# One year of DANE

## (some)

# Lessons Learned

Jaap Akkerhuis
NLnet Labs




NLnet Labs

# Disclaimer

Original work by sys4.de

All errors are mine




NLnet Labs

# DNSSEC & Dane

- DNSSEC is not an application
- Authenticated data enables other use
- Dane (DNSSEC Authenticated Name Entities)
- Secure and Verify

# Encryption models

## Opportunistic

- Expect anything
- Downgrade of not offered
- Silent on failure

## Mandatory

- Expect encryption
- Identify other side
- Force
- Alarm on failure

(What is the priority: message security?)

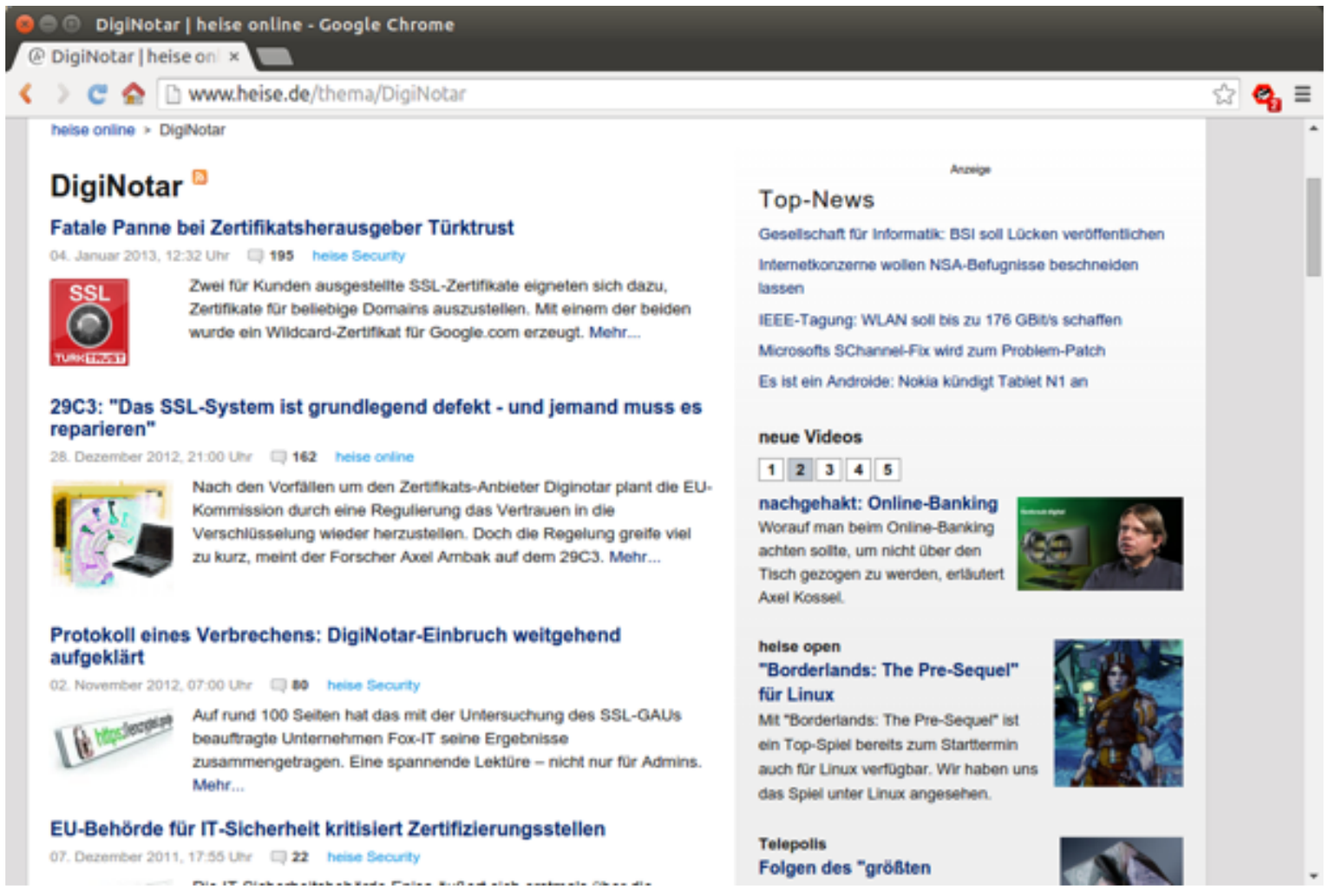
# Opportunistic TLS ISSUES

- CA model
- Downgrade Attack
- MITM attack
- Incomplete automation for certification rollover

