INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

.lu
operated by **Restena**

.DOMAIN NAME SECURITY

TABLE OF CONTENTS

INTRODUCTION

The current evolution of cyber threats and cyber-attacks makes it necessary to elaborate specific guidance and best practices for securing network and information systems. Meanwhile, some topics do not get the attention they need. Not every entity or person has their own network or information system, however, many people and entities have an online presence. When talking about cybersecurity, one also needs to talk about the security of the entity's online presence to avoid quite common scenarios like the defacing of a website.

In this document the Restena Foundation and the Institut Luxembourgeois de Régulation (ILR) are proud to share some insights on how to secure your online presence as well as some security aspects to assure a secure Domain Name Service.

ILR and Restena Foundation aim with this document to raise awareness to the security in relation of the domain names. This document highlights the security measures users of the domain name service should implement to be protected in a state-of-the-art manner against several types of threats to their domain names. The strength of the security and resilience of our society is only as strong as the weakest link of the chain. Accordingly, these guidelines and best practices are produced as part of the NISDUC (NIS Directive User Community) conference, organised on 10 and 11 May 2022 in Luxembourg, where we are discussing "how to tackle the implementation of NIS/NIS2.0?". We consider the security of domain names as a crucial part of the security of the essential services and thus a crucial part to the security of our society.

This guidance is targeting mainly operators of electronic communication networks and services and operators of essential services. Additionally, the recommendations can also be helpful to the management body of our partners and other entities.

The objective of this document is twofold, first it will give an introduction of the Domain Name Service (DNS), describing the structure and principles of DNS to elaborate afterwards on some guidance and hints when doing a registration of a domain. It will explore guidelines on domain name exploitation and where to be vigilant while setting up a domain name.

The second objective focuses on issuing guidance for securing the domain name using DNSSEC (Domain Name System Security Extensions). In this guideline, it will be discussed why DNSSEC is necessary, and explain its principles, strengths and limitations.

From left to right: Cynthia Wagner and Guillaume-Jean Herbiet (Restena Foundation), Sheila Becker and Guy Mahowald (Institut Luxembourgeois de Régulation)

Restena Foundation

Restena manages and operates the high-speed network built to serve the needs of the research and education community in Luxembourg. This infrastructure, which is a building block for the governments ambitions for data-driven research, is complemented with additional services and strong assistance for the community's security operations. Additionally, Restena provides a strong infrastructure for the national economy by managing the .lu domain name registration platform and taking care of most of the technical operations of the national internet exchange LU-CIX.

Institut Luxembourgeois de Régulation

ILR is the single point of contact for Luxembourg for the *« Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne »* (NIS law) as well as the competent authority for the sectors: energy, transport, drinking water, health, digital infrastructure. Additionally, ILR is also in charge of the security provisions in the telecom sector according to the *« Loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques »* (EECC).

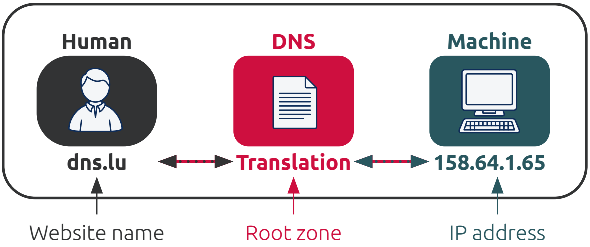
THE DOMAIN NAME SYSTEM – DNS

The Domain Name System (DNS) is one of the core elements of the internet. Its protocol was developed in the late 80s with main functionality to provide a distributed naming system. At that time, priority was given to performance and resilience. Protection against malicious actors were not an important requirement. Over time, security has become a major aspect in the DNS protocol.

DNS structure

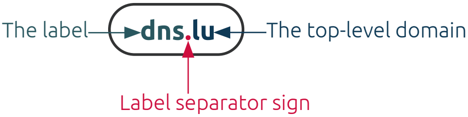
Similar to a phonebook for the internet, the most visible use of the DNS is helping humans by translating meaningful names into the IP addresses that computers need to communicate. Typing a literal address into a browser triggers such a DNS lookup. However, it is important to note that the use of DNS is not limited to web browsing but is an essential part or almost any service or communication over the internet (e.g. email, time services, VOIP).

