API Guides: Introduction

- API Guides: Glossary
- Getting started with Openprovider API

API Guides: Glossary

Domains

Handle - a contact ID of Openprovider containing personal information such as name, surname, address, phone, company name. Types: private individual or company. Format: JA123456-HR (first two letters indicate Name and Surname, e.g. John Appleseed - "JA"; last two letters indicate handle origin, e.g. "DE" - Germany, "NL" - Netherlands, etc.). Please check more information about handle creation.

Reseller - private individual or company registered at Openprovider and offering services from its name.

Extension - suffix or the last part of a domain name - the letters that come after the dot to the right of any domain name.

Premium domain - domain names that are more expensive than a regular ones because of the large number of reasons including length, keywords, and brand-ability.

DNS zone - any distinct, contiguous portion of the domain name space in the Domain Name System (DNS) for which administrative responsibility has been delegated to a single manager.

DNS record - records assigned with DNS servers and works to help users connect their websites to the outside world. Different types of records are designed for different purposes ("A" record assign hostname to IP address, "MX" record assign domain mail server to service, etc.).

Glue record - IP Address of a name server at a domain name registry. Glue Records are fundamental parts of DNS records because they help to resolve DNS servers at a core level. If you would like to change the name servers for a site, you'll have to provide the Glue Records for the new name serves. Without them, a domain name will not work because anyone requiring the DNS information will be stuck in a loop. Glue Records are additional A records that allow the DNS client to locate name servers.

DNSSEC - a technology that can be added to the Domain Name System to verify the authenticity of its data. The works by adding verifiable chains of trust that can be validated to the domain name system.

Domicile - an optional service required if the customer doesn't have an own local address in a country, that is usually required to complete the domain registration.

IDN (**Internationalized Domain Names**) - names that contain at least one label that is displayed in software applications, in whole or in part, in a language-specific script or alphabet, such as Arabic, Chinese, Cyrillic, Tamil, Hebrew or the Latin alphabet-based characters with diacritics or ligatures, such as French. These writing systems are encoded by computers in multi-byteUnicode. Internationalized domain names are stored in the Domain Name System as ASCII strings using Punycode transcription.

Domain registration - the act of reserving a name on the Internet to someone for a certain period.

Domain renewal - the act of domain name period prolongation that delays domain expiration date.

Domain restore - the act of domain name recovery from redemption period, used if expiration date passed, and applicable not for all TLDs. Refer to TLD articles and Global TLD Reference sheet.

Domain transfer - a process of changing the designated registrar of a domain name.
May be incoming and outgoing, Internal (between accounts of one registrar) and External (between different registrars).

Domain trade - a process of changing the designated owner of a domain name.

Authcode (also "EPP Code") - a code created by a registrar to help identify the domain name holder (also known as a registrant or registered name holder) of a domain name in a generic top-level domain (gTLD) operated under contract with ICANN, an authcode usually required for transfer.

Soft Quarantine - a period after the domain name expires and no longer active, but reactivating does not include additional fees.

Hard Quarantine - a period after the domain name expires and no longer active, and reactivating does include additional fees.
WPP (Whois Privacy Protection) - a service designed to hide or replace information shown in WHOIS to anonymous.

gTLD ("Generic TLD") - a category of top-level domains (TLDs) maintained by the Internet Assigned Numbers Authority (IANA) for use in the Domain Name System of the Internet. A top-level domain is the last level of every fully qualified domain name. The core group of generic top-level domains consists of the com, info, net, and org domains.

ccTLD ("Country code TLD") - a category of top-level domains (TLDs) used or reserved for a country, sovereign state, or dependent territory identified with a country code (e.g. "de" for Germany, "ru" for Russia etc.)

nTLD ("new TLD") - a category of hundreds new gTLDs whose release began with 2014. Although these TLDs are quite diverse and won’t always be new, they do belong to a discernible movement whose aim is to introduce widespread novelty online. Right now, they are discussed as a bundle,

distinct from earlier gTLDs; and “nTLD” is one label that has arisen (e.g. tv, pro, travel etc.)

SSL Certificates

SSL Certificate - the file that attests to the identity of an organization or web browser user and is used to verify that data being exchanged over a network is from the intended source.

Certification Authority (CA) - a trusted entity that issues digital certificates, which are data files used to cryptographically link an entity with a public key. Certificate authorities are a critical part of the internet's public key infrastructure (PKI) because they issue the Secure Sockets Layer (SSL) certificates that web browsers use to authenticate content sent from web servers.

Private Key - the key that a user keeps secret in asymmetric encryption. Can encrypt or decrypt data for a single transaction but cannot do both.

Public Key - the key that a user allows the world to know in asymmetric encryption. Can encrypt or decrypt data for a single transaction but cannot do both.

Root Certificate -a self-signed certificate issued from a root level Certificate Authority (CA).

Intermediate Certificate - subordinate certificate issued by the trusted root specifically to issue end-entity server certificates

End-user Certificate - the certificate that it activates the padlock and the secure protocol and allows secure connections from a web server to a browser.

SSL Certificate Chain - list of the root, intermediate and end-user SSL certificates that connected between each other to present the resource as trusted.

Reseller - private individual or company registered at Openprovider and offering services from its name.

SHA-1 - Secure Hash Algorithm, a cryptographic hash function that has a 160-bit message digest (hash value) size but began to be considered unsafe in mid-2000s.

SHA-2 - Secure Hash Algorithm, a cryptographic hash function that includes significant changes from its predecessor, SHA-1 and it's family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits, commonly used in the current time.

