

**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  
pneBLVYuX8C0ZW9zTHCExtXS1kJrNf48sFRa0WwbZvPy  
1vRiB+c46QRG0kwceDUjzZGtpG3Al2LKBVKw4bxMM0zu  
DeqECrf/n1W8XF6UQcrB0PdTY81Y6IZTUovYhak= )
```

# TLSA Resource Record

```
      _25._tcp.mail.sys4.de. IN TLSA 3 0 1 BA0BDD34C498E8...
      |   |   |
port--  |   |
protokoll- |
host-----
resource type-----
Certificate Usage -----
Selector -----
Matching Type -----
Certificate Association Data -----
```

**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?

DigiNotar | heise online - Google Chrome

DigiNotar | heise on | x

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...

### EU-Behörde für IT-Sicherheit kritisiert Zertifizierungsstellen

07. Dezember 2011, 17:55 Uhr 22 heise Security

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.



## Telepolis

# 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

The screenshot shows a Google Chrome browser window with the address bar displaying <https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks>. The page header features the EFF logo and the text "ELECTRONIC FRONTIER FOUNDATION DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD". A navigation menu includes links for HOME, ABOUT, OUR WORK, DEEPLINKS BLOG, PRESS ROOM, TAKE ACTION, and SHOP. The article content is dated November 11, 2014, by Jacob Hoffman-Andrews. The main heading is "ISPs Removing Their Customers' Email Encryption". The text discusses how ISPs like Verizon tamper with web requests to inject tracking cookies and how other providers use email encryption downgrade attacks to strip the STARTTLS security flag from email traffic. A sidebar on the right contains a "Donate to EFF" button, a "Stay in Touch" sign-up form, and a section titled "NSA Spying" with a link to [eff.org/nsa-spying](http://eff.org/nsa-spying).

ISPs Removing Their Customers' Email Encryption | Electronic Frontier Foundation - Google Chrome

ISPs Removing Their

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

**EFF** ELECTRONIC FRONTIER FOUNDATION  
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

SEARCH

HOME ABOUT OUR WORK DEEPLINKS BLOG PRESS ROOM TAKE ACTION SHOP

NOVEMBER 11, 2014 | BY JACOB HOFFMAN-ANDREWS

