

Dutch Internet Standards Platform

DANE for SMTP

ir. Dennis Baaten CISSP

11-11-2021



Who are we?

- **Dutch Internet Standards Platform** is the organization behind the test tool Internet.nl.
- Collaboration between parties from the Internet community and the Dutch government (public / private).
- Our goal is to stimulate the adoption of modern internet standards.





Stimulating adoption of standards

We do a lot of things to stimulate the adoption of standards. The most important and visible things are:

- It starts with our tool on <https://internet.nl>
 - Create insight and measure. Over 2000 tests per day.
 - Automatically generated Hall of Fame (web, email, champions).
 - Hall of Fame for Hosters (manual).
 - Our test norm is based on:
 - Internet Standards on the 'comply-or-explain' list of the Dutch Standardisation Forum.
 - Security advices of the Dutch NCSC.
 - Relevant RFC's of IETF.

The screenshot shows the Internet.nl website with the following content:

- Header:** Internet.nl logo with tagline "IS YOUR INTERNET UP TO DATE?". Navigation links: Home, News, Knowledge base, Hall of Fame, About Internet.nl. Language options: English, Nederlands.
- Main Banner:** "Modern Internet Standards provide for more reliability and further growth of the Internet. Are you using them?"
- Test Tools:** Three panels for "Test your website", "Test your email", and "Test your connection". Each panel includes a description of the test, a "Start test" button, and a link to "about the test".
- News:** A list of recent updates, including "New Internet.nl with improved tests for TLS and CSP" and "Launch of Hall of Fame for Hosters".
- Hall of Fame:** A section titled "Hall of Fame" with a "100%" badge, listing domains like "openateliersharen.nl" and "pubhubs.net" with their compliance status.
- Tests in numbers:** A summary of test results: 415699 unique web domains (100%: 14490, 0-99%: 401209), 164369 unique mail domains (100%: 5177, 0-99%: 159192), and 24033 unique connections (100%: 7656, 0-99%: 16377).
- Footer:** "Internet.nl is an initiative of the Internet community and the Dutch government." and links for "Report vulnerability", "Privacy statement", "Copyright", "Accessibility", and "Follow us on Twitter".



Stimulating adoption of standards

We do a lot of things to stimulate the adoption of standards. The most important test results are:

- It starts with...
- Create...
- Automate...
- champion...
- Hall of Fame for Hosters (manual).
- Our test norm is based on:
 - Internet Standards on the 'comply-or-explain' list of the Dutch Standardisation Forum.
 - Security advices of the Dutch NCSC.
 - Relevant RFC's of IETF.

Email test: [redacted]

Congratulations, your domain will be added to the **Hall of Fame** soon!

100%

- ✓ Reachable via modern internet address (IPv6)
- ✓ All domain names signed (DNSSEC)
- ✓ Authenticity marks against email phishing (DMARC, DKIM and SPF)
- ✓ Mail server connection sufficiently secured (STARTTLS and DANE)

[Explanation of test report](#)

[Permalink test result \(2021-11-10 11:43 CET\)](#)

Seconds until retest option: 148

[Tweet](#)

Secure mail server connection (STARTTLS and DANE)

Well done! Sending mail servers supporting secure email transport (STARTTLS and DANE) can establish a secure connection with your receiving mail server(s). STARTTLS prevents passive attackers from reading emails in transit to you. DANE protects against active attackers stripping STARTTLS encryption by manipulating the mail traffic.

[Show details](#)

TLS

- ✓ STARTTLS available
- ✓ TLS version
- ✓ Ciphers (Algorithm selections)
- ✓ Cipher order
- ✓ Key exchange parameters
- ✓ Hash function for key exchange
- ✓ TLS compression
- ✓ Secure renegotiation
- ✓ Client-initiated renegotiation
- ✓ 0-RTT

Certificate

- ✓ Trust chain of certificate
- ✓ Public key of certificate
- ✓ Signature of certificate
- ✓ Domain name on certificate

DANE

- ✓ DANE existence
- ✓ DANE validity
- ✓ DANE rollover scheme

English Nederlands

[Home](#) [News](#) [Knowledge base](#) [Hall of Fame](#) [About Internet.nl](#)

provide for more reliability and further growth of the Internet.
Are you using them?

Test your email

Modern address? Signed domain? Anti-phishing? Secure connection?

[about the test >](#)

Your email address:

example.nl

[Start test](#)

Test your connection

Modern addresses reachable? Domain signatures validated?

[about the test >](#)

Hall of Fame

105 domains with 2 x 100% test entry: 09-11-2021

[openateliersharen.nl](#)

[pubhubs.net](#)

[www.zakaria.website](#)

[zakaria.website](#)

[www.rijksictdashboard.nl](#)

[werkenbijdesvb.nl](#)

[investarholding.nl](#)

[i24.nl](#)

[beherit.pl](#)

[verkiezingsuitslagen.nl](#)

[to hall of fame - champions! >](#)

Tests in numbers

415699 unique web domains

- ✓ 100%: 14490
- ✗ 0-99%: 401209

164369 unique mail domains

- ✓ 100%: 5177
- ✗ 0-99%: 159192

24033 unique connections

- ✓ 100%: 7656
- ✗ 0-99%: 16377

and the Dutch government.