# Br0ken CA Model?

- Any CA can issue certificates for any domain
- CAs have been compromised in the past
- CAs have issued wrong or unauthorized certificates
- Declining Trust in CA root-certificates since Snowden

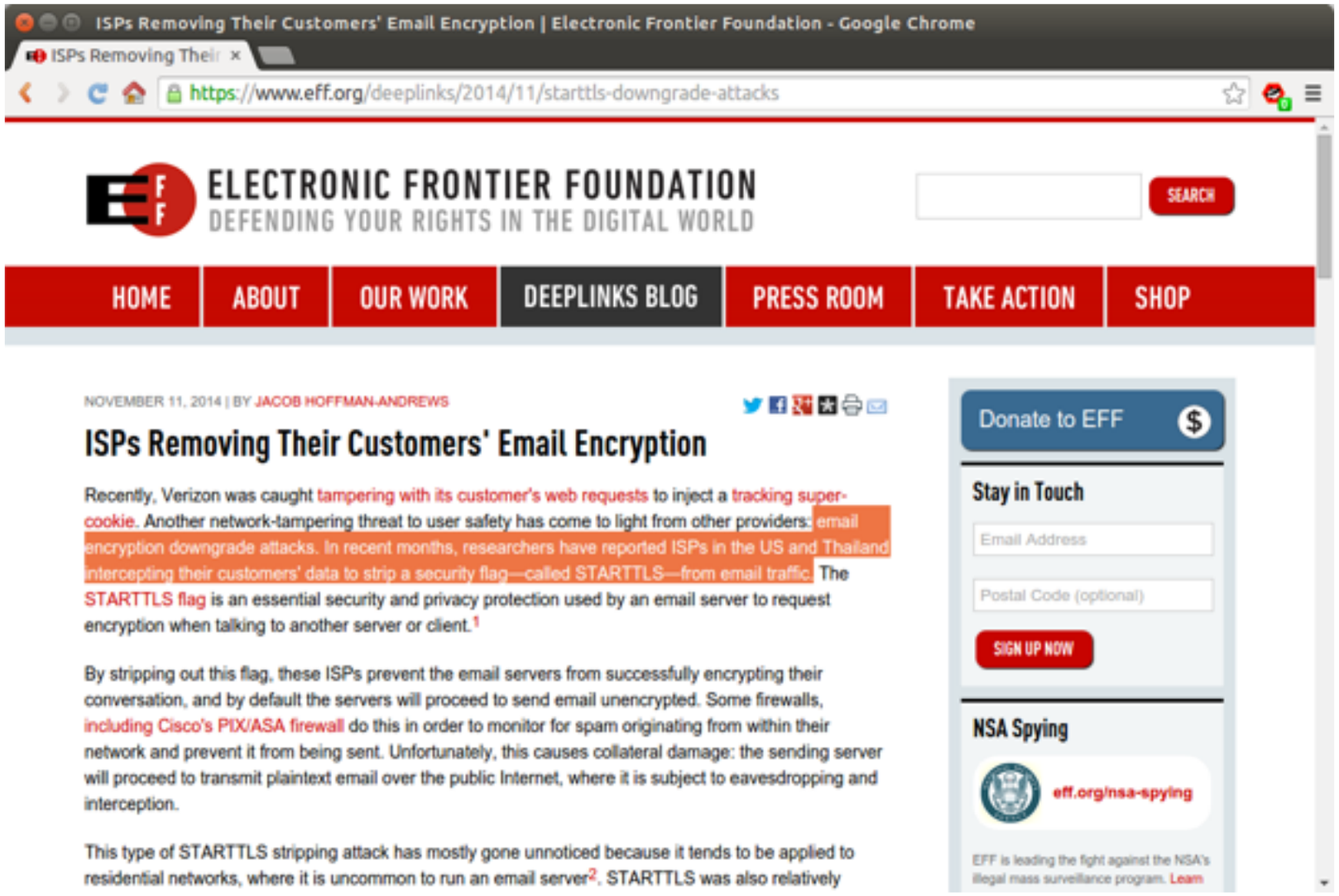
# Türktrust? Diginotar?