SSL Certificate Warranty - insurance for an end user against loss of money when submitting a payment on an SSL-secured site.

Domain Validation Certificate (DV) - certificate used for secured websites and software that proves domain(s) ownership confirmation.

Organization Validation Certificate (OV) - certificate used for secured websites and software that proves domain(s) ownership confirmation and the legal entity controlling the website or software package.

Extended Validation Certificate (EV) - certificate used for secured websites and software that proves domain(s) ownership confirmation and the legal entity controlling the website or software package, often used by worldwide organizations, more complicated than DV/OV but expected to be more trusted and secure, and contains company name near address bar.

SSL (Secure Socket Layer) - the standard security technology for establishing an encrypted link between a web server and a browser, last version (3.0) of that deprecated in June 2015 byRFC 7568.

TLS (Transport Layer Security, ex. 'SSL') - a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions.

Certificate Reissue - the process of replacing certificate to get a brand-new certificate code, often used if some certificate holder data changed, private keys lost, holder feels certificate been compromised. The process does not affect issue and expiration dates and free of charge. It requires CSR change.

Certificate Renew - the process of certificate prolongation, it extends the lifetime for the same period been actual on a moment of issuance, this is paid operation and price usually an equal amount of money been paid for creation.

Openprovider Product ID - Openprovider internal product identification number consisting of 1 or 2 digits related to an exact SSL product. Check the available products table.

Openprovider Order ID - Openprovider internal order indicator related to an exact order stored in the reseller's account.

Wildcard Certificate - single certificate with a wildcard character in the domain name field allowing the certificate to secure multiple subdomain names (hosts) pertaining to the same base domain (e.g. can protect sub1.example.com, sub2.example.com, etc. using one certificate).

MD5 - An MD5 checksum is a 32-character hexadecimal number that is computed on a file. If two files have the same MD5 checksum value, then there is a high probability that the two files are the same.

Domain control validation (DCV) - the process of confirming rights to manage a domain, one of the stages preceding certificate issue.
Known types:
Email validation - the procedure of domain ownership confirmation following a special link sent by CA to an email.
DNS validation - the procedure of domain ownership confirmation by adding DNS records

provided by CA.
HTTP(s) - the procedure of domain ownership confirmation by placing random-content files(s) provided by CA into website(s) folder(s).

Check this article to get familiar with validation methods in details.

Openprovider order status list

ACT - active ;
PAI - purchased but not been requested yet ;
REQ - requested and passing validation ;
REJ - cancel operation requested for an order ;
✖ **FAI** - order canceled;
EXP - expired order.

Getting started with Openprovider API

Who is Openprovider

Openprovider is a wholesaler of Internet services and products with a unique platform from which you can find and manage all the products you need: Domains, new gTLDs, SSL certificates, licenses for Plesk and Virtuozzo, spam filters, and more!

Getting started

Quick Start Guide to our API

You can find our new Quick Start Guide to our API with just one click here!

Openprovider API gives access to the entire Openprovider infrastructure via a standardised interface based on OpenAPI Specification. With the help of Openprovider's API, you can do just about anything you can do in Reseller Control Panel.

The Openprovider API is a RESTful API based on HTTPS requests and JSON responses. If you have your Openprovider account, you can obtain your API authentication token via the following endpoint:

```
POST https://api.openprovider.eu/v1beta/auth/login
```

NB: API token TTL is 48 hours

Endpoints

Openprovider API is accessed by making HTTPS requests to a specific version endpoint URL, in which GET, POST, PUT, and DELETE methods dictate how your interact with the available data. Every endpoint is accessed only via the SSL-enabled HTTPS (port 443) protocol.

Be noted that in order to maintain compatibility in the future, all requests must specify an API version, which is appended to the URL. The latest version is v1beta and the base URL for this version's endpoint is:

```
https://api.openprovider.eu/v1beta/
```

Authentication

At its current state Openprovider API only supports Bearer Authentication which involves acquiring security tokens that are then passed in a request. This token must be sent in the Authorization header when making requests to protected resources:

```
Authorization: Bearer <token>
```

Bearer authentication

```
curl -X POST \
 https://api.openprovider.eu/v1beta/auth/login \
 -d '{"username": "user", "password": "******", "ip": "0.0.0.0"}'
```

```
{
 "data": {
 "token": "6f6d86377bc******feb75cea76d8e8b",
 "reseller_id": 100001
 }
}
```

Where,

username: API/account username (same as RCP username).

password: API/account password (same as RCP password of the user).

ip: Public IP address from which you will be sending API requests (optional field).

Note: If there are multiple contacts (admin/tech/billing) under the reseller account, decide which account/contact you want to use for API connection/integration and use its username and password.

Responses

All successful responses will be returned as a JSON object with at least one key: data.

The data element will contain either a single JSON object or a list of JSON objects, depending on the endpoint.

```
{
 "data": {
 "id": 11195838,
 "status": "ACT",
 "activation_date": "2019-06-27 04:22:39",
 "renewal_date": "2020-06-25 04:22:39",
 "expiration_date": "2020-06-27 04:22:39",
 "auth_code": "*******"
 },
}
```

Moving to Production

You can view here how to enable your API Access.

Note: Our system timezone is set to **CET** (Central European Time). During summer months, it automatically shifts to **CEST (UTC+2)** because of daylight saving time.

- The dates of already created, transferred, or renewed domains or products remain unchanged, regardless of summer time changes.
- However, the summer time change applies to any new domain registrations, renewals, transfers, or products added during that period.