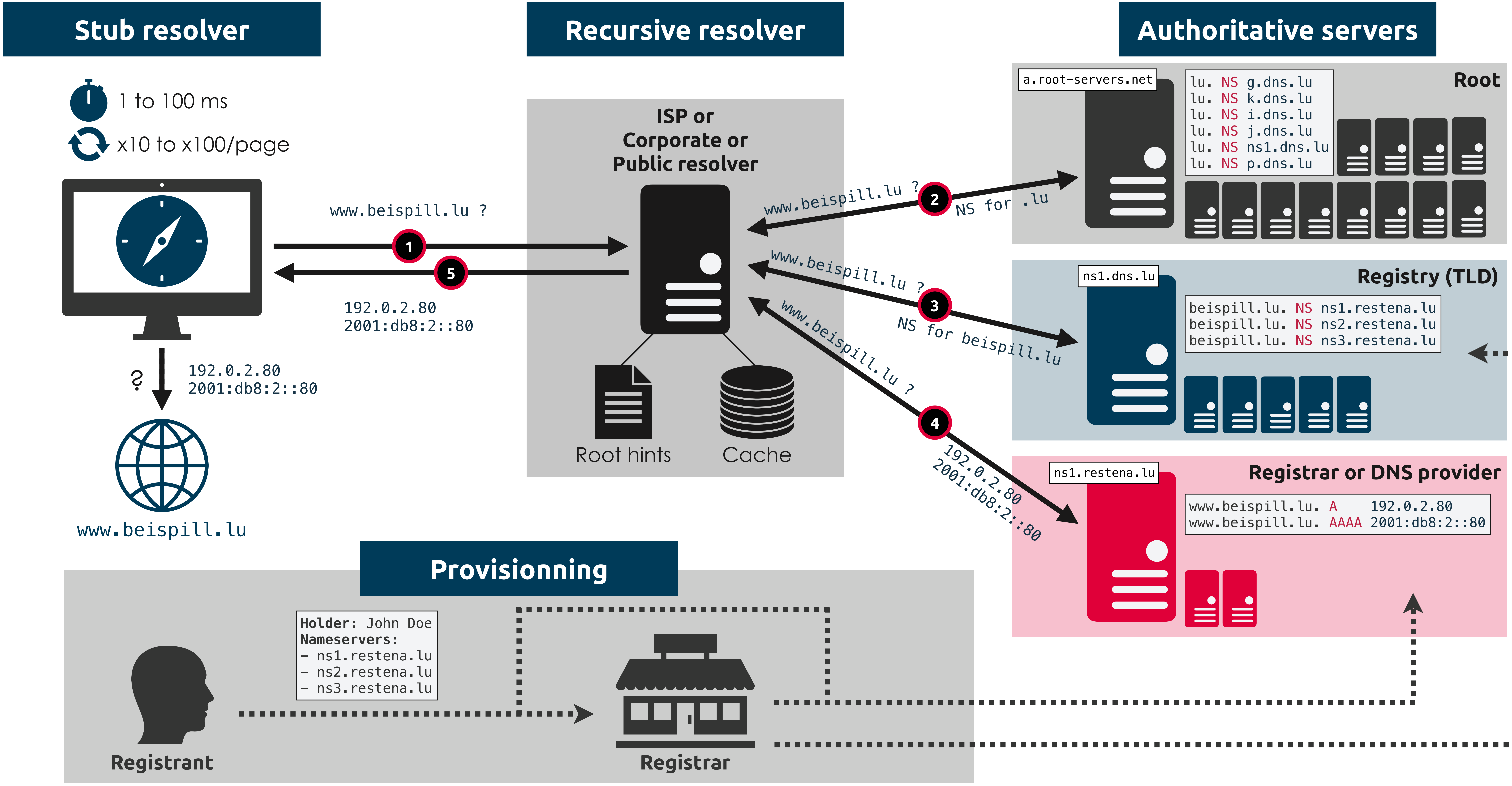
DNS security best practices

A critical infrastructure for essential services

Guillaume-Jean Herbiet
.lu Technical Manager
NISDUC - Tuesday, May 10th 2022

.lu
operated by **Restena**

Domain Name System landscape



Stub resolver

1 to 100 ms

x10 to x100/page

Recursive resolver

ISP or Corporate or Public resolver

Authoritative servers

Root

```
a.root-servers.net
```

```
lu. NS g.dns.lu
lu. NS k.dns.lu
lu. NS i.dns.lu
lu. NS j.dns.lu
lu. NS ns1.dns.lu
lu. NS p.dns.lu
```