Accessibility

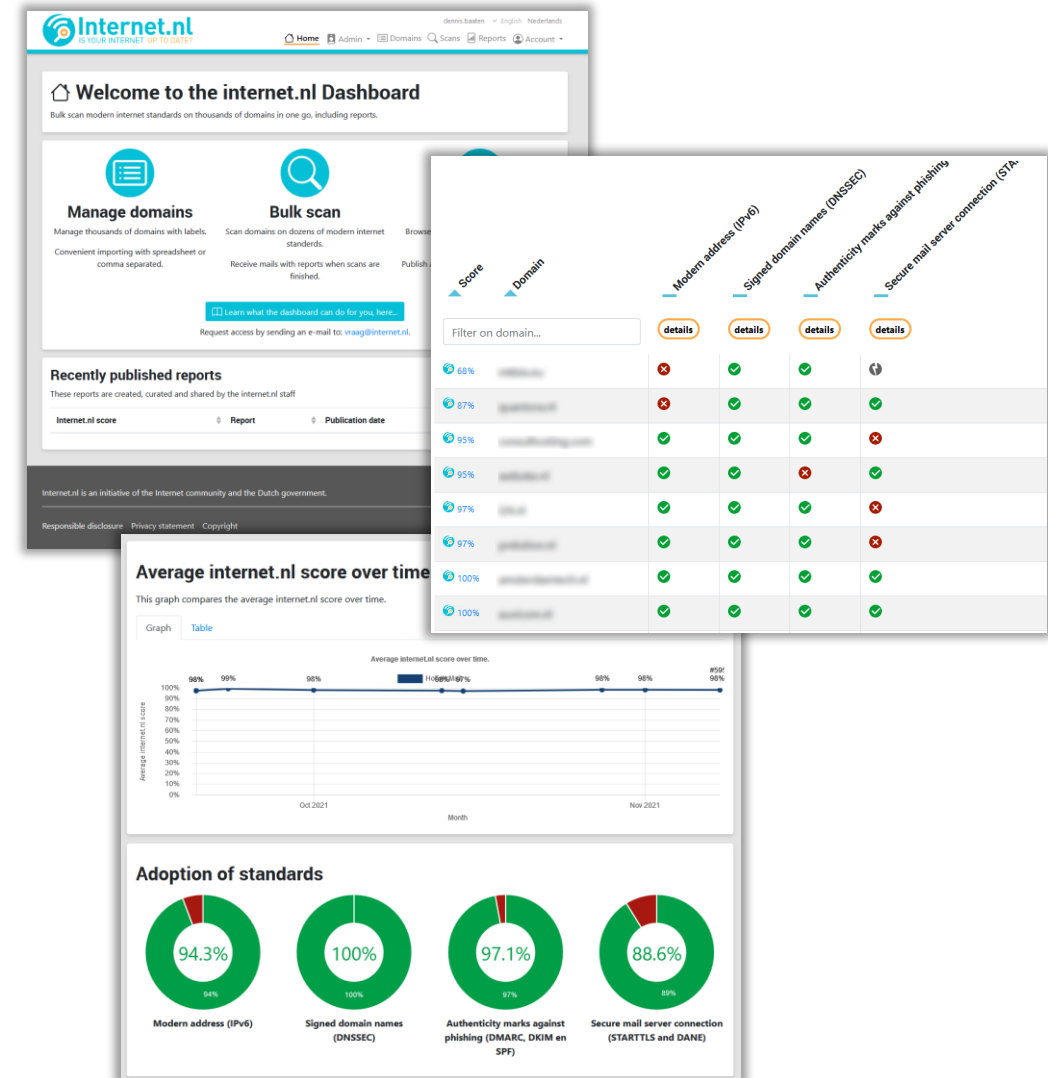
[Follow us on Twitter](#)



Stimulating adoption of standards

We do a lot of things to stimulate the adoption of standards. The most important and visible things are:

- API for bulk testing
 - JSON based REST-like API
 - OpenAPI specification: <http://redocly.github.io/redoc/?url=https://batch.internet.nl/api/batch/openapi.yaml>
 - Available for:
 - Platform members.
 - Government- and not-for-profit organizations.
 - Members of the Dutch Cloud Community (<https://dutchcloudcommunity.nl/>).
 - Members of VvR (<https://www.verenigingvanregistrars.nl/>).
- Dashboard (a GUI for the API).
 - Tracking changes over time.
 - Adoption statistics.





Stimulating adoption of standards

We do a lot of things to stimulate the adoption of standards. The most important and visible things are:

- All tools are open source (GitHub)
 - <https://github.com/internetstandards>
 - Used by several other countries, like the Danish:
<https://sikkerpa nettet.dk/>.
- Active on social media
 - https://mobile.twitter.com/internet_nl.
 - <https://www.linkedin.com/company/internet-nl/>.

The screenshot shows the GitHub profile page for 'Platform Internetstandaarden / Internet Standards Platform'. The profile is verified and located in 'The Netherlands / Europe'. It has 10 repositories. The 'Pinned' section features six repositories: 'Internet.nl' (Python, 70 stars, 25 forks), 'Internet.nl-dashboard' (JavaScript, 4 stars, 7 forks), 'Internet.nl-dashboard-frontend' (Vue, 1 star), 'toolbox-wiki' (67 stars, 14 forks), 'dhe_groups' (6 stars, 1 fork), and 'Internet.nl-API-docs' (2 stars). The 'Repositories' section lists the same six repositories with their respective details, including issue counts and update times.



