SMTP
Sicherheit mit DANE

sys4.de

EMiG :-)

- STARTTLS für Kunden verbindend
- STARTTLS zwischen EMiG-Teilnehmern
- Die EMiG-Teilnehmer decken einen grossen Anteil an deutschen Mailnutzern ab

EMiG :-(

- STARTTLS war überfällig
- Marketing:
  vendor lock-in & competition lock-out
- Technik:
  lokaler Schutz, global unsicher
- Politisch:
  Einmauern wie USA nach 9-11

Was ist DANE?

DANE

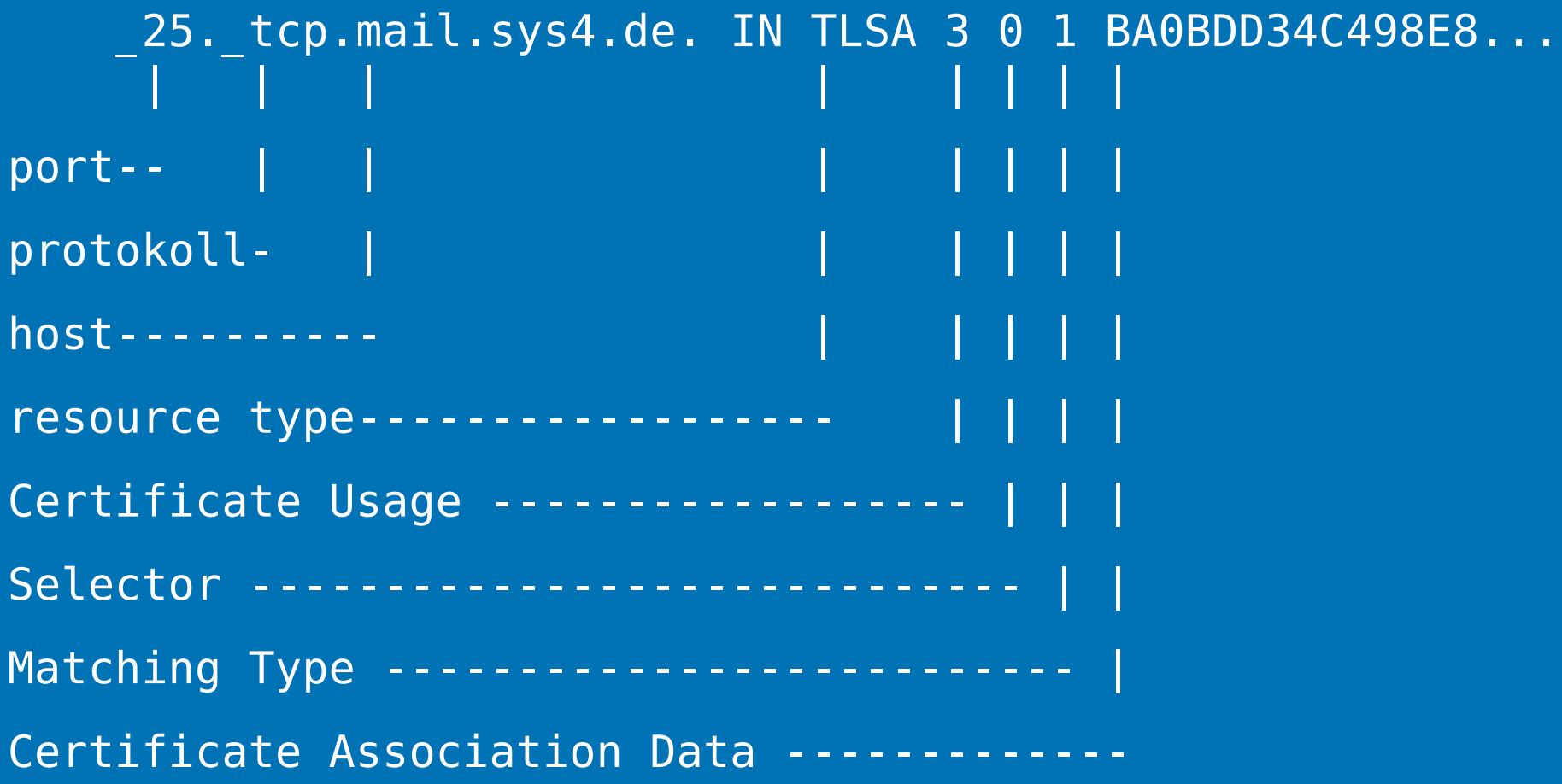
- Akronym für "DNS-based Authentication of Named Entities"
- DANE ist ein RFC (RFC 6698)
- DANE beschreibt einen (neuen) TLSA RR mit dem ein TLS-Zertifikat in einer DNSSEC-signierenden Domain veröffentlicht werden kann
- Eine Identität kann automatisiert über einen vertrauenswürdigen Kanal verifiziert werden

TLSA RR abfragen

```
$ dig TLSA +dnssec +noall +answer +multi \
  _25._tcp.mail.sys4.de


_25._tcp.mail.sys4.de. 3553 IN  TLSA 3 0 1
  (9273B4E9040C1B9EE7C946EFC0BA8AAF2C6E5F05A1B2
        C960C41655E32B15CBE0)
_25._tcp.mail.sys4.de. 3553 IN  RRSIG TLSA 8 5 3600
  (20141124104604 20141117195102 19786 sys4.de.
        afEJbtmKZVn995XiI2BFQwYKC1ZfcsIK/j2JA9C8oYSp
        pneBLVYuX8C0ZW9zTHCExtXS1kJrNf48sFRaOWwbZvPy
        1vRiB+c46QRG0kwceDUjzZGtpG3Al2LKBVKw4bxMMOzu
        DeqECrf/n1W8XF6UQcrB0PdTY81Y6IZTUovYhak= )
```

TLSA Resource Record



Was löst DANE?

