SIDN Labs: use-inspired research for a more secure internet infrastructure

Moritz Müller | ICANN 74

June 13, 2022

SIDN is the operator of the .nl TLD

- Objective: increase society's confidence in the Internet

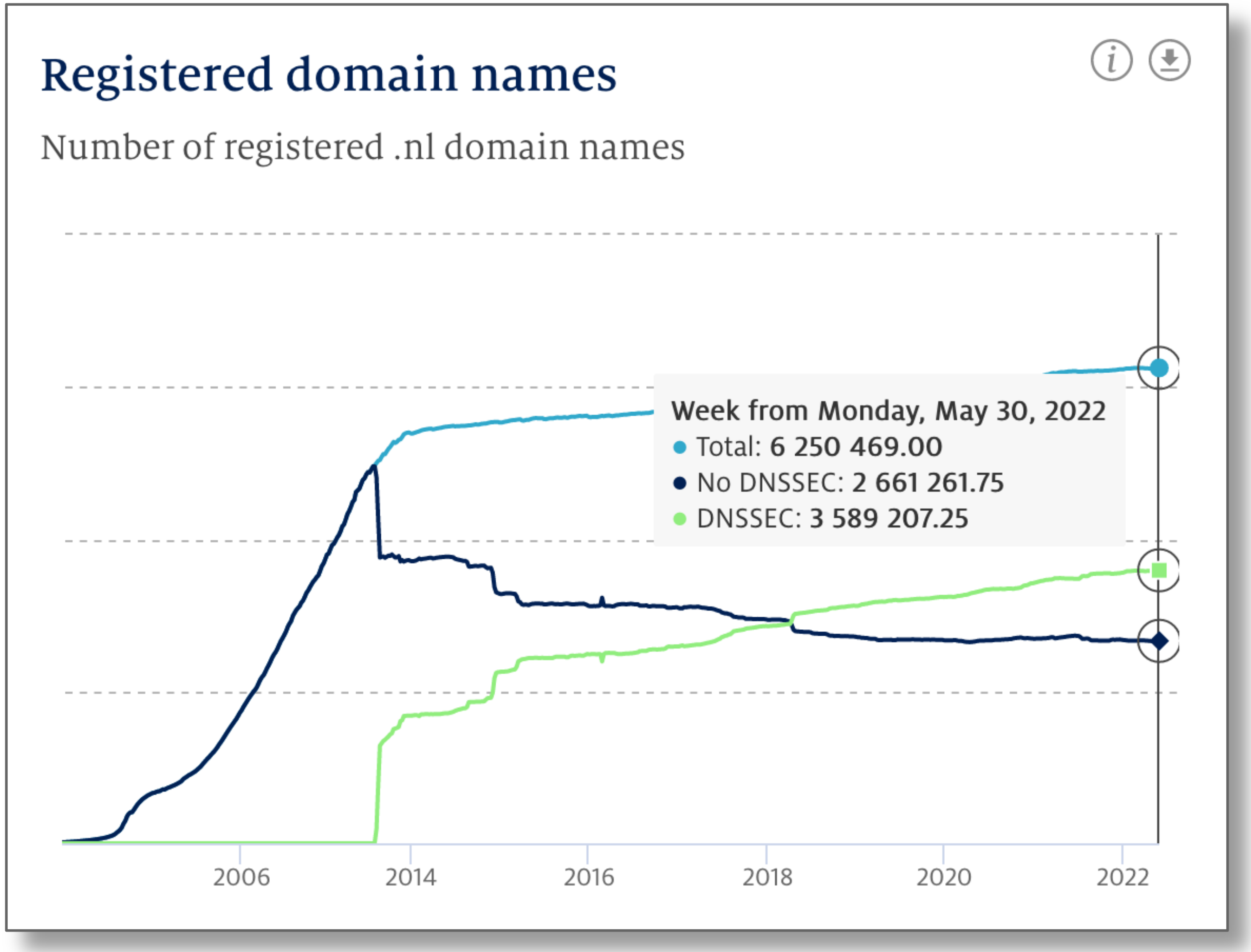
- Provide secure and fault-tolerant registry services for .nl
  - Anycasted DNS services with DNSSEC support
  - Registration and domain protection services

- Increase the value of the Internet in the Netherlands and elsewhere
  - Enable safe and novel uses (SIDN Fonds, IRMA)
  - Increase infrastructure security and trustworthiness (SIDN Labs)

- Not-for-profit private organization with a public role based in Arnhem

.nl = the Netherlands
17M inhabitants
6.2M domain names
3.4M DNSSEC-signed
2.5B DNS queries/day
8.6B NTP queries/day

Number of .nl domain names (stats.sidnlabs.nl)