Stimulating adoption of standards

We do a lot of things to stimulate the adoption of standards. The most important and visible things are:

- Create how-to's for making implementation of standards as easy as possible
 - <https://toolbox.internet.nl> (redirect to GitHub repo)
 - A continuous process: how-to's are 'living documents' and never finished.
 - Lesson learned: difficult to get people to contribute.
 - Feel free to contribute!

The screenshot shows the GitHub repository for 'internetstandards / toolbox-wiki'. The repository is public and has 67 stars and 14 forks. The main branch is 'master' with 1 branch and 0 tags. The repository contains several files and folders, including 'DANE-for-SMTP-how-to.md', 'DKIM-how-to.md', 'DMARC-how-to.md', 'LICENSE-CC-BY-4.0.txt', 'README.md', 'SPF-how-to.md', and 'parked-domain-how-to.md'. The repository description is 'Internet.nl toolbox - how-to's for modern mail security standards (DMARC, DKIM, SPF and DANE)'. The repository also has a README file, no releases published, and no packages published. The contributors section shows 5 contributors.

internetstandards / toolbox-wiki Public

<> Code Issues 2 Pull requests 2 Security Insights

master 1 branch 0 tags Go to file Code About

dennisbaaten Update DANE-for-SMTP-how-to.md 3c822e3 on 20 Sep 221 commits

File	Commit Message	Time Ago
TLS-config_spreadsheet	Add files via upload	6 months ago
images	improve layout	2 years ago
under construction	Delete 20210402_TLS-config_NCSC-NLods	7 months ago
DANE-for-SMTP-how-t...	Update DANE-for-SMTP-how-to.md	2 months ago
DKIM-how-to.md	Merge pull request #9 from cvdwel/patch-1	11 months ago
DMARC-how-to.md	layout improvements	2 years ago
LICENSE-CC-BY-4.0.txt	Add files via upload	2 years ago
README.md	Update README.md	2 years ago
SPF-how-to.md	Update SPF-how-to.md	8 months ago
parked-domain-how-t...	Update parked-domain-how-to.md	11 months ago

README.md

Welcome to the Internet.nl toolbox.

This GitHub repository contains several how-to's for providing practical information and guidance on implementing secure and modern Internet Standards. The how-to's are maintained by the Dutch Internet Standards Platform (the organization behind Internet.nl) and are created in cooperation with industry experts and enthusiasts (hosters, vendors, etc).

Feedback and/or contributions are much appreciated and welcome through issues, pull requests or via question@internet.nl.

Quick access

- DANE how-to
- DKIM how-to
- SPF how-to
- DMARC how-to
- Parked domain how-to



What we are working on

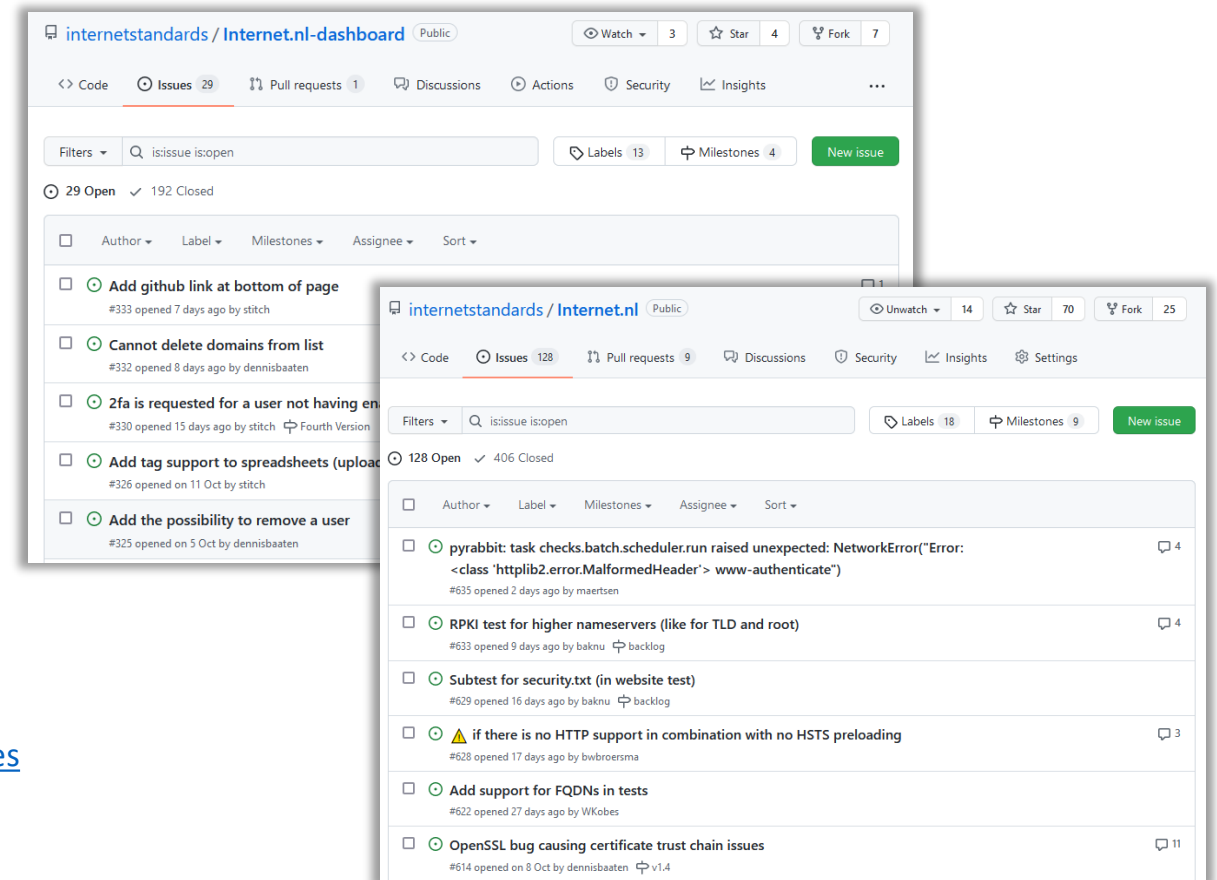
We are constantly seeking for ways to improve our platform and increase our value for our users.

