DNSSEC Validátor - doplněk prohlížečů proti podvržení domény

CZ.NIC z.s.p.o.

Martin Straka / martin.straka@nic.cz

Konference Internet a Technologie 12

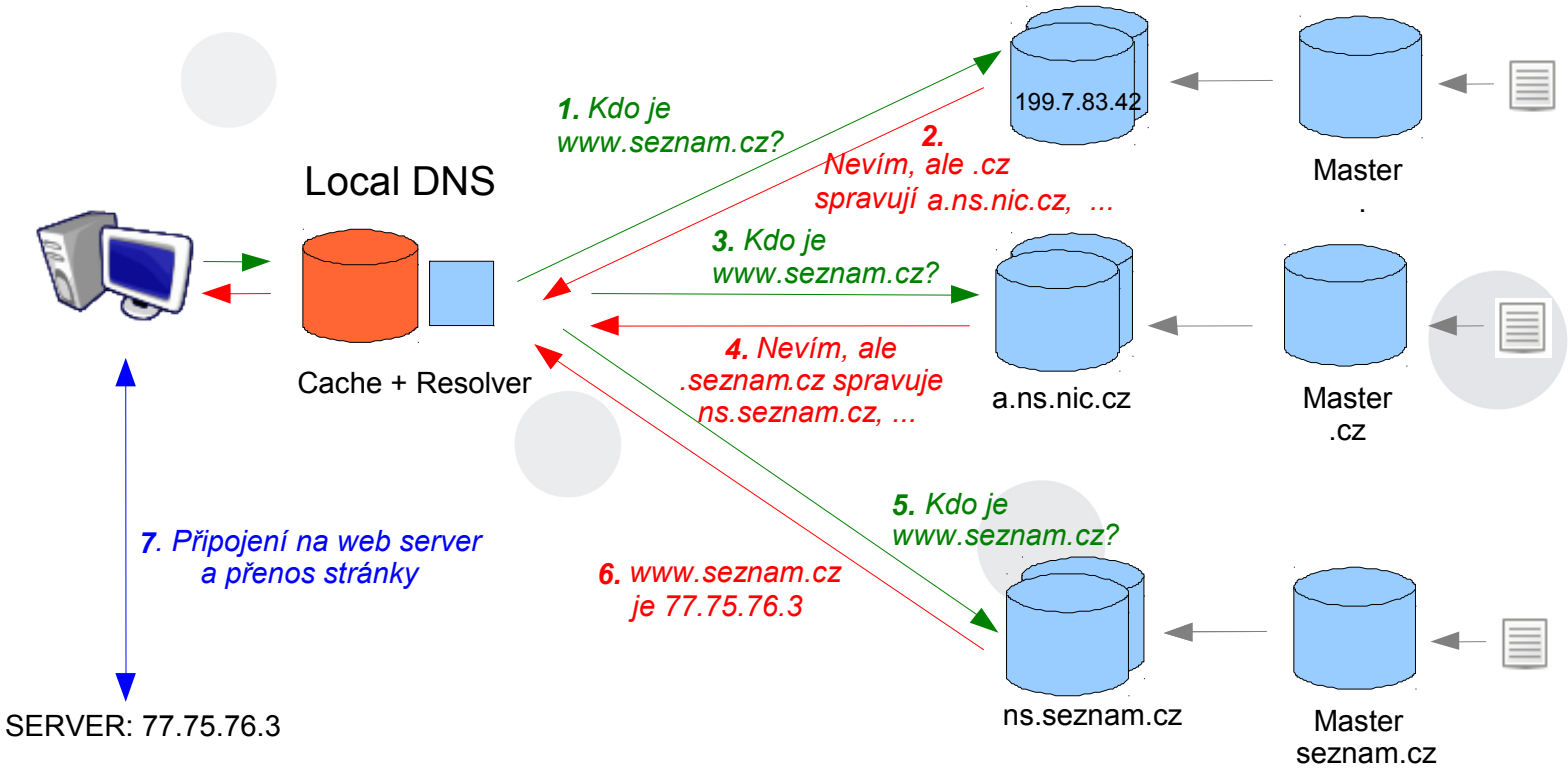
24.11.2012

Obsah prezentace

- Stručný úvod do DNS
- Něco málo o DNSSEC
- DNSSEC Validátor pro internetové prohlížeče
- Závěr a další možná rozšíření

