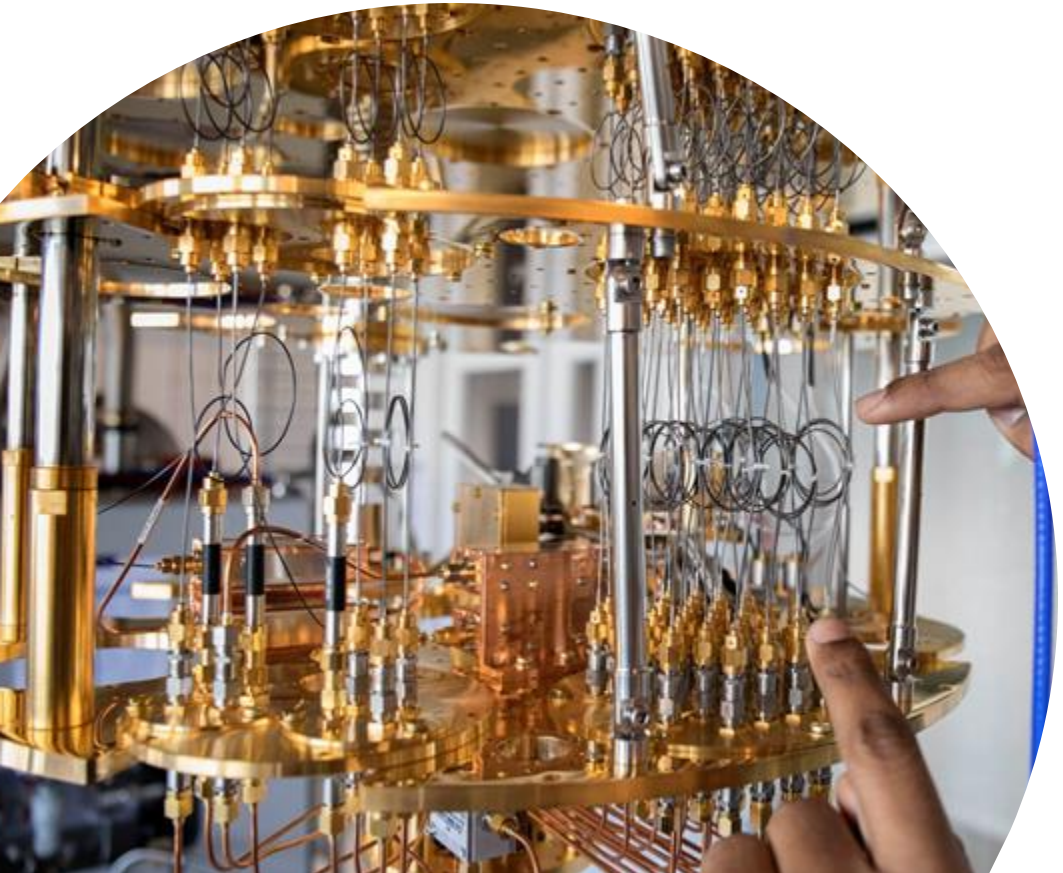


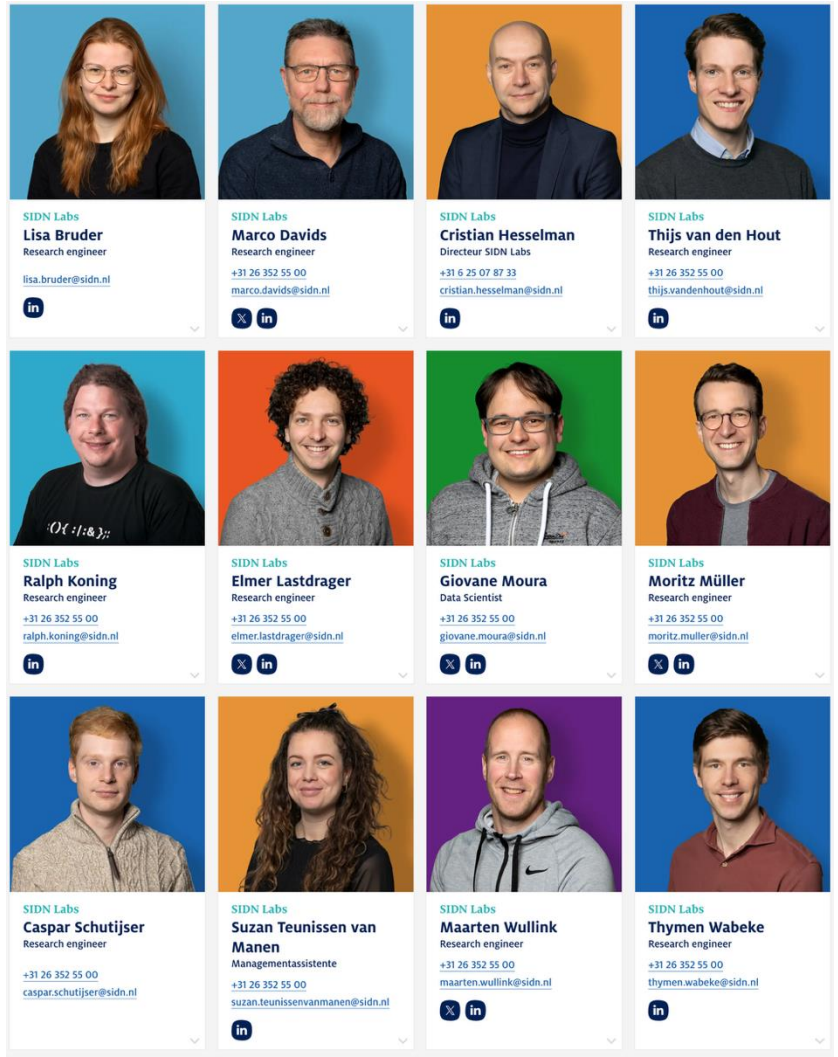
Post-quantum cryptography for DNS (DNSSEC)

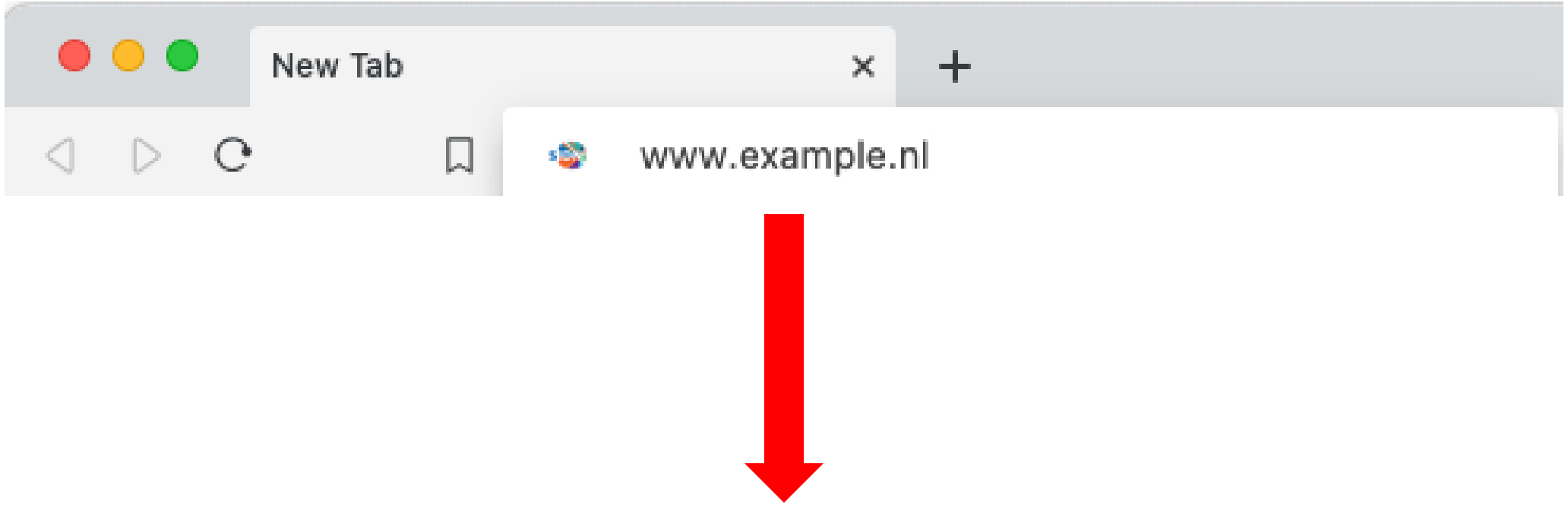
Elmer Lastdrager

PCSI benchmarking knowledge sharing session
Tuesday 20 May 2025

SIDN Labs is the research arm of SIDN

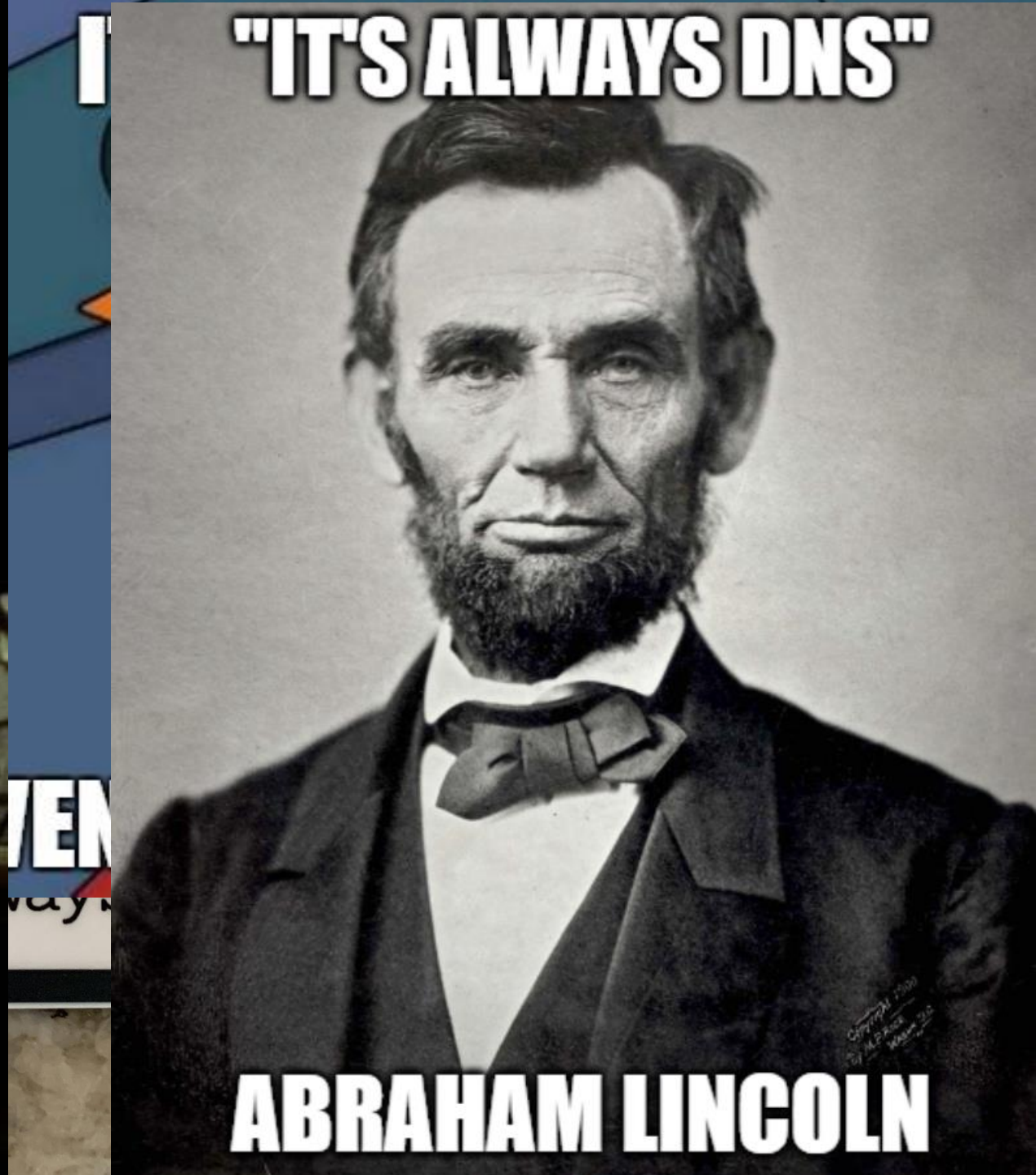
- Goal: further increase the security of the Internet, with a special focus on .nl and the Netherlands
- Applied technical research: large-scale Internet measurements, prototyping new Internet systems, evaluating them, contributing to standards
- Results are public and generic (e.g., measurement methods and insights, designs, software) plus SIDN-specific adaptations for SIDN teams