Registry (TLD)

```
ns1.dns.lu
```

```
beispill.lu. NS ns1.restena.lu
beispill.lu. NS ns2.restena.lu
beispill.lu. NS ns3.restena.lu
```

Registrar or DNS provider

```
ns1.restena.lu
```

```
www.beispill.lu. A    192.0.2.80
www.beispill.lu. AAAA 2001:db8:2::80
```

Provisionning

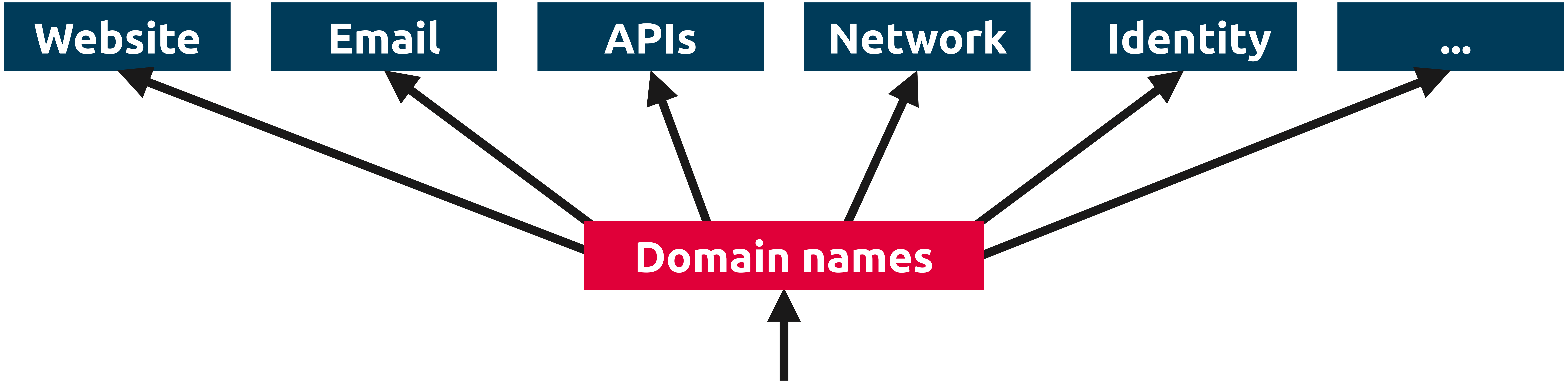
```
Holder: John Doe
Nameservers:
- ns1.restena.lu
- ns2.restena.lu
- ns3.restena.lu
```

DNS: at the core of NIS directive

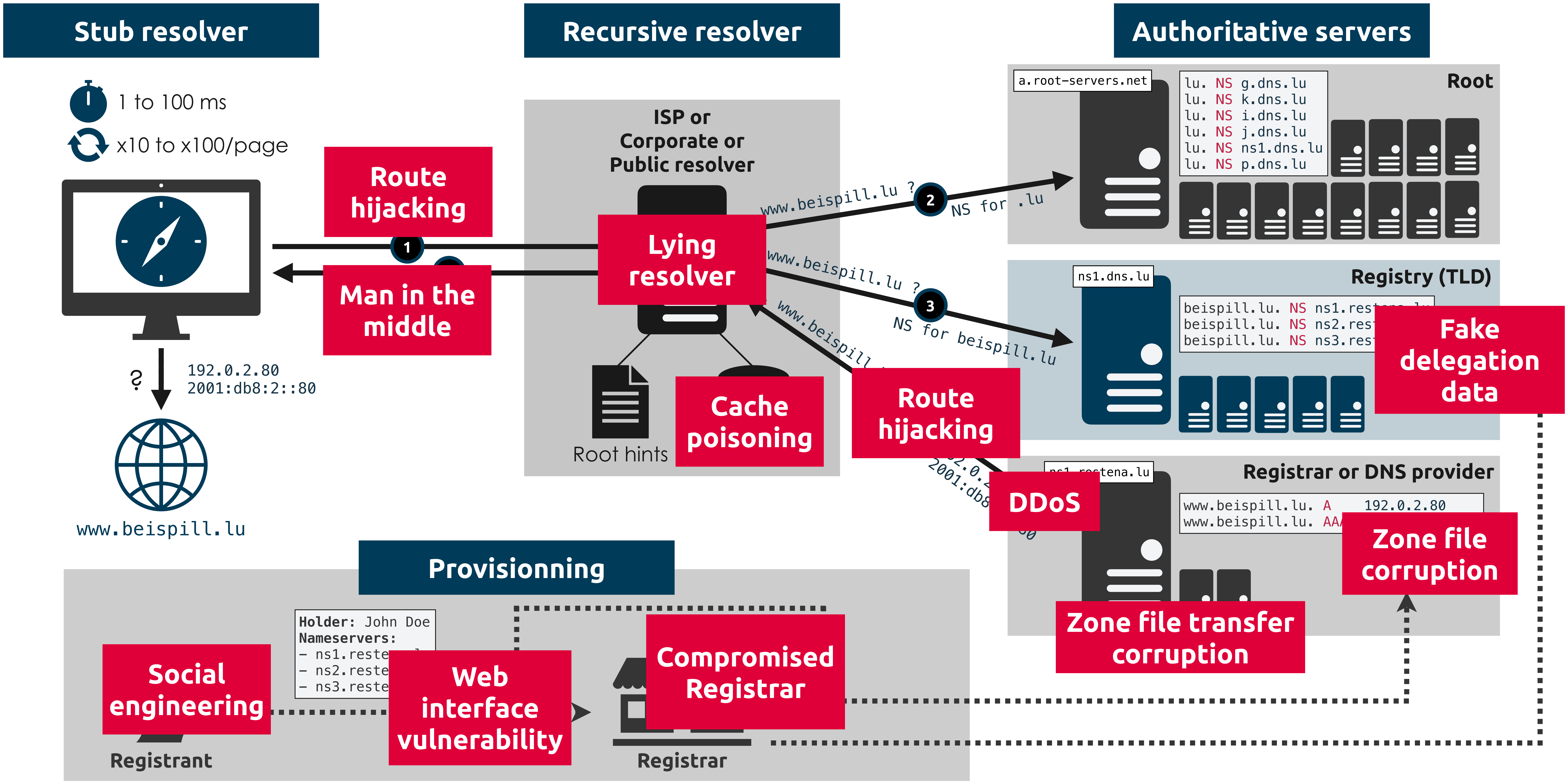
Operators of essential services (Article 4(4) and Annex II)