- **Current/recent:**

- Minor improvements and bugfixes.
- Improving user feedback (test results).
- Maintain / create how-to's.
- New version (version 4) of our Dashboard
 - Public reports
 - Working with tags for domain names (great for filtering results)

- **New:**

- Looking into feasibility of an 'accessibility test'.
- Implementing RPKI check (increased BGP security).
- Interactive mail test for our API environment.
- See also: <https://github.com/internetstandards/Internet.nl/milestones>





One of the standards we are actively stimulating
is **DANE**.

So... let's look at DANE.



Why DANE?

- Our (public) email ecosystem is flawed by default.
- SMTP on its own cannot ensure integrity and confidentiality of email delivery.
- Several measures can and have been taken to improve, but are still not enough.
- Regarding email transport, DANE is the next and final step.



What is DANE?

DNS-based Authentication of Named Entities

RFC 6698 & RFC 7671

[DNS-Based Authentication of Named Entities (DANE) offers the option to use the DNSSEC infrastructure to store and sign keys and certificates that are used by TLS.]

In other words:

- Verifying certificates with information stored in a DNS record.
- No Certificate Authority (CA) needed.
- Using DNSSEC for authenticity and integrity.



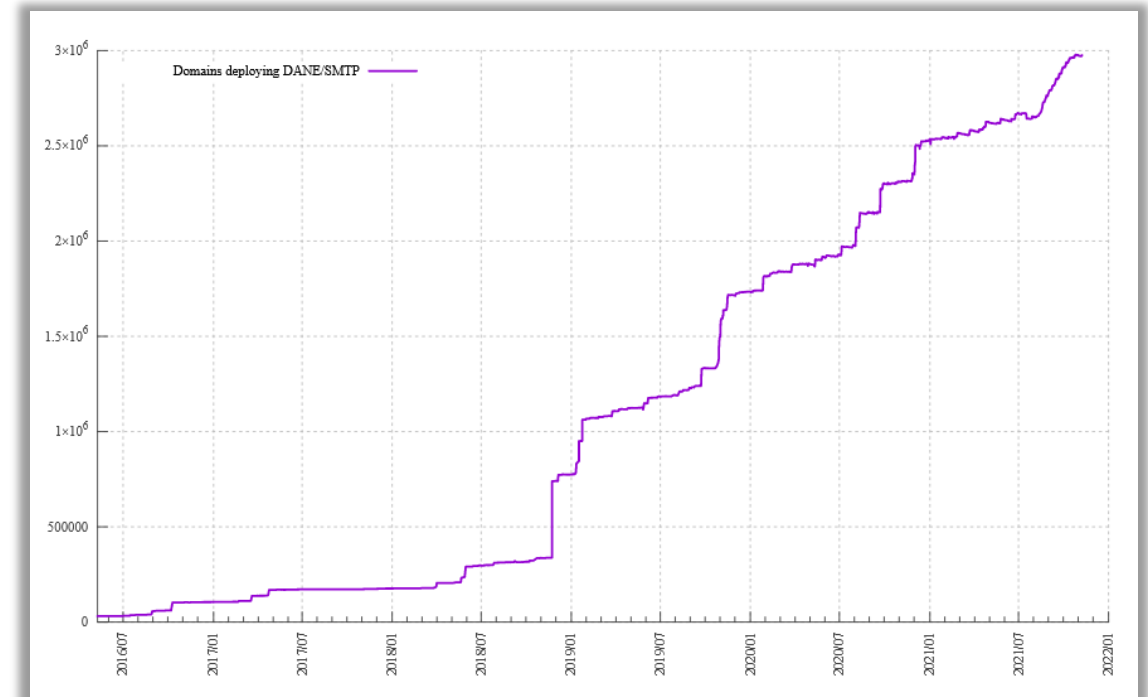
What is DANE?

DANE for web

- Not used due to lack of browser support.

DANE for SMTP

- Usages keeps increasing.
- Oct 2021: almost 3 million domains.

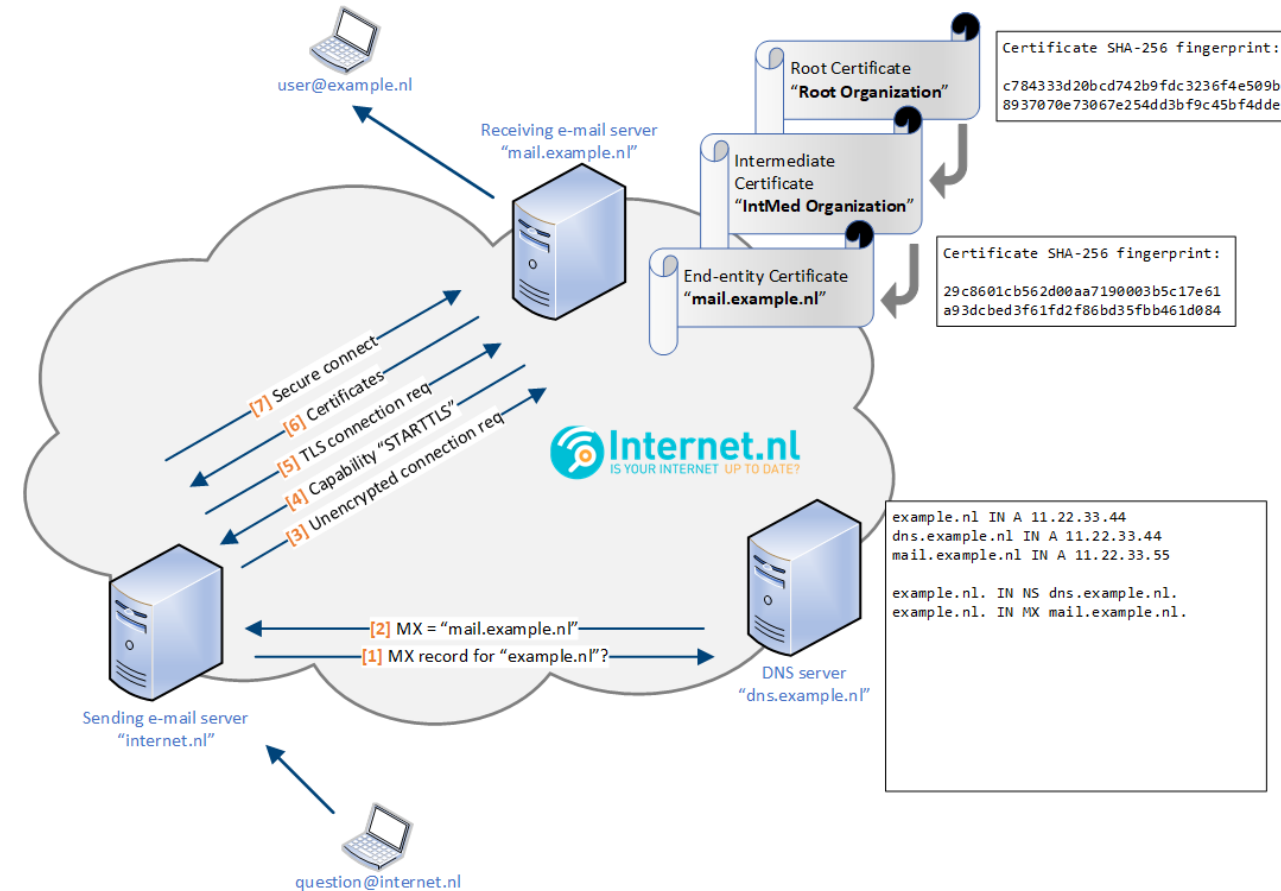




Risks mitigated by DANE

Using an encrypted SMTP connection based on STARTTLS still leaves email transport at risk:

- STARTTLS is **opportunistic**, which means that encryption is only used after being negotiated over an unencrypted connection.
- At the same time SMTP servers, by design, **do not validate the authenticity of another mail server's certificate**; any random certificate is accepted.

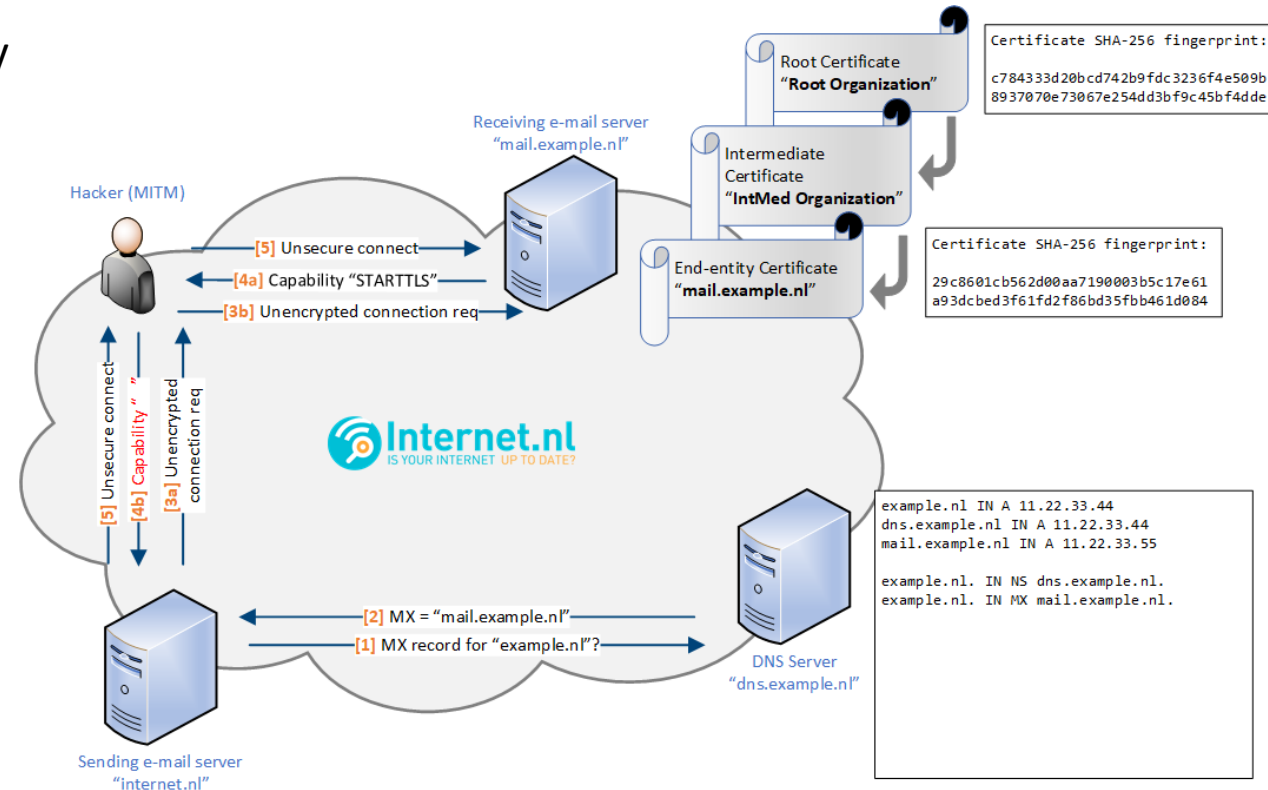




Risk 1: STRIPTLS / downgrade attack

The opportunistic character of SMTP makes it relatively easy for cybercriminals to circumvent the usage of encryption and force transfer of emails over an unencrypted connection.

Without the STARTTLS capability, the sending server will proceed to transport the e-mail unencrypted.

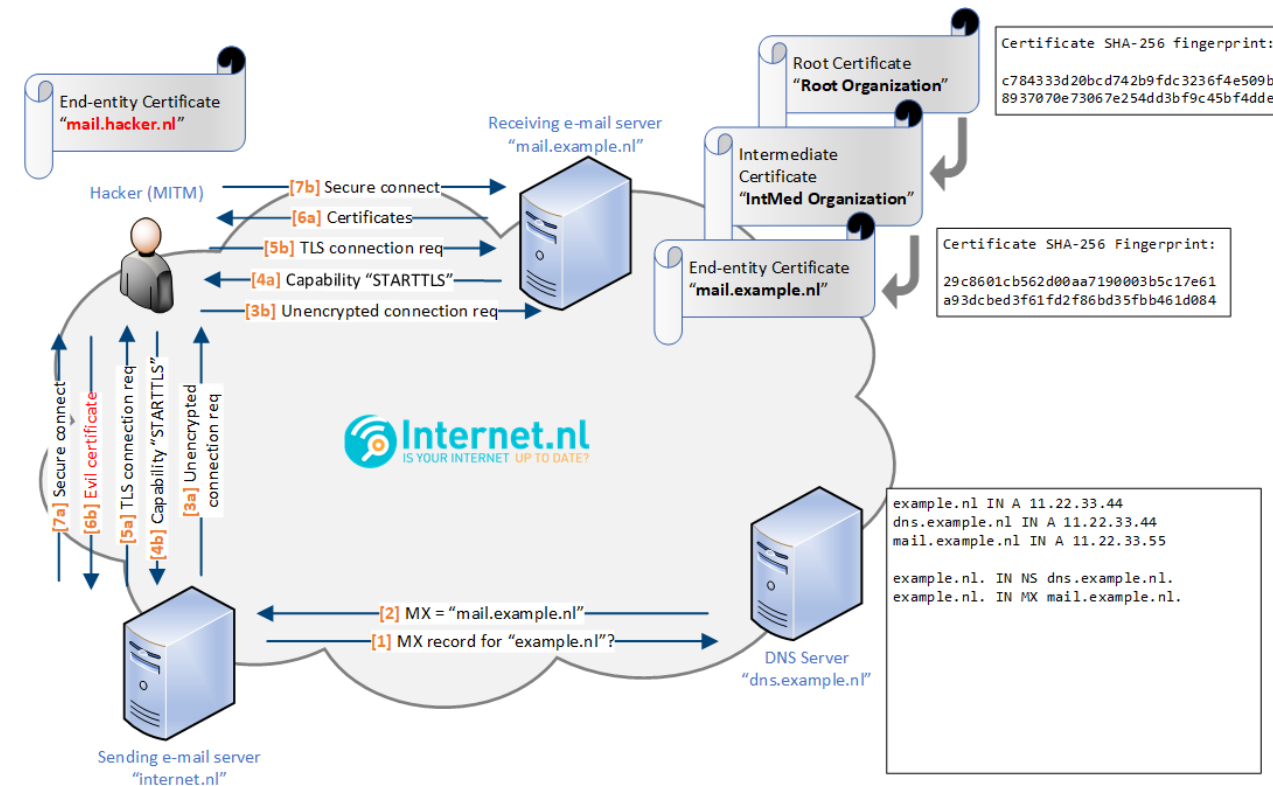




Risk 2: Divert mail traffic

Not validating the authenticity of another mail server's certificate allows for any random certificate to be accepted. This again makes it relatively easy for cybercriminals to manipulate email transport.