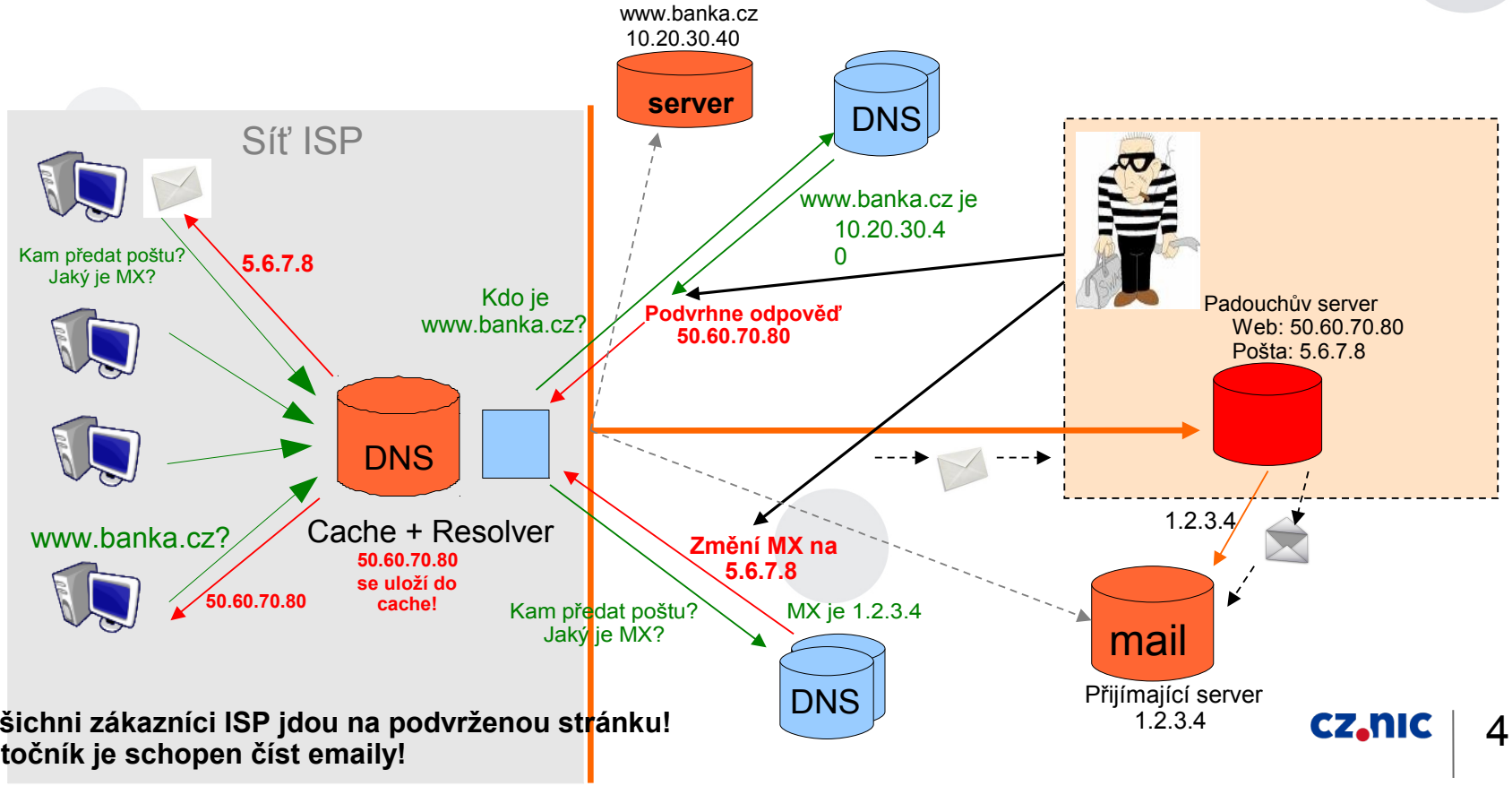
DNS

- Nedílnou součástí internetové infrastruktury.
- Zajišťuje překlad doménových jmen na IP adresy.
- Decentralizovaná hierarchická databáze.
- Komunikace: dotaz – odpověď, nezabezpečený protokol.



Zranitelnost DNS

- Nezabezpečené odpovědi v textové podobě.
- Útočník může podvrhnout obsah DNS odpovědi (např. IP adresu).
- Uživatel netuší, že jde na podvrženou stránku | nežádoucí přesměrování emailu.



