

CONFIGURING YOUR NAME SERVERS ON MY.LU

User manual

Publication date: 29 June 2021



TABLE OF CONTENTS

1.	INTRODUCTION	4
2.	GENERAL INFORMATION ABOUT DNS.....	5
2.1.	The purpose of DNS servers	5
2.2.	Structure of domain names and DNS servers	5
2.3.	The importance of 'glue records'	5
2.4.	The added value of DNSSEC	5
3.	DNS MANAGEMENT ON MY.LU	6
3.1.	Timings for DNS changes propagation	6
3.2.	Number of servers required	6
3.3.	Types of DNS records supported	7
4.	CONFIGURATION OF YOUR OWN DNS SERVERS	8
4.1.	Step 1: Access DNS settings	8
4.2.	Step 2: Activate DNS configuration.....	8
4.3.	Step 3 (optional): Enter your DS records.....	8
4.4.	Step 4: Configure your DNS servers.....	9
4.5.	Step 5: Confirm your DNS records	9
5.	CONFIGURATION OF MY.LU DNS SERVERS.....	10
5.1.	Configuring your hosting	10
5.1.1.	Step 1: Access DNS settings	10
5.1.2.	Step 2: Edit your DNS records.....	10
5.1.3.	Step 3: Activate DNS configuration	10
5.1.4.	Step 4 (optional): Enter your DS records	11
5.1.5.	Step 5: Confirm your DNS records	11
5.2.	The structure of editing DNS records.....	11
5.2.1.	Steps to follow to edit DNS records.....	11
5.2.2.	Table of required information	12
5.2.3.	Explanation of data fields	14

1. Introduction

The use of a domain name - whether for websites or email addresses - requires name servers to be activated and configured.

On the [my.lu](https://www.my.lu) registration platform, users can configure each of their registered domain names in one of two ways:

- using their own servers or those provided by their DNS provider;
- using the DNS servers provided by my.lu.

In its role as a .lu registrar, the Restena Foundation provides, via the my.lu online registration platform, DNS servers that allow you to use your .lu domain name reliably and with total peace of mind thanks to authoritative servers that benefit from DNSSEC (Domain Name System Security Extensions) technology in addition to a high level of resilience owing to the use of anycast servers (distributed across Europe with the aim of being located as close as possible to visitors and their DNS requests).

This service is intended for companies and individuals using the my.lu registration platform to register and manage their .lu domain names.

→ For more information on the 'Registration of .lu' service, visit

<https://www.restena.lu/en/service/registration-lu>

→ For more information on the 'DNS Servers' service, visit

<https://www.restena.lu/en/service/dns-servers>

2. General information about DNS

2.1. The purpose of DNS servers

DNS allows for a domain name to be linked to servers acting as a domain name database. The proper configuration of these DNS servers ensures accessibility to sites and/or email addresses associated with a particular domain name by translating the domain name (intelligible to humans) into an IP address (an encoded address identifying, in a unique way, a particular item on the network) or some other data.

By responding to requests related to the addresses registered within the domain name system, these computers are vital in terms of ensuring the seamless operation of the Internet. It is generally advisable to configure several DNS servers for the same domain name to guarantee continuity of services and to ensure the proper functioning of one's domain name in the event of a technical issue - such as a fire at the data centre, cable break, etc. - that may affect one of the servers.

2.2. Structure of domain names and DNS servers

A domain name is typically displayed in the format: 'nameofmycompany.lu'. This name can provide access to certain services such as websites (www.nameofmycompany.lu) and email addresses (lastname.firstname@nameofmycompany.lu). For this purpose, the name must be activated by introducing DNS servers and configuring related DNS records.

The server name itself displays in the form 'ns1.serverownername.lu'. Several different domains and sub-domains can point to this server. Except for certain exceptions, sub-domains are recognisable by the '.' which punctuate DNS server names.

2.3. The importance of 'glue records'

A 'glue record' is the IP address of the name server announced by the parent when the domain name uses name servers hosted under this same domain. In this case, the DNS server is considered as a sub-domain of the domain name as its name ends with the domain name covered.

This is where a 'glue record' becomes imperative. Without it, the DNS resolver – which allows the elements linked to a certain domain name to be decrypted and displayed - is unable to access the sub-domain.

Example: I want to activate the domain name 'mydomain.lu', using DNS servers called 'ns1.mydomain.lu' and 'ns2.mydomain.lu'. I must encode the IP addresses specific to each server.

