

One year of DANE

Tales and Lessons Learned

sys4.de

DANE secures Security

Why secure Security?

Encryption Models

Opportunistic Encryption

- > Expect anything
- > Proceed if absent
- > Try if offered
- > Proceed unencrypted on failure
- > Silent on failure

Mandatory Encryption

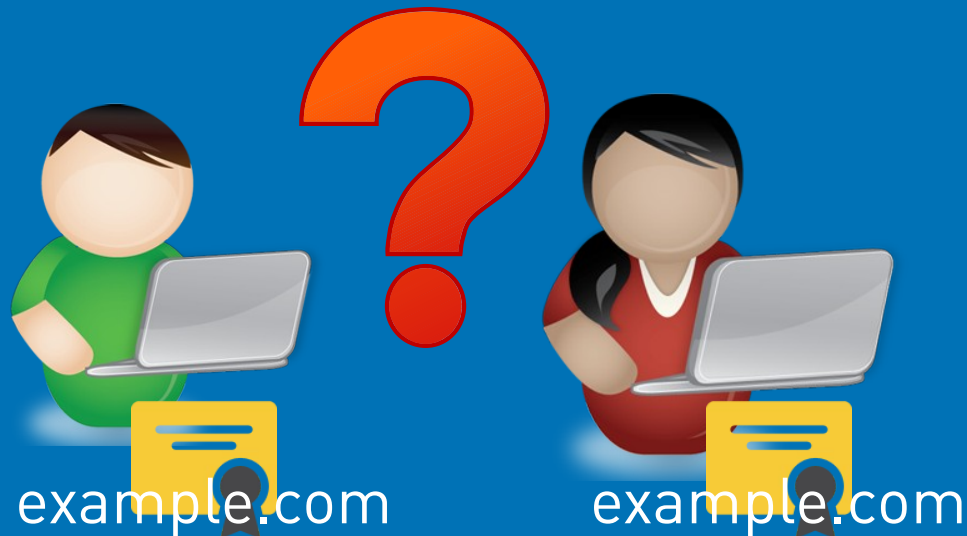
- > Expect encryption
- > Fail and alarm if absent
- > Identify other side
- > Fail and alarm if identity mismatch
- > Encrypt or fail
- > Alarm on failure

Issues with opportunistic TLS

- > 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?

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 Ambak 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 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
```


Session downgrade

The screenshot shows a Google Chrome browser window with the URL <https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks>. The page features the EFF logo and navigation links: HOME, ABOUT, OUR WORK, DEEPLINKS BLOG, PRESS ROOM, TAKE ACTION, and SHOP. The article is dated November 11, 2014, by Jacob Hoffman-Andrews. The main text discusses how ISPs are removing email encryption, specifically mentioning Verizon's tampering with web requests and the STARTTLS flag. A sidebar on the right includes a 'Donate to EFF' button, a 'Stay in Touch' section with email and postal code fields, and an 'NSA Spying' section with a link to eff.org/nsa-spying.

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

ISPs Removing Their x

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

EFF ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

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.¹

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.

Donate to EFF

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying

eff.org/nsa-spying

MITM Attack

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



Automation. NOT!

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

Securing Security

The Plan

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

Welcome to DANE!

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**
Associate Certificates with Domain Names and email addresses

HTTPS

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 -----							

TLSA RR query

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

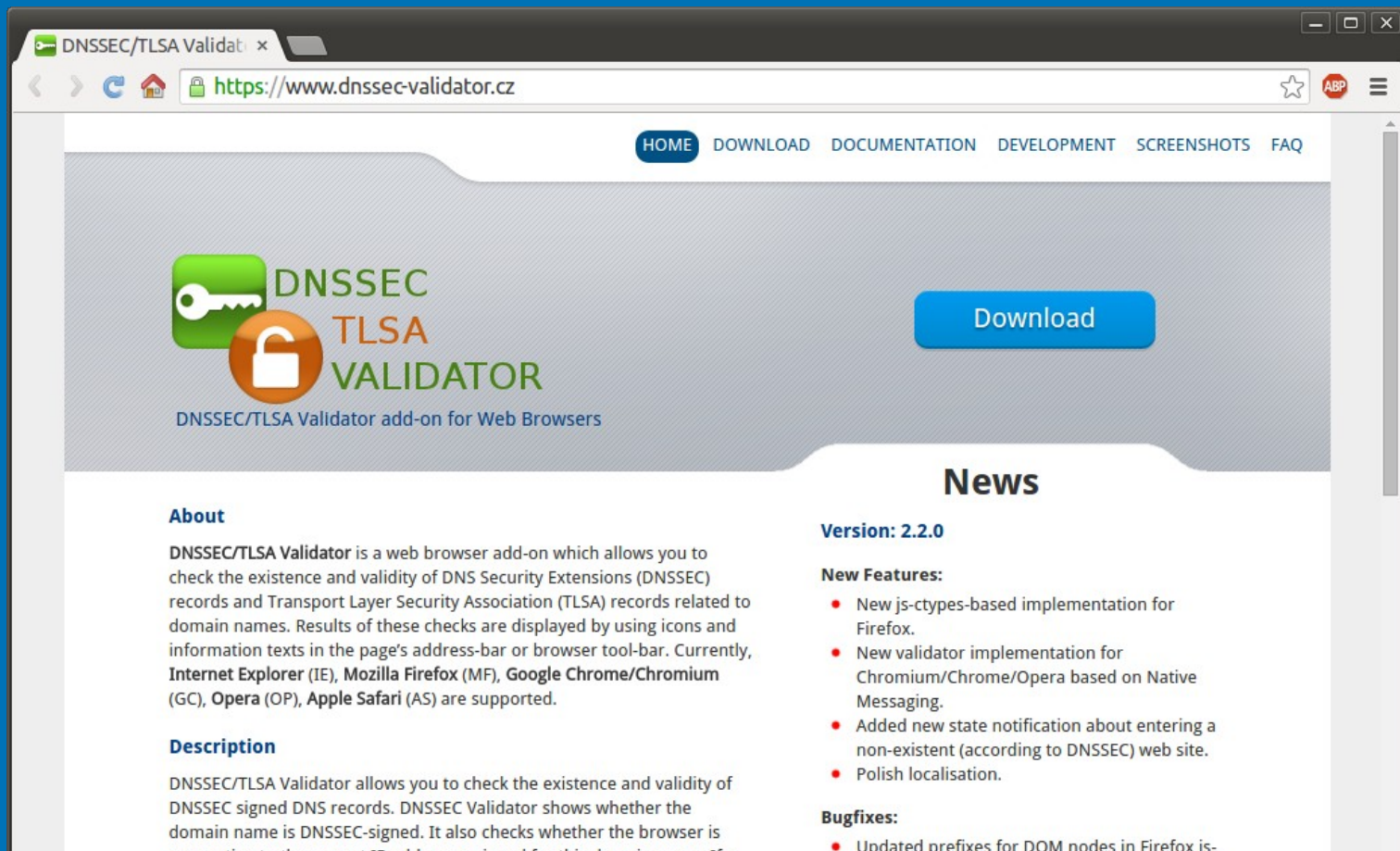
```
_443._tcp.mail.sys4.de.3600 IN TLSA 3 0 1 (
    9273B4E9040C1B9EE7C946EFC0BA8AAF2C6E5F05A1B2
    C960C41655E32B15CBE0 )
```