- **The DNS structure**

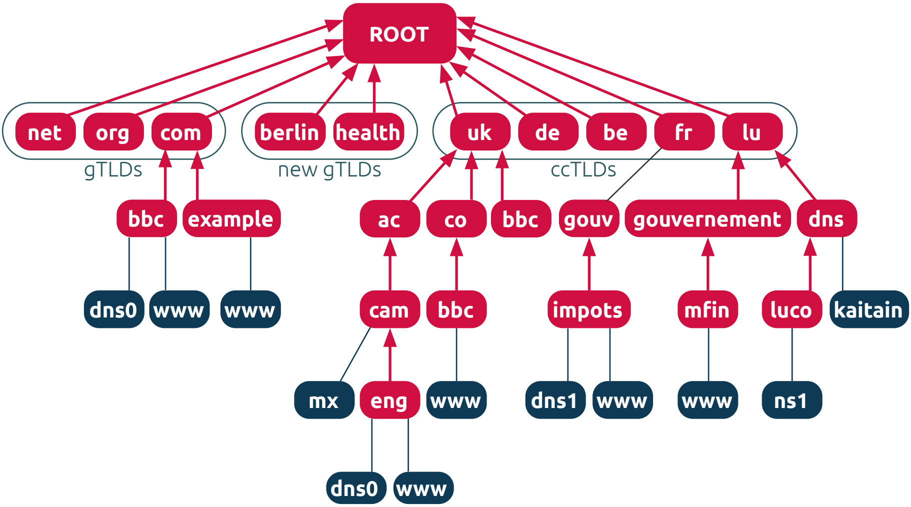


The hierarchical naming structure of the DNS starts at the root zone whose directory enables this translation process. The DNS root zone holds the reference points to top-level domains (country code suffixes or generic/thematic suffixes, namely ccTLDs and gTLDs), which in turn refer to the second-level domains, and so on.

- **Details of a domain name**



- **The DNS tree**



Legend
- Blue colour: hostname or leaf
- Red colour: start of authority (SOA) or beginning of a DNS zone

DNS principles

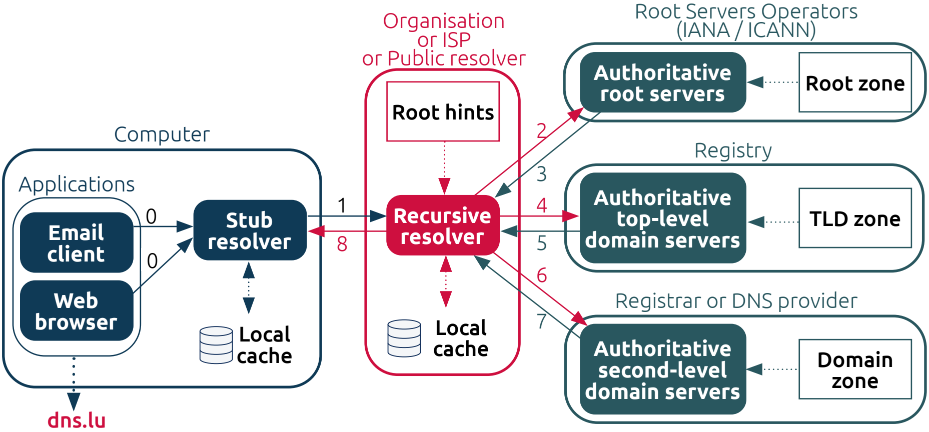
Information related to each domain, such as the IP address of the web server, is contained in the corresponding DNS zone in the form of resource records (RR). For each domain, several authoritative servers have a copy of the zone to reply to requests for information.

In order to retrieve the requested information, a recursive resolver (generally managed by the internet service provider or organisation IT service) is in charge of contacting the various authoritative servers from the DNS root down the DNS tree.

To visit the www.dns.lu website,
a recursive resolver may contact:
- the authoritative servers for the DNS root;
- the authoritative servers for the .lu top-level domain;
- the authoritative servers for the dns.lu domain, where information about www.dns.lu exist in the corresponding zone.

Each received information is stored temporarily
in a local cache to speed up further operations.

- **DNS resolution**



Registration best practices

Starting a new activity on the internet requires a strong online presence. Setting up a reprentative website starts with the registration of a domain name.

- It gives a first impression about the business or activity.
- It provides credibility.
- It completes the domain name as a brand.
- It provides independency of other platform providers, such as from social media pages.

Therefore, the choice of a good domain name as well as a corresponding top-level domain (TLD) is a critical step.

