Zvýšení bezpečnosti transferu objektů registru

22.11.2022 zdenek.bruna@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ

Agenda

- Co to je transfer objektu
- Jak transfer probíhá
- Novinky 2022
- Implementační složitosti
- Další uvažovaná vylepšení
- Situace v jiných registrech
- Možné změny v budoucnu

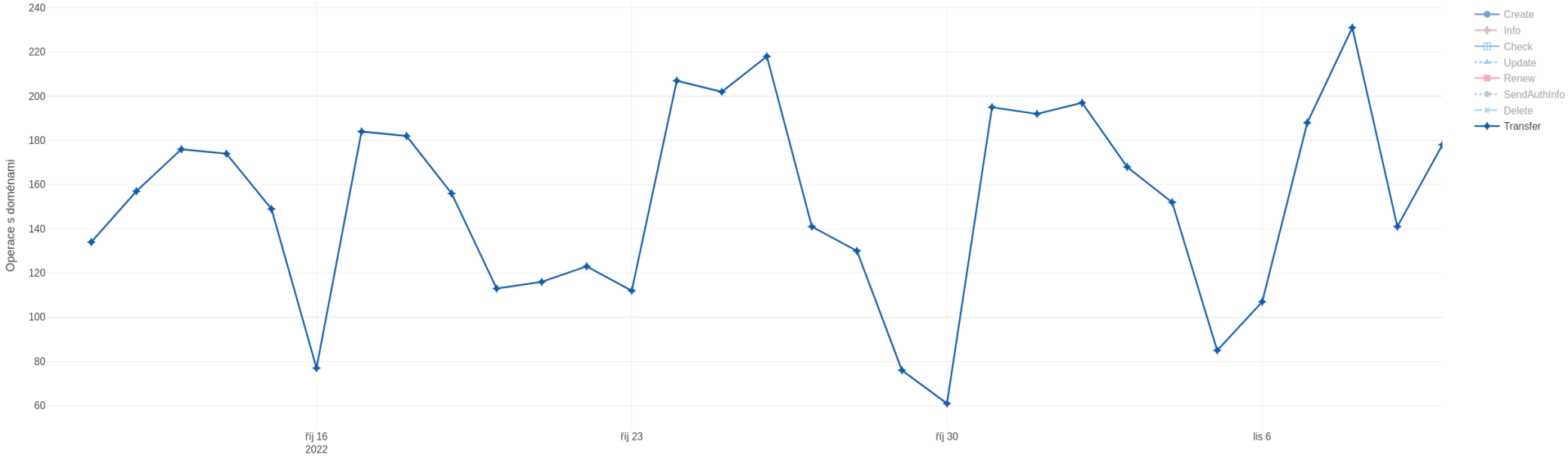
Co to je transfer objektu

- subjekty vázané na doménu – i nepřímo (a lze je měnit)
  - registr
  - držitel
  - administrativní kontakt
  - technický správce (sady nameserverů, DNSSEC klíčů)
  - provozovatel webhostingu, mailhostingu
  - **registrátor**