## ISPs Removing Their Customers' Email Encryption

Recently, Verizon was caught **tampering with its customer's web requests** to inject a **tracking super-cookie**. Another network-tampering threat to user safety has come to light from other providers: **email encryption downgrade attacks**. 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. The **STARTTLS flag** is an essential security and privacy protection used by an email server to request encryption when talking to another server or client.<sup>1</sup>

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. Some firewalls, including **Cisco's PIX/ASA firewall** do this in order to monitor for spam originating from within their network and prevent it from being sent. Unfortunately, this causes collateral damage: the sending server will proceed to transmit plaintext email over the public Internet, where it is subject to eavesdropping and interception.

This type of STARTTLS stripping attack has mostly gone unnoticed because it tends to be applied to

Donate to EFF

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying

[eff.org/nsa-spying](http://eff.org/nsa-spying)

EFF is leading the fight against the NSA's

# 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

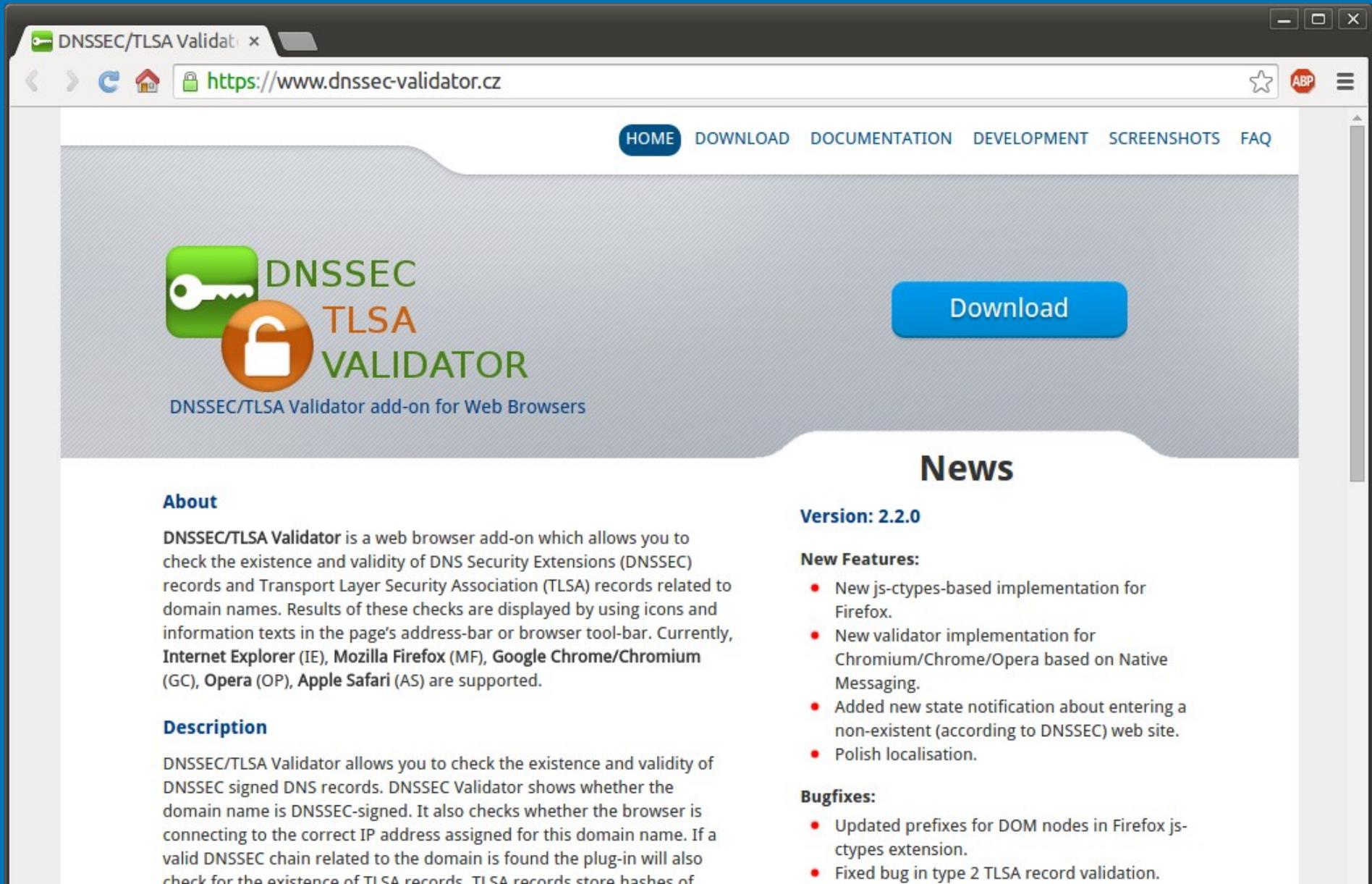
- > **OpenPGP**  
Associate Public Keys mit E-Mail Adresse
- > **S/MIME**  
Associate Certificates with Domain Names
- > **HTTPS**  
Service mit Cert verbinden
- > **SMTP**  
Service mit Cert verbinden

# HTTPS



The screenshot shows a Mozilla Firefox browser window with the title "sys4 Enterprise Experts - Home - Mozilla Firefox". The address bar displays "https://sys4.de/de/". A security notification is visible, stating "https://sys4.de Zertifikat entspricht TLSA" and "Das Serverzertifikat für diese Domäne wurde durch DANE Protokoll bestätigt. Das Zertifikat entspricht dem durch DNSSEC gesicherten TLSA Eintrag." Below the notification is a "Mehr info" button. The website content includes the logo "[\*]sys4", navigation links for "Messaging", "Automation", "Identity Management", and "BLOG", and a language selector for "English". At the bottom, there is a black and white photograph of four men, with a blue text overlay that reads: "Wir sind ein Team namhafter Open-Source-Experten. Unsere Stärke sind interdisziplinäre Systeme."

