How and why of internet.nl

Sasha Romijn
sasha@mxsasha.eu

internet.nl genereert echt zoveel hoofdpijn omdat ze niet doorhebben hoe de echte wereld werkt.

— #nlnog, 2022

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

ik ben blij met internet.nl

— #nlnog, 2025

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Sasha Romijn (she/they)

- Independent developer
  - Internet routing/standards/ infrastructure
- IRRD, IRRexplorer
- RIPE open source wg co-chair
- Contractor for Internet.nl since 2022
- Many other "hobbies"
- Personal ASN 213279
- Not the government

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Platform internet-standaarden

- AKA Dutch internet standards platform
- "increase the use of modern Internet standards to make the Internet more accessible, safer and more reliable for everyone"

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Ministerie van Economische Zaken

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

NLNETLABS

nlnet FOUNDATION

Internet Society

SIDN

Forum Standaardisatie
Standaard Samenwerken

Dutch Cloud Community

VVR VERENIGING VAN REGISTRARS

National Cyber Security Centre
Ministry of Justice and Security

SURF

Internet.nl

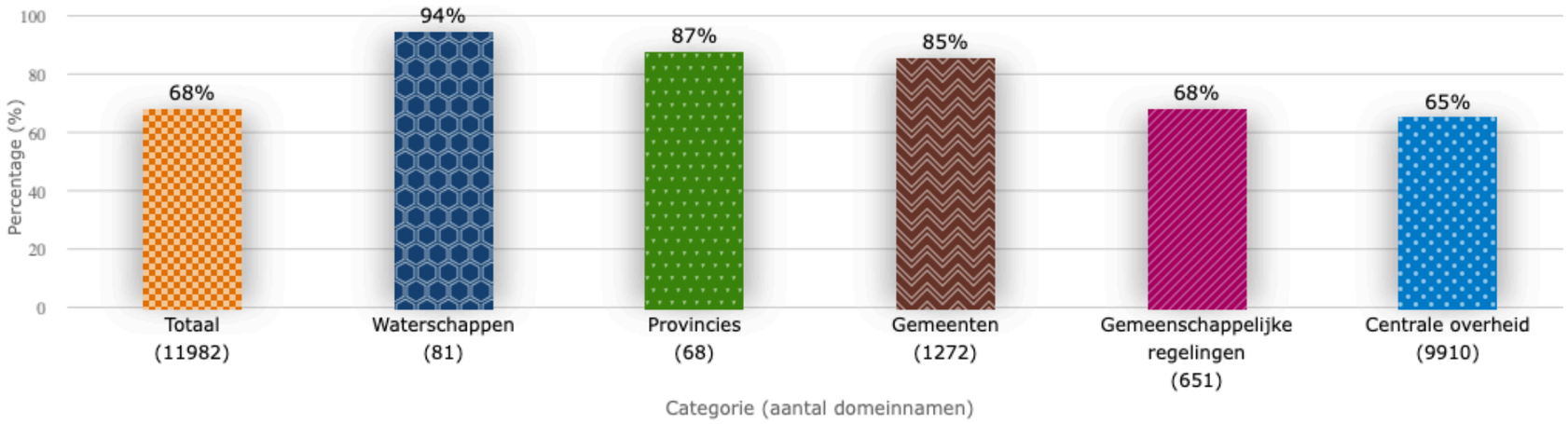
- Testing tool for *internet standards compliance*
  - not a security test
- Web server, mail server, client connection
- 2024: 1M tests
- Dashboard & API for certain groups
  - 8M tests in 2024
- Open source, docker, deploy your own!

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

4.1. IPv6 voor webverkeer per overheidscategorie

De gemeenschappelijke regelingen scoren lager bij het gebruik van IPv6 voor webverkeer. De overheidsbrede afspraken hebben onvoldoende doorwerking gehad naar deze instanties, ondanks dat zij meestal gefinancierd worden vanuit de andere overheden.