2.4. The added value of DNSSEC

DNSSEC (*Domain Name System Security Extensions*) integrate each domain into a chain of trust within the naming convention tree structure on the Internet. It is vital to have these to ensure the reliability of the information broadcast by the DNS and to reinforce the safety and trust of all Internet users. With DNSSEC, all records used within the .lu zone, as well as those signed with DNSSEC cryptographic keys, are authenticated. A public key fingerprint associated with the domain name is used to confirm the validity of DNS responses, right up to the .lu root.

With DNSSEC, records (in other words, everything that is used within a particular zone) is authenticated by signing and creating a chain of trust that extends to the root of the DNS. Thus, a first key signs the registrations, while a second, slightly stronger key signs the first key.

Important: If you want to replace your DNS servers running with DNSSEC with new servers also using this technology, you run the risk of experiencing an interruption to your service. To ensure the continuity of DNSSEC protection while changing DNS servers, simple precautions should be taken: submit the server information concerning names that are active at the time of creating or changing one's domain name, and ensure the co-existence of the old and the new DS records, for a period of two days.

Note: Irrespective of the DNS provider selected, DNS records are configured on the servers introduced on my.lu.

3. DNS management on my.lu

Throughout the lifespan of your domain name, and at no additional cost, DNS configuration can be activated or deactivated, either using your own DNS servers (or those of your DNS provider) or the DNS servers provided by the Restena Foundation under my.lu.

3.1. Timings for DNS changes propagation

When you make a change to DNS servers, certain delays - that cannot be reduced - apply. Three types exist:

→ **Delays at the .lu registry**

The root zone of the .lu is updated 24 hours a day, 7 days a week - at each full hour.

→ **Delay when going online**

When activating DNS servers for the first time, the effect becomes visible within one hour, after the changes have been published by the .lu registry.

→ **Delays for changes to take effect**

When making changes to your name servers, new information will propagate depending on the TTL (Time to Live) associated with your domain name; in other words, the timeframe during which data related to your domain name on the .lu zone is stored in memory.

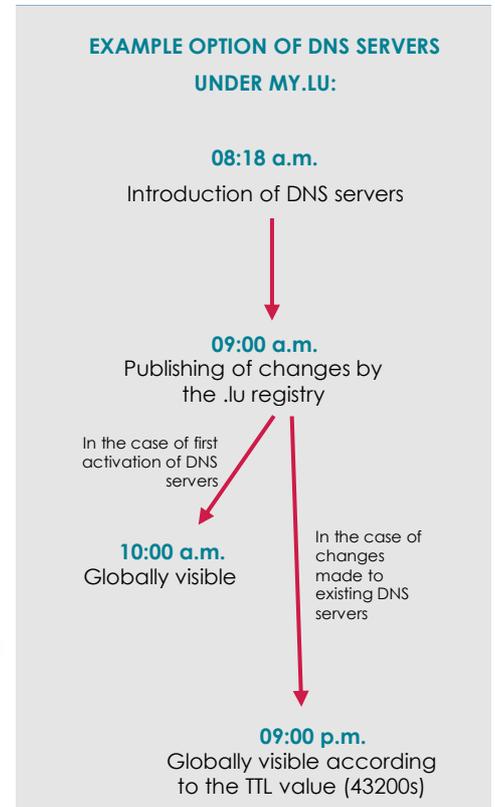
The TTL varies from one DNS provider to another. It is explicitly defined according to a set default value - often 1hr, 6hrs, 12hrs, 24hrs, or even 48hrs - and which may, depending on the specific case, be changed.

Note: The default TTL on the DNS servers provided under my.lu is 43200s, which is 43,200 seconds, or 12hrs. This TTL cannot be changed.

3.2. Number of servers required

In order to activate your domain name, you can communicate between two and six different servers on my.lu.

At least two servers are required for activating your domain name. The encoding order of your servers does not affect their use in any way. There is no set order for DNS servers. Your servers are used to handle DNS requests in an entirely random manner.