# Browser Plugin



The screenshot shows a web browser window with the address bar displaying <https://www.dnssec-validator.cz>. The page features a navigation menu with links for HOME, DOWNLOAD, DOCUMENTATION, DEVELOPMENT, SCREENSHOTS, and FAQ. The main content area includes the DNSSEC/TLSA Validator logo, which consists of a green key icon and an orange padlock icon, followed by the text "DNSSEC TLSA VALIDATOR" and "DNSSEC/TLSA Validator add-on for Web Browsers". A prominent blue "Download" button is positioned to the right of the logo. Below this, there is a "News" section with the following content:

## About

DNSSEC/TLSA Validator is a web browser add-on which allows you to check the existence and validity of DNS Security Extensions (DNSSEC) records and Transport Layer Security Association (TLSA) records related to domain names. Results of these checks are displayed by using icons and information texts in the page's address-bar or browser tool-bar. Currently, **Internet Explorer (IE)**, **Mozilla Firefox (MF)**, **Google Chrome/Chromium (GC)**, **Opera (OP)**, **Apple Safari (AS)** are supported.

## Description

DNSSEC/TLSA Validator allows you to check the existence and validity of DNSSEC signed DNS records. DNSSEC Validator shows whether the domain name is DNSSEC-signed. It also checks whether the browser is connecting to the correct IP address assigned for this domain name. If a valid DNSSEC chain related to the domain is found the plug-in will also check for the existence of TLSA records. TLSA records store hashes of

## News

**Version: 2.2.0**

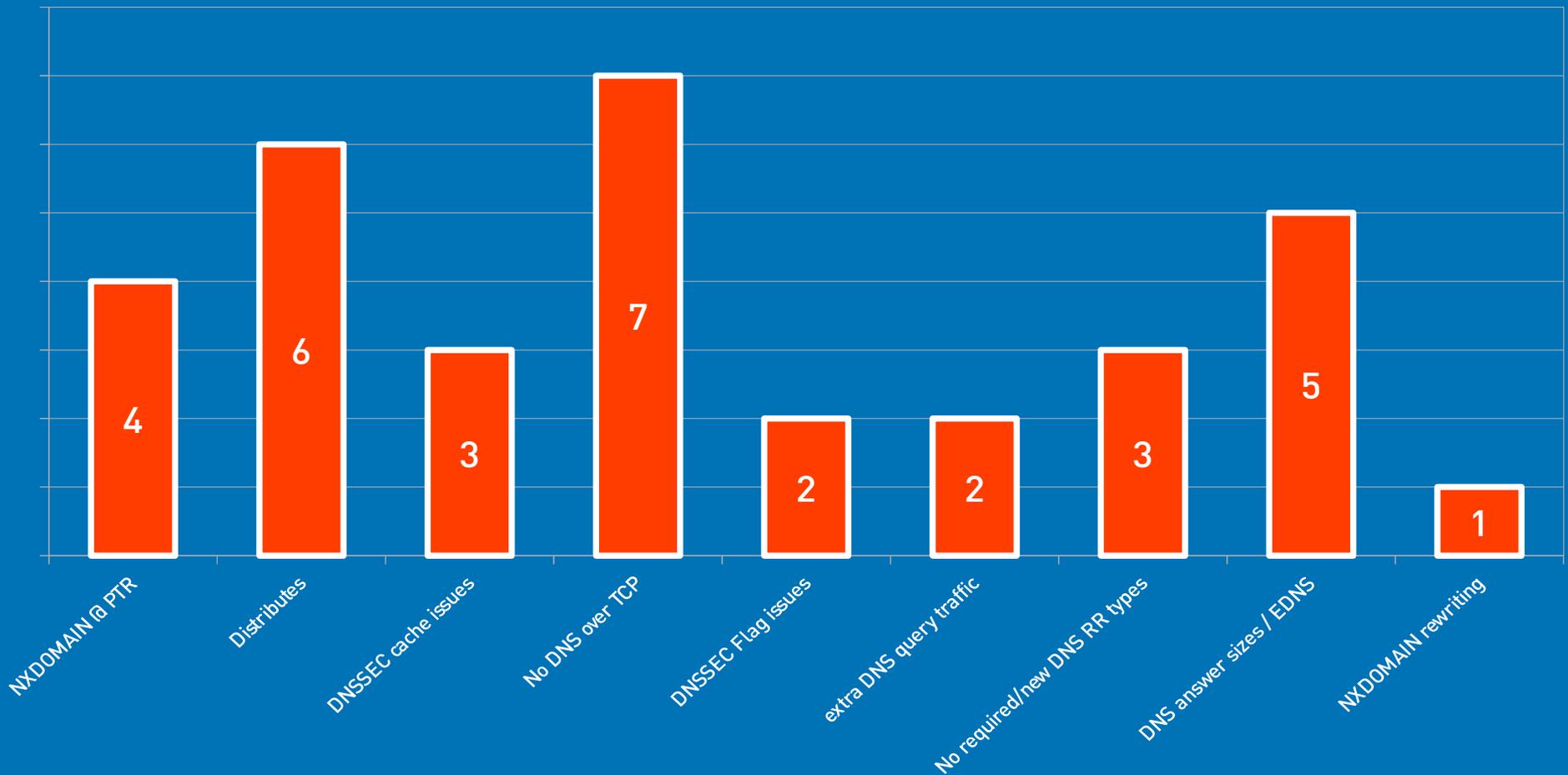
**New Features:**

- New js-ctypes-based implementation for Firefox.
- New validator implementation for Chromium/Chrome/Opera based on Native Messaging.
- Added new state notification about entering a non-existent (according to DNSSEC) web site.
- Polish localisation.

**Bugfixes:**

- Updated prefixes for DOM nodes in Firefox js-ctypes extension.
- Fixed bug in type 2 TLSA record validation.

# 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)
```