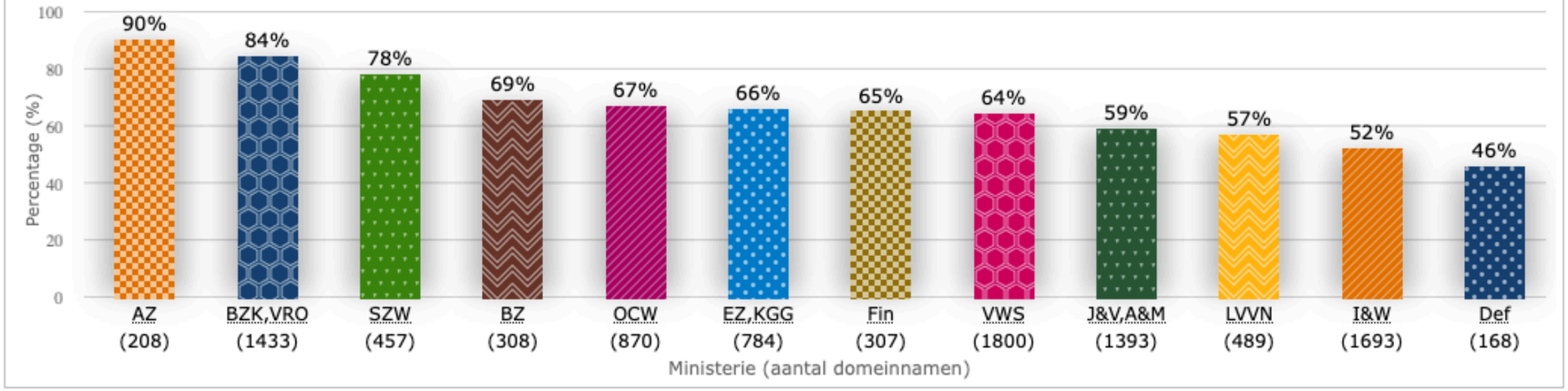
Grafiek 16: Volledige IPv6 adoptie voor webverkeer per overheidscategorie



4.2. IPv6 voor webverkeer per ministerie

Positieve uitschieters zijn de ministeries van Algemene Zaken (90%), Binnenlandse Zaken en Koninkrijksrelaties, Volkshuisvesting en Ruimtelijke Ordening (84%) en Sociale Zaken en Werkgelegenheid (78%). Negatieve opvaller is het ministerie van Defensie (46%), waarvan de websites het minst bereikbaar zijn via IPv6.

