Post Quantum Cryptography in the DNS

Elmer Lastdrager | Lecture Radboud University

10 December 2025

SIDN LABS

SIDN

… is the registry and operator of the Netherlands’ **.nl** country-code top-level domain (ccTLD).

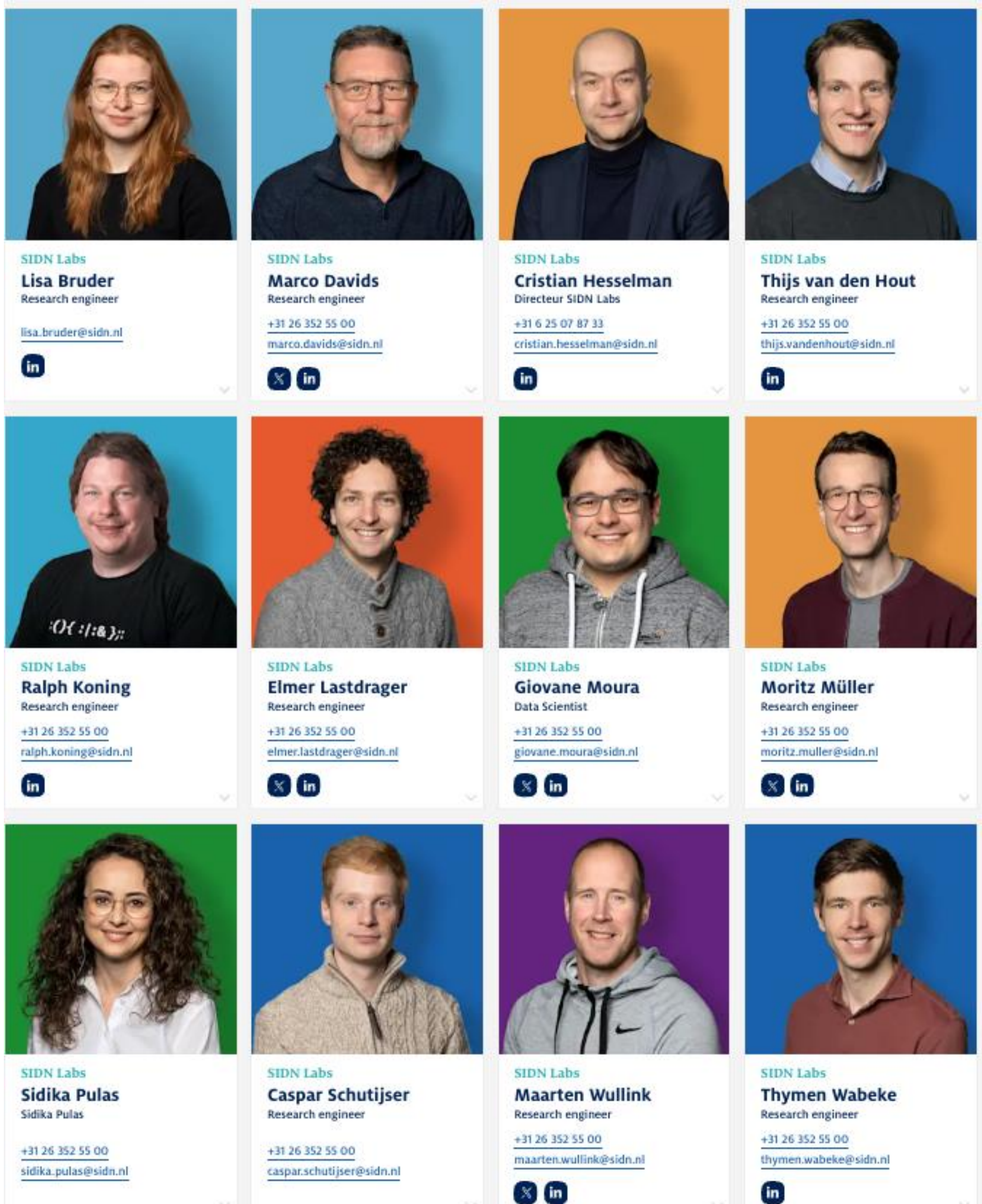
… is a not-for-profit private organization with a public role based in **Arnhem**, the Netherlands.

… aims to increase society’s confidence in the Internet.

.nl = the Netherlands
18M inhabitants
6.0M domain names
3.7M DNSSEC-signed
5.3B DNS queries/day
8.6B NTP queries/day

SIDN LABS

SIDN Labs



Technical experts, divers in seniority and nationality

Help SIDN teams, write open-source software, analyze large amounts of data, conduct experiments, write articles, collaborate with universities

M.Sc students help us advance specific areas

Post Quantum Cryptography in the DNS

SIDN LABS

DNS

The Domain Name System translates human-friendly domain names into IP addresses, forming the backbone of internet navigation.

DNSSEC

Domain Name System Security Extensions add cryptographic signatures to DNS data, protecting against spoofing and ensuring data integrity.

Post-Quantum Cryptography

Advanced cryptographic algorithms designed to resist attacks from quantum computers, ensuring future-proof security for internet communications.

SIDN LABS

DNS

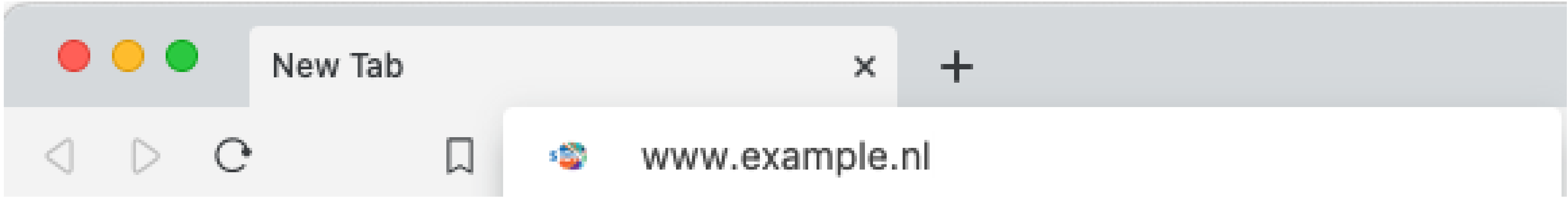
The Domain Name System translates human-friendly domain names into IP addresses, forming the backbone of internet navigation.

DNSSEC

Domain Name System Security Extensions add cryptographic signatures to DNS data, protecting against spoofing and ensuring data integrity.

Post-Quantum Cryptography

Advanced cryptographic algorithms designed to resist attacks from quantum computers, ensuring future-proof security for internet communications.



2a00:d78:0:712:94:198:159:35

rfc.fyi

dns

Show obsolete and historic

sort by:

RFC number | referencing RFCs

Stream

iab ietf independent irtf legacy

Level

bcp experimental historic informational std unknown

Working Group

6man IESG acme add appsawg asid behave bmwg cdni curdle dane dhc dns dnsext dnsind

292 RFCs

RFC9872: Recommendations for Discovering IPv6 Prefix Used for IPv6 Address Synthesis informational v6ops

RFC9859: Generalized DNS Notifications dnsop

RFC9824: Compact Denial of Existence in DNSSEC dnsop

RFC9803: Extensible Provisioning Protocol (EPP) Mapping for DNS Time-to-Live (TTL) Values regext

RFC9799: Automated Certificate Management Environment (ACME) Extensions for ".onion" Special-Use Domain Names acme

RFC9726: Operational Considerations for Use of DNS in Internet of Things (IoT) Devices bcp opsawg

RFC9718: DNSSEC Trust Anchor Publication for the Root Zone informational dnsop

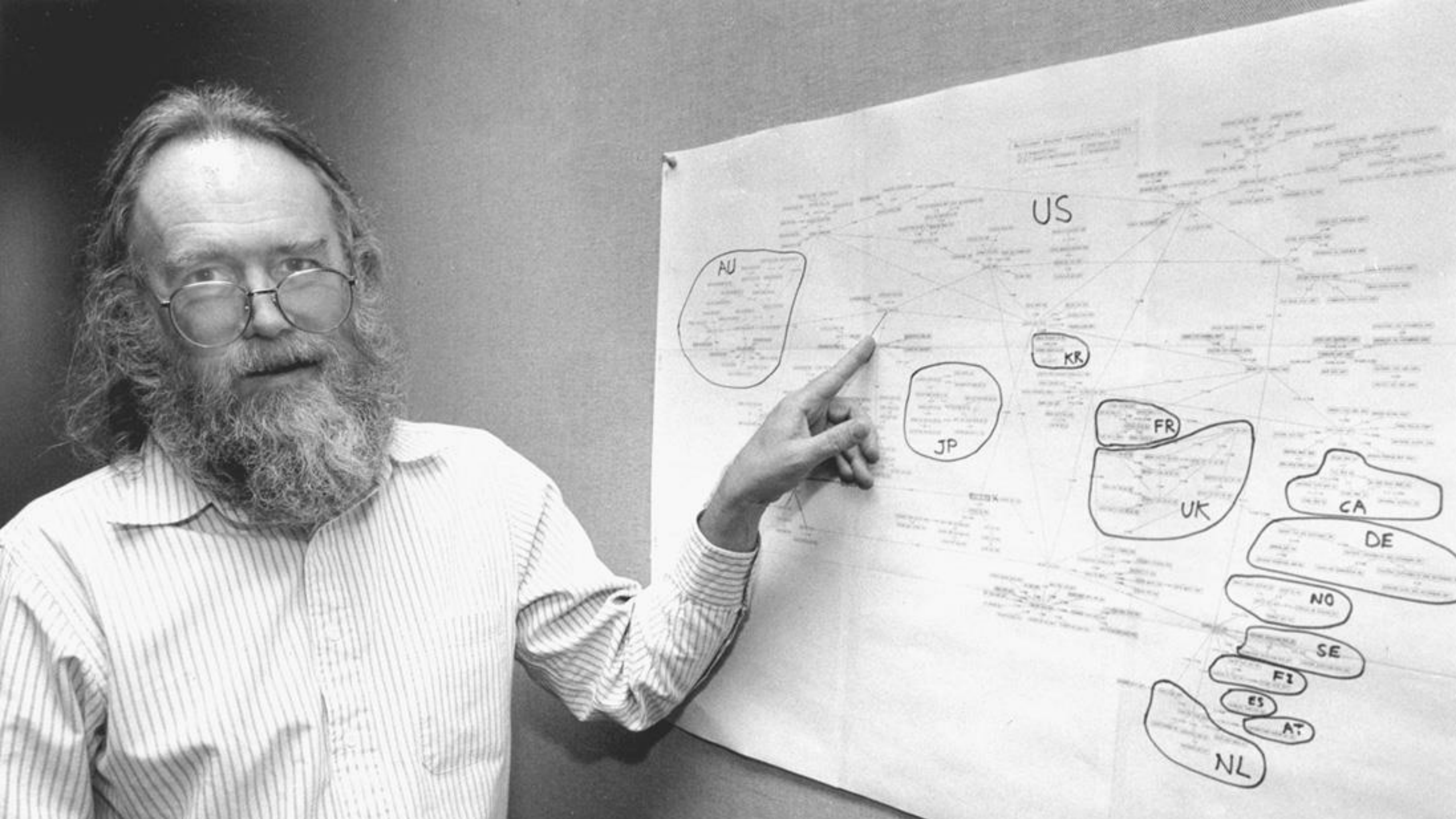
RFC9715: IP Fragmentation Avoidance in DNS over UDP informational dnsop

RFC9704: Establishing Local DNS Authority in Validated Split-Horizon Environments add

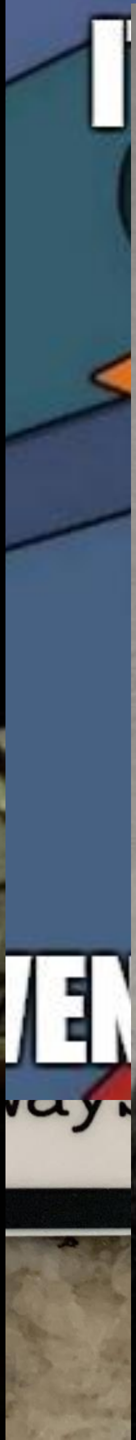
RFC9665: Service Registration Protocol for DNS-Based Service Discovery dnssd

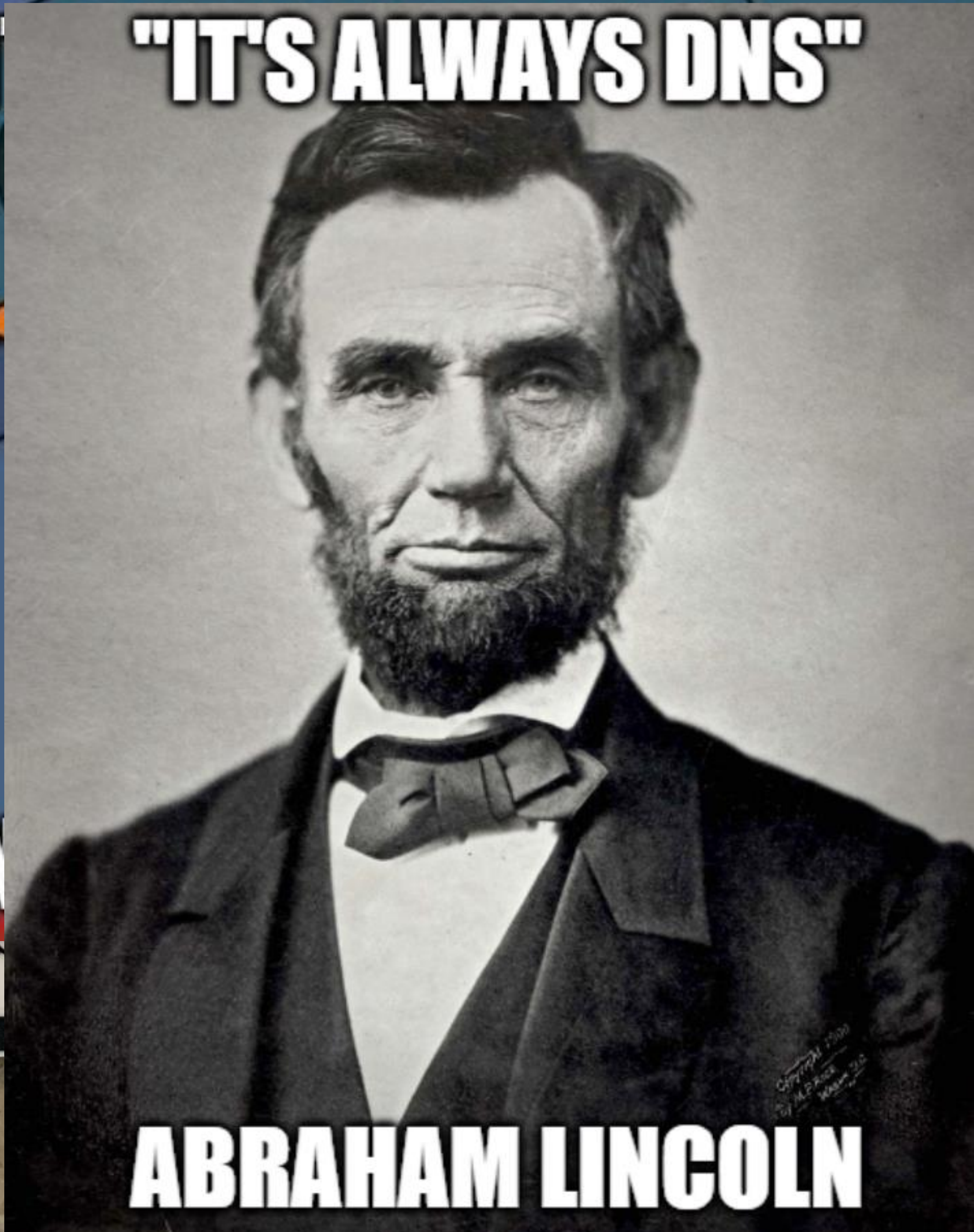
RFC9664: An EDNS(0) Option to Negotiate Leases on DNS Updates dnssd

RFC9660: The DNS Zone Version (ZONEVERSION) Option dnsop


US
AU
KR
JP
FR
UK
CA
DE
NO
SE
FI
ES
AT
NL


Why is it when something happens, it's always you three?
DNS
BGP
DHCP




"IT'S ALWAYS DNS"
ABRAHAM LINCOLN

aws.amazon.com

English Contact us AWS Marketplace Support My account

re:Invent Discover AWS Products More Search Sign in to console Create account

Summary of the Amazon DynamoDB Service Disruption in the Northern Virginia (US-EAST-1) Region

We wanted to provide you with some additional information about the service disruption that occurred in the N. Virginia (us-east-1) Region on October 19 and 20, 2025. While the event started at 11:48 PM PDT on October 19 and ended at 2:20 PM PDT on October 20, there were three distinct periods of impact to customer applications. First, between 11:48 PM on October 19 and 2:40 AM on October 20, Amazon DynamoDB experienced increased API error rates in the N. Virginia (us-east-1) Region. Second, between 5:30 AM and 2:09 PM on October 20, Network Load Balancer (NLB) experienced increased connection errors for some load balancers in the N. Virginia (us-east-1) Region. This was caused by health check failures in the NLB fleet, which resulted in increased connection errors on some NLBs. Third, between 2:25 AM and 10:36 AM on October 20, new EC2 instance launches failed and, while instance launches began to succeed from 10:37 AM, some newly launched instances experienced connectivity issues which were resolved by 1:50 PM.

