Promoting DNSSEC & DANE in telco email services: **the TES project**

Vittorio Bertola – Research & Innovation Engineer

ICANN Copenhagen – March 15, 2017

Stay Open. OX

Email transport is **not** secure today

- **Encryption and authentication** of email transport streams and storage is **severely insufficient**
- Telcos and ISPs **allow surveillance of their customers** by not solving this
- All types of **vital documents and data** go by email
- **Greater public perception** of the issue

Stay Open. OX

The Telegraph

Home Video News World Sport Business Money Comment Culture Travel Life W

HOME » FINANCE » PERSONAL FINANCE » BORROWING » MORTGAGES

'Fraudsters hacked emails to my solicitor and stole £340,000 from my property sale'

In a growing form of cybercrime fraudsters are targeting property sellers and their solicitors

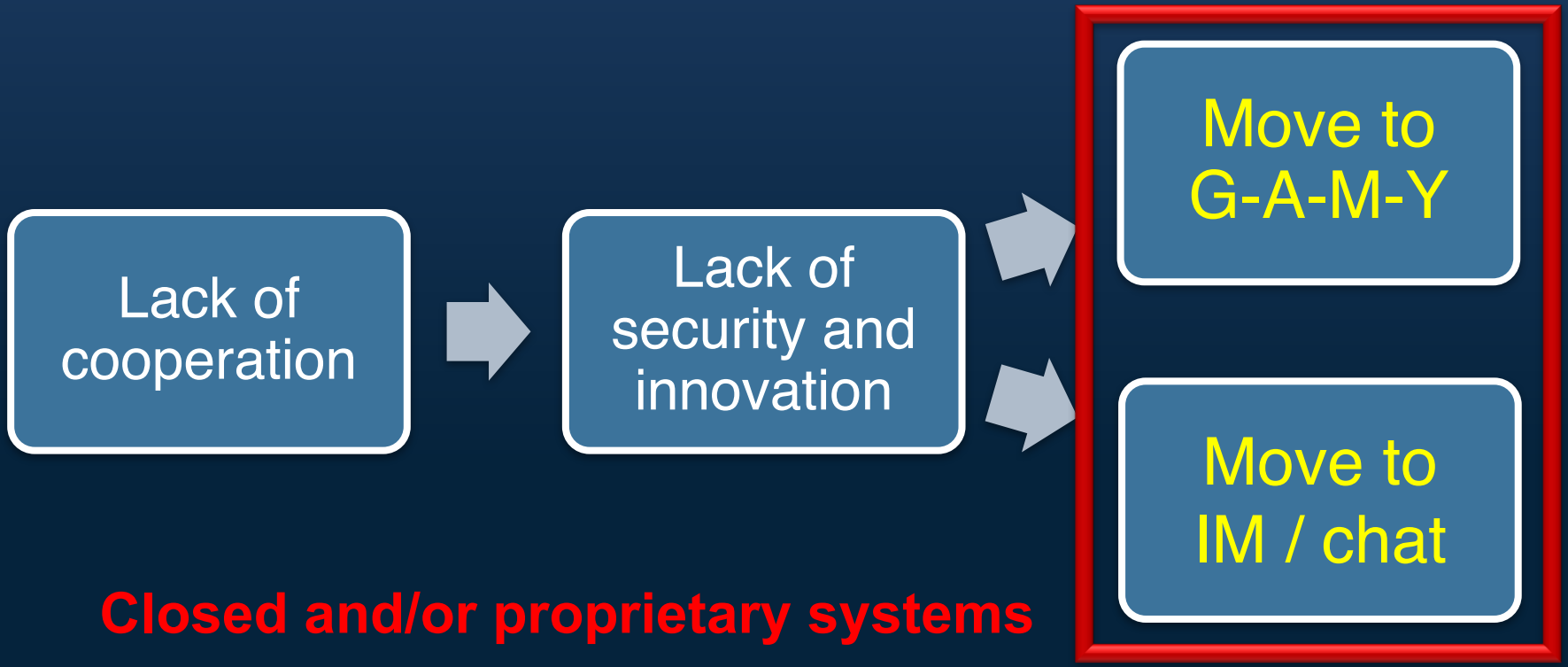
680 0 441 1K Email

theguardian

'I thought I'd bought my first home, but I lost £67,000 in a conveyancing scam'