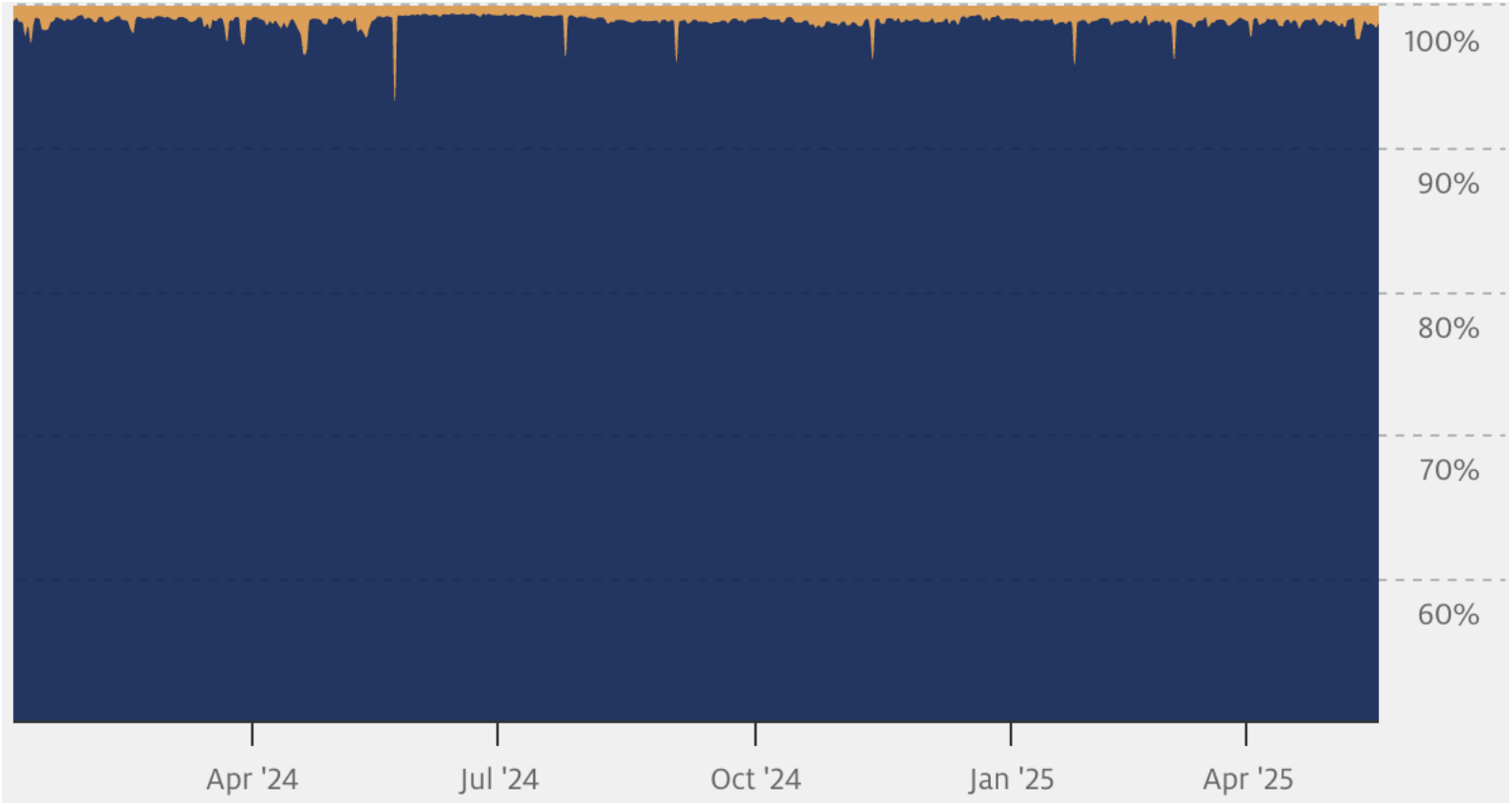


2a00:d78:0:712:94:198:159:35


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


"IT'S ALWAYS DNS"
ABRAHAM LINCOLN


30t
13t



stats.sidnlabs.nl – DNS Traffic

Prio	Requirement	Good	Accepted Conditionally
#1	Signature Size	≤ 1,232 bytes	—
#2	Validation Speed	≥ 1,000 sig/s	—
#3	Key Size	≤ 64 kilobytes	> 64 kilobytes
#4	Signing Speed	≥ 100 sig/s	—

Table 2: Requirements for quantum-safe algorithms.

M. Müller et al, "Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC", ACM SIGCOMM Computer Communication Review, vol. 50, no. 4, 2020.

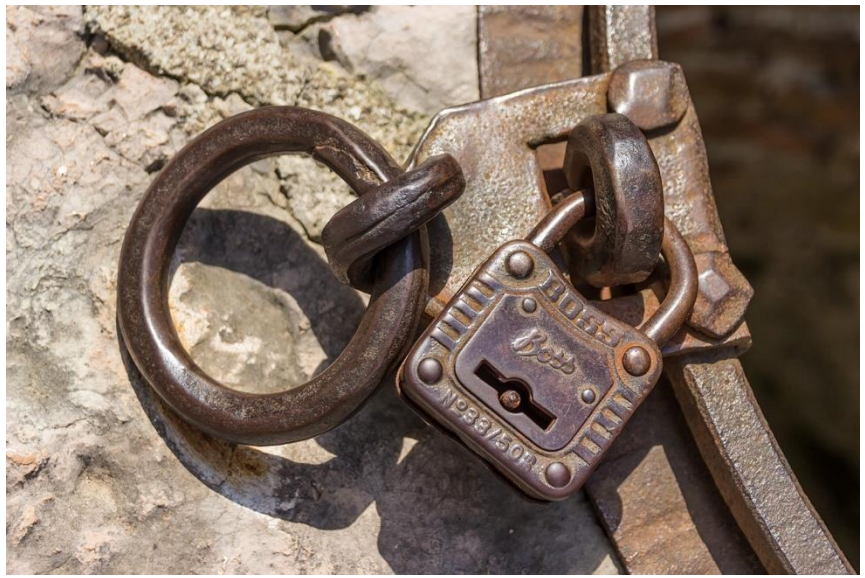
SIDN LABS

Jürgen Henn – 11foot8.com


gifbin.com

User

Resolver



DoH, DoT, DNScrypt

DNSSEC

User

Resolver

.

delegation info nl.
DS-record of .nl

signed by root

.nl

delegation info sidn.nl.
DS-record of sidn.nl
DNSKEY of .nl

signed by .nl

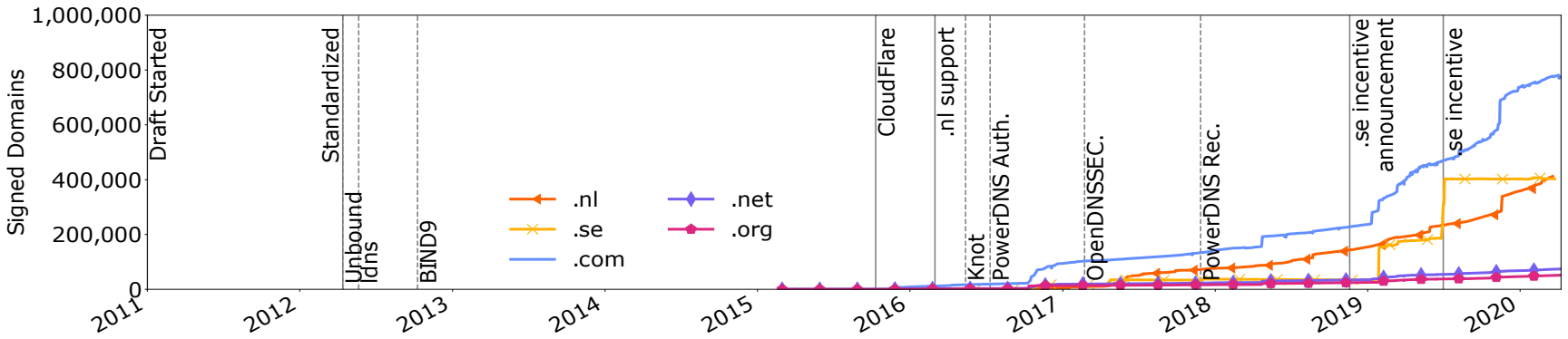
sidn.nl

answers for sidn.nl
DNSKEY of sidn.nl

signed by sidn.nl

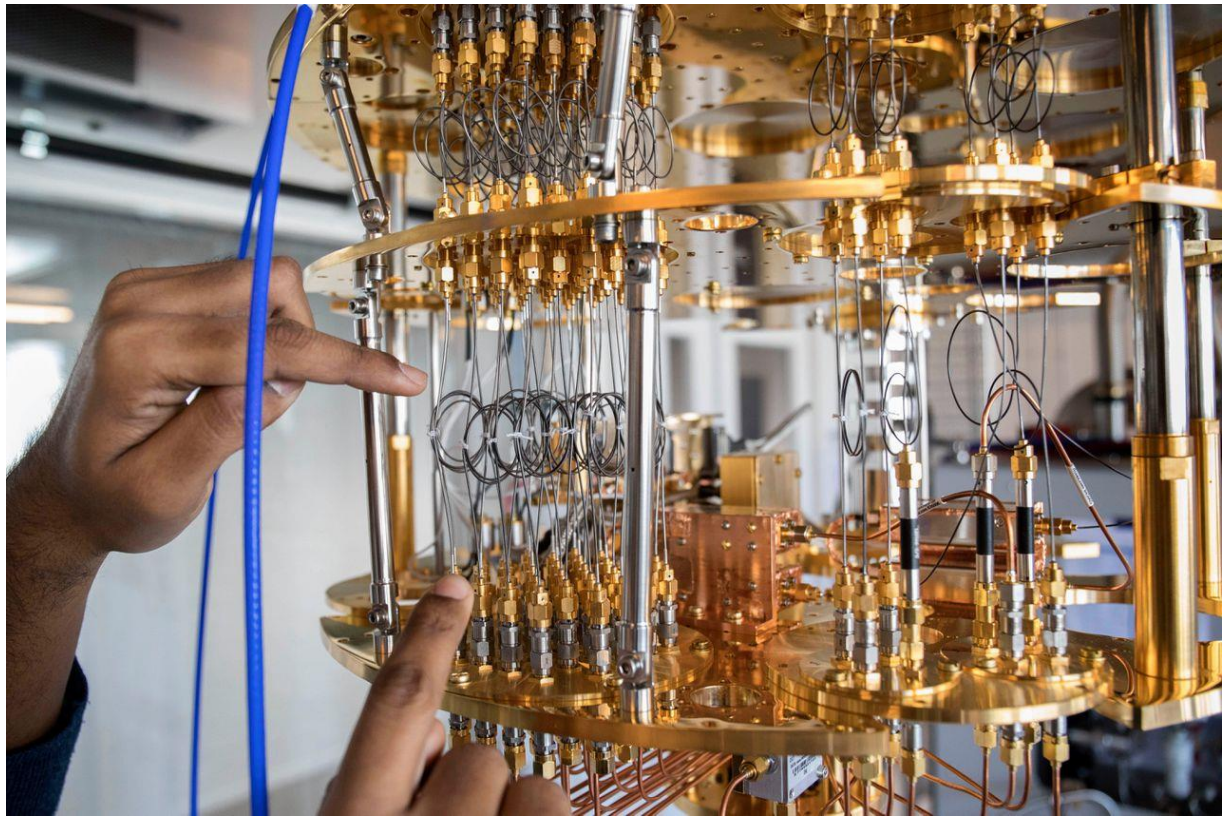
DS: fingerprint of public key
DNSKEY: public key
RRSIG: signature

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

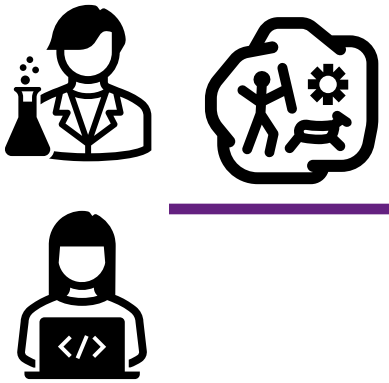


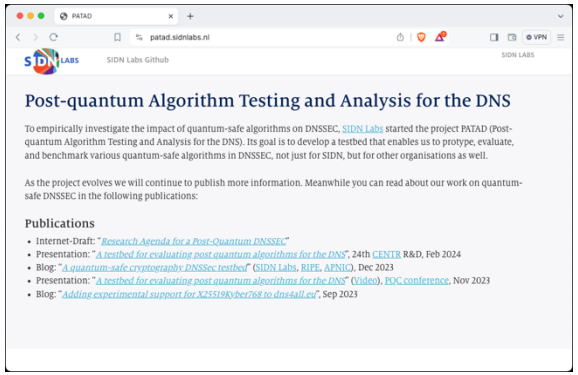
Timeline showing deployment of ECDSA256, from '*Making DNSSEC Future Proof*' by dr. Moritz Müller.

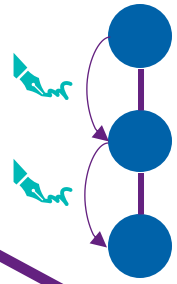
Post-quantum Algorithms Testing and Analysis for the DNS



PATAD testbed: building a testbed



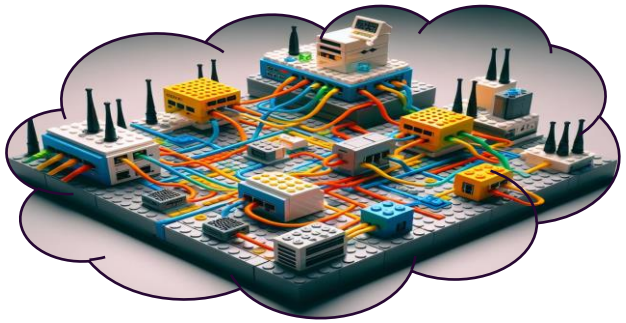




.