```
_443._tcp.mail.sys4.de.3600 IN RRSIG TLSA 8 5 3600 (
    20141124104604 20141117195102 19786 sys4.de.
    afEJbtmKZVn995XiI2BFQwYKC1ZfcsIK/j2JA9C8oYSp
    pneBLVYuX8C0ZW9zTHCExtXS1kJrNf48sFRa0WwbZvPy
    1vRiB+c46QRG0kwceDUjzZGtpG3Al2LKBVKw4bxMM0zu
    DeqECrf/n1W8XF6UQcrB0PdTY81Y6IZTUovYhak= )
```

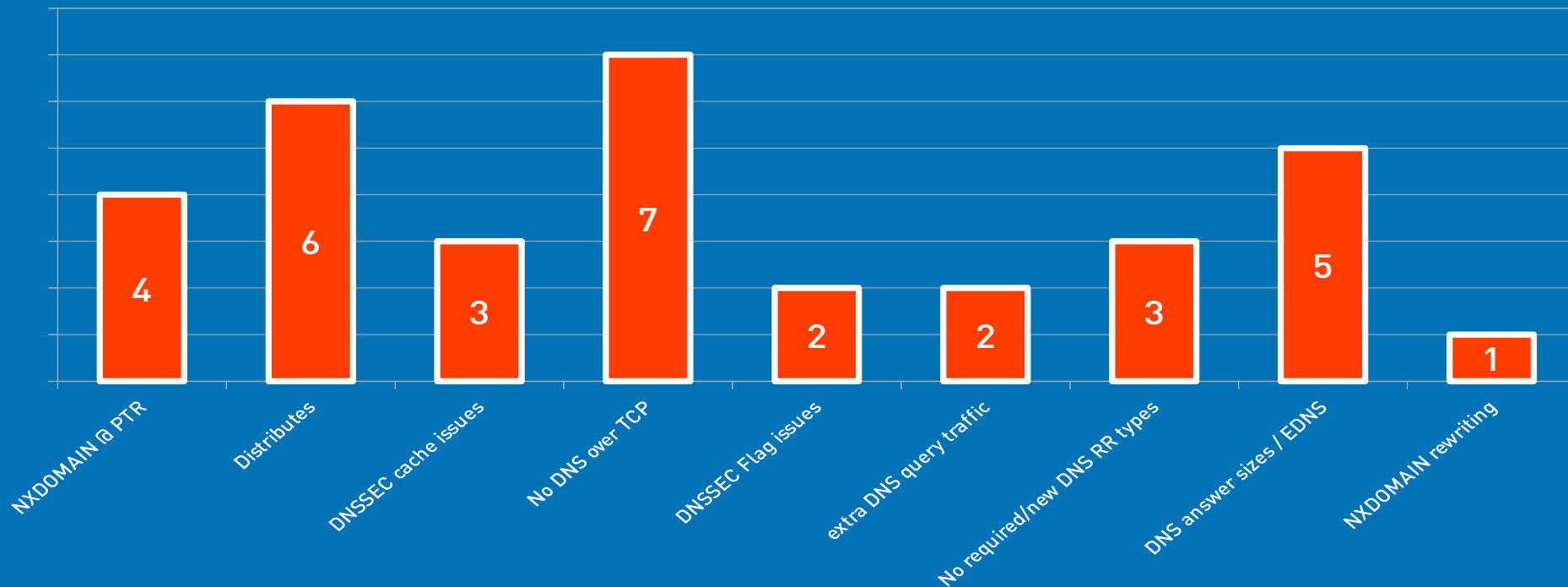
HTTPS

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 popup is visible, stating: "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." Below the popup, the website header includes the "[*]sys4" logo, navigation links for "Messaging", "Automation", "Identity Management", and "BLOG", and a language selector for "English". The main content area features a black and white photograph of four men. At the bottom, a blue banner contains the text: "Wir sind ein Team namhafter Open-Source-Experten."

Browser Plugin



Consumer Market Problems



DNS-Proxy issues, CPE-modem study over 15 common CPE devices
sys4 for Unitymedia Deutschland, August 2014

SMTP

TLSA Resource Record

	_25._tcp.mail.sys4.de.	IN	TLSA	3	0	1	9273B4E9040C1B...
Port--							
Protocol-							
Host-----							
Resource type-----							
Certificate Usage -----							
Selector -----							
Matching Type -----							
Certificate Association Data -----							

SMTP Security via Opportunistic DANE TLS

- > Initial RFC draft published 2013
Wes Hardaker, Viktor Dukhovni
- > Currently in DANE WG „Last Call“ ends 2015-05-07
- > First implementations
 - > Postfix
 - > OpenSMTPd
 - > Exim
- > In production @sys4 since 12/2013

„Verified“ makes all the difference

Today

```
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

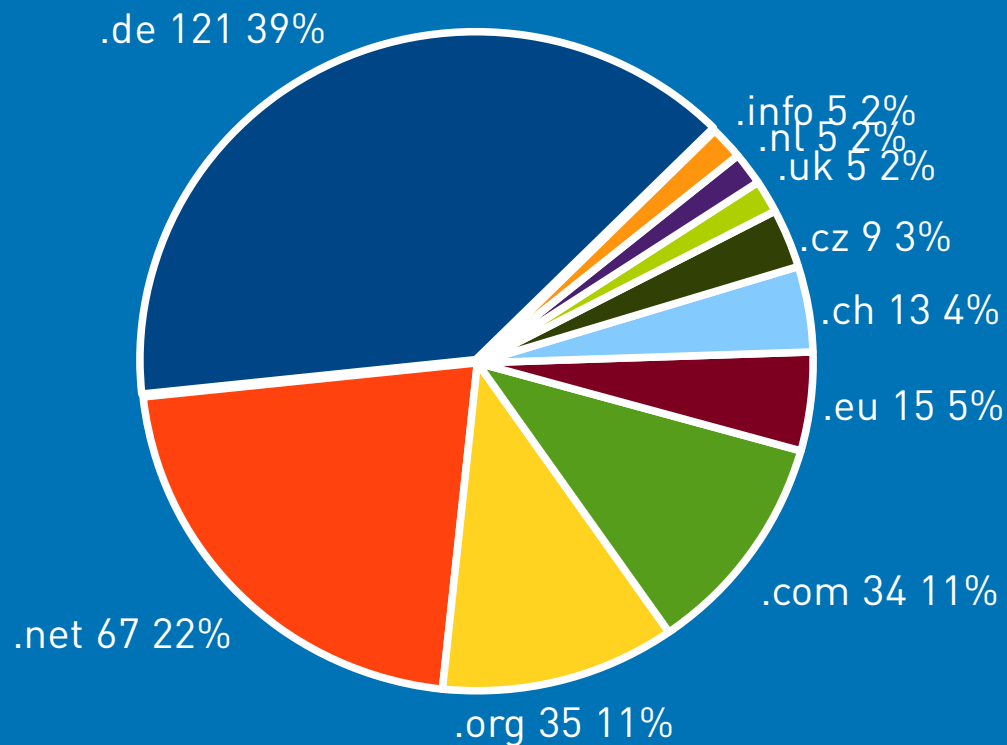
```
Jul 14 11:04:44 mail postfix/smtp[6409]:  
  Verified TLS connection established to mail.sys4.de  
  [194.126.158.139]:25: TLSv1 with cipher  
  ECDHE-RSA-AES256-SHA (256/256 bits)
```