3.3.Types of DNS records supported

Type of record	Purpose	Reference document ¹
A	Associate a domain name with an IPv4 address so that the server is able to communicate.	RFC 1035
AAAA	Associate a domain name with an IPv6 address so that the server is able to communicate.	RFC 3596
CAA (Certification Authority Restriction)	Specify the certification authority(ies) (CA) authorised to issue certificates for a particular domain name.	RFC 6844
CNAME	Redirect one request towards another, in particular in order to bring in traffic from several different domains to a single location. <u>Notes:</u> <ul style="list-style-type: none"> • A CNAME can only be applied to names registered under a particular domain, • Where a CNAME is defined for a particular name, no other DNS record type can be defined for the same name. 	RFC 1035
DNSKEY (DNS Public Key)	Sign and authenticate the DNS's Resource Record Sets (RRsets) using the public keys used in the DNSSEC authentication process.	RFC 4034 RFC 3755
DS (Delegation Signer)	Check the DNSSEC key for a particular sub-domain.	RFC 4034 RFC 3658
MX (mail exchange)	Define the incoming mail servers for email.	RFC 1035
NAPTR (Naming Authority Pointer)	Rewrite a domain name based on common expressions, which could then be used as a URL, search for additional domain names, etc.	RFC 2915 RFC 2168 RFC 3403
NS (authoritative name server)	Specify the authorised host for a specific zone and domain (name servers, delegation).	RFC 1035
SOA (start of authority)	Mark the start of authority for a particular DNS zone. <u>Note:</u> The DNS zone for a particular domain name is automatically pre-populated with a SOA that cannot be changed by the user.	RFC 1035
SPF (Sender Policy Framework)	Specify the hosts authorised to use the names and the ADministrative Management Domain (ADMD) mail recipients.	RFC 7208
SRV (Server Selection)	Associate several servers to a single domain, move services from one host to another without too much difficulty and nominate certain hosts as primary servers for a particular service and others as backup servers.	RFC 2782
SSHFP (Secure Shell Key Fingerprints)	Provide secure, remote login and other secure network services over a non-secure network owing not only to server authentication of a client, but also to user authentication to the server. The fingerprint of the server's public key in the DNS by using DNSSEC is particularly sought.	RFC 4255
TLSA (Transport Layer Security (TLS) Protocol)	Specify the keys used on the TLS servers, in other words, encrypted communications by means of the TLS (Transport Layer Security) protocol.	RFC 6698
TXT	This arbitrary human-read text field is used to: <ul style="list-style-type: none"> • integrate the information requested by instances to check that you are in fact the holder of the domain (Google, Adobe, etc.); • limit the servers able to send emails as part of its use via the SPF protocol. 	RFC 1035

¹ Technical reference documents published by the Internet Engineering Task Force ([IETF](#))

4. Configuration of your own DNS servers

4.1. Step 1: Access DNS settings

→ You are registering a new domain name

When you register an 'available to register' domain name, your DNS servers are configured before your order is completed.

To do this, click on the 'Edit' button from your shopping cart content: 

Shopping cart content

Please check or modify the registration details for each domain name added in your cart before confirming your order.

Domain name	Action	Price VAT exc.	Price VAT inc.	State
mydomain.lu	Registration (1 years)	21.37 €	25.00 €	Incomplete
Total (VAT exc.)		21.37 €		
VAT		3.63 €		
Total (VAT inc.)		25.00 €		

In order to proceed to checkout for your cart contents you must either remove/edit domains marked as "Incomplete" and remove or solve the respective issues for those marked as "FAIL". Click on details (🔍) button to view domain details and the reason of their failure.

Click here 

→ You are editing an already existing domain name

If you already own a domain name or are the new holder of the domain following its transfer or handover from another domain holder and/or another registrar, it is configured in the domain name section linked to your account.

To do this, once logged in to your my.lu account, go to the 'My domain names' section and then click on , the 'Details' button associated with your domain name.

My domain names

The following domain names are linked to your account.

Domain name	Registered on	Expires on	State
mondomaine.lu	25 Mar 2021	25 Mar 2022	Active
mondomainelu.lu	14 Apr 2021	14 Apr 2022	Reserved

The list of your domain names can be exported in XML format. This XML export will contain all your contacts, the details of the domain names with references to the respective contacts. Where appropriate nameservers and zone contents will be included.

Download XML export file

Click here 

4.2. Step 2: Activate DNS configuration

To activate the DNS configuration of your domain name, set your domain status to 'Active'.

To do this, select the 'Active' option in the 'Domain status' section.