.nl

sidnlabs

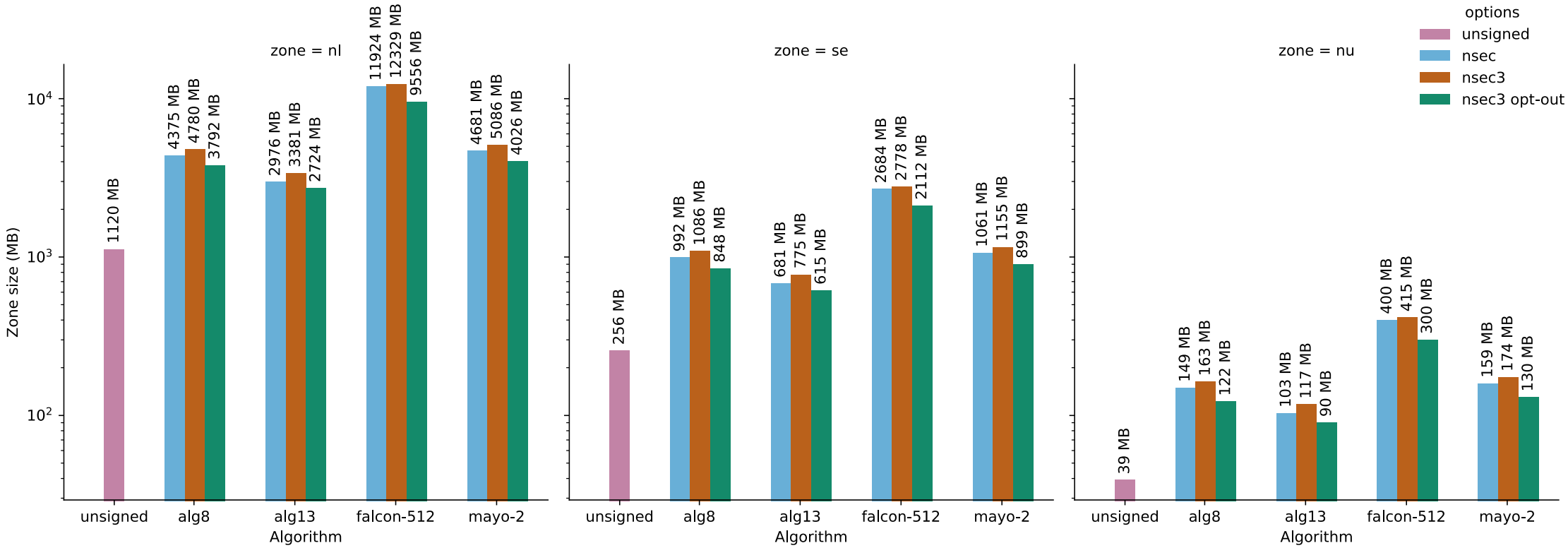


1.1.1.1

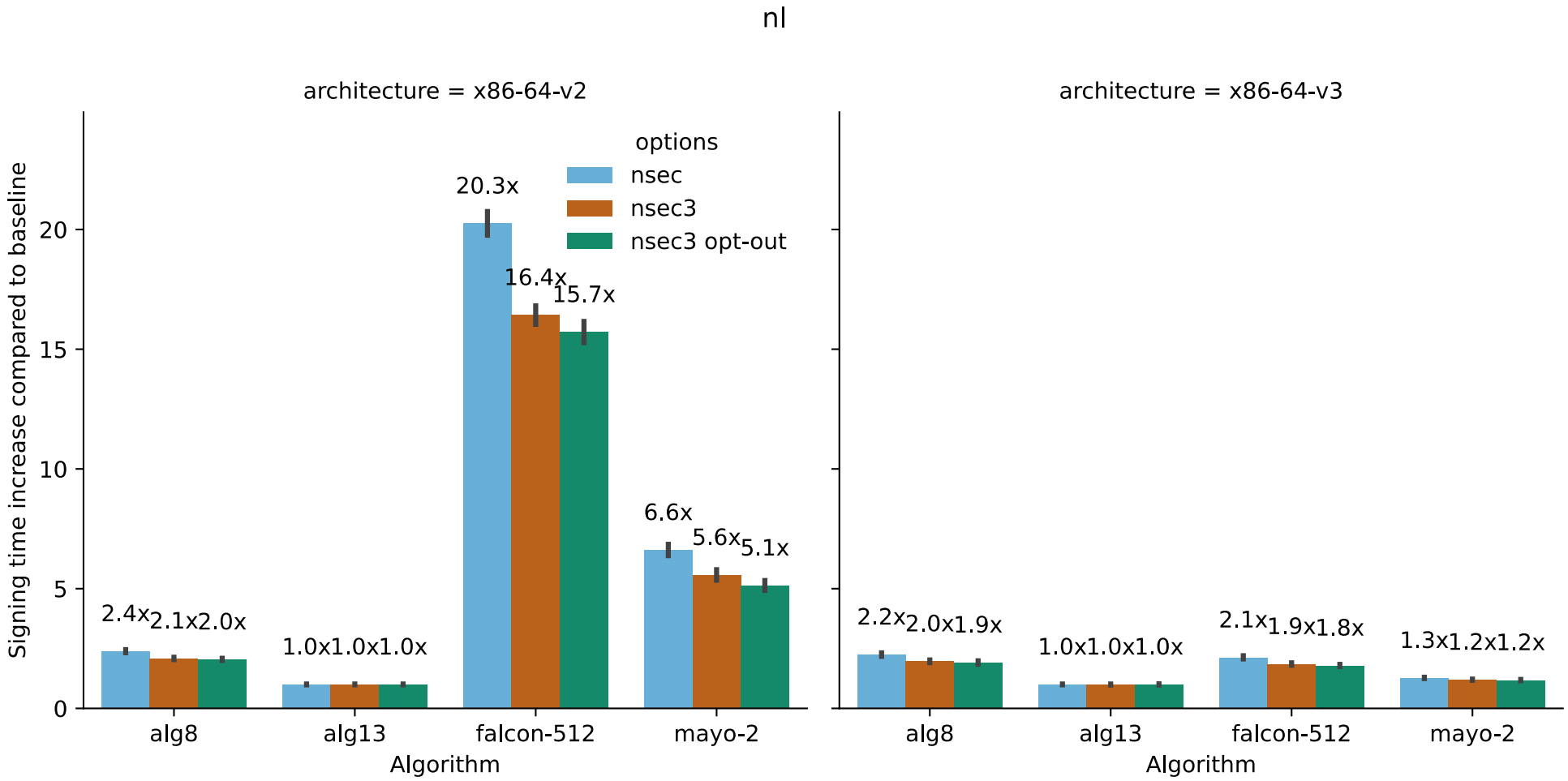
The free app that makes your Internet safer.