- **TLD registries** (Article 4(16)): e.g. Restena for .lu
- **DNS service providers** (Article 4(15)):
  registrars; name server providers; ISPs and public resolvers providers

Service depends on network and information systems (Article 5.2(b))



DNS threats and vulnerabilities



Stub resolver

1 to 100 ms

x10 to x100/page

?

192.0.2.80
2001:db8:2::80

www.beispill.lu

Recursive resolver

ISP or
Corporate or
Public resolver

Root hints

Authoritative servers

Root

a.root-servers.net

```
lu. NS g.dns.lu
lu. NS k.dns.lu
lu. NS i.dns.lu
lu. NS j.dns.lu
lu. NS ns1.dns.lu
lu. NS p.dns.lu
```

Registry (TLD)

ns1.dns.lu

```
beispill.lu. NS ns1.restena.lu
beispill.lu. NS ns2.rest
beispill.lu. NS ns3.rest
```

Registrar or DNS provider

ns1.restena.lu

```
www.beispill.lu. A     192.0.2.80
www.beispill.lu. AA
```

1

2 www.beispill.lu ? NS for .lu

3 www.beispill.lu ? NS for beispill.lu

www.beispill.lu ? 192.0.2. 2001:db8 80

Provisionning

```
Holder: John Doe
Nameservers:
- ns1.reste
- ns2.reste
- ns3.reste
```

Registrant

Registrar

Route hijacking

Man in the middle

Lying resolver

Cache poisoning

Route hijacking

Fake delegation data

DDoS

Zone file corruption

Zone file transfer corruption

Social engineering

Web interface vulnerability

Compromised Registrar

The smart choices for your domain names

The right **top-level domain** (TLD): beyond the price and "hype"

- Not all TLDs are equal: generic TLDs (ICANN) vs. country-code TLDs
- Determine the registry, registration rules and applicable jurisdiction
  - Maturity, PI protection, dispute, services (Registry Lock)
- TLDs carry an image (local/global) and a reputation

The right **registrar** (and DNS service provider)

