

Newsletter May 2021

May Day is the perfect time to catch your next big opportunity. You've come to the right place for the latest news from the domain industry!

.ai, .na and .qpon prices are changing

Price changes have been announced for .ai, .na and .qpon and they are effective immediately.

- **.qpon:** the .qpon registry has increased its prices by \$10.00 for new registrations, transfers and renewals. Domains registered before the 1st of May 2021, 14:00 UTC, will move to a special price tier and renew at \$12.50 instead of the new, higher price.
- **.ai:** after the price change that we announced in our [March newsletter](#) for .ai, as well as the second level domains .com.ai, .net.ai, .org.ai and .off.ai, we have been informed that the transfer price was incorrect. The new transfer price, effective immediately, has increased by \$120.00, which is the transfer fee charged by the registry. The new price for .ai transfers now ranges from \$312.00 to \$350.00 (depending on your tier), which includes a 2-year renewal.
- **.na:** .na prices (including .com.na, .co.na and .org.na) have also changed. The new tier 8 prices are the following (check the price list in your account for the price in other tiers):

Registry (Tier 8)	Transfer, renewal (Tier 8)
na 3 , 2 5 9 (n o w)	€3,551

€co.na 2 7 9 (n o w)	€277
€com.na 3 3 9 (n o w)	€507
€org.na 3 3 9 (n o w)	€497

Small change to the API call for domain name updates

In order to improve our processes, we are optimizing the API commands for modifying a domain name on the 1st of June 2021. A new parameter, *force_registry_update*, will be introduced. Without this parameter, we would only be able to send an update to the registry if the domain's registration data was actually changed.

No changes are required from your side if you do not use our API, or if you use our API for regular domain management. Your updates to your domains' contacts, nameservers or DNSSEC data will still be processed at the registry.

This new parameter will prove useful when the registration data at the registry is different from the data at Openprovider. This might occur, for example, after a transfer or failed update. To force the correct registration data to be sent to the registry again, you can use this new parameter with value *true*.

From the 1st of June, users of our **JSON API** can use this new parameter as follows:

```
put /v1beta/domains/{id}
```

```
{
```

```
... # regular domain data

"force_registry_update": true,

}
```

From the 1st of June, users of our **XML API** can use this new parameter as follows:

```
<?xml version="1.0" encoding="UTF-8"?>

<openXML>

  <modifyDomainRequest>

... # regular domain data

    <forceRegistryUpdate>1</forceRegistryUpdate>

  </modifyDomainRequest>

</openXML>
```

Beware! Scam attempts on .au domains are real

The Australian registry auDA has informed us that an email phishing scam is being performed, targeting .au domain name registrants.

The emails are sent by someone posing as an auDA employee asking for either copies of identification documents or verification of contact information.

If you receive an email of this nature, do not reply to it or click any links included in it. auDA will never reach out to domain holders directly for such documents; any such request will come from Openprovider.

For more information, please refer to the registry's [official notice](#).

UNR is selling out and UniEPS is no longer available

UniEPS is one of the [trademark protection services](#) that we offer our clients: a blocking service for the extensions operated by UNR. However, since the 15th of March 2021, this service can't be ordered anymore! Existing orders will be renewed at no cost, but some extensions might be removed from the service over the next period.

The reason is that registry UNR will publicly auction 23 of its extensions on the 28th of April. UNR's portfolio includes popular extensions like .link, .help and .hosting, which will move to another registry operator after the auction. These new registry operators may decide to cancel the UniEPS

and UniEPS+ services immediately.

Other trademark protection services remain active and can be ordered by contacting us:

- **DPML**, blocking over 240 extensions of registry operator Donuts
- **TREx**, a Trademark Clearinghouse service blocking 40 different extensions
- **AdultBlock**, a blocking service for the adult-targeted extensions .xxx, .adult, .porn and .sex

For more information on included extensions and pricing, take a look at [this article](#) from our Knowledge Base.

We're migrating our domain forwarding service!

To accommodate the growing demand of our domain forwarding service, we are moving it to a newer, faster and more redundant backend on **Tuesday, the 1st of June 2021**. During this migration, from 01:00 to 07:00 AM UTC, it will not be possible to add new forwarders or to update existing ones. There will be no interruption to the availability of existing forwarders.

ACTION REQUIRED: if you use our forwarding service on domain names that use your own nameservers. As the IP address of our service changes, you will need to change it in your DNS zones as well.

The new IP address is **34.90.181.29** (this replaces the old IP address 52.209.188.36). We recommend that you carry out the update during the maintenance window defined above. For existing domain forwarders, we will keep the old server online for at least two weeks, but any changes or new forwarders will be created on the new server.

If you use Openprovider's nameservers, we will update the required configurations ourselves and no action will be required from your side.

Stay safe with DMARC! Soon available at Openprovider

One of the biggest threats online businesses face today comes in the form of *phishing* attacks, where hackers make use of spoofing to perform malicious actions. Spoofing is a technique attackers often use in order to send fake messages on behalf of an organisation by forging the 'From Address' field of those messages.

A well known example of this is when an attacker sends messages that impersonate an organisation and request sensitive information from end users. This typically results in users exposing their credentials or providing sensitive data that can compromise their online accounts and assets.

Another consequence of these attacks is that end users end up reporting some of those fake messages as spam, preventing other legitimate emails coming from official organisations from reaching their inboxes.

Domain-based Message Authentication, Reporting and Conformance, more commonly known as DMARC, is a standard email authentication protocol that helps email administrators understand and prevent spoofing and phishing attacks. Working in combination with other well known standards like SPF and DKIM, DMARC allows your organisation to receive reports from receiving servers and to tell those servers what actions to take when suspicious emails coming from your domain are received.

At Openprovider, security is at the core of what we do and we take our clients' safety very seriously. That's why we are planning to introduce a DMARC solution over the next few months. We will keep you posted for the final release date so stay tuned and don't miss a thing!

Updates to new gTLDs

- **.trust** has been cancelled unexpectedly by the registry. This extension has been in Sunrise since the 24th of March and would enter General Availability on the 28th of April, but it has been suspended indefinitely by the registry in order to apply a new and innovative usage to .trust. Further details will be shared as soon as possible.

Sunrises:

- 6 May: .sbs

Landrushes:

- 26 May: .spa

Early Access Programs:

- 8 June: .sbs

General Availabilities:

- 15 June: .sbs

Upcoming price changes:

- 1 May: .ai, .com.ai, .net.ai, .org.ai, .off.ai transfers
- 1 May: .dk
- 1 May: .na, .com.na, .org.na
- 1 May: .qpon
- 1 July: .club
- 1 September: .com