DNSSEC. Updates and transfers

For general information regarding DNSSEC please refer to the article DNSSEC in Openprovider.

Domain update and transfer with or without DNSSEC

The use cases below describe all steps to be done in order to update or transfer a domain without interruption of DNS services.

Definitions

- DNSKEY-record has the following elements:
  - Flags (e.g. "Zone Key")
  - Algorithm - the public key's cryptographic algorithm
  - Public key data

Unsecuring a secured zone, without nameserver change

1. Disable DNSSEC in the domain update page; Openprovider will automatically remove the DNSKEY-record at the registry; leave the DNS zone itself signed
2. After 24 hours (taking into account registry's zonefile update) unsign the DNS zone
   In case of using Openprovider's DNS, Openprovider will automatically unsign the zone after 24 hours
3. Update complete!

Securing an unsecured zone, without nameserver change

1. Sign the DNS zone
   In case of using Openprovider's DNS, Openprovider will automatically sign the DNS zone when enabling DNSSEC for the domain (step 2)
2. Enable DNSSEC in the domain update page and provide DNSKEY-record (only if not using Openprovider's DNS); Openprovider will automatically send this DNSKEY-record to the registry
   In case of using Openprovider's DNS, Openprovider will automatically sign the DNS zone
3. Update complete!

Key roll-over in a secured zone

If using Openprovider's DNS, key roll-over is done automatically whenever required; the steps below need to be followed only if using other nameservers

1. Add a second DNSKEY to the DNS zone and sign the zone with both keys; retrieve DNSKEY-record
2. Update domain: add new DNSKEY-record; do not remove existing DNSKEY-record yet
3. After 24 hours (taking into account the registry's zonefile update) update domain: remove old DNSKEY-record
4. After 24 hours (taking into account the registry's zonefile update) remove old DNSKEY from the DNS zone; the zone is signed by the new key only
5. Update complete!

Nameserver updates

Nameserver update from non-secure to another non-secure DNS

Not changed compared to the old situation without the existence of DNSSEC:

1. Create (unsigned) zone in the new nameserver
2. Update domain: assign new nameservers
3. After 24 hours (taking into account TTL and registry's zonefile update) remove the old zone
4. Update complete!

Nameserver update from secure DNS to non-secure DNS

1. Create (unsigned) zone in the new nameserver
2. Update domain: assign new nameservers and remove DNSKEY-record from domain
   In case of switching from Openprovider's secure DNS to a non-secure nameserver, Openprovider will automatically remove the DNSKEY-record from the registry

3. After 24 hours (after the registry's zone file update), remove the old, secured zone which is no longer used
   In case of switching from Openprovider's secure DNS to a non-secure nameserver, Openprovider will automatically remove the old zone after 24 hours
4. Update complete!

Nameserver update from non-secure DNS to secure DNS

1. Create zone in the new nameserver and sign it; retrieve DNSKEY-record
   In case of switching to Openprovider's secure DNS, Openprovider will take care of signing the zone; there is no need to retrieve the DNSKEY-record
2. Update domain: assign new nameservers and publish the DNSKEY-record at the registry
   In case of switching to Openprovider's secure DNS, Openprovider will automatically publish the DNSKEY-record at the registry
3. 24 hours (after the registry's zone file update) after the update has finished, remove the old zone which is no longer used
4. Update complete!

Nameserver update from secure DNS to another secure DNS

1. Create (signed) zone in the new DNS, and retrieve DNSKEY-record
   In case of switching to Openprovider's secure DNS, the DNSKEY-record can be found in the zone details
2. Add the DNSKEY-record to the old DNS zone and re-sign zone
   When switching from Openprovider's DNS it is not possible to add the DNSKEY-record to the Openprovider's nameservers. ***Separate deletion of DNSKEY and DS record is not supported****, thus, during the update the domain will temporarily stay unsigned*
3. Update domain: add the new DNSKEY-record, but do not remove the existing DNSKEY-record yet
4. Wait until the TTL is over (safe period: at least 24 hours)
5. Update domain: assign new nameservers
6. After 24 hours (after the registry's zone file update), remove the previous DNSKEY-record from the domain
   In case of switching to or from Openprovider's secure DNS, Openprovider will automatically remove the previous DNSKEY-record
7. 24 hours (after the registry's zone file update) after the update has finished, remove the old zone which is no longer used
   In case of switching from Openprovider's secure DNS, Openprovider will automatically remove the old zone after 24 hours
8. Update complete!

