DNSSEC Validator

CZ.NIC Labs
Ondřej Surý
ondrej.sury@nic.cz
6 May 2010

cz domain registry

Motivation

- DNSSEC is invisible:
  - to end user
  - to domain holder
- Idea came up when using ASnumber Add-On
  - Shows ASN and some more info
  - Credits to the clone Ondrej
  - Coding by Zbynek Michl @ CZ.NIC Labs

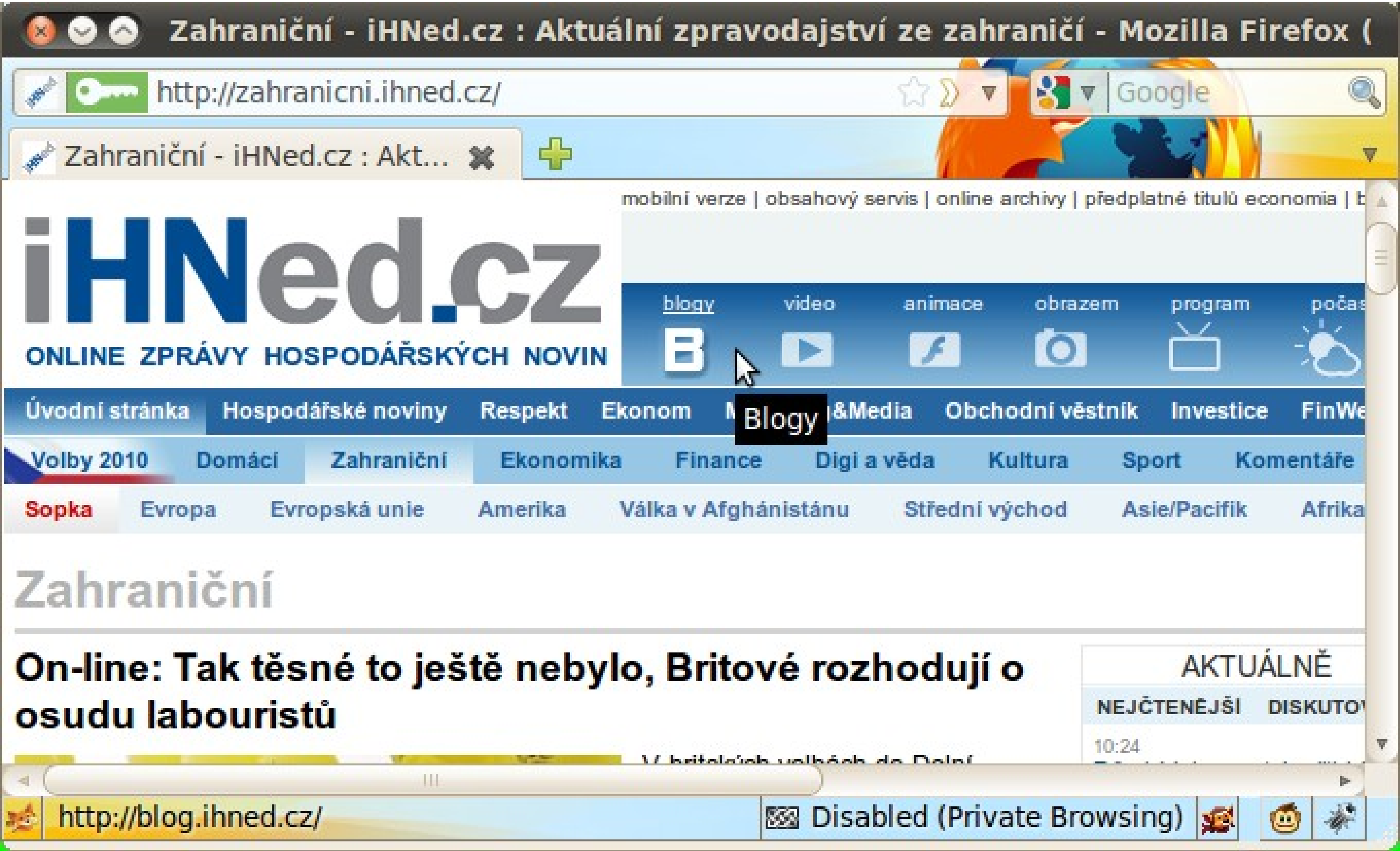
DNSSEC Validator

- Mozilla Firefox Add-On
- Four visible DNSSEC states:
  - Green Key – validated (AD)
  - Orange Key – could validate (RRSIG, no AD)
  - Red Key – validation failure (invalid RRSIG)
  - No Key – no DNSSEC (no RRSIG, no AD)

Visualisation of DNSSEC

- Show DNSSEC validation status
  - Just for the URL
  - Doesn't check links on the page
- Not meant as **security** tool
  - Doesn't check for nested pages, frames, etc.