Trust-Probleme

- CA-Modell
- Downgrade-Attacken
- MITM-Attacken
- mangelhafte Automatisierung

CA-Modell ist br0ken

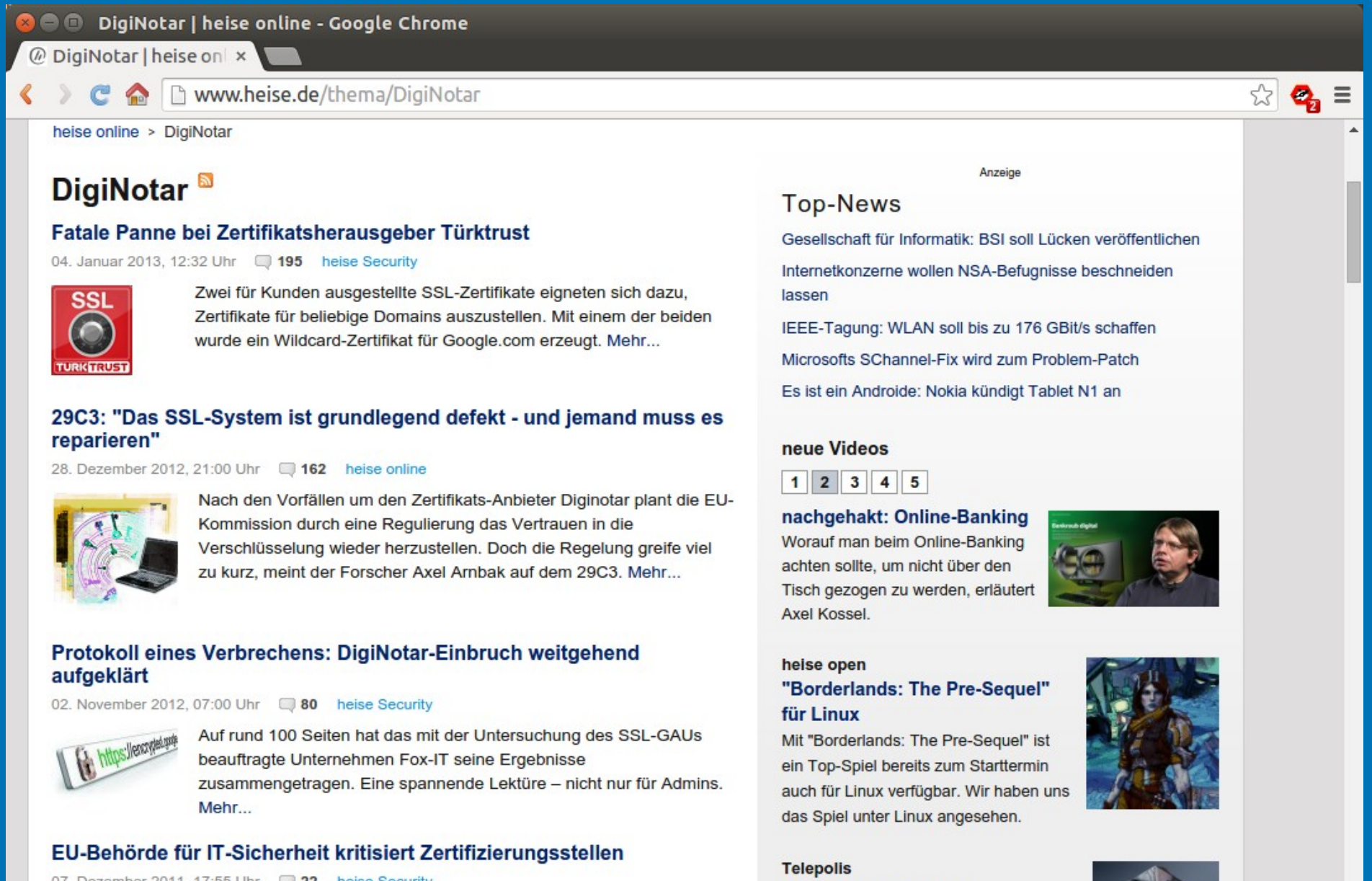
Heute

> Jede CA kann für jede Domain Zertifikate ausstellen
> CAs wurden bereits mehrfach kompromittiert
> Zertifikate wurden unerlaubt erstellt
> Trust in CA root-Zertifikate ist mit Snowden in Frage gestellt

DANE

> kann CA nutzen
> kann self-signed Certs nutzen

Türktrust? Diginotar?



Session downgrade

Heute

- Client kann nicht wissen, ob Server TLS anbietet
- Angreifer kann sich dazwischenstellen und die Session „downgraden“

DANE

- TLSA RR signalisiert TLS-Support („Strong SHOULD“) über vertrauenswürdigen Kanal
- Wenn Server dann kein TLS anbietet „stimmt was nicht“.

Session downgrade

MITM-Attacke

Heute

- Angreifer kann sich mit anderem, „passenden Zertifikat“ (Common Name) dazwischenstellen und Identität fälschen

DANE

- Identifikation über DNSSEC enttarnt falsche Identität
- X509 Fingerprint nur für den wahren Server gültig

Automatisierung. Nicht!

Heute

- Certification Authority ist Bürge
- Manueller Abgleich
- Medienbruch

DANE

- Trusted DNSSEC-Domain tritt als Bürge (CA) auf
- Identifikation in selbem Medium über anderen Dienst
- Automatischer Zertifikat-Rollover ohne Intervention

Was ermöglicht DANE?

