DNSSEC in .CZ

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

5. 11. 2009

cz domain registry

Agenda

- Deployment schedule
- Solution description
- Current statistics
- Supporting projects

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

- Accepting keys from domain registrants
- Generating our own keys
- Zone file generation and signing
- Keys publishing

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)

- DNSSEC keys
  - Generated using dnssec-keygen
- ZSK
  - RSASHA1 - 1024 bits
  - Rollover every 3 month - using ZKT
- KSK
  - RSASHA1 - 2048 bits
  - Rollover every 2 years
  - No rollover yet – waiting for root signed

DNSSEC solution (3/4)

- Zone generation every 30 minutes
  - DS records generated from DNSKEY (SHA-1)
- Signed using BIND dnssec-signzone
  - NSEC
  - Signatures valid for 14 days
- Transfering zone to 19 secondary locations
  - Memory and bandwidth problems
  - Solved with reusing signatures
- HSM integration on the way

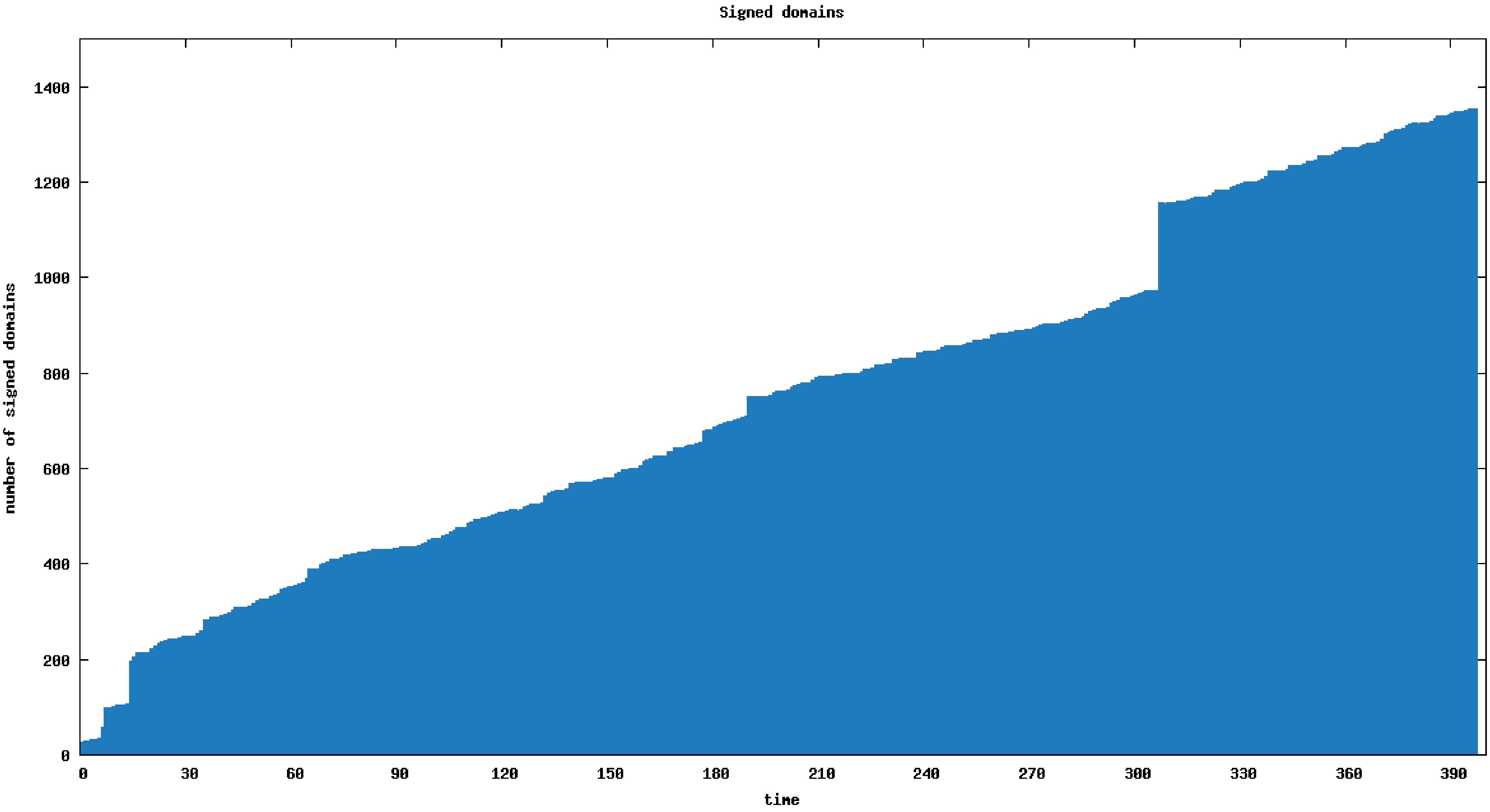
DNSSEC solution (4/4)

