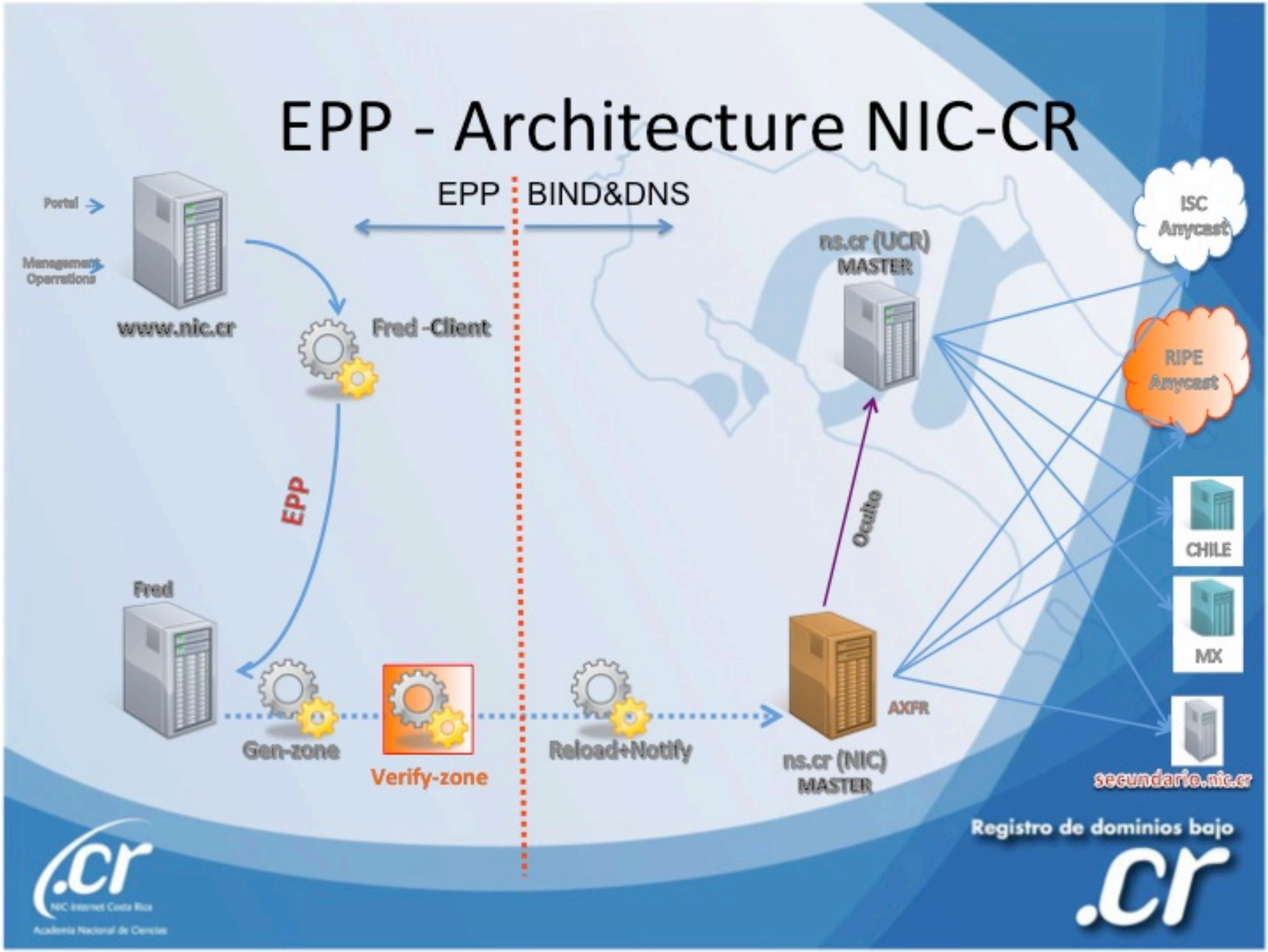