How to choose a domain name

Before thinking about the domain name itself, it is recommended to pick the top-level domain.

1. Select your top-level domain (TLD) based on your goals.

Top-level domains can convey an additional meaning to a name, like .lu suggests an attachment to or presence in Luxembourg, or .de a link to Germany. Generic domains like .com or .org tend to be favoured by more global organisations. The availability of a domain name in a TLD or the reputation of that TLD can also influence a choice.

2. Pay attention to the jurisdiction that applies in case of conflicts.

It is worth having a look at the terms and conditions set by the registry running the top-level domain you have selected.

Automated tools, like DNS Twist can help you identify possible permutations and detect homograph phishing attacks, typo squatting, and brand impersonation.

3. Check the availability of a domain name with the selected top-level domain(s).
Bear in mind that domain names are usually registered on a "first come, first served" basis.

4. Search about conflicts or the literature meaning of the domain name in each country.
It will avoid any embarrassments.

5. Register the most important variations of the original domain name.
It avoids the use of similar domain names by others either for legitimate or malicious use (i.e., typo-squatting), so protecting your online image and the security of all potential visitors.

6. Register your domain name in all relevant top-level domains (TLDs), including generic (like .com or .net) or country-code (like .lu, .fr or .de).
This is especially appropriate for entities with an international presence, as it prevents domain typo squatting and increases the visibility of the chosen name, respectively brand.

How to choose a registrar

End-users (or registrants) generally rely on commercial entities called registrars to manage their domain names. Registrars act as the customer-facing intermediary of registries and usually allow the registration of domains in multiple TLDs. They often provide DNS authoritative servers for registered domains and additional internet services like web hosting and email allowing the domain proper use.

Each top-level domain is administered by a registry, an authority centrally managing all domains registered under its TLD. It set rules for registration of domain names falling under its scope, that accredited registrars agree to follow.

1. Define all internet services you need to connect to your domain name.
Depending on the needs and knowledge, it might be worth choosing a registrar that offers all-in-one solutions in addition to domain names. Working with one provider ensures that all the services are properly integrated and work together with no effort. On the other side, implementing part of the technical infrastructure or using different providers leads to increased independence in the domain name management.

2. Check if the registrar is accredited for all the top-level domains you have selected.
Most registration offices (registrars) offer the possibility to register a name under several top-level domains, this will ease the management of your domain names.

Example

The domain dns.lu is registered with Restena's registrar activity which provides the information to the .lu registry (managed by the Restena Foundation) to add it to its register.

Domain name exploitation guidelines

Once registered, a few guidelines can dramatically increase the reliability and the security of the services associated with a given domain name.

Diversity and redundancy

The resilience of the DNS is based on heavy use of diversity and redundancy. To ensure domain availability, key elements are to be used.

1. **Multiple authoritative name servers.**
   They provide data for your DNS zone.
2. **Different operating systems and software for your servers.**
   This limits the impact of bugs and vulnerabilities.
3. **Anycast servers.**
   They decrease resolution latency and exposure to denial-of-service attacks (each server being a set of different physical instances spread around the world).
4. **Different providers, or servers in different networks.**
   Thanks to them, failure at one entity (i.e., technical problem or a deliberate attack) does not lead to domain name unavailability.

The criticality of a domain name should determine the protections to put in place. Those considerations should drive the choice of DNS providers or the design of the internal DNS infrastructure.

Typo squatting

Syntactic variations of domain name (by deleting, repeating or replacing letters by similar characters, or using additional dashes) is often used to mislead end-users, for instance in spam or phishing campaigns.

This is especially relevant for entities with an international presence when choosing a domain name.

Example: Typo squatting for `dns.lu`

(Export from DNS Twist)