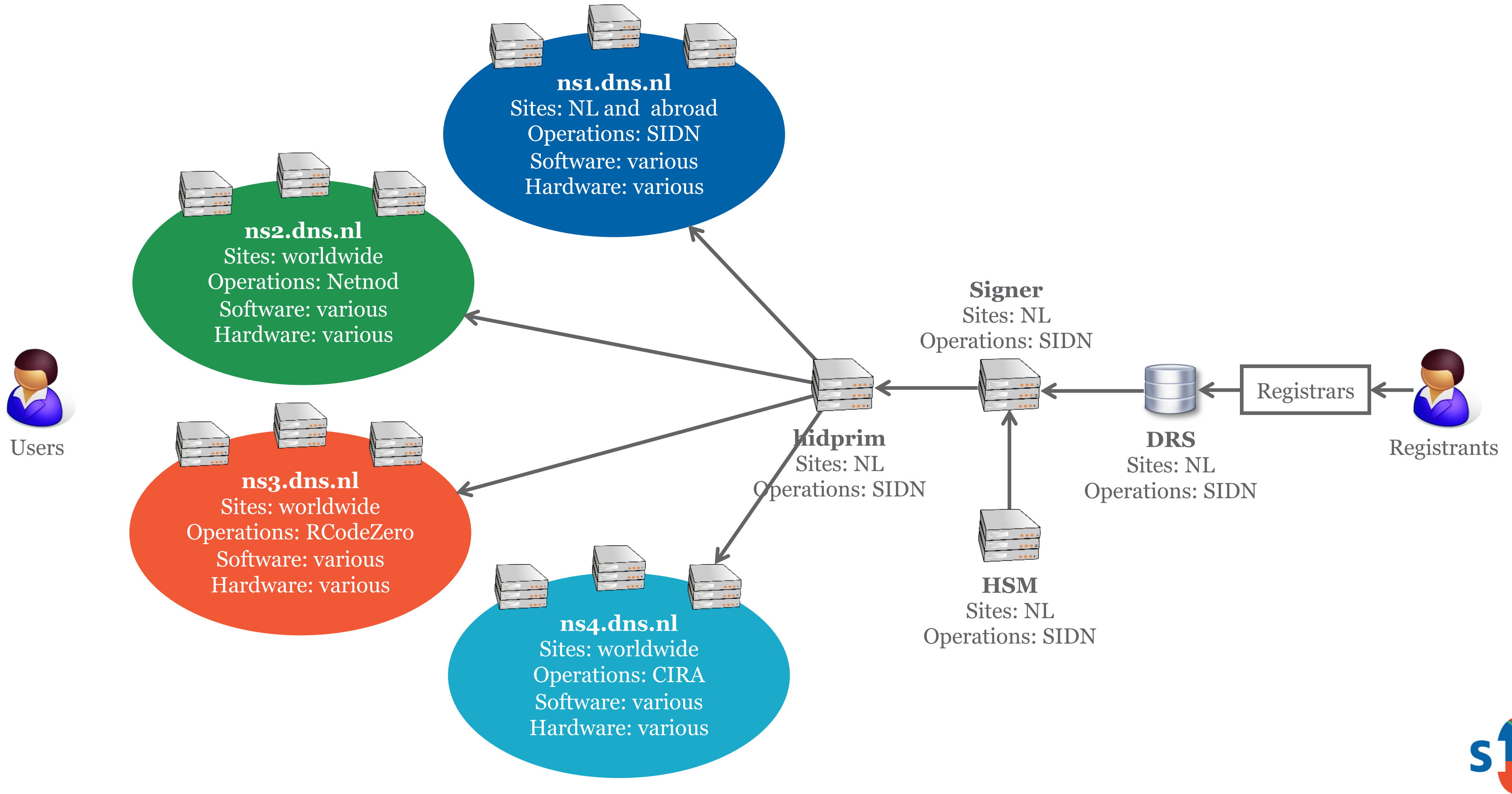


Registered domain names

Number of registered .nl domain names

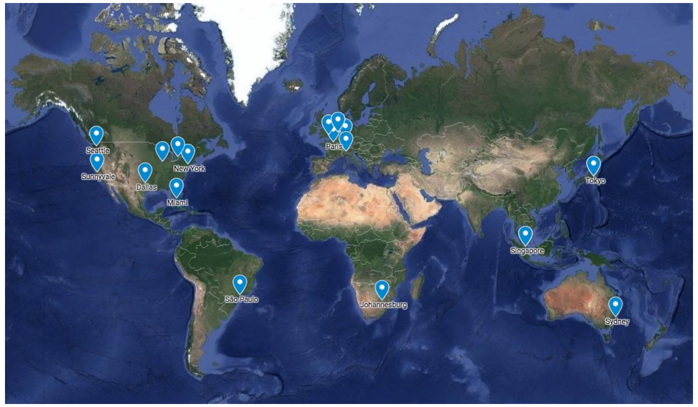
Week from Monday, May 30, 2022
- ● Total: 6 250 469.00
- ● No DNSSEC: 2 661 261.75
- ● DNSSEC: 3 589 207.25

Heterogeneous and fault-tolerant DNS infrastructure

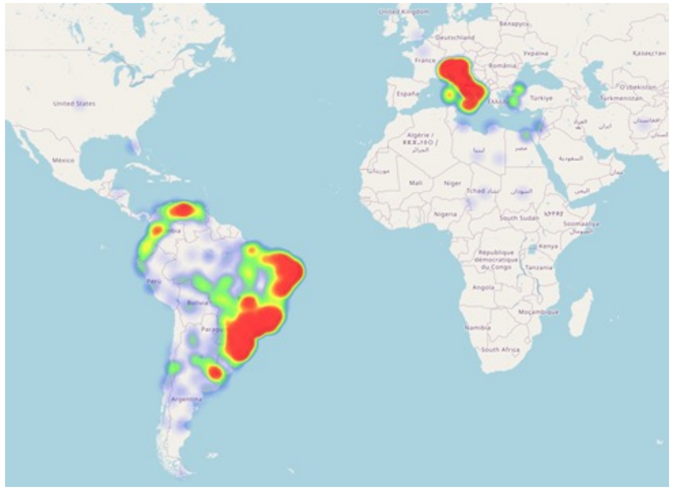


A more flexible DNS infrastructure (ns1.dns.nl)

- Virtual machines at cloud providers
- Vultr, Packet (Equinix), Heficed
- Control over VMs and operating systems
- Complements “as a service” and owned infra
- BIRD-based BGP sessions to cloud providers
  - Path pre-pending
  - BGP communities



Anycast2020 sites



BGP tuning based on catchments

SIDN Labs team

SIDN Labs
Maarten Wullink
Research engineer

SIDN Labs
Thymen Wabeke
Research engineer

SIDN Labs
Moritz Müller
Research engineer

SIDN Labs
Marisca van der Donk
Managementassistente

SIDN Labs
Elmer Lastdrager
Research engineer

SIDN Labs
Thijs van den Hout
Research Engineer

SIDN Labs
Ralph Koning
Research Engineer

SIDN Labs
Jelte Jansen
Research engineer

SIDN Labs
Caspar Schutijser
Research engineer

SIDN Labs
Cristian Hesselman
Directeur SIDN Labs

SIDN Labs
Giovane Moura
Data Scientist

SIDN Labs
Marco Davids
Research engineer

- 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

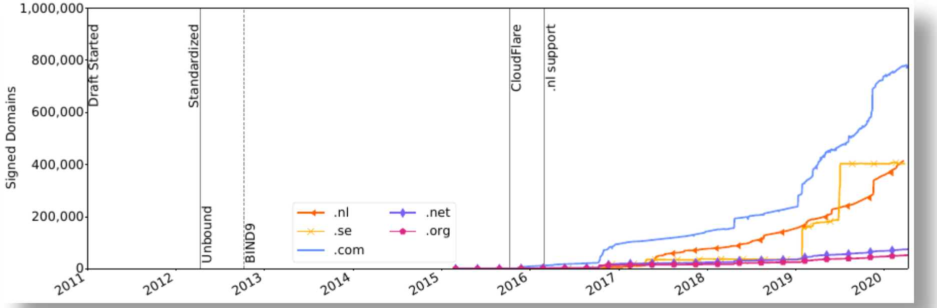
SIDN Labs = research team

- Goal: increase trustworthiness of our society’s internet infrastructure, for .nl and the Netherlands in particular.