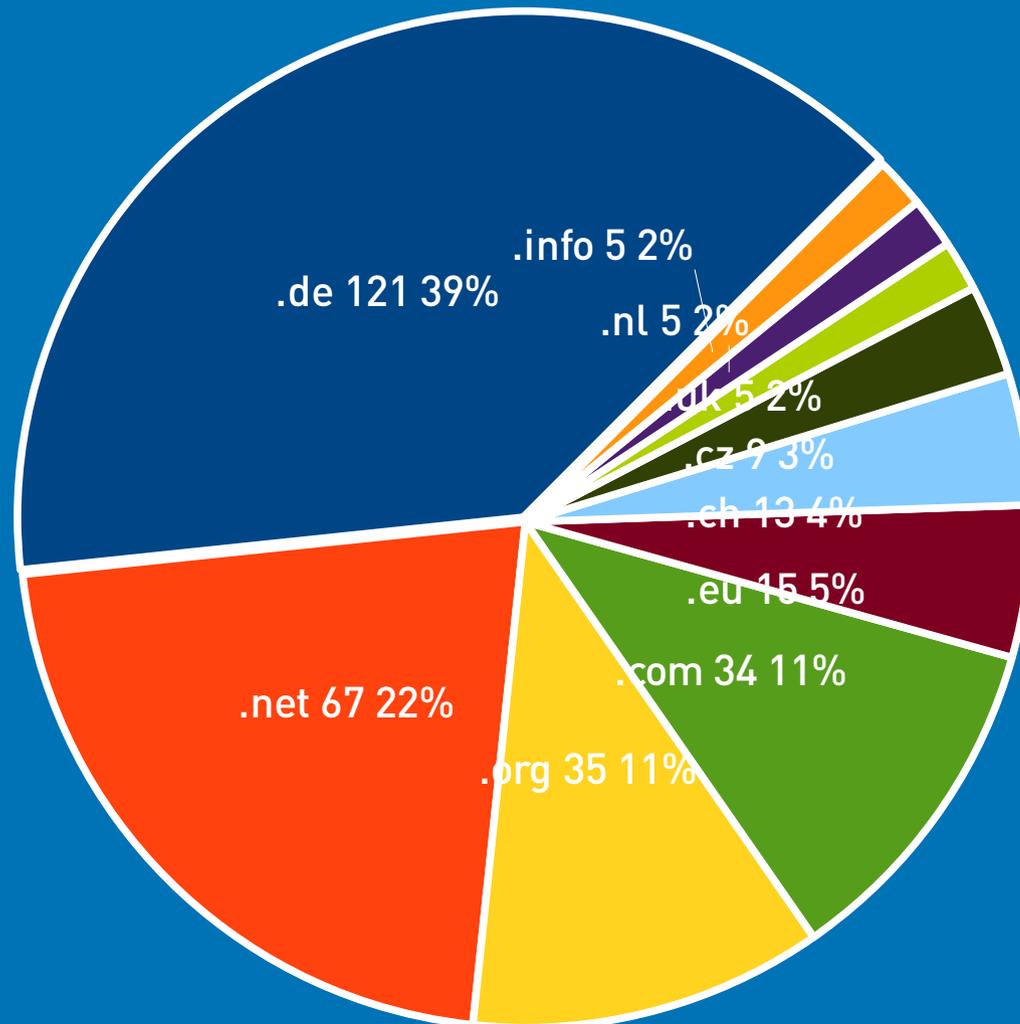
# Next Steps DANE WG

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

# Adoption