Howard Mollett is the victim of 'Friday afternoon fraud', an email scam that is the No 1 cybercrime in the legal sector

A **growing risk** for ISP email



Closed and/or proprietary systems

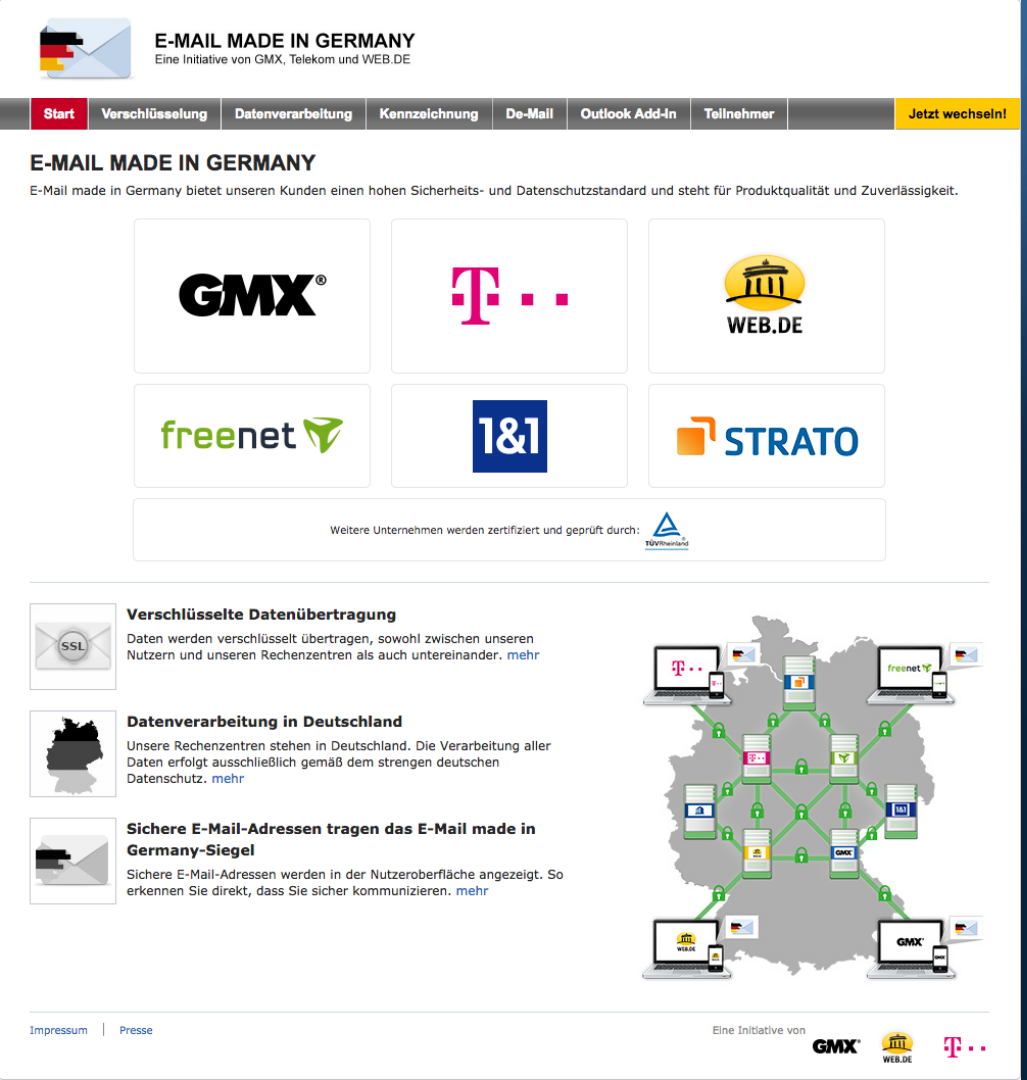
BSI TR-03108-1:
Secure E-Mail Transport

Requirements for E-Mail Service Providers (EMSP)
regarding a secure Transport of E-Mails