- Strategies:
  - Applied technical research (measurements, design, prototyping, evaluation)
  - Make results publicly available and useful for various target groups
  - Work with universities, infrastructure operators, and other labs

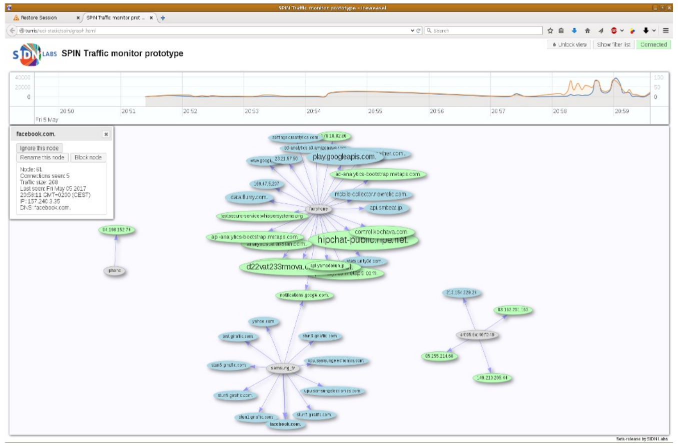
- Three research areas: network security (DNS, NTP, BGP), domain name & IoT security, secure future internet infrastructures

Example projects



Measuring the deployment of newly standardized DNSSEC algorithms [3]

Provide well-managed and secure time services [4]

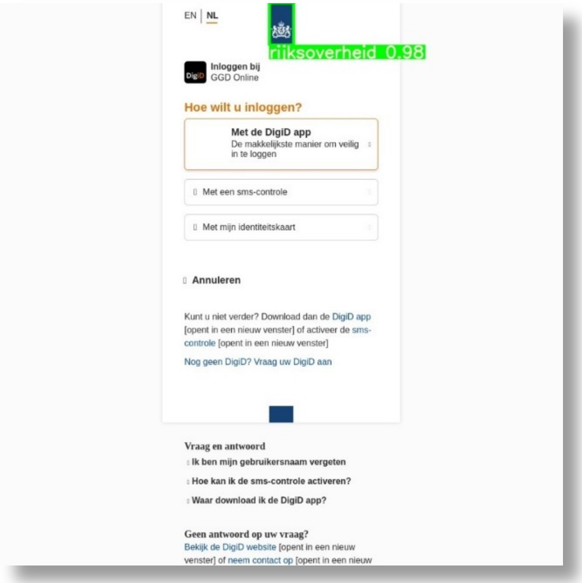


SPIN Traffic monitor prototype

facebook.com.

Node: 61
Connections seen: 5
Traffic size: 268
Last seen: Fri May 05 2017 20:58:11 GMT+0200 (CEST)
IP: 157.240.3.35
DNS: facebook.com.

Making the IoT more secure and transparent and measure its evolution [5]



EN | NL

Inloggen bij
GGD Online

Hoe wilt u inloggen?

Met de DigiD app
De makkelijkste manier om veilig in te loggen

Met een sms-controle

Met mijn identiteitskaart

Annuleren

Kunt u niet verder? Download dan de DigiD app [opent in een nieuw venster] of activeer de sms-controle [opent in een nieuw venster]

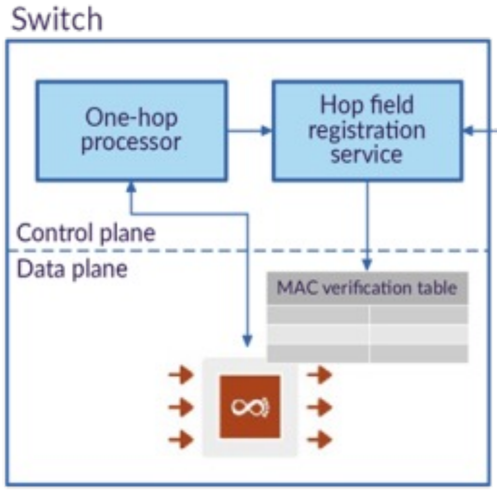
Nog geen DigiD? Vraag uw DigiD aan

Vraag en antwoord

- **Ik ben mijn gebruikersnaam vergeten**
- **Hoe kan ik de sms-controle activeren?**
- **Waar download ik de DigiD app?**

Geen antwoord op uw vraag?
Bekijk de DigiD website [opent in een nieuw venster] of neem contact op [opent in een nieuw

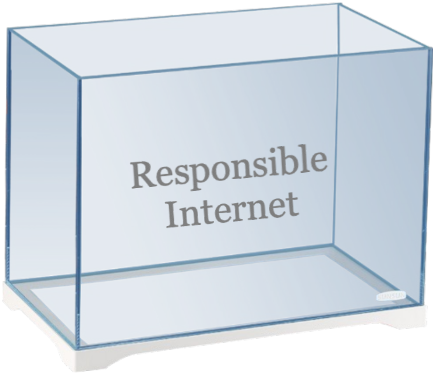
Logo detection technology to identify malicious .nl websites [6]



SCION

P4

Experimenting with secure future networks and programmable networks [7][8]



