Rules of Technical Communication

CZ.NIC Technical Department

20. 1. 2026

Obsah

1 Introduction....2
2 Communication protocol....2
3 Login data and communication limits....2
4 Rules for requesting an SSL certificate to access the EPP system....3
5 Request pricing....3
6 Identifier creation rules....4
7 Automatic merger of duplicate contacts....5
8 Disclosure of personal information in contacts....5
9 Accuracy of data in the Central registry....7
10 Handling of key sets with changes of name-server sets in domains....8
11 Deletion of Domain Names and Domain Name Auctions....8
12 Administrative blocking of Domain Names....9
13 User blocking of object handling....10
14 Deletion of unused contacts, name-server sets and key sets; protection period for deleted objects....10
15 Technical checks of name servers....11
16 Central register communication....12
17 Authorization information (AuthInfo)....16

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 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. Depending on your level of experience, we recommend to explore at least the following chapters:

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

XSD schemas for client-side XML validation are available at Registration system.

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 Central 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 Central 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=Firma, s.r.o./
‹→CN=*.firma.cz/emailAddress=podpora@firma.cz/" -out company_name.csr -newkey␣
‹→ec -pkeyopt ec_paramgen_curve:secp384r1 -sha384 -keyout file_name_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** (Organisation 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 access the EPP, 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 Domain names at the beginning of the month, where one domain is worth 100 free requests. However, the amount of free requests is never lower than 100,000.

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.

6 Identifier creation rules

Object identifiers (the `name` element in Domain names 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[1] separated with a period `.`,
  - **the first label**[1]
    - contains only upper-case and lower-case letters of the English alphabet, digits (characters `0` through `9`), and the hyphen `-`[2] character,
    - does not begin nor end with the `-`[2] character,
    - does not contain two or more consecutive `-`[2] 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[1] (including zone) separated with a period `.`,
- each label[1] 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:

- contains only upper-case and/or lower-case letters of the English alphabet, digits (characters `0` through `9`), and the hyphen `-`[2]character,
- do not begin nor end with the `-`[2] character,
- do not exceed the length of 30 characters.

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

1 Part of the domain name (= *label*) – specific level of the domain name.

2 The character of the basic ASCII set for hyphen.

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.

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.

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 legal regulations governing the protection of personal data, 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) and `contact:update` (syntax update)

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[3], only under specific conditions, see below),
- *telephone* (telephone),
- *fax* (fax),
- *email* (e-mail),
- *vat* (VAT),
- *ident* (identity document),
- *notifyemail* (notification e-mail).

3 The address disclose flag affects disclosure of all addresses in the contact.

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/>
    <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 Accuracy of data in the Central registry

To ensure the data in the Central registry is complete and accurate, CZ.NIC verifies the contact details of Contacts who are Domain Name Holders in accordance with legal regulations. Details on data verification are provided in the document Principles and Procedures Ensuring the Accuracy and Completeness of Registration Data and Rules of Domain Names Registration under the .cz ccTLD.

When a Contact is included in the verification process, the Holder is sent an e-mail request to verify the data, along with instructions. The Holder must log in to the verification portal according to the instructions in the e-mail and select a verification method to successfully complete the Contact verification.

After 15 days have passed without verification of the contact details, the Domain Names for which the contact is the Holder are removed from the zone and the contact is blocked from linking new objects (i.e., it is not possible to list them as the Holder of another Domain Name or another object in the registry).

The maximum limit for data verification is 45 days, and if the Holder does not complete the data verification process, the Domain Names for which the contact is the Holder may be deleted. Domain Names deleted in this way are added to the Auction system on the same day.

A contact that has not been verified and has no object assigned to it in the Central registry (Domain Name, Key set, Nameserver set) may be deleted – see the chapter Deletion of unused contacts, name-server sets and key sets; protection period for deleted objects.

In accordance with the NIS2 regulation, CZ.NIC requires the mandatory provision of a telephone number as part of the data used to contact the Holder, administrative or technical contact (see Annex No. 1 of the document "Rules of Domain Names Registration under the .cz ccTLD").

