Automatická správa KeySetu

Bezdotykový DNSSEC

Jaromír Talíř • jaromir.talir@nic.cz • 03.12.2016

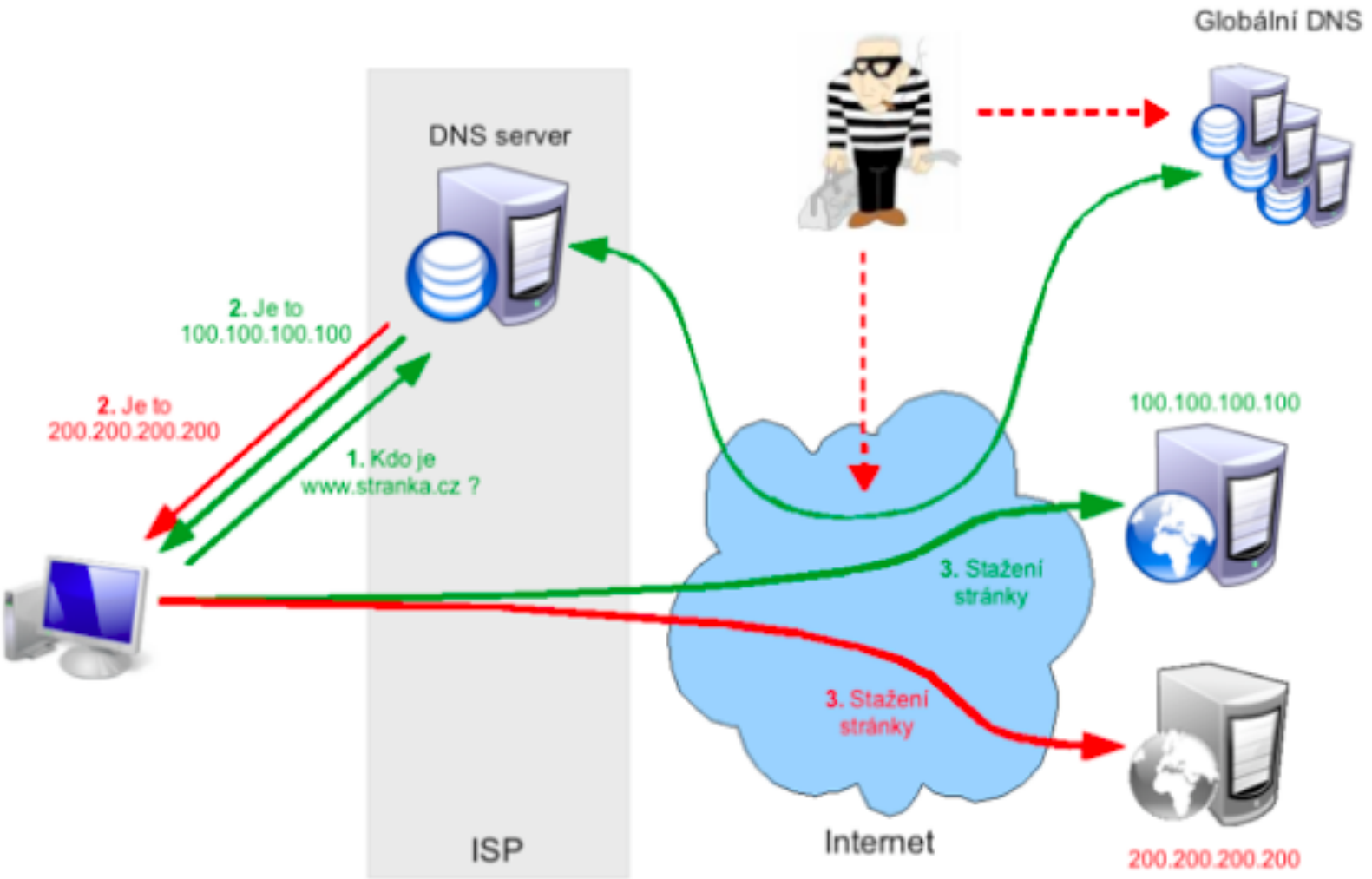
Obsah

- DNSSEC a automatizace
  - Aktuální stav nástrojů a standardů
- Registrační systém FRED a DNSSEC
  - Speciality implementace DNSSEC u nás
- Automatizace v prostředí domény CZ
  - Možnosti nasazení plné automatizace

DNSSEC

- Bezpečnostní rozšíření protokolu DNS
- Zajišťuje důvěryhodnost údajů získaných z DNS
  - Autenticita původu údajů
  - Detekce změn při přenosu
- Využívá asymetrickou kryptografii
  - Řetěz důvěry od jednoho klíče kořenové zóny až do „listů“ DNS „stromu“
- Kritická základna pro další služby (např. DANE)!

