# DANE
# Securing Security

sys4.de

# Warum sichern?

# Verschlüsselungsmodelle

Opportunistic Encryption

- Erwarte alles
- Versuche es
- Scheitere leise

Mandatory Encryption

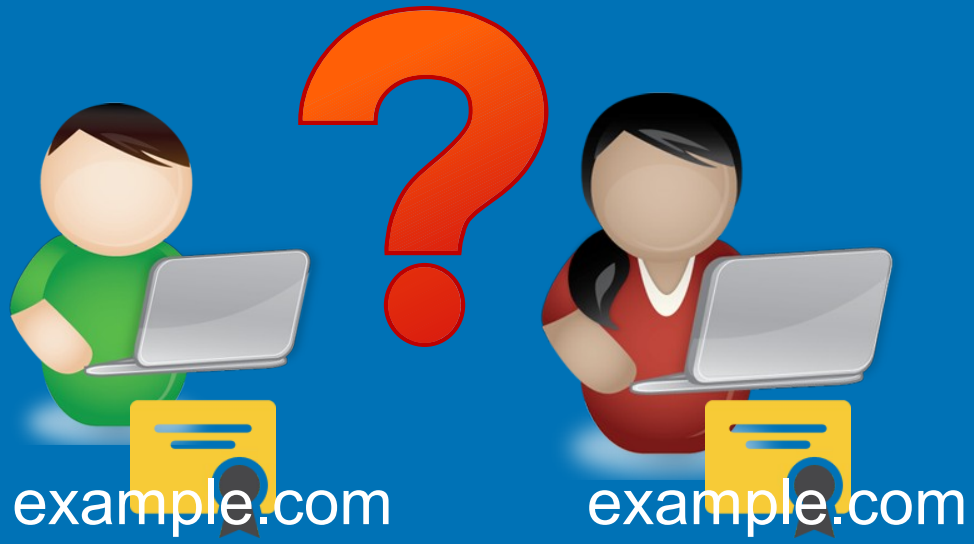
- Erwarte Verschlüsselung
- Scheitere wenn Verschlüsselung fehlt
- Identifiziere die Gegenseite
- Scheitere wenn Identität fehlerhaft
- Alarmiere wenn Verschlüsselung scheitert

# Opportunistisches TLS Probleme

- CA-Modell
- “Downgrade”-Attacke
- “MITM”-Attacke
- Unvollständige Automatisierung

# Kaputtes CA-Modell

- Jede CA kann Zertifikate für jede Domain ausstellen
- CAs in der Vergangenheit kompromittiert
- CAs stellten unautorisiert Zertifikate aus



# Türktrust? Diginotar?

DigiNotar | heise online - Google Chrome

DigiNotar | heise on ×

www.heise.de/thema/DigiNotar

heise online > DigiNotar

## DigiNotar

### Fatale Panne bei Zertifikatsherausgeber Türktrust

04. Januar 2013, 12:32 Uhr 195 heise Security

Zwei für Kunden ausgestellte SSL-Zertifikate eigneten sich dazu, Zertifikate für beliebige Domains auszustellen. Mit einem der beiden wurde ein Wildcard-Zertifikat für Google.com erzeugt. Mehr...

### 29C3: "Das SSL-System ist grundlegend defekt - und jemand muss es reparieren"

28. Dezember 2012, 21:00 Uhr 162 heise online

Nach den Vorfällen um den Zertifikats-Anbieter Diginotar plant die EU-Kommission durch eine Regulierung das Vertrauen in die Verschlüsselung wieder herzustellen. Doch die Regelung greife viel zu kurz, meint der Forscher Axel Arnbak auf dem 29C3. Mehr...

### Protokoll eines Verbrechens: DigiNotar-Einbruch weitgehend aufgeklärt

02. November 2012, 07:00 Uhr 80 heise Security

Auf rund 100 Seiten hat das mit der Untersuchung des SSL-GAUs beauftragte Unternehmen Fox-IT seine Ergebnisse zusammengetragen. Eine spannende Lektüre – nicht nur für Admins. Mehr...

Anzeige

### Top-News

- Gesellschaft für Informatik: BSI soll Lücken veröffentlichen
- Internetkonzerne wollen NSA-Befugnisse beschneiden lassen
- IEEE-Tagung: WLAN soll bis zu 176 GBit/s schaffen
- Microsofts SChannel-Fix wird zum Problem-Patch
- Es ist ein Androide: Nokia kündigt Tablet N1 an

### neue Videos

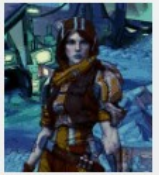
1 2 3 4 5

**nachgehakt: Online-Banking**

Worauf man beim Online-Banking achten sollte, um nicht über den Tisch gezogen zu werden, erläutert Axel Kossel.

**heise open**

**"Borderlands: The Pre-Sequel" für Linux**



Mit "Borderlands: The Pre-Sequel" ist ein Top-Spiel bereits zum Starttermin auch für Linux verfügbar. Wir haben uns das Spiel unter Linux angesehen.

# Session downgrade

- TLS besitzt keinen Policy-Kanal
- Client kennt STARTTLS-Support nicht vor Beginn der SMTP Session
- Angreifer kann Session zu „Non-TLS“ herabstufen

```
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
```

# Not a bug, but a feature…

“In recent months, researchers have reported ISPs in the US and Thailand intercepting their customers' data to strip a security flag—called STARTTLS—from email traffic. (…) By stripping out this flag, these ISPs prevent the email servers from successfully encrypting their conversation, and by default the servers will proceed to send email unencrypted.”

https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks

# MITM-Attacke

- Angreifer fängt TLS-gesicherte Session mit eigenem, passenden Zertifikat ab
- Einfach, weil ohnehin alle selbstsignierte Zertifikate akzeptieren…


# Automation - nicht!

- Manuelle Verifizierung
- Verifizierung setzt Fachwissen voraus
- Verifizierung setzt Anwesenheit voraus
- Ständiges Monitoring möglicher Veränderungen erforderlich

# Securing Security

# Der Plan

- Policy-Kanal hinzufügen
- “Trust layer” hinzufügen
- Verschlüsselung anzeigen
- Identität bekannt geben