DynamoDB

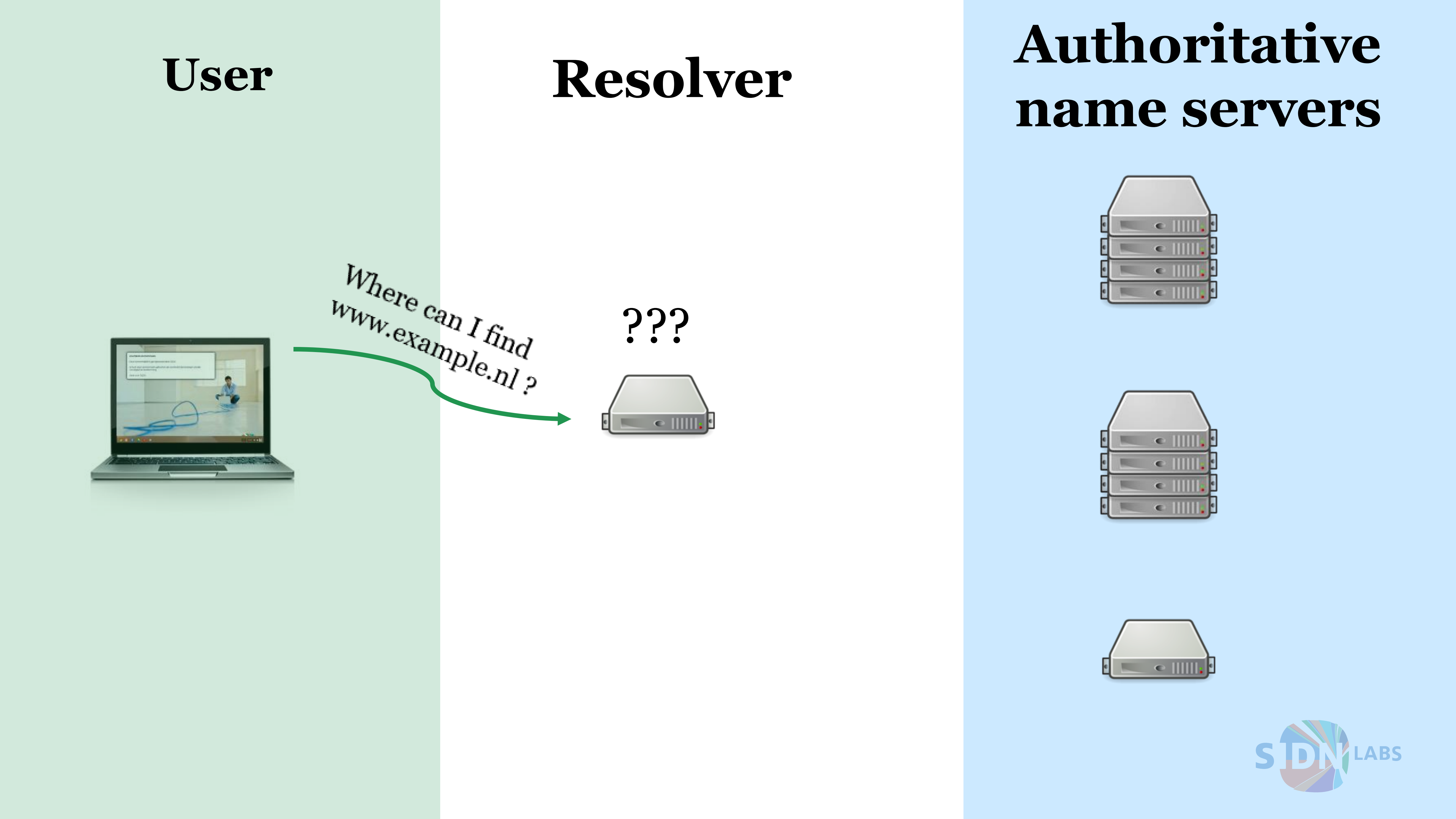
Between 11:48 PM PDT on October 19 and 2:40 AM PDT on October 20, customers experienced increased Amazon DynamoDB API error
N. Virginia (us-east-1) Region. During this period, customers and other AWS services with dependencies on DynamoDB were unable to e
connections to the service. The incident was triggered by a latent defect within the service's automated DNS management system that
endpoint resolution failures for DynamoDB.

Many of the largest AWS services rely extensively on DNS to provide seamless scale, fault isolation and recovery, low latency, and locality. Services like DynamoDB maintain hundreds of thousands of DNS records to operate a very large heterogeneous fleet of load balancers in each Region. Automation is crucial to ensuring that these DNS records are updated frequently to add additional capacity as it becomes available, to correctly handle hardware failures, and to efficiently distribute traffic to optimize customers' experience. This automation has been designed for resilience, allowing the service to recover from a wide variety of operational issues. In addition to providing a public regional endpoint, this automation maintains additional DNS endpoints for several dynamic DynamoDB variants including a FIPS compliant endpoint, an IPv6 endpoint, and account-specific endpoints. The root cause of this issue was a latent race condition in the DynamoDB DNS management system that resulted in an incorrect empty DNS record for the service's regional endpoint (**dynamodb.us-east-1.amazonaws.com**) that the automation failed to repair. To explain this event, we need to share some details about the DynamoDB DNS management architecture. The system is split across two independent components for availability reasons. The first component, the DNS Planner, monitors the health and capacity of the load balancers and periodically creates a new DNS plan for each of the service's endpoints consisting of a set of load balancers and weights. We produce a single regional DNS plan, as this greatly simplifies capacity management and failure mitigation when capacity is shared across multiple endpoints, as is the case with the recently launched IPv6 endpoint and the public regional endpoint. A second component, the DNS Enactor, which is designed to have minimal dependencies to allow for system recovery in any scenario, enacts DNS plans by applying the required changes in the Amazon Route53 service. For resiliency, the DNS Enactor operates redundantly and fully independently in three different Availability Zones (AZs). Each of these independent instances of the DNS Enactor looks for new plans and attempts to update Route53 by replacing the current plan with a new plan using a Route53 transaction, assuring that each endpoint is updated with a consistent plan even when multiple DNS Enactors attempt to update it concurrently. The race condition involves an unlikely interaction between two of the DNS Enactors. Under normal operations, a DNS Enactor picks up the latest plan and begins wor[...] the service endpoints to apply this plan. This process typically completes rapidly and does an effective job of keeping DNS state freshly [...] Before it begins to apply a new plan, the DNS Enactor makes a one-time check that its plan is newer than the previously applied plan. A[...] Enactor makes its way through the list of endpoints, it is possible to encounter delays as it attempts a transaction and is blocked by another DNS Enactor updating the same endpoint. In these cases, the DNS Enactor will retry each endpoint until the plan is successfully applied to all endpoints

User

Resolver

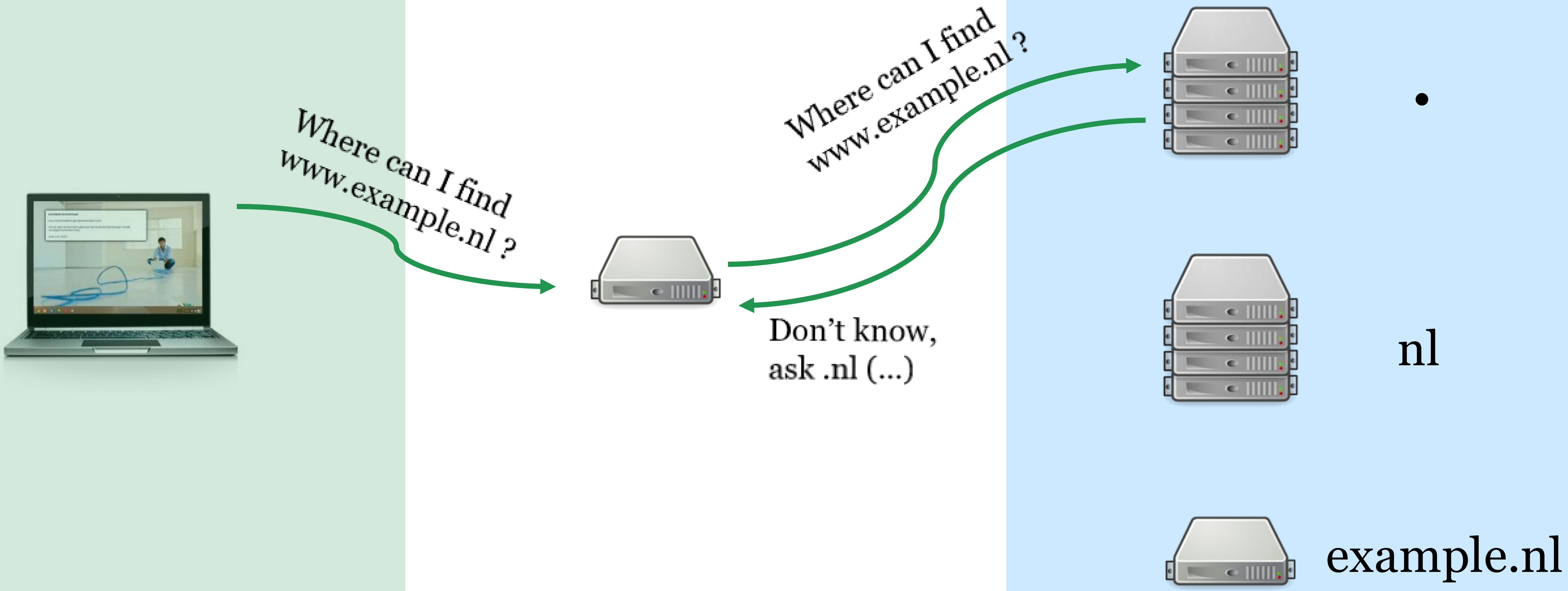
Authoritative name servers

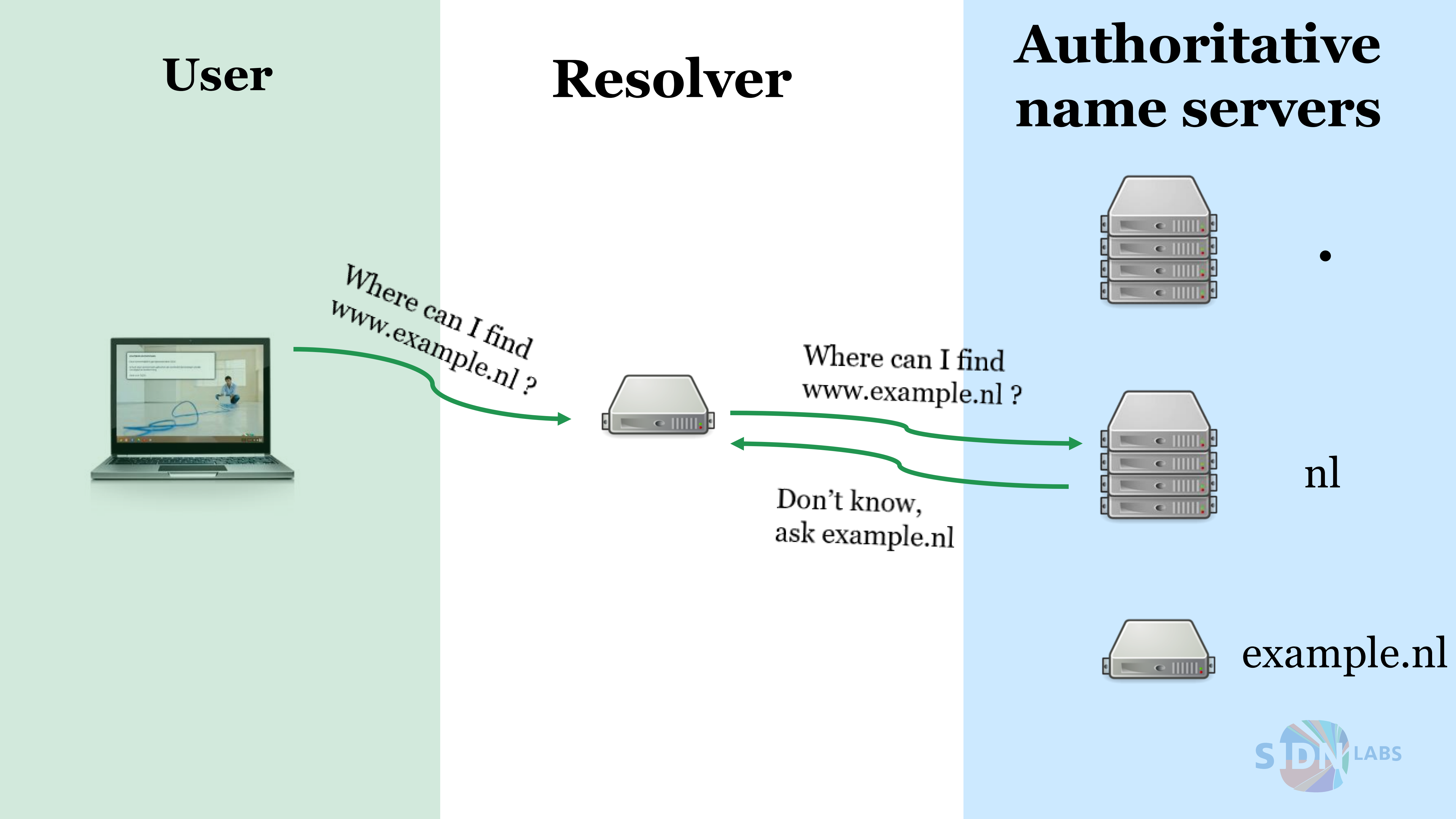

User
Resolver
Authoritative name servers
Where can I find www.example.nl ?
???
SIDN LABS