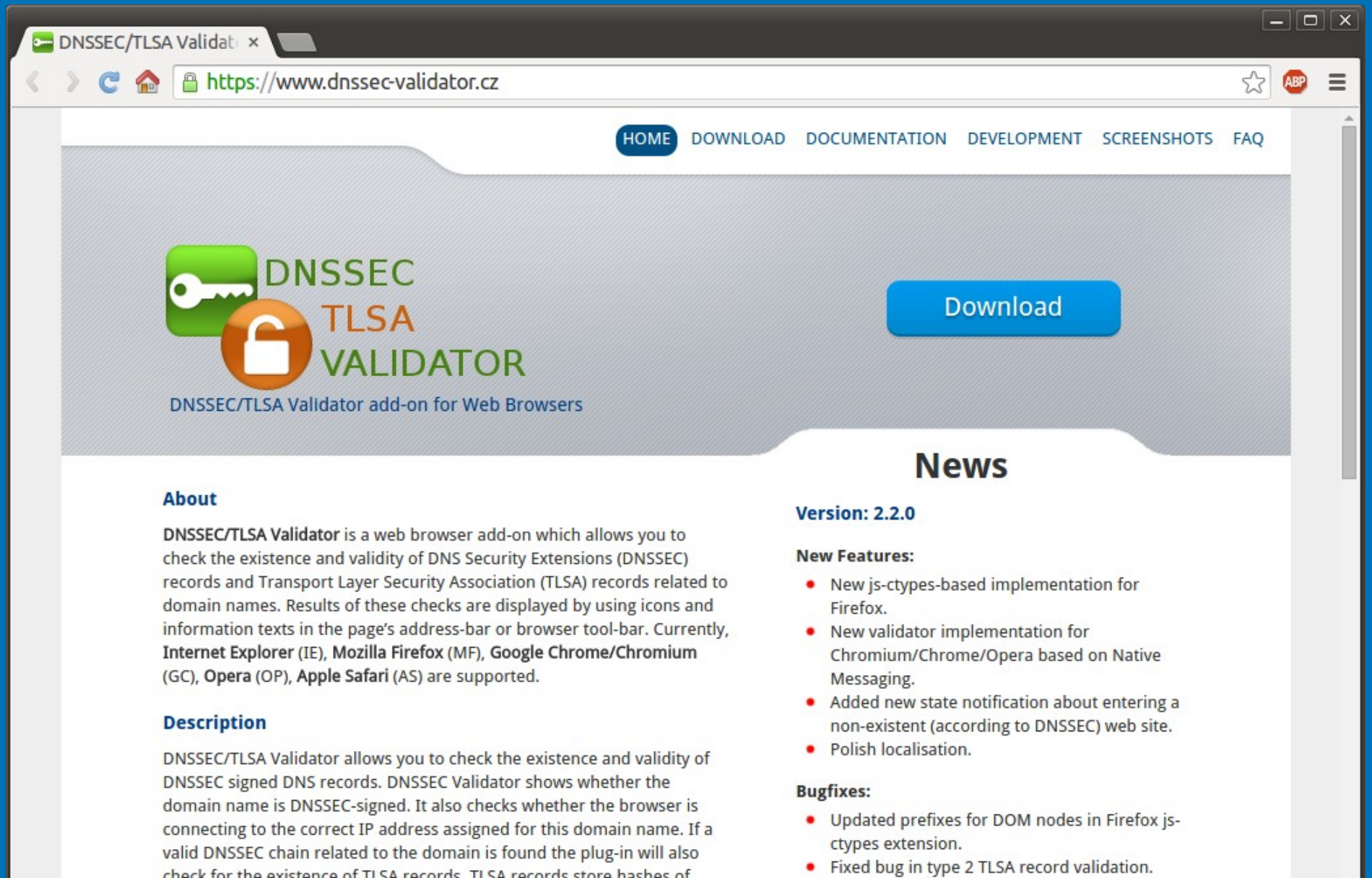
Use Cases

- **OpenPGP**
  Associate Public Keys mit E-Mail Addresse
- **S/MIME**
  Associate Certificates with Domain Names
- **HTTPS**
  Service mit Cert verbinden
- **SMTP**
  Service mit Cert verbinden