Grafiek 17: Volledige IPv6 adoptie voor webverkeer per ministerie



URL	Organisatietype	Organisatie	Suborganisatie	Afdeling	Bezoeken/mnd	Voldoet	Totaal	IPv6	DNSSEC	HTTPS	CSP	RefPol.	X-Cont.	X-Frame.	SecurityTxt	RPKI	Testdatum	Totaal	IPv6	DNSSEC	STARTTLS en DANE	DMARC	DK
http://www.rijksoverheid.nl	Rijksoverheid	AZ (Ministerie van Algemene Zaken)	DPC (Dienst Publiek en Communicatie)	Online Advies	8,469,602	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.knmi.nl	Rijksoverheid	IenW (Ministerie van Infrastructuur en Waterstaat)	KNMI (Koninklijk Nederlands Meteorologisch Instituut)		4,323,990	nee	ja	ja	ja	ja	waarschuwing	info	ja	ja	waarschuwing	ja	20-04-2025	nee	ja	ja	info	ja	nee
http://www.rivm.nl	Rijksoverheid	VWS (Ministerie van Volksgezondheid, Welzijn en Sport)	RIVM (Rijksinstituut voor Volksgezondheid en Milieu)		1,606,223	nee	ja	ja	ja	ja	waarschuwing	waarschuwing	ja	ja	info	ja	20-04-2025	nee	ja	ja	info	ja	nee
http://www.rijkswaterstaat.nl	Rijksoverheid	IenW (Ministerie van Infrastructuur en Waterstaat)	RWS (Rijkswaterstaat)		1,200,540	ja	ja	ja	ja	ja	waarschuwing	info	waarschuwing	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.examenblad.nl	Rijksoverheid	OCW (Ministerie van Onderwijs, Cultuur en Wetenschap)	CvTE (College voor Toetsen en Examens)		1,155,701	ja	nee	ja	ja	nee	waarschuwing	ja	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.nederlandwereldwijd.nl	Rijksoverheid	BZ (Ministerie van Buitenlandse Zaken)			1,147,899	ja	ja	ja	ja	ja	ja	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.defensie.nl	Rijksoverheid	DEF (Ministerie van Defensie)		Directie Communicatie	1,053,985	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.rwsverkeersinfo.nl	Rijksoverheid	IenW (Ministerie van Infrastructuur en Waterstaat)	RWS (Rijkswaterstaat)		989,007	ja	nee	nee	ja	nee	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.werkenvoornederland.nl	Rijksoverheid	BZK (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)	O&P Rijk (Organisatie en Personeel Rijk)	P-direkt	833,920	ja	nee	ja	ja	nee	waarschuwing	info	ja	ja	ja	nee	20-04-2025	ja	ja	ja		ja	
http://www.netherlandsworldwide.nl	Rijksoverheid	BZ (Ministerie van Buitenlandse Zaken)			809,642	ja	ja	ja	ja	ja	ja	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja	info	ja	
http://waterinfo.rws.nl	Rijksoverheid	IenW (Ministerie van Infrastructuur en Waterstaat)	RWS (Rijkswaterstaat)		690,172	ja	nee	nee	ja	ja	waarschuwing	info	ja	info	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.government.nl	Rijksoverheid	AZ (Ministerie van Algemene Zaken)	DPC (Dienst Publiek en Communicatie)	Online Advies	668,359	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.vananaarbeter.nl	Rijksoverheid	IenW (Ministerie van Infrastructuur en Waterstaat)		BSK/DCO	530,769	ja	nee	ja	nee	ja	waarschuwing	info	ja	ja	waarschuwing	ja	20-04-2025	nee	ja	nee	info	ja	nee
http://www.nationaalarchief.nl	Overheid	OCW (Ministerie van Onderwijs, Cultuur en Wetenschap)	NA (Nationaal Archief)		355,681		nee	ja	ja	nee	waarschuwing	waarschuwing	ja	ja	ja	ja	20-04-2025	nee	ja	ja	ja	ja	nee
http://www.coa.nl	Overheid	JenV (Ministerie van Justitie en Veiligheid)	COA (Centraal Orgaan opvang asielzoekers)		326,047		nee	ja	ja	ja	waarschuwing	info	ja	ja	ja	nee	20-04-2025	nee	ja	ja		ja	nee
http://www.nvwa.nl	Rijksoverheid	LVVN (Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur)	NVWA (Nederlandse Voedsel- en Warenautoriteit)		324,768	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://iplo.nl	Rijksoverheid	BZK (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)			313,764	ja	nee	ja	ja	nee	waarschuwing	waarschuwing			info	ja	20-04-2025	ja	ja	ja		ja	