transfer objektu ~ změna registrátora

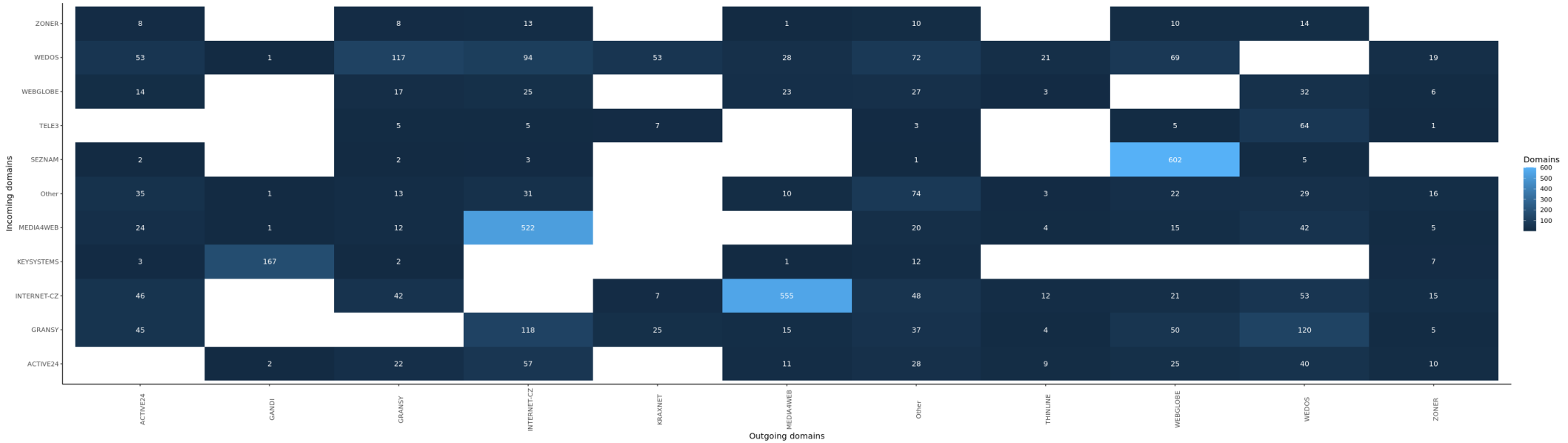
Co to je transfer objektu

- změna registrátora domény: četnost
  - do cca 250 domén denně (přirozená)
  - ~ 3-4% domén ročně



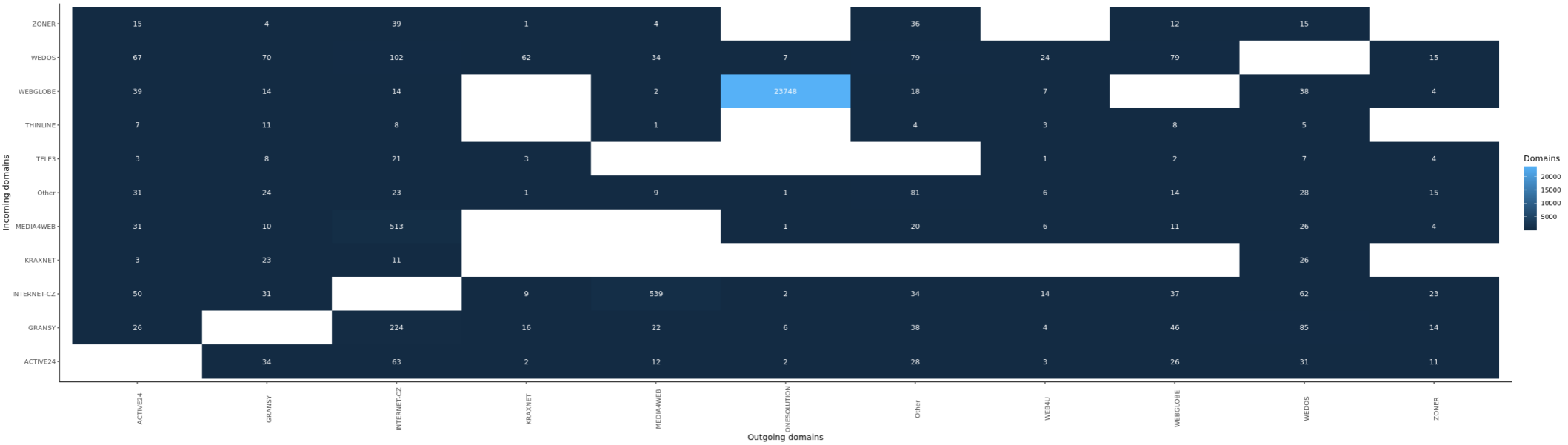
Co to je transfer objektu

- změna registrátora domény: odkud – kam – září 2022



Co to je transfer objektu

- změna registrátora domény: odkud – kam – říjen 2022



Jak transfer probíhá

- přes registrátora
- je třeba znát tzv „authinfo“ ~ „auth-id“ ~ „heslo pro transfer“
  - od určeného registrátora
  - v rozhraní cílového registrátora
  - na webu CZ.NIC: https://www.nic.cz/whois/send-password/
  - v Doménovém prohlížeči: https://www.domenovyprohlizec.cz/
- authinfo se pak předává cílovému registrátorovi
- cílový registrátor volá funkci transferu objektu (s přiložením authinfo kódu)
- registr zapíše změnu registrátora