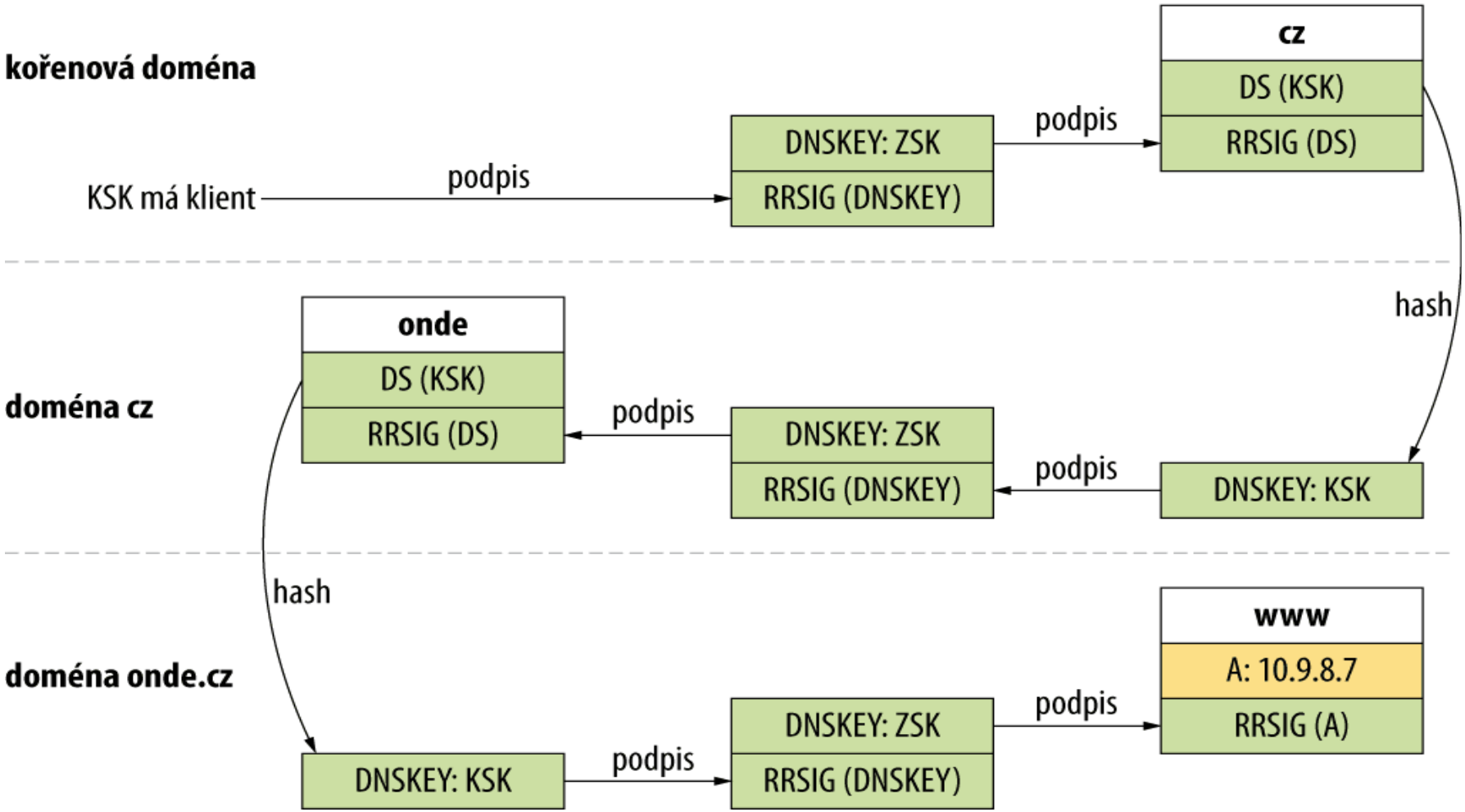
DNSSEC a DNS

- DNSSEC není náhrada za DNS, pouze DNS rozšiřuje.
- Zajišťuje důvěryhodnost získaných záznamů, kontrola pravosti dat.
- Přidává do DNS digitální podpisy.
  - asymetrická kryptografie.
    - **soukromý klíč,** kterým si držitel podepíše záznamy, které o své doméně do DNS vkládá.
    - **veřejný klíč,** kterým je pak možno ověřit pravost podpisu všech záznamů v odpovědi.
- Veřejné klíče a jejich otisky jsou uloženy v DNS záznamech.
- Nové typy DNS záznamů a příznaků.
  - RRSIG – obsahuje digitální podpis příslušných DNS záznamů.
  - DNSKEY – veřejný klíč určený k ověření podpisu dat.
  - DS – delegace otisku veřejného klíče do nadřazené zóny (řetězec důvěry).
  - NSEC/3 – pro informaci o neexistenci dotazovaného záznamu.
  - nový příznak AD v hlavičce DNS odpovědi; v dotazu pak DO a CD.

Jak DNSSEC funguje?