DANE over SMTP Adoption

Currently about 1.200 email domains

- > posteo.de
- > mailbox.org
- > bund.de
- > Unitymedia (UPC Germany)
- > bayern.de
- > SWITCH
- > IETF

Top 10 DANE TLDs



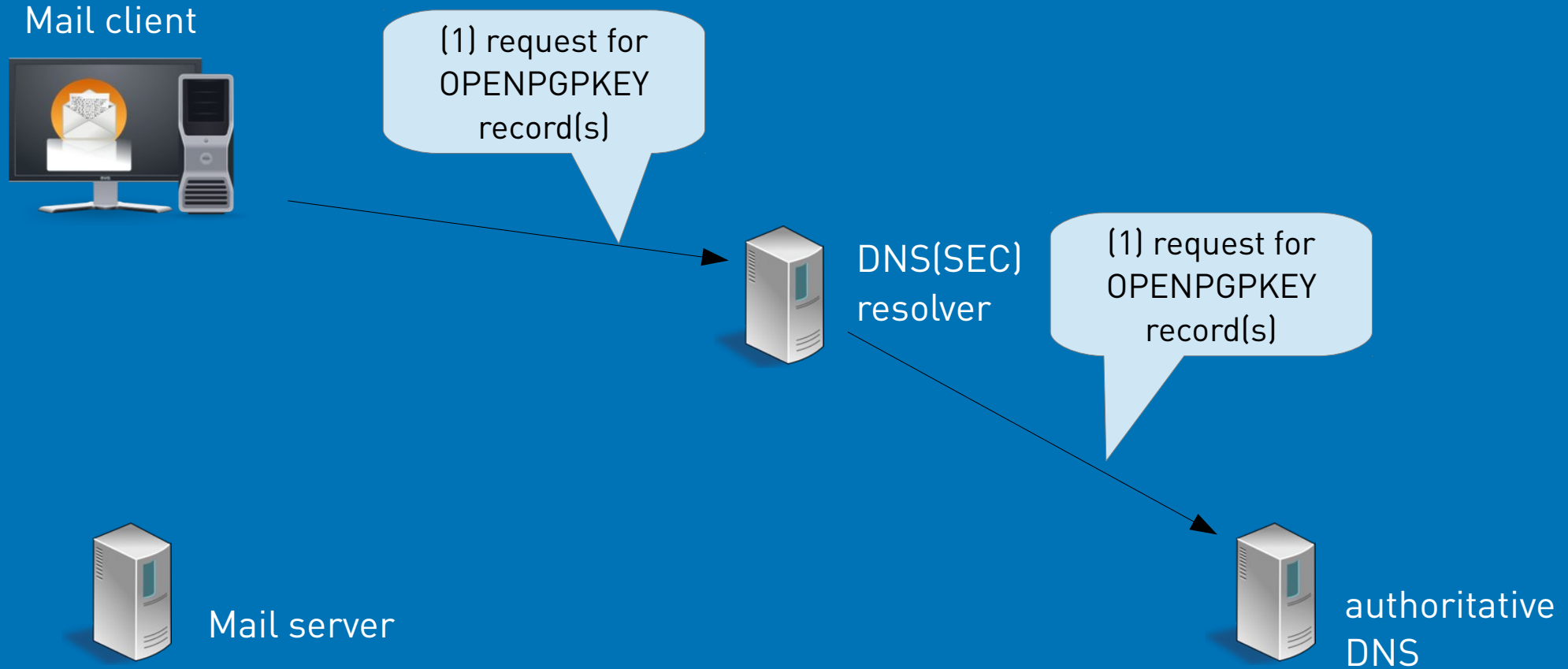
Viktor Dukhovni on IETF DANE mailinglist, 14.11.2014

PGP

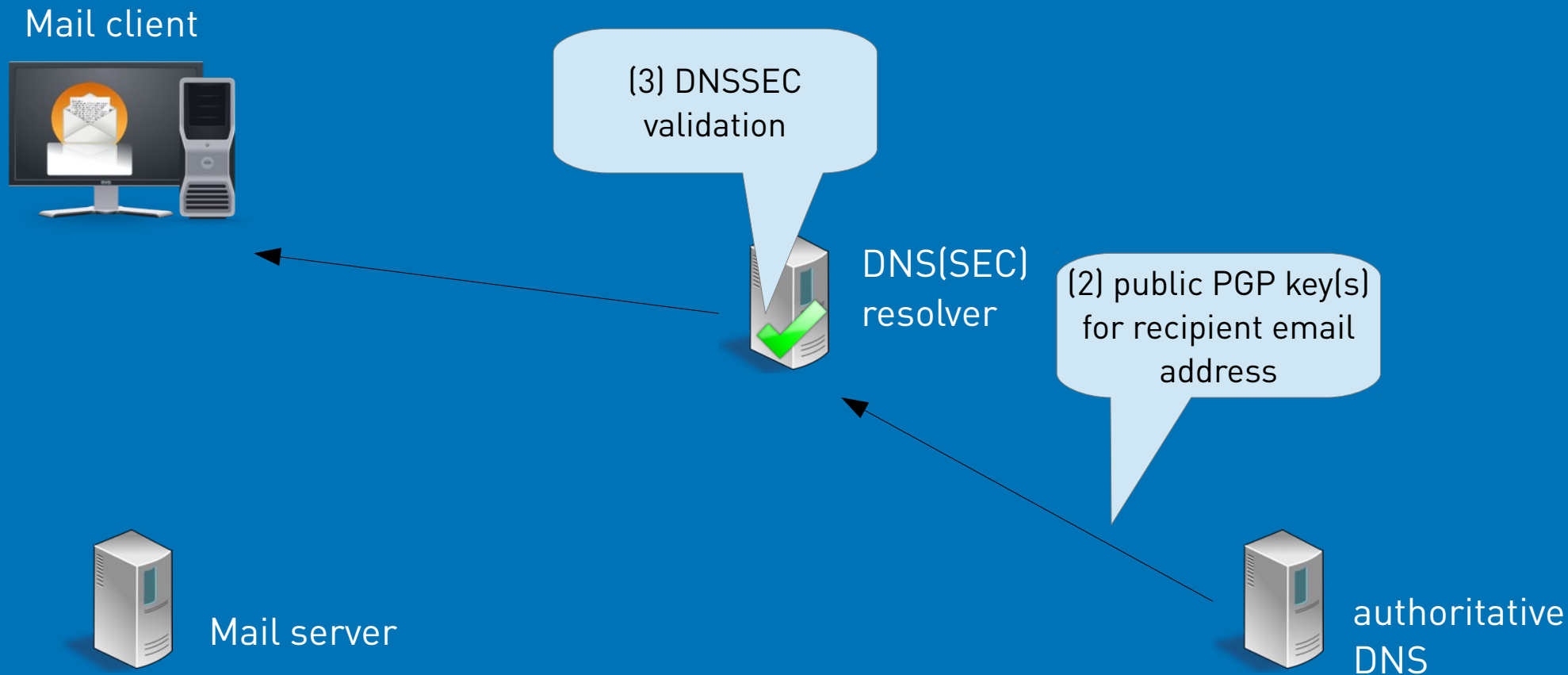
OPENPGPKEY Resource Record

- > Publish PGP/GPG public keys in DNS
- > Local part of mail address hashed
- > Replace or augment PGP-keyserver
- > Benefits over current Keyservers:
 - > Key removal!
 - > Keys authenticated by DNSSEC domain ownership and web-of-trust

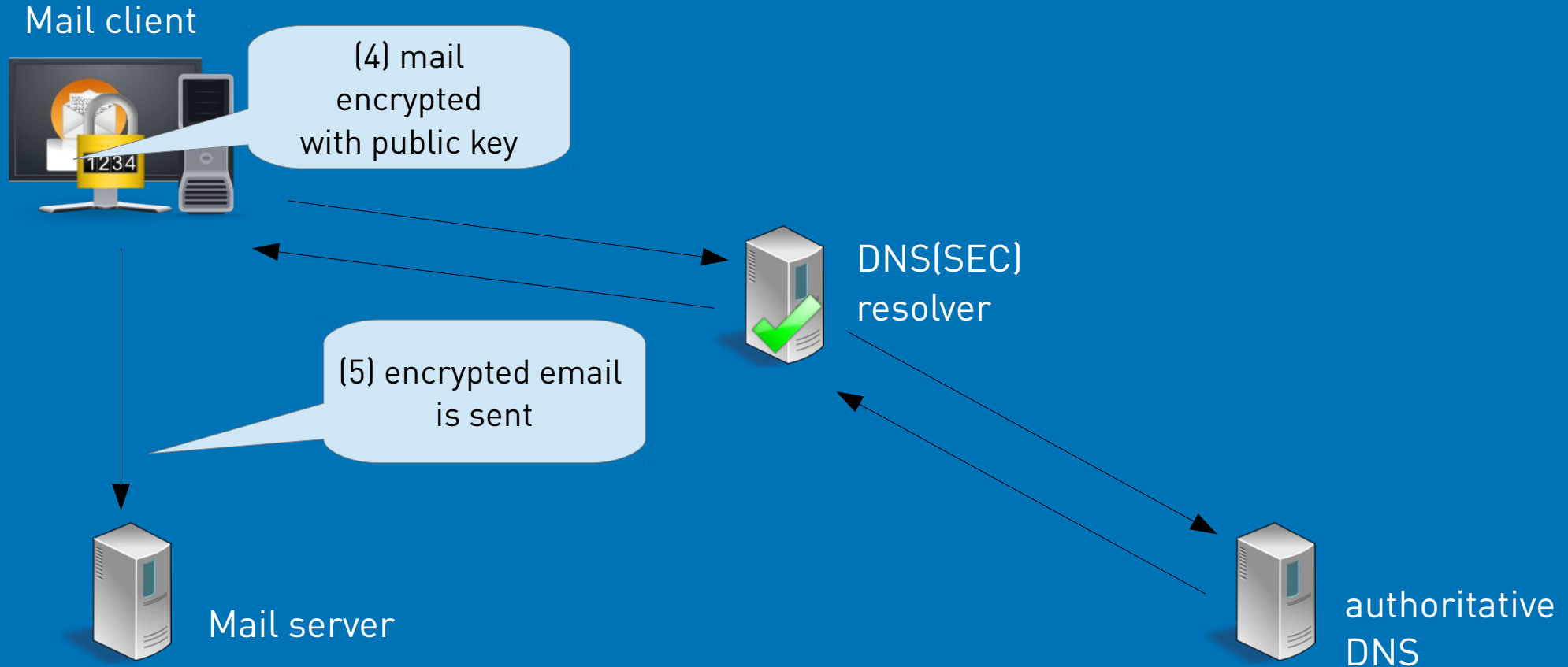
DANE OPENPGPKEY



DANE OPENGPGKEY



DANE OPENGPGKEY

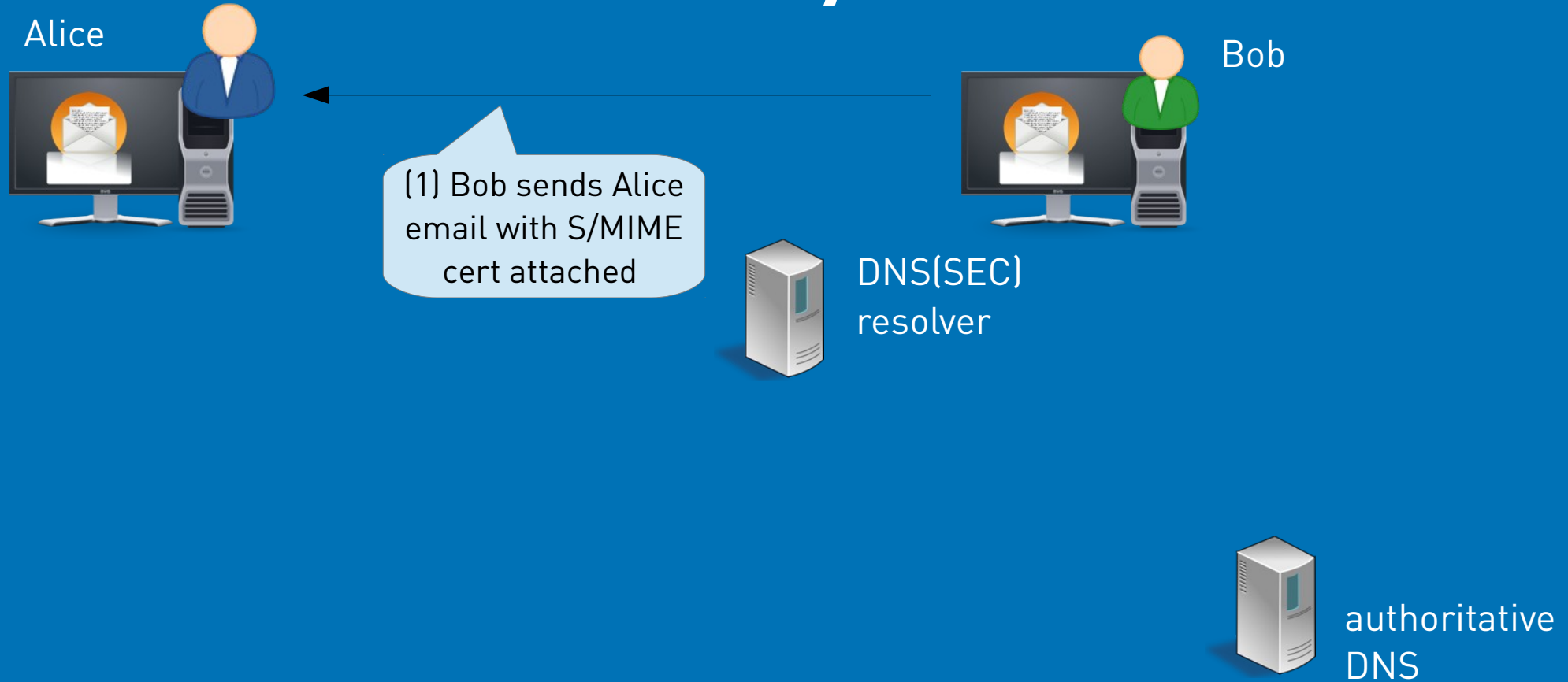


SMIME

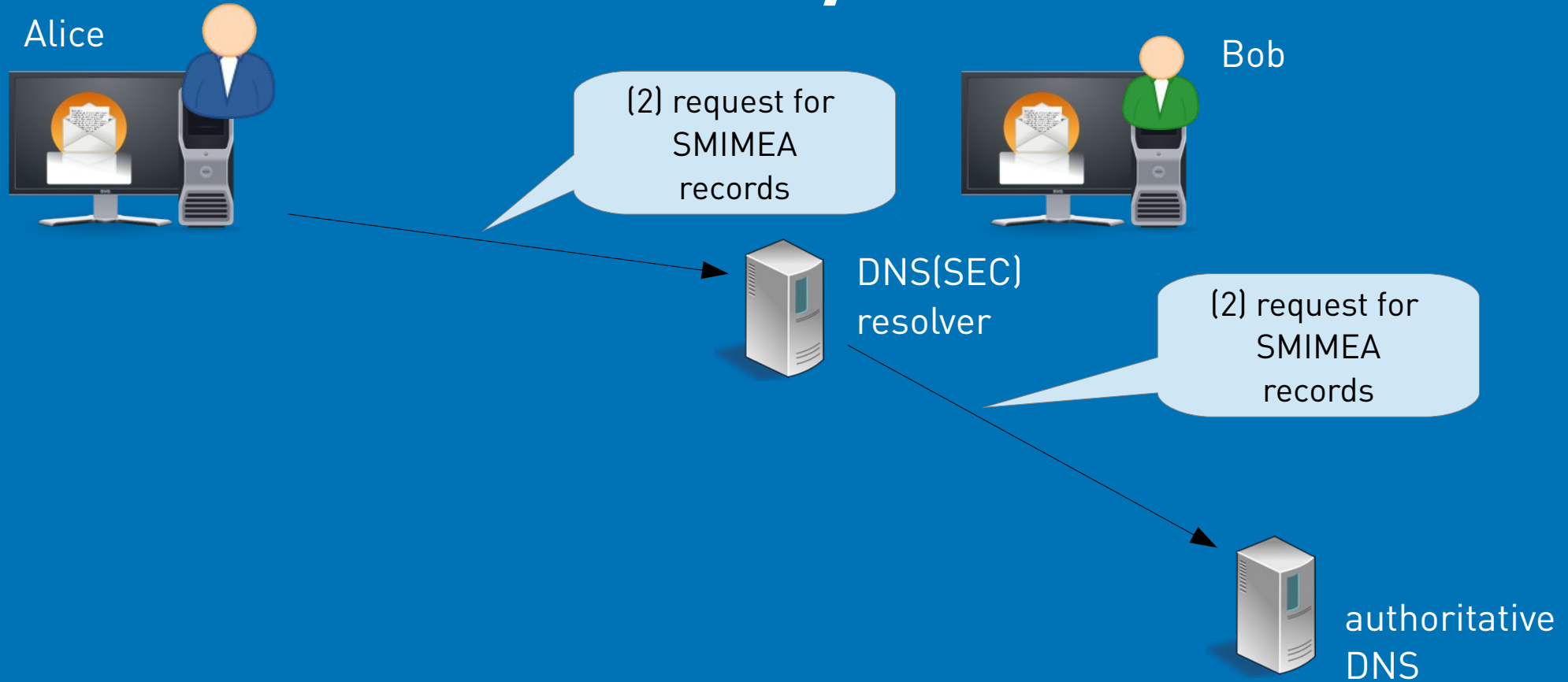
SMIMEA Resource Record

- > Authenticates email x509 certificates for S/MIME
- > Store hash or certificate in DNSSEC secured domain
- > Email localpart hashed
 - > email clients (MUA, mail user agent) validate x509 certificate/public-key in incoming email
 - > email clients fetch x509 public key certificates from DNS

