The Rules of Technical Communication

CZ.NIC Technical Department

04.04.2024

Contents

1 Introduction

This document describes mainly communication between a registrar and the Central register, but also communication of the Central register towards contacts (holders, administrative and technical contacts), which unwinds from activity of registrars and the Central register.

The registrar may communicate using any tools compatible with conditions set forth in this document.

2 Communication protocol

The Extensible Provisioning Protocol (EPP) is used as the communication protocol. The EPP is a XML-based protocol. Our implementation of the EPP is based on RFC standards but it contains unique modifications and extensions.

Everything about our implementation of EPP is described as a part of the register software documentation in the FRED Documentation / EPP Reference Manual[1]. Depending on your level of experience, we recommend to explore at least the following chapters:

- Protocol basics[2]
  An introduction to the EPP protocol and a summary of the main EPP standard.
- Managed objects[3]
  A description of objects that can be managed within the protocol and their atttributes, states, and command-response mappings.
- Command & response structure[4]
  A detailed reference of all commands and responses, including their syntax and constraints.

XSD schemas for client-side XML validation are available at http://www.nic.cz/page/744/registration-system/.

[1] https://fred.nic.cz/documentation/html/EPPReference
[2] https://fred.nic.cz/documentation/html/EPPReference/ProtocolBasics
[3] https://fred.nic.cz/documentation/html/EPPReference/ManagedObjects
[4] https://fred.nic.cz/documentation/html/EPPReference/CommandStructure

3 Login data and communication limits

Every single EPP communication starts with registrar's authentication using their user name and password in the `login` EPP command. The username and password are assigned to the registrar by the register operator.

The TLS security requires a client certificate. The registrar must deliver the certificate fingerprint to the register operator for the purposes of verification procedure. The system accepts commercial certificates issued by any certification authority, which has been accredited for the issuance of qualified certificates in the Czech Republic, or certificates generated directly by the register operator.

The maximum number of a single registrar's concurrent logins is 5.

An inactive session is closed and the registrar is disconnected after 5 minutes.

The speed of opening new connections is limited to 100 per minute. This applies globally to all EPP connections of all registrars.

4 Rules for requesting an SSL certificate to access the EPP system

OpenSSL command to generate the request:

```
openssl req -new -keyform PEM -outform PEM -subj "/C=CZ/L=Prague/O=Company, s.r.o./
↪CN=*.company.cz/emailAddress=support@company.cz/" -out company_name.csr -newkey␣
↪ec -pkeyopt ec_paramgen_curve:secp384r1 -sha384 -keyout filename_with_key.key
```

SSL command specification:

- **Request format:** `Base64 PEM`
  - File name: `company_name.csr`, or `company_name-test.csr`, if the subject uses different certificates for production and for test
  - Delivery method: `E-mail attachment` to the address `registrars@nic.cz`
- **SSL attributes:**
  - **C** (Country): two-letter code (ISO format), e.g., `CZ`
  - **L** (Locality/City): unabbreviated city name, where the organization is registered, e.g., `Prague` or `Praha`
  - **O** (Organization Name): registered name of the organization, e.g., `Company, s.r.o.`
  - **CN** (Common Name): the wildcard of the domain, from which the registrar will test, e.g., `*.company.cz`
  - **emailAddress**: working e-mail/alias, where the organizacion can be contacted, e.g., `support@company.cz`
- **Security:**

- Key type: `ECDSA`
- Key size: `P-384`
- Hash algorithm: `SHA-384`
- Certificate validity: `2 years`

Failure to meet this specification will result in the application being returned for correction.

5 Request pricing

The registrar gains a certain amount of free requests per month.

The amount of free requests is determined individually by the number of registered domains at the beginning of the month, where one domain is worth 100 free requests. However, the amount of free requests is never lower than 25,000.

Once the registrar has spent all free requests, they get charged for all the following requests according to the “Price per EPP query” item in the current price list[5].

[5] https://www.nic.cz/page/349/cenik/

6 Identifier creation rules

Object identifiers (the `name` element in domains and the `id` element in contacts, name-server sets and key sets) may be selected according to the following rules.

Domain names in the `cz` zone

- are composed of 2 labels separated with a period `.`,
- **the first label**
  - contains only upper-case and lower-case letters of the English alphabet, digits (characters 0 through 9), and `-`[6] characters,
  - does not begin nor end with the `-`[6] character,
  - does not contain two or more consecutive `-`[6] characters,
  - has the length of 1–63 characters,
- the second label is the zone `cz`,
- may end with a period.

The register is case-insensitive and presents the domain names transformed to lower case.

Domain names in the `0.2.4.e164.arpa` zone (ENUM)

- are composed of 6–15 labels separated with a period `.`,
- each label preceeding the zone contains exactly one digit (characters 0 through 9),
- ends with the zone `0.2.4.e164.arpa`,
- may end with a period.

The register is case-insensitive and presents the domain names transformed to lower case.

Other identifiers

Identifiers (handles) of contacts, name-server sets and key sets:

- contain only upper-case and/or lower-case letters of the English alphabet, digits (characters 0 through 9), and `-`[6] characters,
- do not begin nor end with the `-`[6] character,
- do not exceed the length of 30 characters.

The register is case-insensitive and presents the identifiers transformed to upper case.

[6] the character of the basic ASCII set for hyphen/minus

7 Automatic merger of duplicate contacts

The Central register merges duplicate contacts that it detects in the database. This procedure is executed once a week on Monday morning.

Contacts are considered duplicates when their key attributes are identical, see FRED Documentation / Contact merger / Identical contacts[7].

Only contacts that have the same designated registrar can be merged.

The Central register selects the *destination contact*, into which the merge will result and it will be used to replace the duplicate contacts in linked objects, automatically with given quality criteria that are stated in the documentation: FRED Documentation / Contact merger / Selection of the destination contact in an automatic merger[8].

Contacts that have CZ.NIC or mojeID as the designated registrar, are excluded from the automatic merger.

8 Disclosure of personal information in contacts

The registry approaches personal information in accordance with the GDPR, meaning most of the information is not disclosed in public interfaces (whois). At the same time, it allows disclosure of some of the attributes based on contact preferences.

The contact preferences are set with the element `<contact:disclose>` in operations `contact:create` (syntax create[9]) and `contact:update` (syntax update[10]).

Preference for disclosure is set by attribute value `flag='1'`, which states that the contact wants to disclose mentioned attributes, and by listing the attribute flag.

Caution: When using `flag='0'` with any data, everything will adjust according to the default server policy. We do not recommend to use it. Because of special conditions with the *address* flag, debugging of the command might be problematic.

It is possible to manipulate disclosure settings with attributes:

- *address* (address[11], only under specific conditions, see below),
- *telephone* (telephone),
- *fax* (fax),
- *email* (e-mail),
- *vat* (VAT),

[7] https://fred.nic.cz/documentation/html/Concepts/ContactMerger.html#merge-auto-identity
[8] https://fred.nic.cz/documentation/html/Concepts/ContactMerger.html#merge-auto-criteria
[9] https://fred.nic.cz/documentation/html/EPPReference/CommandStructure/Create/CreateContact.html
[10] https://fred.nic.cz/documentation/html/EPPReference/CommandStructure/Update/UpdateContact.html
[11] The address disclose flag affects disclosure of all addresses in the contact.

- *ident* (identity document),
- *notifyemail* (notification e-mail).

Settings of the attributes *name* (name) and *organization* (organization) can't be changed, they are always public and are not listed in commands and responses.

Default server policy

If you use an empty element <contact:disclose> in contact:create or leave him out completely, default flags will be set.

Default flags for contact:create:

name	organization	address	telephone	fax	email	vat	ident	notifyemail
show	show	show	hide	hide	hide	hide	hide	hide

If you use an empty element <contact:disclose> in contact:update or leave him out completely, it means that change of flag settings in not required.

Hiding address

Special rules are applied on *address* attribute:

- it can't be set in the operation contact:create, disclosure is set by the server to *show*,
- if the contact with blank attribute *organization* is fully identified (status flag is identifiedContact) or validated (status flag is validatedContact):
  - hiding is automatically set by the server to *hide*,
  - it is possible to change the preference setting in the operation contact:update.
- if the contact loses both states mentioned above, hiding is automatically set by the server to *show*.

Interpretation of the result contact:info

Operation returns contact preference for attributes disclosure.

With the exception of attributes *name* and *organization*, which are set by the registry, attribute disclosure policy is interpreted by the presence of corresponding element.

E.g. response to contact:info contains:

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

(continues on next page)

(pokračujte na předchozí stránce)

```
  <contact:vat/>
  <contact:ident/>
</contact:disclose>
```

Interpretation of the result:

name	organization	address	telephone	fax	email	vat	ident	notifyemail
show	show	show	hide	hide	show	show	show	hide

9 Handling of key sets with changes of name-server sets in domains

If a new name-server set that contains the same name servers as the original set, is assigned to a domain, then the key set is kept.

If a new name-server set that contains different name servers than the original set, is assigned to a domain, then the key set is unlinked automatically.

If the key set identifier is re-entered as a part of the request to update the name-server set in a domain, then the key set is kept.

If a name-server set is unlinked from a domain, then the key set is unlinked as well.

10 Deletion of domains

Domains that are 61 days after expiration, are marked with the `deleteCandidate` status, which denotes that they are to be deleted. Such domains are then randomly deleted during the same day.

Domains in the `deleteCandidate` state appear as registered in the response to the `check_domain` EPP command and their status and details can still be read with the `info_domain` EPP command, but they cannot be renewed anymore.

Public interfaces (WHOIS) display only the information that a domain in the `deleteCandidate` state is to be deleted. This information is available in the public interfaces either till the domain is re-registered (when the details of the new registration are displayed), or till the next day. Hence, the public interfaces do not inform whether a domain has actually been deleted yet and is available for registration.

11 Deletion of unused contacts, name-server sets and key sets; protection period for deleted objects

The contacts which, within the previous 6 months, were not assigned to any domain name, name-server set or key set and, at the same time, no changes were made to such contacts, will be deleted by the central registry.

Name-server sets which, within the previous 6 months, were not assigned to any domain name and, at the same time, no changes were made to such name-server set, will be deleted by the central registry.

Key sets which, within the previous 6 months, were not assigned to any domain name and, at the same time, no changes were made to such key sets, will be deleted by the central registry.

The contacts, name-server sets and key sets which are deleted by the central registry, as a result of not being used, or by the registrar using the respective EPP command are subject to the protection period of 2 months of the deletion.

During the protection period, the identifier (handle) of the contact, name-server set or key set cannot be used as an identifier of a newly registered object (contact, name-server set, key set). After the expiry of the protection period, the deleted identifier (handle) may be used again for the registration of a new contact, name-server set or key set.

12 Technical checks of name servers

Technical checks of name-server sets are carried out in order to monitor the condition of the name servers to which domain names are delegated. A technical check represents a set of individual tests which are, in a certain order, applied to name servers within a name-server set. The tests *do not affect* inclusion or exclusion of a domain to/from a zone, the test results are only informative.

The individual tests, their severity, dependencies and possible results are described in the FRED Documentation / Concepts / Technical checks[12].

The registrar may request a technical check through EPP and specify the level of tests to be performed by their severity with a number from 1 to 6 (inclusive). If the level is not specified, the level given by the `report level` attribute of a name-server set is tested. If that attribute is not set, the default level 3 is tested. The registrar receives the test results in a poll message.

Technical checks are also performed regularly but the registrar is not informed about the results in this case. Only technical contacts of the tested name-server set are notified if the check fails.

[12] https://fred.nic.cz/documentation/html/Concepts/Teccheck.html

13 Central register communication

The table contains a description, time specification and addresses of individual types of Central register communications, including poll messages which are intended for registrar's needs.

Table1: Central register communication

Type	When	Addressee	Note
Notification	after domain change implementation	notify email of the holder	also received as a poll message by the registrar, if the change was made by the register (update, delete)
Notification	after contact change implementation	notify email of the contact	also received as a poll message by the registrar, if the change was made by the register (update, delete)
Notification	after an update of a contact that is linked to a domain of another registrar		received as a poll message by the registrar of the linked domain
Notification	after name-server set change implementation	notify email of the technical contacts	
Notification	after key set change implementation	notify email of the technical contacts	
Notification	after registrar change implementation	notify email of the respective contact	received as a poll message by the original registrar
Periodic request to check and correct contact's data	annually 2 months before the date of registration of the contact	email of the contact	
Sending of domain authorization information	after receiving a request to send AuthInfo	notify email of the holder and administrative contacts	
Sending of contact authorization information	after receiving a request to send AuthInfo	notify email of the contact	
Sending of name-server authorization information	after receiving a request to send AuthInfo	notify email of the technical contact	
Sending of key set authorization information	after receiving a request to send AuthInfo	notify email of the technical contact	

continues on next page

Table 1 – continued from previous page

Type	When	Addressee	Note
Validation	30 days prior to the expiry date of the validation		received as a poll message by the registrar
Validation	15 days prior to the expiry date of the validation	email of the holder and administrative contacts	
Expiration	30 days prior to the expiry date of registration		received as a poll message by the registrar
Expiration	on the expiry date of registration	email of the holder and administrative contacts	also received as a poll message by the registrar
Exclusion from the zone after expiry	30 days after the expiry date	email of the holder, administrative contacts and technical contacts of the name-server set	also received as a poll message by the registrar
Exclusion from the zone – validation	on the expiry date of validation	email of the holder, administrative contacts and technical contacts of the name-server set	also received as a poll message by the registrar
Cancellation warning	33 days after the expiry date	letter to the postal address of the holder	*discontinued* since Jan 1, 2019
Cancellation of a domain name	61 days after the expiration	email of the holder, administrative contacts and technical contacts of the name-server set	also received as a poll message by the registrar
Cancellation of a domain name	on the date of cancellation		received as a poll message by the registrar
Cancellation of an unused contact, name-server set or key set	on the date of cancellation	email of the contact or technical contacts	
Technical check results	upon request		received as a poll message by the registrar
Technical check results	periodical	email of technical contacts of the relevant name-server set	
Invoice – monthly	monthly	email of the registrar	invoice in PDF and XML
Invoice – advance payment	after matching an advance payment	email of the registrar	invoice in PDF and XML

continues on next page

Table 1 – continued from previous page

Type	When	Addressee	Note
Automatic merger of duplicate contacts	after merger	email of the contact	also usual notification of domain, nameserver set or key set update, see the first rows in this table
Automatic key management – acceptance period iniated	after discovery of valid CDNSKEY records on an insecured domain	email of technical contacts of the nameserver set	
Automatic key management – acceptance period broken	if CDNSKEY records change during the acceptance period	email of technical contacts of the nameserver set	
Automatic key management – acceptance period completed	domain update with the new accepted key set		usual notification of domain update, see the first row in this table
Automatic key management – update keys	after discovery of new valid CDNSKEY records on a secured domain	email of technical contacts of the nameserver set	
–			

14 Authorization information (AuthInfo)

The registry requires the authorization information (AuthInfo) when changing the object's designated registrar (`transfer`). AuthInfo allows a registrar other than the designated registrar to access undisclosed attributes of a contact.

AuthInfo is valid (TTL) for 14 days.

Minimum AuthInfo length is 8 characters.

As part of the response to `sendAuthInfo` command, registrars are given a partially hidden hint as to which e-mail the AuthInfo was sent to.

Since FRED 2.48.0, in accordance with RFC 9154, `create` command with non-empty AuthInfo value is forbidden. If `create` command doesn't contain the AuthInfo value or is empty, it will be accepted.