# Willkommen zu DANE!

# DANE

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

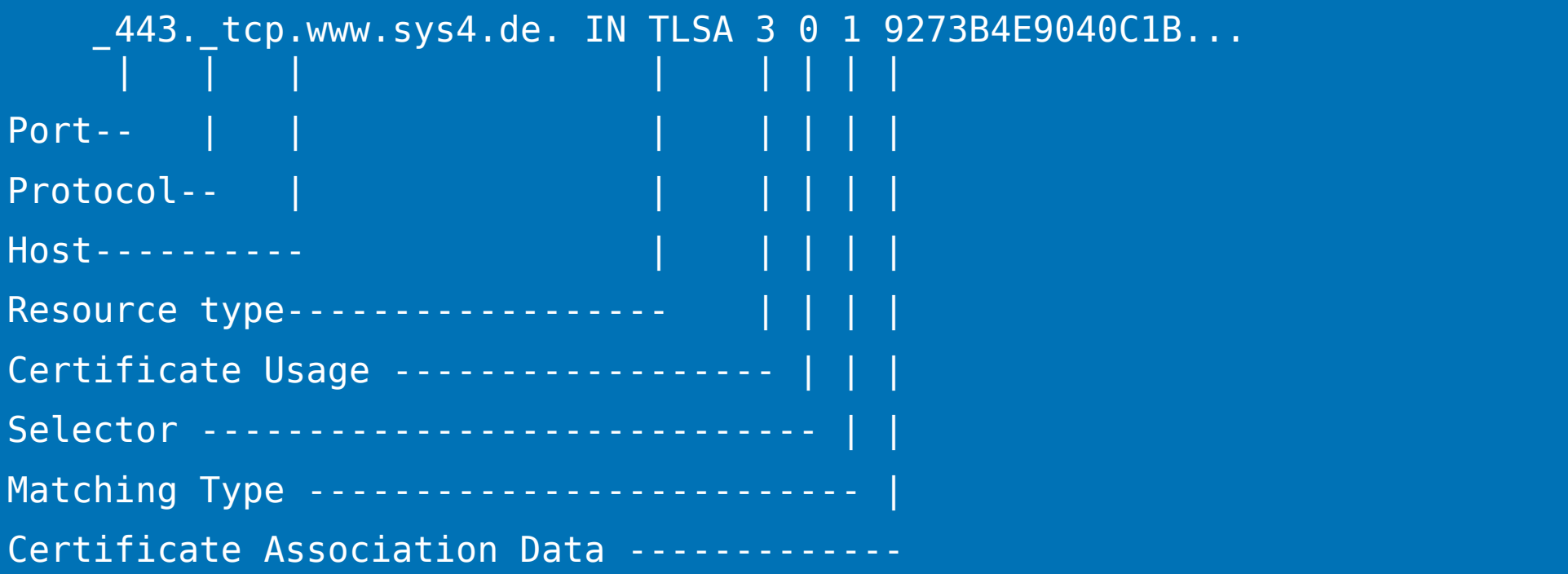
- DANE nutzt/setzt DNSSEC voraus
  - DNS wird Policy-Kanal
  - DNSSEC fügt “trust layer” hinzu
- Neue Resource Records
  - Präsenz zeigt Verschlüsselung an
  - Record gibt Identität bekannt

# Heutige Use Cases

- HTTPS
  Service/Server mit Zertifikat verbinden
- SMTP
  Service/Server mit Zertifikat verbinden
- OpenPGP
  Public Key mit E-Mail-Adresse assoziieren
- S/MIME
  x509-Zertifikat mit E-Mail-Adresse assoziieren

# HTTPS

# TLSA Resource Record



# TLSA RR query

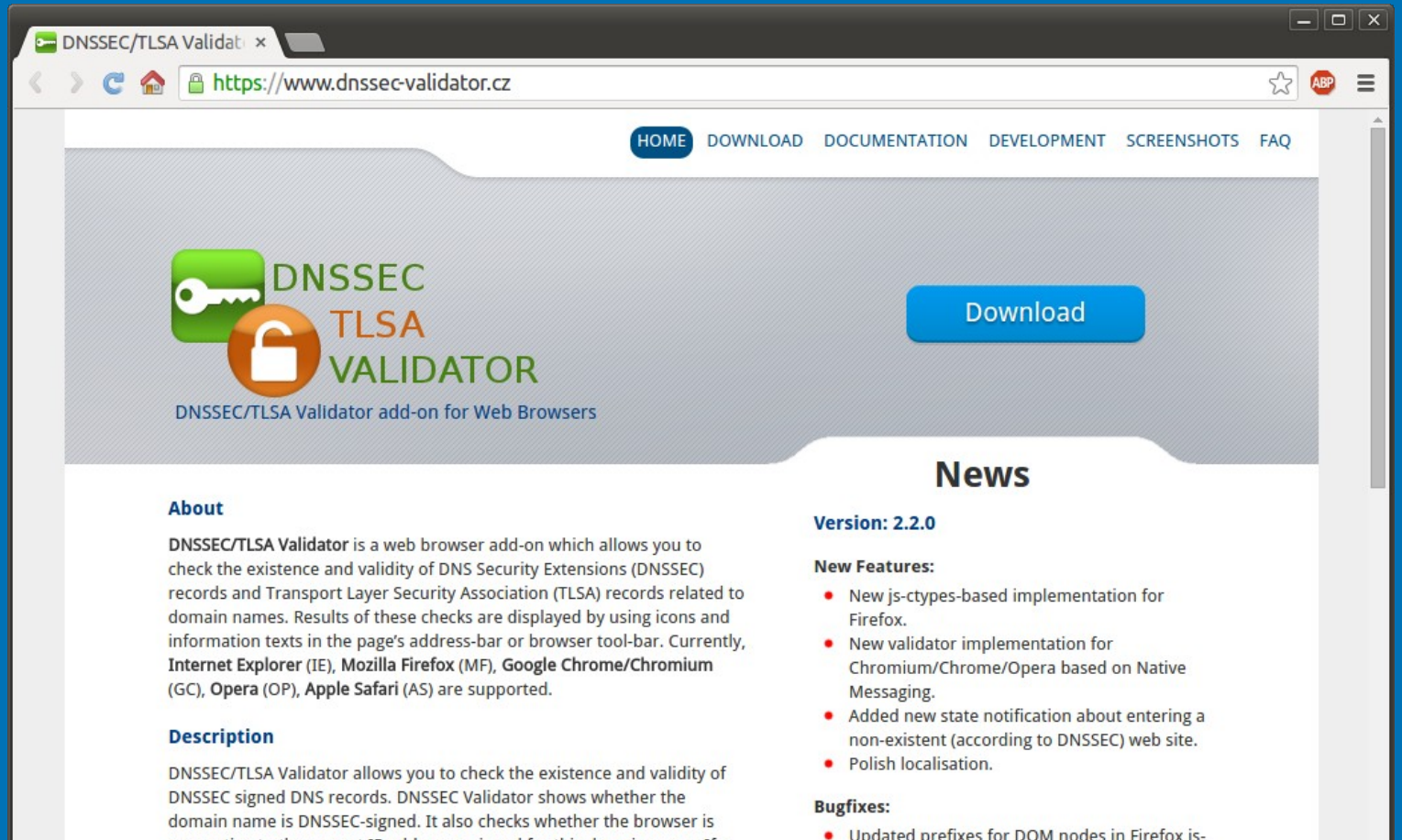
```
$ dig +dnssec TLSA _443._tcp.www.sys4.de

_443._tcp.mail.sys4.de.  3600 IN TLSA 3 0 1 (
      9273B4E9040C1B9EE7C946EFC0BA8AAF2C6E5F05A1B2
  C960C41655E32B15CBE0 )
_443._tcp.mail.sys4.de.  3600 IN RRSIG TLSA 8 5 3600 (
      20141124104604 20141117195102 19786 sys4.de.
    afEJbtmKZVn995XiI2BFQwYKC1ZfcsIK/j2JA9C8oYSp
  pneBLVYuX8C0ZW9zTHCExtXS1kJrNf48sFRaOWwbZvPy
  1vRiB+c46QRG0kwceDUjzZGtpG3Al2LKBVKw4bxMMOzu
  DeqECrf/n1W8XF6UQcrB0PdTY81Y6IZTUovYhak= )
```