RIPE 60 has validating resolvers!



Zahraniční - iHNed.cz : Aktuální zpravodajství ze zahraničí - Mozilla Firefox (

http://zahranicni.ihned.cz/

Zahraniční - iHNed.cz : Akt...

mobilní verze | obsahový servis | online archivy | předplatné titulů economia | b

iHNed.cz

ONLINE ZPRÁVY HOSPODÁŘSKÝCH NOVIN

blogy video animace obrazem program počas

Úvodní stránka | Hospodářské noviny | Respekt | Ekonom | M Blogy &Media | Obchodní věstník | Investice | FinWe

Volby 2010 | Domácí | Zahraniční | Ekonomika | Finance | Digi a věda | Kultura | Sport | Komentáře

Sopka | Evropa | Evropská unie | Amerika | Válka v Afghánistánu | Střední východ | Asie/Pacifik | Afrika

Zahraniční

On-line: Tak těsné to ještě nebylo, Britové rozhodují o osudu labouristů

AKTUÁLNĚ

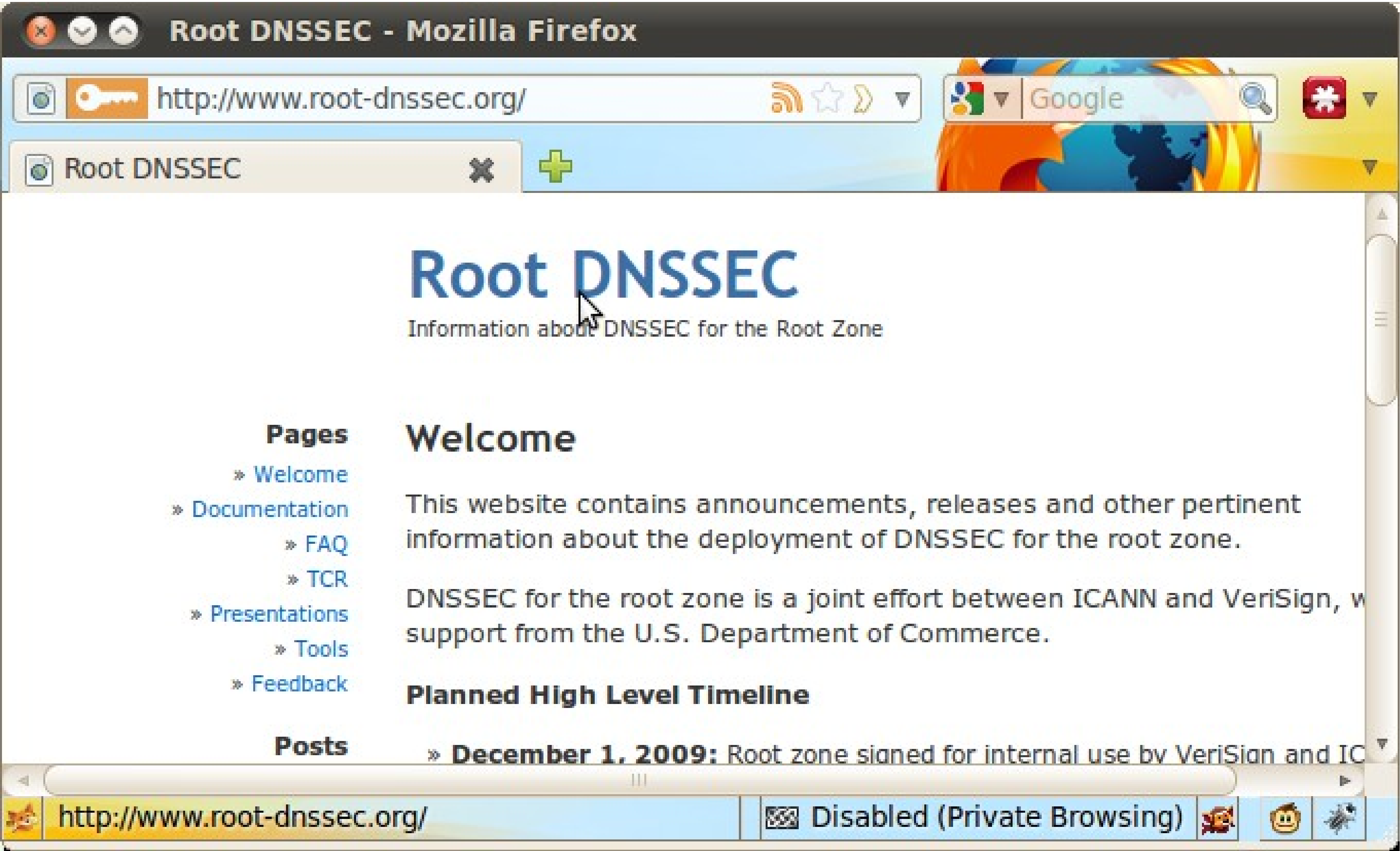
NEJČTENĚJŠÍ DISKUTO

10:24

http://blog.ihned.cz/

Disabled (Private Browsing)

RIPE resolver can't do NSEC3



Root DNSSEC

Information about DNSSEC for the Root Zone

Pages

» Welcome
» Documentation
» FAQ
» TCR
» Presentations
» Tools
» Feedback

Posts

Welcome

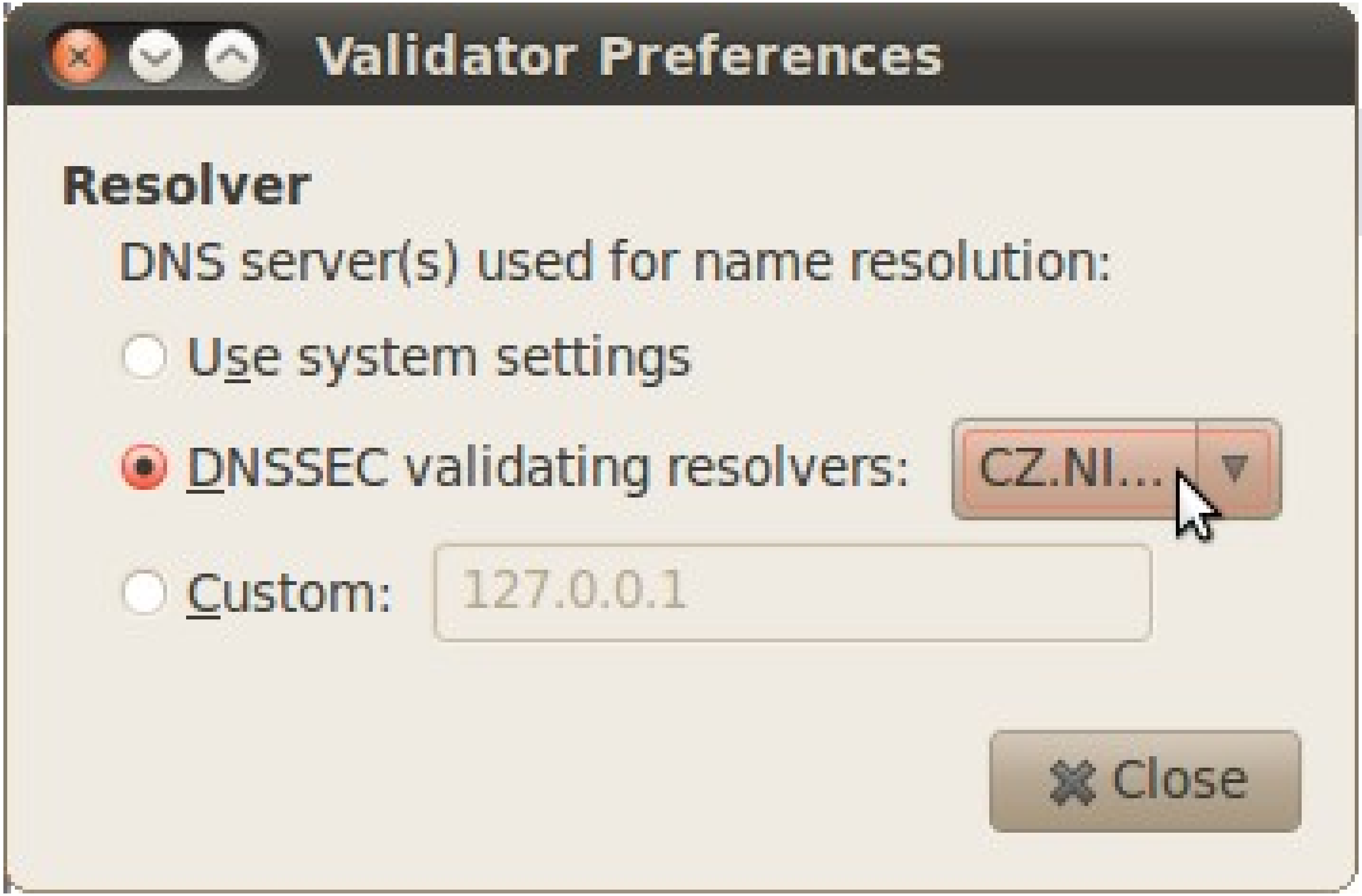
This website contains announcements, releases and other pertinent information about the deployment of DNSSEC for the root zone.