Version: 1.0
Date: 05/12/2016

Efforts ongoing **everywhere**

- Governmental recommendations in USA, Germany, Netherlands...
- National efforts by ISPs in Germany & France to improve Email security



E-mail **made in Germany**

- An agreement among Germany's biggest email providers
- They use DNSSEC and DANE to authenticate the destination server and to ensure that the SMTP connection is encrypted

Stay Open. OX

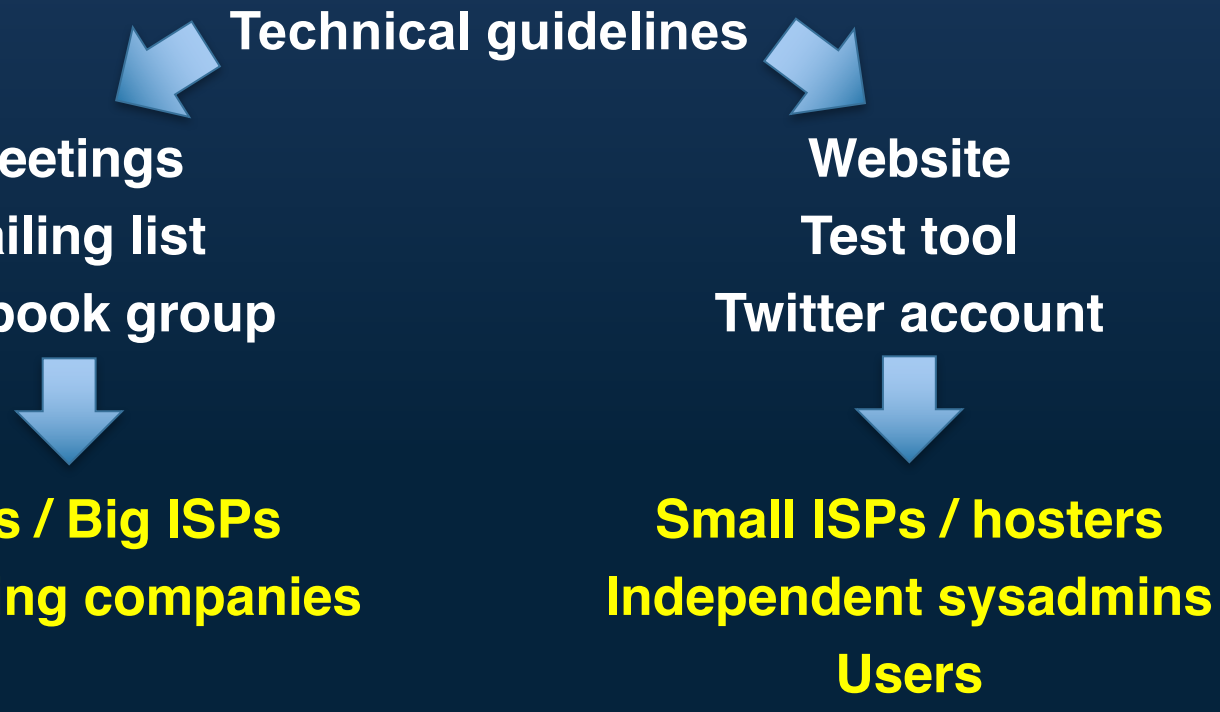
TES

TRUSTED EMAIL SERVICES

https://tesmail.org/

A vendor community initiative

A twofold audience

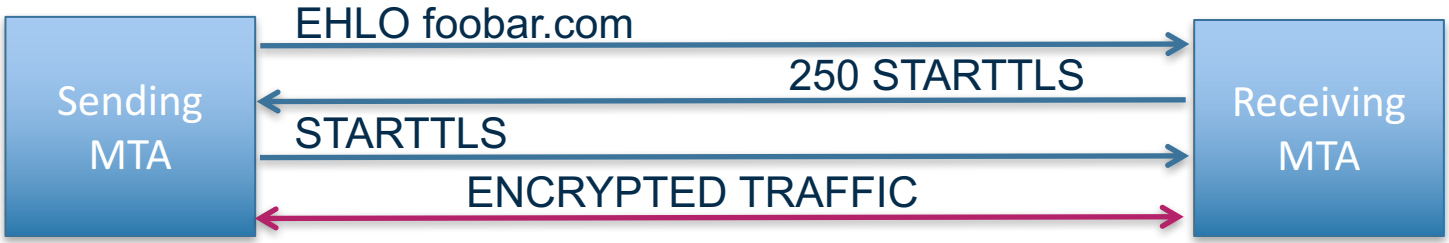


Several technologies recommended

- Provide anti-abuse filters and policies (SPF, DKIM, DMARC)
- Encrypt email traffic (STARTTLS) with secure ciphers
- Authenticate destinations with DNSSEC and DANE
- Deploy end-to-end encryption with PGP and HKP (including mailboxes)