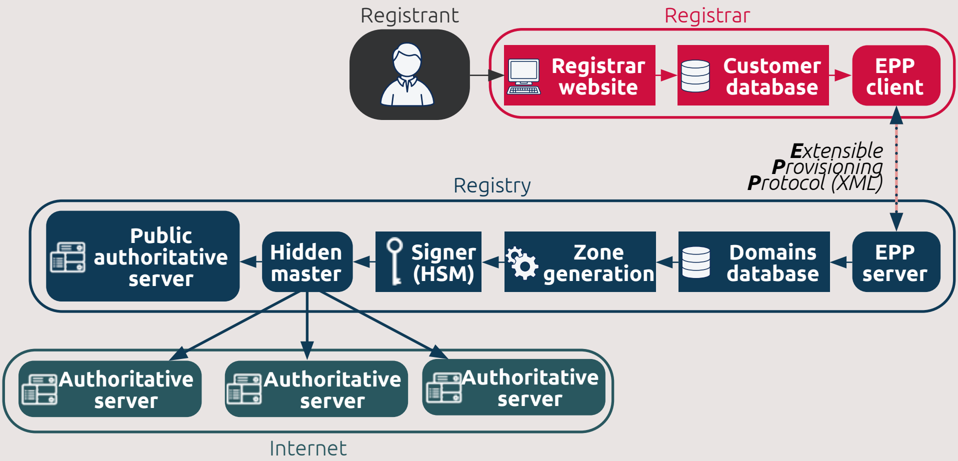
Original:	dns.lu
Additions:	dns1.lu, dns2.lu, dns3.lu
Homoglyph:	bms.lu, bns.lu, dms.lu
Omission:	dn.lu, ds.lu
Repetition:	ddns.lu
Replacement:	cns.lu, dbs.lu, dna.lu, dns.lu, dnx.lu, dny.lu, sns.lu
Transposition:	dsn.lu, nds.lu
Various:	dns.lu.lu

Registry lock

Registrars send information about registered domain to the registries of each TLD using a dedicated communication protocol called Extensible Provisioning Protocol (EPP).

In order to protect a domain name against attacks on the registrar platforms, an increasing number of registries provide registry lock: domain changes received from the registrar via EPP require a direct confirmation from the registrant (often via an administrative procedure) before being implemented by the registry.

The 3R model



This diagram illustrates the whole domain name registration and publication process under the Registrant/Registrar/Registry (or 3R) model, used by most top-level domains, including `.lu`.

The end-user, or registrant, obtains one or several domain names via a registrar, generally using a secure web interface. The registrar maintains its own customers database and may provide registration under several top-level domains.

For each TLD, the corresponding registry receives information from each accredited registrar via a secure communication channel using the Extensible Provisioning Protocol (EPP). The registry generates a DNS zone file from its database of registered domains. This zone file is most often signed by DNSSEC to ensure its authenticity and then published on authoritative servers, operated by the registry or third parties.

Domain name deletion

How to let go a domain name

The control of a domain name by its holder can be terminated by a deletion or trade.

Deletion at any time

Made at the holder's request only.

After deletion the domain name is available for new registration. Some registries implement a quarantine period to revert accidental deletions or cater for changes of mind.

Trade to another holder

May induce some cost (usually payable by the future holder).

The receiving party has a guarantee that the domain name does not become unavailable.

Consequences of a deletion

Removed from the DNS, the deleted domain name no longer provides results for the requested information about services using the domain. This has various consequences.

- **Inaccessibility of services linked to the domain name and all its sub-domains**, without impacting the referenced content. The services and their content are still available but under another domain name or via the IP address directly.
- **Inaccessibility of services provided outside the domain name** but dependent on it for links or automated data collection tools.
- **Inaccessibility of all DNS servers within the domain name**, which may affect other domain names using those servers and third-party organisations depending on them for the operation of their own domain names.
- **Inaccessibility of all sub-domains delegated** from the domain name.

There is an alternative to deleting a domain name.

Some registries allow their customers to reserve a domain name with deactivated access. This option is relevant if the domain name may be of use in a future point of time.
The holder safeguards ownership, but this induces yearly costs.

SECURING YOUR DOMAIN NAME WITH DNSSEC

The original DNS design does not provide strong security against attacks. DNS Security Extensions (DNSSEC) introduce a solution to guarantee data integrity, guaranteeing the outcome of the resolution process is legitimate and hasn't been altered.

Applying DNSSEC provides DNS data authentication and avoids several vulnerabilities.

The need for DNSSEC

Most internet services rely on the DNS to operate properly and efficiently. Besides, DNS has become an important source of truth for security features such as the protection electronic exchanges over the web.

- **DNSSEC identifies authorized certificates and certification authorities** for a domain name using DANE and CAA.
- **DNSSEC fights phishing and spam** by specifying email policies and signatures using SPF, DKIM or DMARC.

Automated certificate issuance protocols like ACME (used for instance by Let's Encrypt) heavily rely on the DNS for their validation process. Hence, control of some DNS data could lead to the malicious generation of certificates considered as genuine by the victims.