http://www.geneesmiddeleninformatiebank.nl	Overheid	VWS (Ministerie van Volksgezondheid, Welzijn en Sport)	CBG (College ter Beoordeling van Geneesmiddelen)		285,104		ja	ja	ja	ja	waarschuwing	info	waarschuwing	info	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.om.nl	Overheid	JenV (Ministerie van Justitie en Veiligheid)	OM (Openbaar Ministerie)		284,664		ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.atlasleefomgeving.nl	Rijksoverheid	IenW (Ministerie van Infrastructuur en Waterstaat)		BSK/DGMI	241,773	ja	ja	ja	ja	ja	waarschuwing	waarschuwing	ja	info	waarschuwing	ja	20-04-2025	ja	ja	ja		ja	
http://rijksvaccinatieprogramma.nl	Rijksoverheid	VWS (Ministerie van Volksgezondheid, Welzijn en Sport)	RIVM (Rijksinstituut voor Volksgezondheid en Milieu)		226,422	nee	ja	ja	ja	ja	waarschuwing	waarschuwing	ja	ja	waarschuwing	ja	20-04-2025	nee	ja	ja	ja	nee	ja
http://www.koninklijkhuis.nl	Overheid	AZ (Ministerie van Algemene Zaken)	RVD (Rijksvoorlichtingsdienst)	CKH	220,860		ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.mijnpgb.nl	Rijksoverheid	VWS (Ministerie van Volksgezondheid, Welzijn en Sport)		Kerndepartement/PG	218,195	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.justis.nl	Rijksoverheid	JenV (Ministerie van Justitie en Veiligheid)	Justis		217,826	ja	nee	ja	ja	nee	waarschuwing	ja	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.denkvooruit.nl	Rijksoverheid	JenV (Ministerie van Justitie en Veiligheid)	NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid)		189,403	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.huurcommissie.nl	Overheid	BZK (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)	Huurcommissie		164,382		ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.caorlik.nl	Rijksoverheid	BZK (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)		DGOO/A&O	163,436	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.regelhulp.nl	Rijksoverheid	VWS (Ministerie van Volksgezondheid, Welzijn en Sport)		Kerndepartement/LZ	163,222	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.zorginstituutnederland.nl	Rijksoverheid	VWS (Ministerie van Volksgezondheid, Welzijn en Sport)	ZIN (Zorginstituut Nederland)		163,067	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.mycoa.nl	Overheid	JenV (Ministerie van Justitie en Veiligheid)	COA (Centraal Orgaan opvang asielzoekers)		159,947		ja	ja	ja	ja	waarschuwing	ja	ja	info	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.netherlandsandyou.nl	Rijksoverheid	BZ (Ministerie van Buitenlandse Zaken)			145,267	ja	nee	nee	nee	nee	waarschuwing	ja	ja	ja	ja	ja	20-04-2025	nee	ja	nee	info	ja	nee
http://www.schadedoormijnbouw.nl	Rijksoverheid	EZ (Ministerie van Economische Zaken)	IMG (Instituut Mijnbouwschade Groningen)		144,899	ja	nee	ja	nee	ja	waarschuwing	info	ja	info	ja	ja	20-04-2025	nee	ja	nee	info	ja	nee
http://www.arboportaal.nl	Rijksoverheid	SZW (Ministerie van Sociale Zaken en Werkgelegenheid)		DGW/G&VW	136,891	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.volkshuisvestingnederland.nl	Rijksoverheid	BZK (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)			126,319	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.p-direkt.nl	Rijksoverheid	BZK (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)	O&P Rijk (Organisatie en Personeel Rijk)	P-direkt	123,698	ja	ja	ja	ja	ja	waarschuwing	info	ja	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.verbeterjehuis.nl	Rijksoverheid	BZK (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)			123,197	nee	ja	ja	ja	ja	waarschuwing	info	ja	ja	waarschuwing	ja	20-04-2025	nee	ja	ja	info	waarschuwing	nee
http://werkenbij.rijkswaterstaat.nl	Rijksoverheid	IenW (Ministerie van Infrastructuur en Waterstaat)	RWS (Rijkswaterstaat)		121,532	ja	nee	nee	ja	ja	waarschuwing	info	waarschuwing	ja	ja	ja	20-04-2025	ja	ja	ja		ja	
http://www.justid.nl	Rijksoverheid	JenV (Ministerie van Justitie en Veiligheid)	Justid (Justitiële		118,490						waarschu						20-04-2025						