- Resolvery ověřují validitu DNSSEC podpisů a poskytují důvěryhodné odpovědi na DNS dotazy (příznak AD v odpovědi).
- Musí být definován aspoň jeden „pevný bod důvěry“
  - veřejný klíč nebo otisk klíče (hash), kterému důvěřujeme, musí být získán bezpečnou cestou.
  - dnes - kořenová zóna – stačí jeden DS záznam.
- Řetězec důvěry – sekvence ověřených DNSSEC záznamů (DNSKEY a DS) vedoucí od pevného bodu důvěry k vlastní validaci podpisu získaných dat (např. ověření RRSIG pro A záznam).
- V každé úrovni doménového stromu máme ověřená data.
- Klient, používající validující resolver tak získává důvěryhodná a nezměněná data (příznak AD v DNS odpovědi).
- První verze DNSSEC - 1999 – publikováno v RFC2535.

DNSSEC – řetězec důvěry



Proč DNSSEC Validátor?

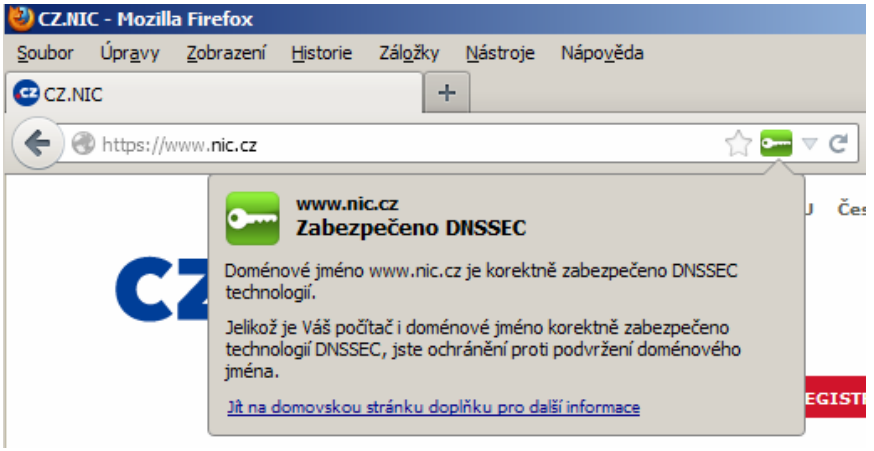
- DNS i DNSSEC je skrytý pro běžného uživatele.
- Internetové prohlížeče jsou hojně používané pro interpretaci informací a zobrazování HTML stránek ze sítě Internet.