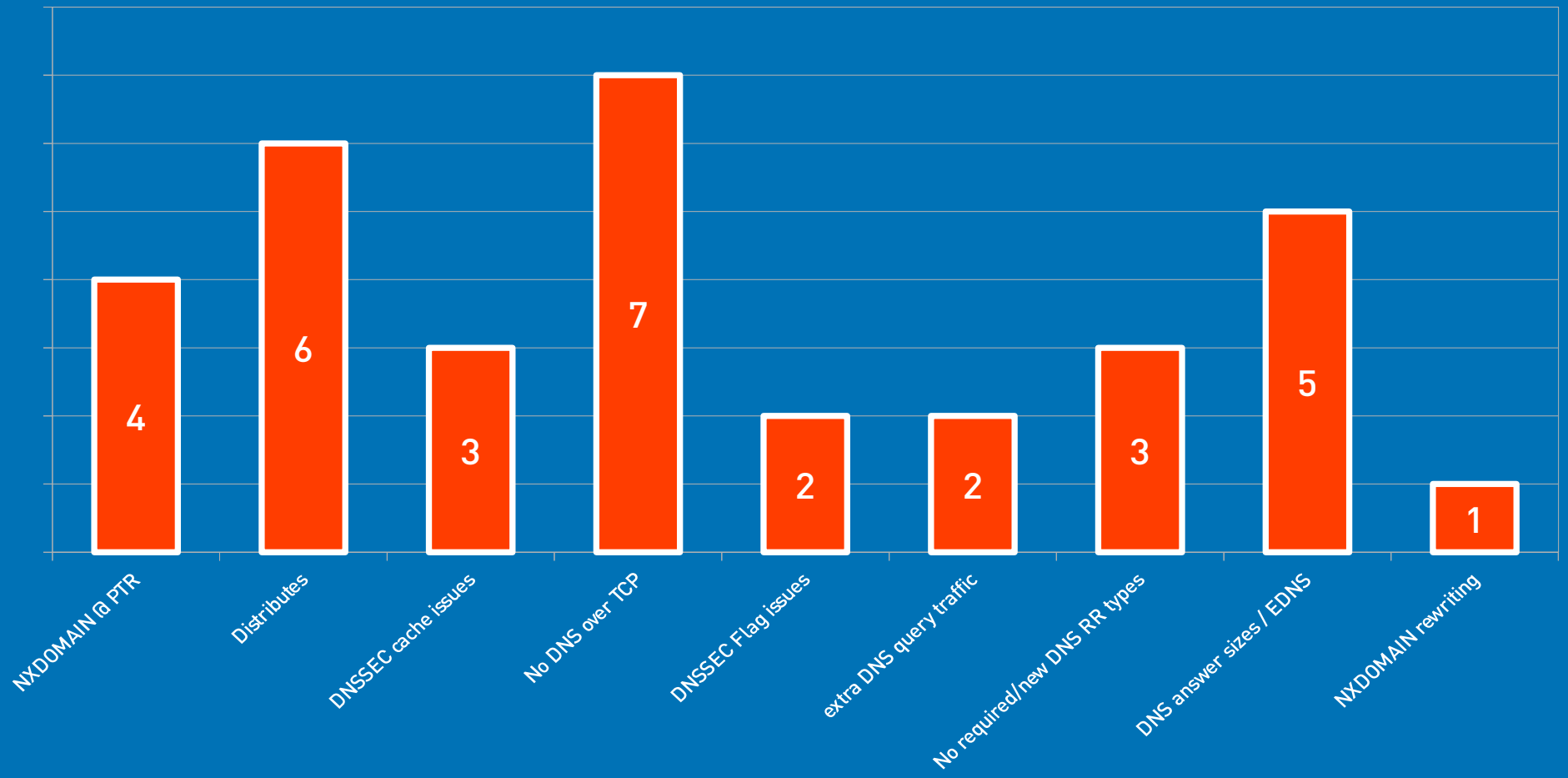
HTTPS


sys4 Enterprise Experts - Home - Mozilla Firefox
[*] sys4 Enterprise Expert...
https://sys4.de/de/
LEO Eng-Deu
https://sys4.de
Zertifikat entspricht TLSA
Das Serverzertifikat für diese Domäne wurde durch DANE Protokoll bestätigt. Das Zertifikat entspricht dem durch DNSSEC gesicherten TLSA Eintrag.
Mehr info
English
Über uns
Kontakt
Messaging
Automation
dentity Management
BLOG
Wir sind ein Team namhafter Open-Source-Experten.
Unsere Stärke sind interdisziplinäre Systeme.

Browser Plugin



Modeme haben Probleme



DNS-Proxy Fehler, CPE-Modem Studie mit 15 Kabelmodemen
sys4 für Unitymedia Deutschland, August 2014

SMTP security via opportunistic DANE TLS

- Erste Veröffentlichung RFC draft Anfang 2013
- Viktor Dukhovni, Patrick Koetter (Lektor)
- RFC final 12/2014 erwartet
- Postfix erste Implementierung
- sys4 Produktivbetrieb ab 12/2013

Der feine Unterschied

Heute

```
Jul 14 11:03:31 mail postfix/smtp[6477]:
  Trusted TLS connection established to mx-ha03.web.de
  [213.165.67.104]:25: TLSv1.1 with cipher
  DHE-RSA-AES256-SHA (256/256 bits)
```

DANE

```
Jul 14 11:04:44 mail postfix/smtp[6409]:
  Verified TLS connection established to mail.sys4.de
  [194.126.158.139]:25: TLSv1 with cipher
  ECDHE-RSA-AES256-SHA (256/256 bits)
```