DNSSEC

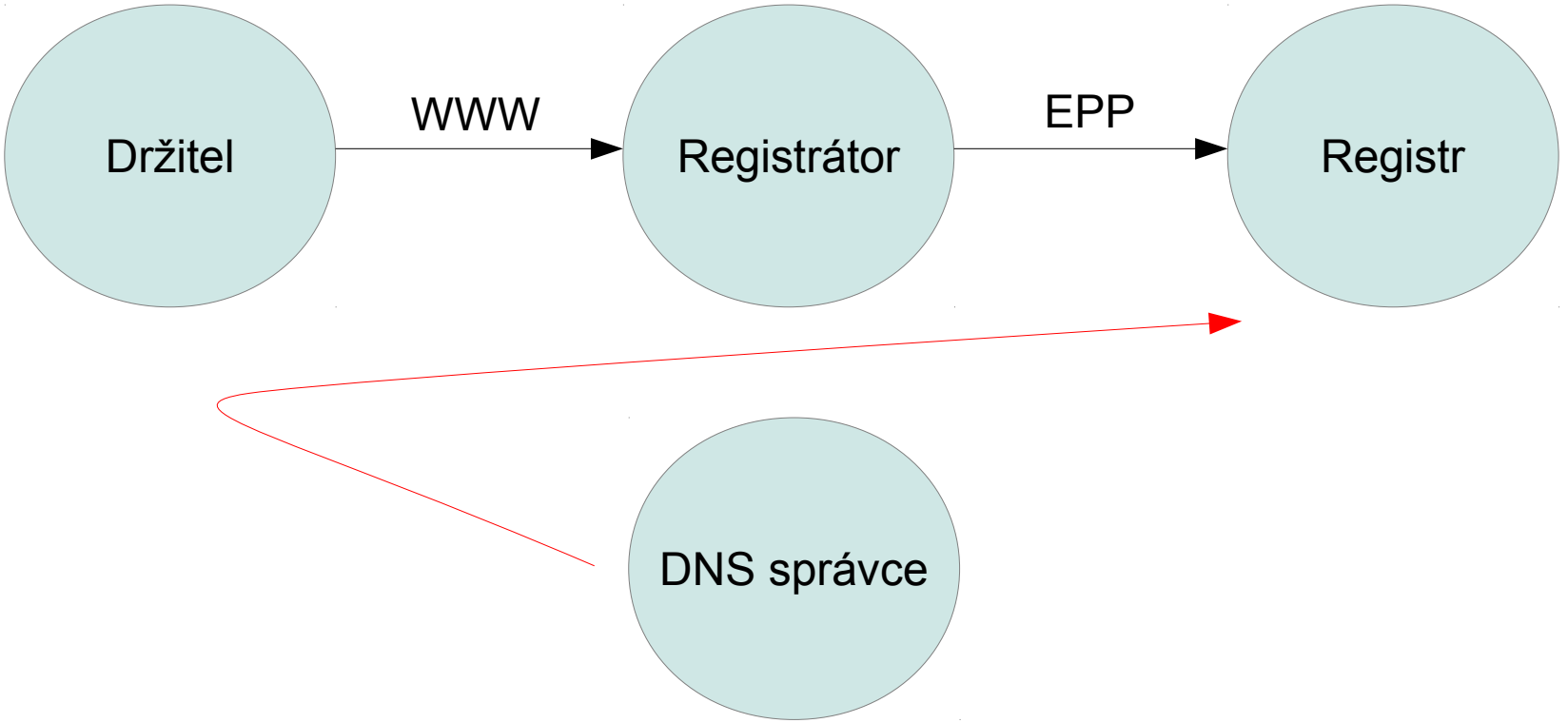

Globální DNS
DNS server
2. Je to
100.100.100.100
2. Je to
200.200.200.200
1. Kdo je
www.stranka.cz ?
100.100.100.100
3. Stažení
stránky
3. Stažení
stránky
ISP
Internet
200.200.200.200