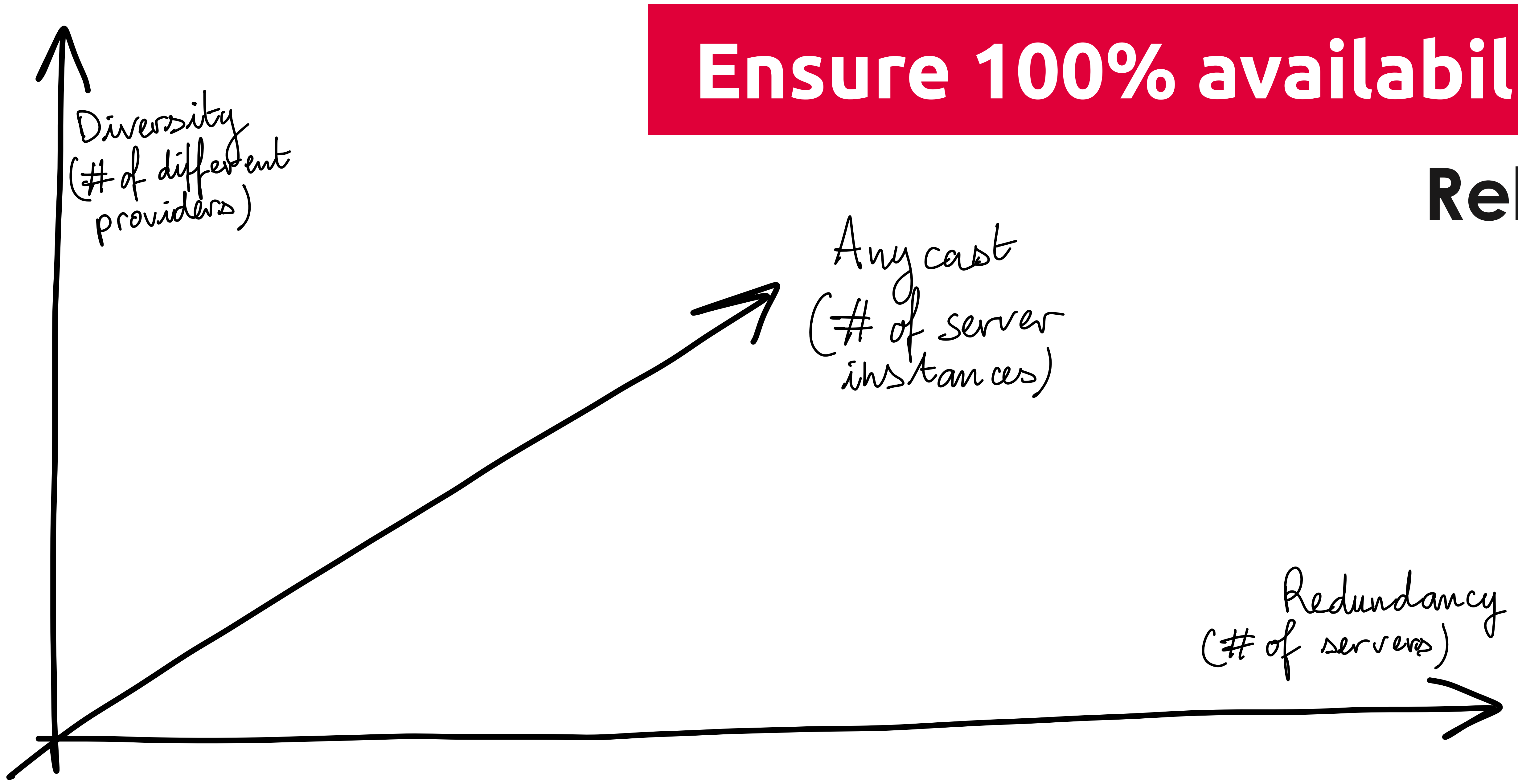
- Maturity, certifications, accreditations
- Multiple factor authentication
- Services (one-stop-shop vs. specialist)

The right **domains names**

- Availability, conflicts, meaning (in different languages...)
- Variations: different TLDs, typosquatting (e.g. `beispill.lu` / `beispil.lu`)
- Those you don't want other to register... (e.g. `beispill.sucks`)