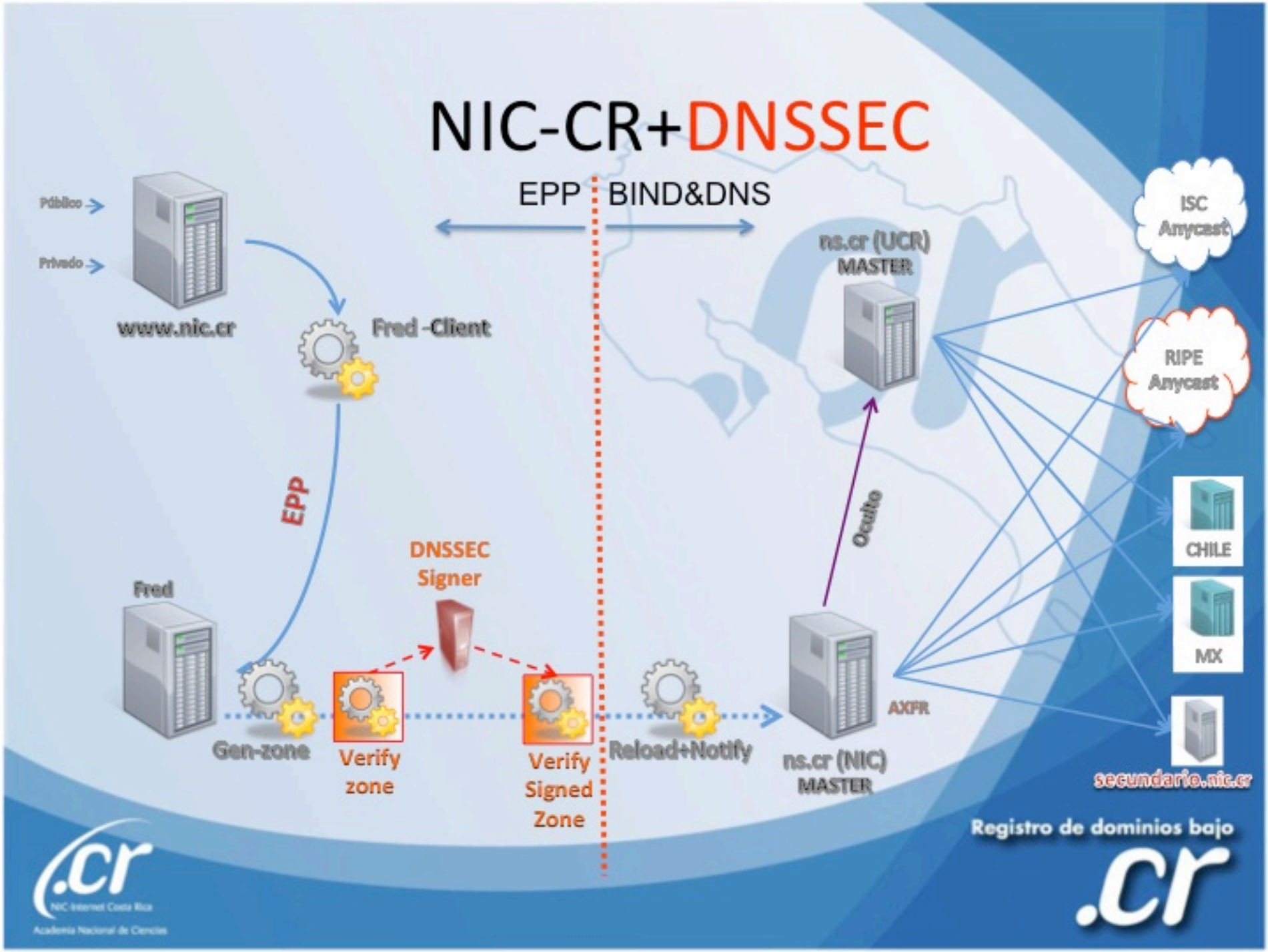
DNSSEC Signer Implementation Hardware