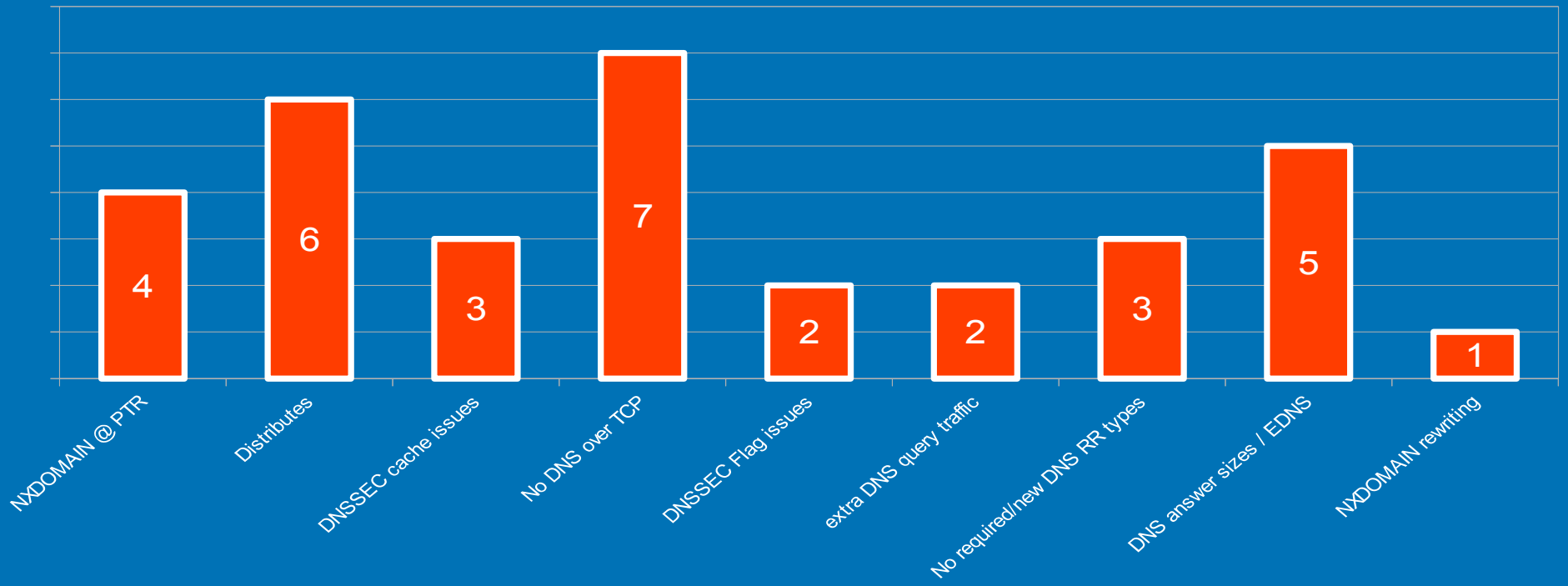
# HTTPS


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.

# Browser Plugin



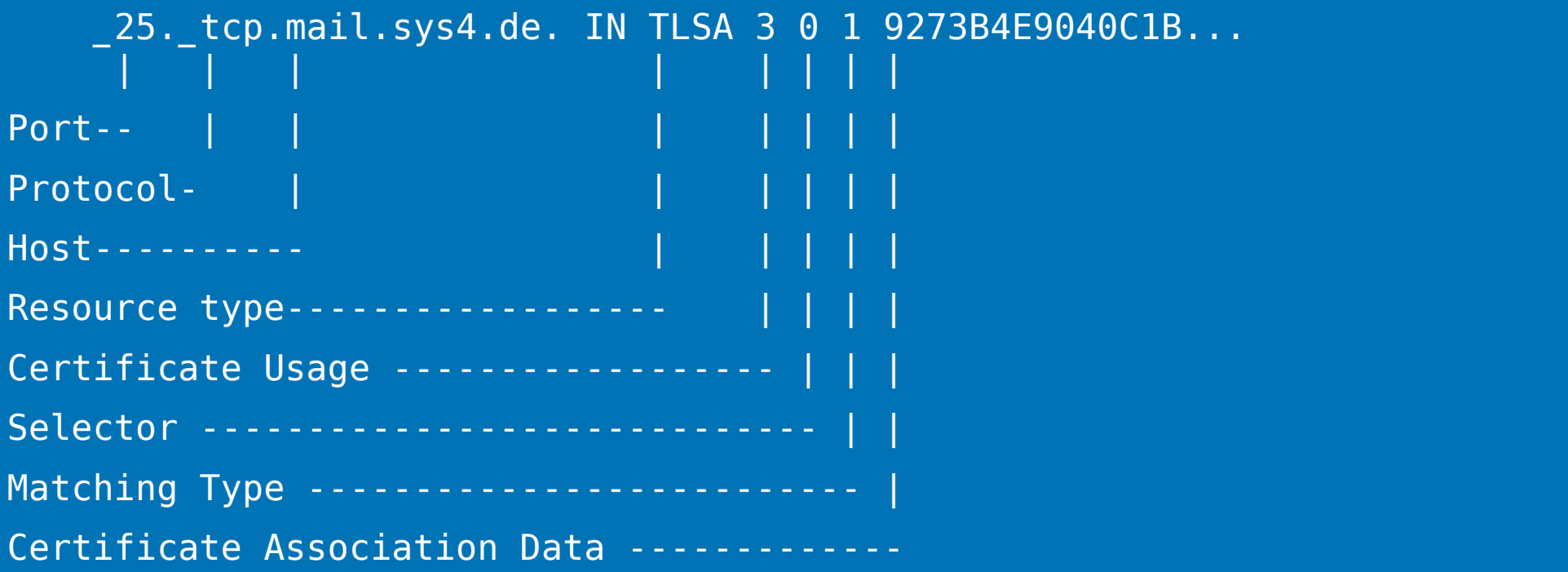
# Consumer Markt Probleme




DNS-Proxy issues, CPE-Modem Studie mit 15 Geräten
sys4 für Unitymedia Deutschland, August 2014

# SMTP

# TLSA Resource Record



# SMTP Security via Opportunistic DANE TLS

- Initial RFC draft published 2013
  Wes Hardaker, Viktor Dukhovni
- RFC 7672 (Standard) seit Oktober 2015
- Erste Implementierungen
  - Postfix
  - OpenSMTPd
  - Exim
- In Produktion @sys4 seit 12/2013

