

.cz DNSSEC status

CZ.NIC

Ondrej Sury / *ondrej.sury@nic.cz*

09.04.2008

Summary

- Schedule
- Whitepaper document
- Encryption hardware in testing
- Signing in software in progress
- EPP changes
- Whois/Web whois
- Policies

Schedule

- January/February 2008 – start (gathering info, etc.)
- March 2008 – White Paper draft published
- April 2008 – White Paper final published
- May 2008 – July 2008 – internal testing
- August 2008 – testing instance for registrars
- September 2008 – DNSSEC launch

White Paper – target audience

- Contains general and technical information
- Target audience:
 - Employees
 - Registrars
 - Government
 - Interested public
- Comments are welcomed!!!

WP – what's in?

- General Introduction
- Implementation details
- Zone signing processes
- Initial policies

WP – General Intro

- Types of DNS threats explained (courtesy of RFC3833)
- DNSSEC explained
- DNSSEC in root zone (SIGN THE ROOT!)
- DLV explained
- Problems of DNSSEC

WP – Implementation details

- DNSSEC implementation
 - Changes in EPP protocol
 - KEYSET object proposal
 - New EPP functions
 - Modifications of existing EPP functions
 - Public interface modifications

WP – Zone signing and policies

- Key signing key(s)
- Zone signing key(s)
- Length of keys, algorithms used
- HSM usage – secure key store
- Key rotations
- Signature lifetime and rotation

EPP – KEYSET object

- One key could be used to sign more domains (zones)
- One key could be maintained by same person/company
- Keyset contains:
 - 1-<n> technical contacts
 - 1-<n> DS records
 - Common stuff (creation date, etc.)
- DS records contains:
 - Key tag
 - Algorithm, digest type
 - Digest (public fingerprint of key)

EPP – functions new & changed

- New functions

- check_keyset
- info_keyset
- create_keyset
- update_keyset
- transfer_keyset
- modify_keyset

- Modifications

- create_domain
- update_domain
- info_domain

Public Interface modifications

- Whois changes
- Web whois changes
- Website with DNSSEC description & explanation

DNSSEC – Sign the zone

- Signing the zone file is very simple
 - Generate some keys
 - Use `dnssec-signzone` to sign the zone
- Keeping it working is difficult!!!
 - DNSSEC introduces time and expiration
 - You need to resign zone regularly
 - You need to change keys regularly
- Policies are very important
 - How often you will change keys
 - How often you will sign the zone

Sign the zone – HSM module

- HSM – Hardware Security Module
 - Private part of the key is kept in the hardware
 - Strong security (four eyes principle, etc.)
- Changing KSK in root zone is time consuming process
 - Takes some time
 - If key is compromised – outage of the zone
 - NEVER allow your KSK to be compromised
- Low cost solution
 - Buy a notebook
 - Use it only for KSK/ZSK generation
 - Lock it in your safebox

HSM in .cz – KSK

- nCipher nShield F3
 - FIPS 140-2 Level 3 certified
 - Could be used for CA
 - Two boxes for failover
 - Performance not important
- PKCS#11 interface & libraries
- Supports:
 - Linux
 - Solaris, HP-UX, AIX
 - Windows Server
- Evaluation agreement signed

HSM in .cz - ZSK

- Sun Crypto Accelerator 6000
 - PCI card
 - Fast
 - Not so secure in terms of policies
 - Secure enough for signing the zone
- PCKS#11 interface
- Supports:
 - Linux (RHEL 4, SUSE)
 - Solaris
- One piece just arrived
 - Testing to start as soon as I get back

HSM in .cz – tools & random notes

- Modified BIND tools for PKCS#11
 - Courtesy of IANA
- IXFR mandatory
 - Zone files could grow very big
 - Time to update slaves grows as well
- Improve your monitoring
 - Check keys lifetimes
 - Check for valid signatures
 - Do checks in advance

Sign the zone – testing in software

- Generate keys (KSK & ZSK) offline
- Generate zone apex
 - Contains all keys signed by KSK
- Transfer ZSK keys and apex to your zone generator
 - (or) Transfer zone to your secure computer
 - Sign the zone
 - Publish the zone to DNS
- Be prepared to do all of this regularly

Implementation problems

- Long times of delivery
- Linux support limited
 - SCA 6000 card support only old version of RHEL 5
- Signing zone takes time
- Transferring zone takes time
- Once you start, there is no way back
 - Recursors get's configured, etc.
- Unless the root is signed, prepare how to distribute your key
 - Secure web page
 - DLV

Implementation problems

- NSEC2 allows zone walk
- NSEC3 just got published
 - Support in software needs to be stabilized
 - Need to investigate that yet

Various tools

- LDNS libraries and tools
 - Alternative implementation for NLNet Labs
 - Doesn't support PKCS#11 yet
- DNSSEC Key Management Tools
 - RIPE NCC
 - Deployment of Internet Security Extensions (DISI)

References

- RFC 3833: Threat Analysis of the Domain Name System.
- RFC 3766: Determining Strengths For Public Keys Used For Exchanging Symmetric Keys.
- RFC 4086: Randomness Requirements for Security.
- RFC 4641: DNSSEC Operational Practices.
- DNSSEC HOWTO, a tutorial in disguise.
http://www.nlnetlabs.nl/dnssec_howto/



Questions?