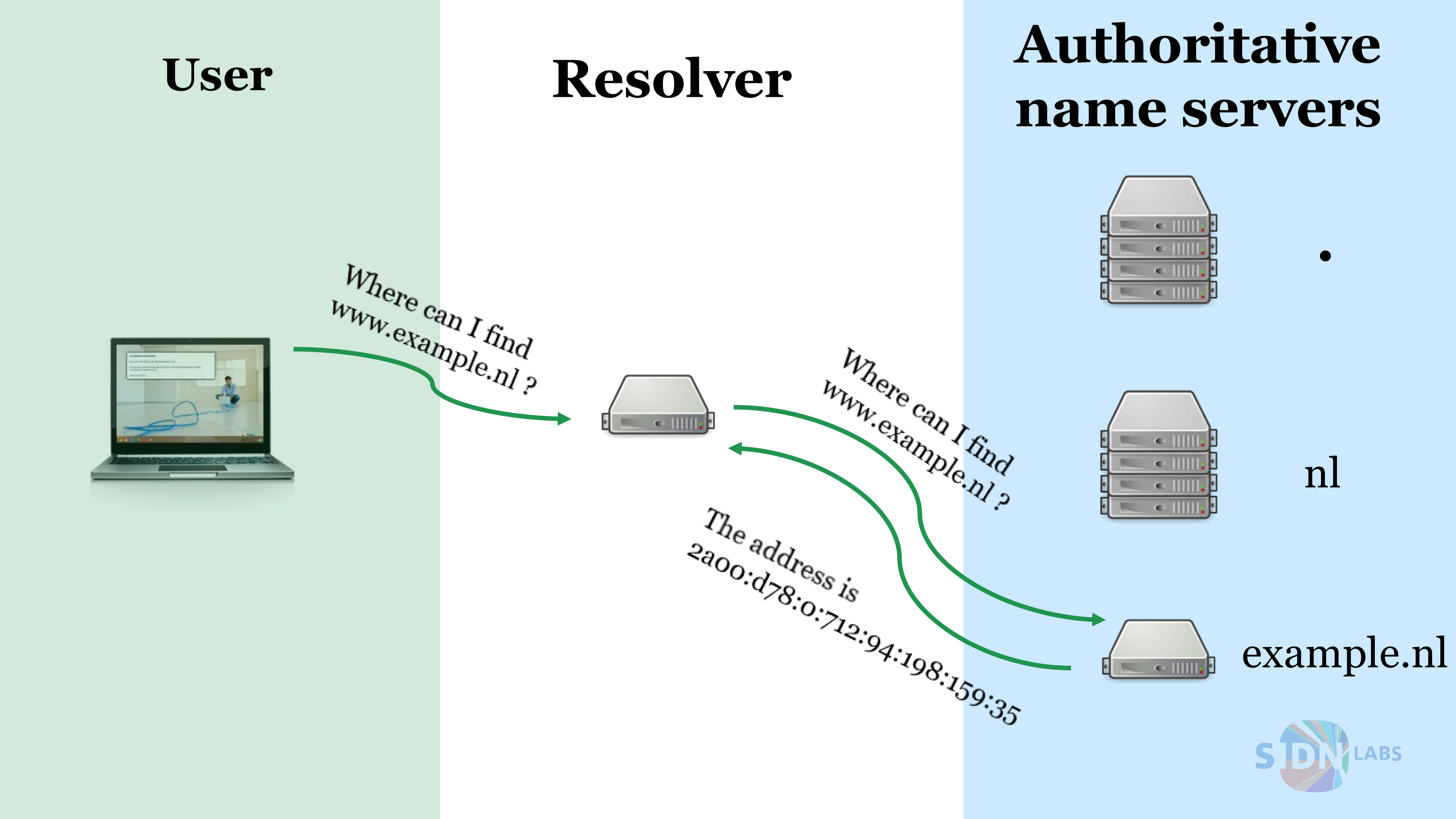
User

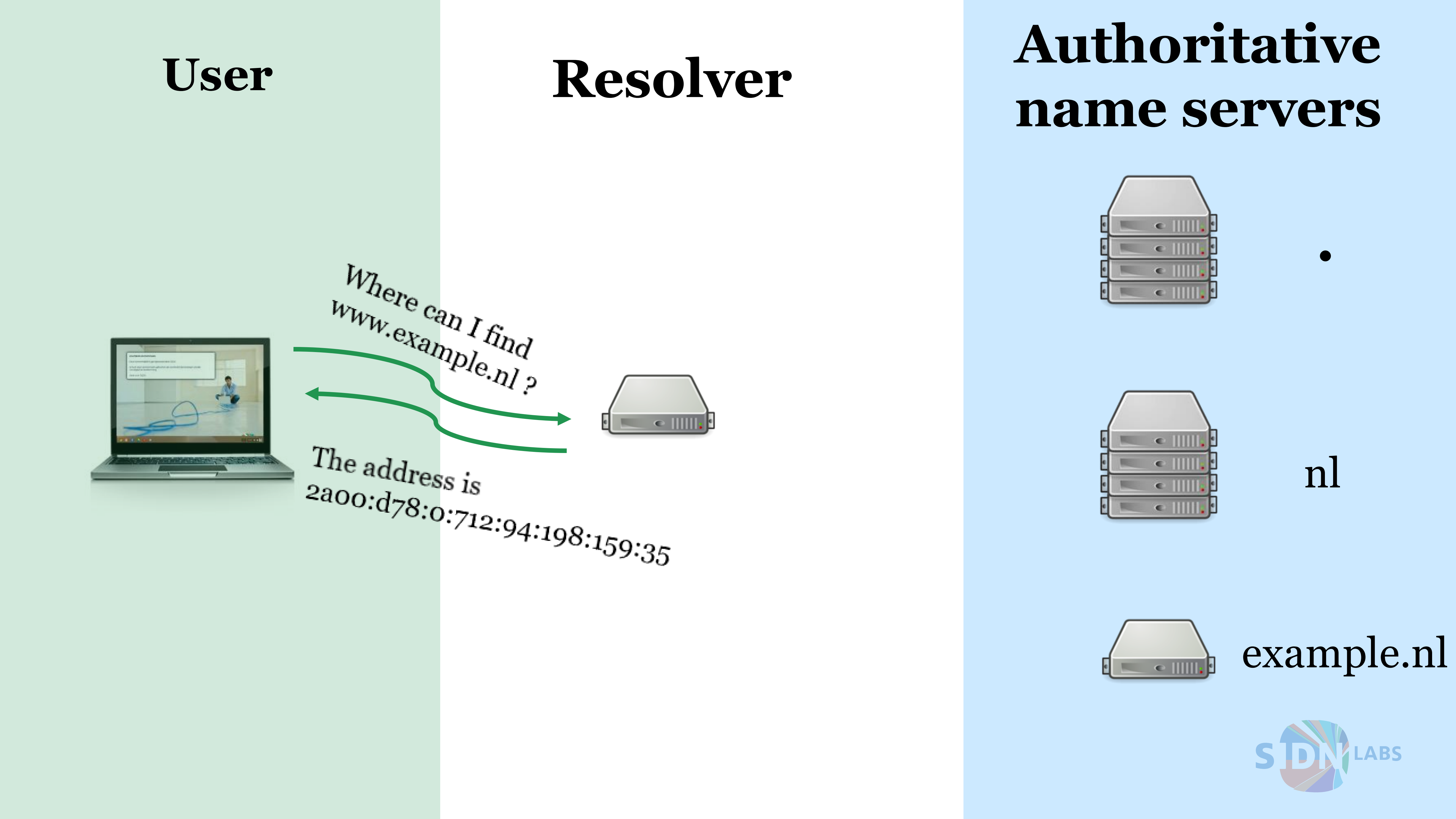
Resolver

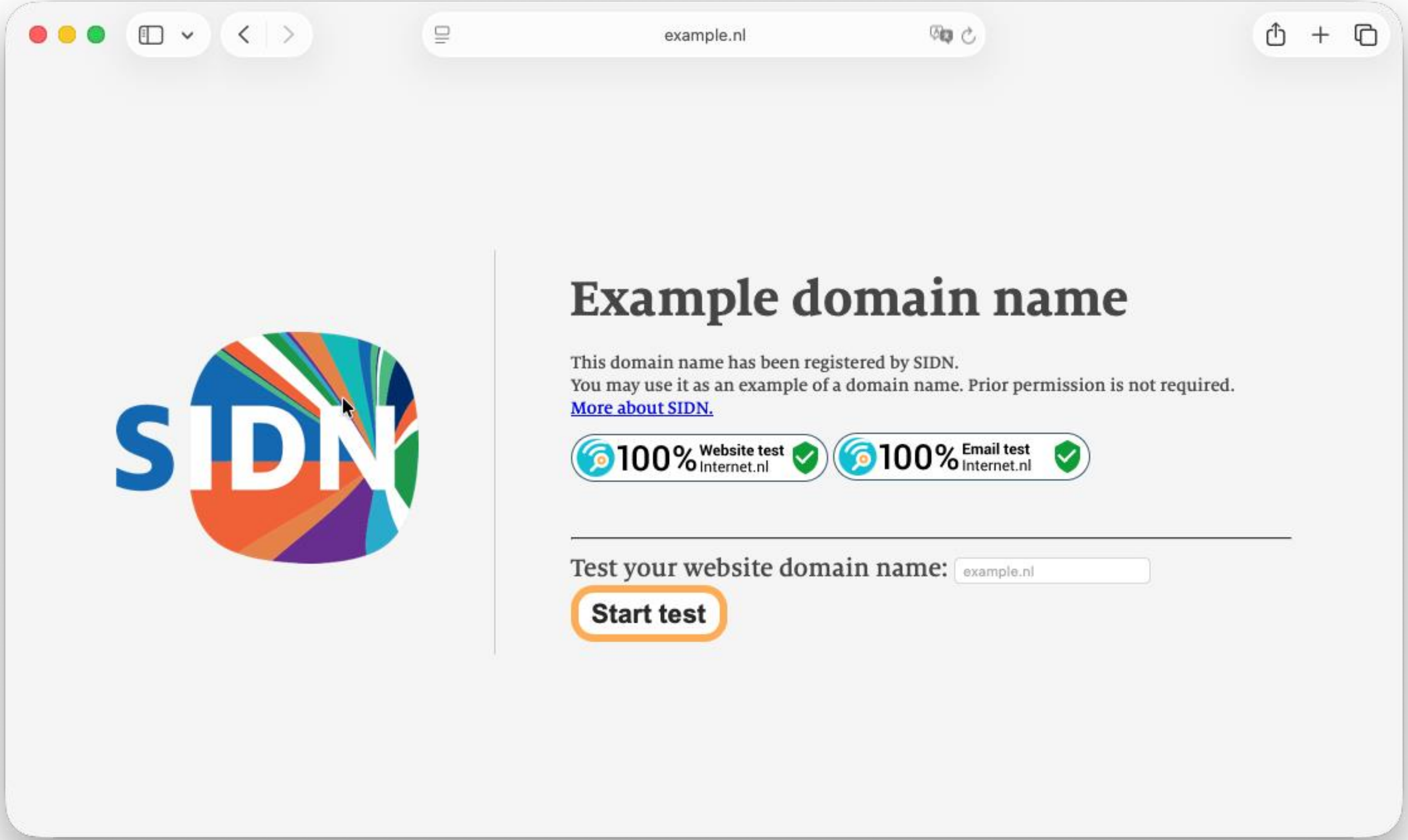
Authoritative name servers

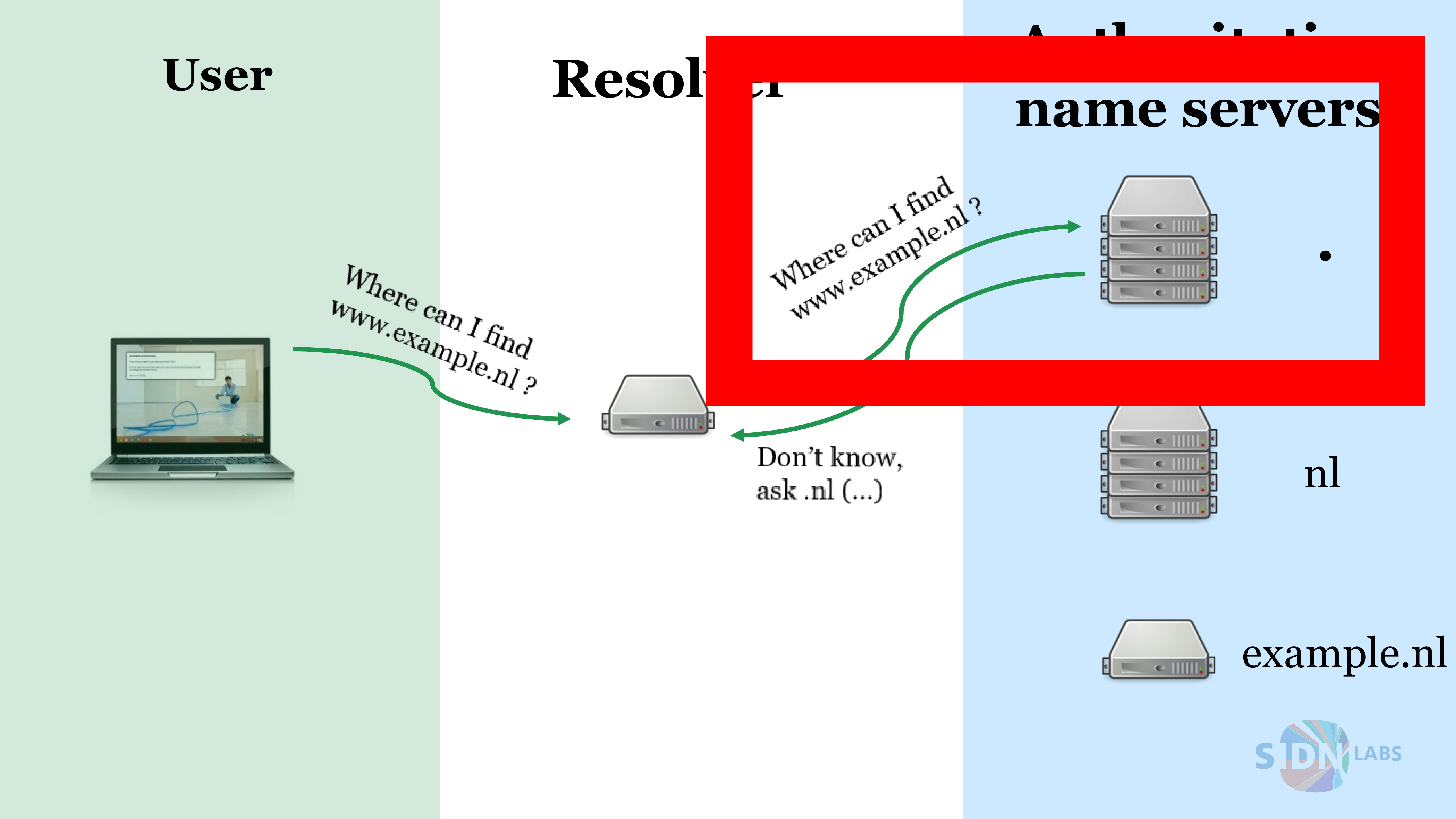



User
Resolver
Authoritative name servers
Where can I find www.example.nl ?
Where can I find www.example.nl ?
Don’t know, ask example.nl
.
nl
example.nl
SIDN LABS


User
Resolver
Authoritative name servers
Where can I find www.example.nl ?
Where can I find www.example.nl ?
The address is 2a00:d78:0:712:94:198:159:35
.
nl
example.nl


User
Resolver
Authoritative name servers
Where can I find www.example.nl ?
The address is 2a00:d78:0:712:94:198:159:35
.
nl
example.nl
SIDN LABS


example.nl
Example domain name
This domain name has been registered by SIDN.
You may use it as an example of a domain name. Prior permission is not required.
More about SIDN.
100% Website test Internet.nl
100% Email test Internet.nl
Test your website domain name:
example.nl
Start test

