NASK

DNSSEC @ .PL

Selection of HSM solution

Krzysztof Olesik • Research and Academic Computer Network • ICANN 44TH Prague 27.06.2012

About NASK

- research institute
- data networks operator
- registry for .PL ccTLD
- CERT

DNSSEC - first approach

- launched in 2006 for 8.4.e164.arpa
- BIND, custom scripts, key stored on hard disk
- no automated management

DNSSEC - second approach

- main focus on security
- partial automation of key rollovers
- project history
  - September 2010 start of the project
  - 20th December 2011 .pl signed
  - 9th February 2012 DS published in root zone
  - 4th June 2012 Registry open for DS RRs

Prerequisites

- HSM only hardware
  - SoftHSM not good for production environment; good for tests
- Key management
  - BIND tools or HSM PKSC#11 tools plus in-house developed scripts
- Signer
  - Bind tool plus plus in-house developed scripts
  - OpenDNSSEC – lack of support for dynamic updates at that time
- Monitoring – zone consistency check
  - In-house developed scripts
  - There were lots of dnssec incidents due to bugs in scripts, solution design and DNSSEC software (still not mature)

HSM selection criteria

- Speed and Storage
- Supported algorithms
- Authorization (m of n)
- Import/export and backup capabilities
- Synchronization and clustering
- Software compatibility (key management & signing)
- **Support!**

Final decision

- many devices tested
  - PCI and network appliances
- **network appliance** most suitable for our needs
- DNS community feedback taken into account
- **SafeGuard® SecurityServer**

Things that matters

- Direct contact with a vendor of HSM
  - software simulator
  - trainings and installation assistance
  - software modifications on demand
  - wishlist taken into account when planning for new software and hardware releases
  - faster problem escalation
  - beta software releases to test
- Interest of Utimaco in DNSSEC as promise “we won't leave you behind”
  - web tutorials

… in return

- valuable feedback from DNS “industry”
  - usability
  - compatibility and
  - stability

Lessons learned

- read carefully all manuals and RFCs
- risk analysis greatly impact a solution design
- HSMs are “novelty” for many DNS admins, help of vendor’s experienced engineers is very important
- do security audits

NASK

Thank you