- Prohlížeč neposkytuje uživateli informaci o tom, jestli obdržel správnou IP adresu cílového serveru a zda-li se připojuje na správný zdroj informací.
- Uživatel se může díky podvrženým záznamům v DNS odpovědi dostat na jiné služby (stránky), aniž by cokoliv tušil nebo byl upozorněn.
  - Problém: internetové obchody, platby kartou na internetu, emaily s důležitými informacemi, atd...

- Možné řešení: DNSSEC Validátor v internetových prohlížečích.

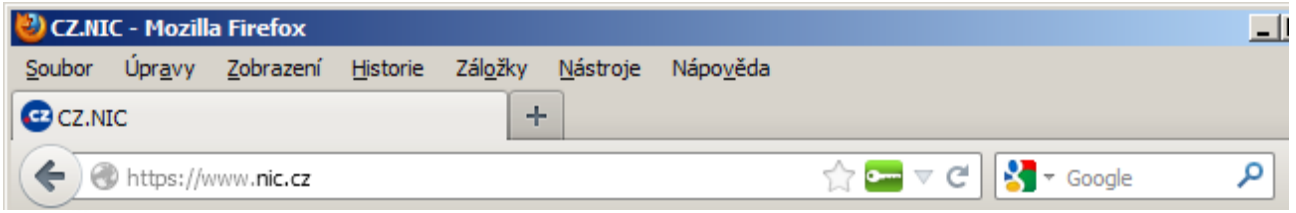
DNSSEC Validátor pro internetové prohlížeče

- Externí zásuvný modul (doplněk).
- Přidává do prohlížeče grafickou i textovou informaci o stavu DNSSEC zabezpečení pro konkrétní doménové jméno.
  - i neexistující.
- Jádro validátoru v jazyce C.
- Nezávislé na interních funkcích prohlížeče.
- IPv4, IPv6.
- Internetové prohlížeče.
  - Mozilla Firefox (FF)
  - Google Chrome (GC)
  - Internet Explorer (IE)

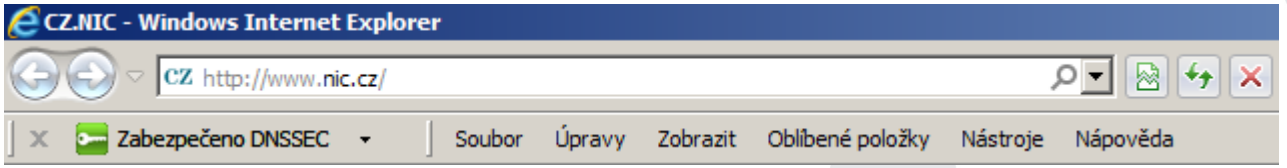


DNSSEC Validátor - vizualizace

- Vizualizace DNSSEC stavu pomocí barevných klíčků.
  - v adresovém řádku u FF a Chrome.