DNSSEC for the root zone is a joint effort between ICANN and VeriSign, w support from the U.S. Department of Commerce.

Planned High Level Timeline

» **December 1, 2009:** Root zone signed for internal use by VeriSign and IC

But you can use ours



Validator Preferences

Resolver

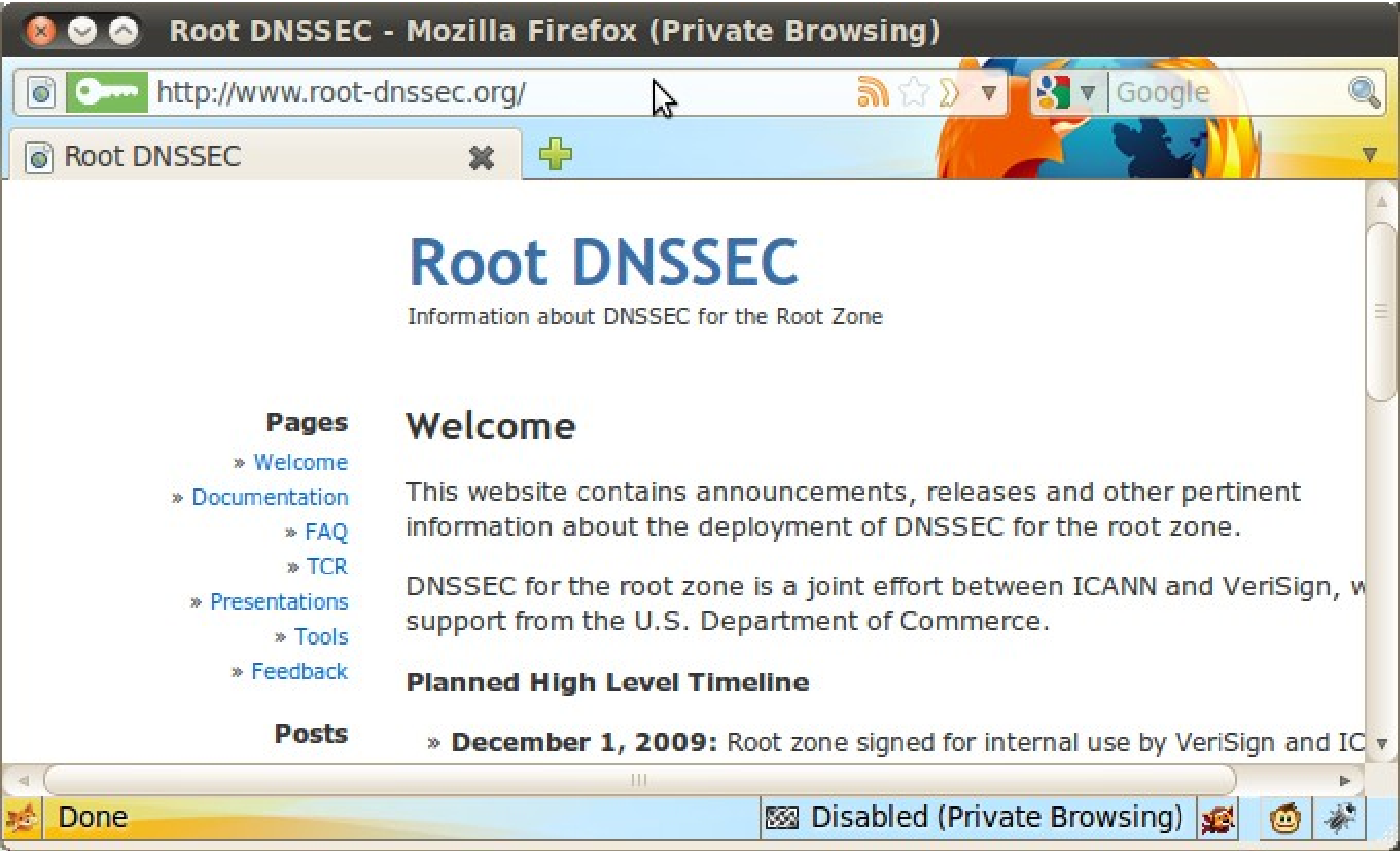
DNS server(s) used for name resolution:

○ Use system settings

● DNSSEC validating resolvers: CZ.NI... ▼

○ Custom: 127.0.0.1

Green Key is better, isn't it?



Root DNSSEC - Mozilla Firefox (Private Browsing)
http://www.root-dnssec.org/
Google
Root DNSSEC
Done
Disabled (Private Browsing)

Root DNSSEC

Information about DNSSEC for the Root Zone

Pages

- » Welcome
- » Documentation
- » FAQ
- » TCR
- » Presentations
- » Tools
- » Feedback

Posts

Welcome

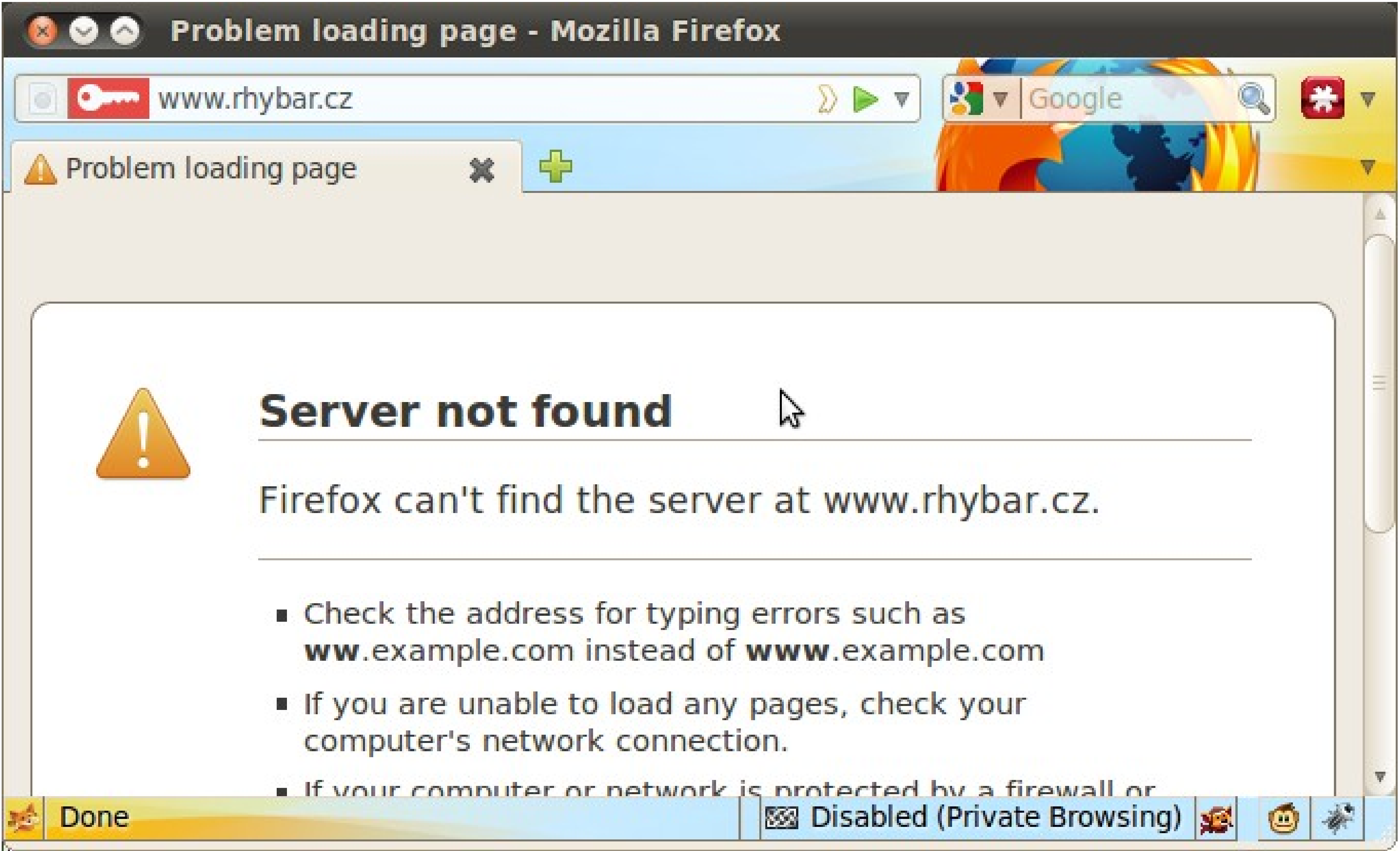
This website contains announcements, releases and other pertinent information about the deployment of DNSSEC for the root zone.