The certificate of the hacker is used for encryption of mail transport. The hacker can now unencrypt traffic and manipulate email transport.





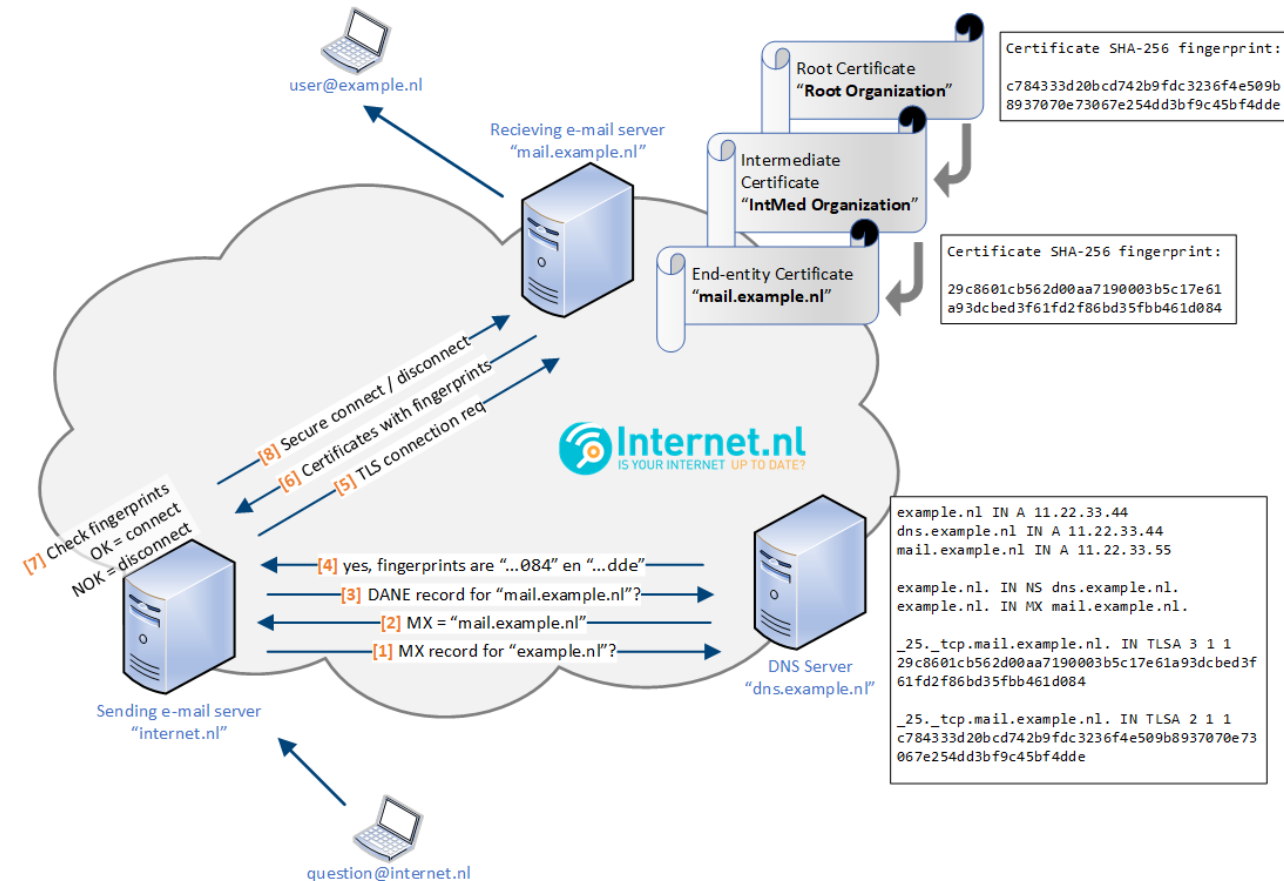
Secure transport with DANE

To ensure reliable TLS connections DNSSEC is used for retrieving information that is published by a domain name's owner or administrator: the TLSA record.

This TLSA record enables SMTP servers to:

- determine up front (before setting up the connection) whether or not another SMTP server supports an encrypted connection.
- validating the authenticity of the other mail server's certificate.

Email transport is now secure.