Novinky 2022

- nemění se proces transferu
- mění se způsob nakládání s authinfo (využití RFC 9154 z 12/2021)
  - **dříve bylo**
    - nastavováno v okamžik vzniku
    - až do transferu objektu neměnné (nehashované)
    - k dispozici pro čtení (určeným registrátorem, přes doménový prohlížeč, pomocí žádosti)

  => potenciální bezpečnostní riziko
    - možný únik relativně trvalých authinfo kódů
    - nutnost přegenerovávat v případě bezp. incidentů

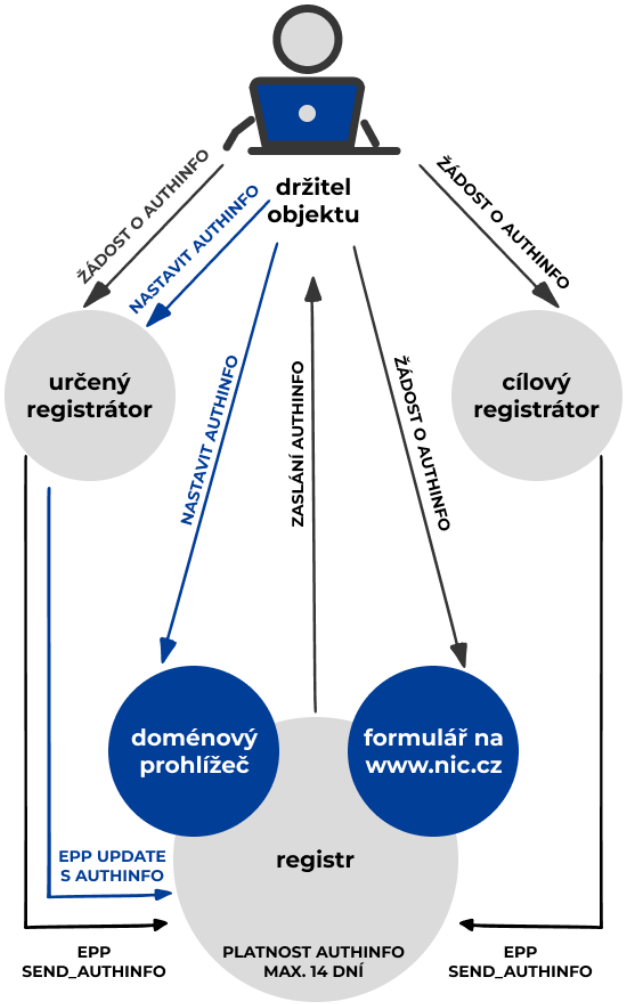
  => nemalá režie s trvalým uchováváním (i historie změn)

Novinky 2022

- mění se způsob nakládání s authinfo
  - **nově**
    - se nezadává při založení objektu
    - si jej držitel vyžádá, až když jej potřebuje
      - zůstává možnost zadat nebo generovat
    - až potom authinfo k objektu ukládáme (už zahashované)
    - platnost authinfo 14 dní (nebo do transferu / přegenerování)
    - možnost více authinfo kódů (každý registrátor 1)

