Automatická správa DNSSEC

I vy můžete zvýšit bezpečnost českého internetu!

Zdeněk Brůna • 22. ledna 2025

CZ DOMAIN REGISTRY

Agenda

- Úvod k DNSSEC
- Možnosti zavedení DNSSEC v registru .CZ domén
- Automatická správa DNSSEC
- Úpravy automatické správy DNSSEC v 2024
- Uvažovaná vylepšení automatické správy DNSSEC

Úvod k DNSSEC

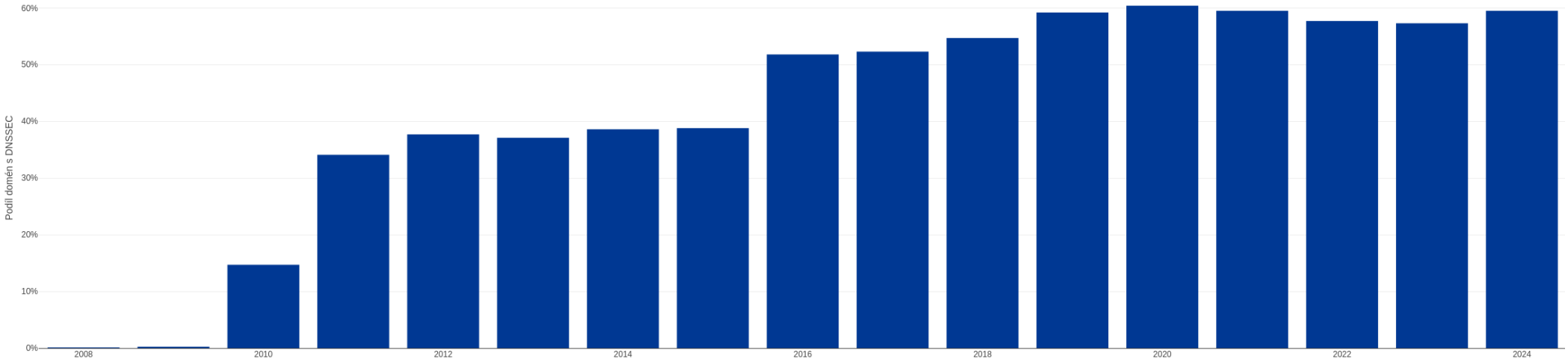
- Co je DNSSEC?
  - bezpečnostní rozšíření DNS
    - úplnost a integrita informací z DNS
    - důvěryhodné DNS
  - princip asymetrické kryptografie
    - podpis vložených záznamů v zoně domény soukromým klíčem
    - publikace veřejného klíče do nadřazené zóny (slouží k ověření podpisu)
  - vyžaduje podporu od
    - registru domén
    - technického správce (autoritativní DNS servery)
    - ISP (rekurzivní DNS servery)

Úvod k DNSSEC

- Podpora DNSSEC v ČR
  - podpora v registru .CZ domén od roku 2008 (FRED)
  - provoz otevřeného DNSSEC validujícího resolveru (ODVR)
  - podpora v našem DNS SW (KNOT DNS, KNOT resolver)
  - různé formy podpory a motivace pro zavedení
    - významné kritérium certifikačního programu pro registrátory
    - nutný bod pro splnění podmínek vstupu do FENIX
    - kurz v Akademii CZ.NIC - https://www.nic.cz/akademie/course/14/detail/
    - PR a MKT podpora (edukativní stránky, videa, kampaně)
  - jak jsme tedy na tom?