TLSA record

_25._tcp.mail.example.nl. IN TLSA

Usage	Selector	Matching-Type
3	1	1

29c8601cb562d00aa7190003b5c17e61a93dcbcd3f61fd2f86bd
35fbb461d084



TLSA record

`_25._tcp.mail.example.nl. IN TLSA 3 1 1`
`29c8601cb562d00aa7190003b5c17e61a93dcbcd3f61fd2f86bd`
`35fbb461d084`

Usage

Selector

Matching-Type

Usage: *about the type of certificate that is used for this TLSA record*

0	PKIX-TA	(not used / not recommended)
1	PKIX-EE	(not used / not recommended)
2	DANA-TA	Specifies an intermediate / root certificate
3	DANE-EE	Specifies an end-entity certificate



TLSA record

_25._tcp.mail.example.nl. IN TLSA 3 1 1
29c8601cb562d00aa7190003b5c17e61a93dcbbed3f61fd2f86bd
35fbb461d084

Usage
Selector
Matching-Type

Selector: *about the scope of the fingerprint regarding this TLSA record*

0	Full certificate	Fingerprint regarding full certificate
1	Public key	Fingerprint regarding public key



TLSA record

_25._tcp.mail.example.nl. IN TLSA 3 1 1
29c8601cb562d00aa7190003b5c17e61a93dcbbed3f61fd2f86bd
35fbb461d084

Usage
Selector
Matching-Type

Matching-Type: about the hashing mechanism used for fingerprinting

0	Exact match	
1	SHA-256	Fingerprint is a SHA-256 hash
2	SHA-512	Fingerprint is a SHA-512 hash



Ensuring DANE validation

- When installing a new certificate, it is important to make sure that there is always a valid TLSA record which can be used to verify the certificate offered.
 - Add the TLSA record of the new certificate well before you start using the new certificate.
 - Take into account the time needed for DNS records to spread across the internet (TTL).

This is called a **roll-over scheme**, and it exists in two flavors.



DANE roll-over: current + next

```
[CURRENT] _25._tcp.mail.example.nl. IN TLSA 3 1 1 current-sha256-publickey
```

```
[NEXT] _25._tcp.mail.example.nl. IN TLSA 3 1 1 next-sha256-publickey
```

- 2 TLSA records.
 - One for the current EE certificate.
 - One for the next EE certificate.



DANE roll-over: current + issuer

```
[CURRENT] _25._tcp.mail.example.nl. IN TLSA 3 1 1 current-sha256-publickey
```

```
[ISSUER] _25._tcp.mail.example.nl. IN TLSA 2 1 1 issuer-sha256-publickey
```

- 2 TLSA records.
 - One for the current EE certificate.
 - One for a TA certificate; an intermediate or root-certificate in the chain-of-trust.



Tips for implementation

- A. DANE is meant to be **used for the MX domain**. So if you are using another domain's mail servers, make sure to ask the administrator of that domain (your mail provider) to support DANE by setting up a TLSA record.
- B. It is highly recommended to use a certificate's **public key for generating a TLSA signature** (selector type "1") instead of the full certificate (selector type "0"), because this enables the (limited) reuse of key materials.
- C. Make sure the **TTL (time-to-live) of your TLSA records is not too high**. This makes it possible to apply changes relatively fast in case of problems. A TTL between 30 minutes (1800) and 1 hour (3600) is recommended.
- D. In case of roll-over scheme "current + issuer", the use of the **root certificate is preferred** because in some contexts (PKIoverheid) this makes it easier to switch supplier / certificate without impacting DANE.
- E. DANE still works when using **self-signed and/or expired certificates**.
- F. Certificate name checks are **not performed** for end-entity certificates (usage type 3). However, they **are performed** for intermediate / root certificates (usage type 2).



Tips for implementation

- G. Check if DANE TLSA records (`_25._tcp.mail.example.nl`) are **properly DNSSEC signed**. A regularly occurring mistake is the presence of "proof of non-existence" (NSEC3) for the ancestor domain (`_tcp.mail.example.nl`). If this happens then resolvers that use Qname minimization (like the resolver used by [Internet.nl](https://www.internet.nl)) think that `_25._tcp.mail.example.nl` does not exist since `_tcp.mail.example.nl` does not exist. Therefore the resolver can't get the TLSA record which makes DANE fail.
- Note that more or less the same principle goes for regular DNS lookups. According to RFC 8020 a NXDOMAIN response means that all the names under it do not exist.
- H. If TLSA records are found but are unusable, email transport will **NOT fallback** to opportunistic TLS (STARTTLS) or ultimately plaintext delivery. Email will NOT be delivered.



How about MTA-STS?

- MTA-STS is less secure compared to DANE for SMTP.
 - Only for domains that are not (yet) able to deploy DNSSEC.
 - MTA-STS is relatively complex because it needs an extra HTTPS interface (including certificate validation).
 - Weaknesses are documented in its specification in section 10 of RFC8461: trust on first use + caching.
- MTA-STS and DANE can co-exists next to each other. They intentionally do not interfere.
- Only a small number of large providers implemented MTA-STS: gmail.com, mail.ru, comcast.net.
- DANE is more popular
 - MTA-STS: 3,000 domains that use (enforce) MTA-STS
 - DANE: almost 3,000,000 domains with TLSA records on the mail server domain

More details: <https://www.isi.edu/~hardaker/news/2021-09-20-DANE-vs-STS.html>



Questions?

Feel free to contact me at question@internet.nl.

Other interesting sources

- <https://github.com/baknu/DANE-for-SMTP/wiki>
- <https://blog.apnic.net/2019/11/20/better-mail-security-with-dane-for-smtp/>
- <https://www.globalcyberalliance.org/resource/layers-of-defense-dane-and-dmarc/>
- <https://stats.dnssec-tools.org/> & <https://dane.sys4.de>