From January 20, 2026, `create` and `update` contact operations require that the Contact have a phone number in a valid format. A valid format means:

- the phone number structure is `+<international country code>.<national number>`;
- the international country code consists of 1 to 3 digits;
- the national number consists of 1 to 14 digits;
- the maximum length of the entire phone number is 17 characters.

When attempting to create (`create_contact`) or modify (`update_contact`) a Contact without specifying the mandatory telephone attribute (`voice` element), the registry returns error code `2003` ("`Required parameter missing`"). If the phone attribute is specified but its value does

not correspond to a phone number in a valid format, the registry returns error code `2001` ("`Command syntax error`").

10 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 Name, 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 Name, 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 Name, then the Key set is kept.

If a Name-server set is unlinked from a Domain Name, then the Key set is unlinked as well.

11 Deletion of Domain Names and Domain Name Auctions

Domain names deleted by the EPP command `delete_domain` and Domain Names that are 61 days after expiration, are immediately deleted and added to the list of Domain Names for which Priority Right to register will be auctioned.

All Domain Names whose registration has expired (been deleted) are included in the Auction system, with exceptions as specified in the Domain Auction Rules. The period during which the list of Domain Names for which Priority Right to register will be auctioned is published, as well as other Auction conditions, are specified in the Domain Auction Rules and Domain Auctions Rules of Operation.

While the Domain Name is in the Auction system, it is not possible to register the Domain Name. The EPP command `check_domain` returns the status `false` and the attribute `reason` has the value "`Auction pending`".

Public interfaces (WHOIS) display about the Domain Name included in the Auction only that the Domain Name is in the Domain Name Auction.

A Domain Name for which a Priority Right has been auctioned may only be registered by the winning auctioneer within the period specified in the Auction Rules; after this period has expired without result, it is included in the next round of auctions or released for free registration.

The Domain Name for which the Priority Right has been auctioned and is awaiting its exercise by the successful auctioneer still appears as unregistrable in response to the EPP command `check_domain`, i.e., the EPP command `check_domain` returns the status `false` and the attribute `reason` has the value "`Only the auction winner is authorized to register this domain.`" The `check_domain` command contains an extension where the Registrar can attach a contact handle to the request. If the query contains the contact handle of the winning auctioneer who has fulfilled the conditions for exercising the Priority Right, the EPP `check_domain` command response will return the status `true` (registerable Domain Name).

An attempt to create a Domain Name using the EPP `create_domain` command may result in one of the following statuses:

- Return code `1000 (Command completed successfully)`: if the Domain Name is not on the list of Domain Names for which Priority Right to register will be auctioned; or if the contact handle that auctioned the Priority Right for the Domain Name and meets the conditions for registration is in a Holder role.
- Return code `2306 (Parameter value policy error)`: if the Domain Name is still on the list of Domain Names for which Priority Right to register right will be auctioned.
- Return code `2201 (Authorisation error)`: if the contact Holder role is held by a contact other than the one who won the Priority Right.

Domain Names removed from the Auction system are released for free registration at random throughout the following day. Until the Domain Name is released for free registration, the EPP command `check_domain` returns status `false` and the attribute `reason` has value "`Auction pending`". From the moment the Domain Name is released from Auctions, it can be re-registered by any Holder.

Registrars who introduce support for Auctions can contact CZ.NIC and provide a link to the page with registration form for domains auctioned in Auctions. It is also advisable to include a link to a page explaining how Auctions work. These links will then be published on the List of Registrars page, listing all registrars that support direct registration of Domain Names with Priority Rights.

12 Administrative blocking of Domain Names

In accordance with the Rules of Domain Names Registration under the .cz ccTLD, in clearly defined cases, the ability to use a Domain Name may be restricted (change of owner, cancellation of registration), or the Domain Name may even be removed from the zone (cancellation of delegation). Depending on the specific case, the Holder's contact may be blocked during administrative blocking, or this contact may be replaced with a copy of the Holder's contact (to avoid restrictions on the use of Domain Names that are not blocked).

