DNSSEC Signer Implementation
Hardware

ICANN 43 Meeting, Costa Rica
12-16 March 2012
Luis Diego Espinoza,
Mario Guerra Araya,
Richard Lamb
Key Management

Offline Laptop with TPM

Generate KSK

Secure Key Generation and Signing Environment

Sign ZSKs with KSK

Transport KSK signed DNSKEY RRsets

Transport public half of ZSKs

Online/off-net DNSSEC Signer with TPM

unsigned zone

Sign zones with ZSK

signed zone

Generate ZSKs

Sign zones with ZSK

Generate ZSKs

Transport signed DNSKEY RRsets

Sign zones with ZSK

Signed zone
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**

- **PKCS11 spec**

- **DNSSEC Practice Statement (DPS)**
  - Spanish Draft
  - Original .SE [https://www.iis.se/dl/DPS-PA9-ENG.pdf](https://www.iis.se/dl/DPS-PA9-ENG.pdf)

- **Some source code**
  - Bind modifications
  - pkcs11 tools
Questions?