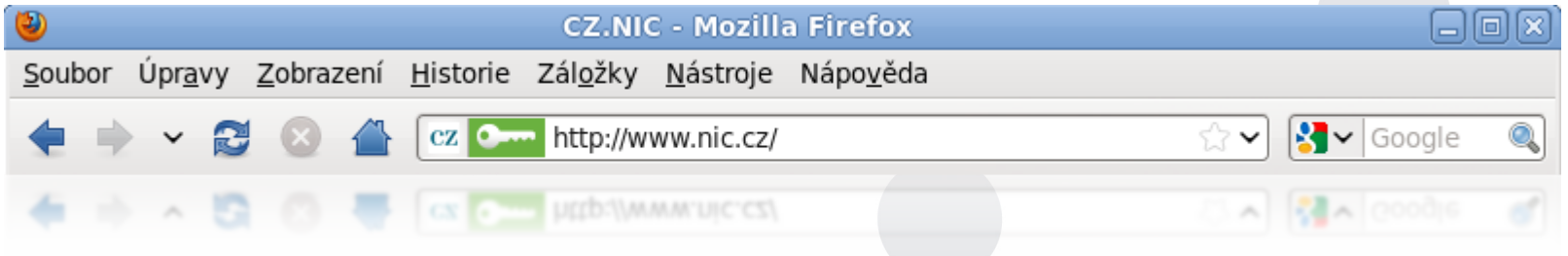


  - samostatný panel nástrojů u IE.



DNSSEC Validátor - verze

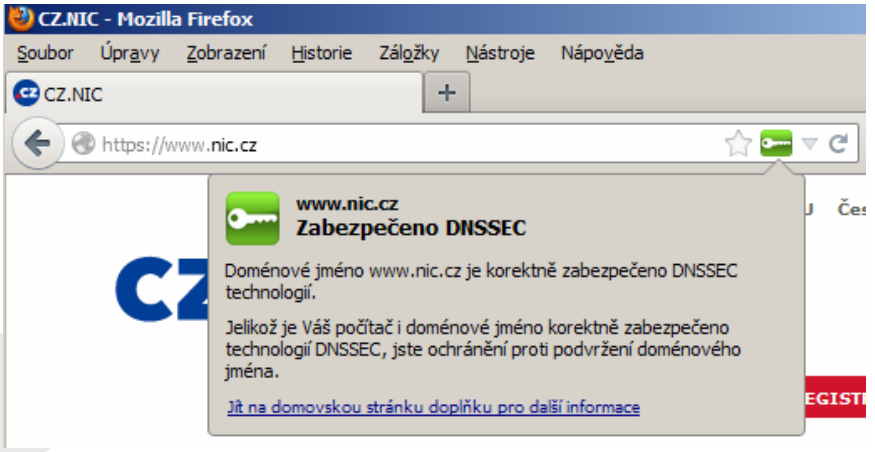
- Starší verze validátoru.
  - založeny na knihovně libldns.
  - spoléhají na rekurzivní resolver pro validaci - využívají AD příznak.
  - rozdílný vzhled pro FF, IE a Chrome.
  - absence cache u některých verzí.
  - absence kontroly IP adresy u některých verzí.
  - stabilní finální verze pouze pro FF.
  - https://labs.nic.cz/dnssec-validator/



- Nově DNSSEC Validátor 2.0

DNSSEC Validátor 2.0

- Založen na knihovně libunbound.
- Opět podpora pro IE, FF a Chrome.
- Sjednocuje vzhled i funkcionalitu pro všechny prohlížeče.
- Kontroluje správnost IP adresy, na kterou se prohlížeč připojuje (IE,FF i GC).
- Není závislý jen na AD příznaku z validujícího resolveru, chová se jako validující cachující resolver, rekurzivní resolving může provádět sám.
- Česká, anglická a německá mutace.
- Zatím v testovací verzi beta1.



- Instalační balíčky dostupné na:

https://labs.nic.cz/page/1253/dnssec-validator-2.0-pro-webove-prohlizece

Stavy zabezpečení DNSSEC

- 5 možných stavů

- stav DNSSEC zabezpečení nelze ověřit – špatně nastavený DNS resolver, nedostupnost sítě, jiná chyba.

- doménové jméno (existující/neexistující) není zabezpečeno pomocí DNSSEC.

