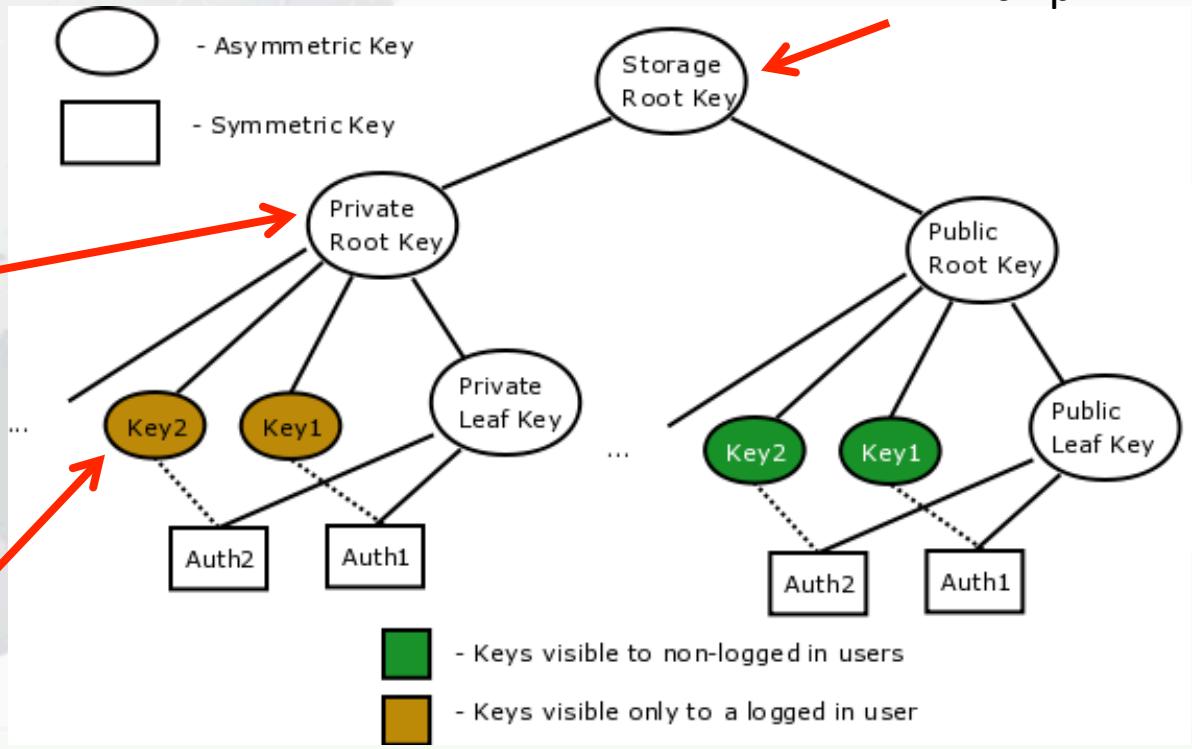
A little about the Trusted Platform Module (TPM)



- Easy to obtain crypto. Built in standard H/W
- Supported by open source software
- Not fast (~1 RSA 1024 sig/s) but may be sufficient and theoretically capable ~10x
- Built in H/W RNG
- PKCS11 interface simplifies upgrade to HSM