  => snížení bezpečnostního rizika

  => nemusíme udržovat platné authinfo u většiny objektů



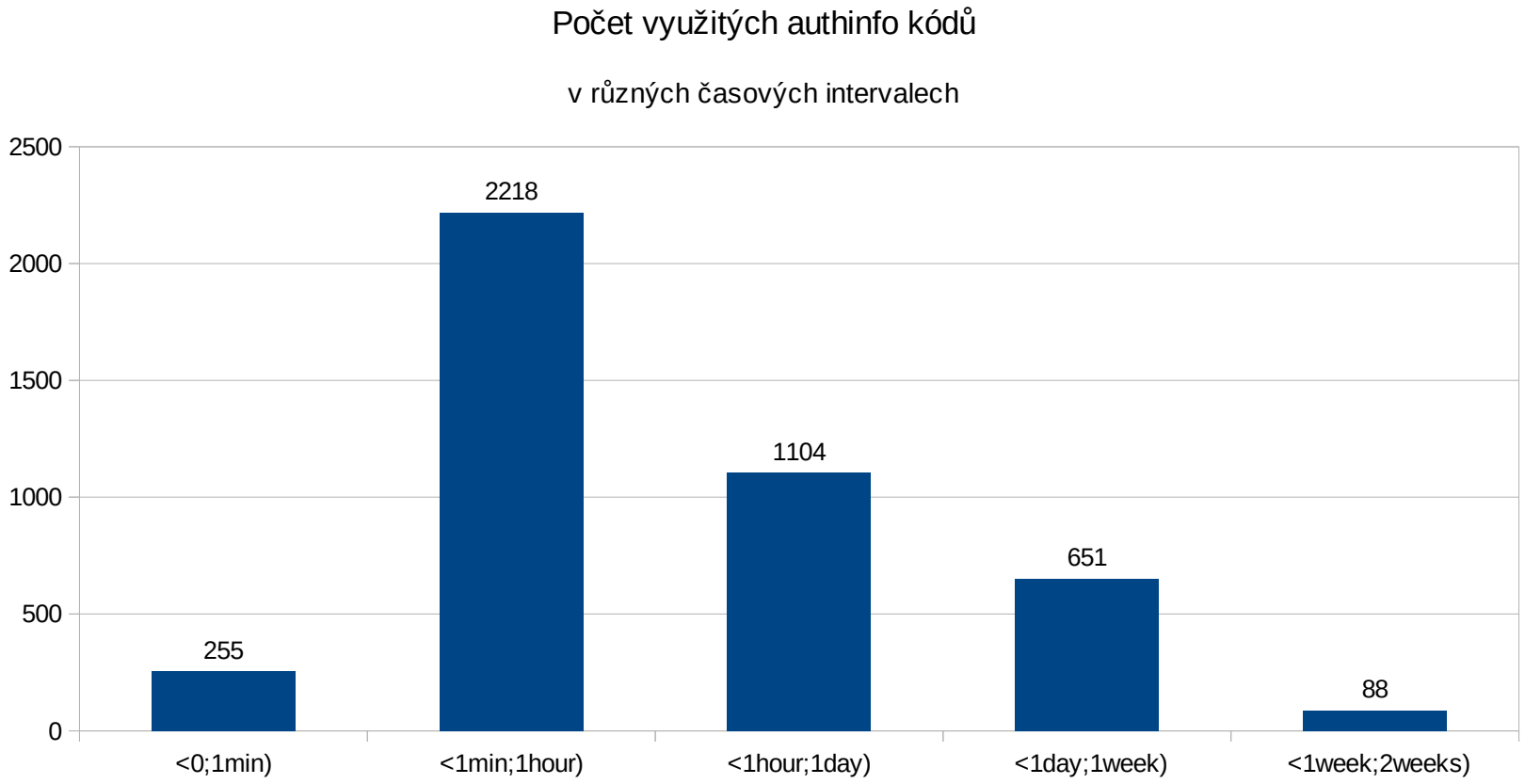
Novinky 2022

- další využití authinfo
  - pro transfer objektu lze využít authinfo oprávněného kontaktu (není novinka)
    - efektivní pro transfer více domén jednoho držitele
    - v tomto případě je nově authinfo platné 14 dní (nezneplatňuje se po transferu 1 objektu)
  - získání skrytých údajů kontaktu
    - registrátor „vidí“ všechny údaje pouze kontaktů, pro které je určeným registrátorem
    - pomocí zadání authinfo mu držitel kontaktu může povolit na údaje nahlédnout
    - v tomto případě také nezneplatňujeme authinfo