2STIC

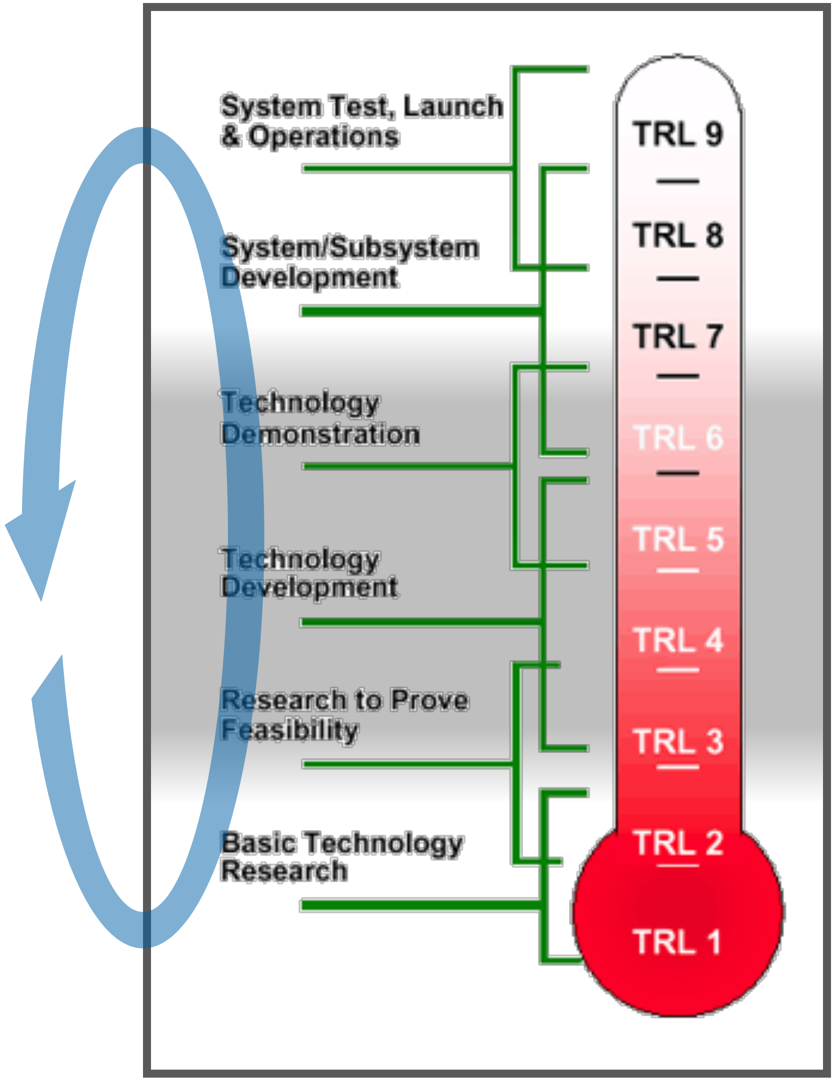
NWO

€1.9M

Developing a new Internet security and autonomy paradigm [9]

SIDN Labs and Technology Readiness Levels

SIDN Labs focuses on the **R** in R&D


System Test, Launch & Operations
System/Subsystem Development
Technology Demonstration
Technology Development
Research to Prove Feasibility
Basic Technology Research
TRL 9
TRL 8
TRL 7
TRL 6
TRL 5
TRL 4
TRL 3
TRL 2
TRL 1

Operations

Experimental

Fundamental research

https://en.wikipedia.org/wiki/Technology_readiness_level
O'Reilly, C. A., & Tushman, M. L. (2013). Organizational ambidexterity: Past, present, and future. Academy of Management Perspectives, 27(4), 324-338

Examples of our research partners

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

UNIVERSITEIT TWENTE.

UNIVERSITEIT VAN AMSTERDAM

ndix

TU Delft Delft University of Technology

SURF

IN·DEI·NOMINE·FELICITER
Radboud Universiteit Nijmegen

No More DDoS
Anti-DDoS-Coalitie

NBIP nationale beheersorganisatie internet providers

USC University of Southern California

ETH zürich

internetnz

NLNETLABS

TILBURG UNIVERSITY

amsix

UNIVERSITÉ Grenoble Alpes

afnic

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Our research in focus:

A lock with many keys:
Spoofing DNSSEC-signed domains in 8.8.8.8

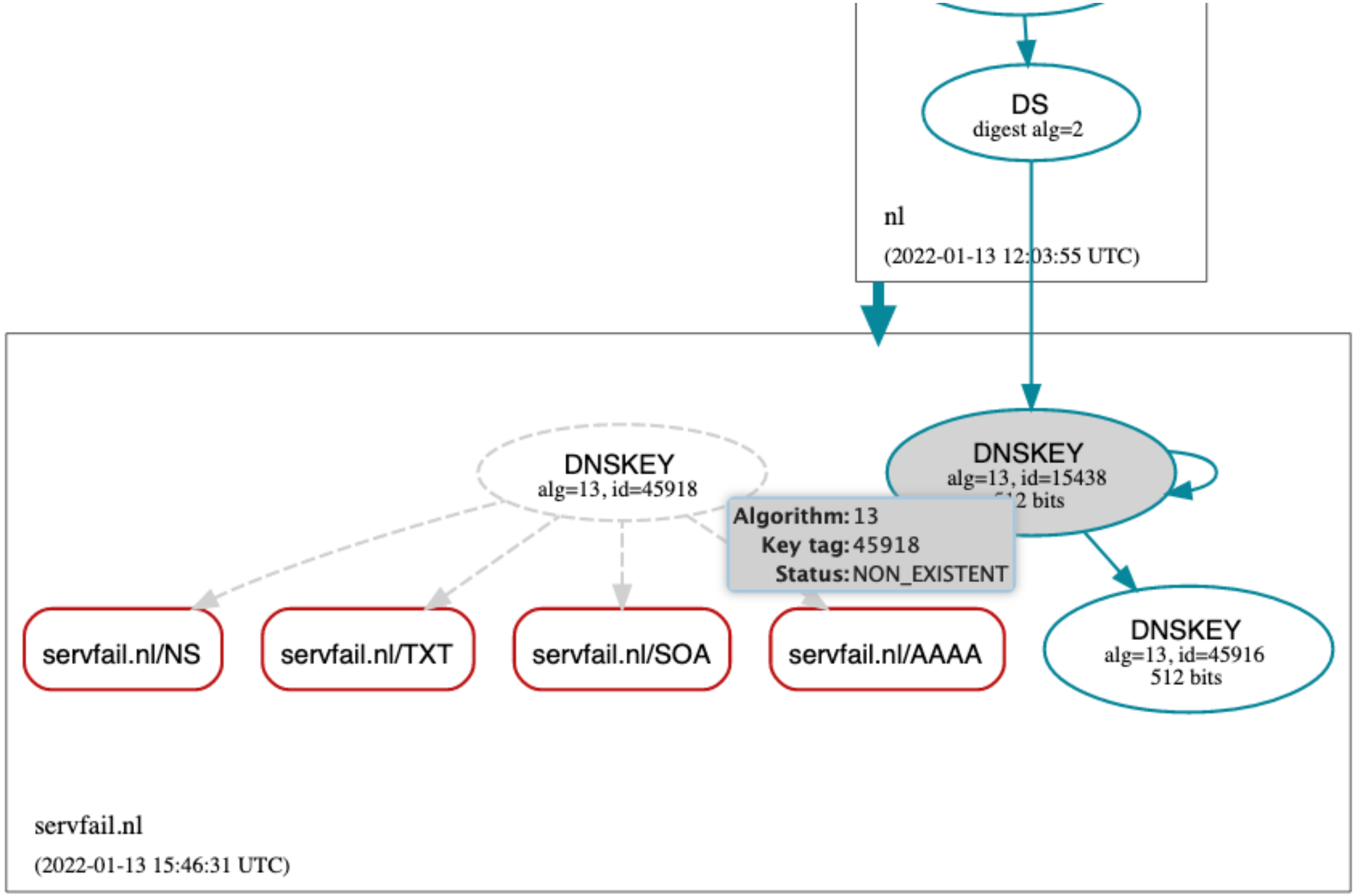
Potential impact

- Spoofing resource records of domain names, despite DNSSEC
- Found early January 2022, fixed by Google end of February