Domain status

Reserved
 Active
 Active, hosted zone

4.3. Step 3 (optional): Enter your DS records

The 'DS records' fields should only contain data if you are using DNSSEC authentication to protect your domain name (see Section '2.4. The added value of DNSSEC'). Also find the process to follow for your particular case below.

→ You are not using DNSSEC and do not want to sign your domain name with DNSSEC

In this case, the field is left blank.

DS records

→ You want to change the DNSSEC signature of your domain name

- Add a new line containing your new DS records, below your existing record(s).
- Keep your existing DS record(s) for at least two days to ensure the continuity of DNSSEC protection.
- 48 hours after recording your changes, log in to your account again and delete the record that has become 'obsolete'.

Do not delete the existing record straight away, wait for 48 hours.

DS records

12345 8 2 0abcde1abcde2abcde3abcde4abcde5abcde6abcde

Add your new record in the line just below your existing record

→ Your domain name is DNSSEC signed and you no longer want to use DNSSEC

By deleting your DS records, you forego the benefits offered by DNSSEC protection (see Section '2.4. The added value of DNSSEC').

4.4. Step 4: Configure your DNS servers

- a. In the 'DNS Server#1' to 'DNS Server#6' fields, at least two DNS servers are required. Enter items to enable identification into the following fields for your servers:

- name (example: ns1.restena.lu)
- address, in IPv4 (example: 158.64.1.23) or IPv6 (example: 2001:a18:1::23) format only if your server name ends with the domain name you are in the process of configuring.

Note: All of this information is available from your DNS provider.

Then click on 'Check nameservers' so that the system can check for proper connection to the encoded servers.

- b. → **The DNS server test has been passed**
Connection with your server(s) has been established. You can pass directly to the next step.

Nameserver test passed
Nameserver test for domain mondomaine.lu
Nameserver nspub-eu.dns.lu at 2a01:3f1:832:0:0:0:53 (provided)
Nameserver nspub-eu.dns.lu at 194.58.196.32 (provided)
Nameserver pdns-test.dns.lu at 158.64.229.11 (provided)
Nameserver pdns-test.dns.lu at 2001:a18:4:0:0:0:11 (provided)

- **The DNS server test has failed**
Connection to your server(s) has not been successfully established, as one or more items of information are incorrect. A message listing all of the errors encountered displays. Work through the various errors point by point and make corrections directly in the fields dedicated to the server (see Point a.).

Nameserver test failed
Nameserver test for domain mondomaine.lu
Nameserver ns1.restena.lu at 158.64.1.23 (provided)
Nameserver ns1.restena.lu at 2001:a18:1:0:0:0:23 (provided)
Nameserver ns2.restena.lu at 2001:610:188:406:145:100:190:186 (provided)
Nameserver ns2.restena.lu at 145.100.190.186 (provided)
Error: External nameserver 'ns2.restena.lu' does not resolve to provided address '2001:a18:1:0:0:0:23'
Error: [UDP] Query failed for nameserver 'ns1.restena.lu' at address '158.64.1.23' (Refused)
Error: [UDP] Query failed for nameserver 'ns1.restena.lu' at address '2001:a18:1:0:0:0:23' (Refused)
Error: [UDP] Query failed for nameserver 'ns2.restena.lu' at address '2001:610:188:406:145:100:190:186' (Refused)
Error: [UDP] Query failed for nameserver 'ns2.restena.lu' at address '145.100.190.186' (Refused)
Error: No working authoritative nameserver found
Error: At least 2 nameservers required

Important: If you encounter the error 'REFUSED' and/or the error 'SERVFAIL', your DNS provider is the only one able to make the necessary correction. In this case, please contact your provider that will treat the issue directly with the my.lu team.

[Check nameservers](#)

Once this has been done, click again on 'Check nameservers'.

Repeat the process as often as necessary, until contact with the servers has successfully been established and the test server succeeds.

Note: You can decide to continue with the registration or change to your domain name despite failure of the DNS test server, however:

- if you register a new domain name: it will automatically be reallocated 'Reserved' status;
- if you change an already existing domain name: the information you enter will be captured, but any changes will be rejected by the registry when these changes are processed.

4.5. Step 5: Confirm your DNS records

- **You are registering a new domain name**

Click on the 'Continue' button at the very bottom so that the my.lu interface can capture your encoded data.

[Continue](#)

→ **You are editing an already existing domain name**

Click on the 'Update domain' button to enable the my.lu interface to apply all of the changes you wish to make.