# „Verified“ makes the difference!

## Opportunistisch

```
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

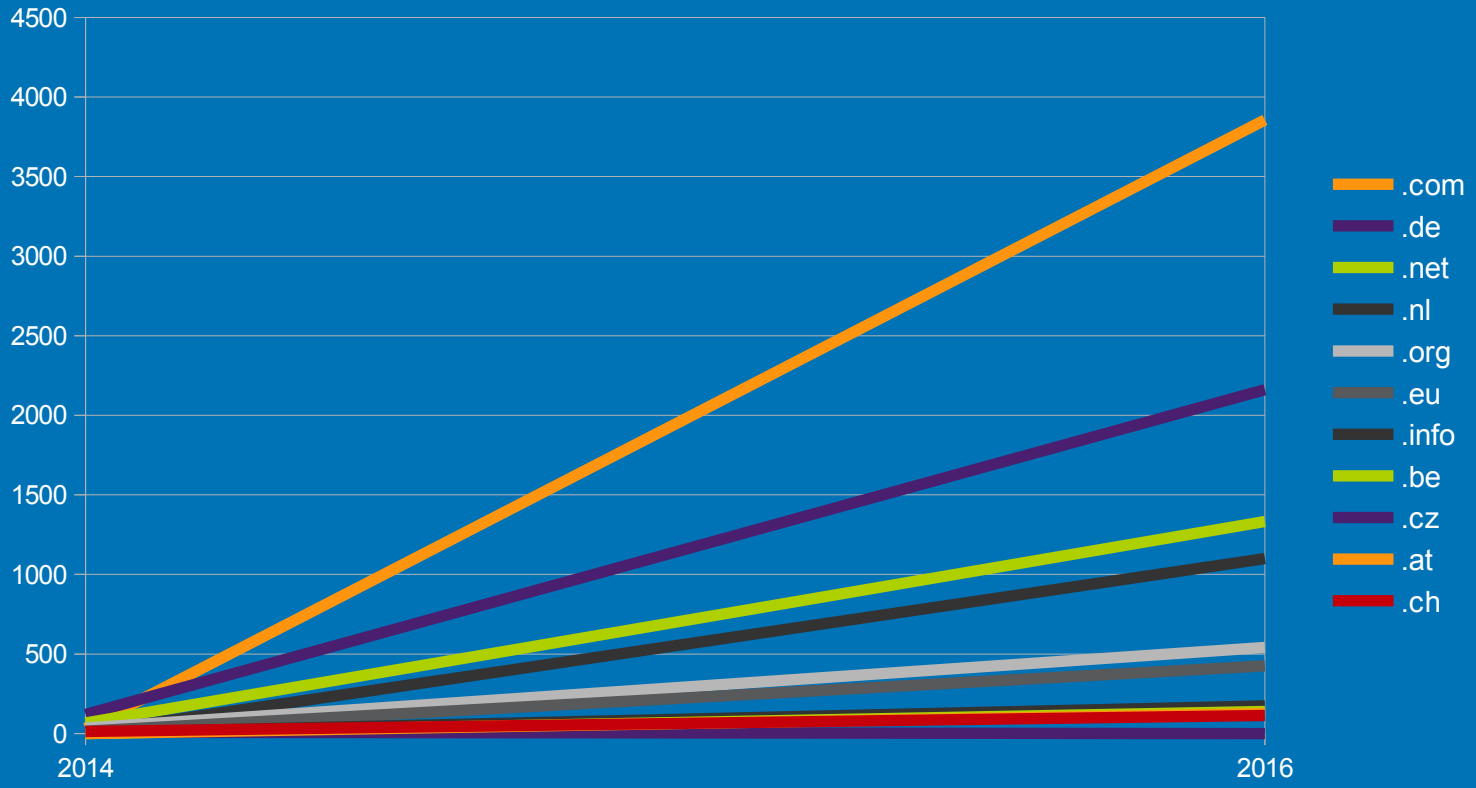
```
Jul 14 11:04:44 mail postfix/smtp[6409]:
  Verified TLS connection established to mail.sys4.de
  [194.126.158.139]:25: TLSv1 with cipher
  ECDHE-RSA-AES256-SHA (256/256 bits)
```

# DANE over SMTP Adoption

Im Februar 2016 ca. 10.780 E-Maildomains

- posteo.de
- mail.de
- bund.de
- Unitymedia (UPC Germany)
- bayern.de
- SWITCH
- IETF

# Top 10 DANE TLDs




Viktor Dukhovni, dane-users@sys4.de mailinglist, 03.02.2016

# Content Encryption

# Ende zu Ende Verschlüsselung

- Brauchbare Sicherheit
- Kein Policy-Kanal
- Komplizierter Schlüsselaustausch
- Komplizierter Widerruf
- Störfaktor Gültigkeit
- Bekannte CA-Probleme

# EasyGPG Ausschreibung BSI

„Das Ziel dieses Projektes ist die einfache, nutzerfreundliche sowie wirksame Ende-zu-Ende E-Mail-Verschlüsselung, bei der im Rahmen des täglichen Gebrauchs alle Vorgänge automatisiert werden. Dazu werden Private und öffentliche Schlüssel automatisch erzeugt und die öffentlichen Schlüssel verteilt.“

http://ausschreibungen-deutschland.de/240960_200_EasyGPG_2015_Bonn

# PGP mit DANE

# OPENPGPKEY Resource Record

- PGP/GPG Public Keys in DNS veröffentlichen