SIDN LABS

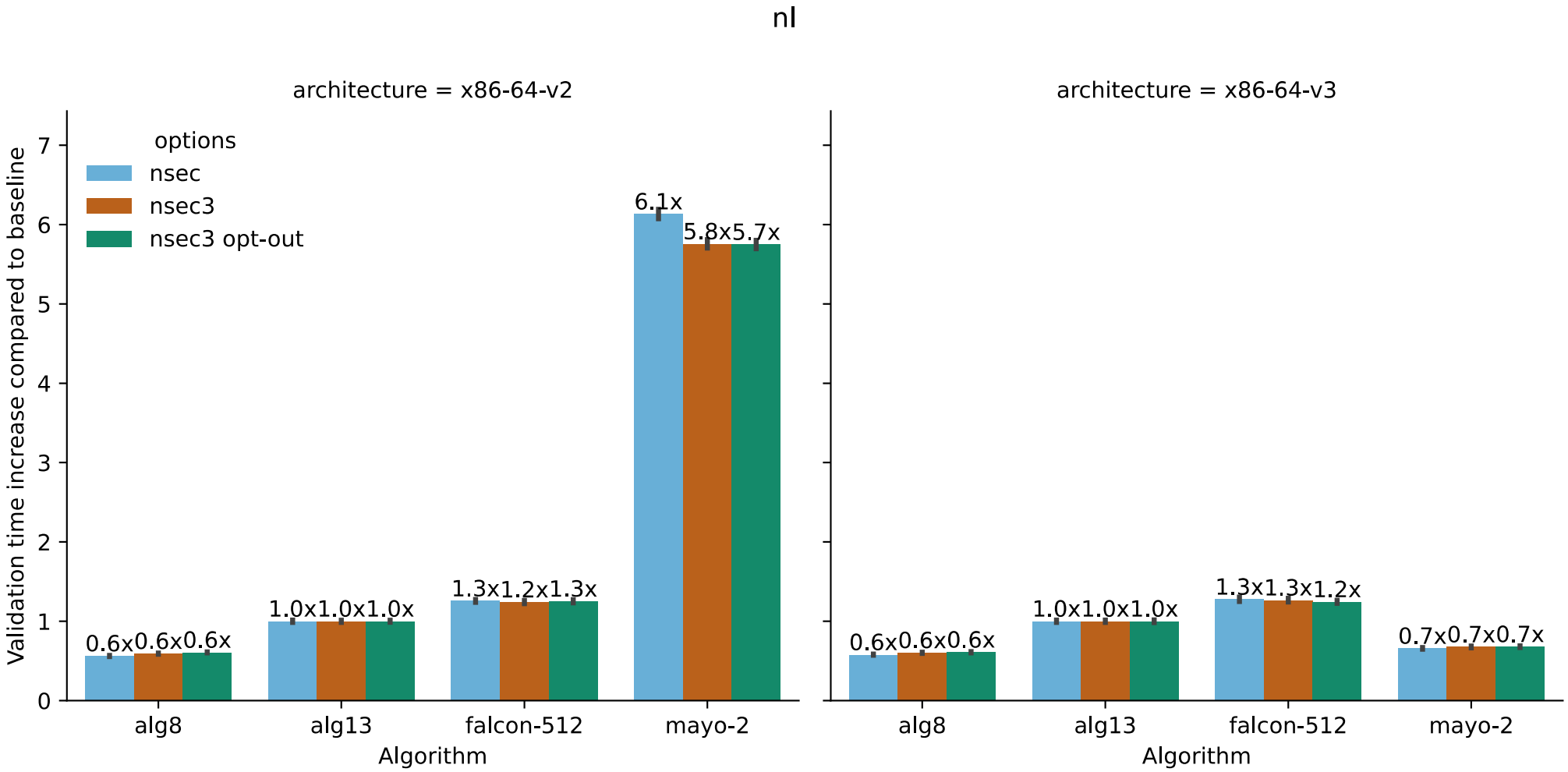
Zone size


zone = nl
zone = se
zone = nu
options
unsigned
nsec
nsec3
nsec3 opt-out
Zone size (MB)
10^4
10^3
10^2
1120 MB
4375 MB
4780 MB
3792 MB
2976 MB
3381 MB
2724 MB
11924 MB
12329 MB
9556 MB
4681 MB
5086 MB
4026 MB
256 MB
992 MB
1086 MB
848 MB
681 MB
775 MB
615 MB
2684 MB
2778 MB
2112 MB
1061 MB
1155 MB
899 MB
39 MB
149 MB
163 MB
122 MB
103 MB
117 MB
90 MB
400 MB
415 MB
300 MB
159 MB
174 MB
130 MB
unsigned
alg8
alg13
falcon-512
mayo-2
Algorithm