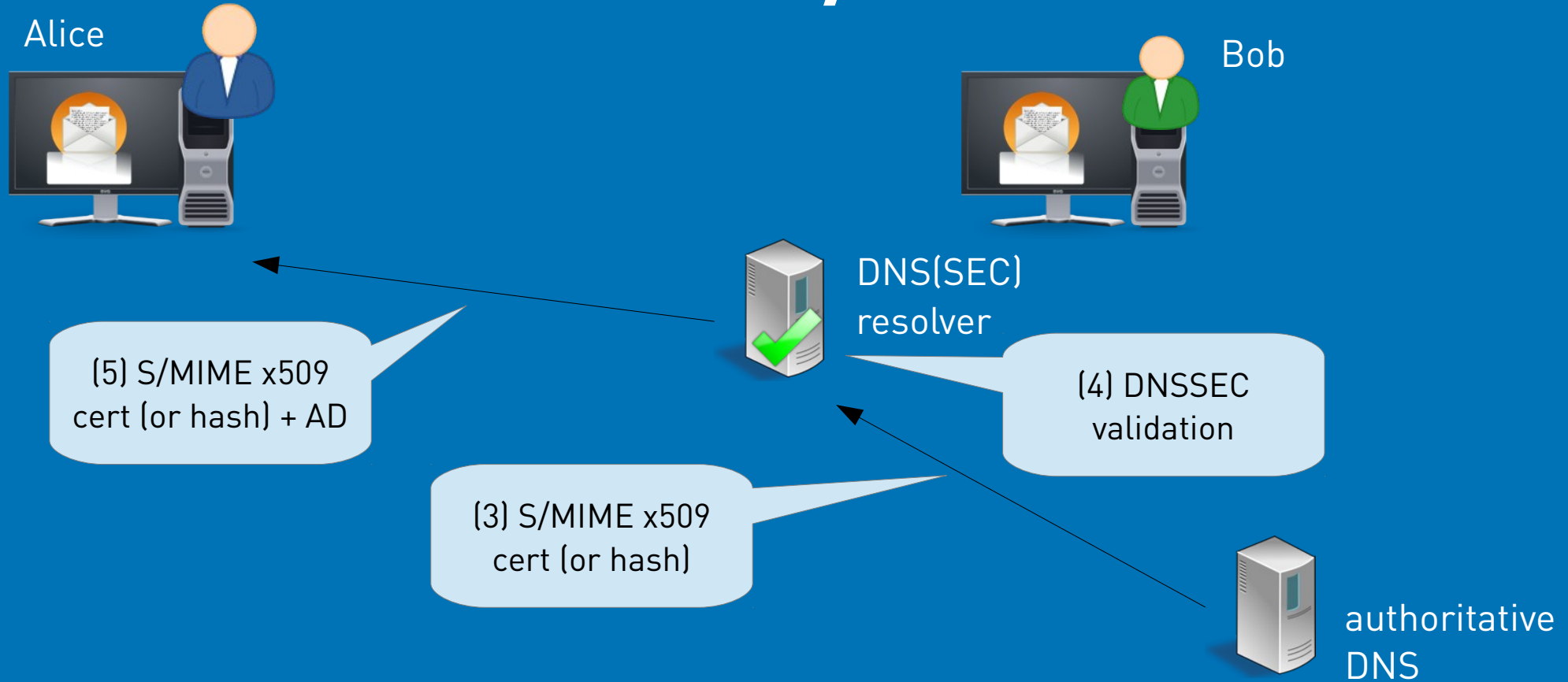
DANE S/MIME



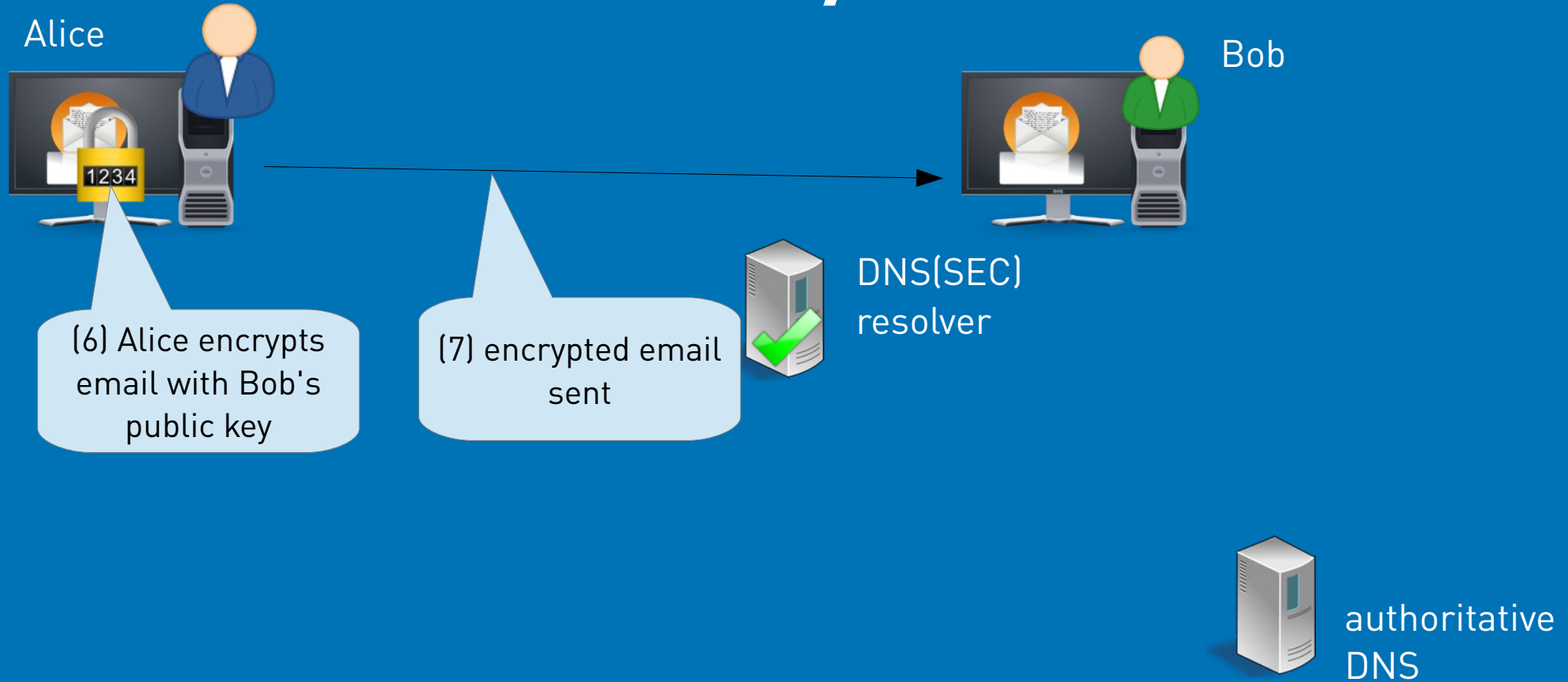
DANE S/MIME



DANE S/MIME



DANE S/MIME



smilla

- > SMIMEA aware Milter
- > „Smilla's Sense of Snowden“
- > Transparent for users
- > In- and outbound encryption
- > To be released as Open Source as soon as RFC becomes standard at <https://github.com/sys4/>

Next Steps DANE WG

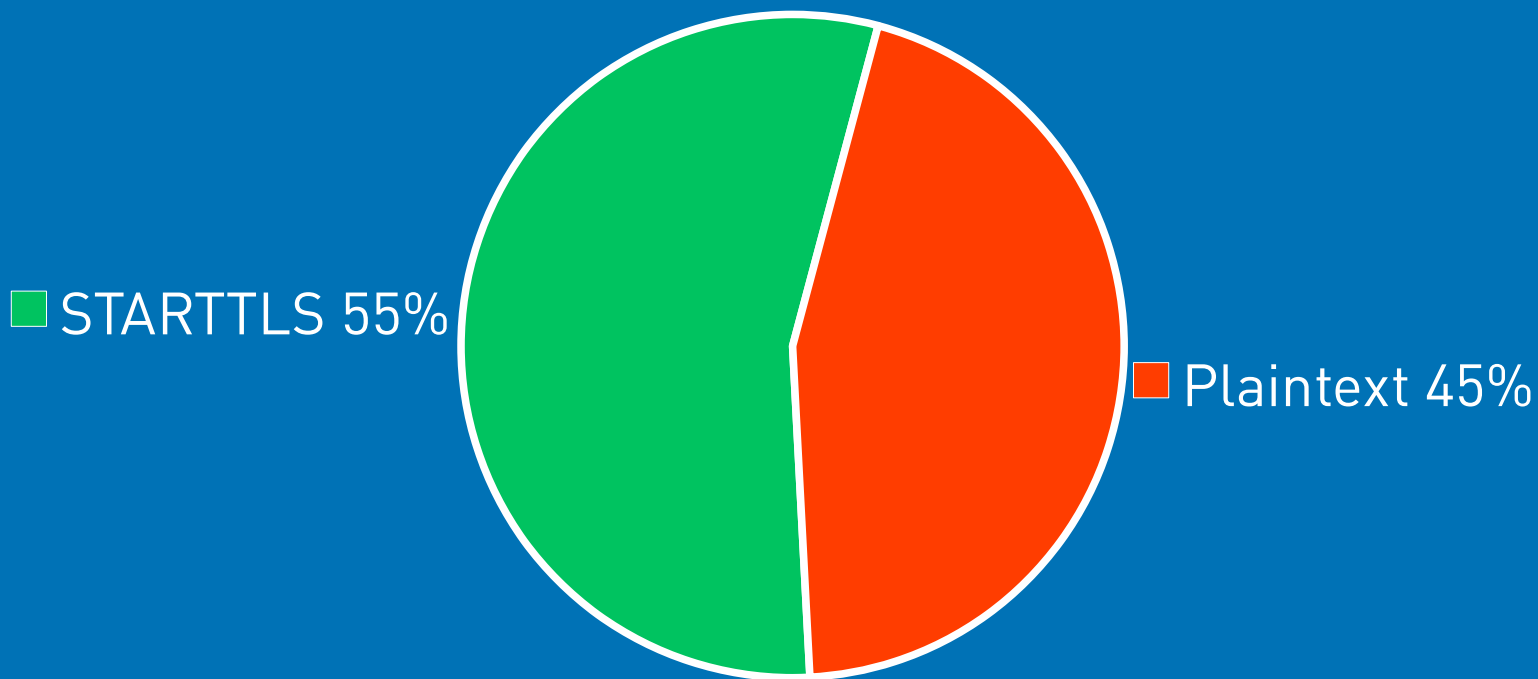
- > **raw-Certificates**
- > **Mutual Authentication**
client-side authentication via TLSA RR
- > **Payment Association Records**
Link account information/bitcoin wallet to a email adress

Markets for DANE

Who benefits from DANE?