- Localpart der E-Mail als hash-Wert
- PGP-Keyserver ersetzen/ergänzen
- Vorteile gegenüber Keyservern:
  - Key entfernen!
  - Server über DNSSEC-Domain identifiziert

# S/MIME mit DANE

# SMIMEA Resource Record

- E-Mail x509-Zertifikat für S/MIME verteilen
- Hash oder Zertifikat in DNSSEC-gesicherter Domain ablegen
- E-Mail localpart als hash

# Referenz SMIMEA-Milter

- SMIMEA Milter
- Transparent für Anwender
- In- und outbound Verschlüsselung
- Open Source
- Download: https://github.com/sys4/smilla

# Nächste Schritte DANE WG

- raw-Certificates
- Mutual Authentication
  Clientseitige Authentifizierung via TLSA RR
- Payment Association Records
  Account information/bitcoin wallet mit E-Mail Adresse assoziieren

# Märkte für DANE

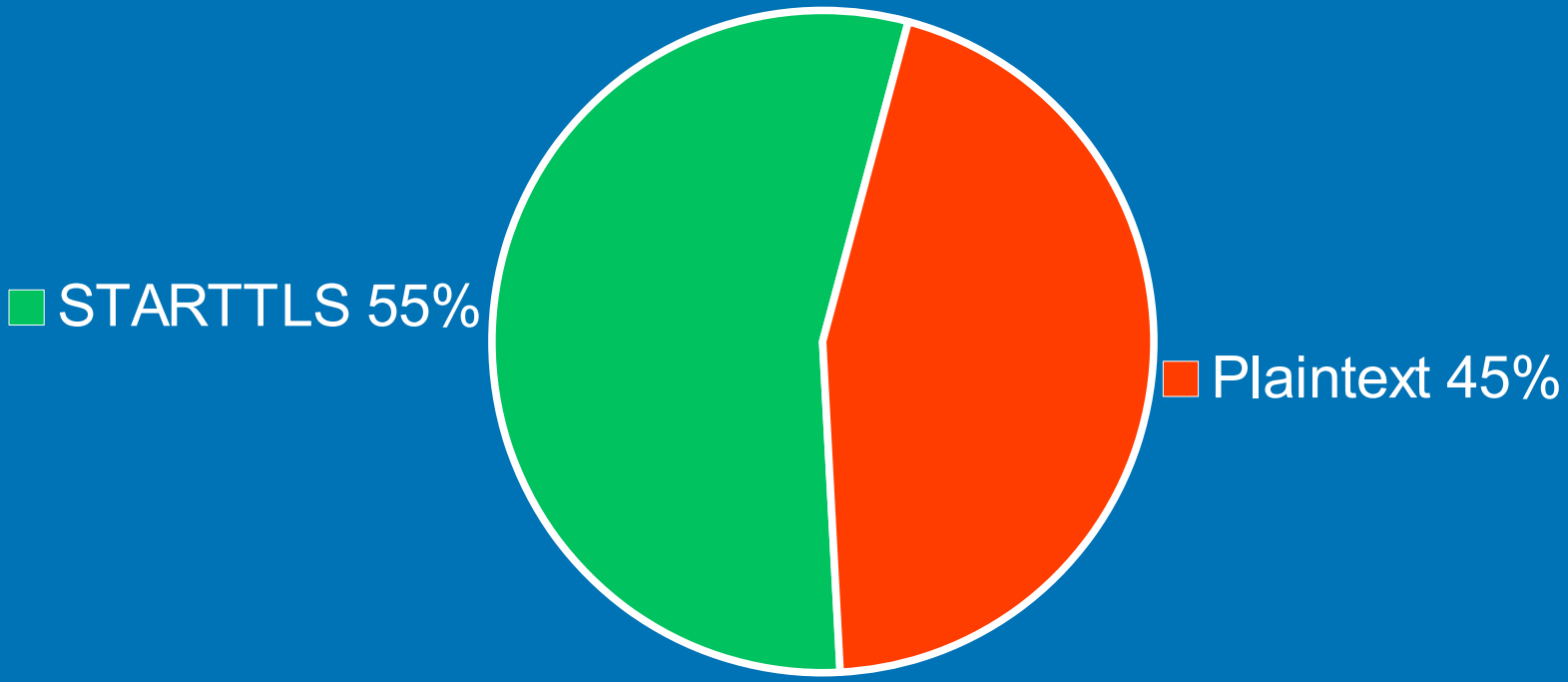
# Wer hat was von DANE?

- „Security services“ Provider
- E-Mailuser mit „definierten“ Sicherheitsanforderungen
- Online-Payment, Versicherungen, Banken
- Unternehmen
- Lieferanten

# Anforderungen des BSI

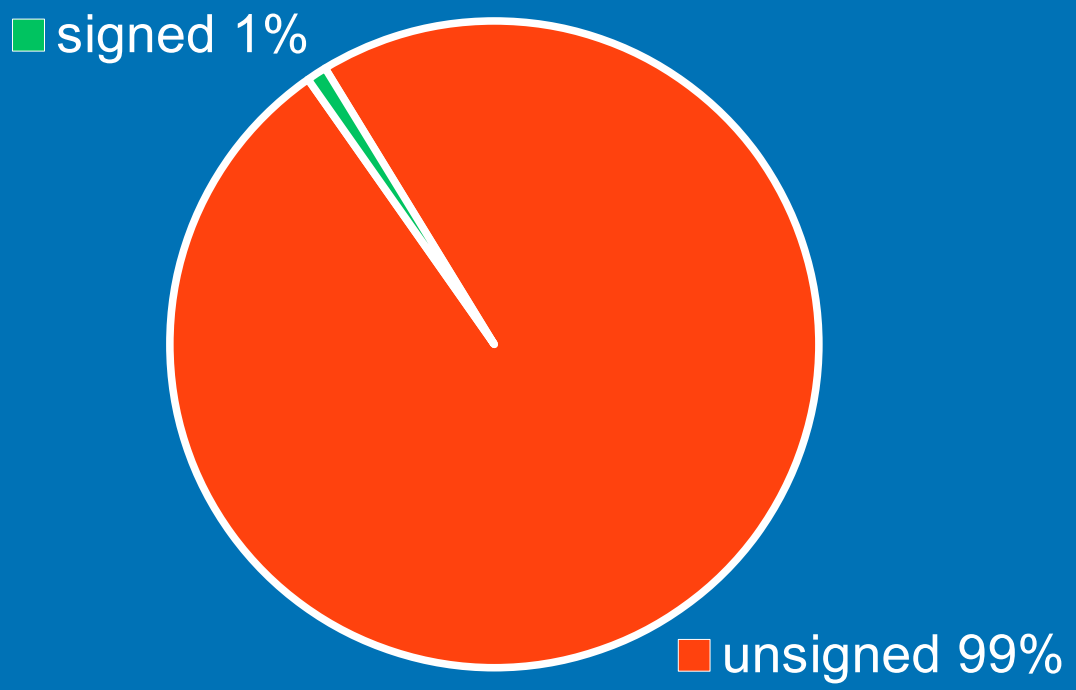
- Technische Richtlinie BSI TR-03108, “Sicherer E-Mail-Transport”
- Anforderungen an E-Mail-Diensteanbieter für einen sicheren Transport von E-Mails
- “Zertifikate … mittelfristig automatisiert durch … DANE/TLSA … über DNSSEC … gesicherte Verbindung vom … EMDA” abrufen
- DANE wird “Verpflichtend bei Rezertifizierung”
- Web.de und GMX führen DANE ein

# TLS in .de

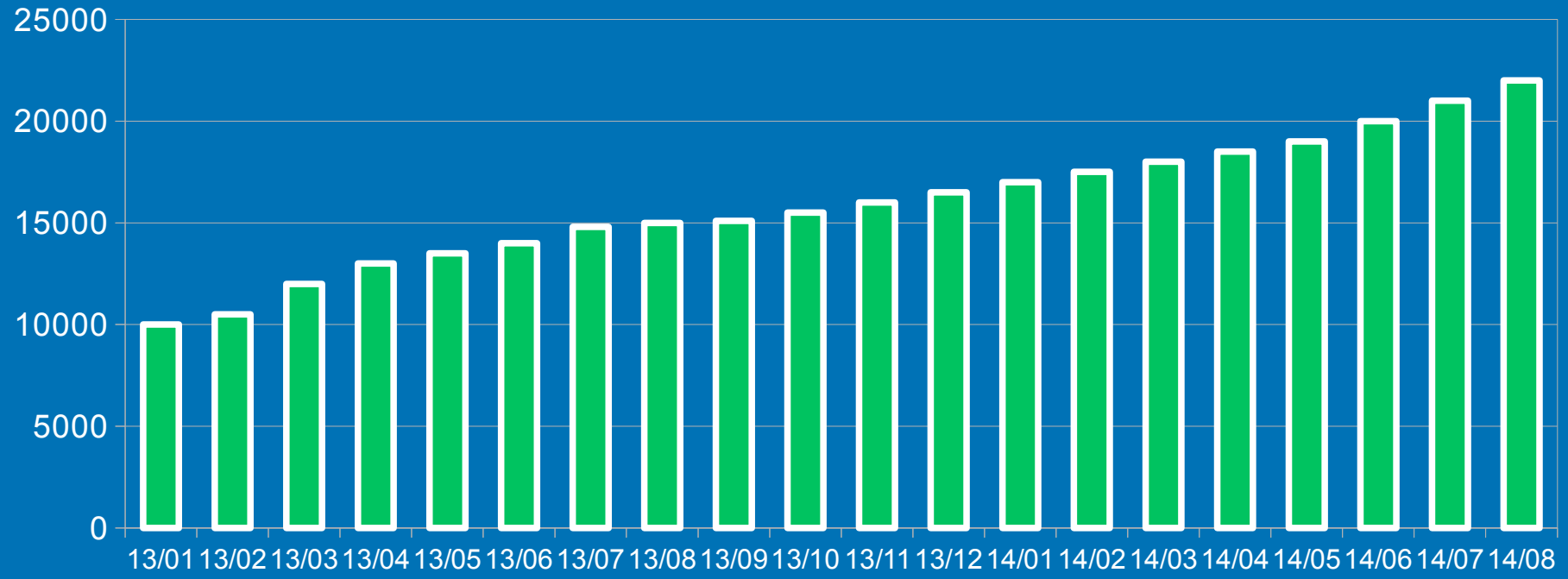



2,7 Mio. MX RR > 275.000 MTAs mit 12.092 IPv6 \o/ MTAs

# DNSSEC in .DE

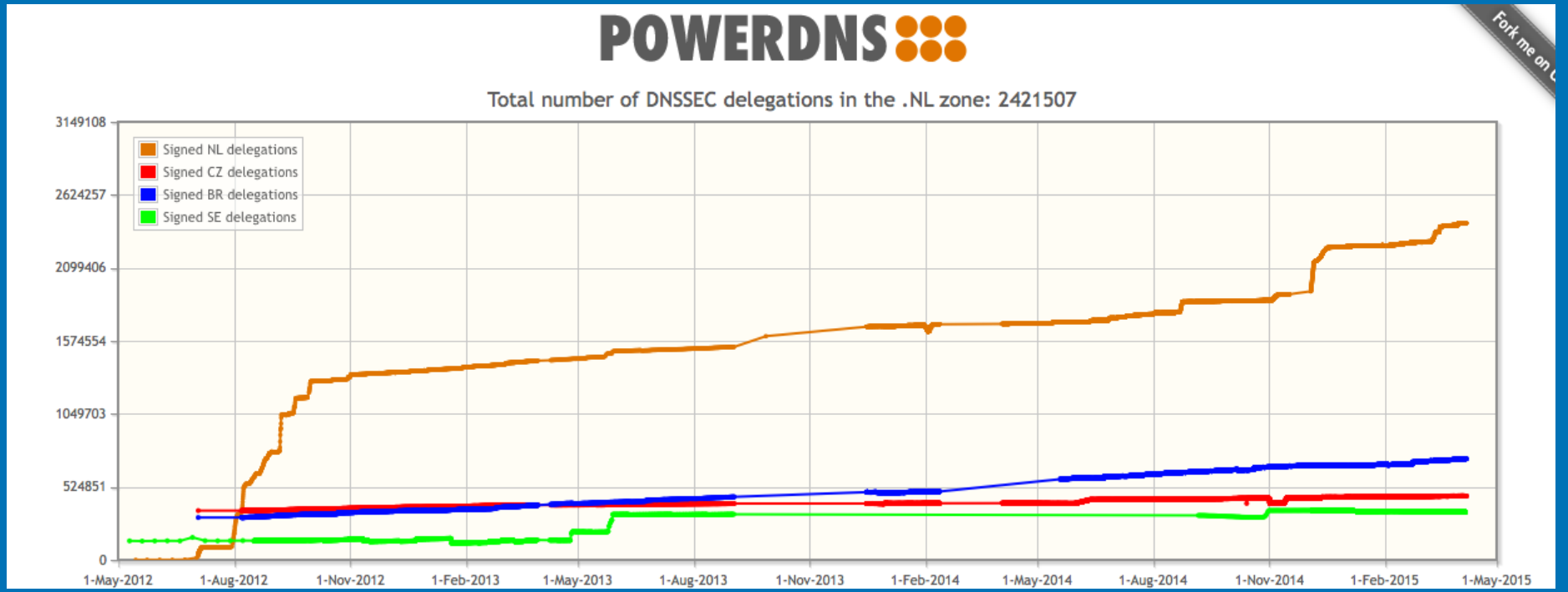


# DNSSEC Wachstum in .de




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

# DNSSEC growth in .NL




PowerDNS DNSSEC deployment graph:
https://xs.powerdns.com/dnssec-nl-graph/

# DANE road-blocks?

# Was man so sagt…

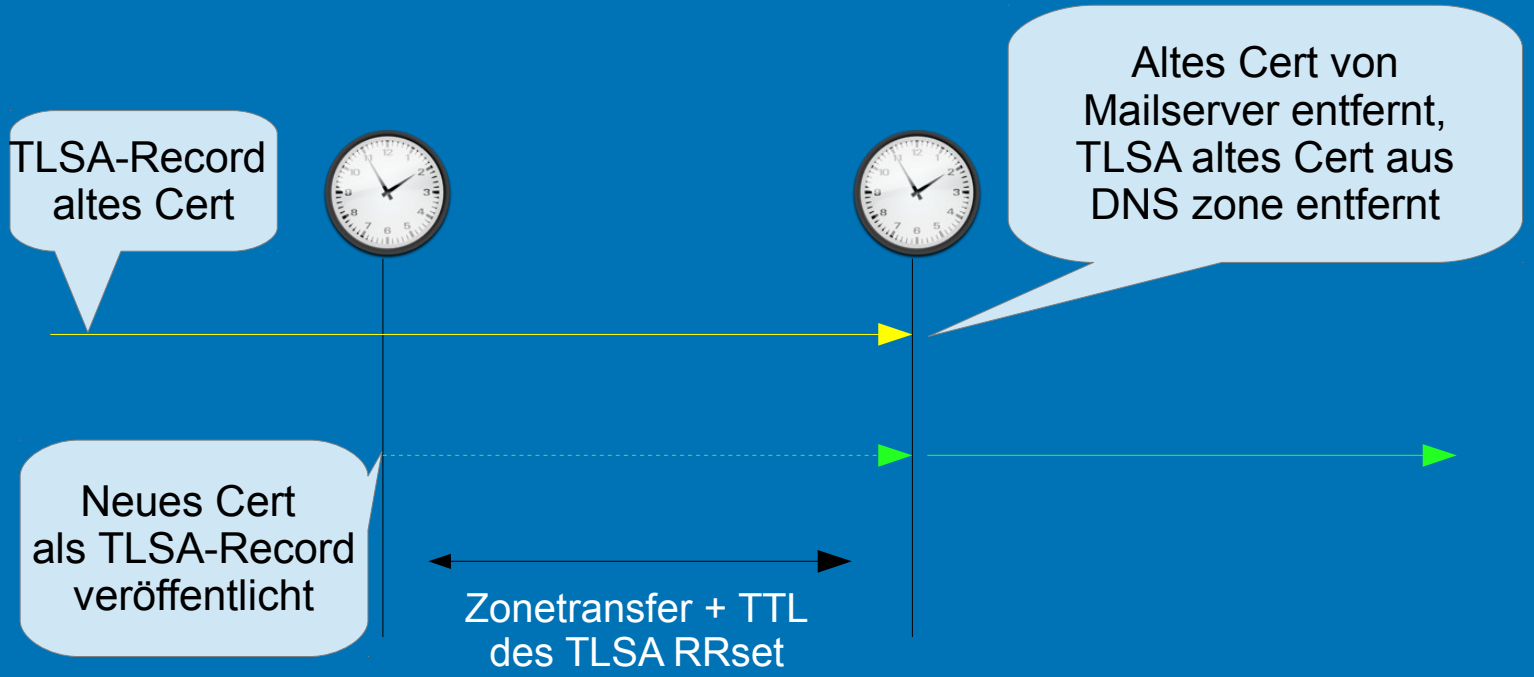
- Registrare bieten keine/unvollständigen DNSSEC-Support an
- DNSSEC ist Technologie aber kein Use Case
- DNSSEC ist mission critical
- Kein Monitoring für DNSSEC/DANE
- Kein Knowhow für automatisiertes Zertifikatsmanagement und/oder DNSSEC-Signing
- Keine Toolchain für automatisiertes Management

# Registrare

- Grosse Registrare bieten kein DNSSEC
- Kosten/Risiken eines Domainumzug zu einem anderen DNSSEC-Registrar
- Hoster und Registrare mit DNSSEC-Diensten

# Koordination

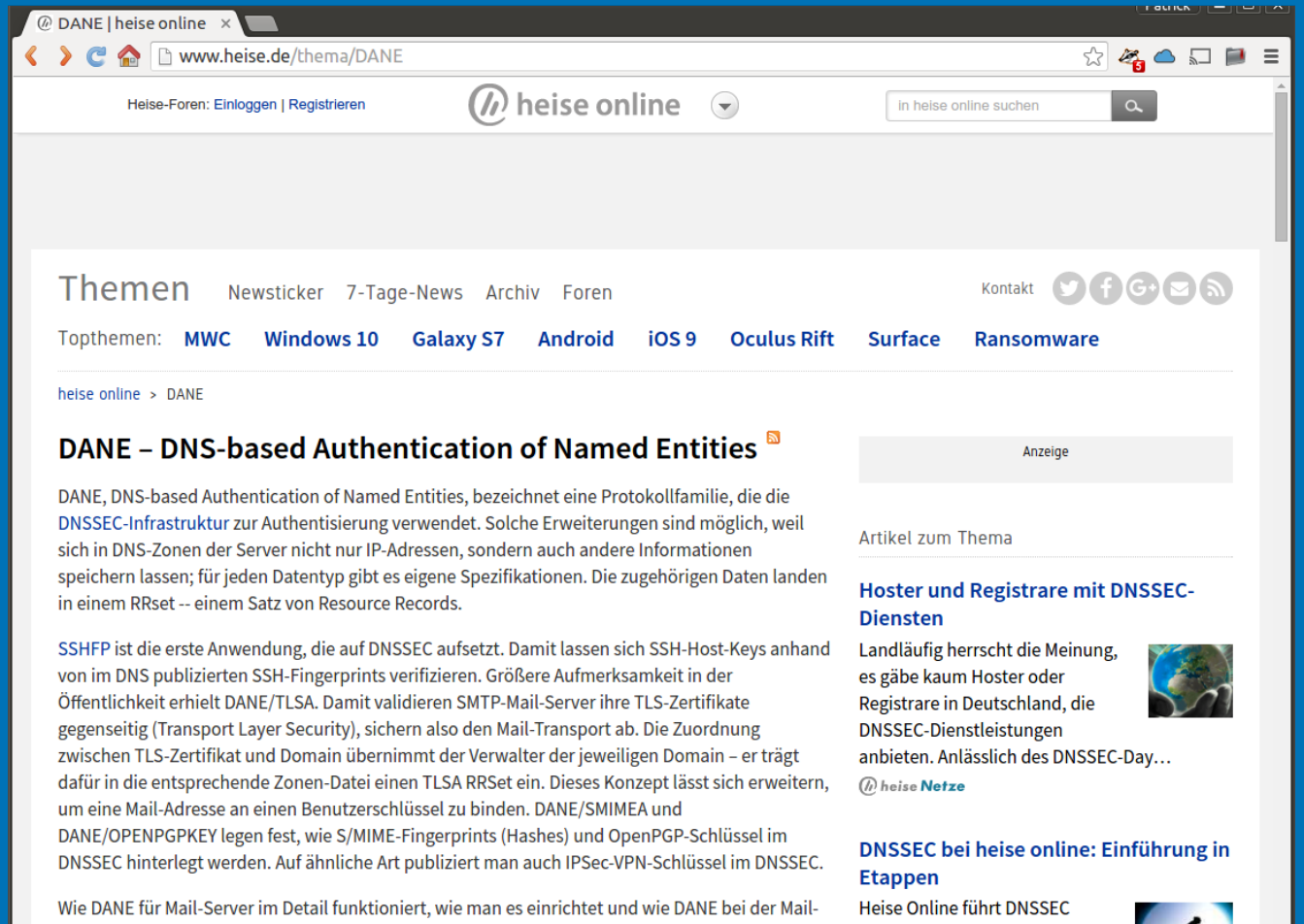
- x509 certs, PGP keys in DNS
- Caches berücksichtigen!



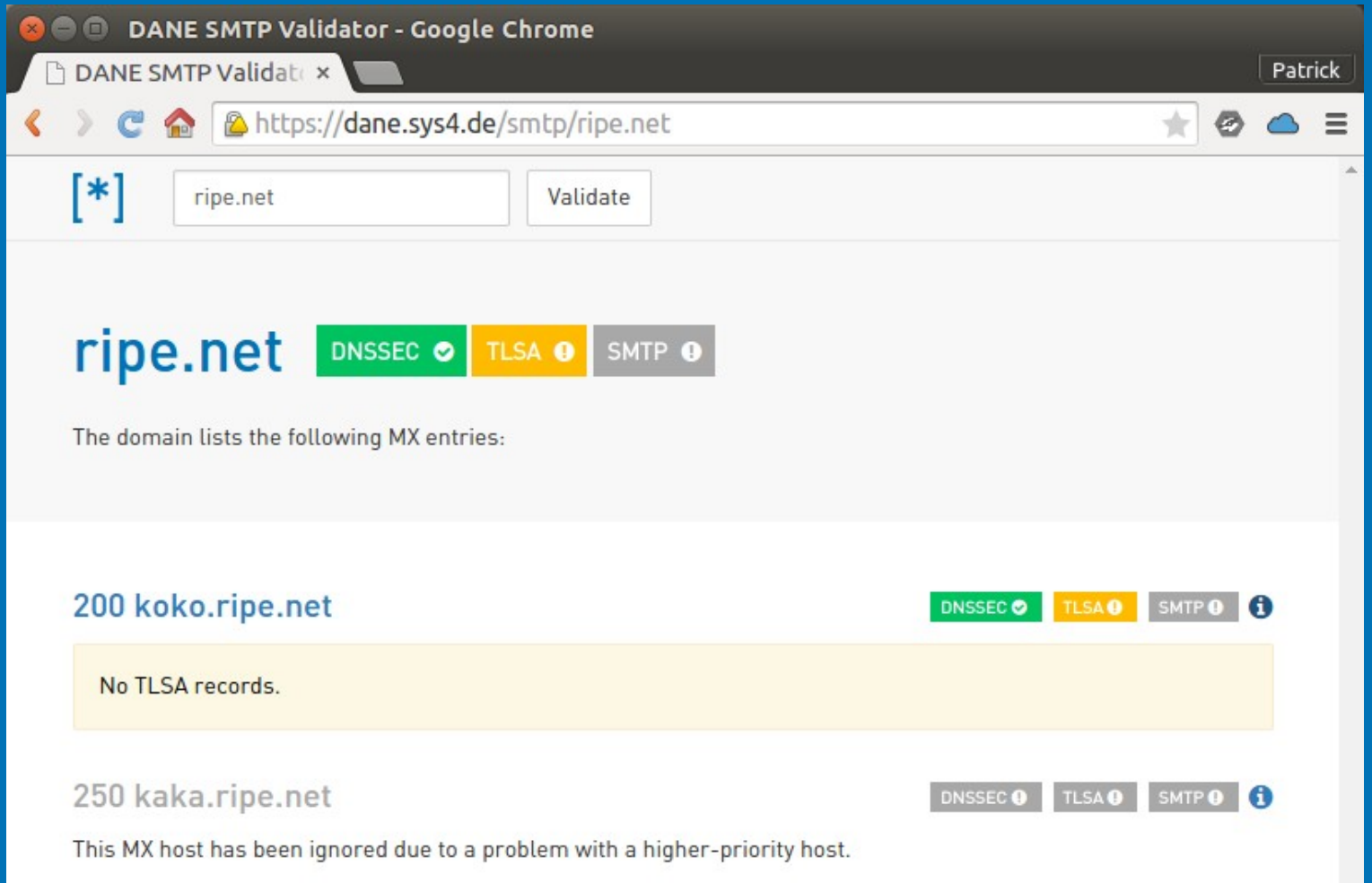
# DNSSEC ist Mission Critical

- DNS ist Stiefkind des Netzwerk Managements