Signing


nl
architecture = x86-64-v2
architecture = x86-64-v3
options
nsec
nsec3
nsec3 opt-out
Signing time increase compared to baseline
0
5
10
15
20
2.4x
2.1x
2.0x
1.0x
1.0x
1.0x
20.3x
16.4x
15.7x
6.6x
5.6x
5.1x
2.2x
2.0x
1.9x
1.0x
1.0x
1.0x
2.1x
1.9x
1.8x
1.3x
1.2x
1.2x
alg8
alg13
falcon-512
mayo-2
Algorithm

Validation


nl
architecture = x86-64-v2
architecture = x86-64-v3
options
nsec
nsec3
nsec3 opt-out
Validation time increase compared to baseline
0
1
2
3
4
5
6
7
0.6x0.6x0.6x
1.0x1.0x1.0x
1.3x1.2x1.3x
6.1x
5.8x5.7x
0.6x0.6x0.6x
1.0x1.0x1.0x
1.3x1.3x1.2x
0.7x0.7x0.7x
alg8
alg13
falcon-512
mayo-2
Algorithm

Demo

User

Resolver

.

delegation info nl.
DS-record of .nl

signed by root

.nl

delegation info sidn.nl.
DS-record of sidn.nl
DNSKEY of .nl

signed by .nl

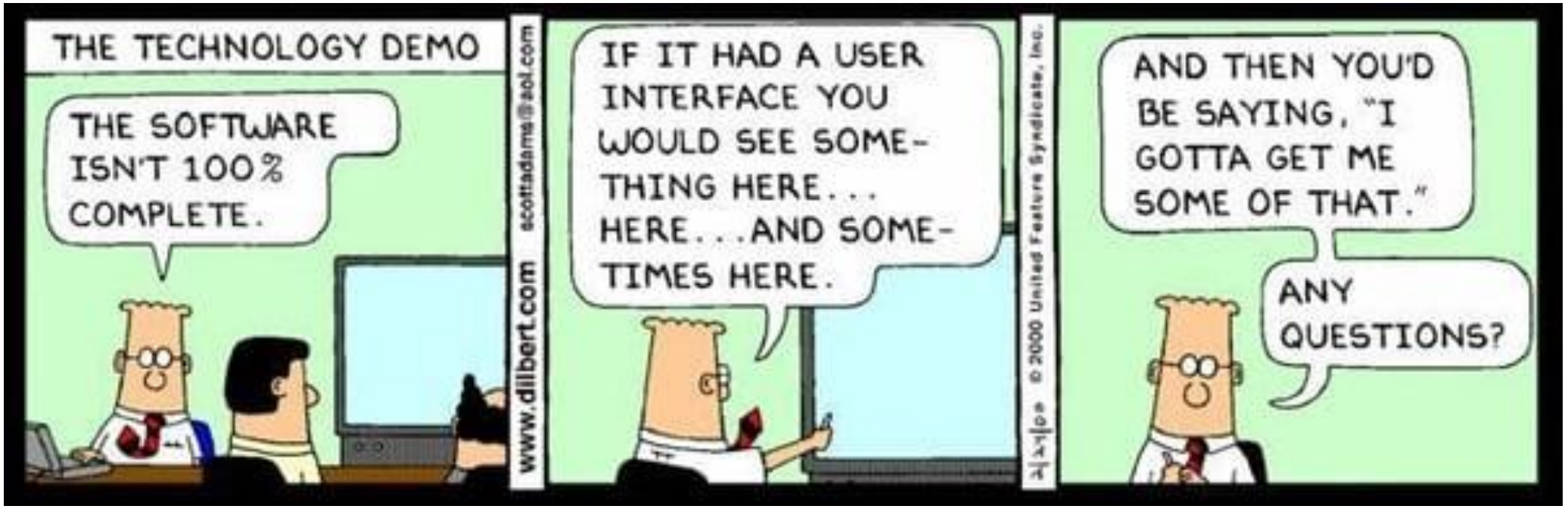
sidn.nl

answers for sidn.nl
DNSKEY of sidn.nl

signed by sidn.nl

DS: fingerprint of public key
DNSKEY: public key
RRSIG: signature

Demo


THE TECHNOLOGY DEMO
THE SOFTWARE ISN'T 100% COMPLETE.
www.dilbert.com scottadams@aol.com
IF IT HAD A USER INTERFACE YOU WOULD SEE SOMETHING HERE... HERE...AND SOMETIMES HERE.
© 2000 United Feature Syndicate, Inc.
AND THEN YOU'D BE SAYING, "I GOTTA GET ME SOME OF THAT."
ANY QUESTIONS?

Thanks for your attention

Elmer Lastdrager
elmer.lastdrager@sidn.nl

https://www.sidnlabs.nl