

Automatizovaná aktivácia DNSSEC prostredníctvom CDS záznamu

(technická implementácia)

Od 1. januára 2020 sa pre doménu .sk zavádza automatizovaná aktivácia DNSSEC na základe údajov na NS serveroch (tzv. CDS skenovanie). Systém CDS skenovania je alternatívou k zapisovaniu DS záznamov (záznamov pre DNSSEC) do Centrálného registra domén .sk prostredníctvom rozhrania EPP alebo registrátorskej konzoly.

Tento systém automatizovane prehľadáva zóny všetkých .sk domén na prítomnosť CDS záznamov v nich.

Systém CDS skenovania funguje v doméne .sk nasledovne:

- Ak je pre doménu nájdený jeden alebo viac CDS záznamov, ktorá v Centrálnom registri domén nemá existujúci DS záznam (t.j. nemá aktivovaný DNSSEC), je uložený a nasledujúcich 72 hodín je periodicky sledovaná jeho stabilita (nesmie prestať existovať, ani sa zmeniť). Po úspešnom uplynutí tejto doby je zapísaný k doméne ako platný DS záznam pre DNSSEC.
- Obdobný princíp platí aj v prípade, ak už má doména v Centrálnom registri domén aktivovaný DNSSEC (t.j. má jeden alebo viac DS záznamov) a na mennom serveri sa identifikuje rozdielny záznam. V tomto prípade sa všetky existujúce záznamy prepíšu novo nájdenými.
- V prípade zhody existujúceho záznamu v registri a CDS záznamu nájdeného na mennom serveri sa nevykoná žiadna akcia.
- Pre odstránenie existujúcich DS záznamov v registri je použiteľný aj tzv. „kill record“ záznam, t.j. špeciálny CDS záznam pre úplný výmaz záznamov pre DNSSEC. Tu sa rovnako ako vyššie aplikuje pravidlo sledovania stability CDS záznamu.

Po úspešnom ukončení každej z vyššie uvedených variant (okrem nevykonania žiadnej akcie pri zhode) je technickému kontaktu domény zaslaná e-mailová notifikácia.

Poznámka: Pre využitie tejto služby je potrebné publikovať v zóne danej domény platný (alebo viacero) CDS záznam správcom menného servera.

Touto službou SK-NIC implementuje CDS záznam v súlade s technickou špecifikáciou RFC 8078 (viď. <https://tools.ietf.org/html/rfc8078>, k dispozícii v anglickom jazyku).

Okrem základného fungovania doplníme aj niekoľko ďalších pravidiel, ktoré platia pre tento systém v doméne .sk:

- CDS záznamy musia byť platné, aby boli systémom použité - algoritmus a typ digestu musia obsahovať platné hodnoty z registrov IANA, digest musí mať správnu dĺžku pre zadaný algoritmus a podobne,
- ak je CDS záznam stabilný a platný po obdobie 72 hodín, záznamy v Centrálnom registri domén sa zodpovedajúco aktualizujú - akékoľvek existujúce DS záznamy sa nahradia novými záznamami odvodenými z CDS záznamu,
- pre použitie „kill recordu“ je potrebné nastaviť údaje v CDS zázname na nulové hodnoty - následne budú pri doméne v registri odstránené všetky existujúce DS záznamy, príklad: *example.tld. 38400 IN CDS 0 0 0 0*
- akékoľvek údaje zaznamenané v DS záznamoch domény prostredníctvom EPP alebo registrátorskej konzoly budú v prípade existencie CDS záznamu pri doméne a odlišnosti od záznamov v registri prepísané údajmi z CDS záznamov.