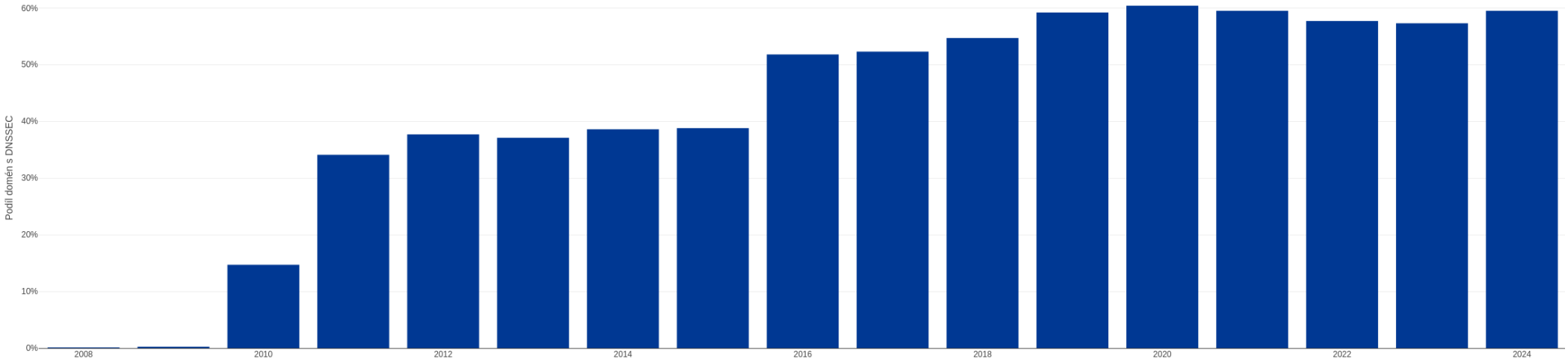
Úvod k DNSSEC

- Podpora DNSSEC v ČR - podpora v registru .CZ domén



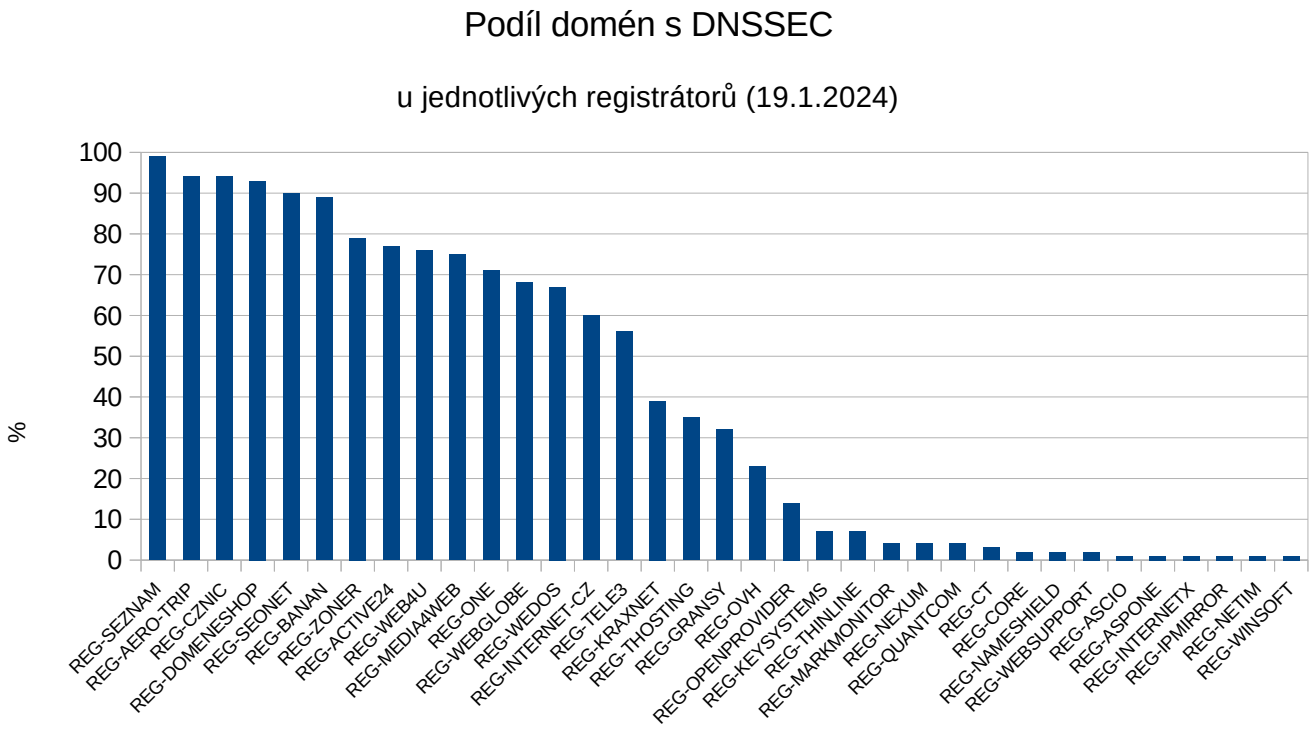
Úvod k DNSSEC

- Podpora DNSSEC v ČR - podpora v registru .CZ domén
  - 5. mezi ccTLD - 1. dk (66,9%), 2. nl (61,5%), 3. no (60,4%), 4. se (59,9%), 5. cz (59%)
    - zdroj: https://stats.dnssec-tools.org/ + https://stats.centr.org/
    - er (75%) ~ jen několik desítek domén



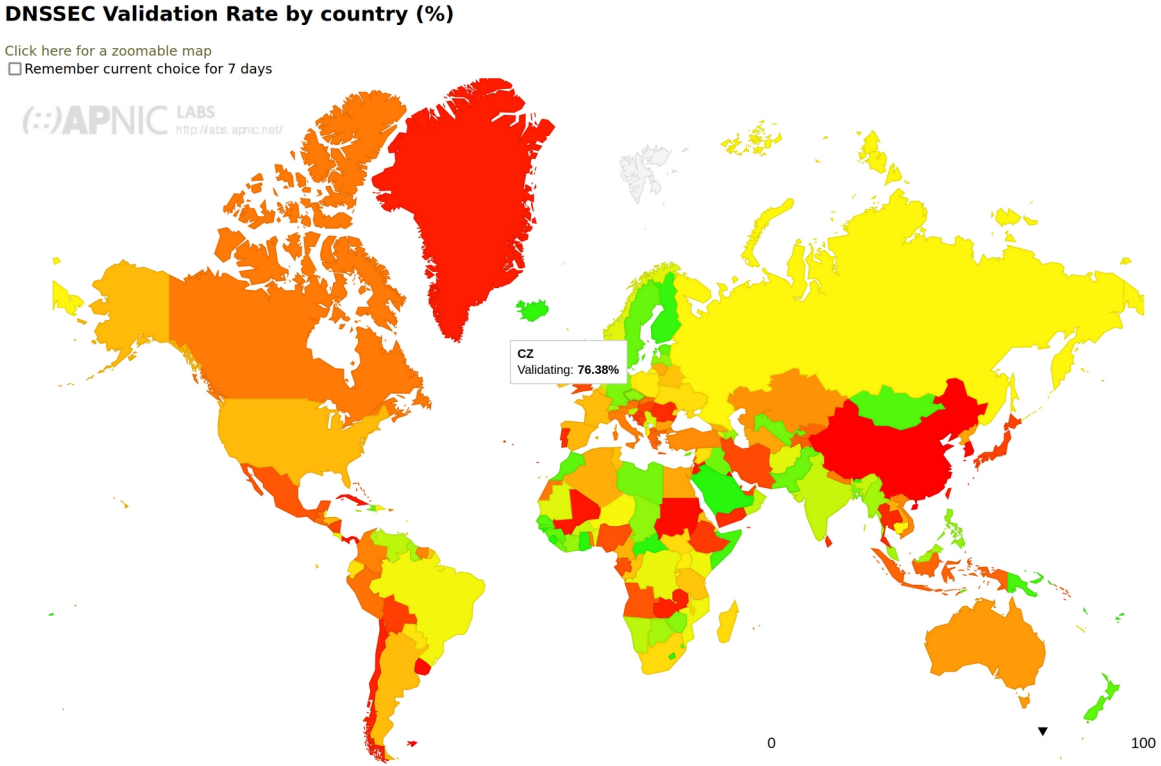
Úvod k DNSSEC

- Podpora DNSSEC v ČR - podpora mezi registrátory



Úvod k DNSSEC

- Podpora DNSSEC v ČR - u ISP (https://stats.labs.apnic.net/dnssec)