DNSSEC a automatizace

- Nové povinnosti pro DNS správce
  - Pravidelné podepisování DNS záznamů – podpisy expirují
  - Výměna podpisových klíčů – bezpečnostní hygiena
- Nástroje na usnadnění práce
  - OpenDNSSEC
  - „In-line“ podepisování v BINDu
  - Automatizované podepisování v KnotDNS

DNSSEC a automatizace

- Změna klíče vyžaduje jeho propagaci do nadřazené zóny – zachování řetězce důvěry



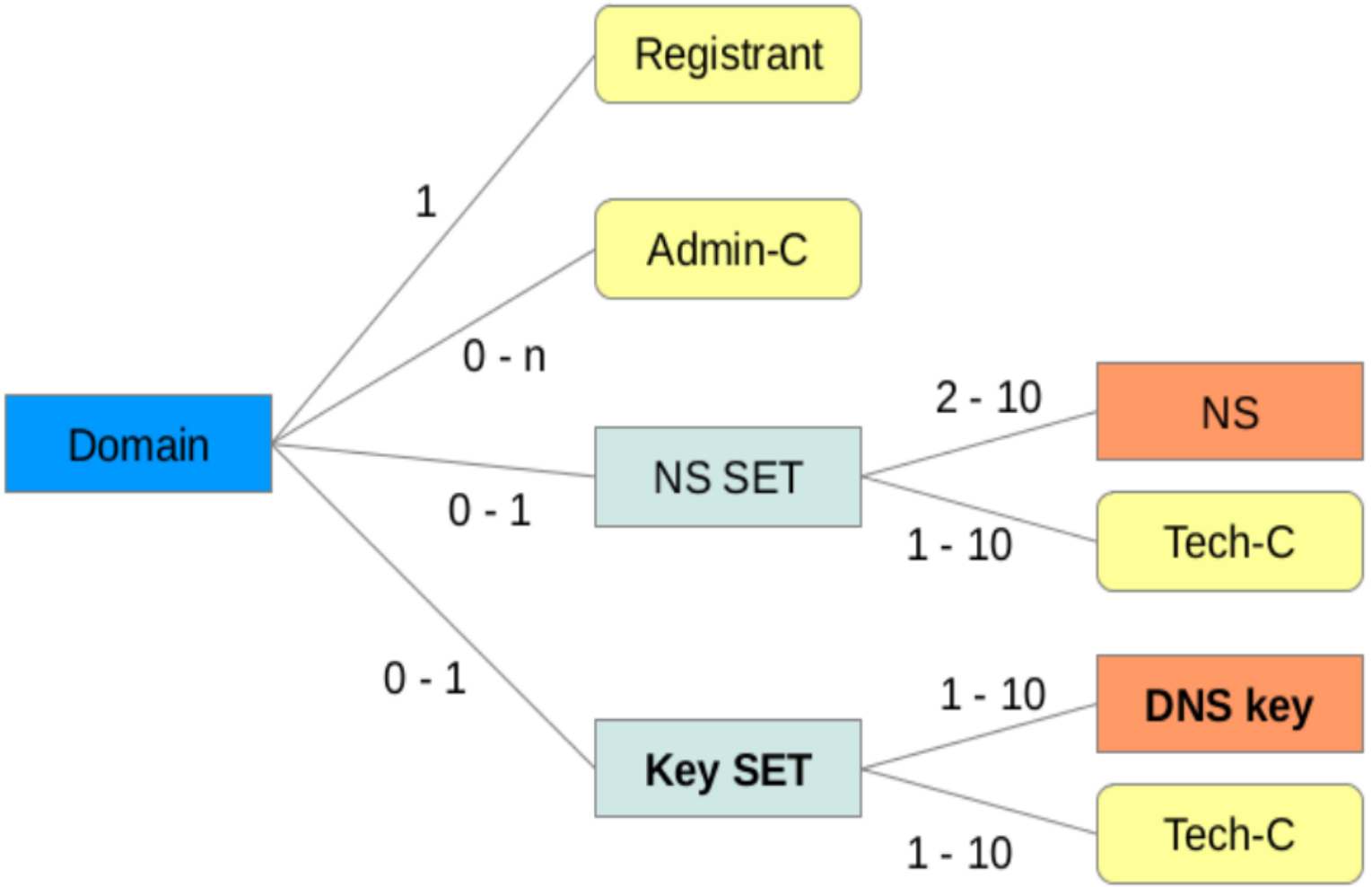
DNSSEC a automatizace

- RFC 7344 - Automating DNSSEC Delegation Trust Maintenance - září 2014
  - Nové typy DNS záznamů – CDS a CDNSKEY
    - Stejný obsah jako DS a DNSKEY
  - DNS správce kterých chce propagovat nový klíč publikuje CDS nebo CDNSKEY záznam
  - Zodpovědná entita detekuje existenci záznamu a provede aktualizace
    - Buď v rámci pravidelného skenu
    - Nebo může nabídnout aktivační „tlačítko“

DNSSEC a automatizace

- Podpora RFC 7344 v nástrojích:
  - V KnotDNS v první polovině 2017
  - OpenDNSSEC zatím podporu neohlásil
  - BIND 9.11
    - Vyšel 5.10.2016 (před dvěma měsíci)
    - Nový automatizační nástroj dnssec-keymgr
    - Ohlašovaná podpora CDS/CDNSKEY jen poloviční
    - S trochou hackování se ale již dá použít

Registrační systém FRED a DNSSEC



Registrační systém FRED a DNSSEC

- Vlastnosti KeySetu
  - Obsahuje několik klíčů (DNSKEY záznamů)
  - Obsahuje kontakty na správce klíčů
  - Má určeného registrátora, je možné ho převést
  - Registrátor ho spravuje pomocí EPP rozšíření
  - Je možné ho sdílet mezi více doménami
  - Delegační DS záznamy jsou generovány na straně registru

Registrační systém FRED a RFC7344

- Existuje několik alternativních scénářů nasazení podpory RFC7344:
  - Registrátoři zavedou podporu pro RFC7344 bez vazby na registr (CZ.NIC)
  - O rotaci klíčů se bude starat registr (CZ.NIC) a pro označené KeySety bude provádět změnu přímo v objektu registrátora
  - Registr (CZ.NIC) se stane „registrátorem“ pro automaticky spravované KeySety

Registrátoři zavedou podporu RFC 7344 sami

- Registrátoři mohou zavést podporu RFC7344 již nyní
  - Implementace detekce přítomnosti CDNSKEY + operace UPDATE_KEYSET v EPP rozhraní do registru
- Plánujeme otevřít diskuzi na nejbližším společném setkání

Registr (CZ.NIC) bude měnit údaje u registrátora

- Aktuální verze pravidel registrace nechává zodpovědnost za obsah objektů na registrátorovi
  - Možnost měnit data registru se omezuje na implementaci rozhodnutí soudu nebo optimalizaci údajů (např. slučování duplicit)
- Registrátor by měl možnost delegovat pravomoc nastavením příznaku u KeySetu

Registr (CZ.NIC) se stane registrátorem pro KeySety

- Využití možnosti převést KeySet od jednoho registrátora ke druhému bez změn u domény
- Již existuje precend v podobě služby mojeID kde je registrátorem ověřených kontaktů přímo CZ.NIC
- Možnost provádění změn přes aplikaci Doménový prohlížeč
- I tak bude nutné vyřešit problém změny KeySetu nebo vložení nového KeySety v doméně

Aktuální stav

- Máme prototypové řešení - Python knihovna z balíčku fred-client + dnspython
- Otazníky:
  - Je třeba vyřešit problém sdílených keysetů
  - RFC7344 neřeší počáteční vložení klíče a ani odstranění klíče:
    - draft-latour-dnsoperator-to-rrr-protocol
- V průběhu roku 2017 bychom chtěli nabídnout funkční službu

Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz