Trusted Platform Module DNSSEC in production environment

Luis Diego Espinoza
Internet Technology Consultant
diego@dibs.cr

ICANN 46 – Beijing April 2013

Motivation

- Need to implement DNSSEC at the country ccTLD (small ccTLD < 15k domains)
- The trust of domain name resolution for a country is critical (Government, Financial, Industry, Education)
- The trust of a digital signature relay on follow best practices and standardized procedures.
- Use of /dev/random was too slow!

First intent for TPM

- RNG – The first intent of use TPM is because it has an internal hardware-based Random Number Generator.
- Digging a little bit more, found a PKCS11 implementation for TPM chip, not only RNG! http://trousers.sourceforge.net
- TPM is included in the existing Dell servers at the ccTLD (for FREE).
- Then Richard Lamb like the idea and put the thinks together and working.

About TPM

- Crypto hardware FIPS-140.
- Supported by open source software.
- Speed: ~1 RSA 1024 sig/sec, but theoretically 10x
- Build in hardware RNG
- PKCS11 interface, simplified migration to HSM

TPM Trousers/opencryptoki Framework

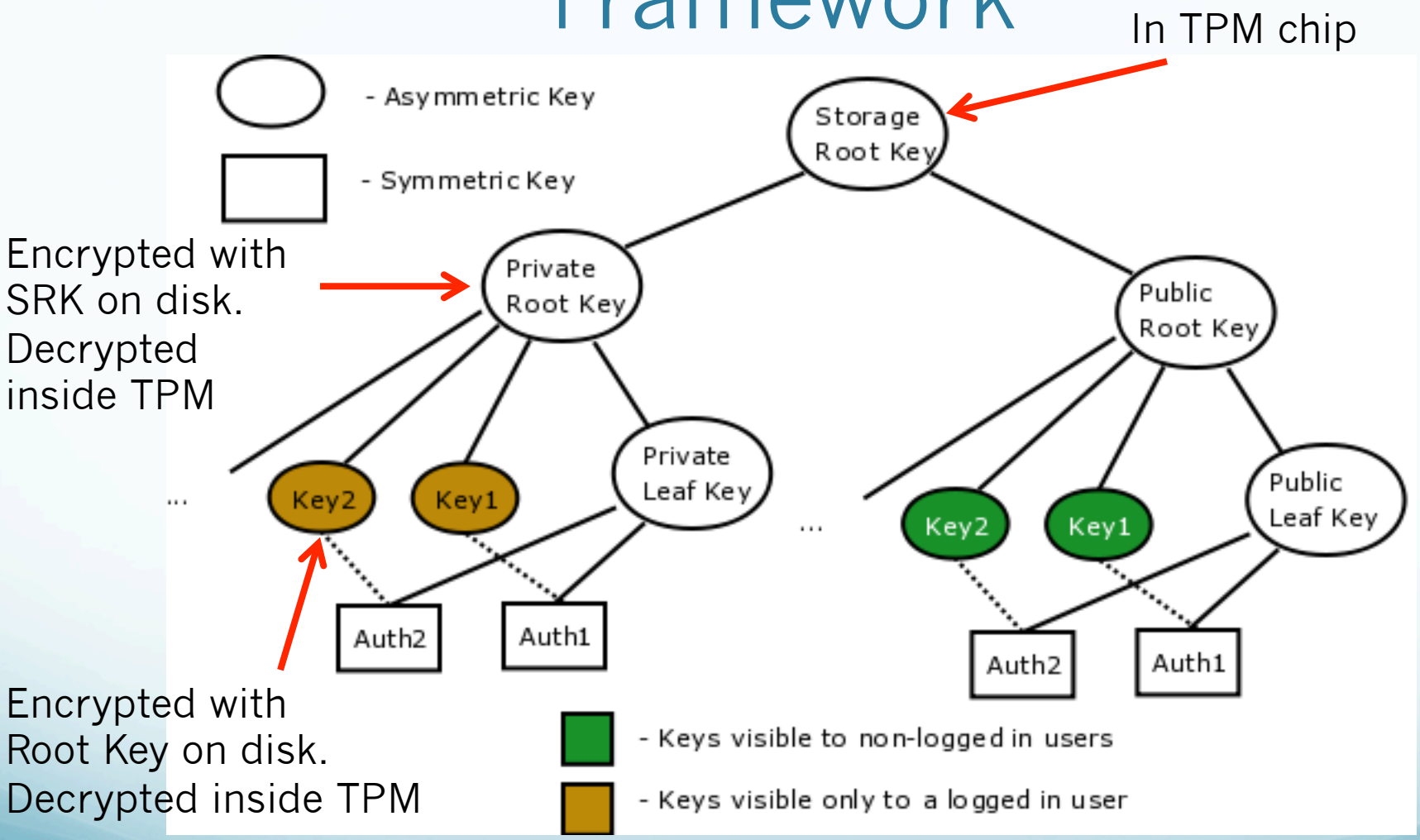

Diagram cortesy of Kent Yoder and Richard Lamb

First implementation (test env)

- Initialize TPM on BIOS
- The firsts tries unsuccessful. Slot 0 in tpm-tools not initialize.
- After too mucho work, it was possible to initialize with some tricks. The procedure should be rigorously.

```
pkcs11-tool --module /usr/lib/opencrytoki/libopencrytoki.so.0 --list-slots
Available slots:
Slot 0          Linux 2.6.32-33-generic-pae Linux (TPM)
  token label:   IBM PKCS#11 TPM Token
  token manuf:   IBM Corp.
  token model:   TPM v1.1 Token
  token flags:   rng, login required, token initialized, other flags=0x880040
  serial num  :  123
Slot 1          Linux 2.6.32-33-generic-pae Linux (Soft)
  token state:   uninitialized
```