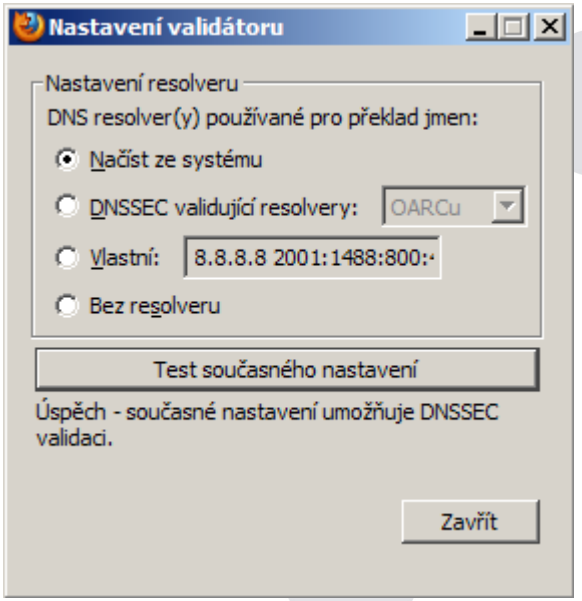
- doménové jméno (existující/neexistující) je korektně zabezpečeno pomocí DNSSEC, byl vytvořen řetězec důvěry a podpis domény (záznamu) je validní.

- doménové jméno je zabezpečeno DNSSEC, podpis byl ověřen, ale IP adresa prohlížeče neodpovídá IP adrese získané DNSSEC validátorem.

- doménové jméno (existující/neexistující) je zabezpečeno DNSSEC, byl však odhalen neplatný podpis nebo nebylo možné vytvořit řetězec důvěry pro validaci podpisu obdržených záznamu.

Nastavení validátoru

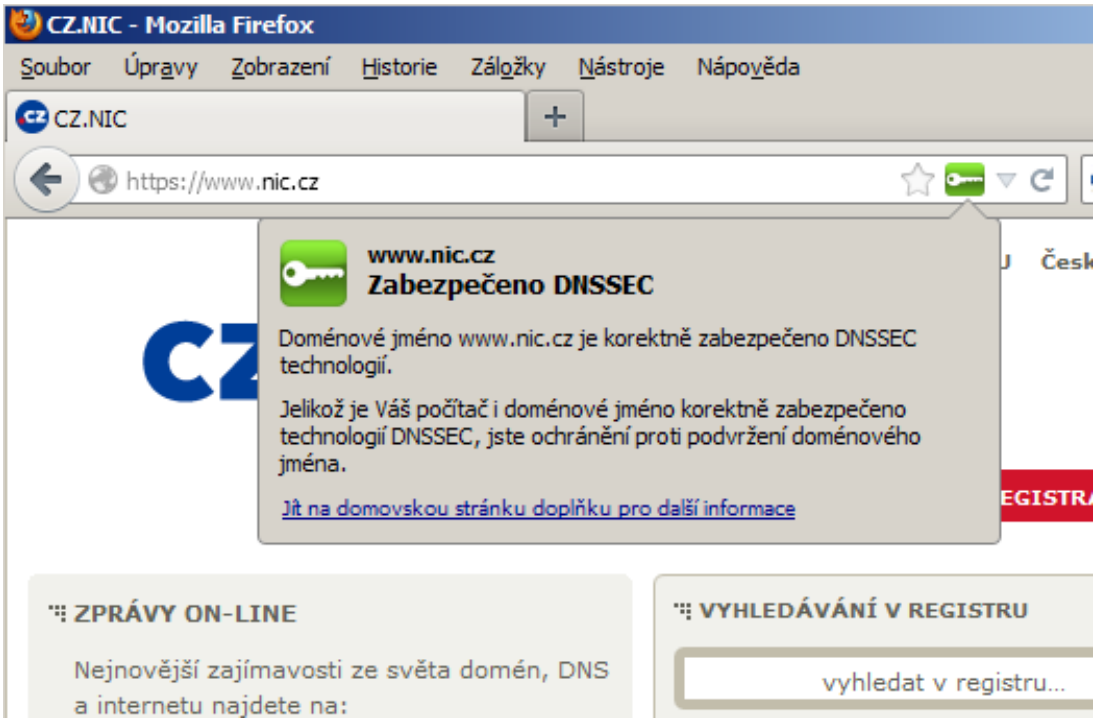
- Možnost nastavovat různé DNS resolvery pro validaci.
  - Systémové nastavení
  - Veřejné DNSSEC validující resolvery
    - CZ.NIC
    - OARC
  - Vlastní resolver(y)
    - 127.0.0.1
    - 8.8.8.8 2001:1488:800:400::130 …
  - Validace bez použití resolveru
    - přímá komunikace s autoritativními DNS servery.