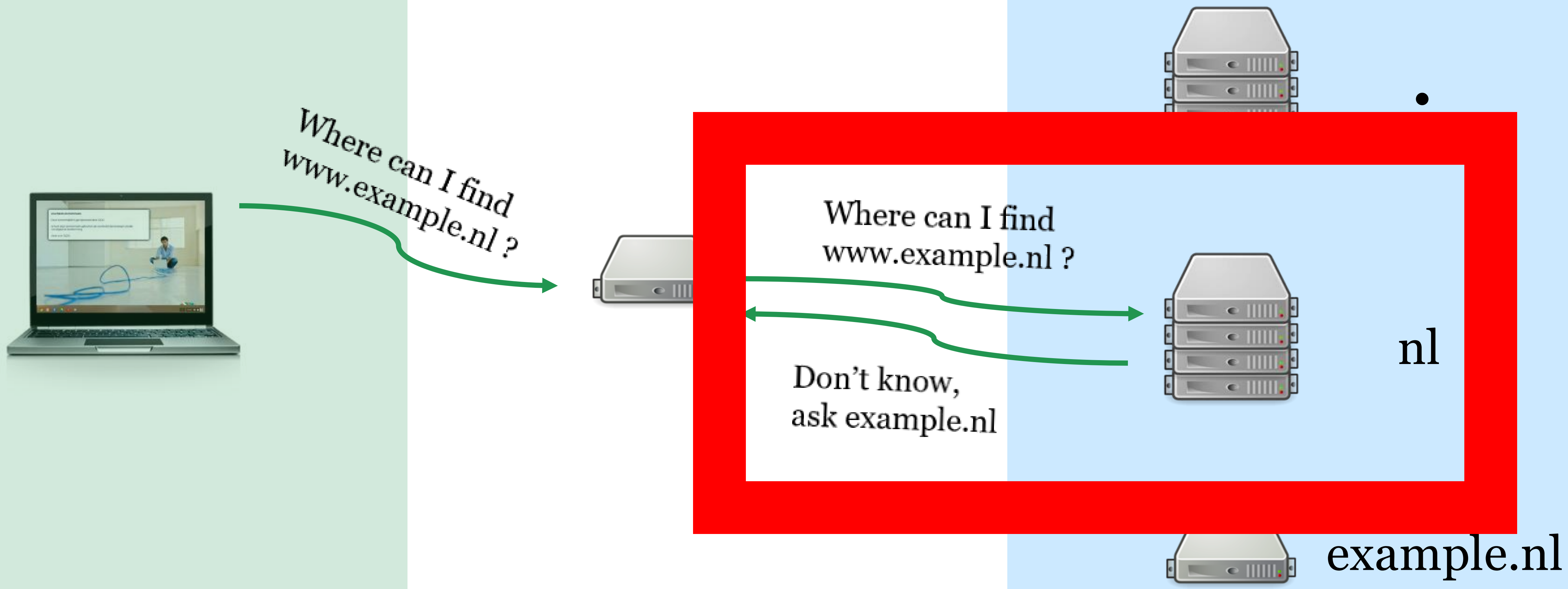


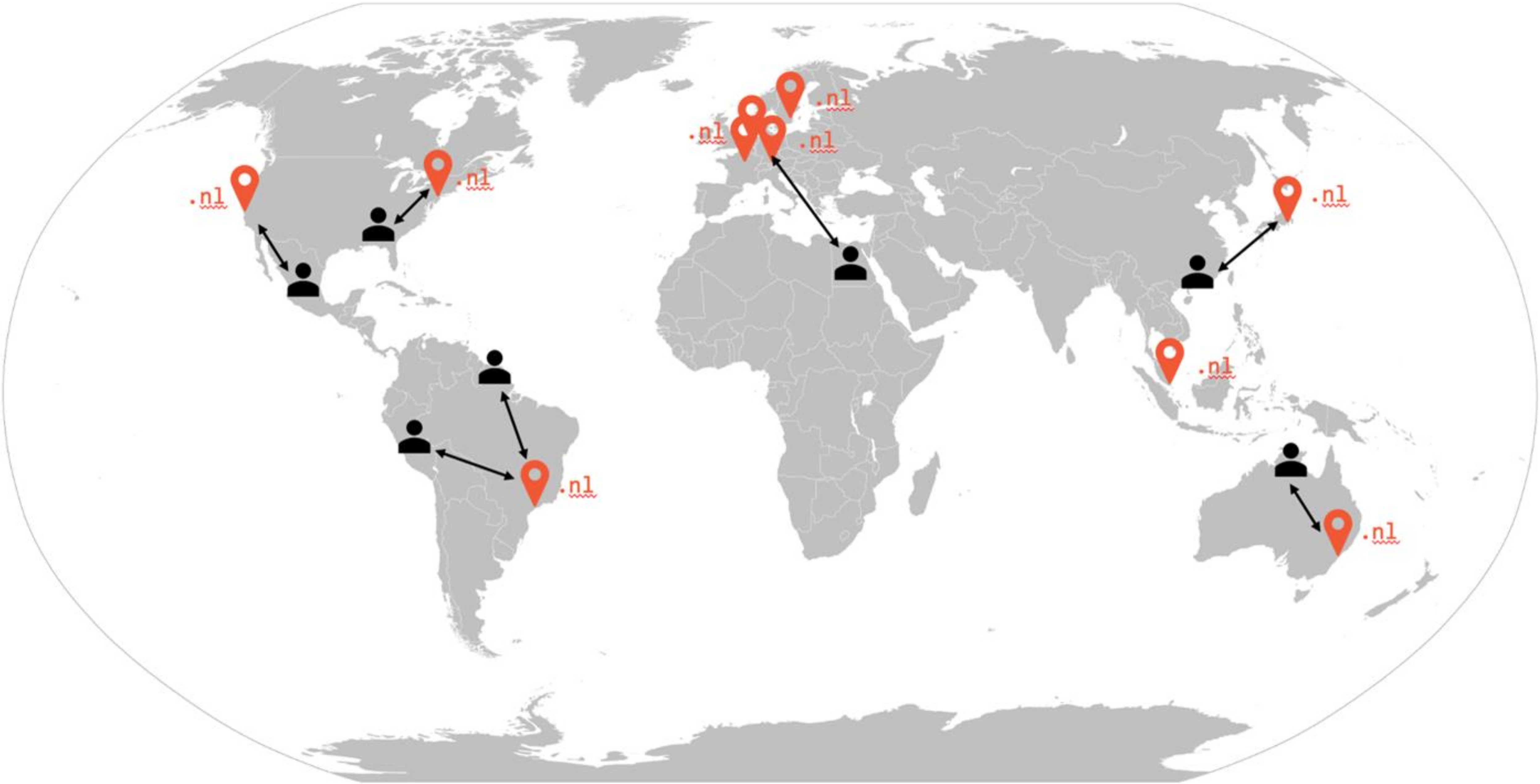
User
Resol
name servers
Where can I find
www.example.nl ?
Where can I find
www.example.nl ?
.
Don't know,
ask .nl (...)
nl
example.nl

User

Resolver

Authoritative name servers




.nl
.nl
.nl
.nl
.nl
.nl
.nl
.nl
.nl

Command line example (1)

We ask for AAAA record

```
$ dig +nodnssec www.example.nl AAAA
@k.root-servers.net

;; AUTHORITY SECTION:

nl. 172800 IN NS ns1.dns.nl.

nl. 172800 IN NS ns3.dns.nl.

nl. 172800 IN NS ns4.dns.nl.
```

Results are NS records

TTL

```
DITIONAL SECTION:

ns1.dns.nl. 172800 IN A 194.0.28.53

ns1.dns.nl. 172800 IN AAAA
2001:678:2c:0:194:0:28:53

ns3.dns.nl. 172800 IN A 194.0.2
```

Glue records

```
ns3.dns.nl. 172800 IN AAAA
2001:678:20::24

ns4.dns.nl. 172800 IN A
185.159.199.200

ns4.dns.nl. 172800 IN AAAA
2620:10a:80ac::200


;; Query time: 7 msec

;; SERVER:
2001:7fd::1#53(k.root-
servers.net) (UDP)

;; WHEN: Tue Nov 11 09:49:01
CET 2025

;; MSG SIZE  rcvd: 221
```

Command line example (2)

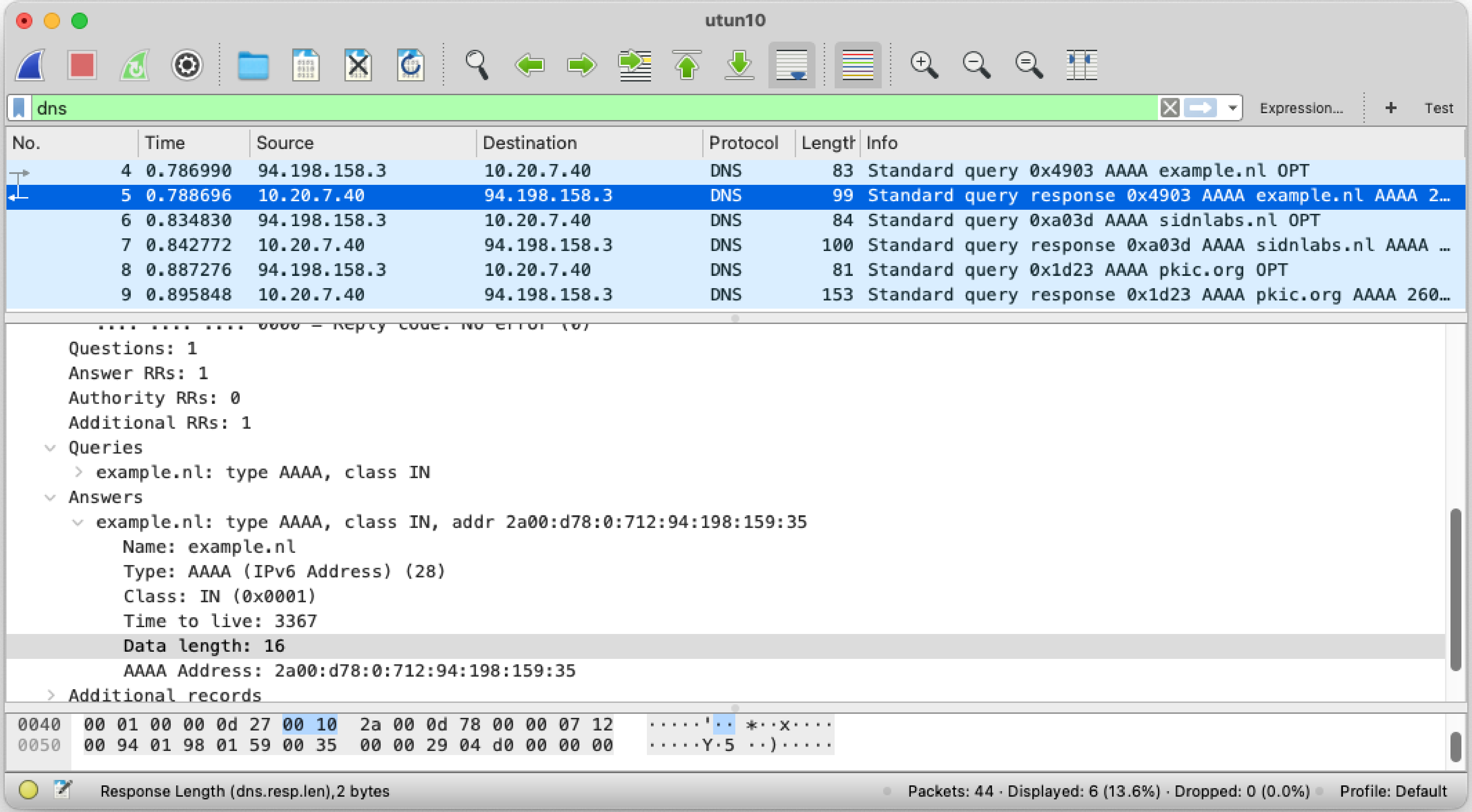
```
$ dig +nodnssec www.example.nl AAAA @ns1.dns.nl

;; AUTHORITY SECTION:
example.nl. 3600 IN NS ex1.sidnlabs.nl.
example.nl. 3600 IN NS ex2.sidnlabs.nl.
example.nl. 3600 IN NS anytest1.sidnlabs.nl.

;; Query time: 31 msec
;; SERVER: 2001:678:2c:0:194:0:28:53#53(ns1.dns.nl) (UDP)
;; WHEN: Tue Nov 11 09:53:26 CET 2025
;; MSG SIZE  rcvd: 111
```

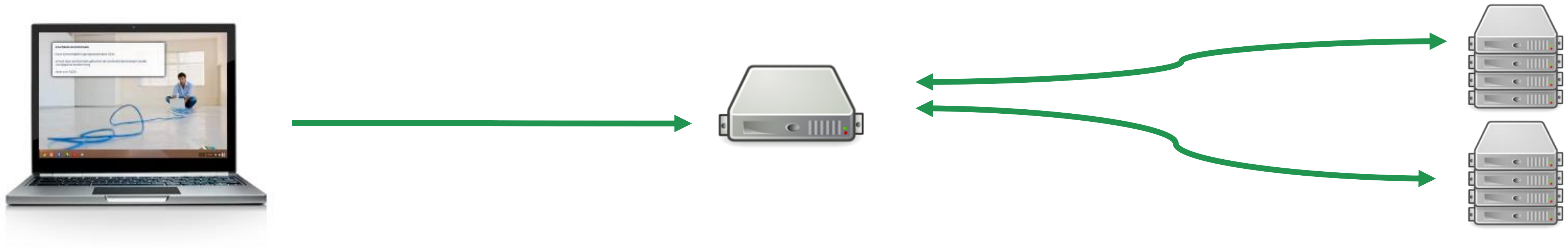
How do we know the IP address of this name server?

SIDN LABS

Command line example (3)

```
$ dig +nodnssec www.example.nl AAAA @anytest1.sidnlabs.nl

www.example.nl. 3600 IN AAAA 2a00:d78:0:712:94:198:159:35

;; Query time: 4 msec
;; SERVER: 2001:678:8::53#53(anytest1.sidnlabs.nl.) (UDP)
;; WHEN: Tue Nov 11 10:49:39 CET 2025
;; MSG SIZE  rcvd: 99
```


utun10
dns
Expression…
+
Test
No. | Time | Source | Destination | Protocol | Length | Info
4 0.786990 94.198.158.3 10.20.7.40 DNS 83 Standard query 0x4903 AAAA example.nl OPT
5 0.788696 10.20.7.40 94.198.158.3 DNS 99 Standard query response 0x4903 AAAA example.nl AAAA 2…
6 0.834830 94.198.158.3 10.20.7.40 DNS 84 Standard query 0xa03d AAAA sidnlabs.nl OPT
7 0.842772 10.20.7.40 94.198.158.3 DNS 100 Standard query response 0xa03d AAAA sidnlabs.nl AAAA …
8 0.887276 94.198.158.3 10.20.7.40 DNS 81 Standard query 0x1d23 AAAA pkic.org OPT
9 0.895848 10.20.7.40 94.198.158.3 DNS 153 Standard query response 0x1d23 AAAA pkic.org AAAA 260…
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
example.nl: type AAAA, class IN
Answers
example.nl: type AAAA, class IN, addr 2a00:d78:0:712:94:198:159:35
Name: example.nl
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 3367
Data length: 16
AAAA Address: 2a00:d78:0:712:94:198:159:35
Additional records
0040 00 01 00 00 0d 27 00 10 2a 00 0d 78 00 00 07 12
0050 00 94 01 98 01 59 00 35 00 00 29 04 d0 00 00 00
Response Length (dns.resp.len),2 bytes
Packets: 44 · Displayed: 6 (13.6%) · Dropped: 0 (0.0%)
Profile: Default



User

Resolver

Name servers

DoH, DoT, DoQ, DNScrypt

DNSSEC

DNS

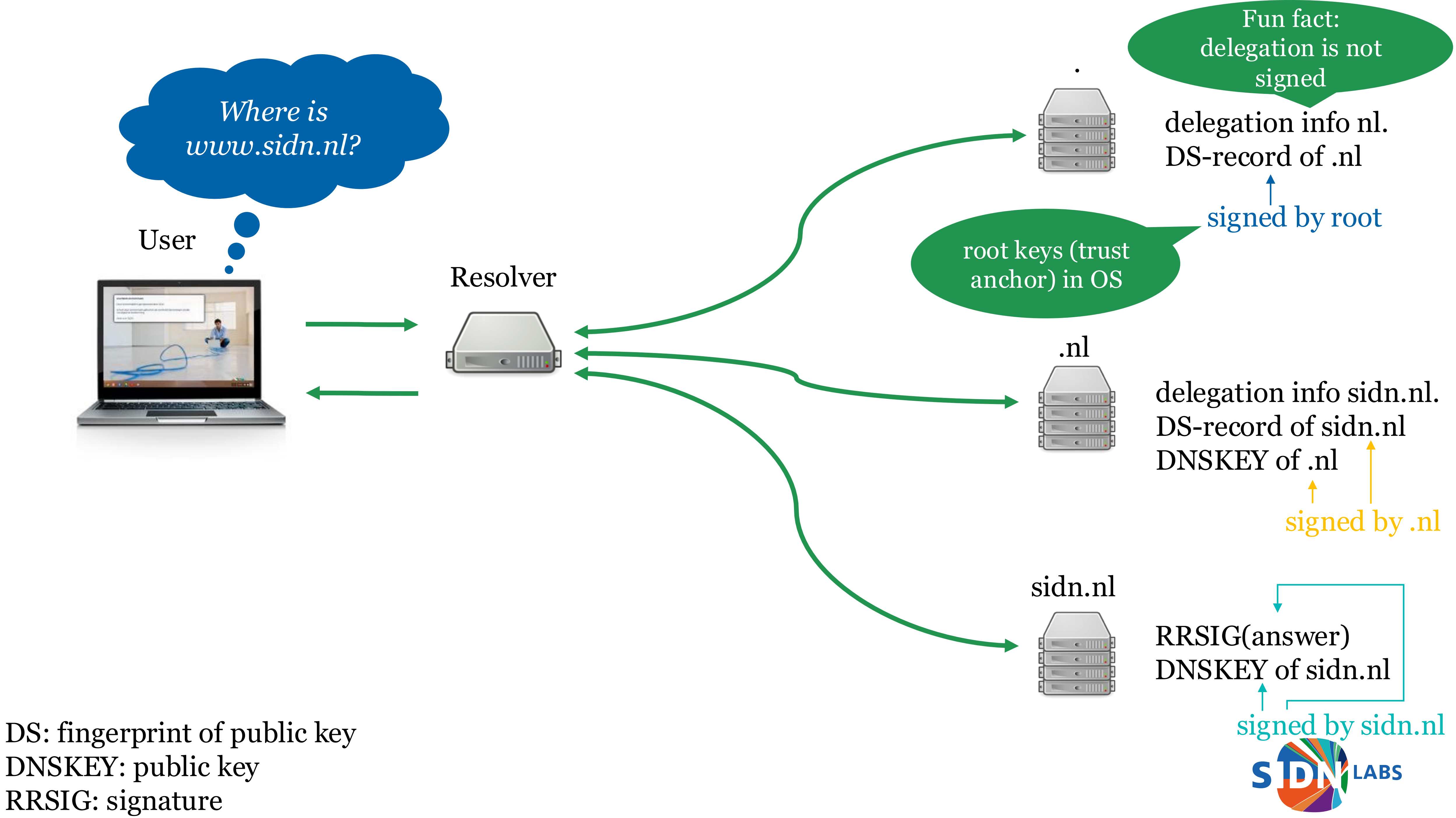
The Domain Name System translates human-friendly domain names into IP addresses, forming the backbone of internet navigation.