ICANN 43 Meeting, Costa Rica
12-16 March 2012

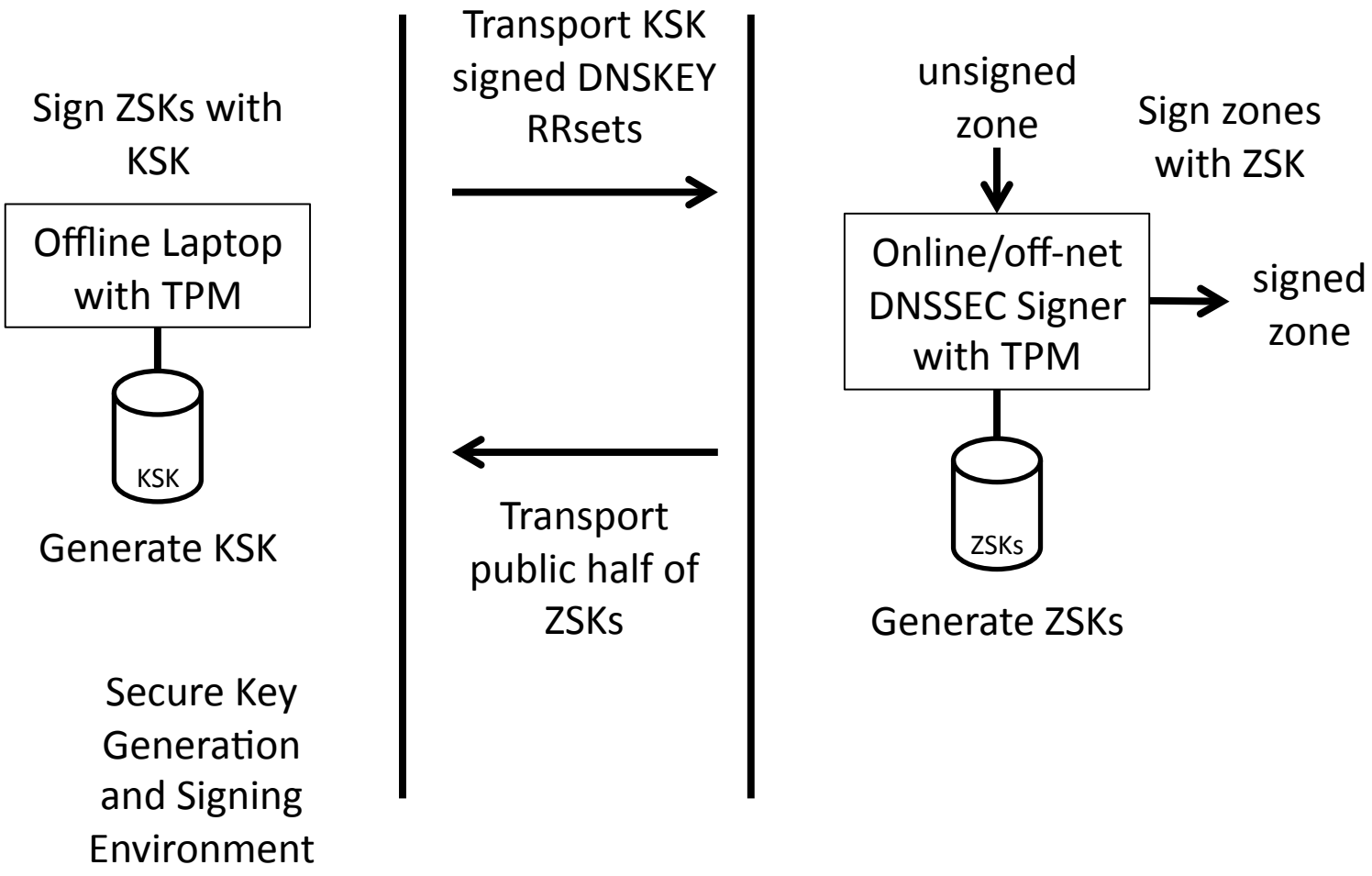
Luis Diego Espinoza,
Mario Guerra Araya,
Richard Lamb

EPP - Architecture NIC-CR

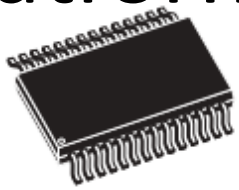



NIC-CR+DNSSEC
EPP
BIND&DNS
Público
Privado
www.nic.cr
Fred -Client
EPP
Fred
DNSSEC
Signer
Gen-zone
Verify
zone
Verify
Signed
Zone
Reload+Notify
ns.cr (UCR)
MASTER
Oculto
ns.cr (NIC)
MASTER
AXFR
ISC
Anycast
RIPE
Anycast
CHILE
MX
secundario.nic.cr
Registro de dominios bajo
.cr
NIC Internet Costa Rica
Academia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