Možnosti zavedení DNSSEC v registru .CZ domén

- Dle způsobu předání veřejného klíče do nadřazené (.cz) zóny
  - 1) držitelem (přes registrátora domény)
    - vygenerování klíčů
    - podepsání záznamů v zóně domény
    - v rozhraní registrátora
      - vytvoření KEYSET (zápis otisku veřejného klíče do registru .CZ přes EPP – publikace DNSKEY záznamu)
      - přiřazení KEYSET k doméně
    - vygenerování a vypublikování odpovídajících DS záznamů v .cz zóně
  - 2) registrátorem domény
    - vygenerování klíčů
    - podepsání záznamů v zóně domény
    - vytvoření KEYSET (zápis otisku veřejného klíče do registru .CZ přes EPP – publikace DNSKEY záznamu)
    - přiřazení KEYSET k doméně
    - vygenerování a vypublikování odpovídajících DS záznamů v .cz zóně

Možnosti zavedení DNSSEC v registru .CZ domén

- Dle způsobu předání veřejného klíče do nadřazené (.cz) zóny

  3) technickým správcem domény (provozovatelem nameserverů)

  - vygenerování klíčů
  - podepsání záznamů v zóně domény
  - vypublikování CDNSKEY záznamu v zóně domény
  - oskenování zóny domény systémem
  - vytvoření KEYSET (zápis otisku veřejného klíče do registru .CZ - DNSKEY)
  - přiřazení KEYSET k doméně
  - vygenerování a vypublikování odpovídajících DS záznamů v .cz zóně

  } vykoná systém Automatické správy DNSSEC

Možnosti zavedení DNSSEC v registru .CZ domén

- Dle způsobu předání veřejného klíče do nadřazené (.cz) zóny

  3) technickým správcem domény (provozovatelem nameserverů)

  - vygenerování klíčů
  - podepsání záznamů v zóně domény
  - vypublikování CDNSKEY záznamu v zóně domény

  možno automatizovat
  např. pomocí KNOT DNS

  - oskenování zóny domény systémem
  - vytvoření KEYSET (zápis otisku veřejného klíče do registru .CZ - DNSKEY)
  - přiřazení KEYSET k doméně
  - vygenerování a vypublikování odpovídajících DS záznamů v .cz zóně

