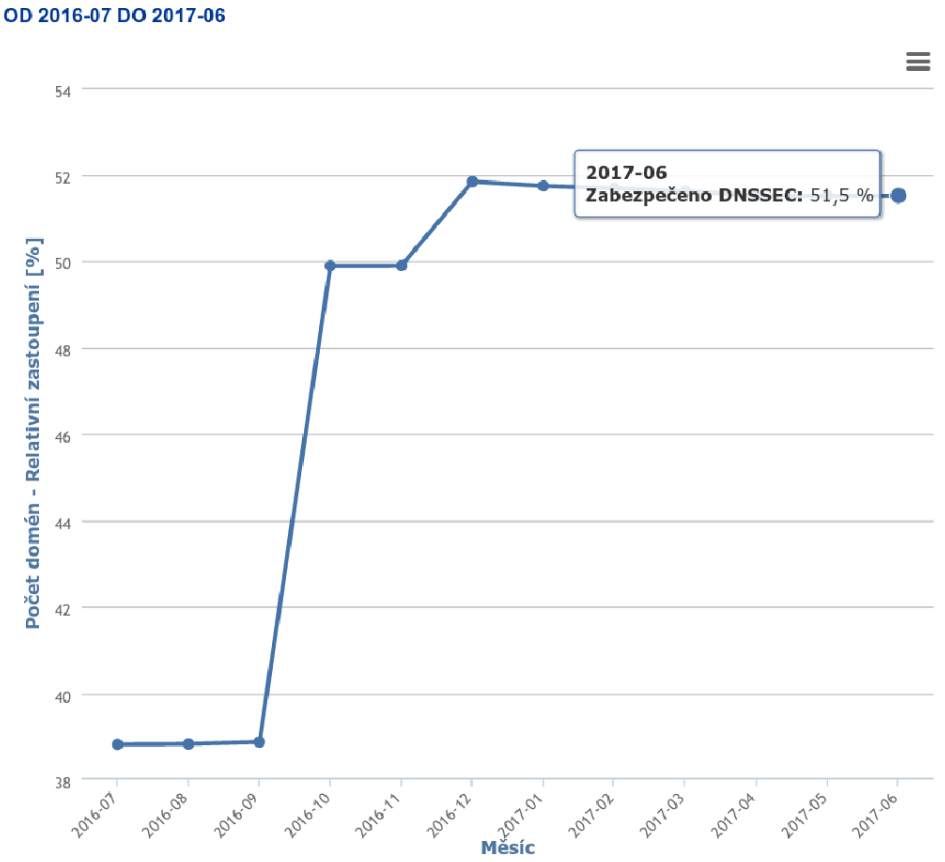
Automatická správa keysetu

Jaromír Talíř • jaromir.talir@nic.cz • 20. 06. 2017

Proč? 51,5% není 100%

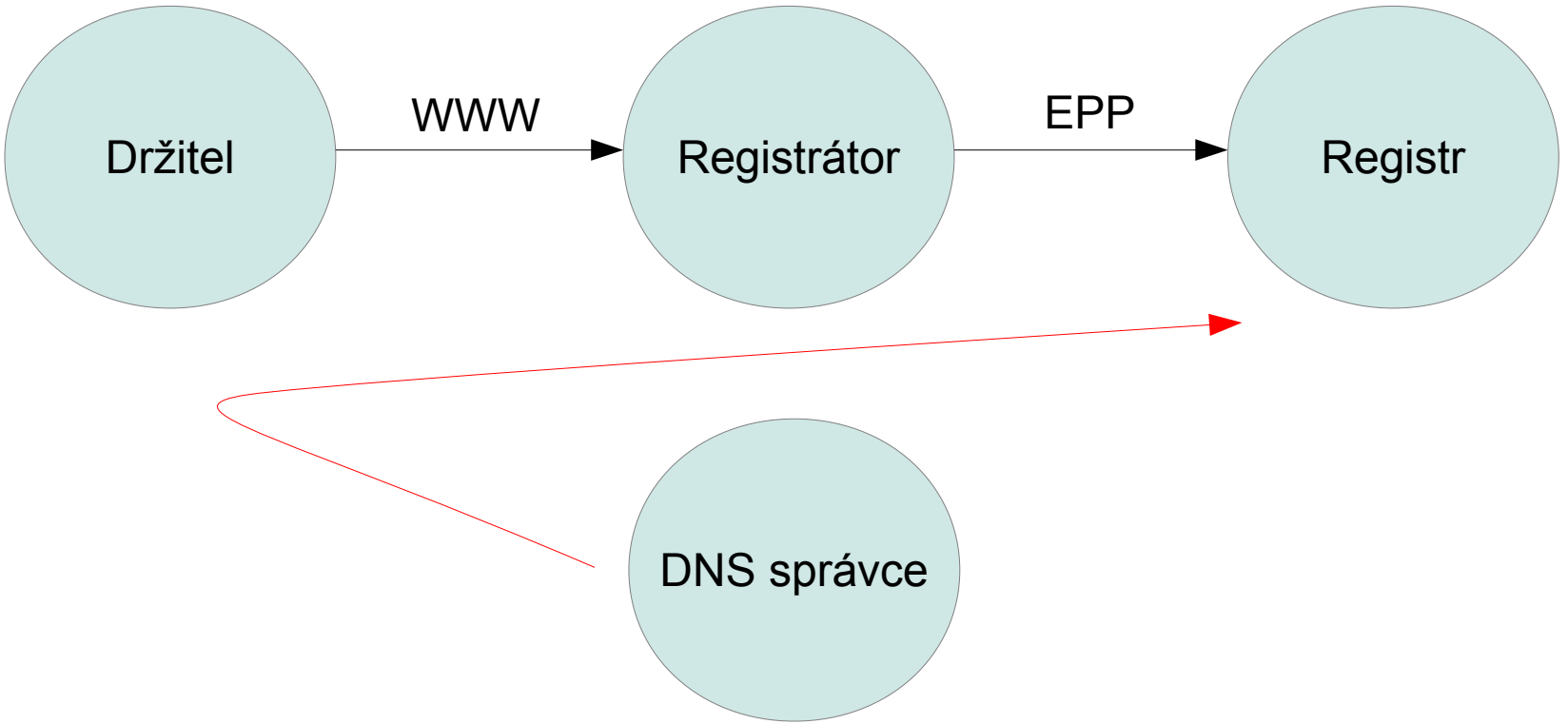


Proč? 51,5% není 100%

- Počet domén zveřejňujících DNSKEY (KSK = flag 257), které nemají nastaven KeySet v registru

21 156

Překážky pro rozšíření DNSSEC



IETF dokumenty řešící automatizaci

- **RFC 7344** - Automating DNSSEC Delegation Trust Maintenance - září 2014
- **RFC 8078** - Managing DS Records from the Parent via CDS/CDNSKEY – březen 2017
- **draft-ietf-regext-dnsoperator-to-rrr-protocol** - Third Party DNS operator to Registrars/Registries Protocol

Cloudflare

CLOUDFLARE

- Služba reverzní proxy pro zákaznické weby – v základní verzi zdarma
- DNS operátor se zapnutím DNSSEC na kliknutí
  - Online podepisování DNS odpovědí
  - ECDSA algoritmus
- Není registrátor! => Změny DNSSEC nastavení musí zajistit držitelé u svých registrátorů
- Podpora CDNSKEY pro všechny domény od **20.6.2017**

Cloudflare - statistiky

Registrátor	Domén	DNSSEC nastaven v CZ	Jen Podepsáno	DNSSEC celkem u registrátora v %
1	1265	231	43	80
2	682	84	9	9
3	537	21	45	64