TPM Trousers/opencryptoki Framework

In TPM chip



Encrypted with SRK on disk. Decrypted inside TPM

Encrypted with Root Key on disk. Decrypted inside TPM

Diagram courtesy Kent Yoder

From http://trousers.sourceforge.net/pkcs11.html

Pros and Cons

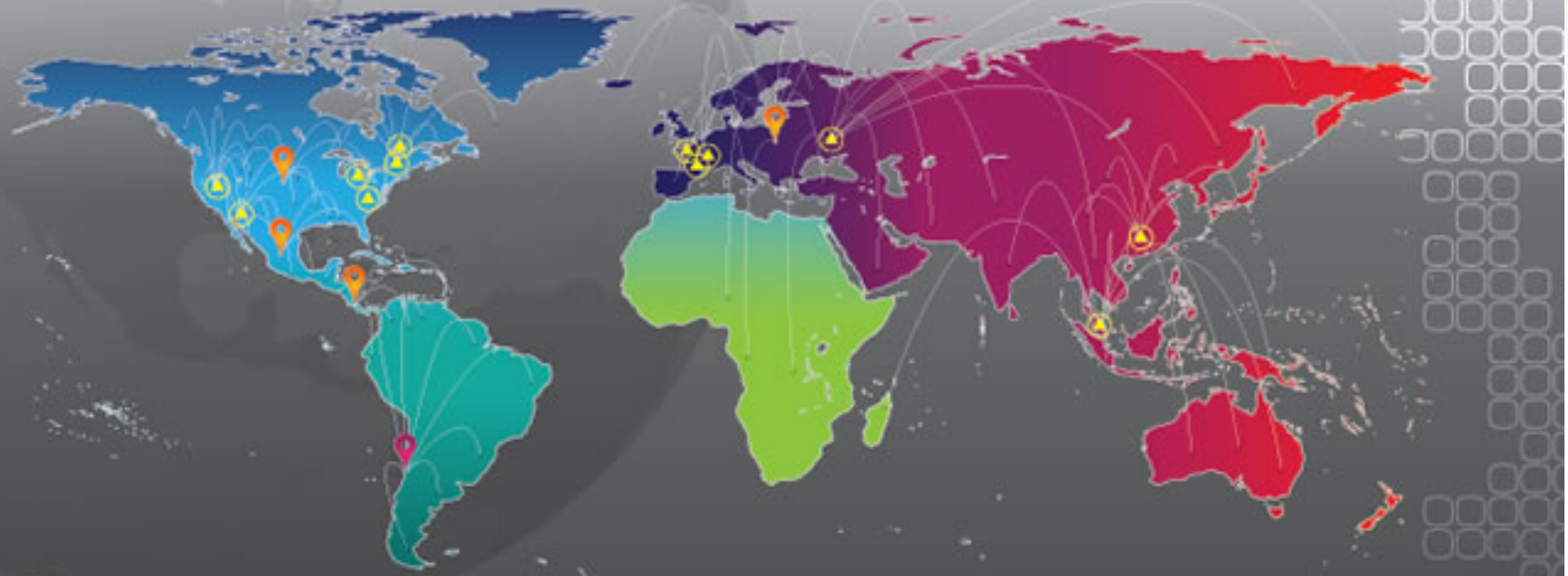
- Cons
  - Key “migration” (i.e., backup) complexity
  - H/W Driver support
  - Slow speed
  - Non-obvious key management framework
- Pros
  - Easy to obtain
  - “free”

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.
- TPM is slow. Total process time 15 minutes.

NIC-Internet Costa Rica
Academia Nacional de Ciencias

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) 2280-6453 / Fax. (506) 2280-5261

NIC-Internet Costa Rica
Academia Nacional de Ciencias

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

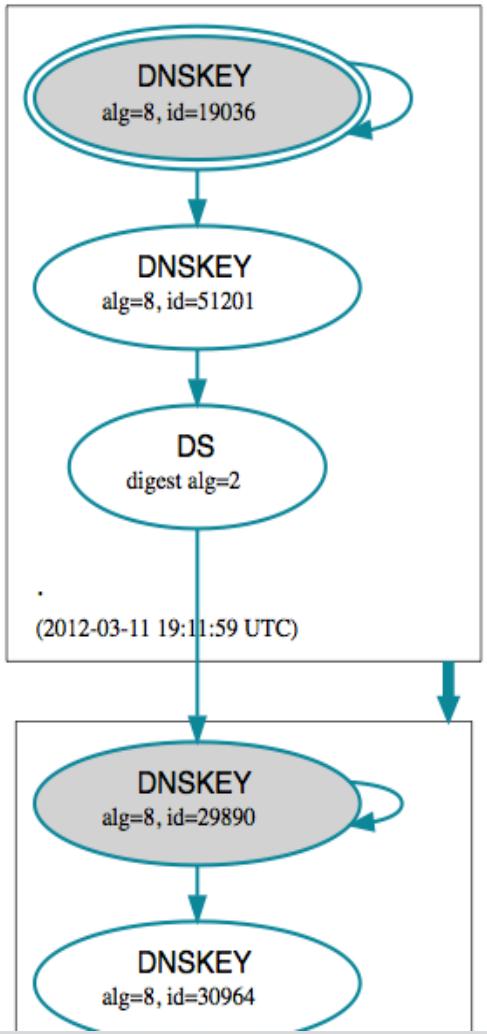
Delegation status

Secure (3)

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

DNSSEC Authentication Chain

Download: png | svg

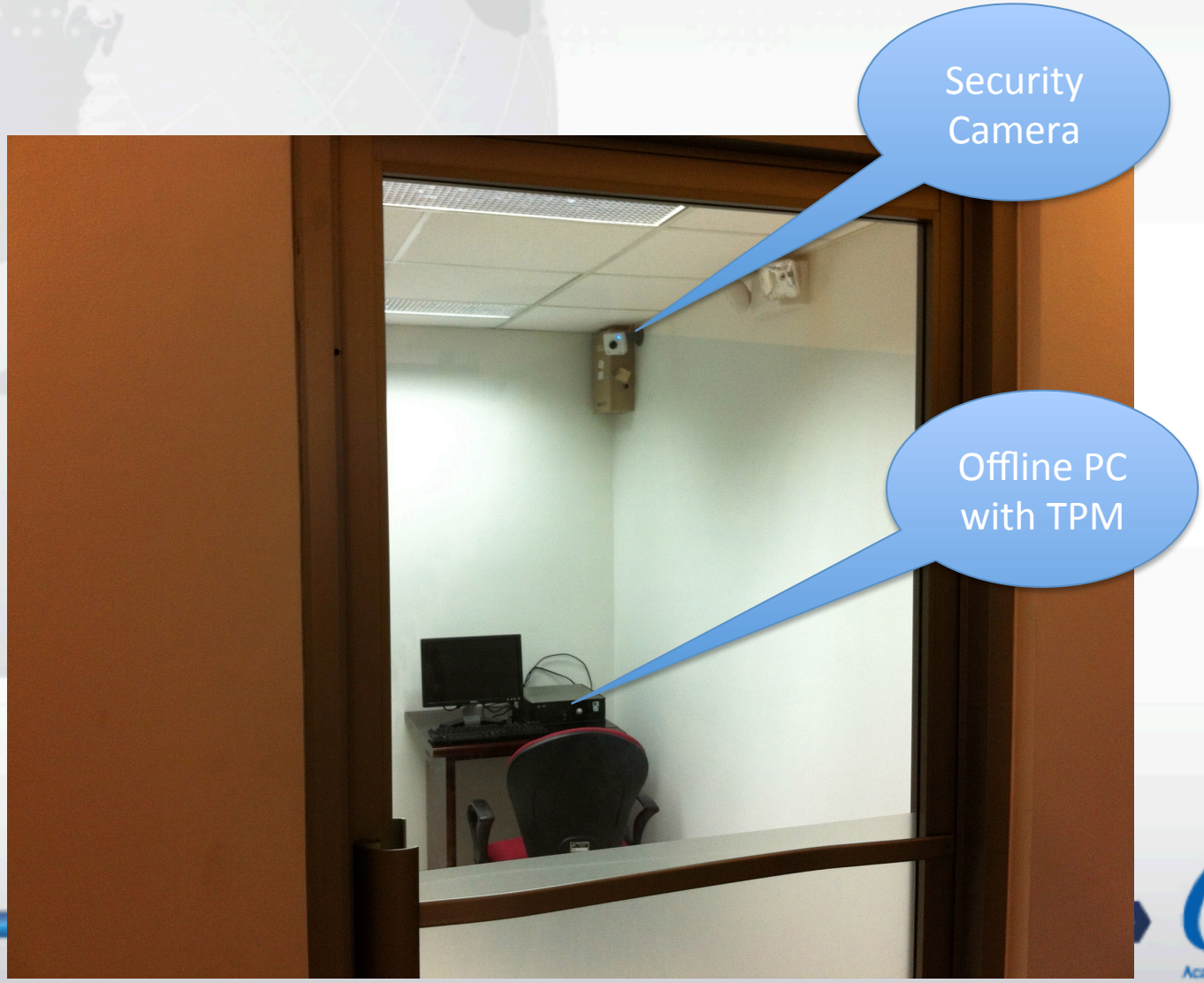


NIC-Internet Costa Rica
Academia Nacional de Ciencias

Questions?

lespinoz@nic.cr

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