DNSSEC in .CZ

CZ.NIC z.s.p.o.
Jaromír Talíř
jaromir.talir@nic.cz
6. 5. 2009

cz nic
cz domain registry

Deployment Schedule

- January 2008 – start
- March 2008 – design ready
- March-April 2008 – community comment period
- April 2008 – signed 0.2.4.e164.arpa.
- August-September 2008 – registrars testing
- September 2008 – signed .cz
- **September 30, 2008** – production launch

DNSSEC solution (1/4)

- Significant registry modification to accept keys
- EPP extended for new primary object – KeySet
  - Container for DNSKEY records
  - Can be attached to domain
- Support sharing between domains
- Support multiple keys for easy key exchange
- Registration of KeySet is free

DNSSEC solution (2/4)

- Zone generation
  - Every 30 minutes
  - DS records generated from DNSKEY (SHA-1)
- DNSSEC keys
  - Generated using dnssec-keygen
  - ZSK (RSASHA1 - 1024 bits)
  - KSK (RSASHA1 - 2048 bits)

DNSSEC solution (3/4)

- Using Bind tool dnssec-signzone
- Increase in zone size, from 40MB to 180MB
- Transfering zone to 19 secondary locations
  - Memory and bandwidth problems
  - Solved with reusing signatures
  - Own scripts based on ldns tools
- Initial tests of HSM machine failed
  - Software bugs – working with ISC to resolve them

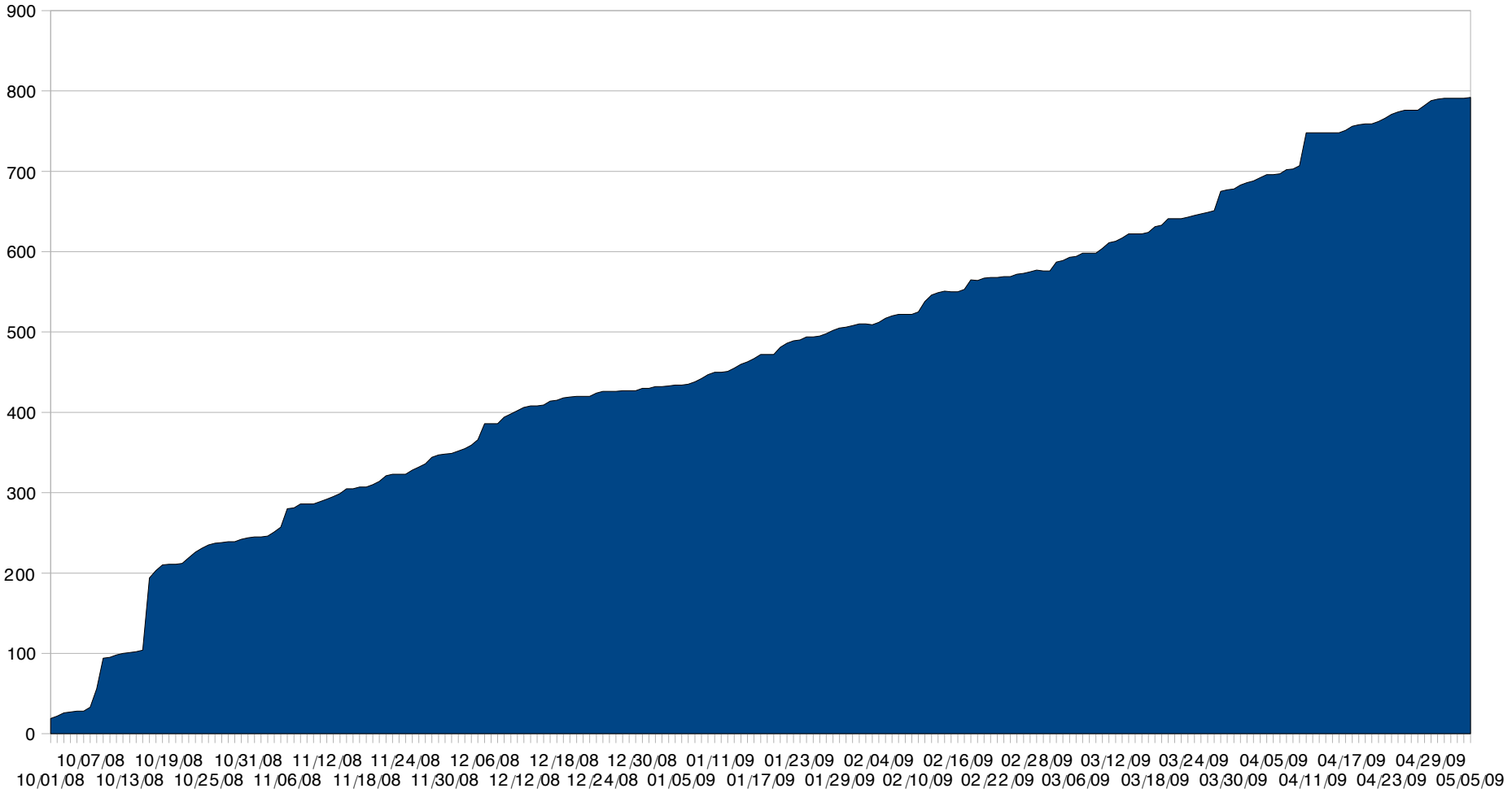
DNSSEC solution (4/4)