- Možnost ověřit, zda-li vybrané nastavení podporuje DNSSEC.

Mozilla Firefox

- OS: Linux, Mac OS X, Windows – 32bit a 64bit.
- FF verze 5.0 a vyšší.

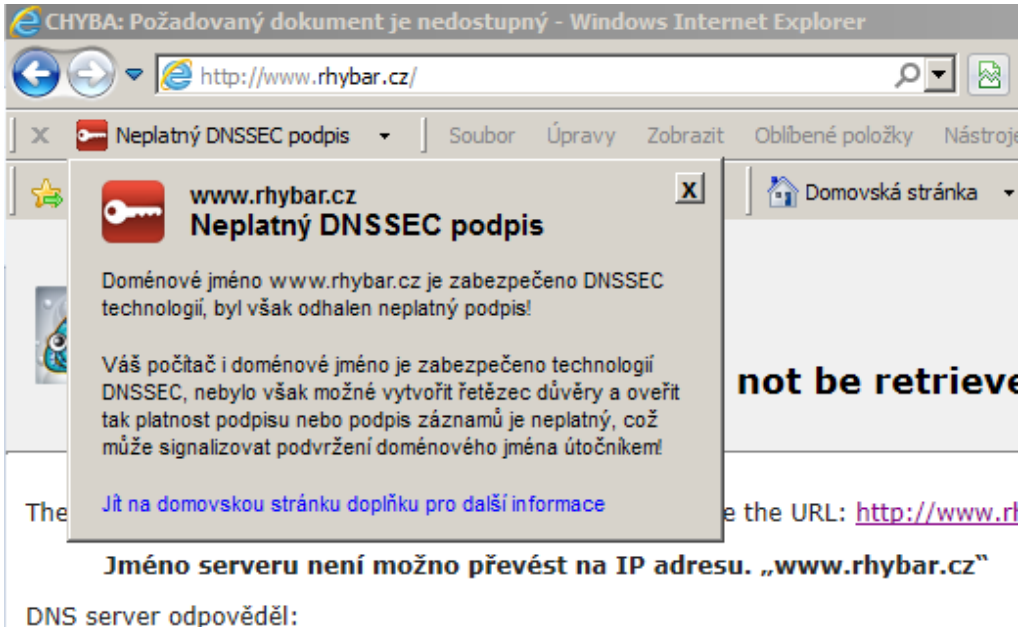


Chrome

- OS: Linux, Mac OS X, Windows – 32bit a 64bit.
- Chrome verze 16.0 a vyšší – API pro detekci IP adresy.

Internet Explorer

- OS: Windows XP, Vista, 7 a 8.
- Podpora pro 32-bitové verze IE 6.0 – 10.0.
- 64-bitové veze IE podporované prozatím nejsou.
- Omezení: IE nemá API pro detekci IP. IP adresa prohlížeče momentálně získaná přes dotaz na stub-resolver Windows.



Závěr a budoucnost?

- Byl představen nástroj pro validaci DNSSEC pro internetové prohlížeče.
- Uživateli umožňuje získat vizuální informaci o autenticitě záznamů obdržených v DNS odpovědi.
- Validátor kontroluje shodu IP adresy získané prohlížečem s IP adresou, kterou obdržel v ověřené DNS odpovědi.

- Podpora pro TLSA, možná i DANE - SSL certifikáty v DNS.
- Mobilní platformy ?
- Podpora pro více prohlížečů ?
  - Safari, Opera, SeaMonkey

Konec

Děkuji za pozornost