Domain name lifecycle best practices

Ensure 100% availability of your domain name



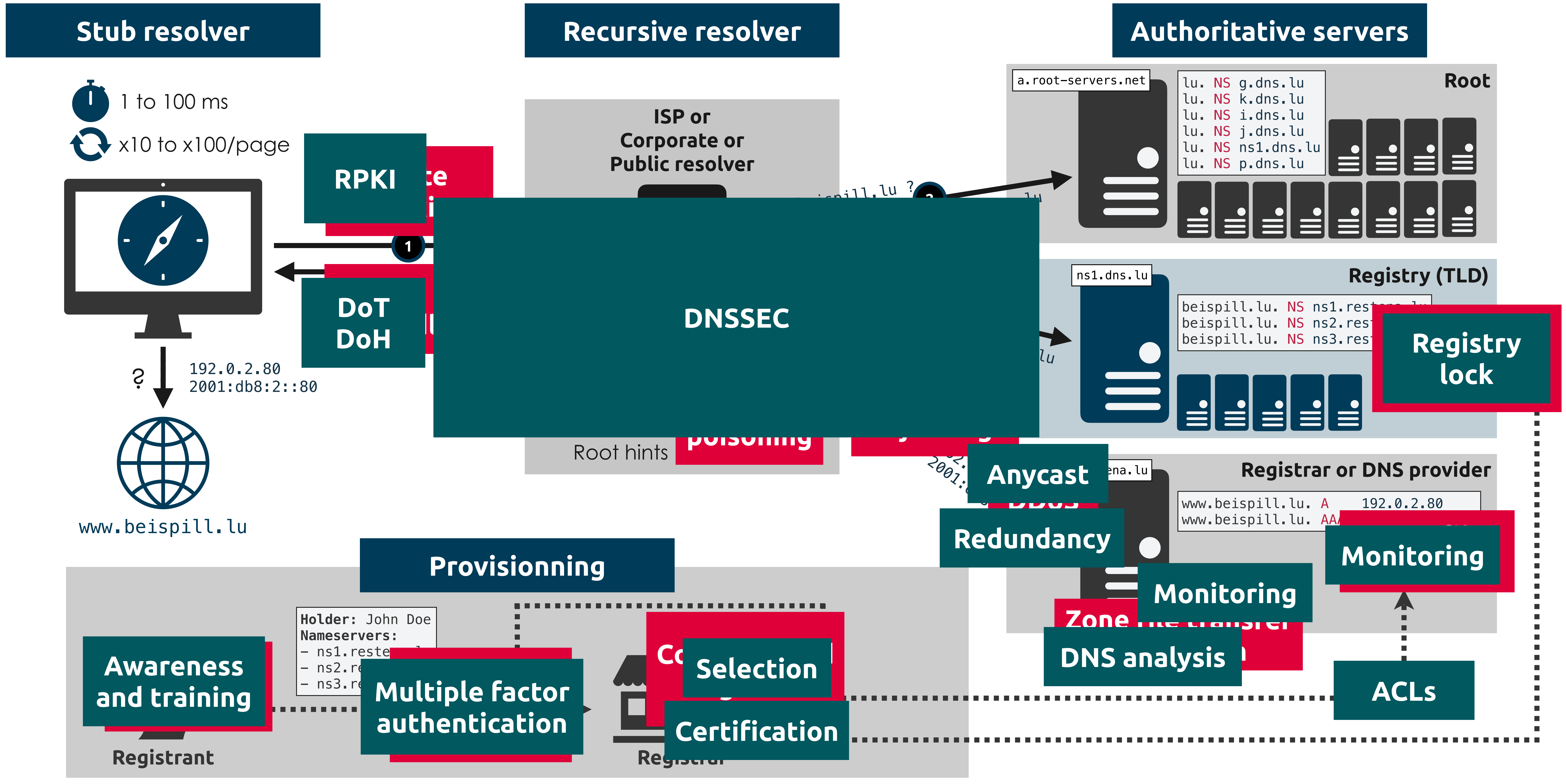
Reliability through diversity and redundancy

1. Multiple name servers (ideally with different software/operating system)
2. Different providers
(or servers in different networks)
3. Anycast servers: multiple server replicas around the world

Handle unused/retired domains properly

- Think twice before deleting a domain:
  - Inaccessibility of services and dependencies
  - Will become available for re-registration by anyone
- Remove DNS data related to de-provisioned services
- Alternative: **domain reservation with deactivated access**

DNS protection measures



Stub resolver

1 to 100 ms

x10 to x100/page

192.0.2.80
2001:db8:2::80

www.beispill.lu

Recursive resolver

ISP or
Corporate or
Public resolver

Root hints

Authoritative servers

Root

a.root-servers.net

```
lu. NS g.dns.lu
lu. NS k.dns.lu
lu. NS i.dns.lu
lu. NS j.dns.lu
lu. NS ns1.dns.lu
lu. NS p.dns.lu
```

Registry (TLD)

ns1.dns.lu

```
beispill.lu. NS ns1.rest
beispill.lu. NS ns2.rest
beispill.lu. NS ns3.rest
```

Registrar or DNS provider

```
www.beispill.lu. A    192.0.2.80
www.beispill.lu. AA
```

Provisionning

```
Holder: John Doe
Nameservers:
- ns1.reste
- ns2.re
- ns3.re
```

