

Pravidla technické komunikace

Obsah

1. Úvod	1
2. Protokol komunikace	1
3. Přihlašovací údaje a limity pro komunikaci	1
4. Pravidla pro tvorbu identifikátorů	2
5. Mazání nepoužívaných kontaktů, sad nameserverů a sad klíčů, ochranná lhůta pro smazané objekty ..	2
6. Popis technických testů	2
7. Komunikace Centrálního registru	3
A. Schémata EPP protokolu	4
B. Popis jednotlivých funkcí	4

1. Úvod

V tomto dokumentu je popsána komunikace registrátorů s centrálním registrem. Registrátoři mohou ke komunikaci použít jakýkoliv nástroj, který bude splňovat podmínky uvedené v tomto dokumentu.

2. Protokol komunikace

Komunikačním protokolem je Extensible Provisioning Protocol (EPP). EPP je protokol založený na XML. Popis jeho základních vlastností a způsobu rozšíření je uveden v RFC 3730 (<http://www.rfc-archive.org/getrfc?rfc=3730>).

Transportní vrstvu pro EPP zprávy zajišťuje protokol TCP/IP se zabezpečením pomocí TLS. EPP komunikace přes TCP je definována v RFC 3734 (<http://www.rfc-archive.org/getrfc?rfc=3734>).

Příkazy pro manipulaci s objektem Kontakt vycházejí z rozšíření EPP pro kontakty, které je definované v RFC 3733 (<http://www.rfc-archive.org/getrfc?rfc=3733>). Změny provedené v této specifikaci jsou přidání nových položek oznamovacího emailu, daňového identifikačního čísla (VAT), osobního identifikačního čísla a jeho typu, nahrazení dvou poštovních adres jednou a výpis seznamu kontaktů držených registrátorem.

Příkazy pro manipulaci s objektem Sada nameserverů částečně vycházejí z rozšíření EPP pro obecné servery, které je definované v RFC 3732 (<http://www.rfc-archive.org/getrfc?rfc=3732>). Specifickým rozšířením je přidání položky „report level“ pro stanovení úrovně technických testů, výpis seznamu sad nameserverů držených konkrétním registrátorem a výpis sad nameserverů příslušejících konkrétnímu kontaktu.

Příkazy pro manipulaci s objektem Sada klíčů částečně vycházejí z rozšíření EPP pro DNSSEC, které je definované v RFC 4310 (<http://www.rfc-archive.org/getrfc?rfc=4310>). Specifickým rozšířením je výpis seznamu sad klíčů držených konkrétním registrátorem a výpis sad nameserverů příslušejících konkrétnímu kontaktu.

Příkazy pro manipulaci s objektem Doména a ENUM doména vycházejí z rozšíření EPP pro doménová jména, které je definované v RFC 3731 (<http://www.rfc-archive.org/getrfc?rfc=3731>). Změny provedené v této specifikaci jsou nahrazení seznamu nameserverů odkazem na objekt skupina nameserverů, přidání sady klíčů, omezení převodu domény, který není možné odložit (provádí se okamžitě), zjednodušení seznamu kontaktních osob na jeden typ kontaktu (admin) a výpis seznamu domén držených registrátorem.

ENUM doména obsahuje navíc datum validace.

Odkazy na uvedená schémata jsou obsahem přílohy.

3. Přihlašovací údaje a limity pro komunikaci

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

TLS zabezpečení vyžaduje klientský certifikát vydaný uznávanou certifikační autoritou. Otisk certifikátu (fingerprint) musí registrátoři 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.

Maximální počet souběžných přihlášení jednoho registrátora je 5.

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

Po každé neúspěšné operaci (EPP návratový kód je ≥ 2000) je spojení drženo po dobu 1 vteřiny

Rychlost otevírání nových spojení je limitována na 100 za minutu. Toto platí celkově pro všechna EPP spojení registrátora.

4. Pravidla pro tvorbu identifikátorů

Identifikátory objektů (element id u kontaktů, sady nameserverů a sady klíčů a element name u domén) je možné volit na základě pravidel definovaných tímto dokumentem a příslušnými schématy.

Název domény odpovídá standardu RFC 1035 (<http://www.rfc-archive.org/getrfc?rfc=1035>). Registr ignoruje velikost písmen, všechna velká písmena jsou převedena na malá. Registr ignoruje velikost písmen, všechna velká písmena jsou převedena na malá.

U identifikátoru kontaktu registr ignoruje velikost písmen, všechna malá písmena jsou převedena na velká.

U identifikátoru skupiny nameserverů registr ignoruje velikost písmen, všechna malá písmena jsou převedena na velká.

U identifikátoru sady klíčů registr ignoruje velikost písmen, všechna malá písmena jsou převedena na velká.

5. Mazání nepoužívaných kontaktů, sad nameserverů a sad klíčů, ochranná lhůta pro smazané objekty

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

Sady nameserverů, které po dobu 6 předcházejících měsíců nebyly přiřazeny k žádnému doménovému jménu a současně u sady nameserverů 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 nameserverů 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 nameserverů nebo sady klíčů použít jako identifikátor nově registrovaného objektu (kontaktu, sady nameserverů, sady klíčů). Po skončení ochranné lhůty lze smazaný identifikátor (handle) opětovně použít při registraci nového kontaktu, sady nameserverů, resp. sady klíčů.

6. Popis technických testů

Technické testy sady nameserverů se provádějí za účelem monitorování stavu nameserverů na něž jsou delegována doménová jména. Testy *nemají vliv* na zařazení nebo vyřazení domény ze zóny. Výsledky testů slouží pouze jako informace pro správce sady nameserverů nebo registrátora.

Technické testy představují sadu jednotlivých testů, které jsou v určitém pořadí aplikovány na nameserver, který je součástí nějaké sady nameserverů. Každý test se zaměřuje na testování jedné specifické věci (vlastnosti nameserveru). Výsledkem testu je status:

- Vyhověl testu
- Nevyhověl testu
- Výsledek neznámý

Poslední výsledek představuje stav, kdy test zkončil neočekávanou chybou nebo výskytem neočekávané okolnosti, která zabránila vyhodnocení výsledku vyhověl/nevyhověl.

Tabulka 1. Výčet jednotlivých testů

Název testu	Závažnost	Závisí na testech	Charakteristika
Existence	1		Testuje, zda-li DNS server běží.
Presence	2	Existence	Testuje přítomnost záznamu domény na DNS serveru.
Authoritative	3	Existence, Presence	Testuje, zda odpověď DNS serveru na danou doménu je autoritativní.
Recursive	4	Existence	Testuje, zda-li DNS server je rekurzivní na základě toho, co o sobě DNS server tvrdí.
Recursive4all	4	Existence	Testuje, zda-li DNS server je rekurzivní na základě praktické zkoušky.
Autonomous	5		Alespoň dva z DNS serverů musí být v různých autonomních systémech.
Heterogenous	6	Existence	Alespoň dva softwarově různé DNS servery.

Název testu je unikátní jednoslovné pojmenování testu, které vyjadřuje testovanou vlastnost nameserveru. Závažnost testu určuje, jak moc je podstatné selhání v tom kterém testu. Některé testy se zaměřují na testování základní funkčnosti nameserveru a některé na větší detaily, jejichž nesplnění vyloženě neohrožuje delegaci domény. Závažnost je reprezentovaná stupnicí čísel od 0 do 10. Nižší číslo znamená větší závažnost testu. V úrovni 0 se nenachází žádné testy, nejvyšší využitá úroveň je v současnosti úroveň 6. Defaultní nastavení úrovně technických testů je 3.

7. Komunikace Centrálního registru

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

Tabulka 2. Komunikace Centrálního registru

Typ	Kdy	Adresát	Poznámka
notifikace	po provedené změně domény	notify e-mail držitele	
notifikace	po provedené změně kontaktu	notify e-mail kontaktu	
notifikace	po provedené změně sady nameserverů	notify e-mail technických kontaktů	
notifikace	po provedené změně sady klíčů	notify e-mail technických kontaktů	
notifikace	po změně registrátora	notify e-mail příslušného kontaktu	jako poll message obdrží původní registrátor
pravidelná žádost o kontrolu a opravu dat u kontaktu	2 měsíce před datem registrace kontaktu	e-mail kontaktu	
zaslání autorizační informace domény	po provedené změně domény	notify e-mail držitele	
zaslání autorizační informace kontaktu	po provedené změně kontaktu	notify e-mail kontaktu	

zaslání autorizační informace sady nameserverů	po provedené změně sady nameserverů	notify e-mail technických kontaktů	
zaslání autorizační informace sady klíčů	po provedené změně sady klíčů	notify e-mail technických kontaktů	
validace	30 dní před vypršením data validace		jako poll message obdrží registrátor
validace	15 dní před vypršením data validace	držitel, administrativní kontakty	
expirace	30 dní před datem expirace		jako poll message obdrží registrátor
expirace	v den expirace	držitel, administrativní kontakty	jako poll message obdrží i registrátor
vyřazení ze zóny po expiraci	30 dní po datu expirace	držitel, administrativní kontakty, tech. kontakty sady nameserverů	jako poll message obdrží i registrátor
vyřazení ze zóny – validace	v den vypršení validace	držitel, administrativní kontakty, tech. kontakty sady nameserverů	jako poll message obdrží i registrátor
upozornění na konec ochranné lhůty	33 dní po datu expirace	dopis pozemní poštou na adresu držitele	
zrušení doménového jména	61 dní po expiraci	držitel, administrativní kontakty, tech. kontakty sady nameserverů	jako poll message obdrží i registrátor
zrušení doménového jména	v den zrušení		jako poll message obdrží registrátor
zrušení nepoužívaného kontaktu, sady nameserverů nebo sady klíčů		kontakt, resp. technické kontakty	
výsledky technických testů	na požádání		jako poll message obdrží registrátor
výsledky technických testů	periodicky	tech. kontakty přísl. sady nameserverů	jako poll message obdrží i registrátor
daňové doklady	měsíčně	registrátor	daň. doklad v pdf a xml
daňové doklady na přijatou zálohu	po spárování zálohy	registrátor	daň. doklad v pdf a xml

A. Schémata EPP protokolu

XSD schéma EPP protokolu jsou k dispozici na adrese <http://www.nic.cz/page/744/registracni-system/>

B. Popis jednotlivých funkcí

Popis jednotlivých funkcí EPP a význam jejich parametrů spolu s omezujícími podmínkami na jejich hodnoty lze nalézt na adrese <http://www.nic.cz/files/nic/doc/constraints.pdf> .