- 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

Statistics

- Daily graph of number of signed domains
- Registrars and signed domains
- Keysets sharing and DNSSEC hosting
- Interesting signed domains/registrants

Statistics – signed domains



Statistics - registrars

Registrar	Domains	Signed	Keysets
INTERNET CZ, a.s.	149649	31	26
IGNUM, s.r.o.	105637	103	6
ACTIVE 24, s.r.o.	104794	1159	9
ZONER software, a. s.	57231	3	2
GENERAL REGISTRY, s.r.o.	50448	14	12
Media4Web s.r.o	34584	3	3
Web4U s.r.o.	20256	5	2
Gransy s.r.o.	15217	7	1
...	...	...	...
40	616056	1363	81

Statistics - keysets

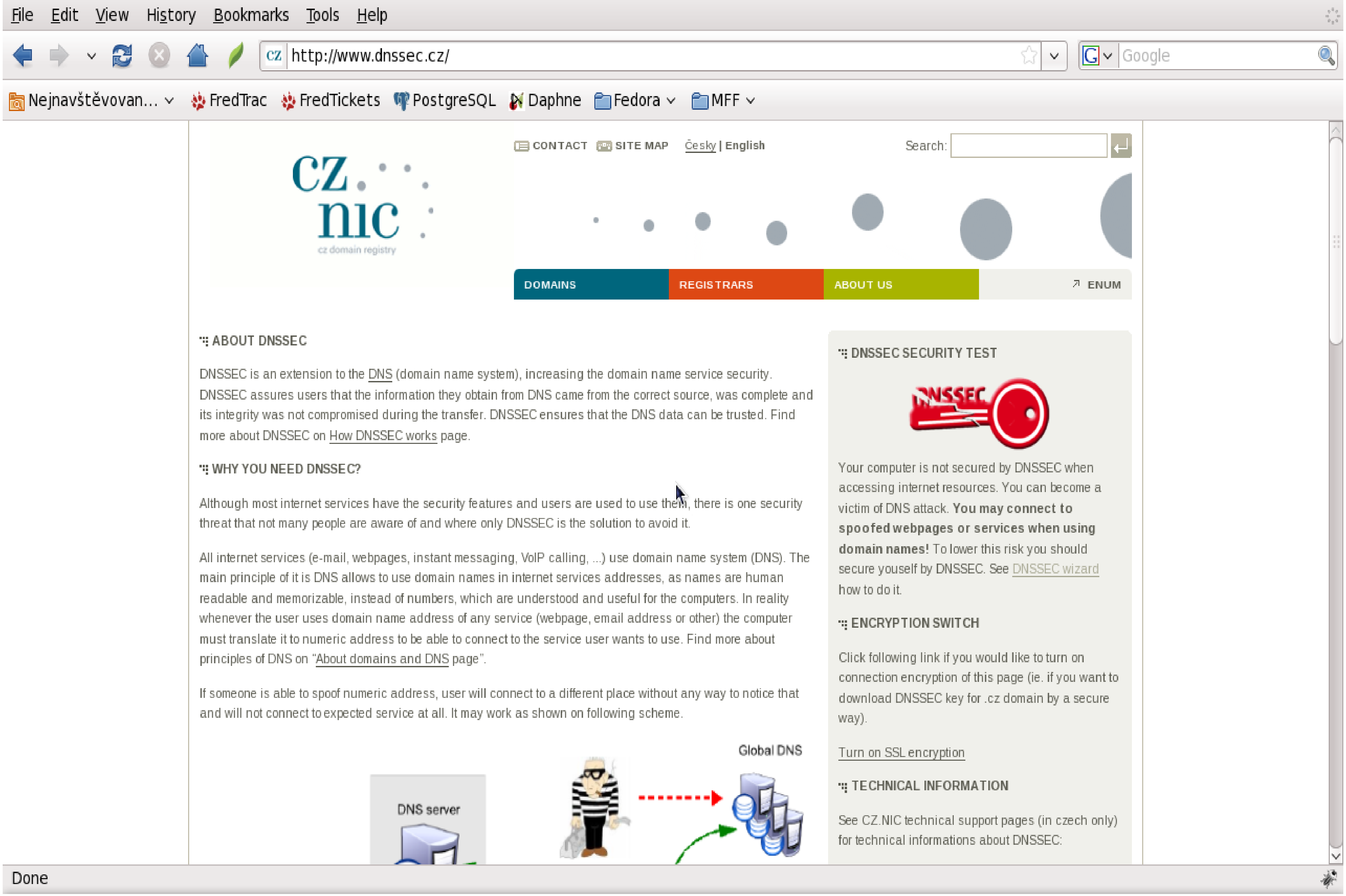
Number of keysets	Having this number of domains
1	1203
1	72
1	6
1	3
2	2
75	1