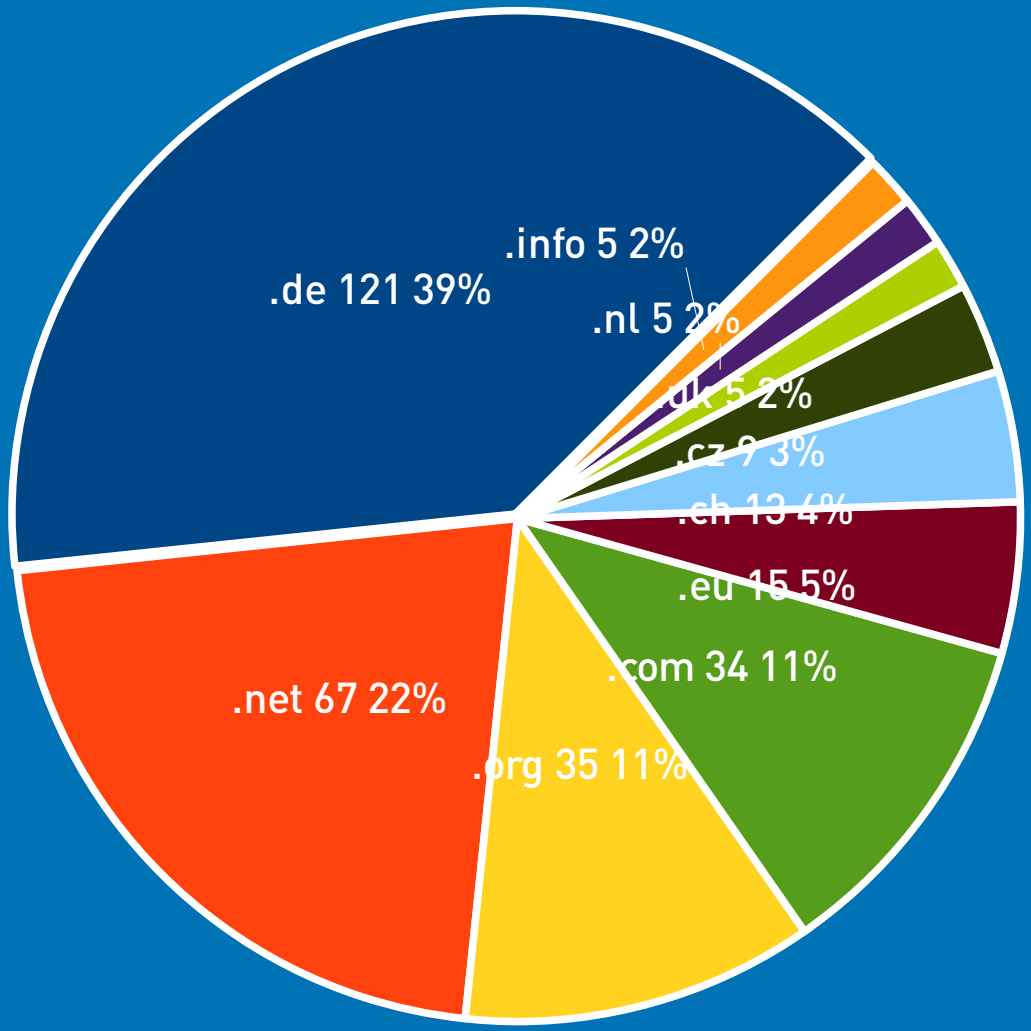
Next Steps DANE WG

- raw-Zertifikate
- mutual authentication
  client-seitige Identifizierung über TLSA RR

Adoption

- posteo.de
- mailbox.org
- bund.de
- Unitymedia
- ...

Top 10 DANE TLDs



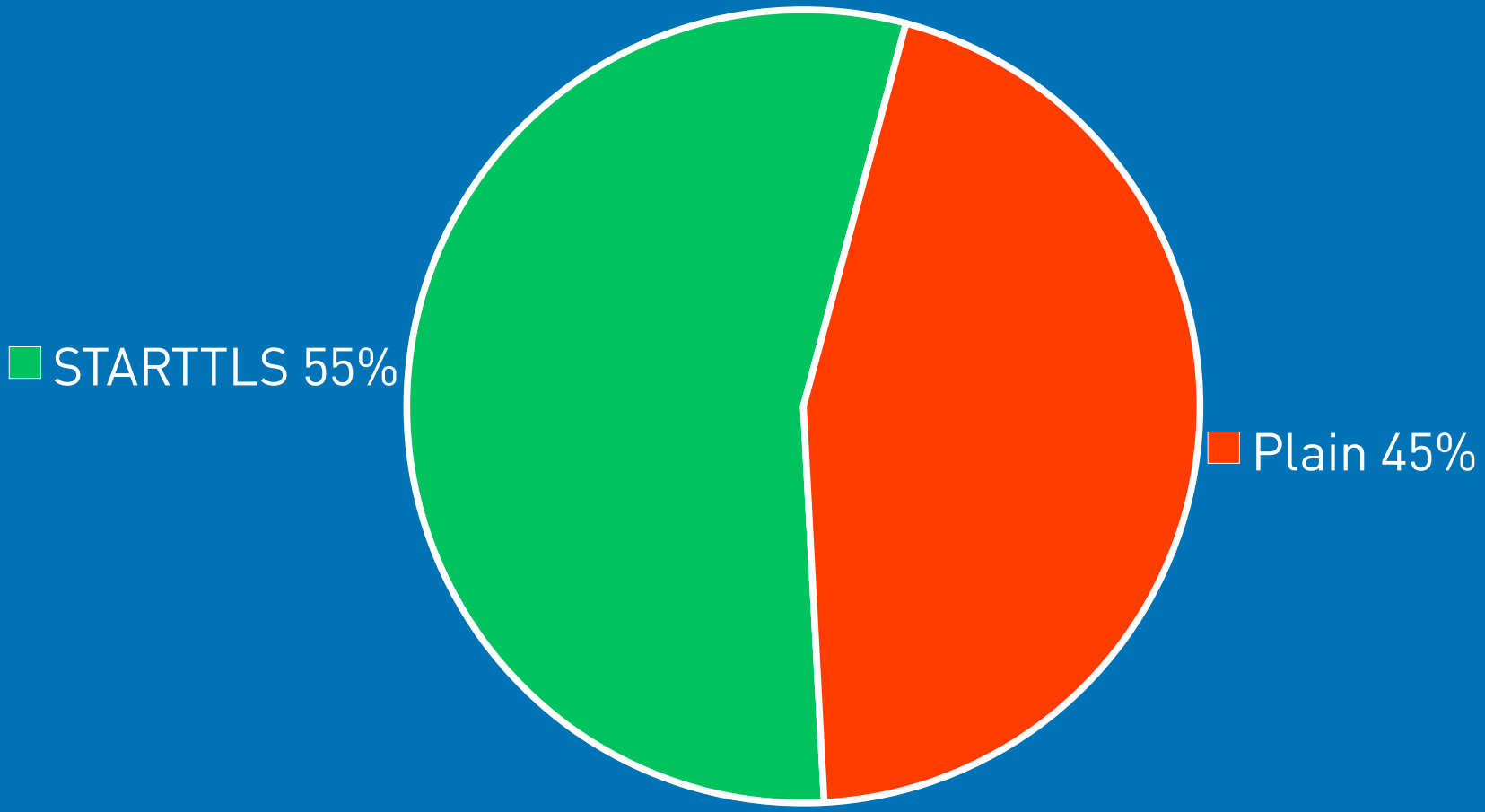
Viktor Dukhovni auf IETF DANE Mailingliste, 14.11.2014

Märkte für DANE

Wer braucht DANE?