DNSSEC

Domain Name System Security Extensions add cryptographic signatures to DNS data, protecting against spoofing and ensuring data integrity.

Post-Quantum Cryptography

Advanced cryptographic algorithms designed to resist attacks from quantum computers, ensuring future-proof security for internet communications.


Where is www.sidn.nl?
User
Resolver
.
Fun fact: delegation is not signed
delegation info nl.
DS-record of .nl
signed by root
root keys (trust anchor) in OS
.nl
delegation info sidn.nl.
DS-record of sidn.nl
DNSKEY of .nl
signed by .nl
sidn.nl
RRSIG(answer)
DNSKEY of sidn.nl
signed by sidn.nl
DS: fingerprint of public key
DNSKEY: public key
RRSIG: signature
SIDN LABS

Command line example DNSSEC

```
$ dig +dnssec +nocrypto nl NS @k.root-servers.net

nl. 172800 IN NS ns1.dns.nl.
nl. 172800 IN NS ns3.dns.nl.
nl. 172800 IN NS ns4.dns.nl.
nl. 86400 IN DS 17153 13 2 ([omitted] )
nl. 86400 IN RRSIG DS 8 1 86400 (
               20251124050000 20251111040000 61809 .
               [omitted] )
[.........]
```

delegation is not signed at this level

Command line example DNSSEC (2)

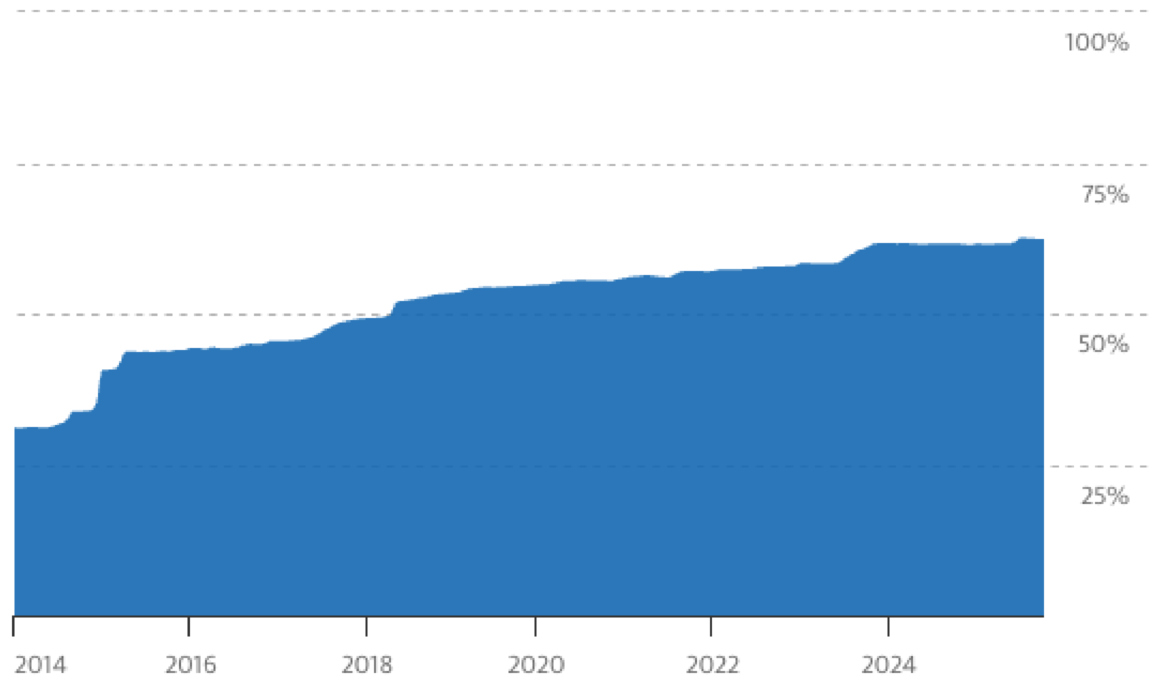
```
$ dig +dnssec +nocrypto nl NS @ns1.dns.nl
nl. 172800 IN NS ns1.dns.nl.
[...]
nl. 172800 IN RRSIG NS 13 1 172800 (20251120235718
20251106230727 12711 nl. [omitted] )

;; ADDITIONAL SECTION:
ns1.dns.nl. 3600 IN A 194.0.28.53
ns1.dns.nl. 3600 IN RRSIG A 13 3 3600 (20251120083310
20251106050725 12711 nl. [omitted] )
```

delegation is signed here

also records are signed

DNSSEC for .nl

Domain names with DNSSEC



~62%

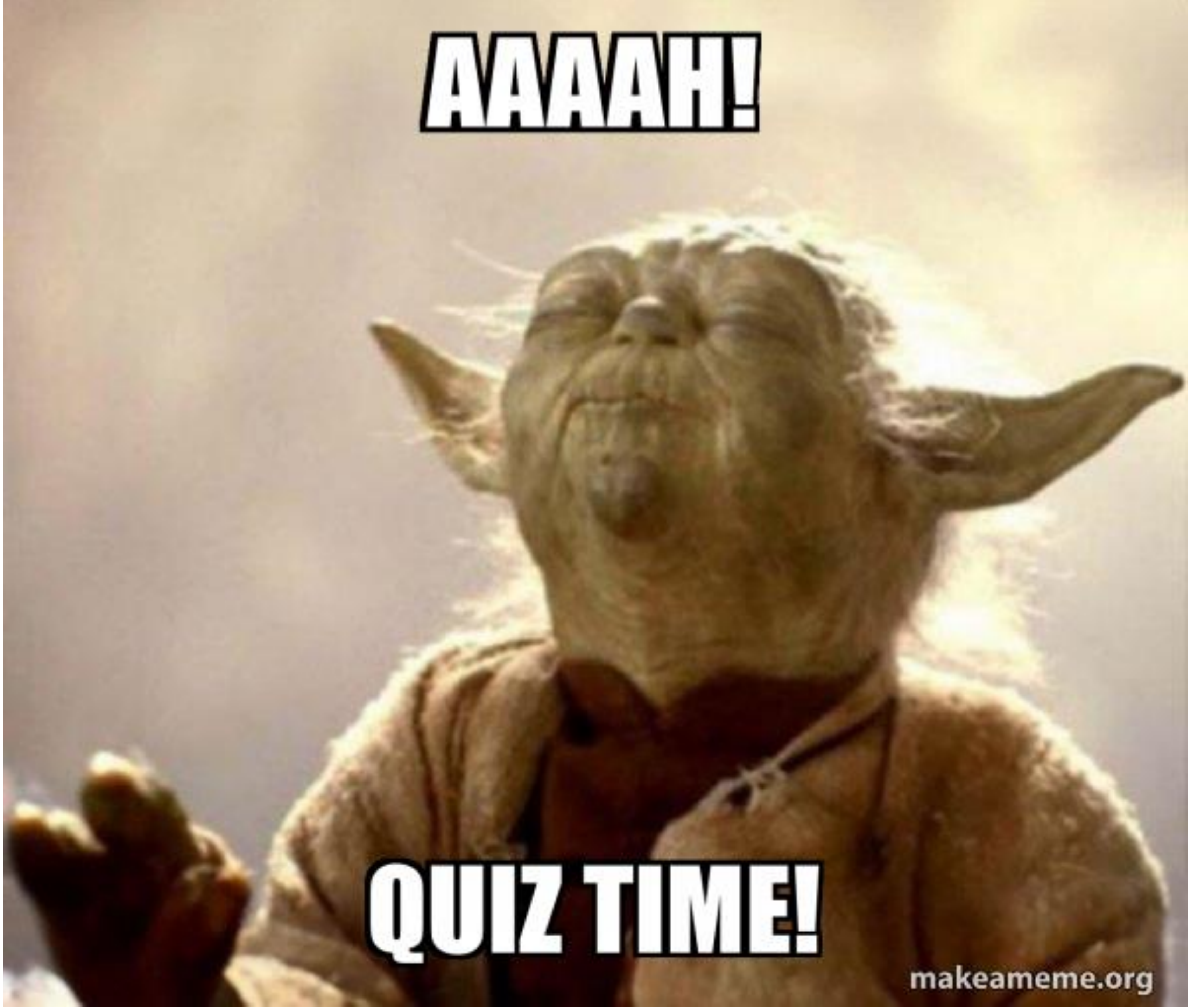
Queries from validating resolvers

~60%

Source: https://stats.sidnlabs.nl/en

Jürgen Henn – 11foot8.com


gifbin.com


AAAAH!
QUIZ TIME!
makeameme.org

DNS

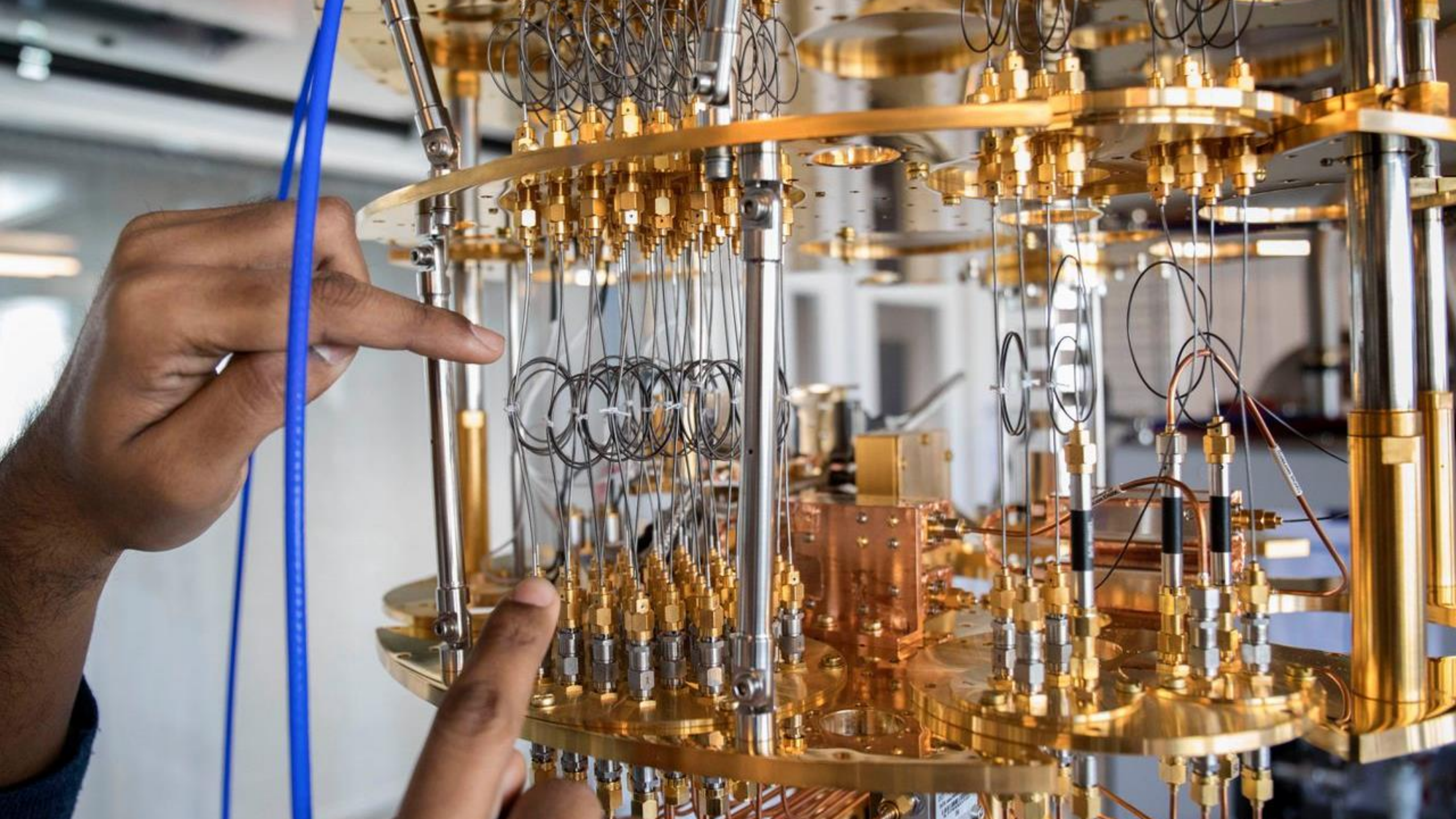
The Domain Name System translates human-friendly domain names into IP addresses, forming the backbone of internet navigation.

DNSSEC

Domain Name System Security Extensions add cryptographic signatures to DNS data, protecting against spoofing and ensuring data integrity.

Post-Quantum Cryptography

Advanced cryptographic algorithms designed to resist attacks from quantum computers, ensuring future-proof security for internet communications.



Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

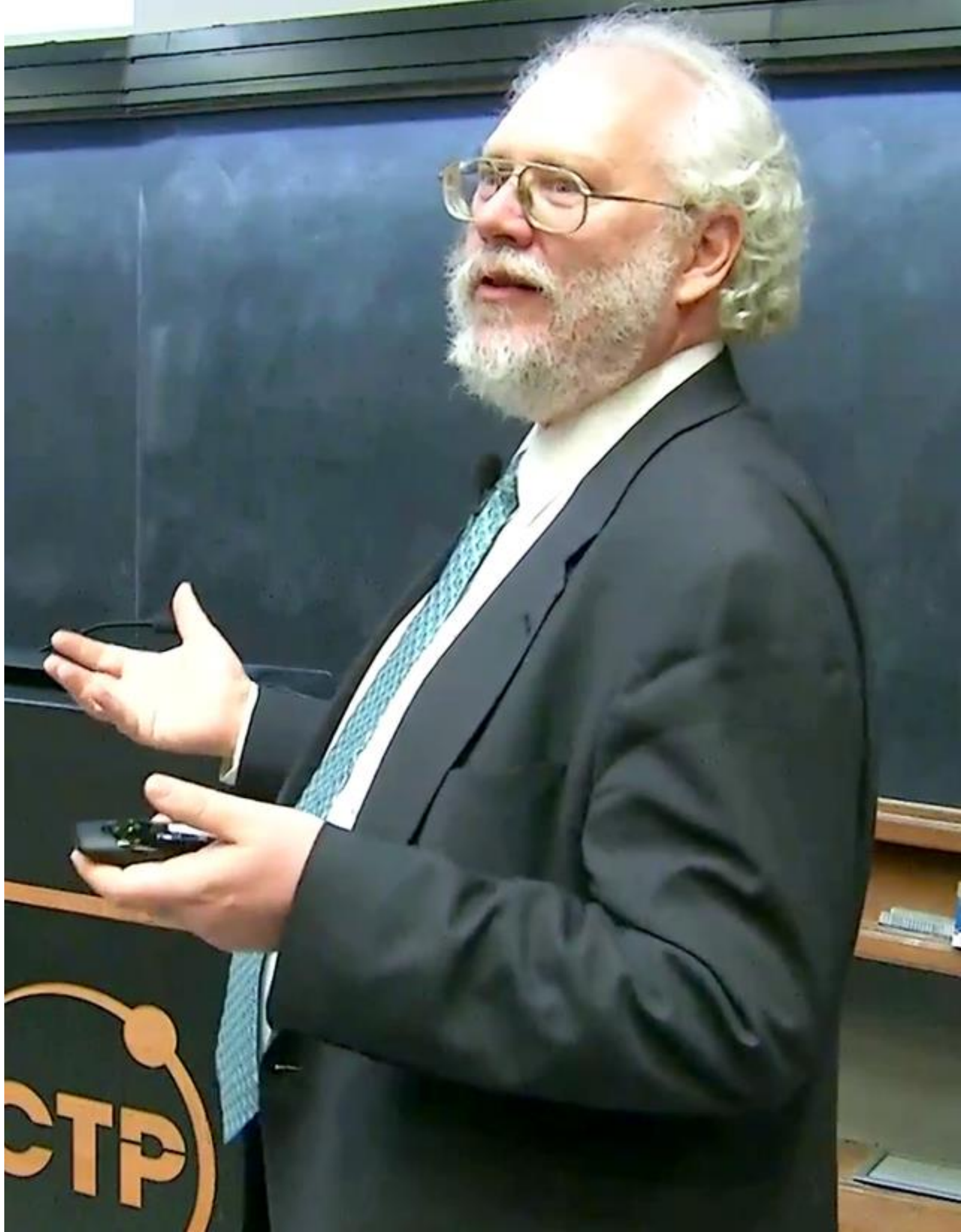
Peter W. Shor†

Abstract

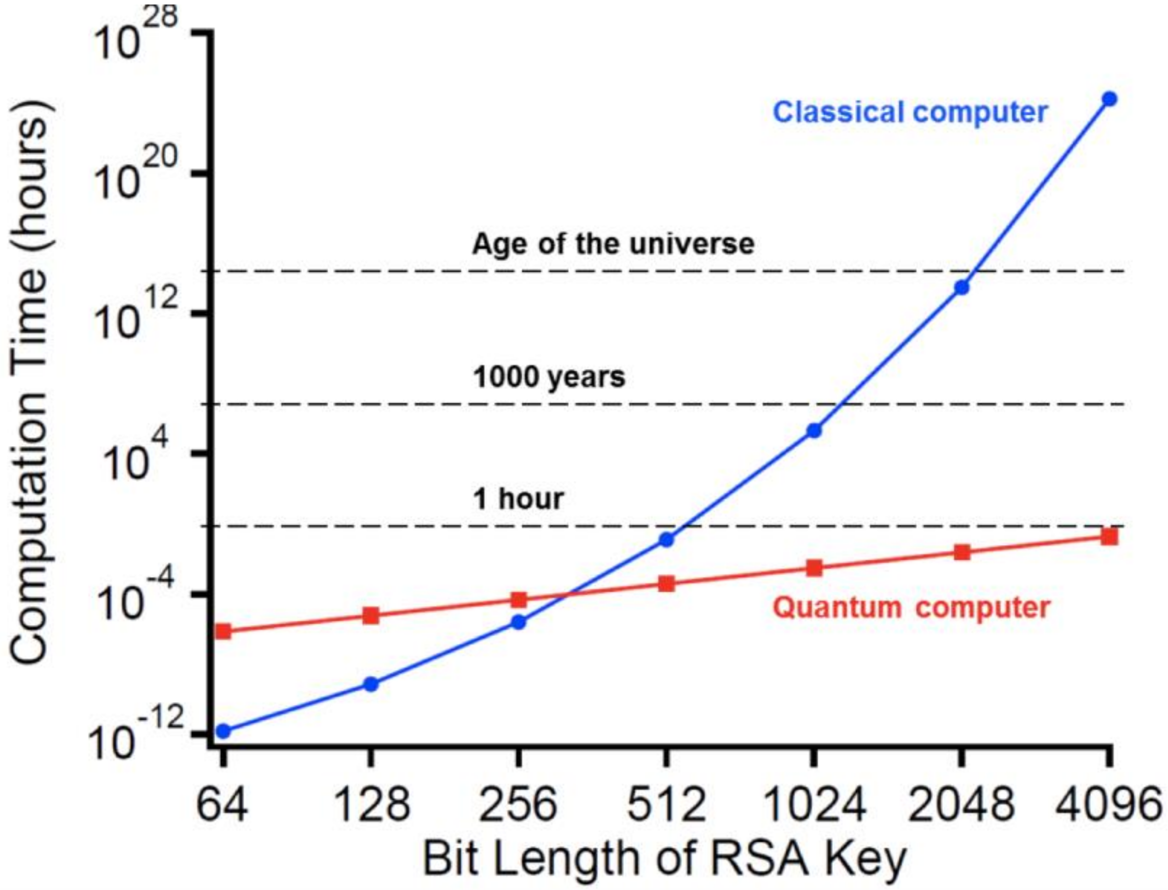
A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

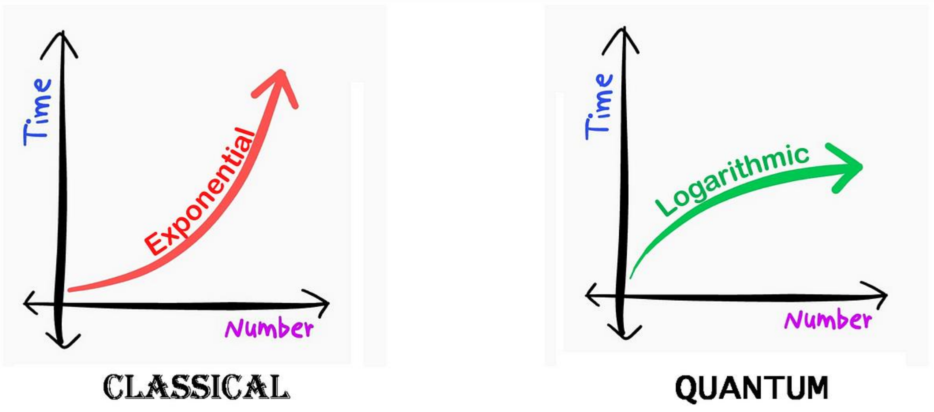
Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

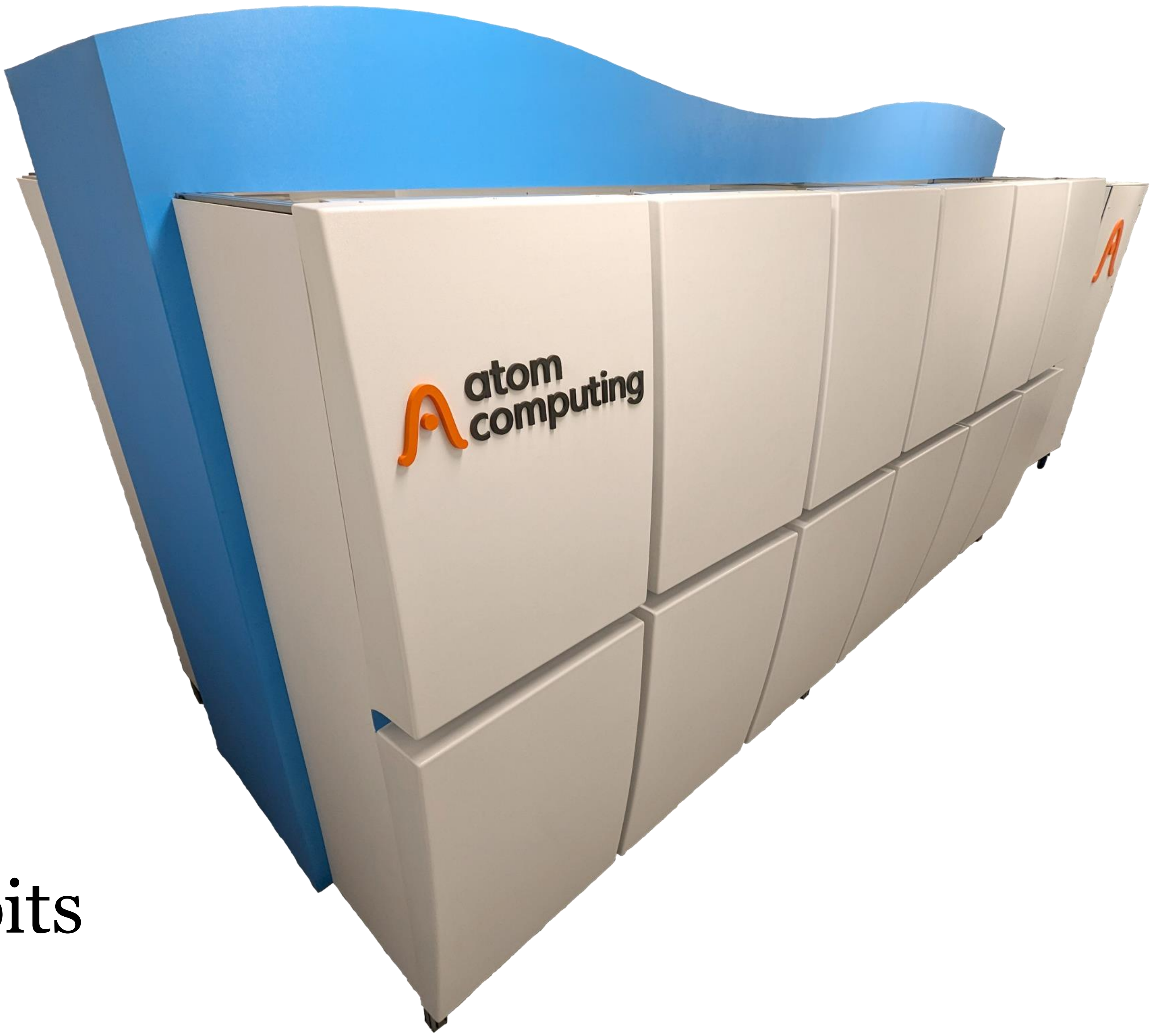
AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10



Quantum computers and cryptographic keys







1180 qubits

SDN LABS

Algorithm	Key size	Security	Logical qubits	Physical qubits	Time to break
RSA	1024 bits	80 bits	2.290	~ 2.560.000 bits	3.5 uur
RSA	**2048 bits**	**112 bits**	**4.338**	**~ 6.200.000 bits**	**29 uur**
RSA	4096 bits	128 bits	8.434	~ 14.700.000 bits	10 dagen
ECC	256 bits	128 bits	2.330	~ 3.210.000 bits	11 uur

Source: National Academies of Sciences, Engineering, and Medicine 2018. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196. Tabel 4.1

SIDN LABS

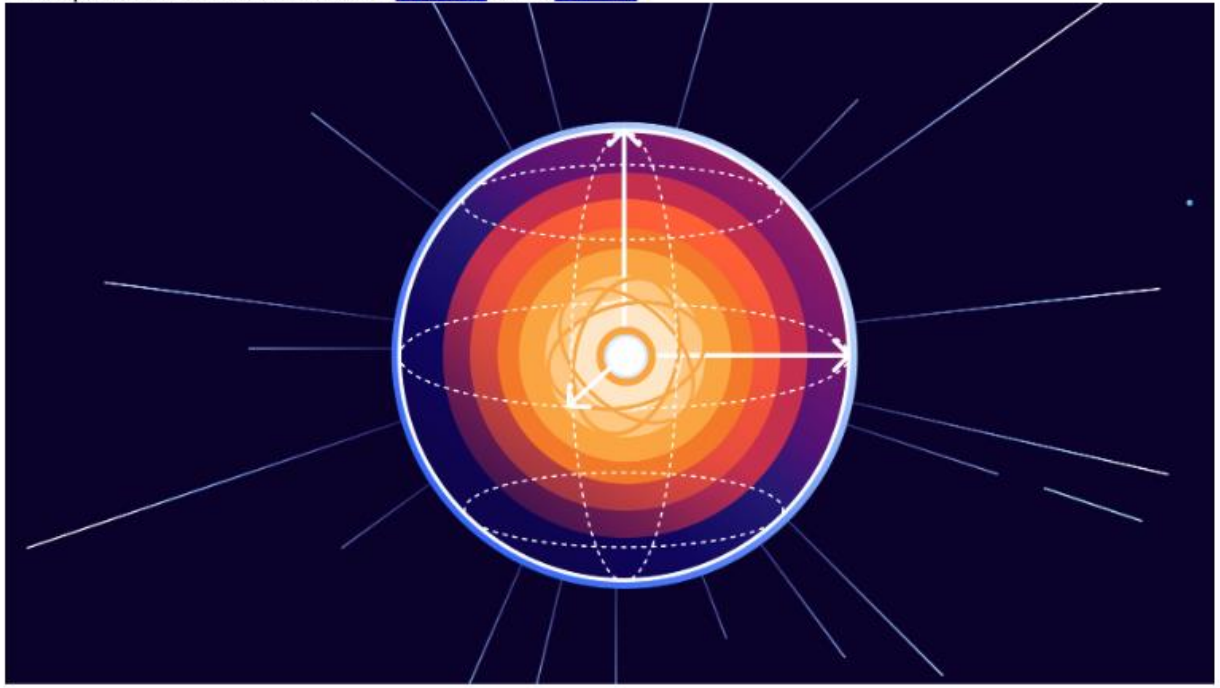
State of the post-quantum Internet in 2025

2025-10-28

Bas Westerbaan

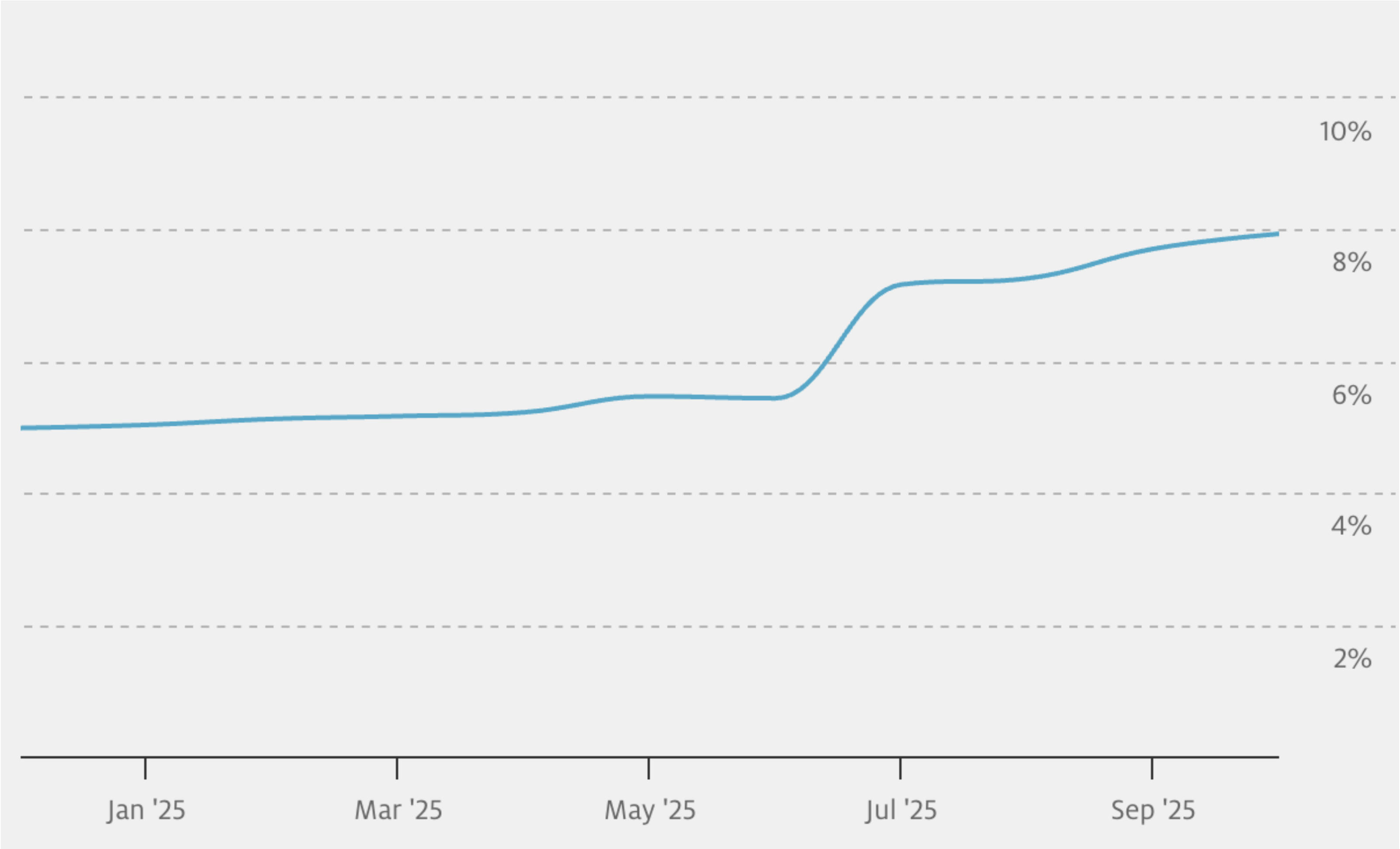
41 min read

This post is also available in 日本語 and 한국어.