- DNSSEC erfordert oft besseres Service Design
- DNSSEC erfordert „trusted peers“
- Erloschene DNSSEC Signatur läßt Domain „verschwinden“ (bis Signaturen erneuert werden)

# DNSSEC Day

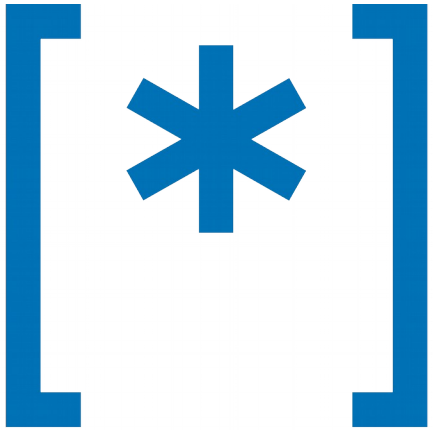

DANE | heise online
www.heise.de/thema/DANE
Heise-Foren: Einloggen | Registrieren
heise online
in heise online suchen
Themen
Newsticker
7-Tage-News
Archiv
Foren
Kontakt
Topthemen:
MWC
Windows 10
Galaxy S7
Android
iOS 9
Oculus Rift
Surface
Ransomware
heise online > DANE
DANE – DNS-based Authentication of Named Entities
DANE, DNS-based Authentication of Named Entities, bezeichnet eine Protokollfamilie, die die DNSSEC-Infrastruktur zur Authentisierung verwendet. Solche Erweiterungen sind möglich, weil sich in DNS-Zonen der Server nicht nur IP-Adressen, sondern auch andere Informationen speichern lassen; für jeden Datentyp gibt es eigene Spezifikationen. Die zugehörigen Daten landen in einem RRset -- einem Satz von Resource Records.
SSHFP ist die erste Anwendung, die auf DNSSEC aufsetzt. Damit lassen sich SSH-Host-Keys anhand von im DNS publizierten SSH-Fingerprints verifizieren. Größere Aufmerksamkeit in der Öffentlichkeit erhielt DANE/TLSA. Damit validieren SMTP-Mail-Server ihre TLS-Zertifikate gegenseitig (Transport Layer