[Update domain](#)

5. Configuration of my.lu DNS servers

5.1. Configuring your hosting

5.1.1. Step 1: Access DNS settings

→ **You are registering a new domain name**

When you register an 'available to register' domain name, your DNS servers are configured before your order is completed.

To do this, click on the 'Edit' button from your shopping cart content: 

Shopping cart content

Please check or modify the registration details for each domain name added in your cart before confirming your order.

Domain name	Action	Price VAT exc.	Price VAT inc.	State	
mydomain.lu	Registration (1 years)	21.37 €	25.00 €	Incomplete	 
Total (VAT ex.)		21.37 €			
VAT		3.63 €			
Total (VAT inc.)		25.00 €			

In order to proceed to checkout for your cart contents you must either remove/edit domains marked as "Incomplete" and remove or solve the respective issues for those marked as "FAIL". Click on details (🔍) button to view domain details and the reason of their failure.

[Click here](#)

→ **You are editing an already existing domain name**

If you already own a domain name or are the new holder of the domain following its transfer or handover from another domain holder and/or another registrar, it is configured in the domain name section linked to your account.

To do this, once logged in to your my.lu account, go to the 'My domain names' section and then click on , the 'Details' button associated with your domain name.

My domain names

The following domain names are linked to your account.

Domain name	Registered on	Expires on	State	
mondomaine.lu	25 Mar 2021	25 Mar 2022	Active	
mondomainelu.lu	14 Apr 2021	14 Apr 2022	Reserved	

The list of your domain names can be exported in XML format. This XML export will contain all your contacts, the details of the domain names with references to the respective contacts. Where appropriate, nameservers and zone contents will be included.

[Download XML export file](#)

[Click here](#)

5.1.2. Step 2: Edit your DNS records

→ **You are registering a new domain name**

DNS records cannot be edited at the time of registering a domain name, as the information relevant to the DNS servers as well as a DNSSEC key are automatically generated and integrated into my.lu only while processing the order.

In this case, skip this step and go directly to Step 3. DNS records can be edited after the order has been paid for.

Note: The 'Edit DNS records' option is only accessible when a change is made to an existing domain name associated with your my.lu account.

DNS records can only be edited once your order has been completed, and, by definition, only when making a change to an already existing domain name.

→ **You are changing an already existing domain name**

To configure your initial DNS records, scroll down towards the bottom and in the 'Domain status' section, click on 'Edit DNS records'.

[Refer to Section '5.2.1. Steps to follow to edit DNS records'](#) in this manual for more information on the steps to follow to edit DNS records.

Domain status

- Reserved
- Active
- Active, hosted zone

[Edit DNS records](#)

When a domain is active, hosted zone the DNS records like web server, e-mail server and others can be configured in my.lu.

5.1.3. Step 3: Activate DNS configuration

To activate the DNS configuration of your domain name using the servers provided by my.lu, select the option 'Active, hosted zone' in the 'Domain status' section.

Domain status

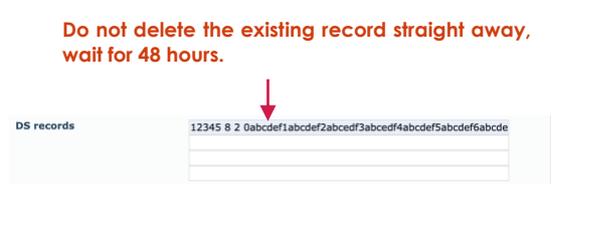
- Reserved
- Active
- Active, hosted zone

[Edit DNS records](#)

When a domain is active, hosted zone the DNS records like web server, e-mail server and others can be configured in my.lu.

5.1.4. Step 4 (optional): Enter your DS records

The 'DS records' fields should only contain data if you are using DNSSEC authentication to protect your domain name (see Section '2.4. The added value of DNSSEC'). By using the DNS servers provided under my.lu, a DNSSEC key is automatically generated and new related DS records are automatically entered by the my.lu interface after the successful confirmation of your order or your changes. Below you will find the process to follow, depending on your specific situation.

