Pravidla technické komunikace

Technické oddělení CZ.NIC

10.12.2024

Obsah

1 Úvod....2
2 Protokol komunikace....2
3 Přihlašovací údaje a limity pro komunikaci....2
4 Pravidla pro vytvoření požadavku o SSL certifikát k přístupu do EPP systému....3
5 Nacenění dotazů do registru....4
6 Pravidla pro tvorbu identifikátorů....4
7 Automatické slučování duplicitních kontaktů....5
8 Skrývání osobních údajů u kontaktu....5
9 Zacházení se sadou klíčů při změně sady jmenných serverů u domény....7
10 Mazání domén....7
11 Mazání nepoužívaných kontaktů, sad jmenných serverů a sad klíčů; ochranná lhůta pro smazané objekty....8
12 Technické kontroly jmenných serverů....8
13 Komunikace Centrálního registru....9
14 Autorizační informace (AuthInfo)....12

CZ.NIC, z. s. p. o.
Milešovská 1136/5, 130 00 Praha 3
IČ 67985726
DIČ CZ67985726
T +420 222 745 111
M +420 731 657 660
kontakt@nic.cz
www.nic.cz

1 Úvod

Tento dokument popisuje především pravidla komunikace mezi registrátorem a Centrálním registrem, ale také komunikaci Centrálního registru směrem ke kontaktům (držitelům, administrativním a technickým kontaktům), která se odvíjí od činnosti registrátora nebo Centrálního registru.

Registrátor může ke komunikaci použít jakýkoliv nástroj, který bude splňovat podmínky uvedené v tomto dokumentu.

2 Protokol komunikace

Komunikačním protokolem je Extensible Provisioning Protocol (EPP) založený na XML. Naše implementace EPP vychází ze standardů RFC, ale zavádí zvláštní přizpůsobení a rozšíření.

Vše o naší implementaci EPP je sepsáno jako součást dokumentace softwaru registru v referenční příručce FRED Documentation / EPP Reference Manual. Podle toho, jaké máte znalosti protokolu, doporučujeme prostudovat alespoň následující kapitoly:

- Kapitola Protocol basics obsahuje úvod do protokolu EPP a shrnuje obsah hlavního standardu k EPP.
- Kapitola Managed objects obsahuje popis typů objektů spravovaných registrem, jejich atributů, stavů a přehled příkazů, které jsou vázané na daný typ objektu.
- Kapitola Command & response structure obsahuje detailní referenci všech příkazů a odpovědí, včetně jejich syntaxe a dalších omezení; zahrnuje také praktické příklady.

Schémata XSD pro validaci XML na straně klienta jsou k dispozici na stránce Registrační systém.

3 Přihlašovací údaje a limity pro komunikaci

Každá jednotlivá komunikace EPP začíná autentizací registrátora uživatelským jménem a heslem v EPP příkazu `login`. Uživatelské jméno a heslo přidělí registrátorovi provozovatel registru.

Zabezpečení TLS vyžaduje klientský certifikát. Otisk certifikátu (fingerprint) musí registrátor doručit provozovateli registru pro jeho zavedení do ověřovacího procesu. Systém akceptuje komerční certifikáty vydané kteroukoliv z certifikačních autorit akreditovaných v ČR pro vydávání kvalifikovaných certifikátů nebo certifikáty vygenerované přímo provozovatelem registru. V testovacím režimu je možné použít pouze certifikáty vygenerované přímo provozovatelem registru.

Maximální počet souběžných přihlášení jednoho registrátora je 5.

Doba, po které je neaktivní sezení uzavřeno a registrátor odpojen, je 5 minut.

Rychlost otevírání nových spojení je limitována na 100 za minutu. Toto platí celkově přes všechna EPP spojení všech registrátorů.

4 Pravidla pro vytvoření požadavku o SSL certifikát k přístupu do EPP systému

OpenSSL příkaz pro vygenerování requestu:

```
openssl req -new -keyform PEM -outform PEM -subj "/C=CZ/L=Prague/O=Firma, s.r.o./
‹→CN=*.firma.cz/emailAddress=podpora@firma.cz/" -out jmeno_spolecnosti.csr -newkey␣
‹→ec -pkeyopt ec_paramgen_curve:secp384r1 -sha384 -keyout nazev_souboru_s_klicem.key
```

Specifikace SSL příkazu:

- **Formát requestu: `Base64 PEM`**
  - Název souboru: `jmeno_spolecnosti.csr`, případně `jmeno_spolecnosti-test.csr`, pokud subjekt používá rozdílné certifikáty pro produkci a pro test
  - Způsob dodání: `Přílohou v e-mailu` na adresu registrars@nic.cz
- **SSL atributy:**
  - **C** (Country): dvoupísmenný název (ISO formát), např. `CZ`
  - **L** (Locality/City): nezkrácený název města, kde je organizace registrovaná, např. `Prague` nebo `Praha`
  - **O** (Organisation Name): registrovaný název organizace, např. `Firma, s.r.o.`
  - **CN** (Common Name): uvede se wildcard domény, ze které bude registrátor testovat, např. `*.firma.cz`
  - **emailAddress**: uvede se funkční e-mail/alias, na kterém lze kontaktovat společnost, např. `podpora@firma.cz`
- **Zabezpečení:**
  - Key type: ECDSA
  - Key size: `P-384`
  - Hash algoritmus: `SHA-384`
  - Platnost certifikátu: `2 roky`

Při nesplnění této specifikace bude žádost vrácena k opravení.

5 Nacenění dotazů do registru

Registrátor získává každý měsíc určité množství nezpoplatněných (volných) dotazů.

Množství volných dotazů je určeno individuálně na začátku měsíce podle aktuálního počtu zaregistrovaných domén, přičemž na každou doménu připadá 100 volných dotazů. Celkový počet volných dotazů však nikdy není menší než 25 000 ks.

Jakmile registrátor vyčerpá volné dotazy, jsou všechny další dotazy zpoplatněny podle položky „Cena za jeden EPP dotaz“ dle aktuálního ceníku.

6 Pravidla pro tvorbu identifikátorů

Identifikátory objektů (u domén uváděných v elementu `name` a u kontaktů, sad jmenných serverů a sad klíčů v elementu `id`) je možné volit na základě následujících pravidel.

Doménová jména v zóně `cz`

- skládají se ze 2 částí[1] oddělených tečkou `.`,
  - **první část jména**[1]
    - obsahuje pouze písmena anglické abecedy (malá i velká), číslice (znaky `0` až `9`) a znak spojovník `-`[2],
    - nezačíná ani nekončí znakem `-`[2],
    - neobsahuje 2 či více znaků `-`[2] za sebou,
    - má délku 1 až 63 znaků,
- druhá část jména je zóna `cz`,
- smí mít na samém konci tečku.

Registr nerozlišuje velikost písmen a prezentuje doménová jména převedená na malá písmena.

Doménová jména v zóně `0.2.4.e164.arpa` (ENUM)

- skládají se z 6 až 15 částí[1] (včetně zóny) oddělených tečkou `.`,
- každá část jména[1] předcházející zóně obsahuje právě jednu číslici (znaky `0` až `9`),
- končí zónou `0.2.4.e164.arpa`,
- smí mít na samém konci tečku.

Registr nerozlišuje velikost písmen a prezentuje doménová jména převedená na malá písmena.

1 Část jména (= *label*) – popisek na dané úrovni v doménovém jménu.

2 Znak základní sady ASCII pro spojovník.

Ostatní identifikátory

Identifikátory (handle) kontaktů, sad jmenných serverů a sad klíčů:

- obsahují pouze písmena anglické abecedy (malá i velká), číslice (znaky `0` až `9`) a znak spojovník `-`[2],
- nezačínají ani nekončí znakem `-`[2],
- délka nepřekračuje 30 znaků.

Registr nerozlišuje velikost písmen a prezentuje identifikátory převedené na velká písmena.

7 Automatické slučování duplicitních kontaktů

Centrální registr pravidelně slučuje duplicitní kontakty, které sám detekuje ve své databázi. Tato procedura je spouštěna jednou týdně v pondělí dopoledne.

Kontakty jsou považovány za duplikáty, pokud mají shodné hodnoty klíčových atributů, viz FRED Documentation / Contact merger / Identical contacts.

Slučují se pouze kontakty, které mají stejného určeného registrátora.

Centrální registr automaticky vybírá cílový kontakt, do něhož se duplikáty sjednotí a jímž se pak nahradí ostatní duplikáty u navázaných objektů, podle daných kvalitativních kritérií, jež jsou stanovena v dokumentaci viz FRED Documentation / Contact merger / Selection of the destination contact in an automatic merger.

Kontakty, jejichž určeným registrátorem je CZ.NIC nebo MojeID, nejsou do automatického slučování zahrnuty.

8 Skrývání osobních údajů u kontaktu

Registr přistupuje k osobním údajům v souladu s regulací GDPR, tedy většinu z nich nezveřejňuje ve veřejných rozhraních (whois). Zároveň však umožňuje nastavit odkrytí některých údajů na základě preference kontaktu.