Implementační složitosti

- nemožnost nasadit pouze na straně registru
  - nutná souhra s registrátory
    - příprava konceptu → seminář s registrátory → změny → nasazení na veřejném testu → testování registrátory → další změny → nasazení do produkce
    - příklad změn parametrů:
      - TTL 2 dny → 14 dní
      - nemožnost nastavení authinfo určeným registrátorem → povoleno
      - zneplatnění authinfo po využití pro čtení skrytých údajů o kontaktu → zůstává platné
      - vytváření objektů registrátorem se zadaným authinfo selže → nezapíše authinfo
- vyřešit co s aktuálně probíhajícími transfery
  - aplikace TTL 14 dní pro 0-14 dní „staré“ authinfo kódy
  - ostatní museli získat authinfo znovu

Implementační složitosti

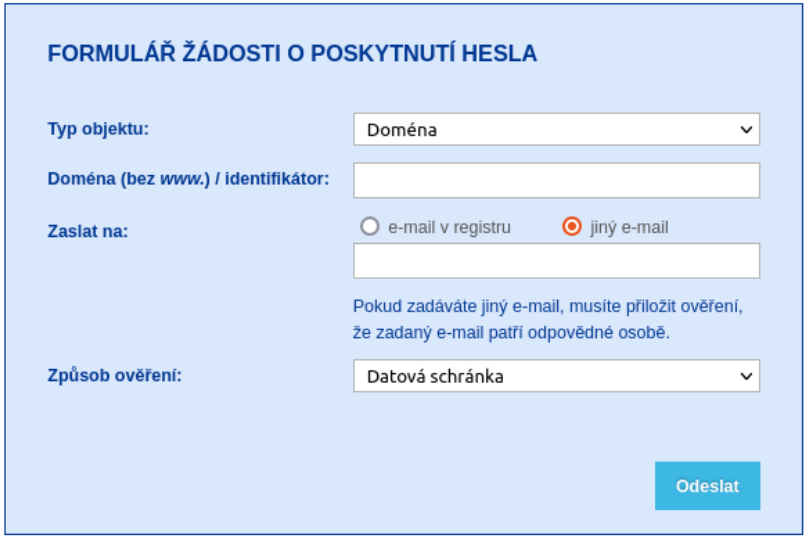


Další uvažovaná vylepšení

- v Doménovém prohlížeči
  - možnost generovat a zaslat authinfo
  - nastavit authinfo i pro navázané objekty (doména, nsset, keyset)
  - zobrazit aktuálně platné authinfo záznamy (registrátor, platnost, zrušení)

Další uvažovaná vylepšení

- v rozhraní pro helpdesk (FERDA)
  - zobrazit aktuálně platné authinfo záznamy (registrátor, platnost, zrušení)
  - možnost generovat a poslat authinfo (i na jiný e-mail)
    - pro zpracování žádostí z: https://www.nic.cz/whois/send-password/



Další uvažovaná vylepšení

- u registrátorů
  - provést analýzu síly zadávaných authinfo kódů (v souladu s RFC 9154)
    - přejít na model volání generování authinfo kódů přes registr
      - 2/3 registrátorů aktuálně využívají funkce nastavování authinfo kódů jimi
    - zavést vynucování minimální síly nastavovaných authinfo kódů
      - aktuálně je nejčastěji počet znaků mezi 10-15 (objevují se ale i délky 6 nebo 30+ znaků)
      - v Doménovém prohlížeči máme tato pravidla:
        - délka minimálně 8 znaků
        - znaky alespoň ze 3 z následujících 4 skupin: číslice, malá písmena, velká písmena, ostatní znaky.
        - malá podobnost jinému údaji
        - zamezení opakování stejných hesel
    - bude předmětem dalších jednání s registrátory