  vykoná systém Automatické správy DNSSEC

Automatická správa DNSSEC

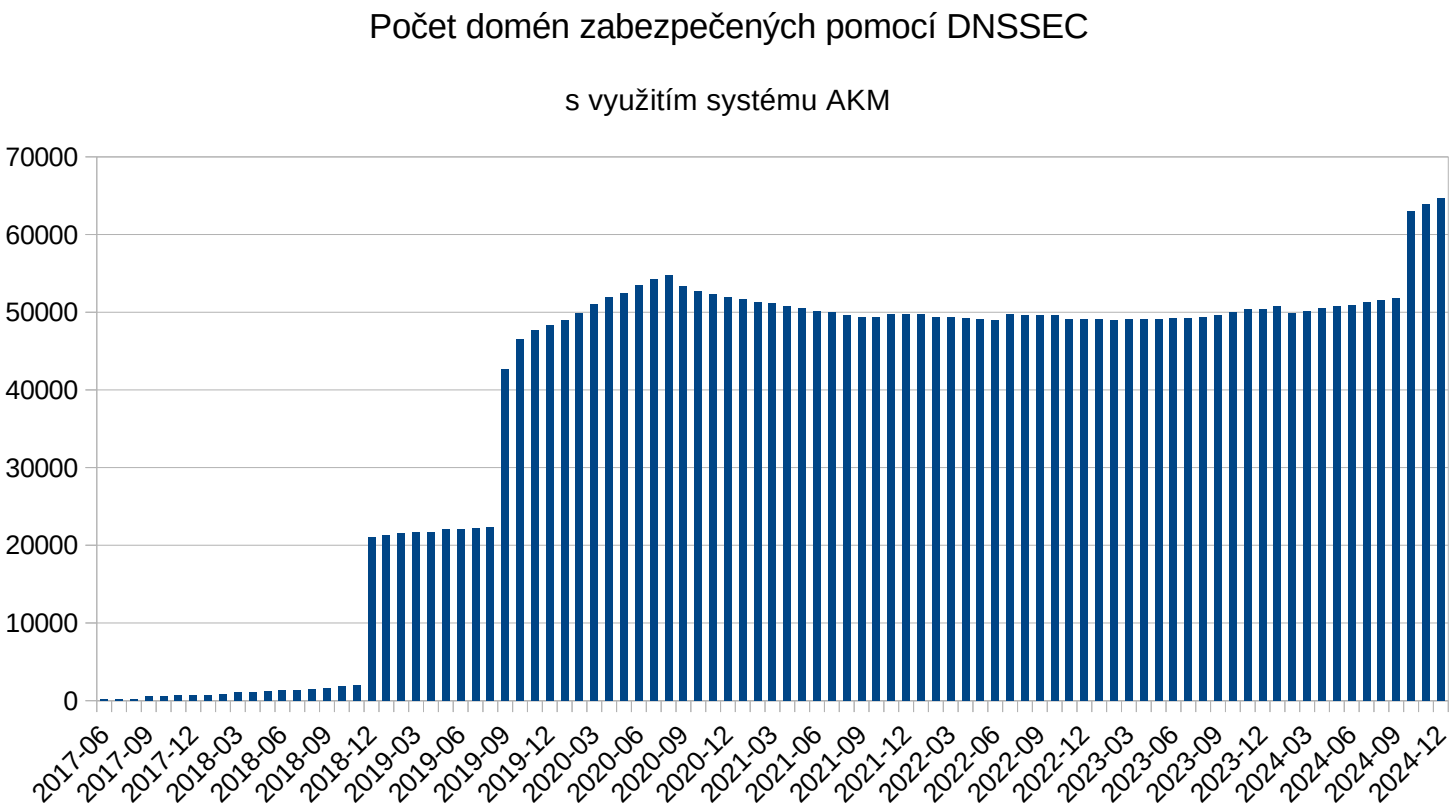
- Vznikla díky
  - RFC 7344 Automating DNSSEC Delegation Trust Maintenance
  - RFC 8078 Managing DS Records from the Parent via CDS/CDNSKEY
- Umožnění správy KEYSET prostřednictvím speciálních DNS záznamů
- Není třeba spolupráce držitele ani registrátora domény
- FRED (registr .CZ) podporuje od 2017
  - Automated KEYSET management (AKM)
- KNOT DNS podporuje od verze 2.5.0
  - automatické zavedení i rotace klíčů

možnost úplné automatizace správy DNSSEC!

Automatická správa DNSSEC

- Stručný popis implementace v systému FRED z roku 2017
  - vyhledávání CDNSKEY záznamů u domén (skenování DNS)
  - nález u domény se zavedeným DNSSEC
    - výměna klíče hned po nálezu
  - nález u domény bez DNSSEC
    - opakování skenu ještě 7x (nesmí dojít k přerušení / změně)
    - e-mailová notifikace na technický kontakt NSSETu u domény (E-mail pro oznámení / E-mail)
    - vytvoření KEYSET (zápis otisku veřejného klíče do registru .CZ - DNSKEY)
    - přiřazení KEYSET k doméně
    - vygenerování a vypublikování odpovídajících DS záznamů v .cz zóně
  - nález CDNSKEY záznamu se specifickými hodnotami (CDNSKEY 0 3 0 AA==)
    - odpojení KEYSET od domény