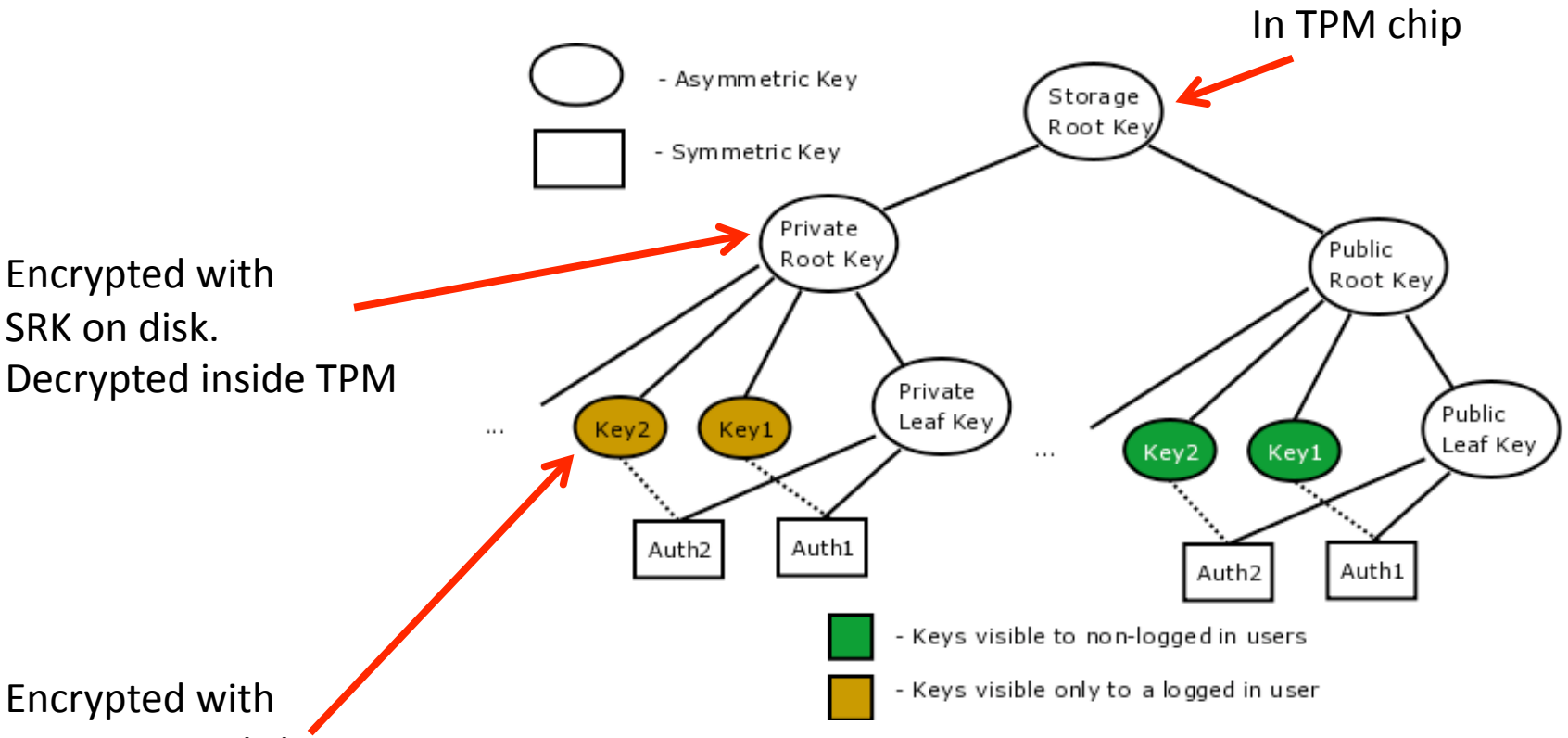


Diagram courtesy Kent Yoder

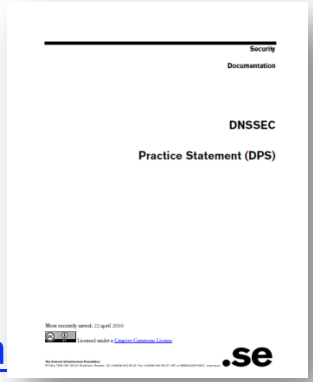
From http://trousers.sourceforge.net/pkcs11.html

Pros and Cons

- Cons
  - Slow speed
  - H/W Driver support
  - Non-obvious key management framework
- Pros
  - Easy to obtain
  - “free”

Other Resources

- TPM links
  - Trousers http://trousers.sourceforge.net/pkcs11.html
  - opencryptoki http://www.ibm.com/developerworks/linux/library/s-pkcs/
- PKCS11 spec
  - http://www.rsa.com/rsalabs/node.asp?id=2133
- DNSSEC Practice Statement (DPS)
  - Spanish Draft
  - Original .SE https://www.iis.se/dl/DPS-PA9-ENG.pdf
  - RFC draft http://datatracker.ietf.org/doc/draft-ietf-dnsop-dnssec-dps-fra



- Some source code
  - Bind modifications
  - pkcs11 tools

Questions?