4	332	3	9	45
5	236	20	12	82
6	172	0	4	0
7	112	0	2	0
8	109	1	0	58
9	107	4	7	40
10	99	4	4	74
11	83	21	6	7
12	62	1	1	28
13	53	0	0	0
14	22	0	2	0
15	22	0	1	50
16	19	0	1	0
17	16	0	0	96

Registrátor	Domén	DNSSEC nastaven v CZ	Jen Podepsáno	DNSSEC celkem u registrátora v %
18	12	0	0	0
19	12	0	0	0
20	9	0	0	0
21	8	0	0	0
22	8	0	0	0
23	7	0	0	0
24	6	0	1	1
25	5	0	0	0
26	4	0	0	0
27	2	0	0	91
28	2	0	0	8
29	2	0	0	52
30	1	0	0	48
31	1	0	0	0
32	1	0	0	0
33	1	0	0	26
34	1	0	0	0

Populární nástroje pro DNSSEC automatizaci

- OpenDNSSEC
  - Zatím podporu oficiálně neohlásily
  - Neoficiálně by to letos mělo být
- BIND
  - Částečná podpora ve verzi 9.11 (vyšel 5.10.2016)
  - Nový automatizační nástroj dnssec-keymgr spouštěný z cronu
  - Podpora CDS/CDNSKEY jen přes dnssec-settime

Knot DNS a podpora rotace KSK

- Podpora KSK rotace ve verzi 2.5 vydané **6.6.2017**
- Rotace řešena dvojitým podpisem novým a starým klíčem a výměnou DS v nadřazené zóně
- Periodické kontroly existence DS záznamu
  - Možnost konfigurace všech autoritativních NS nadřazené zóny a/nebo resolveru
  - Všechny NS musí dávat stejnou odpověď
  - Nevaliduje se odpověď, je možné použít validující resolver