zien jullie ook allerlei klanten vragen hoe ze ROAs moeten maken voor hun PI/PA space nu internet.nl erover 'klaagt'?

— #nlnog, 2022

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

De enige keer dat ik bij huidige klant "ipv6" heb horen vallen was in een ticket "we moeten 100% bij internet.nl, en daar staat dat we eeh ipv6 dns of zo moeten doen, kunnen jullie dat even fixen ?"

— #nlnog, 2024

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Internet.nl test areas

- IPv6
- DNSSEC
- HTTPS
- HTTP security headers+security.txt
- DMARC+DKIM+SPF
- STARTTLS+DANE
- RPKI

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

But, what to test, to which criteria?

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Good or bad?

Domain has 3 NS. Two have an IPv6 address. One of those is unreachable.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Good or bad?

Domain has 3 NS. Two have an IPv6 address. They respond, but only over TCP.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Good or bad?

TLS 1.2 with TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Good or bad?

TLS 1.1 with TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Good or bad?

The web server IP is covered by one BGP announcement. There is no matching ROA.

Good or bad?

- The web server IP is covered by two BGP announcements.
- The most specific route has a ROA.
- A less specific route does not.

Who decides what we test?

Ideally, clear consensus with existing normative references. To some degree with local bias.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

References

- IETF RFC/BCP
- CA/Browser forum
- Netherlands Standardisation Forum
  - Comply-or-explain or Streefbeeldafspraken
- Dutch NCSC
- Dutch law
  - Besluit beveiligde verbinding met overheidswebsites en -webapplicaties
- Industry convention

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

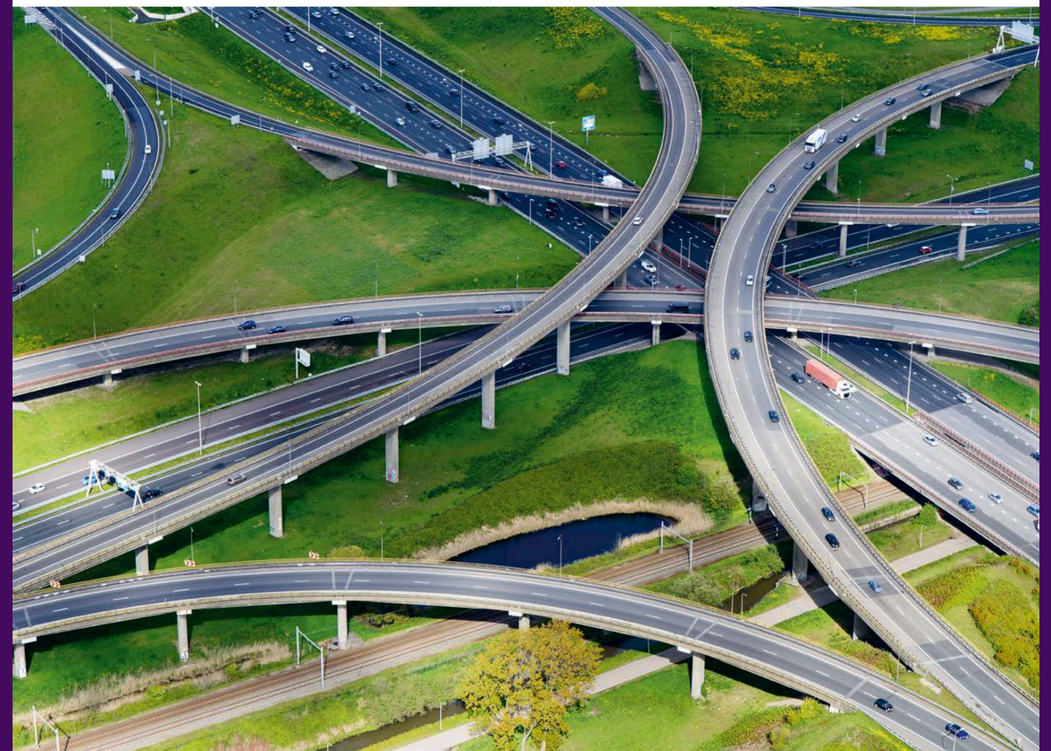
And, must be possible to test:

- Remotely
- In reasonable time and resources
- Without special privileges
- Without harming the test target
- Consistently

… most of the time

National Cyber Security Centre
Ministry of Justice and Security

IT Security Guidelines for Transport Layer Security (TLS)



(2021)

- 2025
- Based on BCP 195
  - RFC 8996: Deprecating TLS 1.0 and TLS 1.1
  - RFC 9325: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
- CA/Browser forum
- Existing work from BSI, NIST, NÚKIB, UK NCSC

Het is een van de latest internet.nl fads he. Groene vinkjes. DNSSEC, DANE, SPT, DKIM, DMARC, … ;)

— #nlnog, 2024

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

DNSSEC - RFC 4033 & more (2005)

- Domain Name System Security Extensions.
- Already has very wide support, misconfigurations happen a lot.
- We check whole chain, following CNAME.