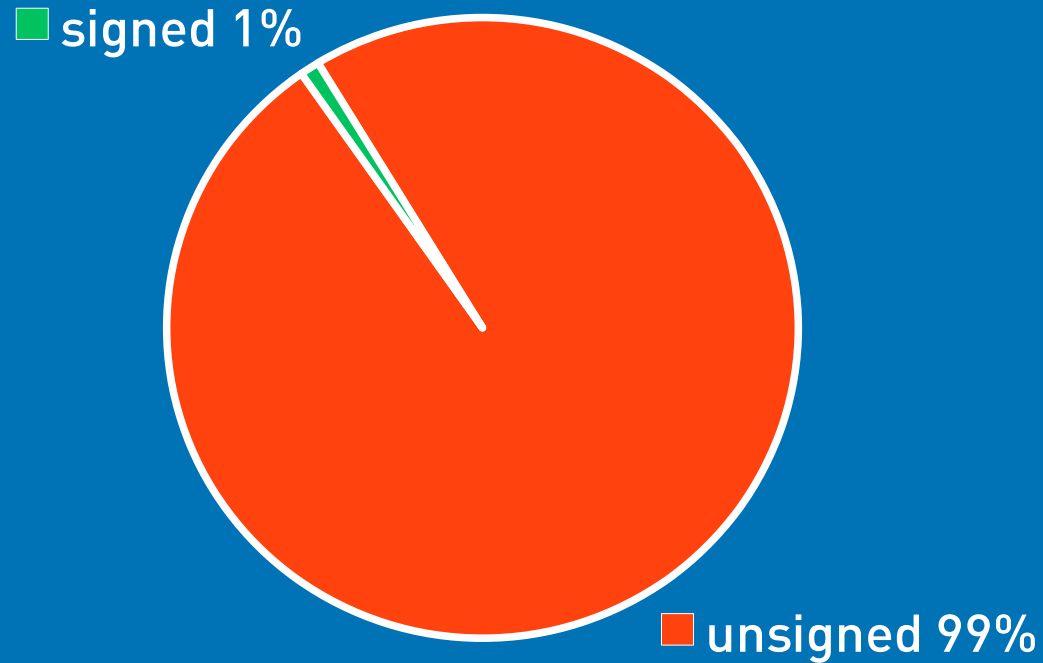
- > „Security services“ providers
- > Email users with „defined“ security requirements
- > Online-Payment, insurance, banks
- > Enterprises
- > Subcontractor

TLS in .de

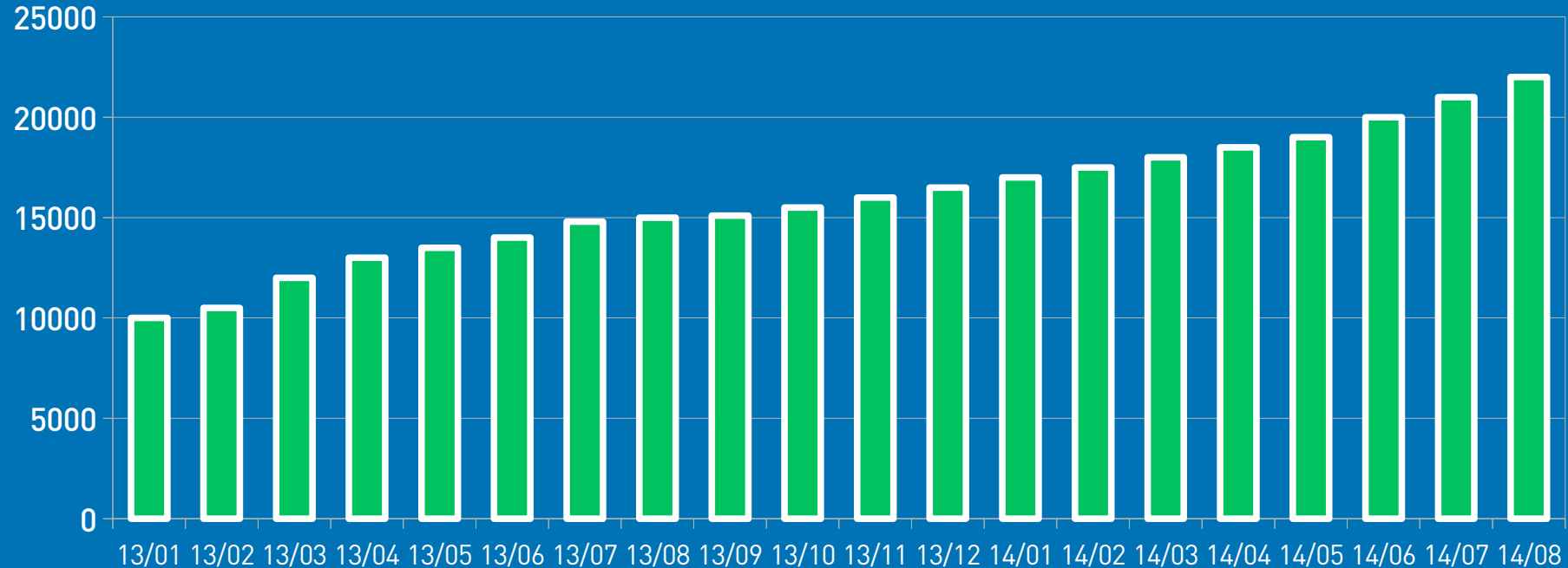


2,7 Mio. MX RR > 275.000 MTAs with 12.092 IPv6 \o/ MTAs

DNSSEC in .DE

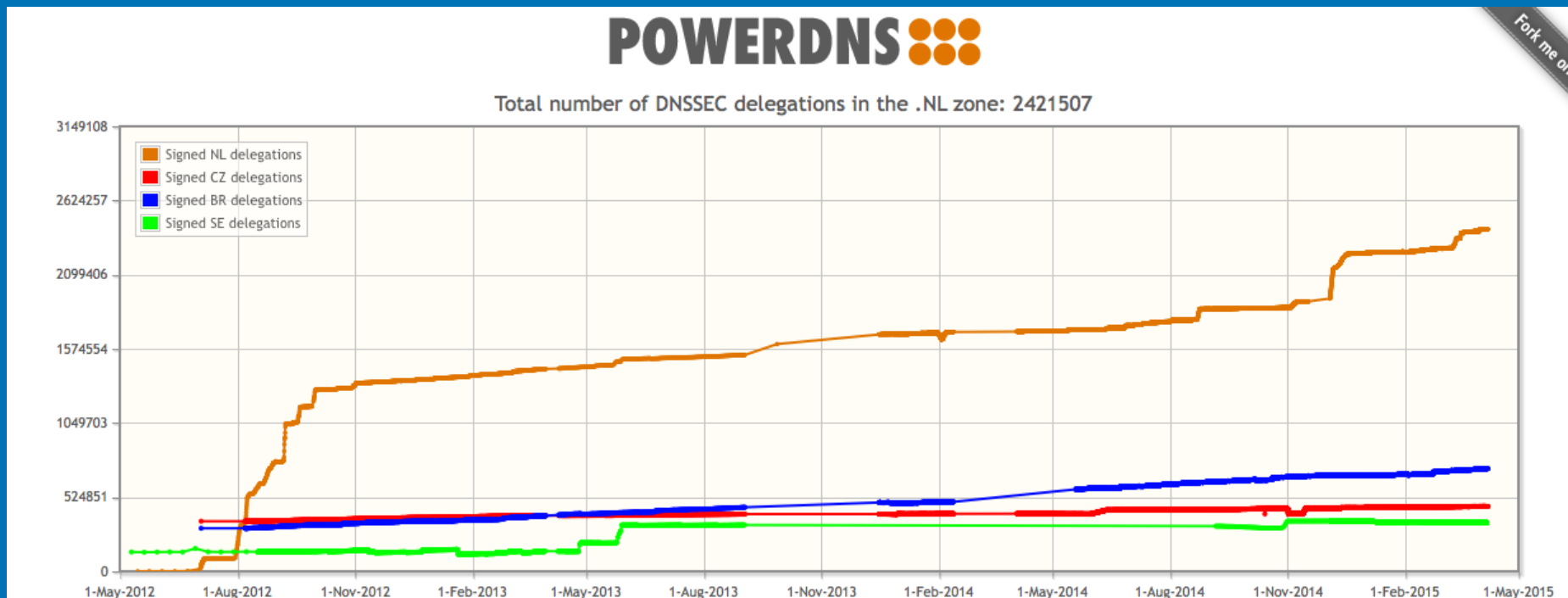


DNSSEC growth in .de



„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?

What people tell

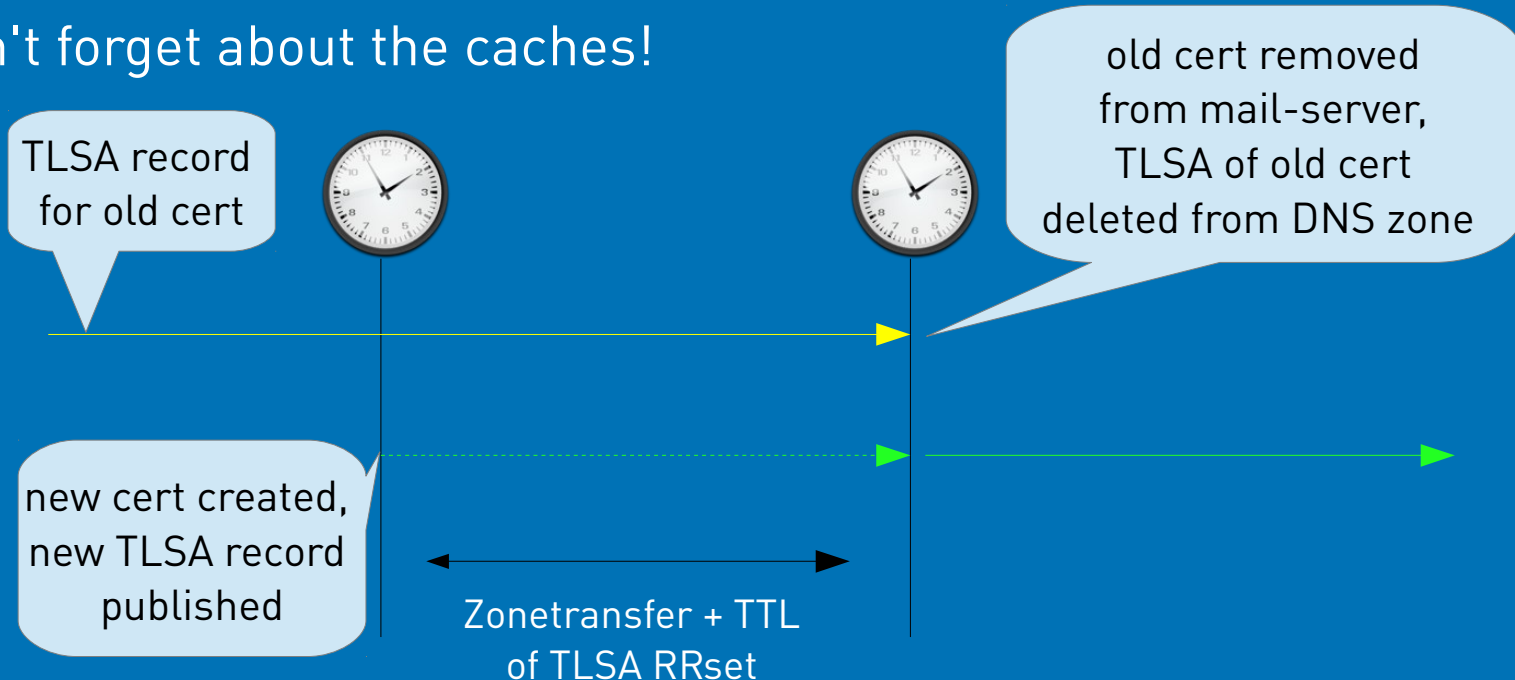
- > DNS provider with incomplete or non-existent DNSSEC-support
- > DNSSEC is technology but not a use case
- > With DNSSEC issues become mission critical
- > Missing DNSSEC/DANE monitoring and alarming
- > Missing know-how for automated certificate-management and DNSSEC signing
- > Missing toolchain for automated management

Registrars

- > Major registrars do not offer DNSSEC
- > Costs/risks of moving domains between registrars

Coordination

- > x509 certs, PGP keys in DNS
- > DNS is a loosely consistent database
 - > don't forget about the caches!



DNSSEC is Mission Critical

- > DNS is the „ugly duckling“ of network management
- > DNSSEC might require a new/better DNS design
- > DNSSEC requires „trusted peers“
- > Expired DNSSEC signatures can make domain „vanish“ (until the SIGs are renewed)

DANE Validator

DANE SMTP Validator - Google Chrome

DANE SMTP Validator x Patrick

https://dane.sys4.de/smtp/ripe.net

[*] ripe.net Validate

ripe.net DNSSEC ✓ TLSA ⓘ SMTP ⓘ

The domain lists the following MX entries:

200 koko.ripe.net DNSSEC ✓ TLSA ⓘ SMTP ⓘ ⓘ

No TLSA records.

250 kaka.ripe.net DNSSEC ⓘ TLSA ⓘ SMTP ⓘ ⓘ

This MX host has been ignored due to a problem with a higher-priority host.

Takeaway

- > DNSSEC as a „one-time-cost“
- > Open standard
- > DANE allows scalable and secure trust-management
- > Reduces management costs
- > Automates rollover
- > Software support is here: Postfix, Exim, OpenSMTPd, OpenPGPKEY milter, smilla



We do ASCII

sys4.de



<https://sys4.de/download/dane-ripe.pdf>