Security), sichern also den Mail-Transport ab. Die Zuordnung zwischen TLS-Zertifikat und Domain übernimmt der Verwalter der jeweiligen Domain – er trägt dafür in die entsprechende Zonen-Datei einen TLSA RRSet ein. Dieses Konzept lässt sich erweitern, um eine Mail-Adresse an einen Benutzerschlüssel zu binden. DANE/SMIMEA und DANE/OPENPGPKEY legen fest, wie S/MIME-Fingerprints (Hashes) und OpenPGP-Schlüssel im DNSSEC hinterlegt werden. Auf ähnliche Art publiziert man auch IPSec-VPN-Schlüssel im DNSSEC.
Wie DANE für Mail-Server im Detail funktioniert, wie man es einrichtet und wie DANE bei der Mail-
Anzeige
Artikel zum Thema
Hoster und Registrare mit DNSSEC-Diensten
Landläufig herrscht die Meinung, es gäbe kaum Hoster oder Registrare in Deutschland, die DNSSEC-Dienstleistungen anbieten. Anlässlich des DNSSEC-Day…
heise Netze
DNSSEC bei heise online: Einführung in Etappen
Heise Online führt DNSSEC

# DANE Validator



# Takeaway

- DNSSEC ist einmaliger Aufwand
- Offener Standard
- DANE ermöglicht skalierbares und sicheres Trust Management
- DANE reduziert Managementkosten
- DANE stabilisiert TLS Policies
- Open Source Software ist verfügbar: Postfix, Exim, OpenSMTPd, smilla-MILTER



We do ASCII

sys4.de

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