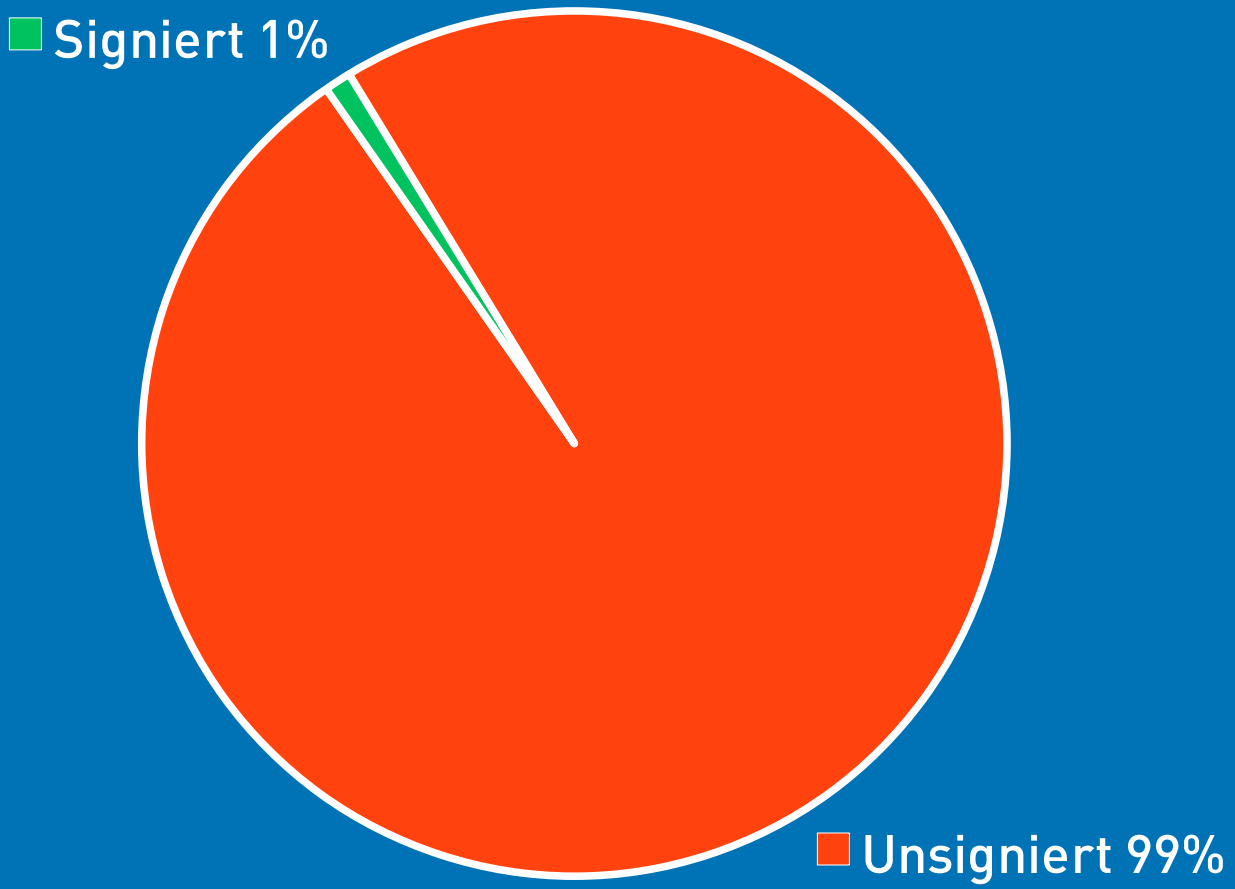
- Anbieter gesicherter Dienste
- Mailteilnehmer mit „definiertem Sicherheitsbedürfnis“
- Online-Payment, Versicherungen, Banken
- Großunternehmen
- Zulieferer