As a consequence, many cyberattacks involved replying to compromised DNS responses to the targeted victims, leading them to malicious servers where sensitive information like credentials could be collected by the attacker.

Falsification of the DNS response data could happen at any level of the resolution process, with either the authoritative server or the network path being compromised by an attacker.

DNSSEC protects against many attacks aiming at the DNS infrastructure.

- **Authoritative server hijacking or spoofing** as long as the DNSSEC keys are not stored on the compromised server.
- **Zone data compromission at the authoritative server**.
- **Zone data compromission during zone transfer** between authoritative servers providing replicas of the zone for sake of redundancy.
- **Cache poisoning** at the resolver level.
- **Man-in-the-middle** tampering resolution data between recursive resolver and client.

DNSSEC principles

DNSSEC extends DNS communications and builds a cryptographic chain of trust from the DNS root to any signed resource record.

Each received DNS response is then checked against this chain of trust by a validating recursive resolver during the resolution process.

• Zone signature

DNSSEC guarantees the authenticity and integrity of each existing set of resource records of the same type (RRSET) by adding to the zone data an associated cryptographic hash called a resource Record Signature (RRSIG).

The signature of each resource record set is generally achieved using a pair of cryptographic keys with different properties.

- **The Zone Signing Key (ZSK) signs most of the content of the zone.**
  Operational considerations (like signing speed and signatures size) tend to bound the complexity of this key which is hence likely to be regularly rotated.
- **The Key Signing Key (KSK) only signs the resource record set related to the DNSSEC keys themselves**.
  This key can have stronger cryptographic properties but requires coordination with the parent zone when rotated.

The generalization of elliptic curve cryptography allows the generation of strong keys of limited size and enables an alternative signing model where both the ZSK and a KSK are replaced by a single Common Signing Key (CSK) that signs the entire zone content.

The zone signature process also creates additional resource records, named Next Secure (NSEC or NSEC3), authenticated with their own RRSIG, that link each existing resource record with the next one. This process allows to cryptographically prove the non-existence of data in the zone.

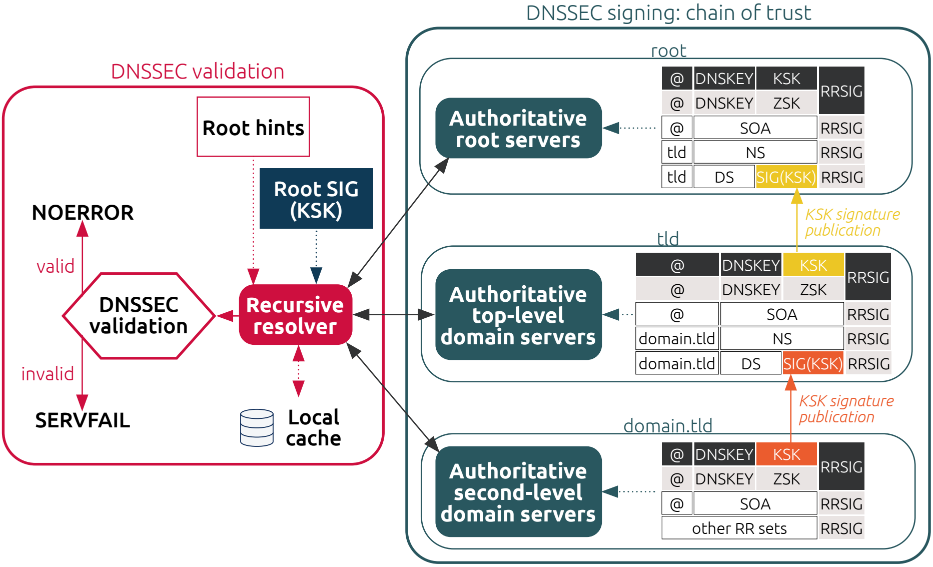
Contrary to the X.509 certificates (used in HTTPS), DNSSEC keys do not expire: it is up to the operator to decide whether and when keys are rotated.

However, in DNSSEC, the signature of each resource record set has a limited lifetime: the zone shall hence be regularly re-signed to remain valid.
Due to the use of caching in the DNS, rotating the DNSSEC keys need to follow an established schedule for signatures to remain valid during the whole process, called a key roll-over.

