DNSSEC status in CZ.NIC

CZ.NIC
Ondřej Surý / *ondrej.sury@nic.cz*
8. 5. 2008

cz nic
cz domain registry

0.2.4.e164.arpa DNSSEC status

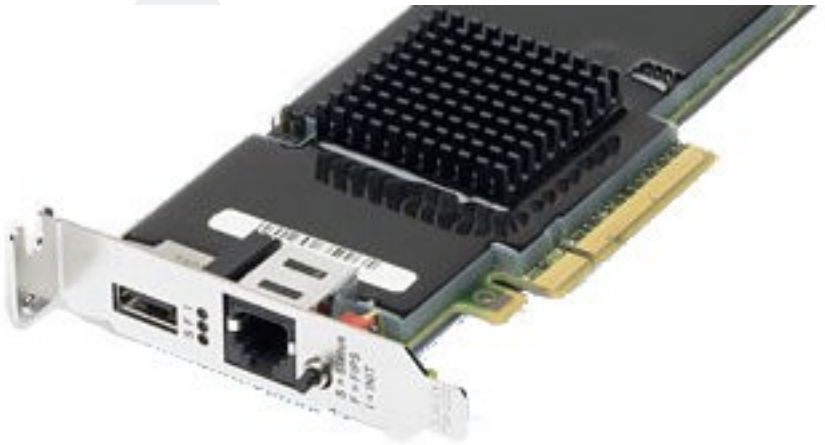
- First ENUM zone with DS records in e164.arpa :)
- Zone signed and DS records uploaded on Apr 28 2008
- Sign on every generation or weekly (what comes first)
- Using DISI tools
- Plan to switch to HSM signing after we make it work

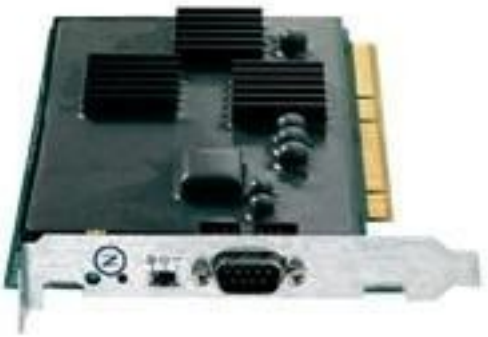
.cz DNSSEC status

- Nothing done yet
- Waiting for HSM

HSM – two cards in testing now

- Sun SCA6000 PCI card
  - ZSK storage and zone signing
- nCipher nShield F3-500
  - KSK storage and keys signing





Sun Crypto Accelerator 6000 PCIe

- Pros
  - Fast (13.000 RSA per sec)
  - Cheap (€ 1 150,00 list price)
  - FIPS 140-2 Level 3
- Cons
  - Solaris, RHEL 4 and SLES 9.x support only
  - Protected only by password
  - Few ciphers available (SHA1, RSA, ...)
- Status
  - dnssec-keygen can generate key
  - dnssec-signzone stuck on C_SignInit (CKR_OBJECT_HANDLE_INVALID)

nCipher nShield F3-500 PCI card

- Pros
  - Secure Card certificate storage, 4+-eye principle
  - FIPS 140-2 Level 3
  - More ciphers (SHA-1, SHA-2, RSA, DSA, ...)
  - More platforms supported (AIX, HP-UX, Linux, Windows)
- Cons
  - Slower
  - More expensive (€ 12 700,- list price)
- Status
  - We can use PKCS#11
  - dnssec-keygen and dnssec-signzone doesn't work yet

Future

- Near future – make HSM work
- Not-so-near future – .cz signed
- August 2008 – EPP interface testing
- September 2008 – production

Questions?