TLS in .de



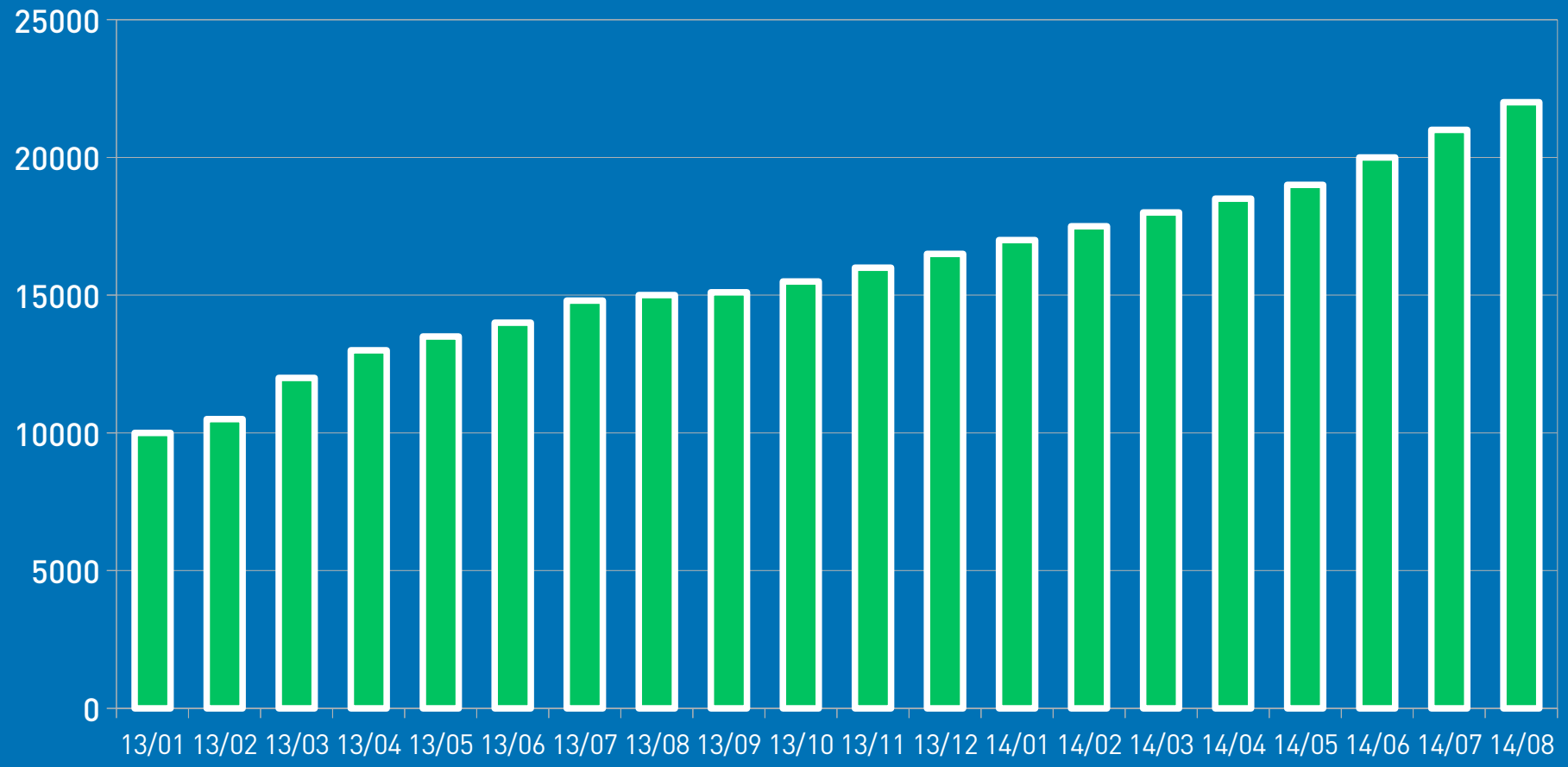
2,7 Mio. MX RR > 275.000 MTAs davon 12.092 IPv6 MTAs \o/

Anteil DNSSEC in .de



„SMTP, STARTTLS, DANE - Wer spielt mit wem?“, Peter Koch, DENIC eG
DENIC – Technisches Meeting, Frankfurt, 2014-09-30

Wachstum DNSSEC in .de



Was hindert DANE?

Was wir hören

- DNSSEC-Support bei Registraren unbekannt
- DNSSEC ist Technologie, aber kein Use Case
- DNSSEC-Fehler sind Mission Critical
- Kein DNSSEC-Monitoring und Alarming
- Knowhow für automatisierte Verwaltung fehlt
- Tools für automatisierte Verwaltung fehlen