Signed zone delegation

Integration of a signed zone to the DNSSEC chain of trust is achieved by publishing the digest of the currently used KSK (or CSK) to the parent zone in the form of a Delegation Signer (DS) resource record. This comes in addition to other delegation data (such as the list of authoritative name servers for the zone and their IP addresses when required).

DNS resolution


DNSSEC signing: chain of trust
DNSSEC validation
Root hints
Root SIG (KSK)
NOERROR
valid
DNSSEC validation
invalid
SERVFAIL
Recursive resolver
Local cache
root
Authoritative root servers
KSK signature publication
tld
Authoritative top-level domain servers
KSK signature publication
domain.tld
Authoritative second-level domain servers

root

@	DNSKEY	KSK	RRSIG
@	DNSKEY	ZSK	
@	SOA		RRSIG
tld	NS		RRSIG
tld	DS	SIG(KSK)	RRSIG

tld

@	DNSKEY	KSK	RRSIG
@	DNSKEY	ZSK	
@	SOA		RRSIG
domain.tld	NS		RRSIG
domain.tld	DS	SIG(KSK)	RRSIG

domain.tld

@	DNSKEY	KSK	RRSIG
@	DNSKEY	ZSK	
@	SOA		RRSIG
other RR sets			RRSIG

Each time the KSK (or CSK) is rotated, the DS record published at the parent zone must be updated. This additional coordination point has to be integrated in the whole key roll-over process.

Example

The digest of the KSK used for signing the dns.lu zone is published in the corresponding DS record in the .lu zone. Following the same logic, the digest of the KSK used for signing the .lu zone is published in the corresponding DS record in the root zone.

DNSSEC validation

For DNSSEC to fulfull its purpose, the zone must not only be signed, but signatures verified. This validation is usually performed by the recursive resolver during the resolution process.

Besides the root hints (list of the IP addresses of all root servers) required to initiate the resolution, the configuration files of validating recursive resolvers also include the digest of the KSK signing the root zone. This trust anchor is used to ensure all received resource record matches their corresponding signature (RRSIG), signed with the proper key as defined in the chain of trust.

> As the DNSSEC validation is generally performed at the recursive resolver level, this implies the end-user trusts this component of the DNS chain, which can be operated by an external entity. Security can be improved by running a validating resolver locally (on each machine or inside a given network).

If this validation fails, the validating recursive resolver will reply with a DNS error, with the objective of preventing the end-user from accessing an incorrect, and potentially malicious, resource.

DNSSEC strengths and limitations

Strengths

- **Origin authentication of DNS data**

Resolvers validate that data has originated from a legitimate authoritative server.

- **Data integrity**

Resolvers validate those responses were not modified.

- **Authenticated denial of existence**

Authoritative servers provide a response that proves no data exists (signed NSEC resource record).

Limitations

- **Protection span only from publication to validator**

DNSSEC cannot protect against manipulation at the registrar or registry level. Tampering between resolver and client remains also undetectable unless local validation is enabled.

- **Potential misuse of DNS responses**

Because it adds cryptographic signatures, DNSSEC generates larger DNS responses that can be filtered out by poorly configured firewalls or be used as an amplification vector for Distributed Denial of Service (DDoS) attacks.

DNSSEC implementation and best practices

DNSSEC is a real shift in DNS operations and is too often reluctantly considered in the Information Security toolbox. However, since the end of the 2010 decade the service and software offerings for DNSSEC has matured a lot.

Today, many options exist to safely enable DNSSEC on domains, especially when respecting some best practices.

Implementation options

DNSSEC is now often provided "as a service" by many domain name registrars and DNS providers, including in Luxembourg and for .lu domains. In this situation, implementing DNSSEC for a domain can be as simple as flipping a switch.

Mature software solutions also exist when in-house signing is required, from the simplest to the most elaborate and secure options.

- Many DNS software (such as Bind, Knot or PowerDNS) nowadays provide built-in DNSSEC inline signing functions that include (for the former two) management of keys roll-over which can be enabled with only a few directives or commands.
- When advanced options and security are required, OpenDNSSEC is a powerful alternative that automatically manages the whole life cycle of DNSSEC keys using a dedicated Hardware Security Module (HSM) as secure enclave and fine-grained configuration of the roll-over processes.

Dedicated utilities (ValiDNS, LDNS) and online tools (DNSViz, DNSSEC analyzer) also allow easy validation of the signed zone.