Knot DNS a podpora rotace KSK

```
remote:
  - id: odvr
    address: 193.29.206.206@53

submission:
  - id: my_subm
    parent: [odvr]
    check-interval: 30m
```

```
policy:
  - id: my_policy
    algorithm: ECDSAP256SHA256
    dnskey-ttl: 1h
    zsk-lifetime: 30d
    propagation-delay: 30m
    rrsig-lifetime: 14d
    rrsig-refresh: 7d
    nsec3: on
    ksk-lifetime: 300d
    ksk-submission: my_subm

zone:
  - domain: test-cdnskey.cz
    file: "db.test-cdnskey.cz"
    dnssec-signing: on
    dnssec-policy: my_policy
```

Knot DNS a podpora rotace KSK

- Ve vývoji
  - PUSH mechanismus přes REST rozhraní
    - Implementace draft-ietf-regext-dnsoperator-to-rrr-protocol
  - Podpora CSK (Combined Signed Key) rotace
    - Parametr single-type-signing
  - Podpora změny algoritmu při rotaci

Scénáře nasazení podpory v .CZ

- Registrátoři zavedou podporu pro CDNSKEY 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) bude přímo spravovat automatizované KeySety**
  - **Implementace vyhledáváním CDNSKEY záznamů u domén**

Vyhledávání CDNSKEY

- Domény které nemají přiřazen KeySet
  - Dotaz na CDNSKEY na všechny autoritativní NS v registru DNS dotazem po TCP
  - V případě nalezení záznamu se stává doména kandidátem na zavedení DNSSEC
  - Informujeme e-mailem technického správce NSSetu
  - Pokud každý den po dobu 7 dní uvidíme stejný výsledek vytvoříme nový KeySet s údaji z CDNSKEY záznamu a přiřadíme ho doméně
  - Informujeme registrátora přes EPP a držitele na notifikační e-mail

Vyhledávání CDNSKEY

- Domény které mají přiřazen automatizovaný KeySet
  - Dotaz na CDNSKEY přes resolver s lokální DNSSEC validací
  - V případě nalezení záznamu provedeme aktualizaci KeySetu – stávající klíče se nahradí obsahem CDNSKEY odpovědi
  - V případě že CDNSKEY má speciální tvar pro zrušení DNSSEC, provedeme odebrání KeySetu, informujeme registrátora přes EPP a držitele na notifikační e-mail
  - V obou případech informujeme e-mailem technického správce NSSetu

Vyhledávání CDNSKEY

- Domény které mají přiřazen KeySet u registrátora
  - Dotaz na CDNSKEY přes resolver s lokální DNSSEC validací
  - V případě nalezení záznamu provedeme vytvoření nového KeySetu jako v případě domén bez KeySetu a u domény se nastaví tento nový KeySet
  - V případě že CDNSKEY má speciální tvar pro zrušení DNSSEC, provedeme odebrání KeySetu
  - Informujeme e-mailem technického správce NSSetu
  - Informujeme registrátora přes EPP a držitele na notifikační e-mail

Vlastnosti automatizovaného KeySetu

- Automaticky generovaný identifikátor „AUTO-“ + náhodný řetězec
- Registrátor CZ.NIC
- Technický kontakt CZ.NIC
- DNSSEC klíče na základě obsahu zjištěného CDNSKEY
- Neblokujeme jeho přiřazení k jiné doméně, ale pokud to vlastník domény provede, nebude mu doména fungovat správně

Blokování změn

- Pokud nechcete změnu provést
  - Odstraňte CDNSKEY z konfigurace vaší domény nebo kontaktujte vašeho DNS operátora ať záznamy nepublikuje
  - Nastavte si blokaci domény pro změnu přes webové stránky CZ.NIC nebo doménový prohlížeč
- Pokud chcete zvrátit provedenou změnu
  - U registrátora který podporuje DNSSEC smažte KeySet
  - U ostatních registrátorů můžete provést aktualizci NSSetu s použitím stejného identifikátorem NSSetu (trik!)

Aktuální stav

- Spouštíme pilotní provoz ve kterém jednou denně vyhledáváme CDNSKEY u domén bez KeySetu
  - První nastavení DNSSEC domény tedy nejdřív za týden
- Za týden spustíme vyhledávání CDNSKEY u domén s automatizovaným KeySetem
- O plném spuštění pro domény s již existujícími KeySety budeme informovat

Závěr

- Podpora CDNSKEY v registračním systému FRED a DNS serveru Knot DNS
  - Ideální kombinace pro správu CZ domény
  - Zatím žádný jiný registr oficiálně podporu pro CDS/CDNSKEY nespustil
- Další kroky
  - Vyhodnocení pilotního provozu
  - Podpora PUSH modelu jak ve FREDu tak v KNOTu

Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz