DNSSEC with SmartcardHSM

Not as Easy as One Thinks

Eberhard W Lisse

Namibian Network Information Centre

2015-06-24

Introduction

Why?

- DNSSEC is Easy!
  - Is it Secure?
- Secure DNSSEC is Expensive!
  - Is it really?

So, what are we looking for?

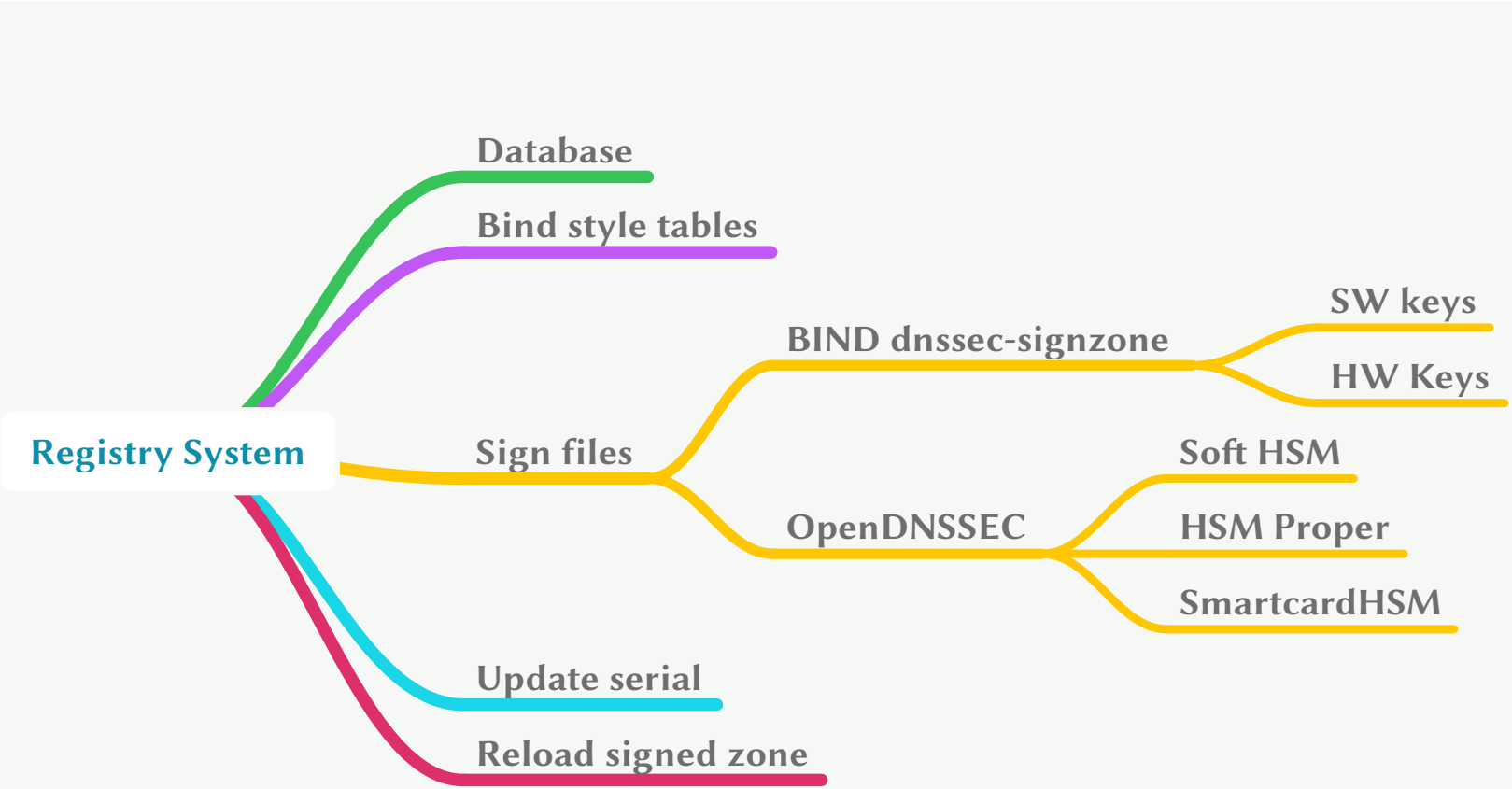
- Easy
  - off the shelf
- Secure
  - hardware based
- Cheap