<p>→ Your domain name is not DNSSEC signed In this case, the field is left blank.</p>	
<p>→ Your domain name is already DNSSEC signed</p> <ul style="list-style-type: none"> Keep your existing DS record(s) for at least two days in order to ensure the continuity of DNSSEC protection; 48 hours after recording your changes, log in to your account again and delete the record that has become 'obsolete'. 	<p style="color: red; text-align: center;">Do not delete the existing record straight away, wait for 48 hours.</p> 

5.1.5. Step 5: Confirm your DNS records

<p>→ You are registering a new domain name Click on the 'Continue' button at the very bottom so that the my.lu interface can capture your encoded data.</p>	
<p>→ You are editing an already existing domain name Click on the 'Update domain' button to ensure that the my.lu interface is able to apply all of the changes you want to make.</p>	

5.2. The structure of editing DNS records

When a domain name is marked as 'Active, hosted zone', the DNS records supported by my.lu (See Section '3.3. Types of DNS records supported') must be managed (added, changed or deleted) directly in the my.lu interface.

DNS records can, however, be prepared ahead, i.e. added, changed or deleted in the my.lu platform before the name is marked as 'Active, hosted zone'. In this case, the relevant records are recorded on the platform but will only take effect once the domain name is marked 'Active, hosted zone'.

5.2.1. Steps to follow to edit DNS records

<p>a. In the DNS zone editor, click on  and then select from the displayed list the type of DNS record you want to create (see Section 5.2.2. 'Table of required information' for more detailed information)</p> <p>Once the selection has been made, click on 'Continue'.</p> <p>Note: You can only edit/create one record at a time.</p>	 <p style="color: red; text-align: right;">Click here</p>
<p>b. Depending on the type of record selected, enter the requested data. The mandatory fields are circled in red.</p> <p>Once entered in the required format, click on 'Save'.</p>	<p style="color: red;">Details of the various record types can be found in section '5.2.2. Table of required information'.</p>

c. Your record has successfully been processed, your change(s) will appear in your DNS record list, marked in the following background colour:

- green for an added record;
- orange for an edited record;
- red for a deleted record.

If you have several DNS records to edit/create/delete, reiterate points 2. and 3. for each of them.

Then, once you have finished, click on 'Publish DNS changes'. The background colour disappears. All of your changes are recorded, but at this stage they have not yet been applied. They will only be published and therefore visible once all of your changes have been confirmed (see section '5.1.5. Step 5: Confirm your DNS records').

Important : The visibility of the introduced records - which only has an effect if the domain name is marked 'Active, hosted zone' - will apply within delays defined by the TTLs (Time to Live) associated with your domain name (see section '3.1. Timings for DNS changes propagation'). Please note that if the records entered modify the value of one or more TTLs, the old value applies to the current record. The new TTL(s) will apply for future changes.

Note: you can change your records at any time by clicking on  or delete them by clicking on , the buttons associated with your record.



5.2.2. Table of required information

For more technical details on the following records, refer to the descriptions and reference documents (RFCs) listed in Section '3.3. Types of DNS records supported'.

A	<p>Label <input type="text"/></p> <p>Time to live (TTL) 43200</p> <p>Record type A</p> <p>IP address 127.0.0.1</p>
AAAA	<p>Label <input type="text"/></p> <p>Time to live (TTL) 43200</p> <p>Record type AAAA</p> <p>IP address 0:0:0:0:0:0:1</p>
CAA (Certification Authority Restriction)	<p>Label <input type="text"/></p> <p>Time to live (TTL) 43200</p> <p>Record type CAA</p> <p>Flags Default (0)</p> <p>Tag Non-wildcard issuer (issue)</p> <p>Value ;</p>
CNAME	<p>Label <input type="text"/></p> <p>Time to live (TTL) 43200</p> <p>Record type CNAME</p> <p>Target <input type="text" value="."/></p>
DNSKEY (DNS Public Key)	<p>Label <input type="text"/></p> <p>Time to live (TTL) 43200</p> <p>Record type DNSKEY</p> <p>Flags Key-signing key (256)</p> <p>Protocol 3 (3)</p> <p>Algorithm RSASHA256 (8)</p> <p>Public key 000000000000</p>