Preferenci kontaktu nastavuje element `<contact:disclose>` v operacích `contact:create` (syntaxe create) a `contact:update` (syntaxe update).

Preference pro odkrytí se nastavuje pomocí hodnoty atributu `flag='1'`, který říká, že uvedené údaje chce kontakt zveřejnit, a vyjmenováním příznaku údajů.

Upozornění

Pokud použijete `flag='0'` s libovolným obsahem, vše se nastaví podle výchozí politiky serveru. Nedoporučujeme používat; kvůli zvláštním podmínkám nastavení příznaku u *address* může být odladění příkazu problematické.

Lze manipulovat s nastavením odkrytí údajů:

- *address* (adresy[3], jen za určitých podmínek, viz dále),
- *telephone* (telefon),
- *fax* (fax),
- *email* (e-mail),
- *vat* (DIČ),
- *ident* (identifikační údaj),
- *notifyemail* (notifikační e-mail).

S nastavením údajů *name* (jméno) a *organization* (organizace) nelze manipulovat, ty jsou vždy zveřejněné a v příkazech ani odpovědích se neuvádí.

Výchozí politika serveru

Pokud v `contact:create` použijete prázdný element <`contact:disclose`> nebo ho vynecháte úplně, nastaví se výchozí příznaky.

Výchozí příznaky pro `contact:create`:

name	organization	address	telephone	fax	email	vat	ident	notifyemail
zveřejni	zveřejni	zveřejni	skryj	skryj	skryj	skryj	skryj	skryj

Pokud v `contact:update` použijete prázdný element <`contact:disclose`> nebo ho vynecháte úplně, znamená to, že není požadována změna nastavení příznaku.

Skrývání adresy

Na údaj *address* se vztahují zvláštní pravidla:

- nelze jej nastavit v operaci `contact:create`, skrývání je nastaveno serverem na *zveřejni*,
- jakmile je kontakt, který nemá vyplněn údaj *organization*, plně identifikovaný (má stav `identifiedContact`) nebo validovaný (má stav `validatedContact`):
  - skrývání je automaticky nastaveno serverem na *skryj*,
  - je možné změnit nastavení preference v operaci `contact:update`.
- pokud kontakt přijde o oba výše uvedené stavy, skrývání je automaticky serverem přepsáno opět na *zveřejni*.

Interpretace výsledku `contact:info`

Operace vrací preferenci kontaktu na zveřejnění údajů.

S výjimkou údajů *name* a *organization*, které registr nastavuje napevno, se nastavení zveřejnění údaje interpretuje podle přítomnosti odpovídajícího elementu.

3 Příznak adresy ovlivňuje zobrazení všech adres v kontaktu.

Např. odpověď na `contact:info` obsahuje:

```
<contact:disclose flag="1">
    <contact:addr/>
    <contact:email/>
    <contact:vat/>
    <contact:ident/>
</contact:disclose>
```

Interpretace výsledku:

name	organization	address	telephone	fax	email	vat	ident	notifyemail
zveřejni	zveřejni	zveřejni	skryj	skryj	zveřejni	zveřejni	zveřejni	skryj

9 Zacházení se sadou klíčů při změně sady jmenných serverů u domény

Pokud se doméně přiřadí nová sada jmenných serverů, která obsahuje stejné jmenné servery jako ta původní, tak se sada klíčů ponechá.

Pokud se doméně přiřadí nová sada jmenných serverů, která obsahuje jiné jmenné servery než ta původní, sada klíčů se automaticky odebere.

Pokud je součástí požadavku na změnu sady jmenných serverů i zopakování identifikátoru sady klíčů, tak ten zůstane nastavený.

Pokud se doméně odebere sada jmenných serverů, odebere se automaticky i sada klíčů.

10 Mazání domén

Domény, které mají již 61 dní po expiraci, jsou označeny stavem `deleteCandidate`, čímž jsou určeny ke smazání. Týž den se takto označené domény průběžně a nahodile mažou.

V odpovědi na EPP příkaz `check_domain` se domény ve stavu `deleteCandidate` jeví jako obsazené a jejich stav i podrobné informace lze zjistit z odpovědi na EPP příkaz `info_domain` až do okamžiku, kdy jsou skutečně smazány, avšak již není možné jejich registraci prodloužit.

Veřejná rozhraní (WHOIS) zobrazují o doménách ve stavu `deleteCandidate` pouze informaci o tom, že doména je určena ke zrušení. Tato informace je pak ve veřejných rozhraních k dispozici až do okamžiku další registrace (kdy se zobrazí údaje související s novou registrací) nebo do následujícího dne. Veřejné služby tudíž v den rušení domény neinformují o tom, zda už doména byla fyzicky zrušena a je volná k registraci.

11 Mazání nepoužívaných kontaktů, sad jmenných serverů a sad klíčů; ochranná lhůta pro smazané objekty

Kontakty, které po dobu 6 předcházejících měsíců nebyly přiřazeny k žádnému doménovému jménu, sadě jmenných serverů nebo sadě klíčů, a současně u kontaktu nebyla provedena žádná změna, jsou Centrálním registrem smazány.

Sady jmenných serverů, které po dobu 6 předcházejících měsíců nebyly přiřazeny k žádnému doménovému jménu, a současně u sady jmenných serverů nebyla provedena žádná změna, jsou Centrálním registrem smazány.

Sady klíčů, které po dobu 6 předcházejících měsíců nebyly přiřazeny k žádnému doménovému jménu, a současně u sady klíčů nebyla provedena žádná změna, jsou Centrálním registrem smazány.

Kontakty, sady jmenných serverů a sady klíčů, které jsou smazány Centrálním registrem pro jejich nepoužívání nebo registrátorem pomocí příslušného příkazu EPP, jsou zařazeny do ochranné lhůty v trvání 2 měsíců od data smazání.

V průběhu ochranné lhůty nelze identifikátor (handle) kontaktu, sady jmenných serverů nebo sady klíčů použít jako identifikátor nově registrovaného objektu (kontaktu, sady jmenných serverů, sady klíčů). Po skončení ochranné lhůty lze smazaný identifikátor (handle) opětovně použít při registraci nového kontaktu, sady jmenných serverů, resp. sady klíčů.

12 Technické kontroly jmenných serverů

Technické kontroly sad jmenných serverů se provádějí periodicky za účelem monitorování stavu jmenných serverů, na něž jsou delegována doménová jména. Technická kontrola spustí kompletní sadu testů přes službu Zonemaster u každé jednotlivé domény, která je k určitému jmennému serveru přiřazena. Test každé domény končí výsledkem závažnosti (critical, error, warning, notice, info). Jednotlivé testy a výsledky závažnosti jsou popsány v dokumentaci projektu Zonemaster.

Technické kontroly následně zpracují výsledky testů domén a přiřadí sadě jmenných serverů hodnocení dle nejzávažnějšího nalezeného výsledku. Poté je odeslán e-mail technickým správcům sady jmenných serverů dle nastavené úrovně reportingu. Rozlišujeme tyto úrovně reportování:

- 0 – reportování zcela vypnuto
- 1 – reportování probíhá jen pokud je výsledek „critical“
- 2 – reportování probíhá jen pokud je výsledek „critical“ nebo „error“ (výchozí nastavení)
- 3 – reportování probíhá jen pokud je výsledek „critical“, „error“ nebo „warning“
- 4 – reportování probíhá jen pokud je výsledek „critical“, „error“, „warning“ nebo „notice“

Testy nemají vliv na zařazení nebo vyřazení domény ze zóny, výsledky testu jsou pouze informativní.

13 Komunikace Centrálního registru

Tabulka obsahuje popis, časové určení a adresáty jednotlivých typů komunikace Centrálního registru se zohledněním poll zpráv, které jsou určeny pro potřeby registrátorů.

Tabulka 1: Komunikace Centrálního registru

Typ	Kdy	Adresát	Poznámka
Notifikace	po provedené změně domény	notifikační e-mail držitele	jako poll zprávu obdrží i registrátor, pokud změnu provedl registr (update, delete)
Notifikace	po provedené změně kontaktu	notifikační e-mail kontaktu	jako poll zprávu obdrží i registrátor, pokud změnu provedl registr (update, delete)
Notifikace	po provedeném updatu kontaktu, který je navázán na doménu jiného registrátora		jako poll zprávu obdrží registrátor domény, ke které je kontakt navázán
Notifikace	po provedené změně sady jmenných serverů	notifikační e-mail technických kontaktů	
Notifikace	po provedené změně sady klíčů	notifikační e-mail technických kontaktů	
Notifikace	po změně registrátora	notifikační e-mail příslušného kontaktu	jako poll zprávu obdrží původní registrátor
Pravidelná žádost o kontrolu a opravu dat u kontaktu	každoročně 2 měsíce před datem registrace kontaktu	e-mail kontaktu	
Zaslání autorizační informace domény	po přijetí žádosti o zaslání AuthInfo	notifikační e-mail držitele a administrativních kontaktů	

Pokračování na další stránce

Tabulka 1 – pokračování

Typ	Kdy	Adresát	Poznámka
Zaslání autorizační informace kontaktu	po přijetí žádosti o zaslání AuthInfo	notifikační e-mail kontaktu	
Zaslání autorizační informace sady jmenných serverů	po přijetí žádosti o zaslání AuthInfo	notifikační e-mail technických kontaktů	
Zaslání autorizační informace sady klíčů	po přijetí žádosti o zaslání AuthInfo	notifikační e-mail technických kontaktů	
Validace	30 dní před vypršením data validace		jako poll zprávu obdrží registrátor
Validace	15 dní před vypršením data validace	e-mail držitele a administrativních kontaktů	
Expirace	30 dní před datem expirace		jako poll zprávu obdrží registrátor
Expirace	v den expirace	e-mail držitele a administrativních kontaktů	jako poll zprávu obdrží i registrátor
Vyřazení ze zóny po expiraci	30 dní po datu expirace	e-mail držitele, administrativních kontaktů a tech. kontaktů sady jmenných serverů	jako poll zprávu obdrží i registrátor
Vyřazení ze zóny – validace	v den vypršení validace	e-mail držitele, administrativních kontaktů a tech. kontaktů sady jmenných serverů	jako poll zprávu obdrží i registrátor
Upozornění na konec ochranné lhůty	33 dní po datu expirace	papírový dopis na adresu držitele	*zrušeno*, od 1.1.2019 už se neposílá
Zrušení doménového jména	61 dní po expiraci	e-mail držitele, administrativních kontaktů a tech. kontaktů sady jmenných serverů	jako poll zprávu obdrží i registrátor
Zrušení doménového jména	v den zrušení		jako poll zprávu obdrží registrátor

Pokračování na další stránce

Tabulka 1 – pokračování

Typ	Kdy	Adresát	Poznámka
Zrušení nepoužívaného kontaktu, sady jmenných serverů nebo sady klíčů	v den zrušení	e-mail kontaktu, resp. technických kontaktů	jako poll zprávu obdrží i registrátor
Výsledky technické kontroly	na žádost		jako poll zprávu obdrží registrátor
Výsledky technické kontroly	periodicky	e-mail tech. Kontaktů přísl. sady jmenných serverů	
Daňový doklad	měsíčně	e-mail registrátorovi	daň. doklad v PDF a XML
Daňový doklad na přijatou zálohu	po spárování zálohy	e-mail registrátorovi	daň. doklad v PDF a XML
Automatické sloučení duplicitních kontaktů	po sloučení záznamů	e-mail kontaktu	navíc i běžnou notifikaci při změně domény, sady jmenných serverů nebo sady klíčů, viz první řádky tabulky
Automatická správa klíčů – zahájení zkušební doby	po nalezení platného záznamu CDNSKEY na nezabezpečené doméně	e-mail tech. Kontaktů přísl. sady jmenných serverů	
Automatická správa klíčů – zrušení zkušební doby	při změně CDNSKEY záznamu nebo jeho odstranění během zkušební doby	e-mail tech. Kontaktů přísl. sady jmenných serverů	
Automatická správa klíčů – dovršení zkušební doby	aktualizace domény s nově přijatou automaticky spravovanou sadou klíčů		jedná se o běžnou notifikaci při změně domény, viz první řádek tabulky
Automatická správa klíčů – aktualizace klíčů	při nalezení platného záznamu CDNSKEY na zabezpečené doméně	e-mail tech. Kontaktů přísl. sady jmenných serverů	

14 Autorizační informace (AuthInfo)

Autorizační informaci (AuthInfo) registr vyžaduje při změně určeného registrátora objektů (transfer). Dále AuthInfo umožňuje jinému než určenému registrátorovi získat přístup ke skrytým údajům kontaktu.

AuthInfo má dobu platnosti (TTL) 14 dní.

Minimální délka AuthInfo je 8 znaků.

V rámci odpovědi na příkaz `sendAuthInfo` se registrátorům vrátí maskovaná informace, na který e-mail bylo AuthInfo zasláno (např. a*****@b*****.**).

Od FRED verze 2.48.0, v souladu s RFC 9154, je příkaz `create` obsahující neprázdnou hodnotu AuthInfo zakázaný. Pokud `create` hodnotu AuthInfo vůbec neobsahuje či je prázdná, bude akceptován.