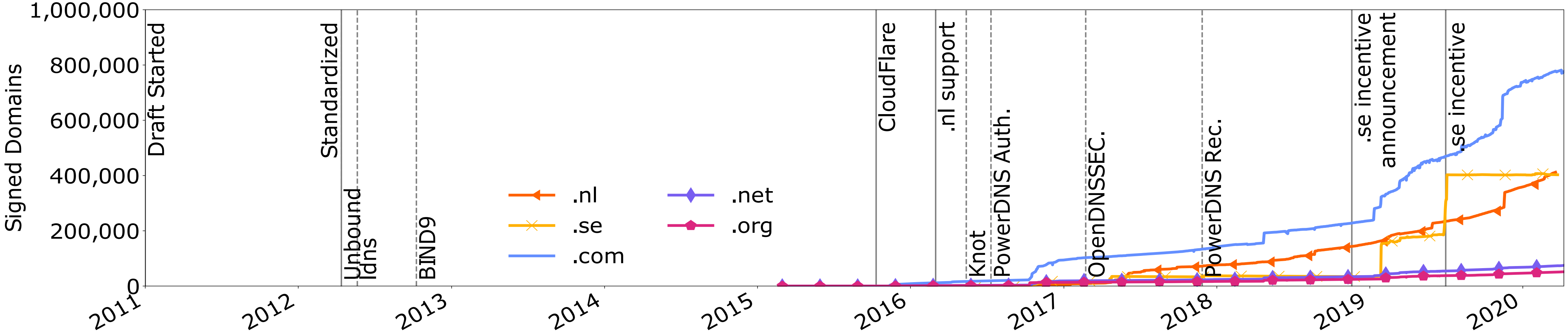
This week, the last week of October 2025, we reached a major milestone for Internet security: the majority of human-initiated traffic with Cloudflare is using post-quantum encryption mitigating the threat of harvest-now/decrypt-later.

.nl websites HTTPS secured with PQC algorithm



https://stats.sidnlabs.nl/en/web.html#websites%20secured%20with%20pqc%20algorithm

Time to deploy new algorithm in DNSSEC, +- 10 years



Timeline showing deployment of ECDSA256
from '*Making DNSSEC Future Proof*' by Moritz Müller.

SIDN LABS

Post-quantum Algorithms Testing and Analysis for the DNS

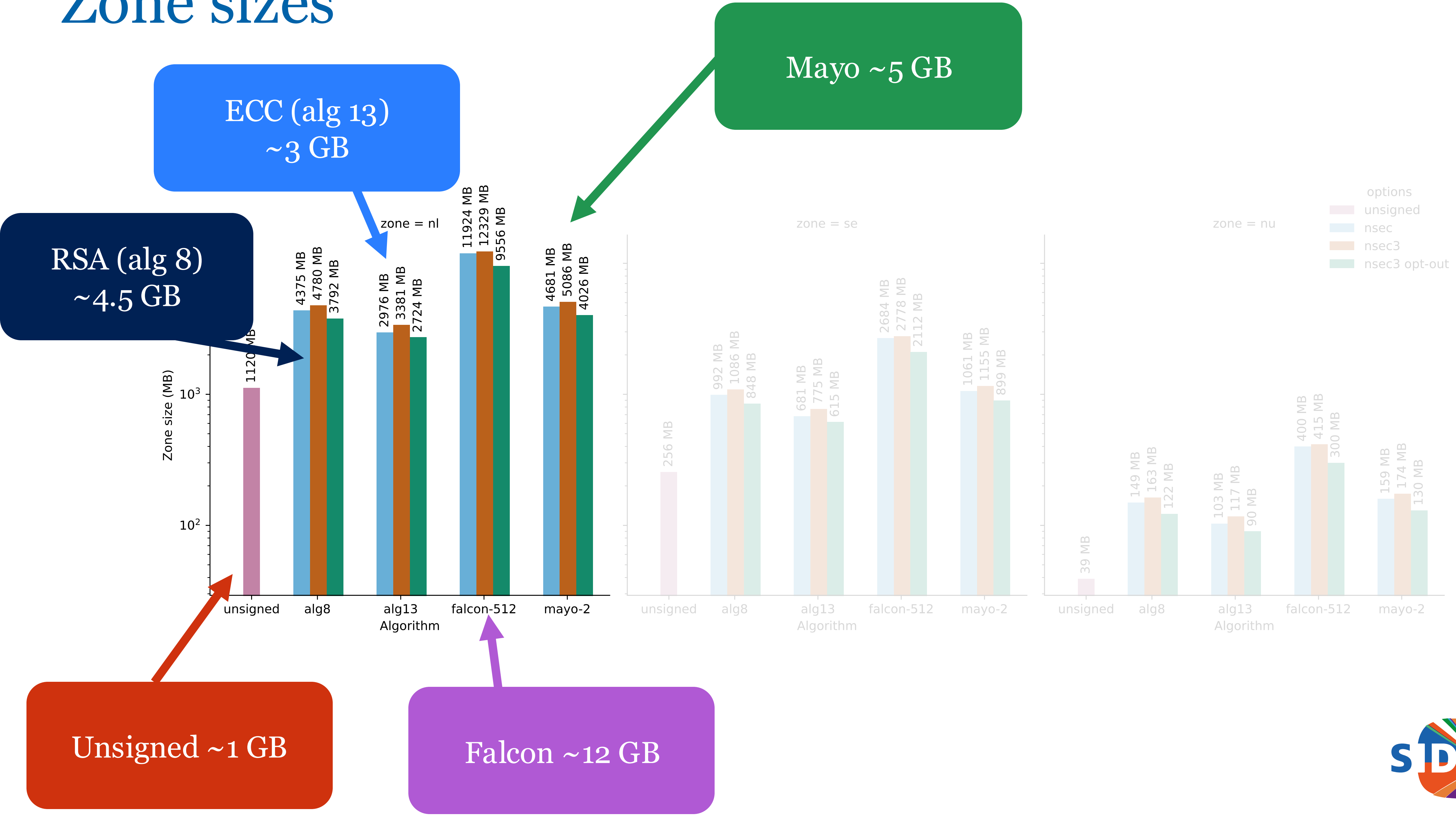
Hardware support (AVX2)	Proof of nonexistence
4 algorithms	3 zone files

Algorithm	Public key size	Signature size
RSA-1280	162*	160
ECDSA-P256	64	64
Falcon-512	897	666
MAYO-2 (R1)	5488	180

all numbers are in bytes

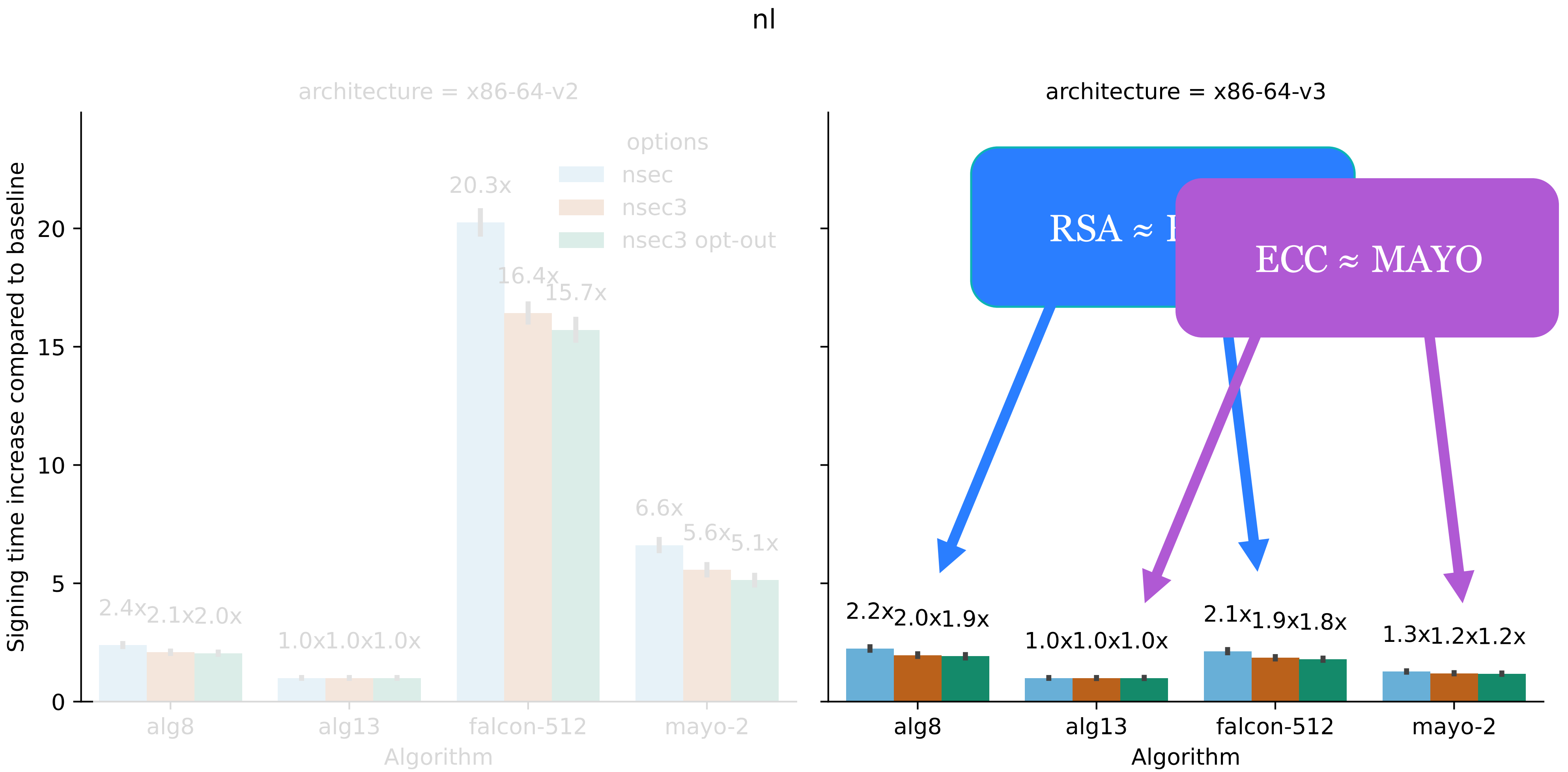


Zone sizes

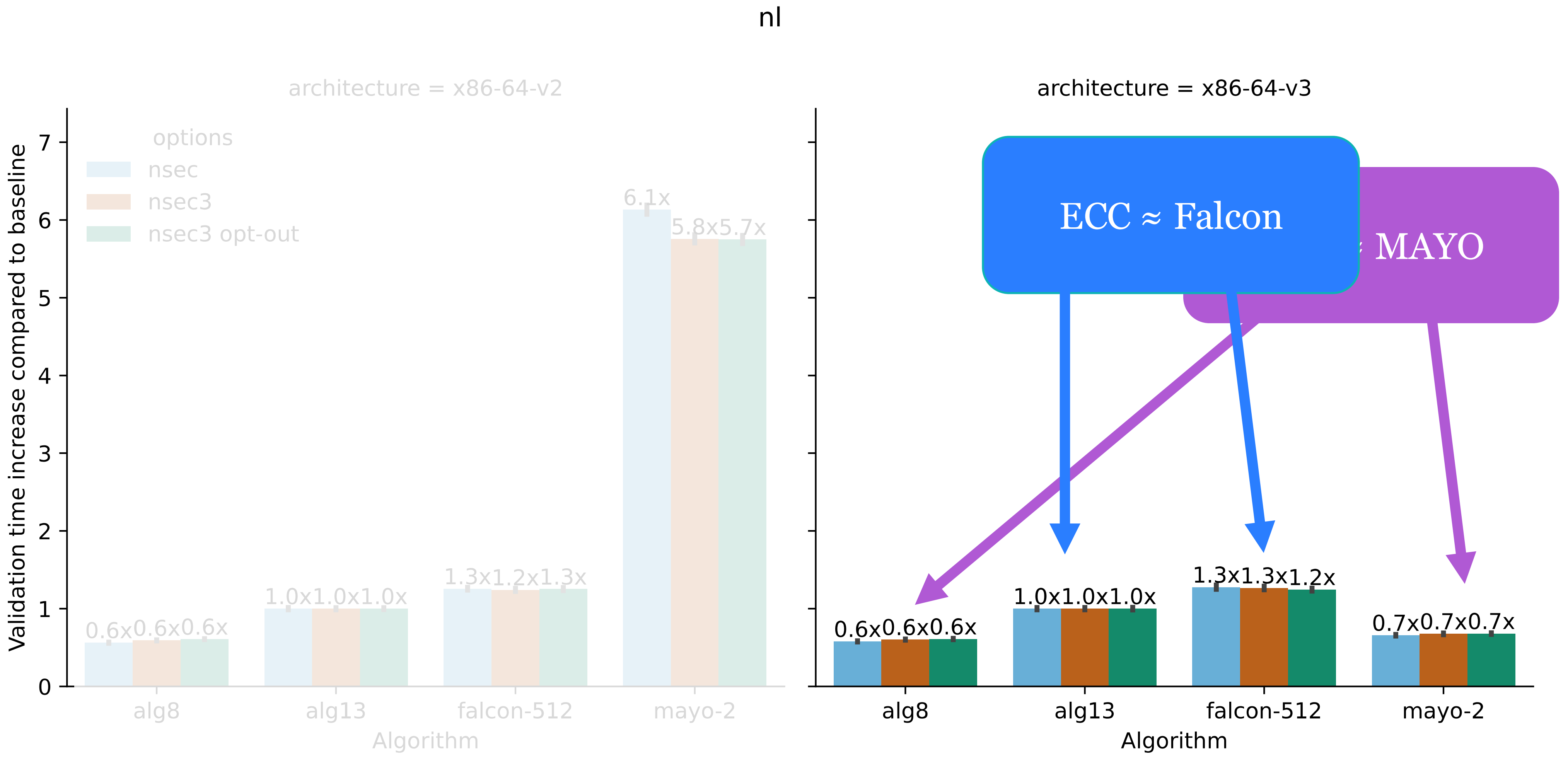


SIDN LABS

Signing time of entire .nl zone



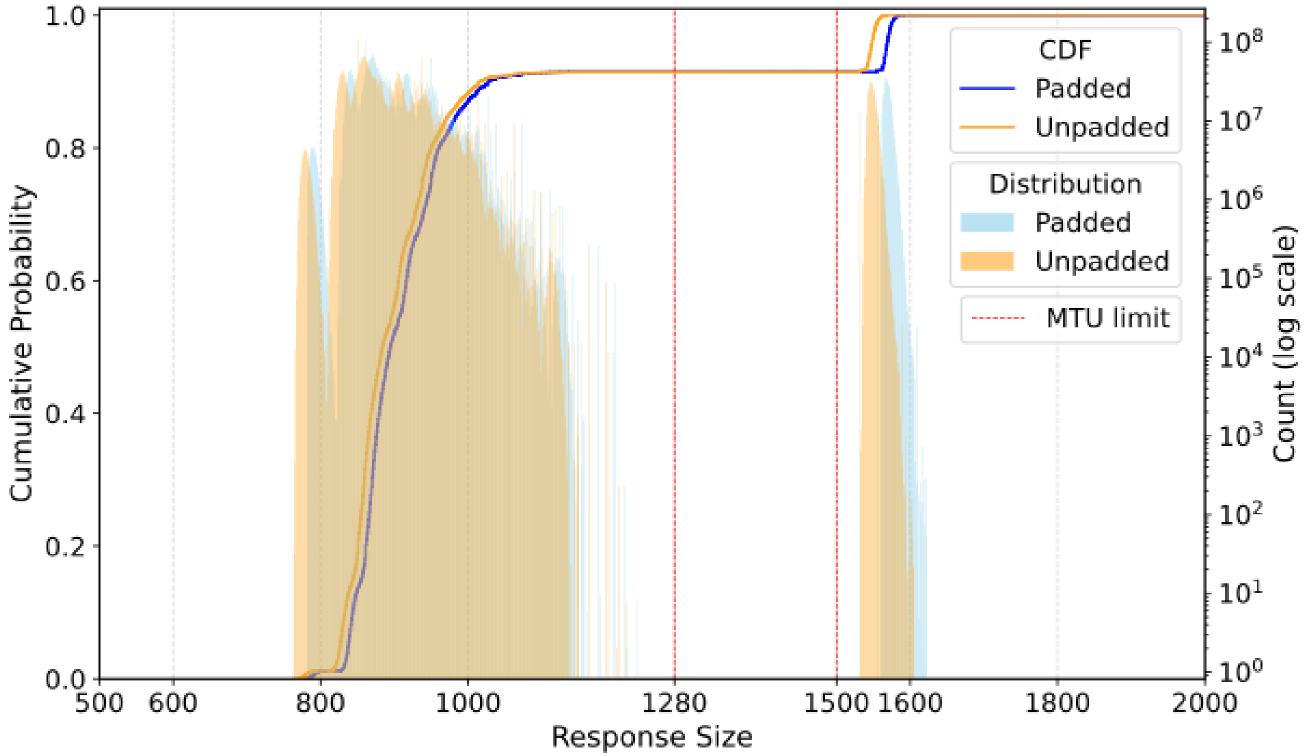
Validating the entire .nl zone




CAN WE FIX IT ?
YES WE CAN!!