# MITM Attack

- Attacker can intercept TLS secured communication with a matching certificate (Common Name)
- Easily done since everyone accepts self signed certificates…

# Session downgrade



# Session downgrade

- TLS comes without policy channel
- Client can't know server supports STARTTLS before SMTP Session starts
- MITM-Attacker may downgrade session to „Non-TLS“

```
220 mail.example.com ESMTP
EHLO client.example.com
250-mail.example.com
250-PIPELINING
250-SIZE 40960000
250-ETRN
~~250-STARTTLS~~
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

# Automation? NOT!

- Certification Authority is warrantor
- Manual verification
- Verification requires knowledge
- Verification requires presence
- Need to monitor certificate change

# Trust but Verify!




NLnet Labs

# The Plan

- Add a policy channel
- Add a trust layer
- Indicate encryption
- Indicate identity

# DANE

"DNS-based Authentication of Named Entities" (RFC 6698)

- DANE uses/requires DNSSEC
  - DNS becomes policy channel
  - DNSSEC adds trust layer
- New Resource Records
  - Presence indicates service availability
  - Record carries service specific data

# Current Use Cases

- HTTPS
  Connect service/server to a certificate
- SMTP
  Connect service/server to a certificate
- OpenPGP
  Associate Public Keys to  email address
- S/MIME

# HTTPS



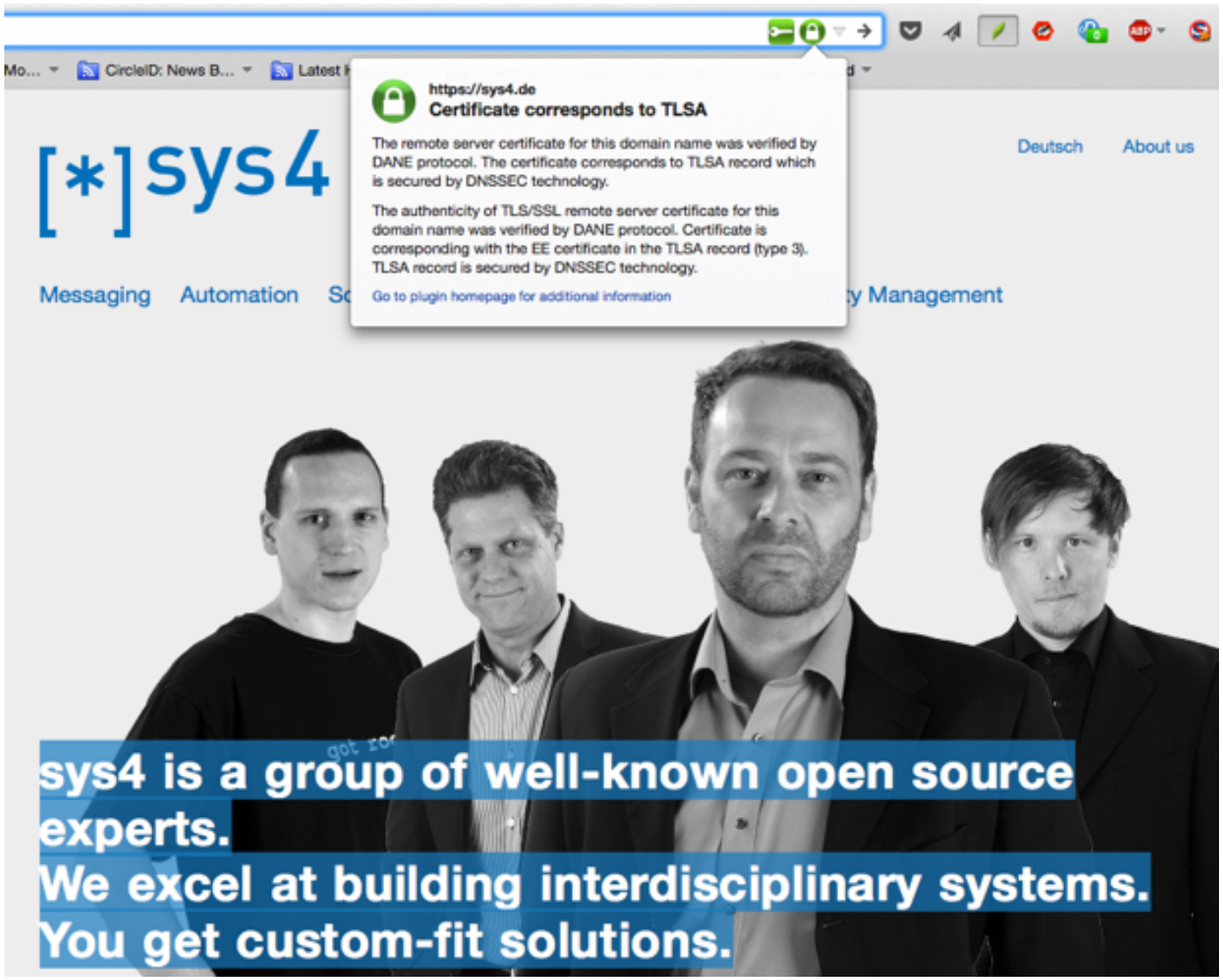

NLnet Labs

# TLSA Resource Record

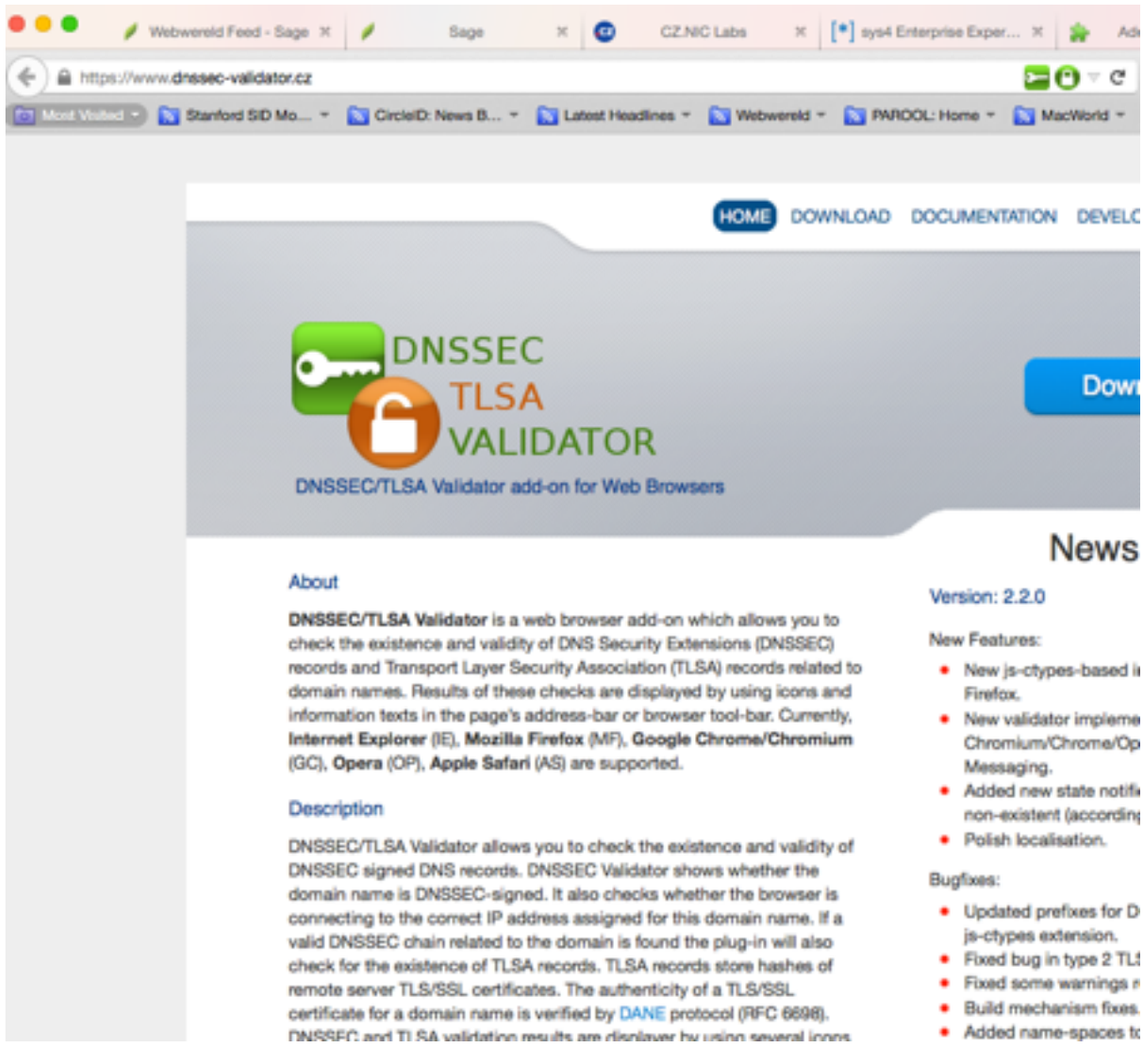
```
  _443._tcp.www.sys4.de. IN TLSA 3 0 1 9273B4E9040C1B…
     |   |   |                    |    | | | |
Port--   |   |                    |    | | | |
Protocol--   |                    |    | | | |
Host----------                    |    | | | |
Resource type--------------------    | | | |
Certificate Usage ------------------ | | |
Selector ------------------------------ | |
Matching Type ---------------------------- |
Certificate Association Data -------------
```




NLnet Labs



cz.nic | SPRÁVCE DOMÉNY CZ







NLnet Labs

# SMTP




NLnet Labs

# TLSA Resource Record

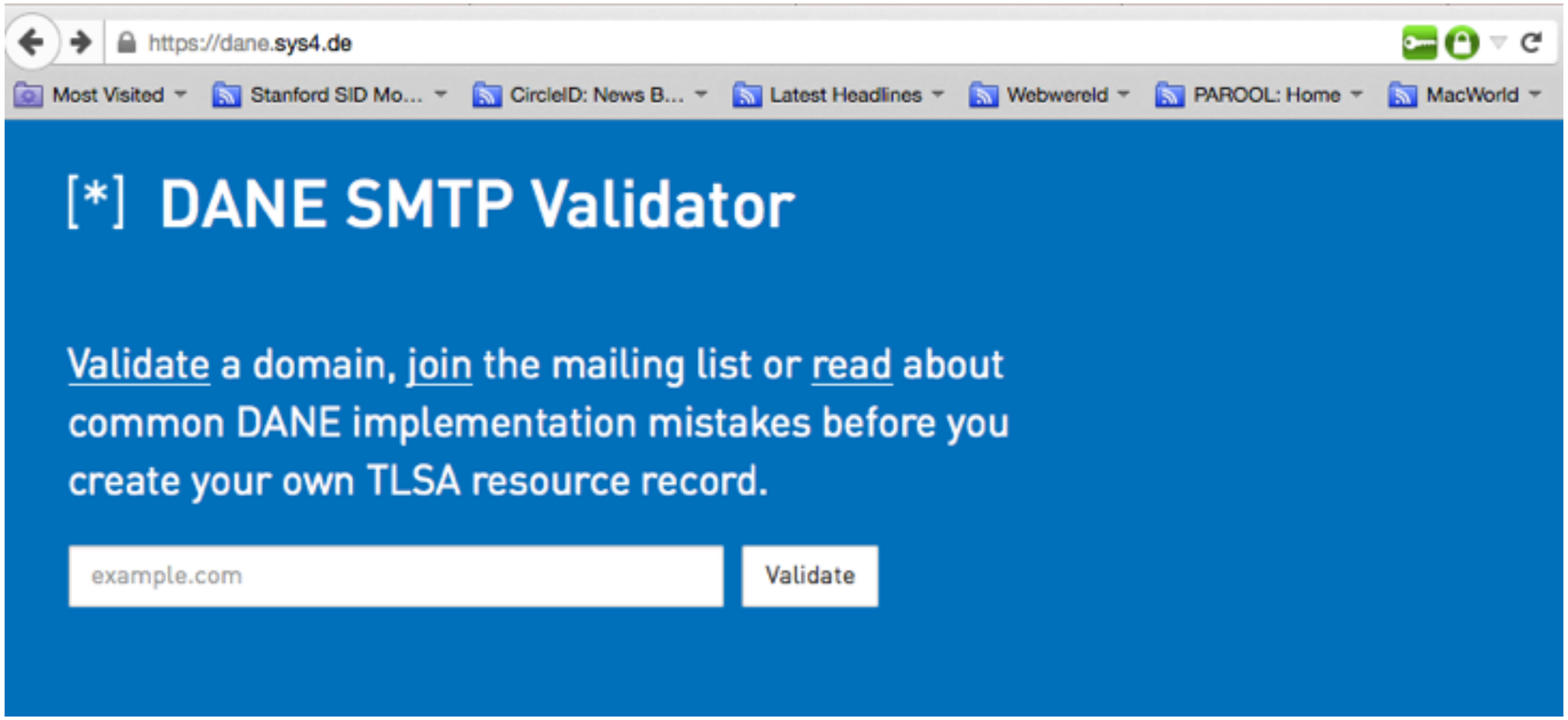
```