Nov 19 2011 Production environment

- TPM Initialized and used for create ZSK and KSK for a small zone.
- sa.cr signed with DNSSEC:
  - KSK and ZSK generated inside server
  - pkcs11-backup (by Richard Lamb)
  - Opencryptoki configured to use tpmd (trousers)
- After a week of subzone resigns each hour with no errors, decide to sign all subzones and .cr TLD

Key Management

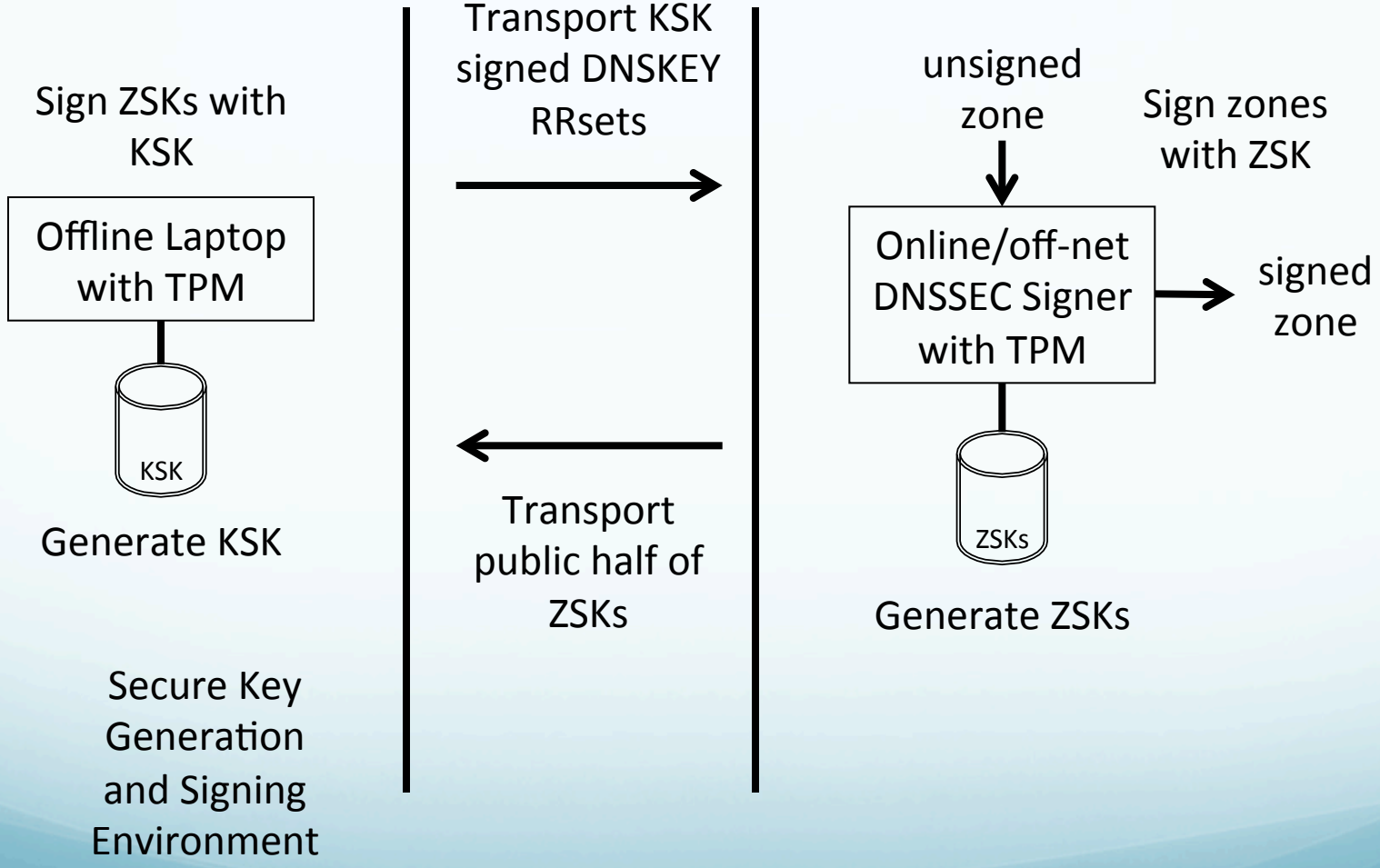

Diagram by Richard Lamb

TPM on BIOS


System
System Info
Processor Info
Memory Info
PCI Info
Date/Time
Boot Sequence
Drives
Onboard Devices
Video
Performance
Security
Admin Password
System Password
SATA-0 Password
SATA-1 Password
SATA-2 Password
Password Changes
TPM Security
TPM Activation
Execute Disable
Computrace(R)
Signed Firmware U
Power Management
TPM Security
Off
On
This field controls the TPM security device.
Off = TPM security device is Off
On = TPM security device is On
The factory default setting is Off

Results

- 8 different zones (all available)
  - .fi.cr, .go.cr, .ac.cr, .or.cr, .sa.cr, .co.cr, .ed.cr., .cr
- Near 400 signs each hour.
- 12.000 hours since start.
- 4.800.000 signs without errors in 1 year, 4 months
- About 15 minutes all signing process:
  - Sign of subzones, and sing of TLD
  - Sequential signing process
  - A little bit slow
- Did some test signing in parallel and it is increase the speed.

Conclusions

- For a small zone (or at least a few signed records) it is possible to use TPM in production environment.
- Very low cost and easy to access crypto hardware.
- It is enough reliable according with our probes.
- It is trusty enough (Ej. FIPS-140 level 2) to provide the initial phase for an HSM environment.
- TPM is not a cryptographic accelerator.

Questions?

More info:

DNSSEC support page of NIC-CR https://dnssec.nic.cr

diego@dibs.cr