Automatická správa DNSSEC

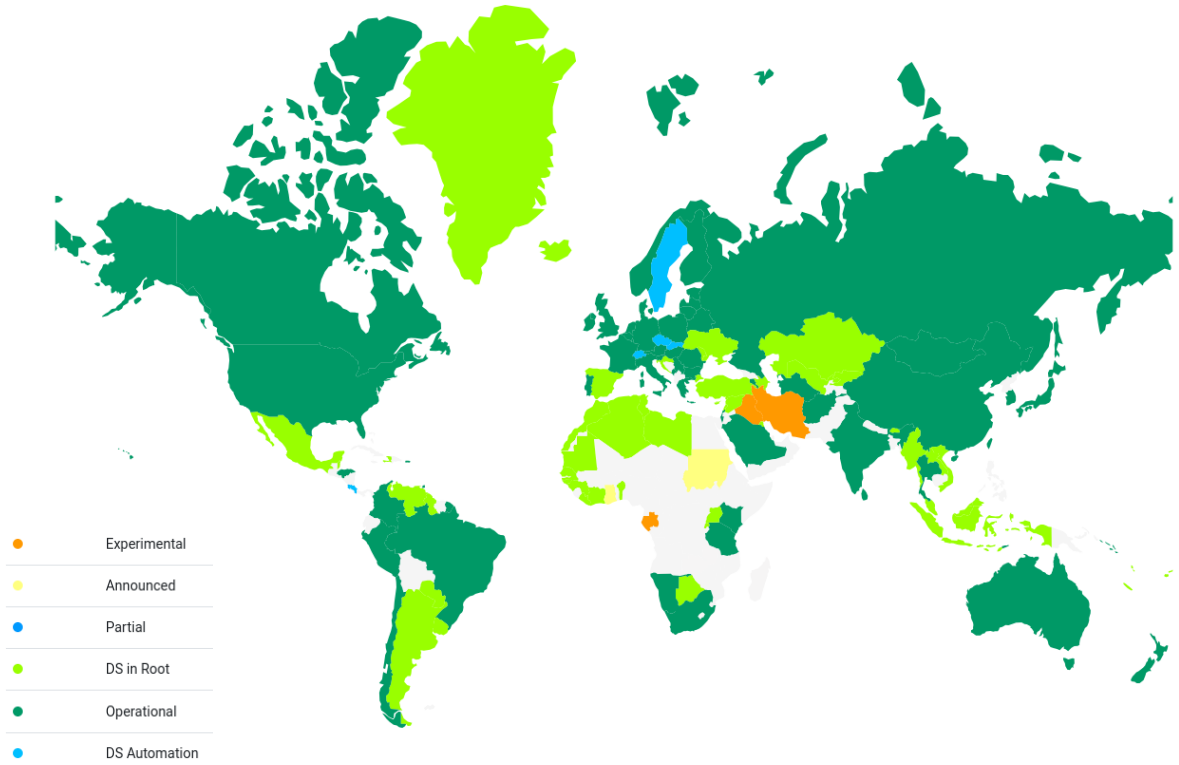


Nejvíce zastoupené NSSETy s doménami pod AKM

- Seonet Multimedia
- Gransy
- Váš Hosting
- Blueboard.cz
- THINline

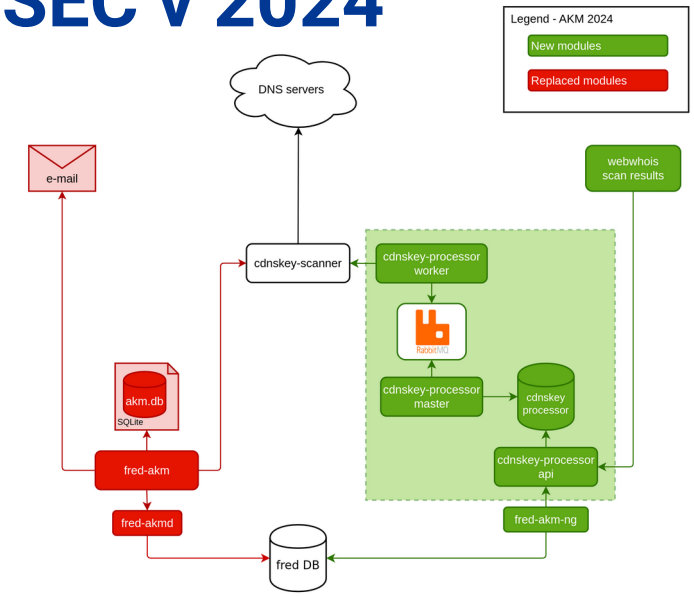
Automatická správa DNSSEC

- Podpora DNSSEC ve světě
  - https://maps.dnssec.gmu.edu/
  - podpora AKM jen v 7 ccTLDs
    - .cz, .sk, .ch, .li, .se, .nu, .cr



Úpravy automatické správy DNSSEC v 2024

- Zvýšení technologické robustnosti
  - vyčlenění z jádra FRED
    - FRED komunikuje s cdnskey-processorem pomocí API
    - obecně použitelný nástroj s otevřeným API
  - oddělené servery pro AKM
  - přechod AKM databáze z SQLite na PostgreSQL
  - distribuovaná architektura skenování s RabbitMQ
    - možnost restartu některé části cdnskey-processor bez ztráty rozpracovaného skenovacího jobu
  - skenování dělíme na dílčí skupiny
    - při přerušení skenování není třeba opakovat sken celé zóny, ale jen aktuálně zpracovávanou část



Úpravy automatické správy DNSSEC v 2024

- Zvýšení odolnosti vyhodnocení věrohodného CDNSKEY záznamu
  - ověřovací lhůta skenů pro nezabezpečenou doménu umožňuje “výpadek” skenu pokud nepřekročí 48 hodin
    - např. síťová nedostupnost nameserverů dané domény v době skenování
- Zrušení e-mailových notifikací na technický kontakt NSSETu u domény
- Zlepšení pro technického správce domény