Where it all started

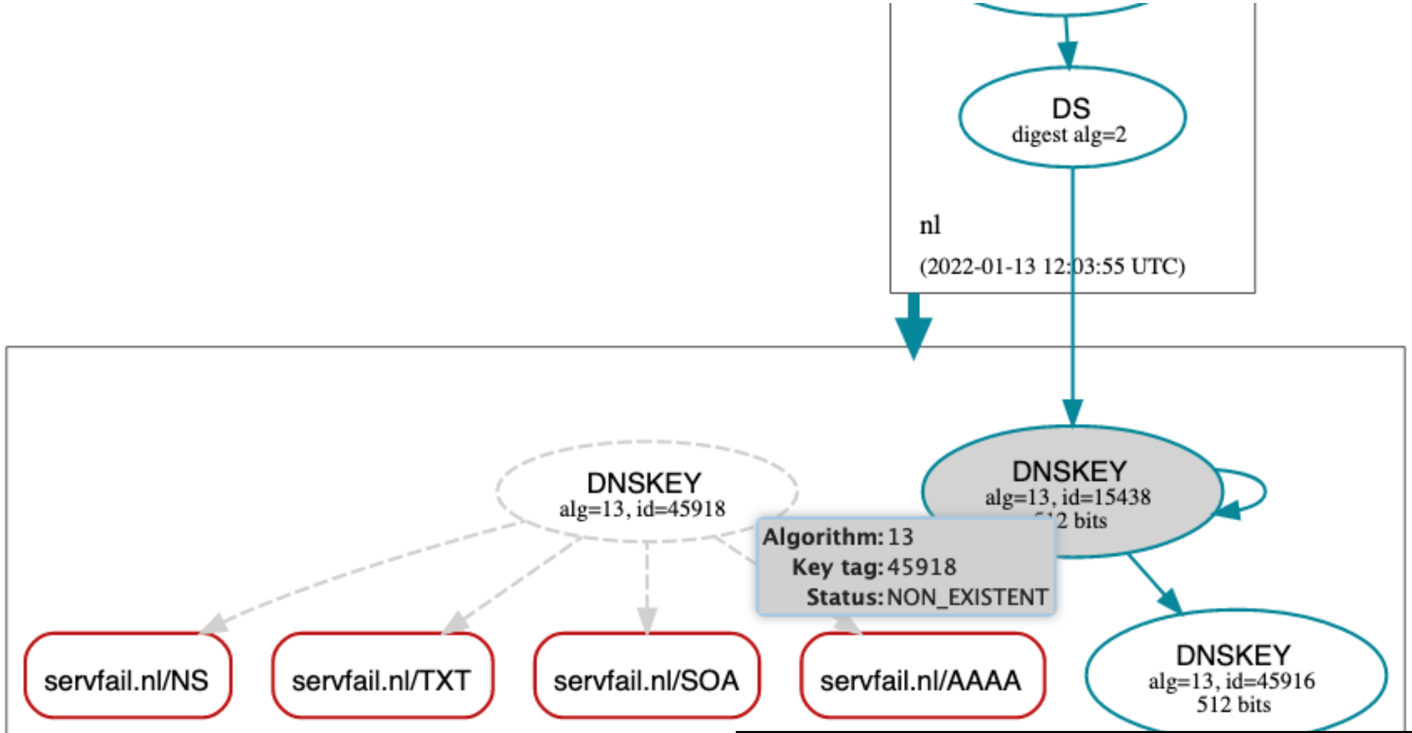
- Tinkering with servfail.nl
  - On purpose bogus domain name
  - Goal: make it bogus by signing records with non-existing key