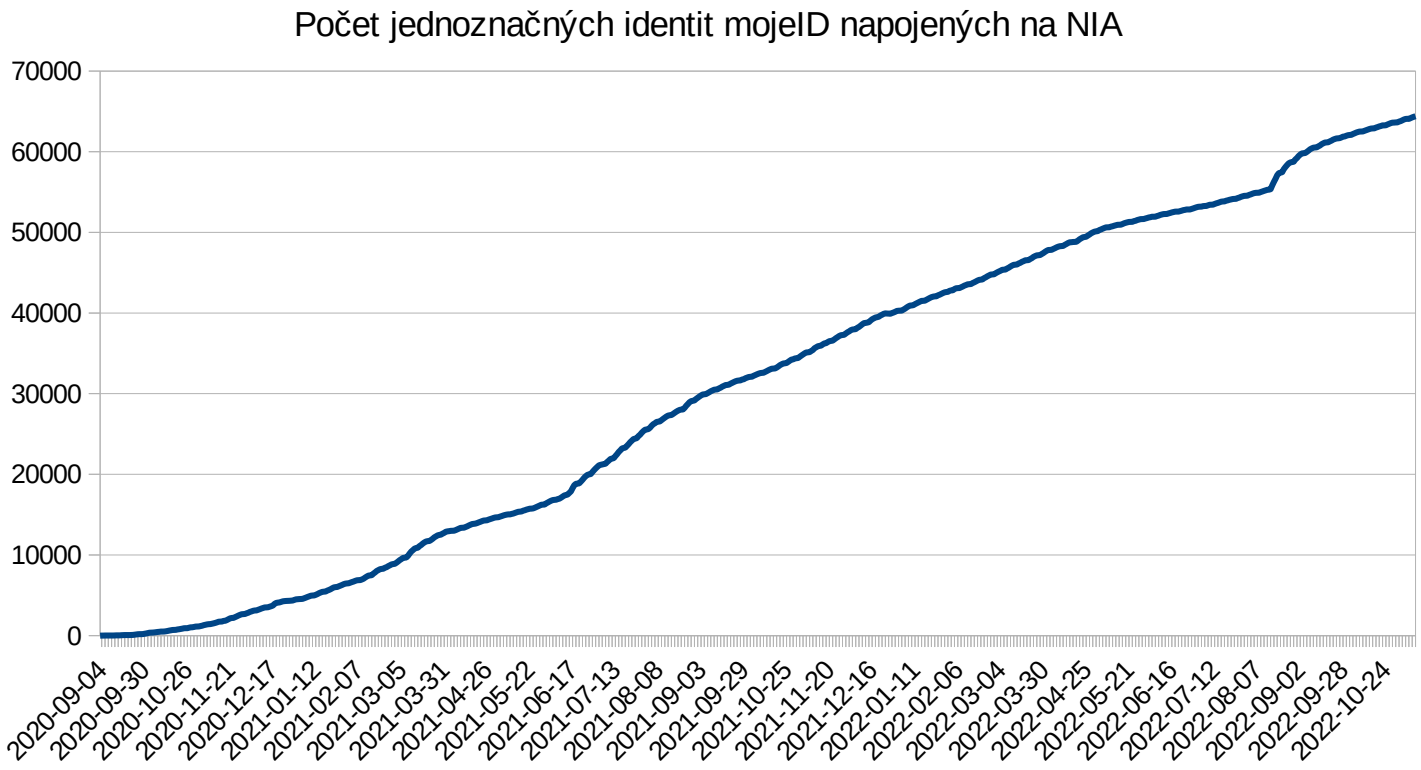
Situace v jiných registrech

- jak to mají jinde
  - s hashováním authinfo kódů se začíná
    - DENIC používá hashování (ale nemají EPP)
    - NIC.AT chce zavést (zatím se nedomluvili s registrátory)
    - SK-NIC o tom zatím neuvažuje
    - NASK.PL o tom zatím neuvažuje

Možné změny v budoucnu

- jsou i jiné způsoby jak získat souhlas uživatele s transakcí
  - OAuth 2.0 Authorization Framework (RFC 6749)
  - rozšíření EPP o tzv. alokační token (RFC 8495)
  - využití ověřených identit napojených na registr

Možné změny v budoucnu



Z toho 6397 jako držitel nebo admin-c u domén (< 1%)

Děkuji vám za pozornost!

Zdeněk Brůna

22.11.2022 zdenek.bruna@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