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

# Top 10 DANE TLDs



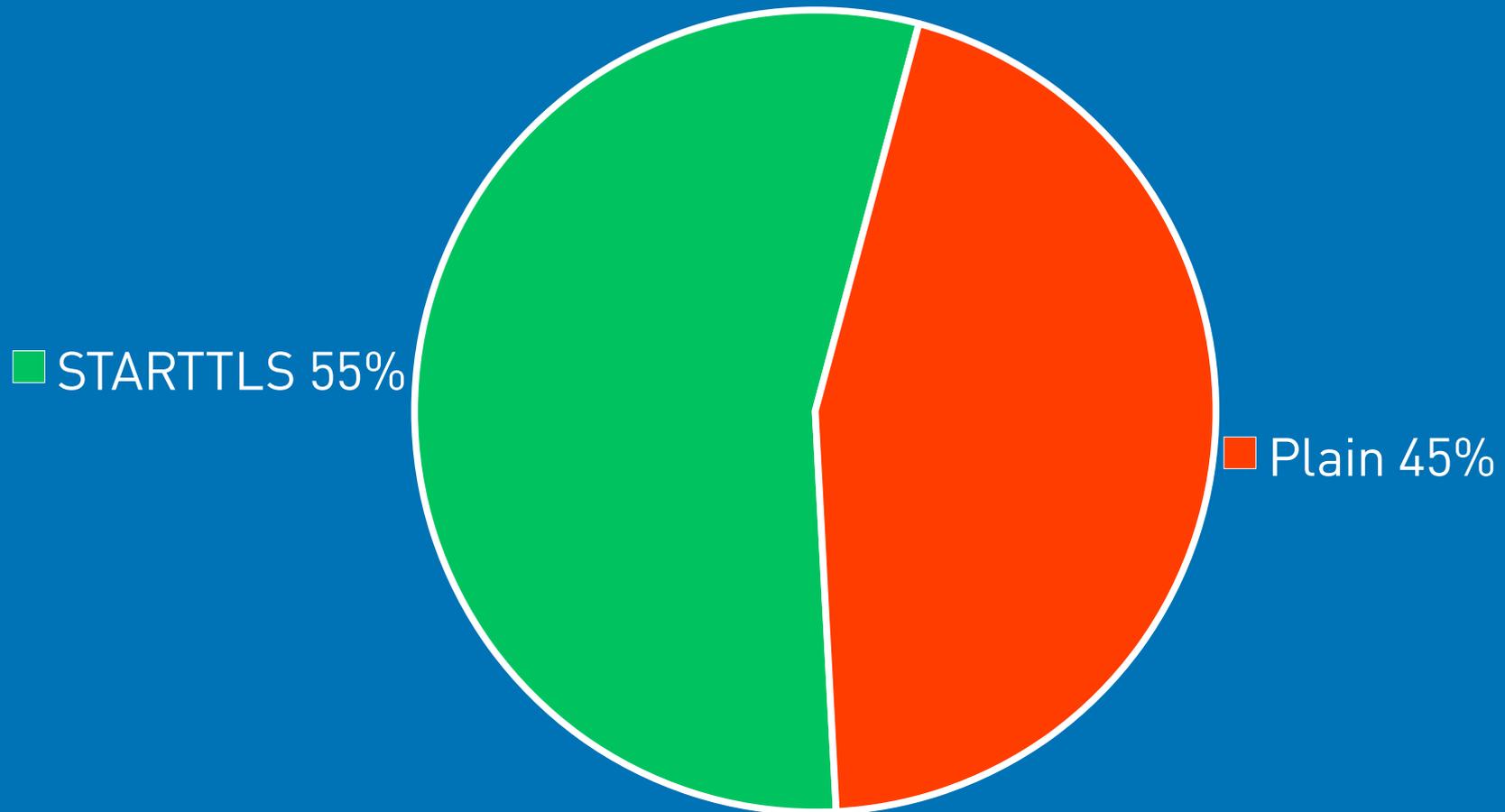
Viktor Dukhovni auf IETF DANE Mailingliste, 14.11.2014