DS (Delegation Signer)	Label <input type="text"/> Time to live (TTL) 43200 Record type DS Keytag 0 Algorithm RSAMD5 (1) ▾ Digest type SHA-1 (1) ▾ Digest 000000000000
MX (mail exchange)	Label <input type="text"/> Time to live (TTL) 43200 Record type MX Priority 0 Target <input type="text" value="."/>
NAPTR (Naming Authority Pointer)	Label <input type="text"/> Time to live (TTL) 43200 Record type NAPTR Order 0 Preference 0 Flags <input type="text"/> Service <input type="text"/> Regular expression <input type="text"/> Replacement value <input type="text" value="."/>
NS (authoritative name server)	Label <input type="text"/> Time to live (TTL) 43200 Record type NS Target <input type="text" value="."/>
SPF (Sender Policy Framework)	Label <input type="text"/> Time to live (TTL) 43200 Record type SPF SPF constraints v=spf1 ~all
SRV (Server Selection)	Label <input type="text"/> Time to live (TTL) 43200 Record type SRV Priority 0 Weight 0 Port 0 Target <input type="text" value="."/>
SSHFP (Secure Shell Key Fingerprints)	Label <input type="text"/> Time to live (TTL) 43200 Record type SSHFP Algorithm RSA (1) ▾ Fingerprint type SHA-1 (1) ▾ Fingerprint 000000000000
TLSA (Transport Layer Security (TLS) Protocol)	Label <input type="text"/> Time to live (TTL) 43200 Record type TLSA Certificate use CA certificate (0) ▾ Selector Full certificate (0) ▾ Match type Exact match (0) ▾ Certificate 000000000000
TXT	Label <input type="text"/> Time to live (TTL) 43200 Record type TXT Free text <input type="text"/>

5.2.3. Explanation of data fields

The items to incorporate in each DNS record follows a special syntax that must be observed, failing which you run the risk of encountering a 'Please follow the required format' error message and red marking of the field concerned:

- **IP addresses:**
 - IPv4: 4 numbers between 0 to 255, bounds included, separated by dots and not containing any unnecessary 0s (e.g. 158.64.1.23)
 - IPv6: short or long notation, but no mixed notation 'IPv4-IPv6' for IPv6-mapped-IPv4 (e.g. 2001:a18:1::23).
- **Algorithm:** select the appropriate value from the list displayed
- **Certificate:** value follows the selector's choice, displayed in hexadecimal format
- **Certificate use:** select the appropriate format from the list displayed
- **Digest:** hash value, presented in hexadecimal format²
- **Digest type:** select the appropriate format from the list displayed
- **Flags:**
 - under the CAA type, select the appropriate format from the list displayed
 - under the DNSKEY type, select the appropriate format from the list displayed
 - under the NAPTR type, incorporate one or more of the following data items: 's', 'a', 'u', 'p'
- **Time to Live (TTL):** numerical value (expressed in seconds) between 300 and 31536000 (inclusive)
- **Fingerprint:** hexadecimal representation² of the SSH key fingerprint
- **Fingerprint type:** select the appropriate format from the list displayed
- **Free text:** text without any accents or special characters, and without any limitation of length
- **Keytag:** numerical value between 0 and 65535
- **Label:** blank field or @ for records applying to the domain name as such, or the part that precedes the domain name (e.g. www)
- **Match type:** select the appropriate format from the list displayed
- **Order:** numerical value between 0 and 65535
- **Weight:** numerical value between 0 and 65535
- **Port:** numerical value between 0 and 65535
- **Preference:** numerical value between 0 and 65535
- **Priority:** numerical value between 0 and 65535
- **Protocol:** select the appropriate format from the list displayed
- **Public key:** hexadecimal value² containing numbers between 0 and 9 and letters from A to F
- **Regular expression:** text without any accents or special characters, and without any limitation of length as defined in the usage details for NAPTR record RFCs
- **Replacement value:** full name of the existing DNS, written in lowercase, to which a full stop is added (e.g. server.of.my.provider.tld.)
- **Selector:** select the appropriate format from the list displayed
- **Service:** according to NAPTR record RFC reference documents
- **SPF constraints:** According to SPF standard, defined in the technical reference document [RFC 7208](#)

² Hexadecimal = value as a base-16, noted in the form of a series of pairs comprised of numbers from 0 to 9 or letters from a to f, in uppercase or lowercase

- **Tag:** select the appropriate format from the list displayed
- **Target:** full name of the existing DNS written in lowercase, to which a full stop is added at the end (e.g. server.of.my.provider.tld.). For IDN targets, enter the ASCII/ACE representation.
Warning: the target cannot be identical to the domain name. In the event it falls under the domain name, a DNS record related to the target must have been created beforehand.
- **Value:** CAA value provided by your certification authority