SPF - RFC 7208 (2014)

- TXT record.
- Which hosts can send email.
- Lookup limit!

```
example.com. IN TXT "v=spf1 mx a -all"
```

DKIM - RFC 6376 (2011)

- Email signatures authenticated through DNS.
- TXT record under selector key.
- How do we find your selector? We don't ;)

```
selector._domainkey.example.com. IN  TXT
                                ("v=DKIM1; p=MI...AB")
```

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

DMARC - RFC 7489 (2015)

- Builds on SPF and DKIM.
- Detailed policy on SPF/DMARC success/fail.
- Reporting options

```
_dmarc IN TXT "v=DMARC1;
  p=reject;
  rua=mailto:dmarc-feedback@example.net;
  ruf=mailto:auth-reports@example.net"
```

Good or bad?

```
_dmarc.example.com. TXT "v=DMARC1; p=none;
ruf=mailto:dmarc@example.com,ftp://ftp.example.com"
```

DANE - RFC 6698 (2012)

- DNS-Based Authentication of Named Entities
- TLSA records, forcing TLS.
- Optional in web, important in mail.

```
_25._tcp.example.org TLSA (
      3 1 1 308203073082201efa003020102020... )
```

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

CAA - RFC 8657/8659 (2019)

- Certification Authority Authorization
- Restrict issue of certificates

```
mtg.ripe.net.          86400   IN  CAA 0 issue ";"
mtg.ripe.net.          86400   IN  CAA 0 issuewild ";"
```

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

HTTP security headers

- `Content-Security-Policy`: allowlist of various types of content.
- `Referrer-Policy`: restrict browsers passing referrer headers.
- `security.txt`: security contact info.
- `X-Frame-Options`: CSP fallback for frame embedding.
- `X-Content-Type-Options`: disable content type guessing.

These are mostly recommended, i.e. no score impact.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Standards are not always as clear as we might hope.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

security.txt

> Section 2.5.2 contains the definition of the
> Canonical field. I am not sure how to interpret
> this in the event of a HTTP redirect?

It is vague intentionally as per section 5.2.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Certificate Authority Authorization

RFC 8659 4.4. CAA iodef Property

http or https:
The IODEF report is submitted as a web service request to the HTTP address specified *using the protocol specified in [RFC6546]*.

RFC 6546

RFC6546: Transport of Real-time Inter-network Defense (RID) Messages HTTP/*TLS*

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

spftrace internet.nl

```
├   "v=spf1 a include:spfinc.prolocation.net ~all"
├── a → internet.nl (lookups: 1/10)
│   └── 62.204.66.10
├   not-match
├── include:spfinc.prolocation.net → spfinc.prolocation.net (lookups: 2/10)
│   spfinc.prolocation.net
│   ├   "v=spf1 mx ip4:94.228.133.0/24 ip4:94.228.129.0/24 ip6:2a00:d00:ff:129::/64
│   │    ip6:2a00:d00:ff:133::/64 -all"
│   ├── mx → spfinc.prolocation.net (lookups: 3/10, nested: 3/10)
│   │   ├── vmx01.prolocation.nl
│   │   │   └── 94.228.142.130
│   │   ├── vmx03.prolocation.net
│   │   │   └── 94.228.129.7
│   │   └── vmx02.prolocation.nl
│   │       └── 94.228.142.131
│   ├   not-match
│   ├── ip4:94.228.133.0/24 not-match
│   ├── ip4:94.228.129.0/24 not-match
│   ├── ip6:2a00:d00:ff:129::/64 not-match
│   ├── ip6:2a00:d00:ff:133::/64 not-match
│   └── all match result=fail
├   not-match
└── all match result=softfail
```

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Key challenges

- Many standards have rough edges.
- Many implementations are slightly wrong.
- People do strange things on the internet.
- We communicate to a widely diverse backgrounds.
- Some standards are essential but hard to test.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

"Easy"

- RPKI
- DNSSEC
- NS connectivity
- SPF
- DMARC

Medium

- HTTPS
- HTTP headers
- DKIM

Hard

- Mail TLS

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

TLS has no method to communicate the config

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

I definitely absolutely do not have rate limiting on my mail server, the test is broken.