# Märkte für DANE

# Wer braucht DANE?

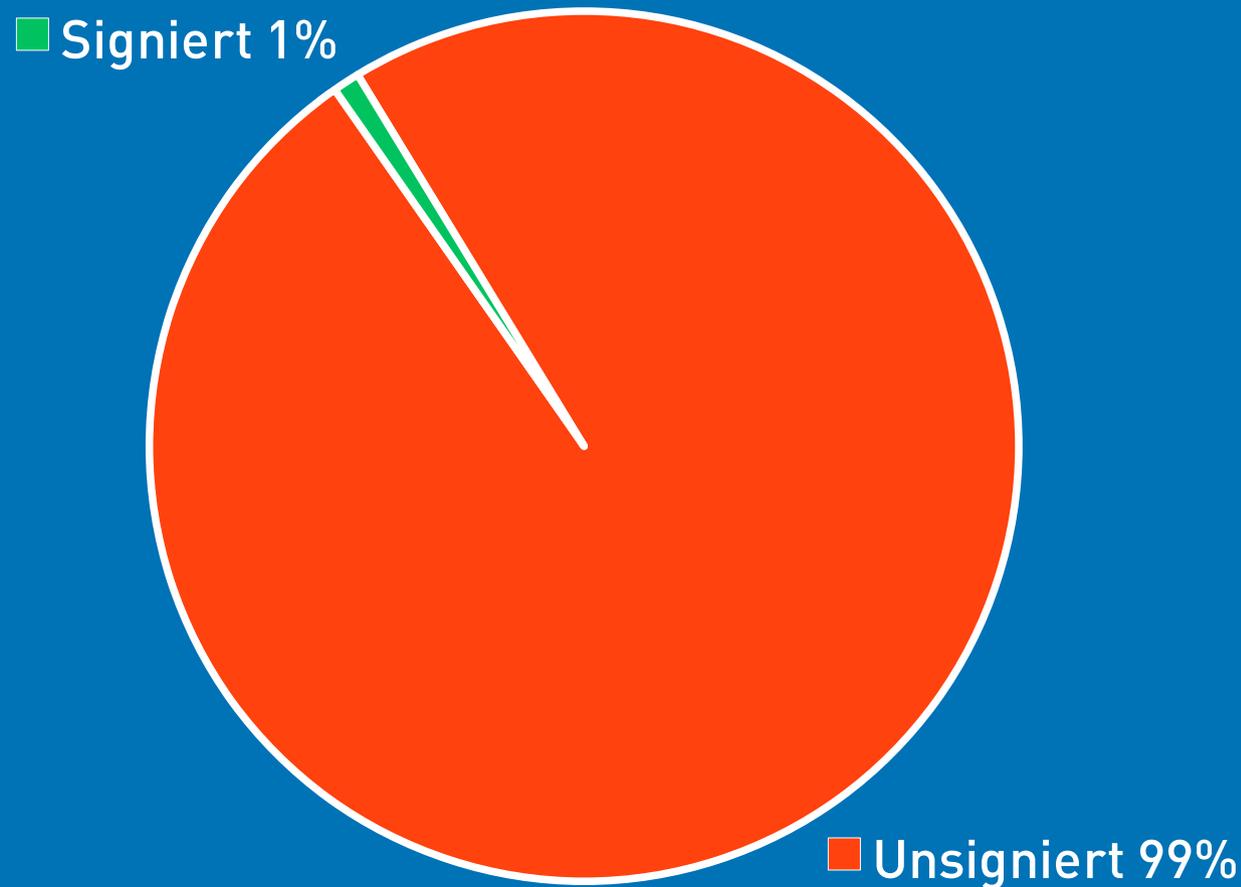
- > Anbieter gesicherter Dienste
- > Mailteilnehmer mit „definiertem Sicherheitsbedürfnis“
- > Online-Payment, Versicherungen, Banken
- > Großunternehmen
- > Zulieferer