- Currently 4 ways of publishing of our keys
- Public key available on our web pages
- Mailing list for notification of changes
- DLV registry of ISC
- ITAR solution from IANA

Where are we now?

- 6 month in production
- 793 signed domains (0.14% of total 556 483)
- 10 registrars (out of total 49)
  - 6x 1-2 domains (just testing)
  - 2x 10-20 domains
  - 1x 83 domains (share 1 key)
  - 1x 649 domains (share 1 key)
- Several ISPs enabled validation

Signed domains



Evangelization

- Contacting important domain holders
- Success:
  - Biggest online bookstore - kosmas.cz
  - Popular IT news portals – lupa.cz, root.cz
- Promising:
  - eu2009.cz, one ministry, one bank
- Failure:
  - google.cz

Education

- CZ.NIC Academy project (started in 2008)
  - Training center for 20 people
- DNS and DNSSEC courses
  - Association members (registrars, ISPs...)
  - Governmental IT staff
  - Now open to public
- DNSSEC homepage (www.dnssec.cz)
  - DNSSEC setup wizard
  - Simple check of local resolver

File Edit View History Bookmarks Tools Help

http://www.dnssec.cz/

Nejnavštěvovan... FredTrac FredTickets PostgreSQL Daphne Fedora MFF

CONTACT SITE MAP Česky | English Search:

CZ NIC cz domain registry

DOMAINS REGISTRARS ABOUT US ENUM

ABOUT DNSSEC

DNSSEC is an extension to the DNS (domain name system), increasing the domain name service security. DNSSEC assures users that the information they obtain from DNS came from the correct source, was complete and its integrity was not compromised during the transfer. DNSSEC ensures that the DNS data can be trusted. Find more about DNSSEC on How DNSSEC works page.

WHY YOU NEED DNSSEC?

Although most internet services have the security features and users are used to use them, there is one security threat that not many people are aware of and where only DNSSEC is the solution to avoid it.

All internet services (e-mail, webpages, instant messaging, VoIP calling, ...) use domain name system (DNS). The main principle of it is DNS allows to use domain names in internet services addresses, as names are human readable and memorizable, instead of numbers, which are understood and useful for the computers. In reality whenever the user uses domain name address of any service (webpage, email address or other) the computer must translate it to numeric address to be able to connect to the service user wants to use. Find more about principles of DNS on "About domains and DNS page".

If someone is able to spoof numeric address, user will connect to a different place without any way to notice that and will not connect to expected service at all. It may work as shown on following scheme.

DNSSEC SECURITY TEST

Your computer is not secured by DNSSEC when accessing internet resources. You can become a victim of DNS attack. **You may connect to spoofed webpages or services when using domain names!** To lower this risk you should secure youself by DNSSEC. See DNSSEC wizard how to do it.

ENCRYPTION SWITCH

Click following link if you would like to turn on connection encryption of this page (ie. if you want to download DNSSEC key for .cz domain by a secure way).

Turn on SSL encryption

TECHNICAL INFORMATION

See CZ.NIC technical support pages (in czech only) for technical informations about DNSSEC:

Done

Questions?