Domain transfers

Transfer if no DNSSEC is used at old and new provider (either with or without changing nameservers)

Not changed compared to the old situation without the existence of DNSSEC:

1. If nameservers change, create (unsigned) zone in the new nameserver
2. Transfer domain
3. If nameservers change, remove the old zone 24 hours (taking into account TTL and registry's zonefile update) after the transfer finished
4. Transfer complete!

Transfer from secure DNS to non-secure DNS (this implies a nameserver change)

1. Disable DNSSEC on the existing zone:
   1. Remove DNSKEY-record from domain
   2. After 24 hours (or shorter, but keeping in mind the registry's zonefile update frequency), unsecure DNS zone
      In case currently Openprovider's secure DNS is used, you can unsecure the domain via the 'update domain' page or command. Openprovider will automatically remove the DNSKEY-record at the registry, and after 24 hours unsecure the zone
2. Create (unsigned) zone in the new nameserver
3. Transfer domain
4. 24 hours (after the registry's zone file update) after the transfer has finished, remove the old zone which is no longer used
5. Transfer complete!

Transfer from non-secure DNS to secure DNS (this implies a nameserver change)

1. Create zone in the new nameserver and sign it; retrieve DNSKEY-record
   In case of switching to Openprovider's secure DNS, Openprovider will take care of signing the zone; there is no need to retrieve the DNSKEY-record
2. Transfer domain: assign new nameservers and publish the DNSKEY-record at the registry
   In case of switching to Openprovider's secure DNS, Openprovider will automatically publish the DNSKEY-record at the registry
3. 24 hours (after the registry's zone file update) after the transfer has finished, remove the old zone which is no longer used
4. Transfer complete!

Transfer while the domain keeps the same secure DNS

1. Retrieve the current DNSKEY-record for this domain
2. Start the transfer, include the DNSKEY-record in the transfer request

3. No other actions are required, just wait for the transfer to be completed

Transfer from secure DNS to another secure DNS (including nameserver change)

1. Create (signed) zone in the new DNS, and retrieve DNSKEY-record
2. Add the DNSKEY-record to the old DNS zone and re-sign zone
   Unfortunately, when switching from Openprovider's secure DNS it is not possible to add the DNSKEY-record to the Openprovider's DNS as this is not supported yet by PowerDNS. During the update, the domain will temporarily be unsigned
3. Add the DNSKEY-record to the domain at the current provider, do not remove the existing one
4. Wait until the TTL is over (safe period: at least 24 hours)
5. Transfer domain: assign new nameservers and add both DNSKEY-record elements to the domain
6. After 24 hours after completion of the transfer (after the registry's zonefile update), remove the old DNSKEY-record from the domain
   In case of switching to or from Openprovider's secure DNS, Openprovider will automatically remove the previous DNSKEY-record
7. Transfer complete!

⚠ **Important note:** It is currently not possible to sign a DNS zone for a domain that has not yet been transferred to Openprovider. This means a seamless transfer from a third-party DNSSEC-signed DNS service to Openprovider with DNSSEC enabled is not supported.

Before initiating a transfer to Openprovider, you must first disable DNSSEC at your current provider. Once the transfer is complete, you can enable and configure DNSSEC on Openprovider's DNS.

Revision #2
Created 2026-08-07 14:27:38 UTC by Sarath
Updated 2026-08-07 15:45:14 UTC by Sarath