In relation with the administrative blocking of a Domain Name, depending on the reasons, the Domain Name may be administratively removed from the zone (the Domain Name has the status `serverOutzoneManual`), administratively included in the zone (`serverInzoneManual`), or administratively blocked (`serverBlocked`). Managing the Domain Name may also be blocked, i.e., some of the following blocks may be set – Domain Name changes (`serverUpdateProhibited`), changes of the Designated registrar (`serverTransferProhibited`), deletion (`serverDeleteProhibited`), Holder changes (`serverRegistrantChangeProhibited`), and blocking of registration period renewal (`serverRenewProhibited`).

An administratively blocked Domain Name cannot be cancelled due to the nature of the block (even after the protection period expires; such a Domain Name is not cancelled for the duration of the block and subsequently included in the Auction system), its Holder cannot be changed, and the delegation of such a Domain Name cannot be cancelled (it is removed from the zone).

Administrative blocking is usually ended:

- upon expiry of the maximum duration of the block (blocking according to Article 20 of the Registration Rules) or cancellation (termination) of the decision of the competent authority on the block (on the restriction of the Holder's right to use the Domain Name): if the

protection period has expired during the blocking period, the date of termination of the blocking is set as the new expiration date and a new protection period begins for the Holder;

- by a decision of the competent authority (e.g., court, arbitration tribunal) and enforcement of that decision:
  - Domain Name transfer (transfer of the Holder): CZ.NIC will end the block and change the Holder; the expiration date remains unchanged; if the domain name has already expired during the block, a new expiration date will be set, which is equal to the date of the end of the block;
  - cancellation of registration and subsequent re-registration: CZ.NIC will lift the block and cancel the registration of the Domain Name, and then re-register it in accordance with the decision. In such a case, the expiration date will be the same as the registration date (the new Holder must transfer the Domain Name to one of the Registrars);
  - cancellation of registration: CZ.NIC will terminate the block and cancel the Domain Name; such Domain Name will be included in the Auction system on the same day.

13 User blocking of object handling

The Holder can increase the security of their objects in the Central registry, i.e. Contact, Domain Name, Key Set (keyset), and Name Server Set (nsset), by blocking access to these objects. They can do this using publicly accessible Requests on the CZ.NIC website or using the Domain Browser application. Depending on the required security level, objects in the Central Registry have corresponding blocking statuses – object changes (`serverUpdateProhibited`) and changes to the Designated Registrar (`serverTransferProhibited`).

User blocking in the case of a Domain Name does not affect the running of the protection period and the consequences of its expiry in accordance with the Registration Rules.

14 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.

15 Technical checks of name servers

Technical checks of Name-server sets are carried out periodically in order to monitor the condition of the name servers to which Domain names are delegated. Technical check runs a complete set of tests through the Zonemaster service for each individual Domain name that is associated with a particular name server. Each Domain name test ends with a severity result (critical, error, warning, notice, info). The individual tests and severity results are described in the Zonemaster project documentation.

Technical checks process the Domain name test results and assign the Name-server set rating according to the most severe result found. Then an e-mail is sent to the technical administrators depending on the set level of reporting. The following reporting levels are distinguished:

- 0 – reporting completely disabled
- 1 – reporting only takes place if the result is „critical“
- 2 – reporting only takes place if the result is „critical“ nebo „error“ (výchozí nastavení)
- 3 – reporting only takes place if the result is „critical“, „error“ nebo „warning“
- 4 – reporting only takes place if the result is „critical“, „error“, „warning“ nebo „notice“

The tests do not affect inclusion or exclusion of a domain to/from a zone, the test results are only informative.

16 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.