# TLS in .de



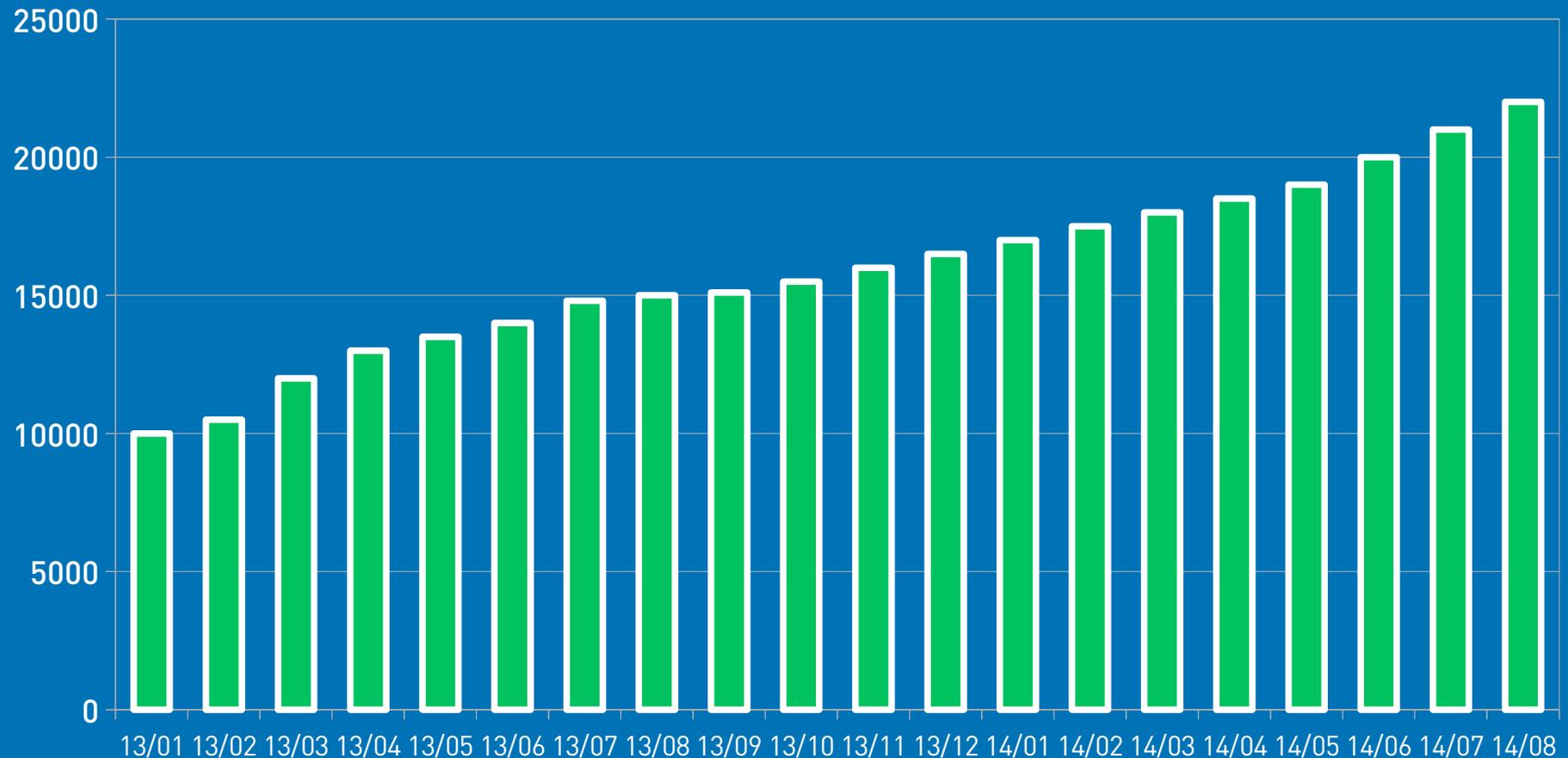
2,7 Mio. MX RR > 275.000 MTAs davon 12.092 IPv6 MTAs \o/