     _25._tcp.open.nlnetlabs.nl. IN TLSA 3 1 1 544F284D6..
      |   |   |                       |    | | | |
Port--    |   |                       |    | | | |
Protocol--    |                       |    | | | |
Host----------                        |    | | | |
Resource type-------------------------    | | | |
Certificate Usage------------------------ | | |
Selector ---------------------------------- | |
Matching Type ------------------------------- |
Certificate Association Data ------------------
```




NLnet Labs

# SMTP Security via DANE TLS

- Initial RFC draft published 2013 Wes Hardaker, Viktor Dukhovni
- Currently for IESG DANE
- First implementations
  - Postfix
  - OpenSMTPd
  - Exim



# nlnetlabs.nl DNSSEC TLSA SMTP

The domain lists the following MX entries:

## 50 open.nlnetlabs.nl

DNSSEC TLSA SMTP Show Details

| IP Addresses |
| --- |
| 185.49.140.10 |
| 2a04:b900:0:0:1:0:0:10 |

| Usable TLSA Records |
| --- |
| 3, 1, 1 544f284d66af2de0[...]a62b55ab7ac269be |
| 3, 1, 1 f7db964ed80ed077[...]37ad0ccfbfe2359f - certificate not trusted: [27] - certificate not trusted: [27] |