WHAT'S
NEXT?

Falcon for .nl: padded or unpadded



Fabrizio et al, *PQC for DNSSEC: a format size analysis on Falcon signatures*
In: ANRW 2025.

https://doi.org/10.1145/3744200.3744767

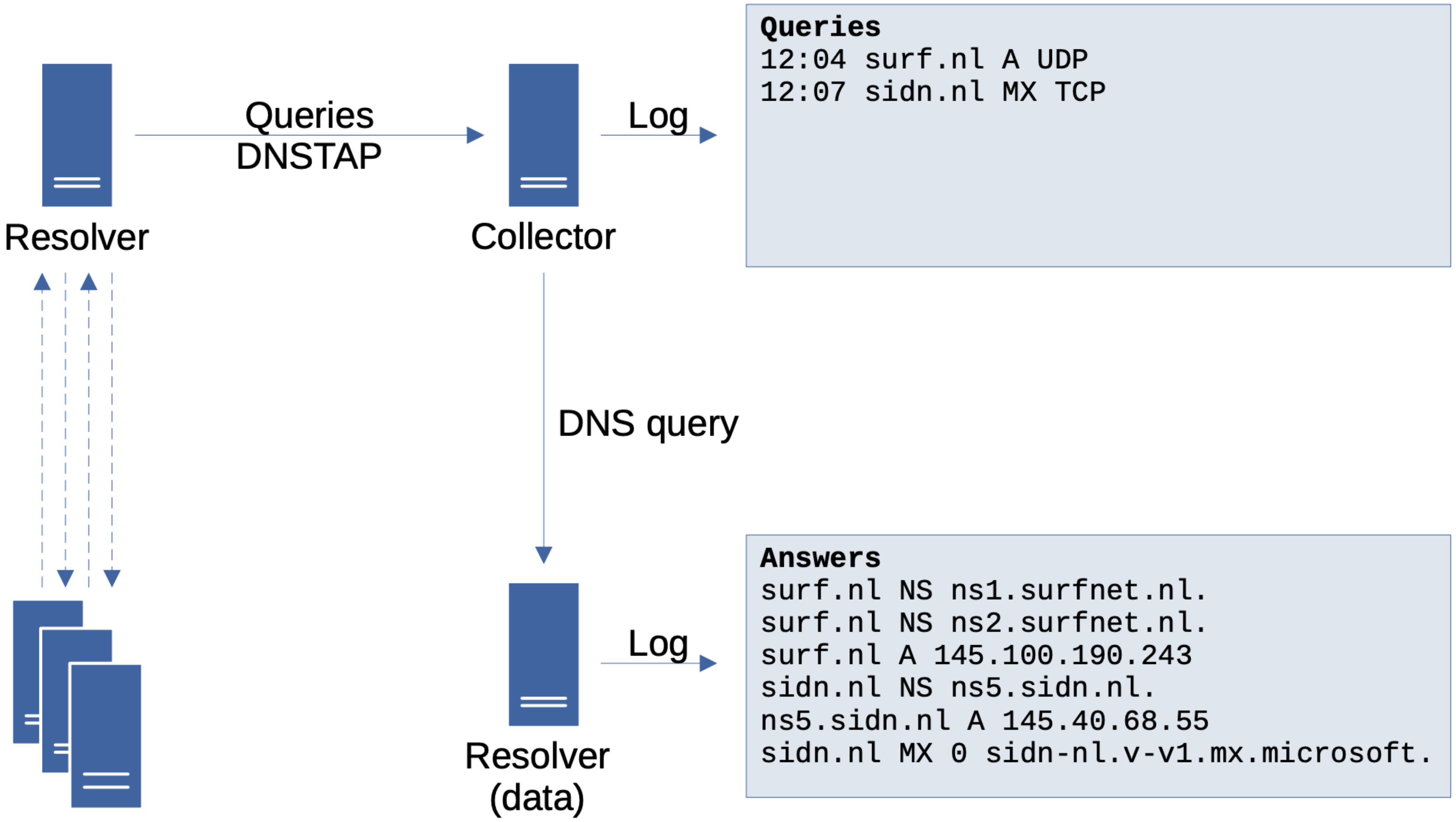
Response size	Response code	Response behavior
<77*	REFUSED (5)*	empty response*
764–1,229	NOERROR (0)	the requested records
1,532–1,622	NOERROR (0)	1 signed NSEC3 record
2,269–2,420	NXDOMAIN (3)	2 signed NSEC3 records
3,075–3,767	NXDOMAIN (3)	3 signed NSEC3 records

*Not shown in Figures 2 and 3.

Table 2: DNS response sizes clearly map to certain response behaviors

Impact of more TCP on authoritative nameservers

Measuring impact on resolvers



Add more algorithms to our testbed

SQIsign

About QR-UOV

The QR-UOV is an efficient signature scheme for the UOV scheme by using a polynomial quotient ring. The polynomial multiplication is embedded in a special matrix for fast processing.

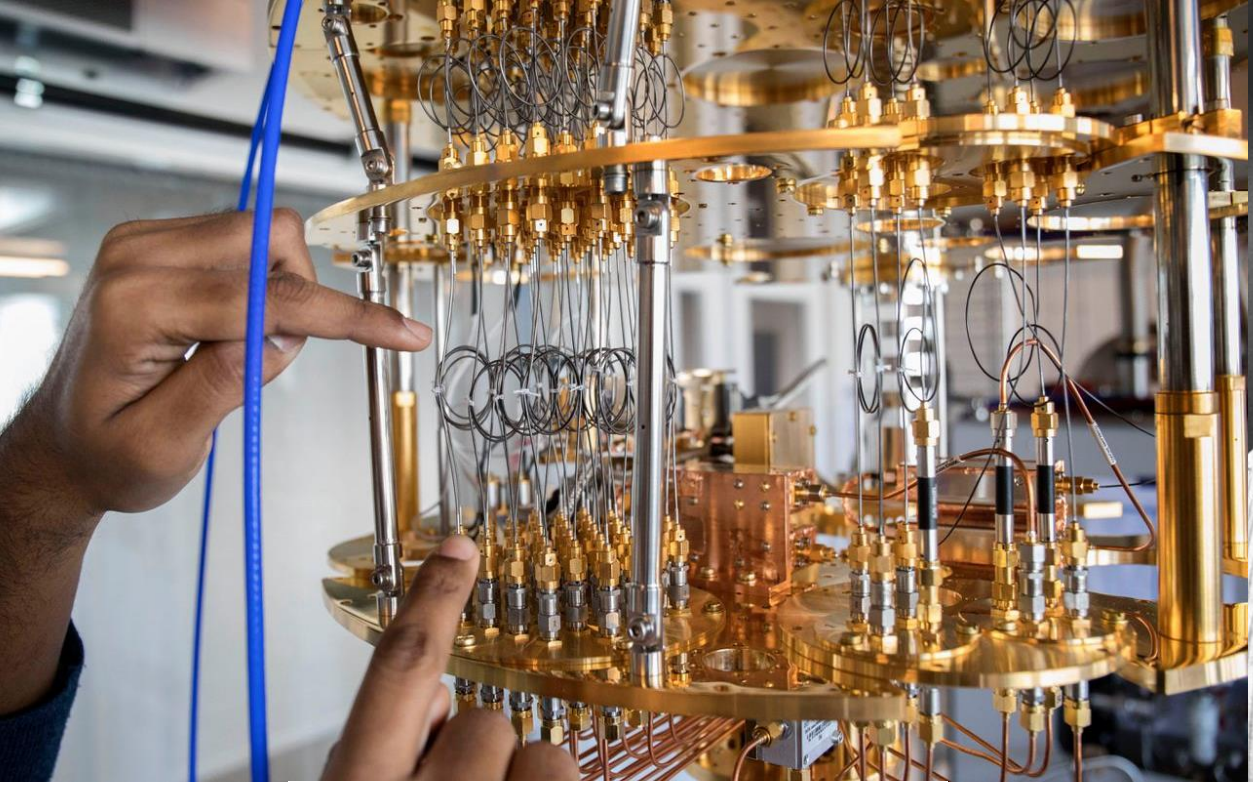
MTL

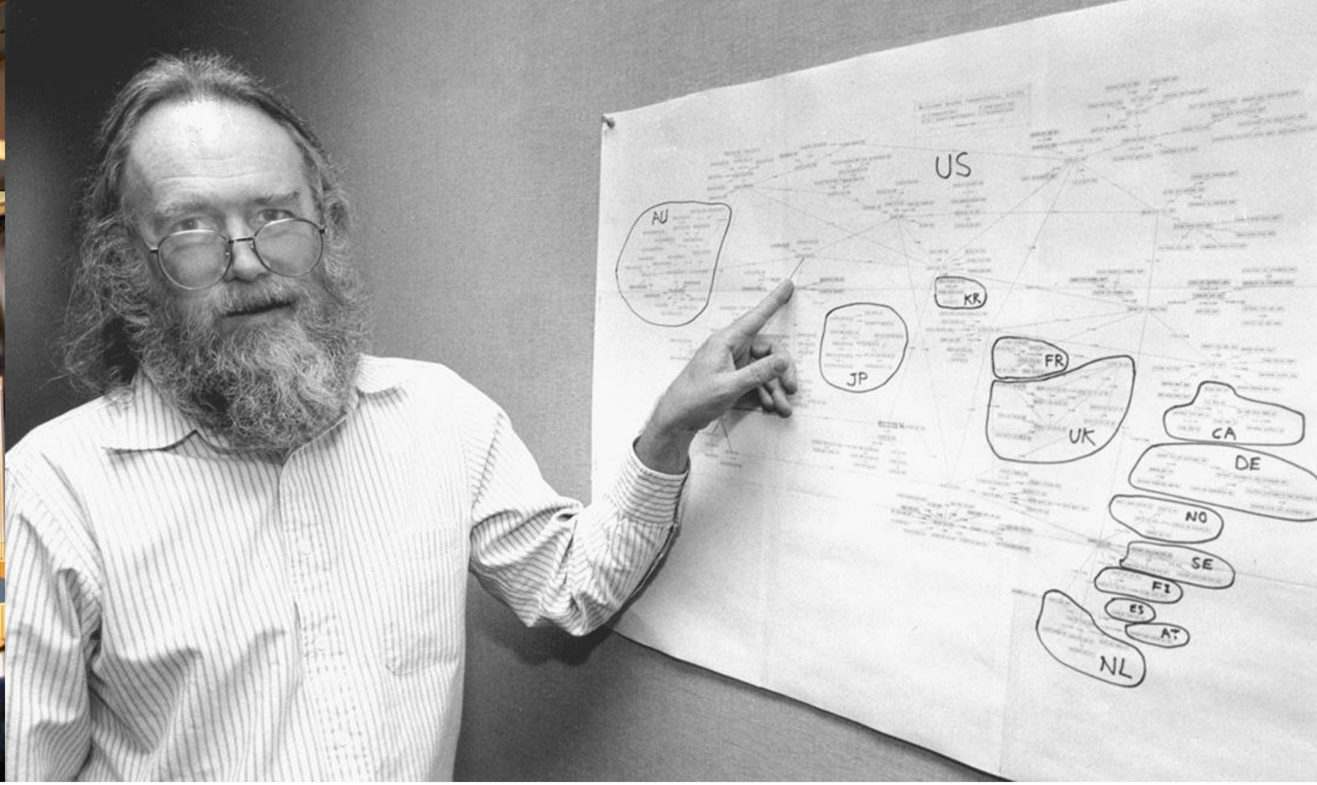
MTL Reference Library Implementation based on [draft-harvey-cfrg-mtl-mode-00]

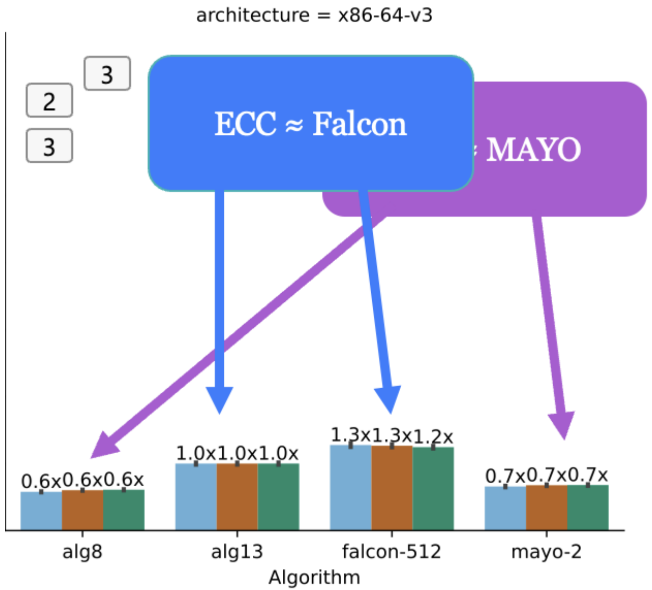
Dependencies

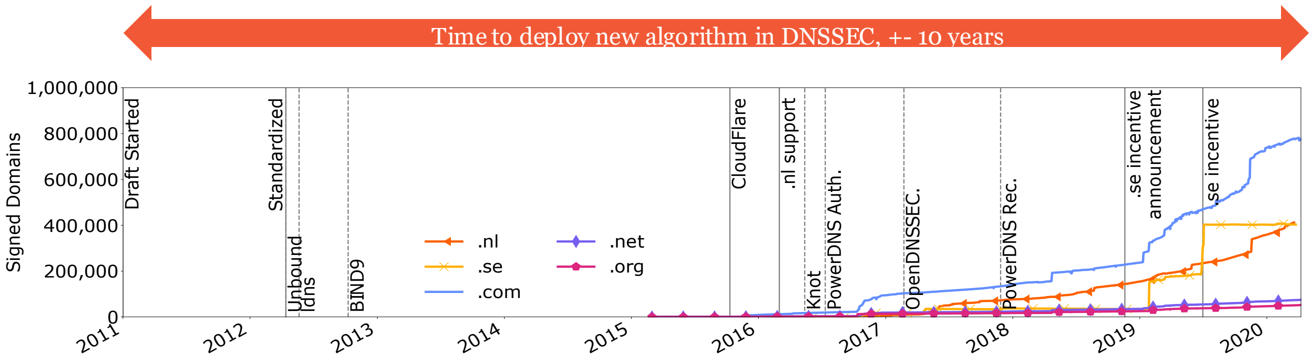
- libcrypto from openssl version 3.1.0 or newer (or substitute crypto operations t functions)
- liboqs version 0.7.2 or newer (for the examples). To include the liboqs library as change the -loqs to -l:*path*/liboqs.a in the examples/Makefile.am.
- Applications using the MTL Reference Library should also link with the C math

SIDN LABS




US
AU
KR
JP
FR
UK
CA
DE
NO
SE
FI
ES
AT
NL


architecture = x86-64-v3
3
2
3
ECC ≈ Falcon
MAYO
0.6x0.6x0.6x
1.0x1.0x1.0x
1.3x1.3x1.2x
0.7x0.7x0.7x
alg8
alg13
falcon-512
mayo-2
Algorithm


Time to deploy new algorithm in DNSSEC, +- 10 years
Signed Domains
1,000,000
800,000
600,000
400,000
200,000
0
Draft Started
Standardized
Unbound
ldns
BIND9
CloudFlare
.nl support
Knot
PowerDNS Auth.
OpenDNSSEC.
PowerDNS Rec.
.se incentive announcement
.se incentive
.nl
.se
.com
.net
.org
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020

Thank you for your attention!

Elmer Lastdrager
Research Engineer SIDN Labs
elmer.lastdrager@sidn.nl