DNSSEC for the root zone is a joint effort between ICANN and VeriSign, w support from the U.S. Department of Commerce.

Planned High Level Timeline

- » **December 1, 2009:** Root zone signed for internal use by VeriSign and IC

Does your ISP do DNSSEC?



Problem loading page - Mozilla Firefox

www.rhybar.cz

Problem loading page

Server not found

Firefox can't find the server at www.rhybar.cz.

- Check the address for typing errors such as **ww**.example.com instead of **www**.example.com
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or

Done

Disabled (Private Browsing)

No support :-(– use own DNS

- CZ.NIC ODVR
  - ITAR Trust Anchors
  - Unbound

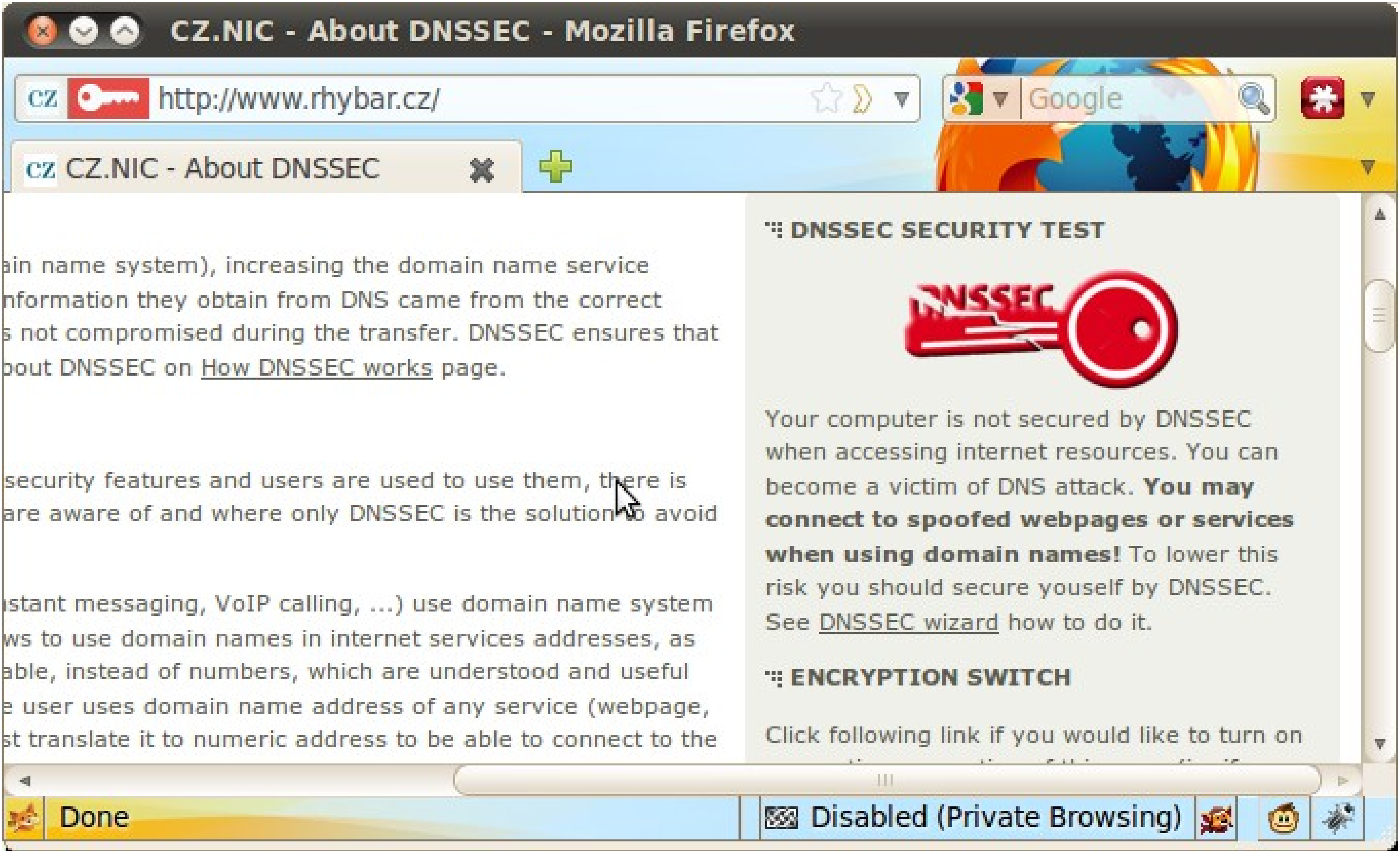
    nameserver 217.31.204.130

    nameserver 2001:1488:800:400::130
  - Bind 9

    nameserver 217.31.204.131

    nameserver 2001:1488:800:400::131
  - Webpage in progress

You get “some” security


CZ.NIC - About DNSSEC - Mozilla Firefox
http://www.rhybar.cz/
Google
CZ.NIC - About DNSSEC
Done
Disabled (Private Browsing)

ain name system), increasing the domain name service
nformation they obtain from DNS came from the correct
s not compromised during the transfer. DNSSEC ensures that
bout DNSSEC on How DNSSEC works page.

security features and users are used to use them, there is
are aware of and where only DNSSEC is the solution to avoid

istant messaging, VoIP calling, ...) use domain name system
ws to use domain names in internet services addresses, as
able, instead of numbers, which are understood and useful
e user uses domain name address of any service (webpage,
st translate it to numeric address to be able to connect to the

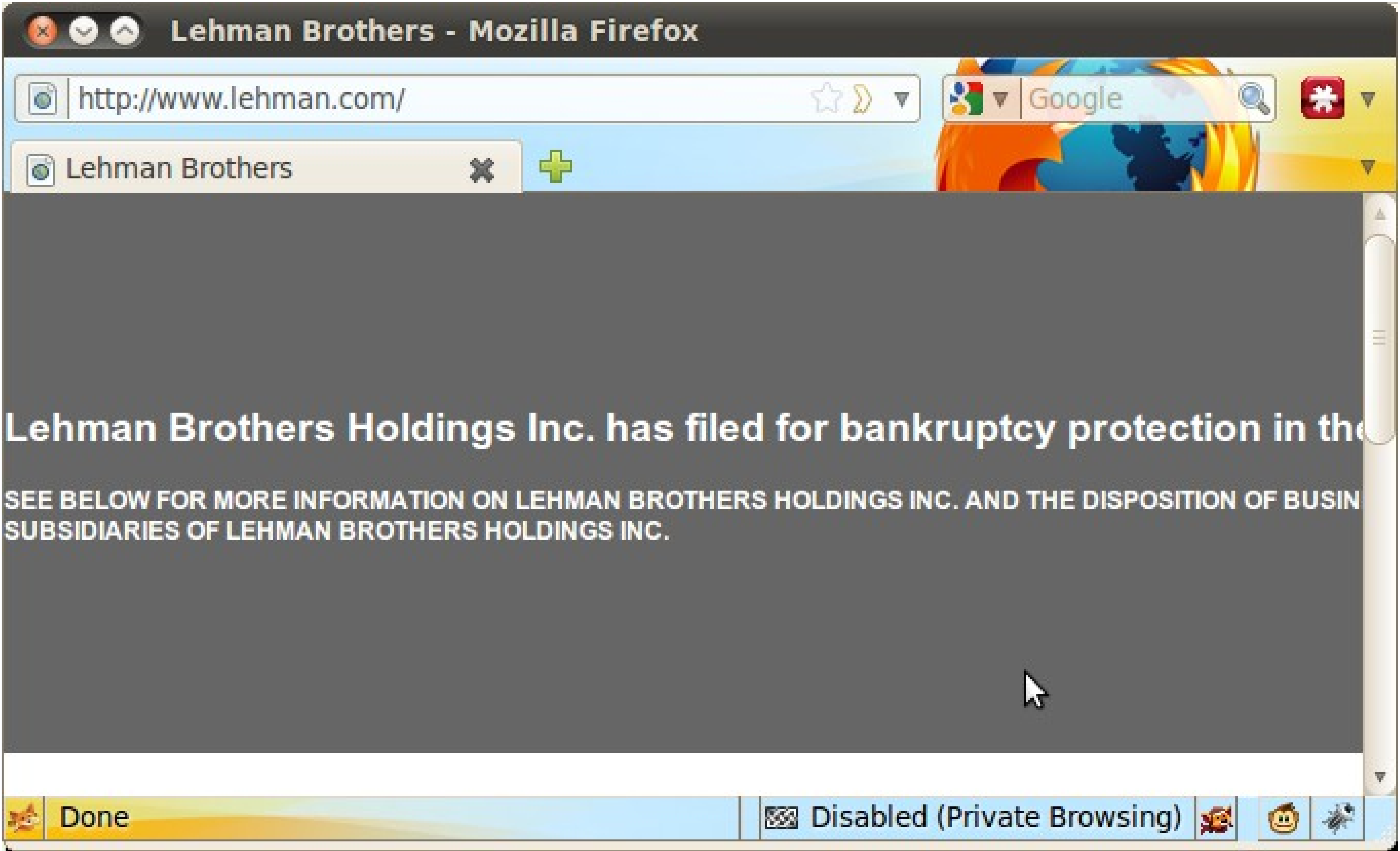
DNSSEC SECURITY TEST

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

No security at all



Lehman Brothers - Mozilla Firefox
http://www.lehman.com/
Google
Lehman Brothers
Done
Disabled (Private Browsing)

Lehman Brothers Holdings Inc. has filed for bankruptcy protection in the

SEE BELOW FOR MORE INFORMATION ON LEHMAN BROTHERS HOLDINGS INC. AND THE DISPOSITION OF BUSIN
SUBSIDIARIES OF LEHMAN BROTHERS HOLDINGS INC.

Where to get it?

- Nice new shiny webpage
  - http://www.dnssec-validator.cz/
- Add-ons for Firefox (https://addons.mozilla.org/)
  - Search for DNSSEC
  - Or go to: http://bit.ly/aWHguB
  - Still in sandbox, waiting for review

Technical background

- Written in C (XPCOM), XUL, JavaScript, CSS.
- Uses bundled ldns, openssl
  - Found some issues in ldns
- Hidden configuration
  - about:config
- Developer Info:
  - https://labs.nic.cz/dnssec/
- Bug reports to:
  - dnssec-validator@nic.cz

Known issues in 0.15.1

- Windows XP need msvcr90.dll
  - Microsoft Visual C++ 2008 Redistributable Package
  - http://bit.ly/6wTQ
- Validation status cache
  - Shared between tabs
  - Not shared between windows

Questions?