## 90 mcvax.nlnet.nl

DNSSEC TLSA SMTP Show Details

# OpenPGP & S/MIME




NLnet Labs

# OpenPGP & S/MIME

Under Construction

- Local email parts are a mess
  - “Local Part”@email.example.org
- Non RFC-compliant behaviour
- Non standard  Variations
- Foo.Bar synonym for foobar?
- Déjà vu all over again…




NLnet Labs

# Some Lessons

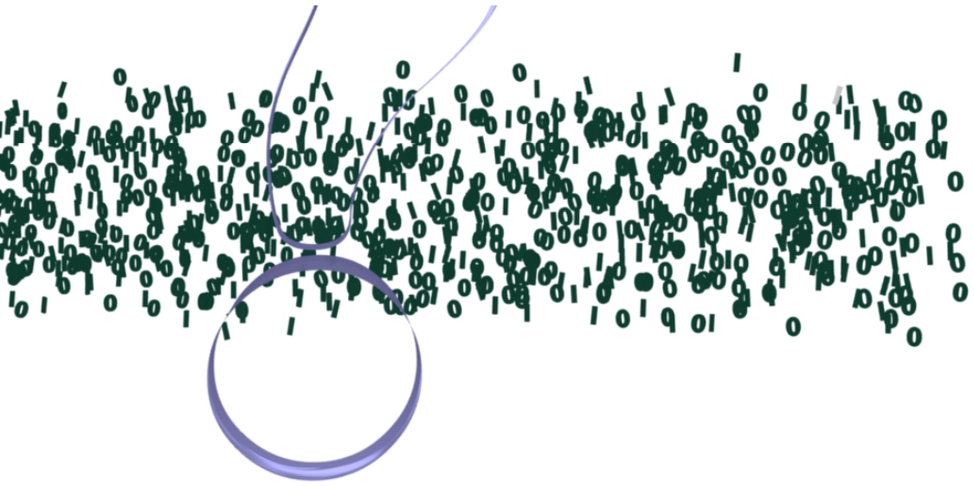
- DNS is infrastructure to build upon
- DNSSEC is an security enabling technology
- DANE verifies “trustworthiness” level

# What people tell

- DNS provider with incomplete or non-existent DNSSEC-support
- With DNSSEC issues become mission critical
- Missing DNSSEC/DANE monitoring and alarming
- Missing know-how for automated certificate-management and DNSSEC signing
- Missing toolchain for automated management

# “Takeaways”

- DNSSEC as a „one-time-cost“ infrastructure
- Open standard
- DANE allows scalable and secure trust-management
- Reduces management costs
- Automates rollover



# Questions




NLnet Labs

NLnet Labs