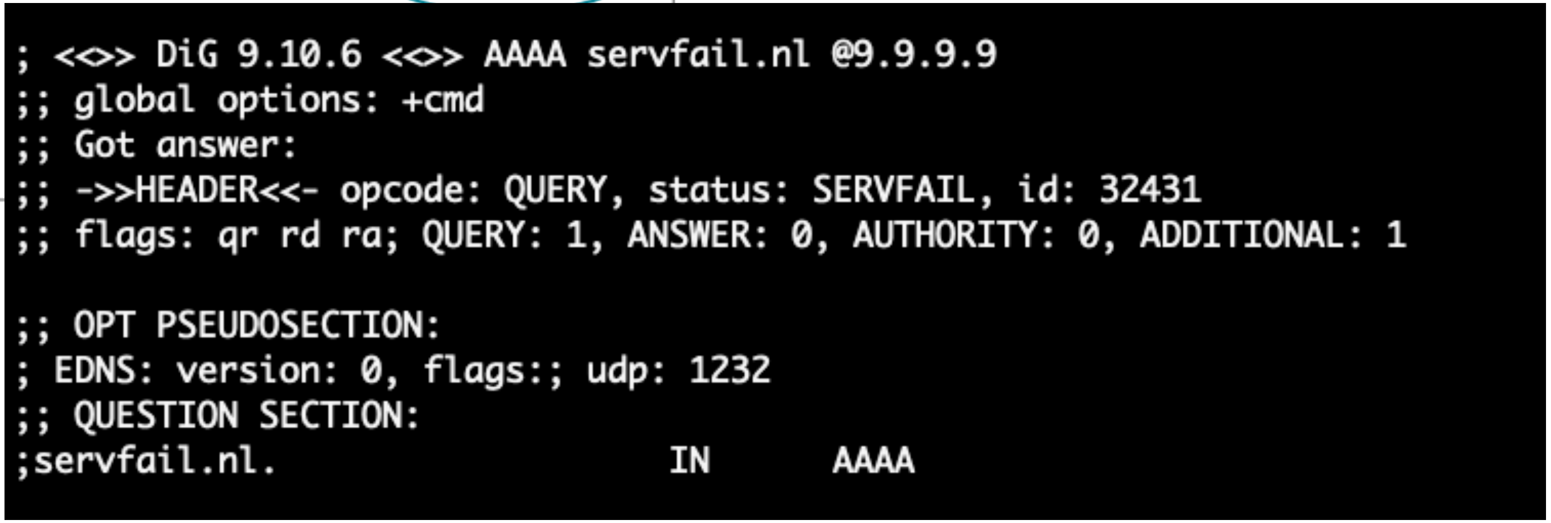
Where it all started



Algorithm: 13
Key tag: 45918
Status: NON_EXISTENT

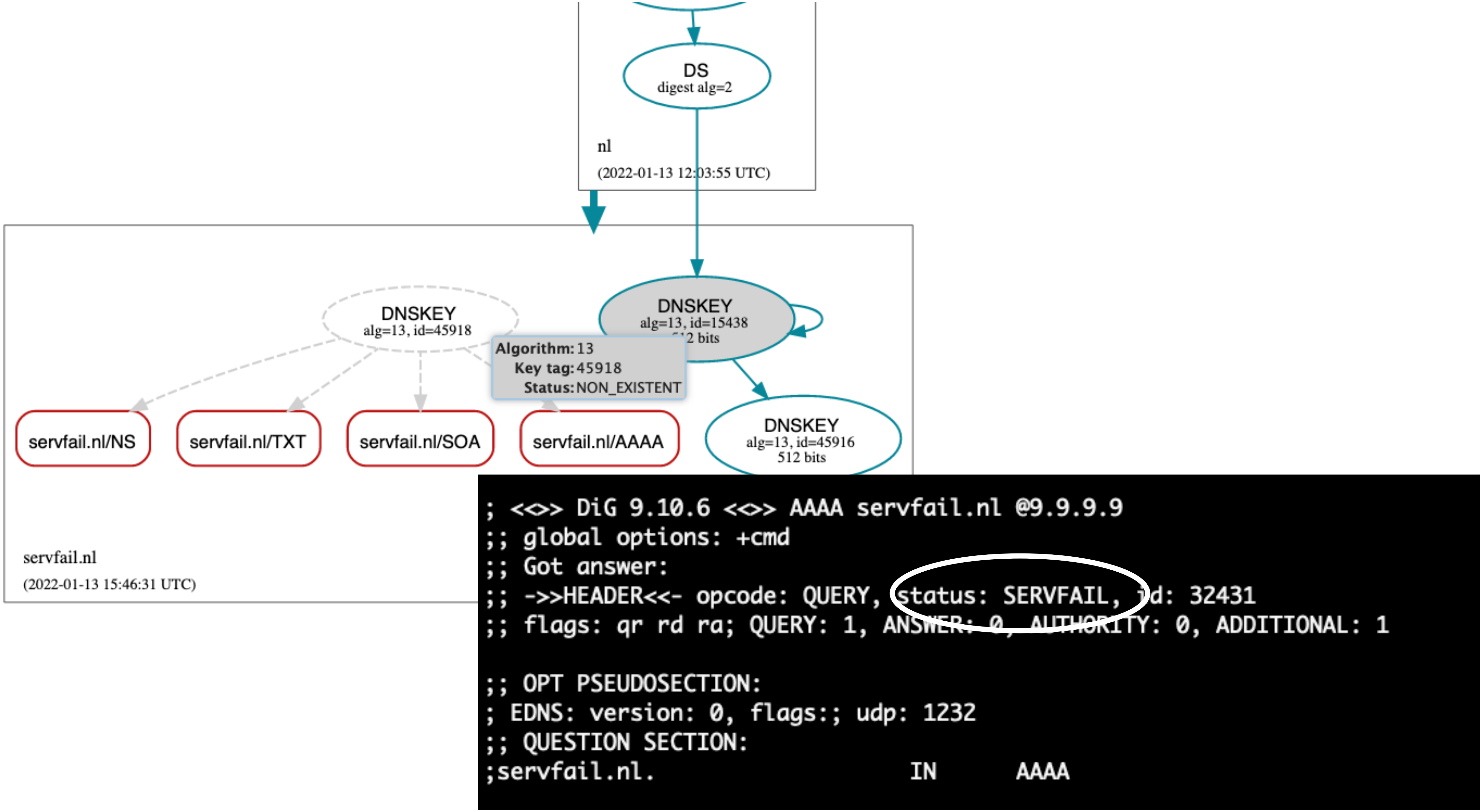
Where it all started





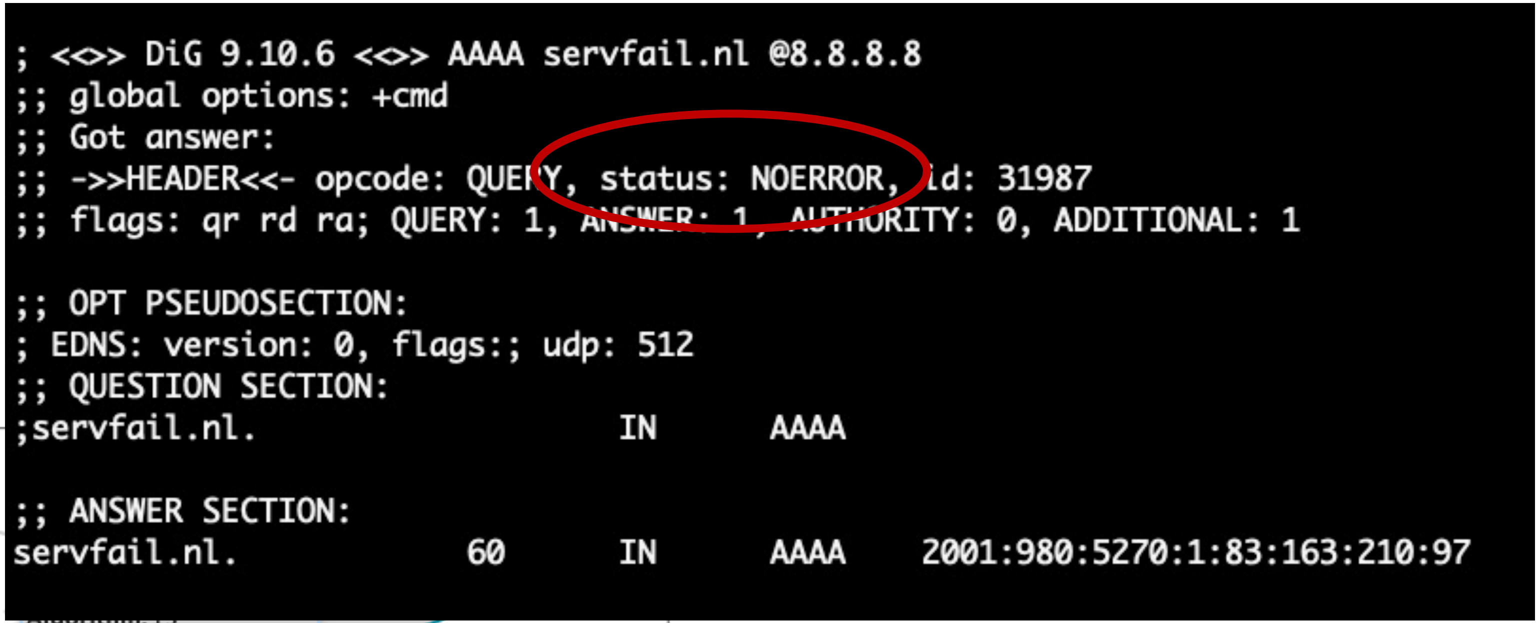
```
; <<>> DiG 9.10.6 <<>> AAAA servfail.nl @9.9.9.9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32431
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;servfail.nl.                   IN      AAAA
```