Solution for

- small (cc)TLDs
- individual domains

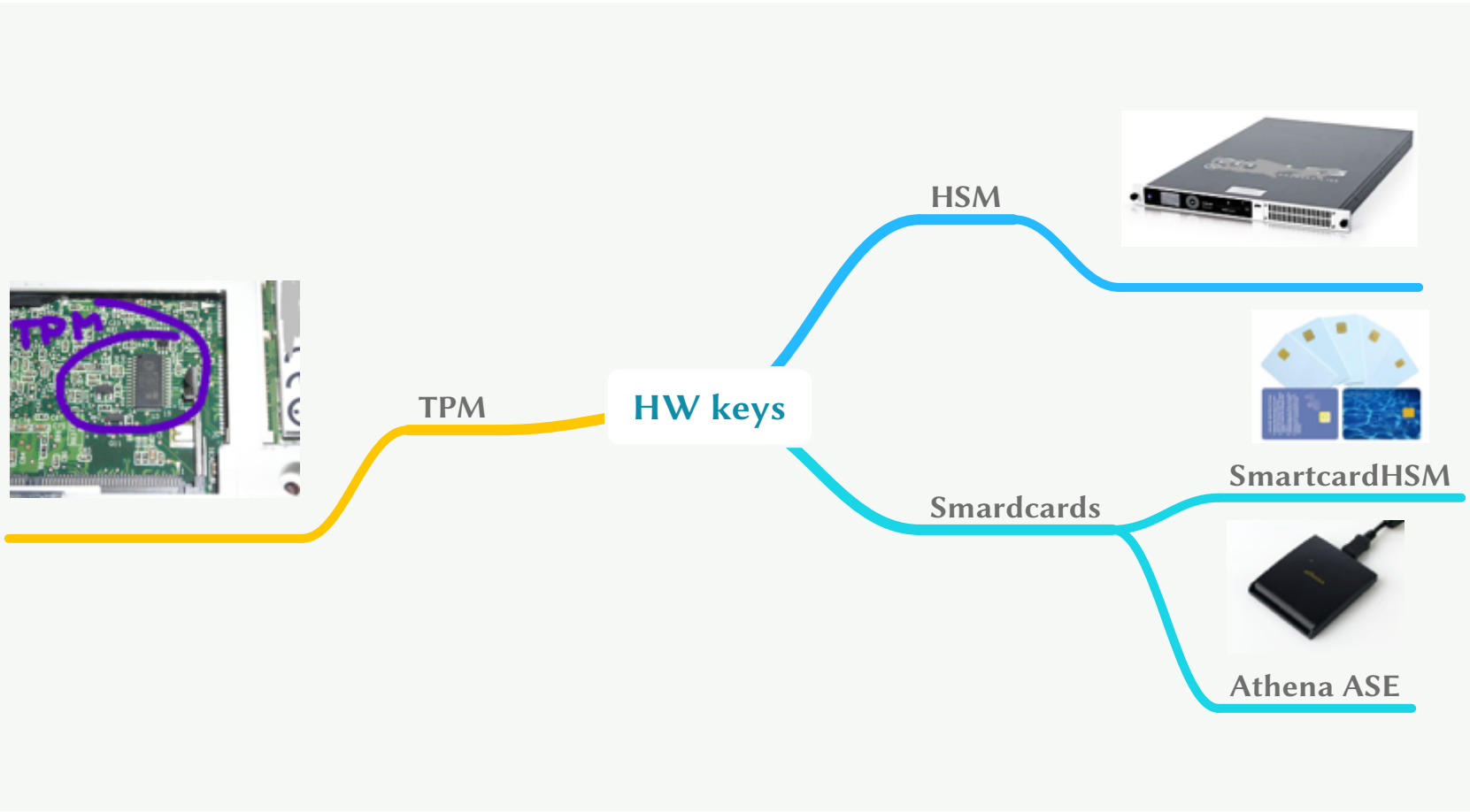
Workflow

Registry System with BIND



Hardware Keys

From the Esoteric to the Expensive



Smartcard

Many Brands

- SmartcardHSM
  - Linux and OS X
  - Key Signing Scripts
    - Rick Lamb
  - Flexible number of *Crypto Officers*
    - generate backup cards
  - Speed is not an issue
    - 2 signings per second = 7200 per hour (reload)

dnssec-signzone

BIND Needs a Patch

- Works quite well with a Software Key
  - Security Issue
- Requires a Patch for SmartcardHSM
  - Works well
    - Rick Lamb
  - Not in the repositories
    - manual re-patching of source after each update
    - does not scale
  - ISC has looked at it

openDNSSEC

Ubuntu 12.04 LTS and 14.04 LTS

- Special Repository
  - Maintainer: Ondřej Surý
- OpenSC
  - v0.14.0 (14.04 LTS)
  - v0.15.0 (source)
- pcscd
  - daemon to interface to the reader(s)
- Choice of Database
  - MySQL
  - SQLite3

- Nontrivial Configuration for SmartcardHSM
  - conf.xml
    - <TokenLabel>*SmartCard-HSM* (*UserPIN*)</TokenLabel>
  - pkcs15-tool -D
    - PKCS#15 Card [*SmartCard-HSM*]
    - PIN [*UserPIN*]
- Significant Learning Curve
  - short RRSIG <Validity> Interval

Conclusion

Not Ready for Prime Time Yet

- There were no hardware issues
  - Once inserted the cards were always visible if pcscd was working
- Significant software issues
  - pcscd stopped working all the time
    - different readers (different brands)
    - different cards (same brand)
    - cause not yet found
    - developers not yet contacted
  - openDNSSEC then failed to sign
    - short RRSIG Validity caused resolution to fail
  - heartbeat script resolved this to some extent
    - not acceptable for production

Back to the Drawing Board

PowerDNS to the Rescue?

- http://jpmens.net/2015/03/30/powerdns-with-a-smartcard-hsm-for-dnssec/
  - not yet studied
- Approach perhaps:
  - Stealth Server
    - on uncommon port
    - only accessible from local host
  - Notify Master on local host
    - which does AXFER of signed zone
- A number of CoCCA users seem to use OpenDNSSEC
  - Usually with SoftHSM
  - CoCCA has support for PowerDNS built in
    - Might just be what the doctor ordered...