  - publikace naskenovaných CDNSKEY záznamů ve web whois
    - https://www.nic.cz/whois/domain/example.cz/scan-results
  - procesy AKM ignorují “zámek” na doméně ~ “domain lock”
    - dříve zámek zavedení (správu) DNSSEC na doménách blokoval

Uvažovaná vylepšení automatické správy DNSSEC

- Distribuované skenování z více lokalit (najednou)
  - další snížení rizika útoku typu Man-in-the-middle
  - možnost zkrácení doby zavedení DNSKEY do registru
- Průběžné vyhodnocování skenů
  - aktuálně probíhá až na konci dne (po všech skenech – které jsou rozloženy do celého dne)
  - dřívější změny v registru
- Vyladění zobrazení informací o skenu ve WHOIS
  - srozumitelnější informace o aktuálním stavu skenu
  - dostupnost informací přes REST API
  - propojení s nápovědou

Uvažovaná vylepšení automatické správy DNSSEC

- Podpora RFC 9615
  - vložení CDNSKEY záznamu do jiné již podepsané zóny DNS operátora
  - není třeba skenovat 7 dní, update možno provést okamžitě
- Sledujeme draft “Generalized DNS Notifications”
  - možnost využití signalizace ze strany DNS operátora, že došlo ke změně v zóně
  - sken pouze těch zón, kde byl přidán CDNSKEY záznam
- Implementace CSYNC
  - obecnější mechanismus pro synchronizaci NS záznamů mezi TLD a SLD

Otázky?

Zdeněk Brůna • 22. ledna 2025

Pomůžete nám na 1. místo?

kurz v Akademii CZ.NIC - https://www.nic.cz/akademie/course/14/detail/