Table 1: Central register communication

Type	When	Addressee	Note
Notification	after domain change implementation	notify e-mail 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 e-mail 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 name of another Registrar		received as a poll message by the Registrar of the linked Domain name
Notification	after Name-server set change implementation	notify e-mail of the technical contacts	
Notification	after Key set change implementation	notify e-mail of the technical contacts	
Notification	after Registrar change implementation	notify e-mail 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 anniversary of the Contact registration date	e-mail of the Contact	
Sending of Domain name authorization information	after receiving a request to send AuthInfo	e-mail of the Holder and administrative contacts	

Continues on next page

Table 1 – part 2

Type	When	Addressee	Note
Sending of Contact authorization information	after receiving a request to send AuthInfo	e-mail of the Contact	
Sending of Name-server authorization information	after receiving a request to send AuthInfo	e-mail of the technical contact	
Sending of Key set authorization information	after receiving a request to send AuthInfo	e-mail of the technical contact	
Validation of ENUM Domain name	30 days prior to the expiry date of the validation		received as a poll message by the Registrar
Validation of ENUM Domain name	15 days prior to the expiry date of the validation	e-mail 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	e-mail 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	e-mail 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	e-mail 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

Continues on next page

Table 1 – part 3

Type	When	Addressee	Note
Cancellation of a Domain name	61 days after the expiration	e-mail 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	e-mail of the Contact or technical contacts	also received as a poll message by the Registrar
Technical check results	upon request		received as a poll message by the Registrar
Technical check results	periodical	e-mail of technical contacts of the relevant Name-server set	
Invoice – monthly	monthly	e-mail of the Registrar	invoice in PDF and XML
Invoice – advance payment	after matching an advance payment	e-mail of the Registrar	invoice in PDF and XML
Automatic merger of duplicate contacts	after merger	e-mail of the Contact	also usual notification of Domain name, Name-server set or Key set update, see the first rows in this table
Automatic key management – acceptance period initiated	after discovery of valid CDNSKEY records on an insecured domain	e-mail of technical contacts of the Name-server set	

Continues on next page

Table 1 – part 4

Type	When	Addressee	Note
Automatic key management – acceptance period broken	if CDNSKEY records change during the acceptance period	e-mail of technical contacts of the Name-server set	
Automatic key management – acceptance period completed	Domain name update with the new accepted Key set		usual notification of Domain name update, see the first row in this table
Automatic key management – update keys	after discovery of new valid CDNSKEY records on a secured domain	e-mail of technical contacts of the Name-server set	
Verification – start (request for Contact verification)	at the beginning of the verification process	e-mail of the Contact, administrative contacts of the Domain Names	
Verification – notification of upcoming removal of Domain Names from the zone	8 days after verification begins / 7 days before removing Domain Names from the zone	e-mail of the Contact, administrative contacts of the Domain Names	
Verification – removal of Domain Names from the zone	15 days after verification begins	e-mail of the Contact, administrative contacts of the Domain Names	
Verification – final verification request	38 days after verification begins / 7 days before the verification deadline	e-mail of the Contact, administrative contacts of the Domain Names	
Verification – unsuccessful Contact verification and deletion of Domain Names	upon unsuccessful verification	e-mail of the Contact, administrative contacts of the Domain Names	
Verification – successful Contact verification	upon successful verification	e-mail of the Contact, administrative contacts of the Domain Names	

Continues on next page

Table 1 – part 5

Type	When	Addressee	Note
Verification – cancelled	after verification is cancelled	e-mail of the Contact, administrative contacts of the Domain Names	
Verification – manual check result	sending the result of manual check	e-mail of the Contact, administrative contacts of the Domain Names	
Verification – information about adding Contact to manual check	when adding Contact to manual verification	e-mail of the Contact, administrative contacts of the Domain Names	
Verification – letter with verification code	when selecting verification by letter	letter to the address of the Contact	letter can be sent only twice
Verification – letter with verification code to the Contact representative	when selecting verification by letter to the representatives	letter to the address of the representative	for Contacts outside of EU/EEA, letter can be sent only twice

17 Authorization information (AuthInfo)

The Central 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.