Registrant

Registrar

RPKI

DoT
DoH

DNSSEC

Registry lock

Anycast

Redundancy

Monitoring

Monitoring

Zone file transfer

DNS analysis

ACLs

Awareness and training

Multiple factor authentication

Selection

Certification

DNSSEC: the building block of DNS security

Authentication and integrity of DNS data using **cryptographic signatures**

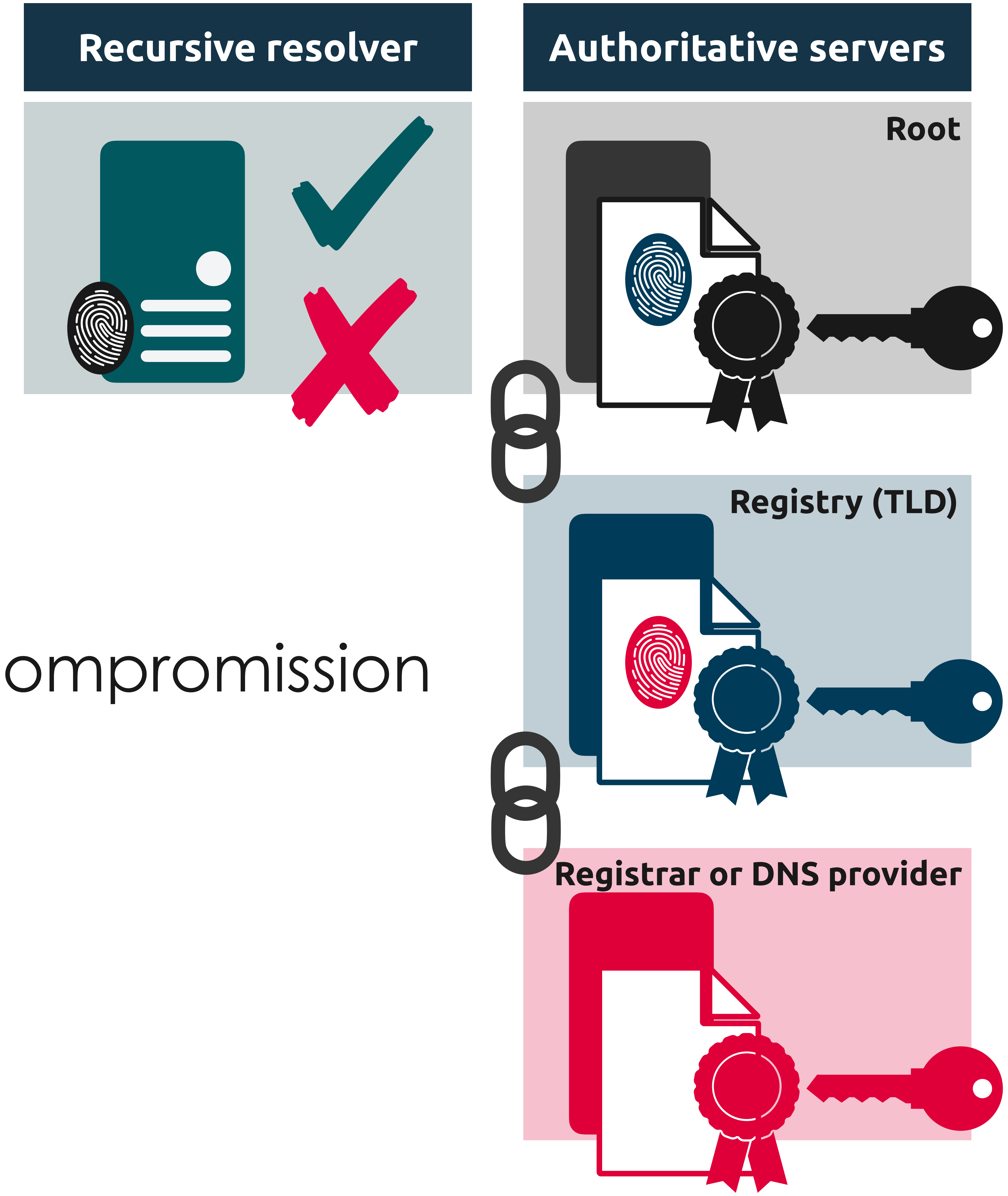
1. **Chain of trust** from the DNS root to each signed data
2. **Validation** during resolution, preventing access to invalid resources

Provides **protection against DNS attacks**

- **On the authoritative server**: hijacking, data compromission
- **On the recursive resolver**: cache-poisoning, man-in-the-middle

Leverages **DNS-based security**

- Email (spam, fishing): SPF, DKIM, DMARC
- Certificates ("too many CAs"): DANE, CAA



Don't be afraid of DNSSEC

DNSSEC misuse might lead to service unavailability

- Usual suspects: signature expiration and key roll-over
- HTTPS certificate expiration? Password expiration? Firewall misconfig?