# 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



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

**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

The screenshot shows the NLnet Labs website homepage. The browser address bar displays 'www.nlnetlabs.nl'. The page features a navigation menu with links for 'NLnetLabs', 'Projects', 'Publications', 'Support', and 'Blog'. The main content area is divided into several sections:

- About:** A paragraph describing Stichting NLnet Labs as a not-for-profit foundation founded in 1999 in the Netherlands, with a mission to provide globally recognized innovations and expertise for those technologies that turn a network of networks into an Open Internet for All. It also mentions that NLnet Labs is a charitable foundation (ANBI) and its main source of income is a subsidy from the NLnet Foundation.
- Downloads:** A list of software releases including NSD 4.1.0, Unbound 1.4.22, and Idns 1.6.17. It also lists subsidy providers: OpenNetlabs, nlnet, and SIDN, and contributors: SECURE44.
- Software updates:** A section titled 'NSD 4.1.0 released' dated Thu, 4 Sep 2014, highlighting features for less memory use, faster read/write, wildcard includes, bugfixes, and fixes slowdown after a long time.
- Publications:** A section titled 'NLnet Labs Annual Report 2013' dated Wed, 27 MAy 2013, stating that they are happy to present the annual report and describe their impact.
- News:** A section titled 'Wanted: software developer and senior developer/architect' dated Mon, 1 Sep 2014, indicating they are looking for a software developer and a senior developer/architect to design and implement Open Source software.

SMTP- und DNS-Referenztools von Referenzpartnern

# DANE Validator

sys4 DANE Test - Google Chrome

sys4 DANE Test x

https://dane.sys4.de

Domain:

Start DANE Test

**unitybox.de:** Checking DANE validity...

**unitybox.de**

mx4.unitybox.de. IN MX 0 mx4.unitybox.de.

usable TLSA record: \_25\_tcp.mx4.unitybox.de. IN TLSA 3 0 1 F66EA43B85F27B9C1105800B180E84B1CC1B5C0C47A770E8702F44A07BF3512A

**mx4.unitybox.de**

IP v4	Result
80.69.98.122	
IP v6	Result
2a02:908:2:1200:0:0:0:122	

# In wenigen Worten...

- › DANE ist ein offener Standard  
(WGGLC 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>