Best practices

With the proper tooling, DNSSEC signing is not more complicated than other security process. However, like any other security feature, its use opens the path to new failure mode and thus needs some care:

- **Training**
  To prevent signing errors, a proper understanding of DNS and DNSSEC operations with a certain level of details is essential.

- **Planning**
  Changes in the DNSSEC configuration, such as key roll-overs, including a rollback strategy would something go wrong, need to be carefully planned ahead.

- **Monitoring**
  As DNSSEC-protected zones need to be periodically re-signed, it is of vital importance to continuously monitor the signing process and the validity of its output.

- **Maintenance**
  DNSSEC requires regular maintenance of the signed zone and is less tolerant to configuration errors. Mistakes can have dramatic effects on service availability then deployed without understanding nor planning.

DNSSEC errors generally gain a lot of press as their impact on service availability could be important. They are most often caused by lack of one or several of the previous points and could have been easily avoided with sufficient training, planning, monitoring and maintenance.

Even when signed with DNSSEC, a zone is only considered in the validation process when the corresponding DS record is published in the parent zone. It is hence possible to test a DNSSEC setup before going live.

DNSSEC in Luxembourg

DNSSEC adoption results in Luxembourg are mixed: while the DNS infrastructure already meets the prerequisites for a wide adoption of DNSSEC, the number of signed .lu domain names remains low.

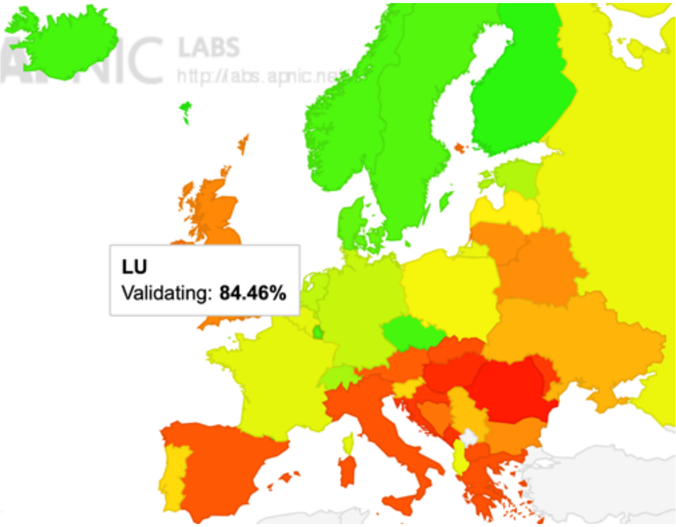
DNSSEC implementation in Luxembourg, as in other countries, still requires to step-up to be fully effective.

Ready for wide adoption

The .lu zone, managed and operated by the Restena Foundation, has been signed by DNSSEC since February 2011, and the signature of its KSK published in the root zone since June 2011. The signing infrastructure has since then been kept up to date to meet all newest standards.

According to continuous measurements by APNIC Labs, almost 87% of all DNS requests from users in Luxembourg are performed by a validating recursive resolver, meaning that most local internet users could be protected by DNSSEC during their day-to-day internet usage. This positions Luxembourg in the top 10 of European countries, and a leader in the Greater Region.

DNSSEC Validation Rate by country (%) map, with a focus on the .lu zone, 24 March 2022
(source: APNIC Labs)

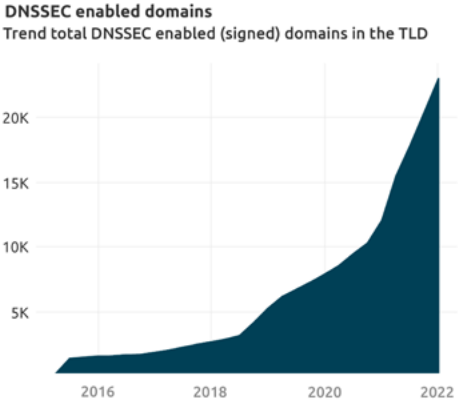


A rising fraction of signed domains

A limited fraction of .lu domains have their zone signed by DNSSEC.

According to CENTR Stats, only 7% of zones under the .lu top-level domain are signed as of the first quarter 2022. While this number has almost doubled in 2022, it still places Luxembourg at the rear of the European pack in terms of adoption.