As any security measure, DNSSEC adds complexity

Proper tooling exists to automate, validate and monitor DNSSEC

- **Signature**: now built in most DNS servers
- **Key management**: built-in or dedicated tools (interface with HSM)
- **Validation/Monitoring**: local or online dedicated tools

You can also **delegate DNSSEC signature** to your registrar/DNS provider

Key elements for proper DNSSEC deployment:

Training **Planning** **Validation** **Monitoring**

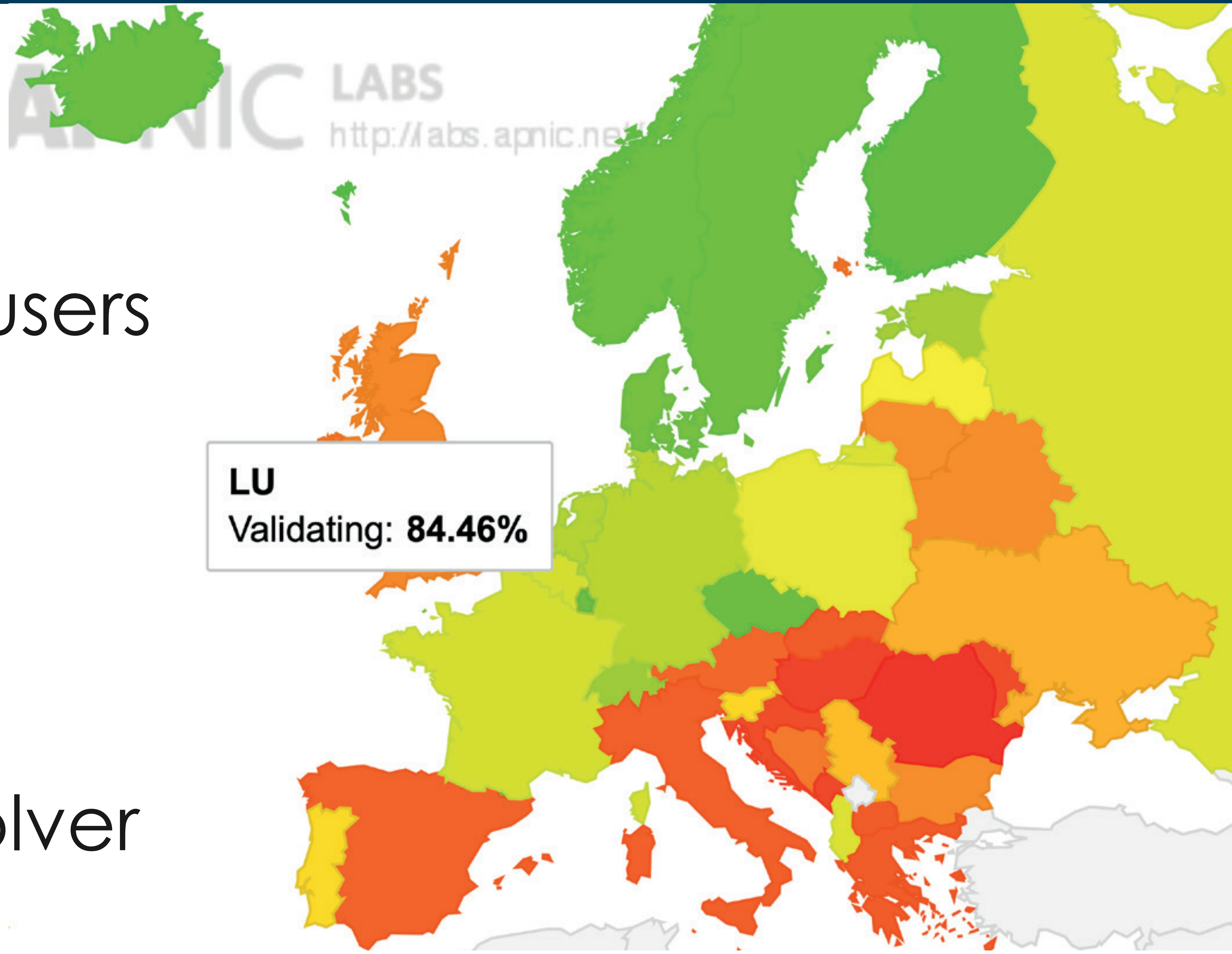
The importance of DNSSEC validation

Resolvers perform the DNSSEC validation

- Widely deployed in Luxembourg
- DNSSEC signing protects most domestic users

Ensure you are behind a validating resolver

- Home: Most ISPs in Luxembourg do it
- Corporate:
  - Rely on your ISP or a trusted public resolver
  - **Run your own resolver in your network (preferred)**