Where it all started

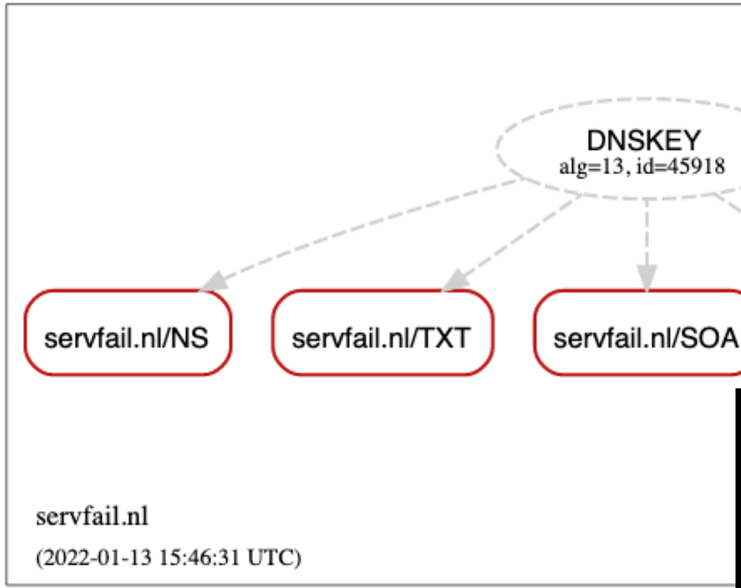


```
; <<>> DiG 9.10.6 <<>> AAAA servfail.nl @9.9.9.9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32431
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;servfail.nl.                   IN      AAAA
```

Where it all started

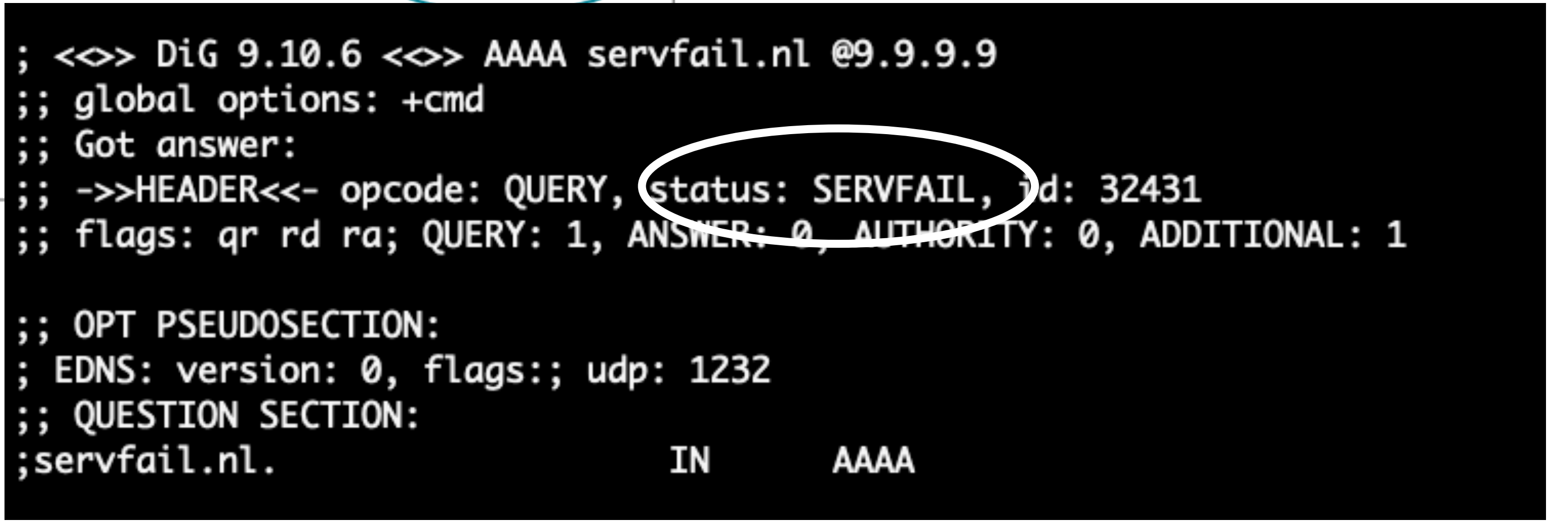


```
; <<>> DiG 9.10.6 <<>> AAAA servfail.nl @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31987
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;servfail.nl.                   IN      AAAA

;; ANSWER SECTION:
servfail.nl.            60      IN      AAAA    2001:980:5270:1:83:163:210:97
```



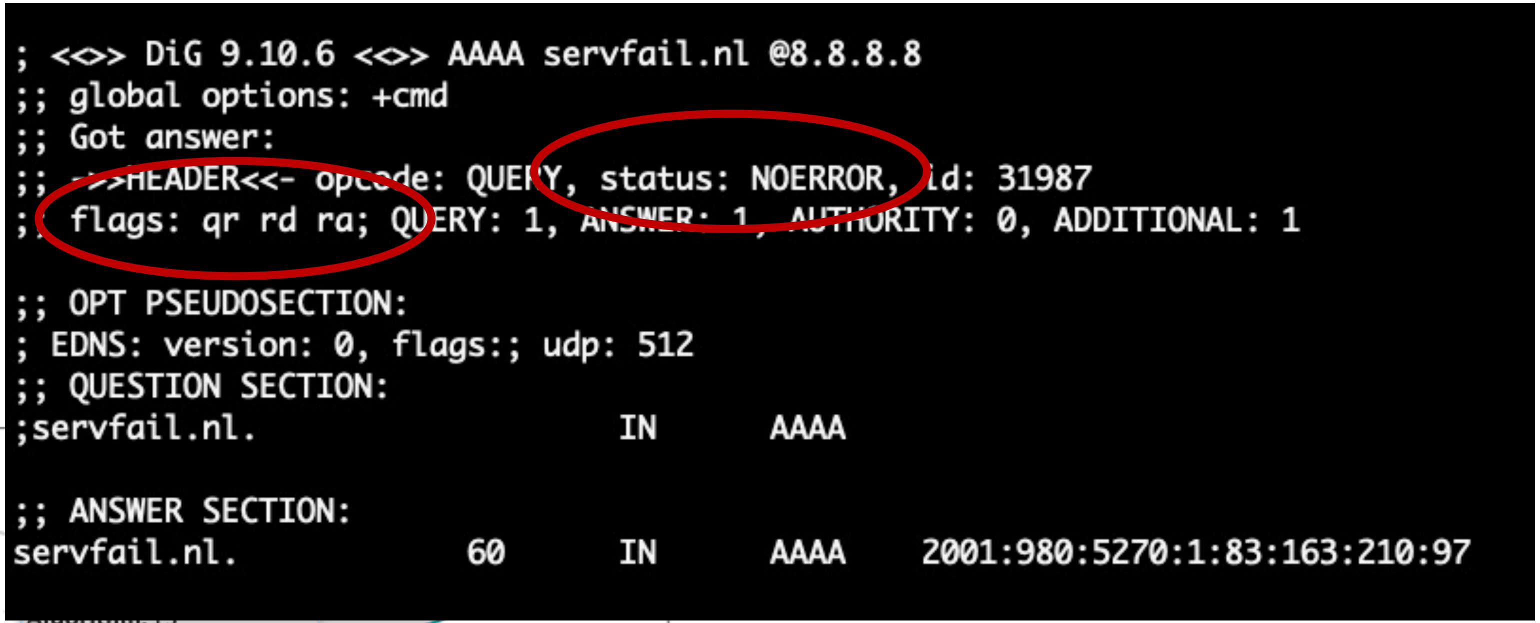
servfail.nl

(2022-01-13 15:46:31 UTC)