Statistics – domain registrants

- Online bookstore
  - kosmas.cz
- News portals
  - ihned.cz, lidovky.cz, lupa.cz
- Bank
  - hypotecnibanka.cz
- Government
  - eu2009.cz

Supporting projects

- Web page with resolver test
  - http://www.dnssec.cz
  - Importing CSS style from badly signed domain
- Firefox DNSSEC plugin
  - CZ.NIC Labs project http://labs.nic.cz
  - Linux, MacOS, Windows versions
- DNSSEC hardware tester
  - http://www.dnstester.cz
  - Desktop application + Web result browser


File Edit View History Bookmarks Tools Help
http://www.dnssec.cz/
Google
Nejnavštěvovan… FredTrac FredTickets PostgreSQL Daphne Fedora MFF
CONTACT SITE MAP Česky | English
Search:
cz nic
cz domain registry
DOMAINS REGISTRARS ABOUT US ENUM
DNSSEC
DNS server
Global DNS
Done

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.

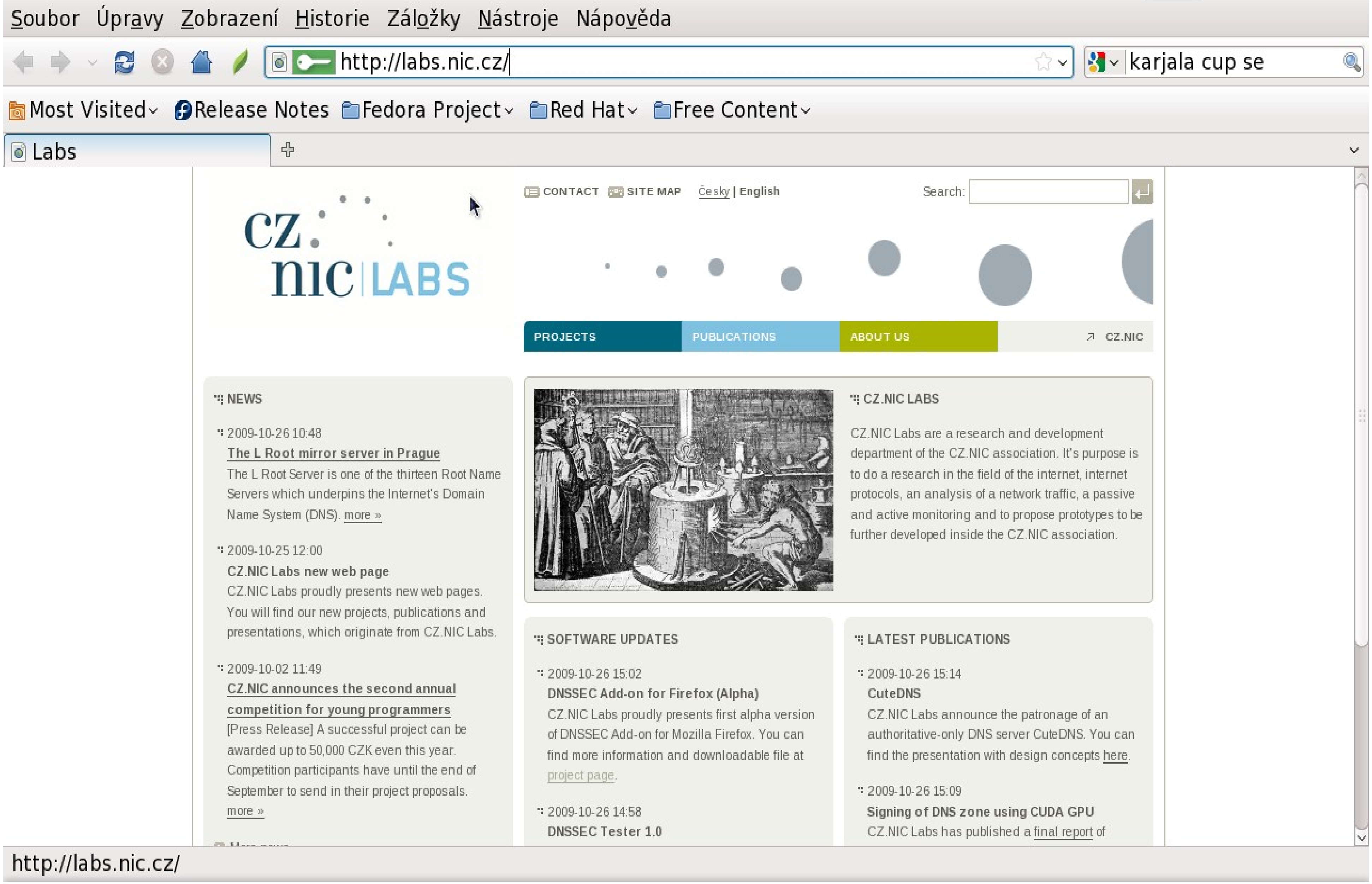
ENCRYPTION SWITCH

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:



CONTACT SITE MAP Česky | English Search:

CZ.NIC LABS

PROJECTS PUBLICATIONS ABOUT US CZ.NIC

NEWS

2009-10-26 10:48
The L Root mirror server in Prague
The L Root Server is one of the thirteen Root Name Servers which underpins the Internet's Domain Name System (DNS). more »

2009-10-25 12:00
CZ.NIC Labs new web page
CZ.NIC Labs proudly presents new web pages. You will find our new projects, publications and presentations, which originate from CZ.NIC Labs.

2009-10-02 11:49
CZ.NIC announces the second annual competition for young programmers
[Press Release] A successful project can be awarded up to 50,000 CZK even this year. Competition participants have until the end of September to send in their project proposals. more »

More news

CZ.NIC LABS

CZ.NIC Labs are a research and development department of the CZ.NIC association. It's purpose is to do a research in the field of the internet, internet protocols, an analysis of a network traffic, a passive and active monitoring and to propose prototypes to be further developed inside the CZ.NIC association.