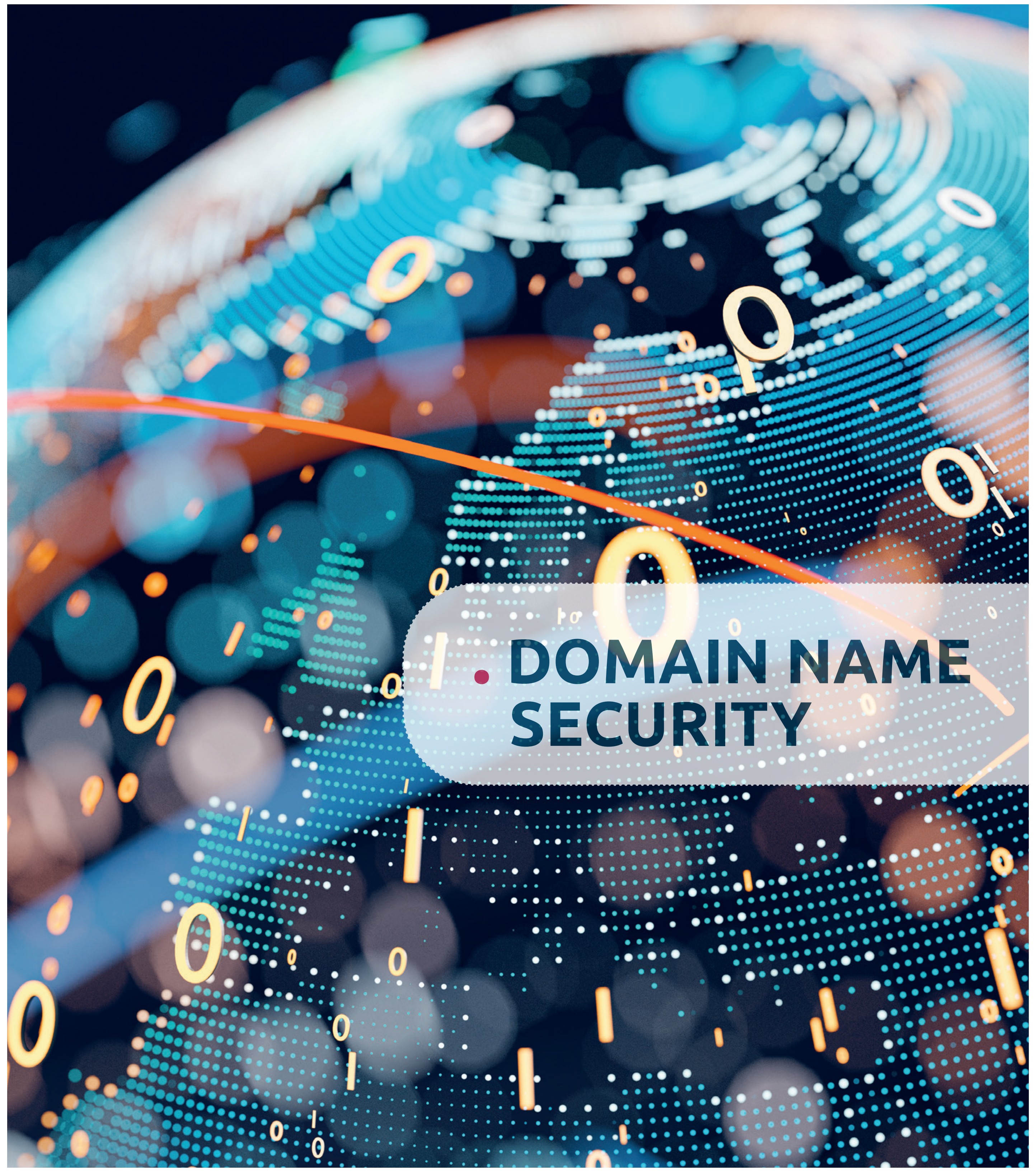
Ensure you trust your validating resolver!

Going further

Domain Name Security brochure

ILR
INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

.lu
operated by **Restena**



See: https://dns.lu/publications

Hands-on **DNSSEC** training

Secure DNS infrastructure with DNSSEC

DLH
DIGITAL
LEARNING
HUB

First session:
Tuesday, June 28th 2022

Thank you

.lu
operated by **Restena**

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

2, avenue de l'Université
L-4365 Esch-sur-Alzette
LUXEMBOURG

+352 42 44 09-1
admin@dns.lu

dns.lu