— *person who absolutely has bizarrely strict rate limiting on mail*

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

All our work is open source, and we try to give back to others.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Verification may be falsely rejected when root cert has authorityCertIssuer field #11461

New issue

Closed #11462

mxsasha opened on Aug 20, 2024 · edited by mxsasha

Edits

Cryptography's x509 verification appears to reject verification on a certificate when the authorityCertIssuer field is present in the authority key identifier extension of the root certificate. This may be correct per CABF baseline, but is suspiciously different from all other implementations I tested.

I have written a small script that isolates the issue. This fails on `cryptography.hazmat.bindings._rust.x509.VerificationError: validation failed: CandidatesExhausted(Other("authorityKeyIdentifier must not contain authorityCertIssuer"))`. The leaf and intermediate do not contain authorityCertIssuer - the root does.

The error message originates in the code here. This code seems to have an exception that allows the authority key identifier extension to be absent, but if it is found, the presence of authorityCertIssuer will lead to an error.

This is a widely trusted root certificate, and no browsers and other testing tools don't seem to have an issue with it. I do see the CABF baseline does not allow authorityCertIssuer. But this was introduced in 2020, the root certificate is from 2006. Perhaps there are other details I don't know - I'm not too familiar with these policies and their implementations. It definitely seems strange and undesirable that cryptography rejects a certificate where other implementations find it valid.

It would be great if someone with more experience in this area could look at this and determine if cryptography is too strict in

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Fix typo in SSL_get_shared_sigalgs docs #26151

New issue

Closed **mxsasha** wants to merge 1 commit into `openssl:master` from `mxsasha:patch-2`

Conversation 4 Commits 1 Checks 80 Files changed 1 +1 −1

mxsasha commented on Dec 11, 2024 Contributor

psighash -> psignhash

CLA: trivial

Fix typo in SSL_get_shared_sigalgs docs ... Verified 1c2d058

t8m approved these changes on Dec 11, 2024 View reviewed changes

t8m commented on Dec 11, 2024 Member

OK with CLA: trivial

t8m added branch: master approval: review pending triaged: documentation branch: 3.0 branch: 3.1

Reviewers
t8m
paulidale

Assignees
No one assigned

Labels
approval: ready to merge branch: master branch: 3.0 branch: 3.1 branch: 3.2 branch: 3.3 branch: 3.4 tests: exempted triaged: documentation

Projects
None yet

We are not

But we do appreciate, refer and cross-check.

- DNSviz
- Zonemaster
- IRRexplorer
- email-security-scans.org
- SSL labs
- RIPE Atlas
- NLNOG RING
- …

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

What if you don't like our tests or criteria?

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Internet.nl is not mandatory except perhaps partially for some scenarios.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

We are always happy to hear from you on ***question@internet.nl***

Preferably with substantiated views and references.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

A

The entire government scores 100% on internet.nl, as everything runs on $BIGCLOUD, which meets all requirements.

B

All government mail is self-hosted through diverse providers but has DHE enabled on TLS.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

My future ideas

- Design refresh, less 2000s
- Technical debt, like an improved database design for more clarity and better debugging data.
- "Tests" for data location.
- Improved scoring model: better representation of severity.

Sasha Romijn | sasha@mxsasha.eu | @sash@hachyderm.io | @mxsash.bsky.social

Thank you!

Sasha Romijn
sasha@mxsasha.eu
@sash@hachyderm.io
@mxsash.bsky.social