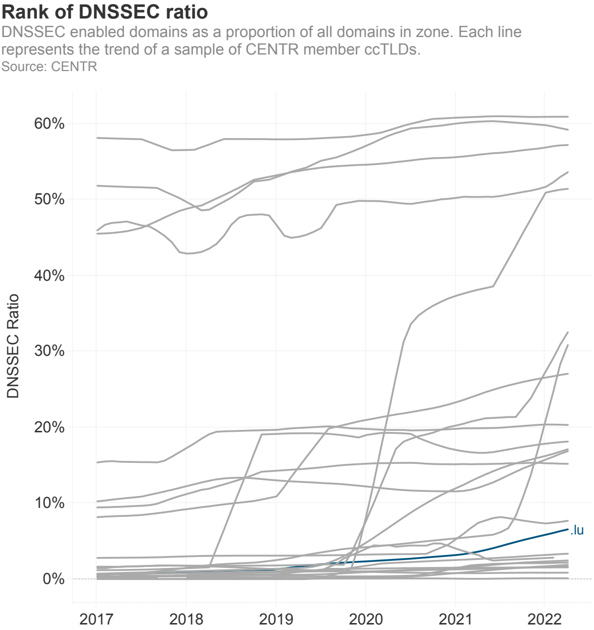
A deeper analysis reveals that amongst the 2,500 most popular .lu domain names (according to lists like Alexa, DomCop, Majestic and Cisco Umbrella) only 90 are signed. Especially the lack of signed domain names for services with high exposure to attacks leaves room for improvement.



DNSSEC enabled domains for under .lu
(source: CENTR Stats)

Despite the recent increase, there is hence a real effort to make to fully exploit the existing DNSSEC infrastructure and increase security of internet communications in Luxembourg.

DNSSEC ratio in European ccTLDs with a focus on .lu
(source: CENTR)



INDEX

Glossary

CAA – Certification Authority Authorization

ccTLD – Country Code Top-Level Domain

DANE – DNS-based Authentication of Named Entities

DDoS – Distributed Denial of Service

DKIM – Domain Keys Identified Mail

DMARC – Domain-based message authentication

DNS – Domain Name System

DNSSEC – Domain Name System Security Extensions

DS – Delegation Signer

EPP – Extensible Provisioning Protocol

gTLD – Generic Top-Level Domain

HSM – Hardware Security Module

KSK or **CSK** – Key Signing Key

RR – resource records

RRSET – resource records of the same type

RRSIG – resource Record Signature

NSEC or **NSEC3** – Next Secure

SOA – start of authority

SPF – Sender Policy Framework

TLD – Top-Level Domain

ZSK – Zone Signing Key

Useful links

Generic information

APNIC Labs – https://stats.labs.apnic.net/dnssec/XE

CENTR – https://www.centr.org/

CENTR Stats – https://stats.centr.org/

DNS Twist – https://github.com/elceef/dnstwist

DNS protocols definition – https://www.ietf.org

Tools

Bind – https://bind9.readthedocs.io/en/latest/dnssec-guide.html

DNSSEC analyzer – https://dnssec-analyzer.verisignlabs.com

DNSViz – https://dnsviz.net

Knot – https://www.knot-dns.cz/docs/2.6/html/configuration.html#automatic-dnssec-signing

LDNS – https://www.nlnetlabs.nl/projects/ldns/about/

OpenDNSSEC – https://www.opendnssec.org/

PowerDNS – https://doc.powerdns.com/authoritative/dnssec/index.html

ValiDNS – https://github.com/DENICeG/validns

Lists

Alexa – https://www.alexa.com/topsites

Cisco Umbrella – http://s3-us-west-1.amazonaws.com/umbrella-static/index.html

DomCop – https://www.domcop.com/top-10-million-websites

Majestic – https://majestic.com/reports/majestic-million

IMPRESSUM

Editor: Fondation Restena

May 2022

All rights reserved

Author: Fondation Restena, Institut Luxembourgeois de Régulation

Layout: Fondation Restena

Photo and image credits: istock, Fondation Restena, APNIC Labs, CENTR, CENTR Stats

**Institut Luxembourgeois
de Régulation**

17, rue du Fossé
L-1536 Luxembourg
+352 28 228 228 — info@ilr.lu

ilr.lu

Fondation **Restena**
Service **.lu**

2, avenue de l'Université
L-4365 Esch-sur-Alzette
+352 42 44 09-1 — admin@dns.lu

dns.lu **my.lu**