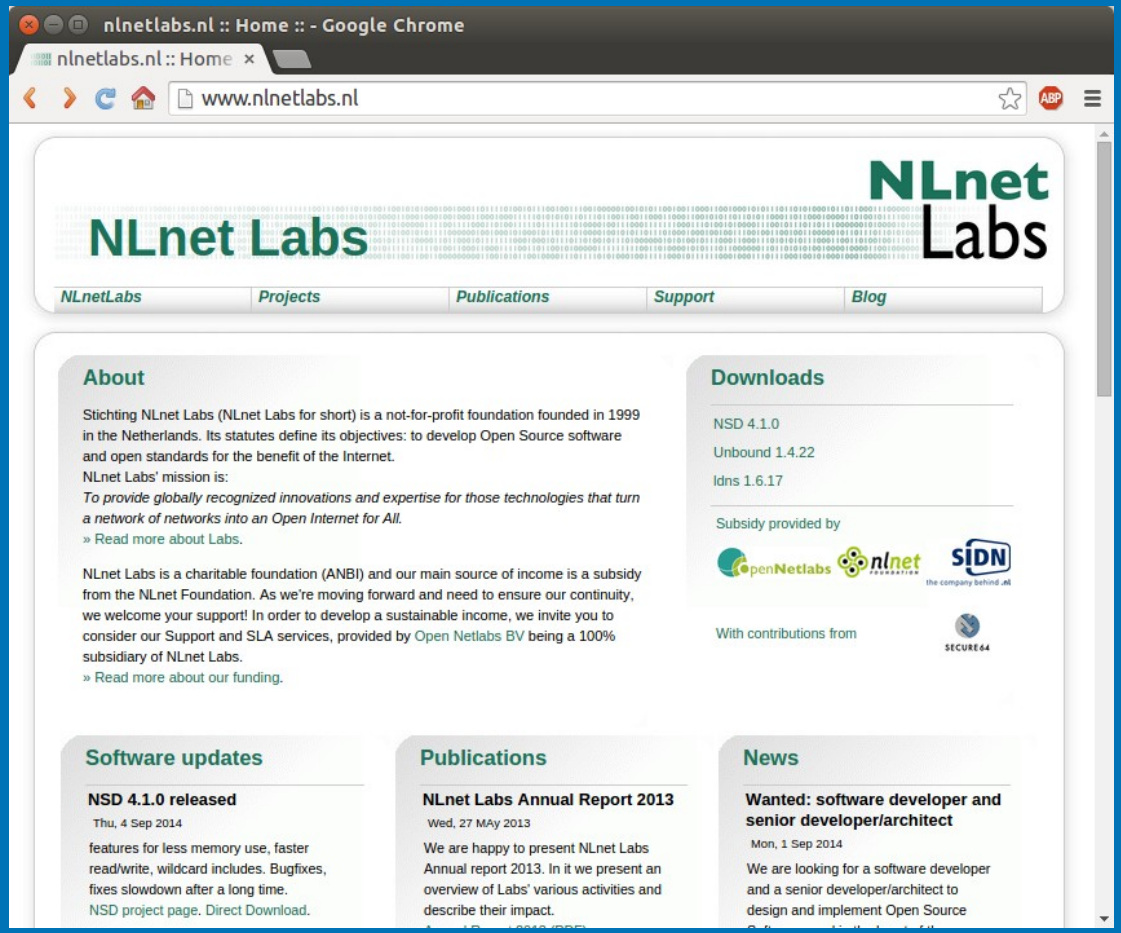
Registrare

- ~ 1/3 der .de-Registrare bieten DNSSEC
- DENIC darf einzelne Mitglieder nicht bevorzugt herausstellen
- Registrare haben Interesse
- sys4 schult DNSSEC für Registrare bei DENIC

DNSSEC ist Mission Critical

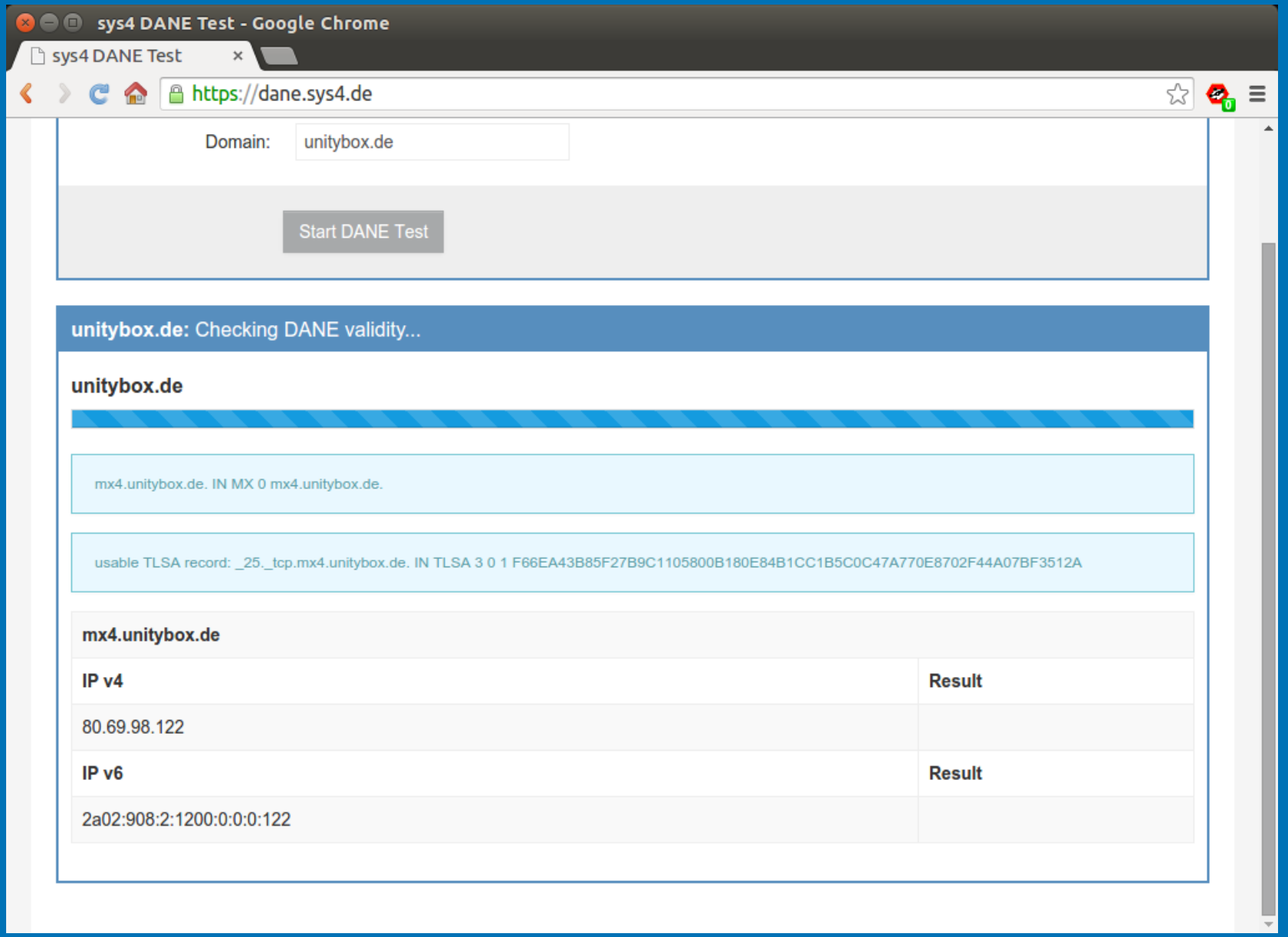
- DNS oft vernachlässigtes Stiefkind
- DNSSEC verlangt andere Host-Konfiguration
- DNSSEC verlangt „trusted peers“
- Abgelaufene TTLs lassen DNSSEC-Domain „verschwinden“

sys4 und NLnet Labs



SMTP- und DNS-Referenztools von Referenzpartnern

DANE Validator



In wenigen Worten...

- DANE ist ein offener Standard
  (WGLC December 4'th at 23:59 UTC)
- DANE ermöglicht finanzierbares Trust-Management
- DANE kostet einmalig DNSSEC-Aktivierung
- Postfix bietet einen DANE-capable client, Exim und Port25 folgen
- Jetzt braucht es Wissen und Erfahrung!

We do ASCII

sys4.de

https://sys4.de/download/dane-denog.pdf