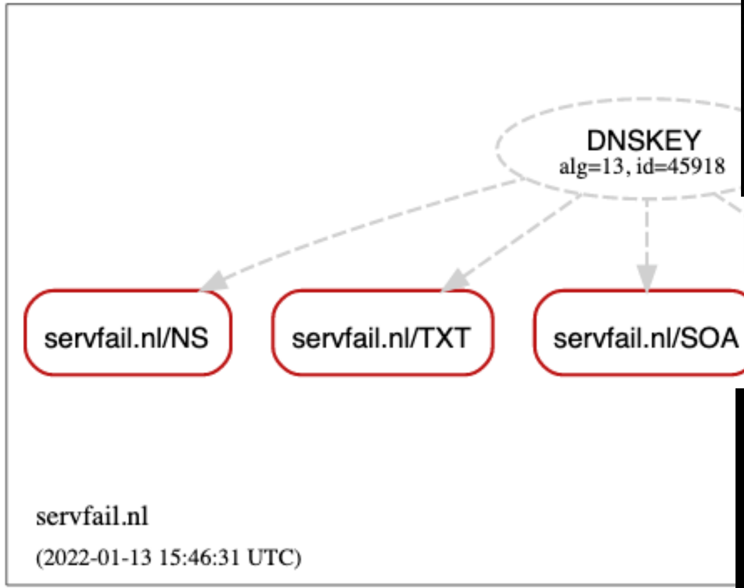


```
; <<>> DiG 9.10.6 <<>> AAAA servfail.nl @9.9.9.9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32431
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;servfail.nl.                   IN      AAAA
```

Where it all started

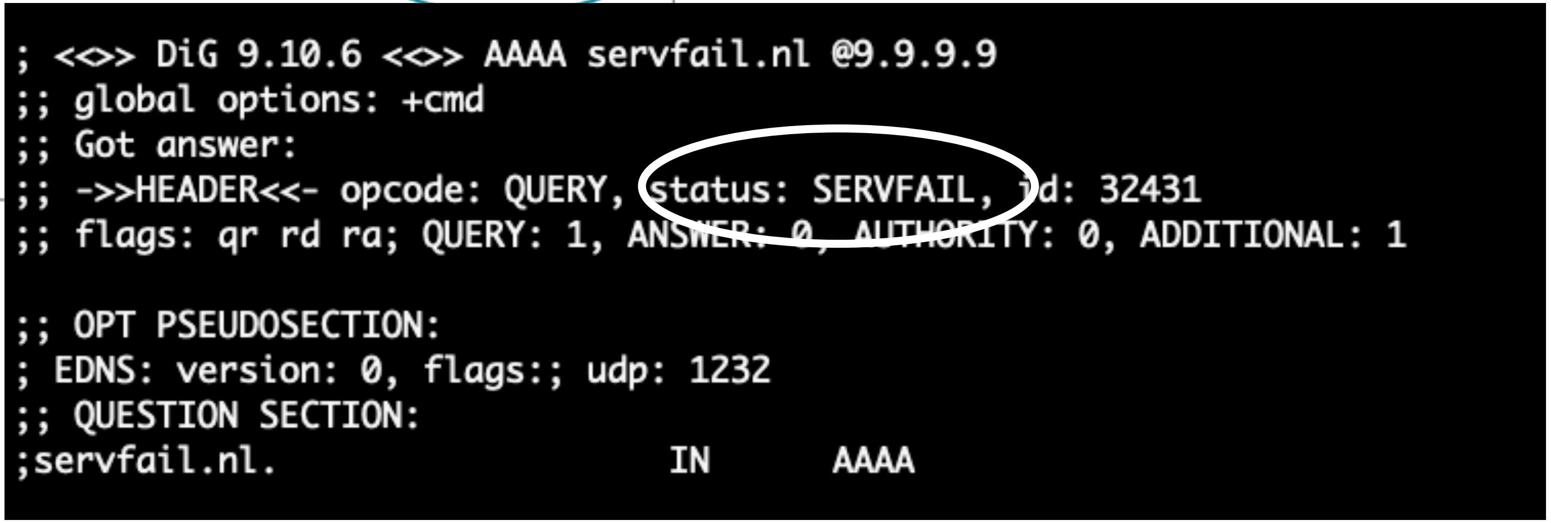


```
; <<>> DiG 9.10.6 <<>> AAAA servfail.nl @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31987
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;servfail.nl.                    IN      AAAA

;; ANSWER SECTION:
servfail.nl.            60      IN      AAAA    2001:980:5270:1:83:163:210:97
```



servfail.nl

(2022-01-13 15:46:31 UTC)



```
; <<>> DiG 9.10.6 <<>> AAAA servfail.nl @9.9.9.9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32431
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;servfail.nl.                    IN      AAAA
```

The attack, in theory

1. Create fake resource record of targeted and signed domain name
2. Create fake signature of the resource record, with non-existing key
3. Perform cache poisoning attack against Google Public DNS
   - Using spoofed malicious record
   - Using fake signature

The actual impact

- Google Public DNS likely the only affected resolver
- Google does not believe that it has been misused
- Fixed within 1 1/2 months

- Public disclosure: https://www.sidnlabs.nl/en/news-and-blogs/a-lock-with-many-keys-spoofing-dnssec-signed-domains-in-8-8-8-8

Takeaways

- DNSSEC is (still) hard with many corner cases, see also: https://github.com/PowerDNS/pdns/pull/11168
- Recommendation: rely on existing and established libraries and resolver software, when trying to implement DNSSEC

Photo by Maksym Kaharlytskyi on Unsplash

Volg ons

- SIDN.nl
- @SIDN
- SIDN

Q&A

www.sidnlabs.nl | stats.sidnlabs.nl

Moritz Müller
moritz.muller@sidn.nl | @moritzcm_