SOFTWARE UPDATES

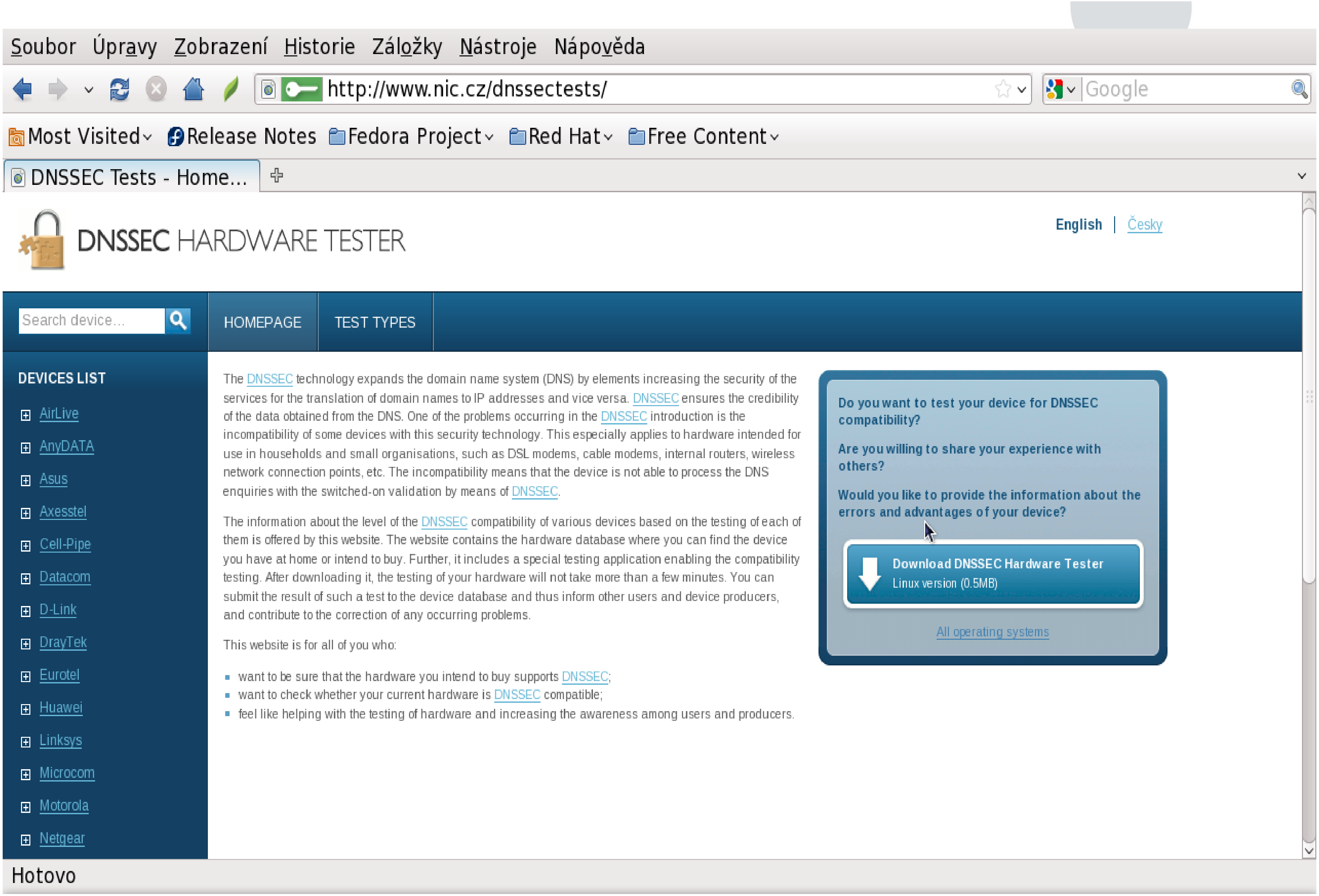
2009-10-26 15:02
DNSSEC Add-on for Firefox (Alpha)
CZ.NIC Labs proudly presents first alpha version of DNSSEC Add-on for Mozilla Firefox. You can find more information and downloadable file at project page.

2009-10-26 14:58
DNSSEC Tester 1.0

LATEST PUBLICATIONS

2009-10-26 15:14
CuteDNS
CZ.NIC Labs announce the patronage of an authoritative-only DNS server CuteDNS. You can find the presentation with design concepts here.

2009-10-26 15:09
Signing of DNS zone using CUDA GPU
CZ.NIC Labs has published a final report of



DNSSEC HARDWARE TESTER

The DNSSEC technology expands the domain name system (DNS) by elements increasing the security of the services for the translation of domain names to IP addresses and vice versa. DNSSEC ensures the credibility of the data obtained from the DNS. One of the problems occurring in the DNSSEC introduction is the incompatibility of some devices with this security technology. This especially applies to hardware intended for use in households and small organisations, such as DSL modems, cable modems, internal routers, wireless network connection points, etc. The incompatibility means that the device is not able to process the DNS enquiries with the switched-on validation by means of DNSSEC.

The information about the level of the DNSSEC compatibility of various devices based on the testing of each of them is offered by this website. The website contains the hardware database where you can find the device you have at home or intend to buy. Further, it includes a special testing application enabling the compatibility testing. After downloading it, the testing of your hardware will not take more than a few minutes. You can submit the result of such a test to the device database and thus inform other users and device producers, and contribute to the correction of any occurring problems.

This website is for all of you who:

- want to be sure that the hardware you intend to buy supports DNSSEC;
- want to check whether your current hardware is DNSSEC compatible;
- feel like helping with the testing of hardware and increasing the awareness among users and producers.

Do you want to test your device for DNSSEC compatibility?

Are you willing to share your experience with others?

Would you like to provide the information about the errors and advantages of your device?

Thank You!
and
Questions?