STARTTLS MITM Downgrade

Normal STARTTLS Negotiation

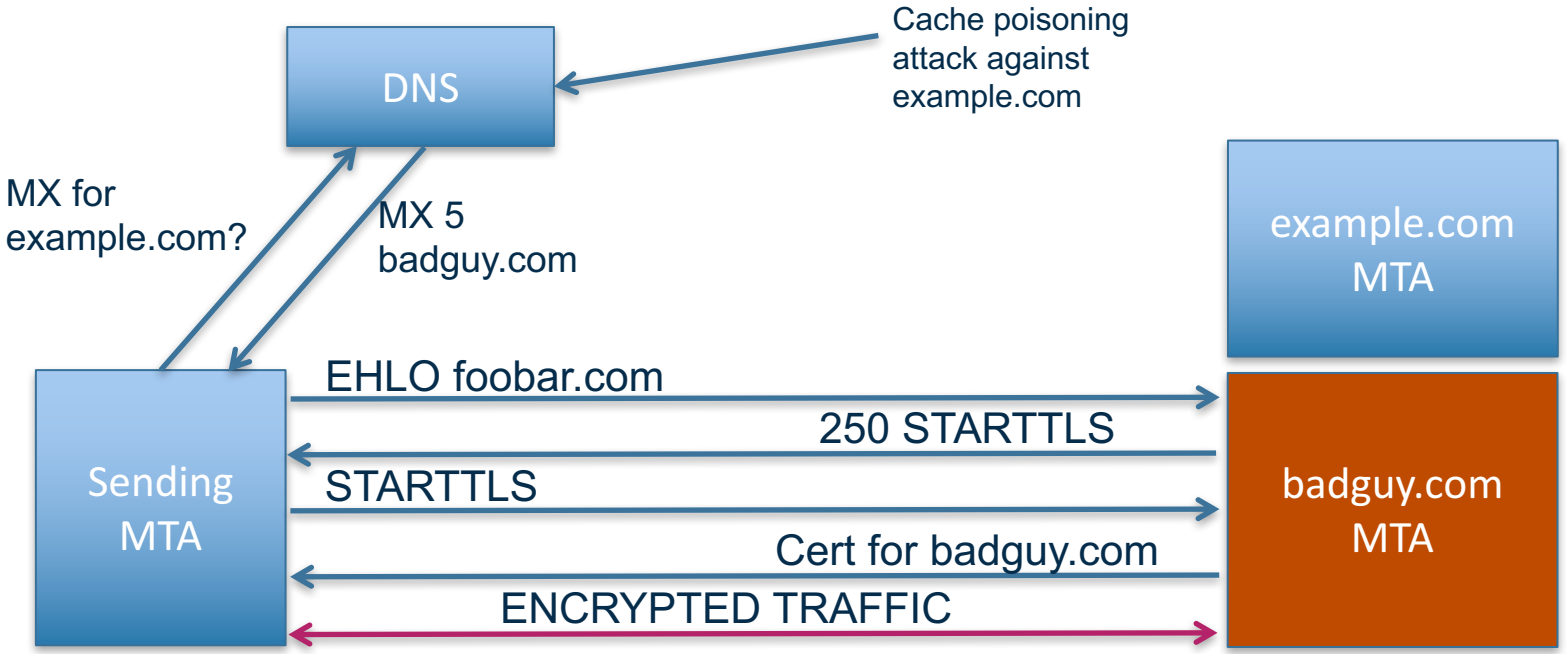


STARTTLS MITM Downgrade

STARTTLS Negotiation with MITM

Spoofed MX Domain Attack

Works even if MTA checks certificate validity



Quick Digression on DANE

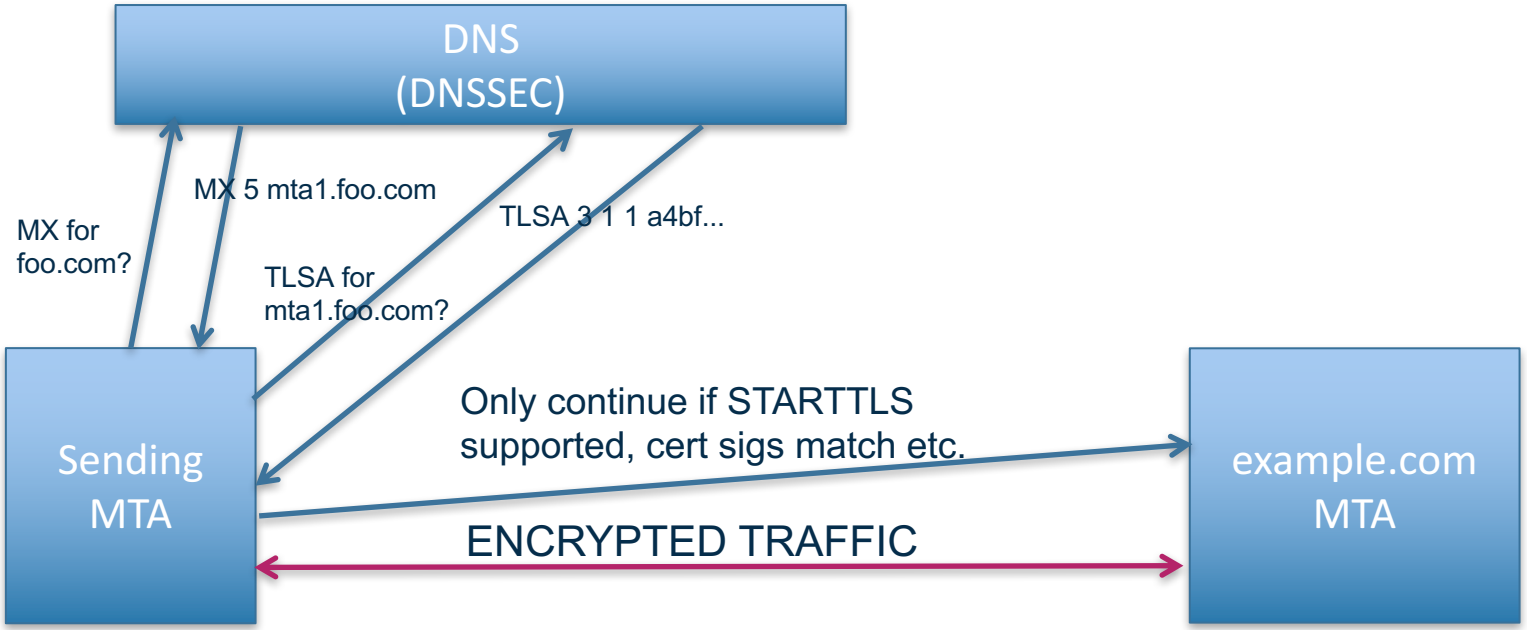
RFC 6698: DNS-based Authentication of Named Entities for TLS

- DANE defines a new record type in DNS: TLSA Record
- Can be used to securely authenticate TLS certificates:
  - By specifying constraints on CAs that are valid or explicitly specifying certificates
  - By allowing self-signed certificates to be explicitly specified
  - ***Using DNSSEC as a trust-anchor***

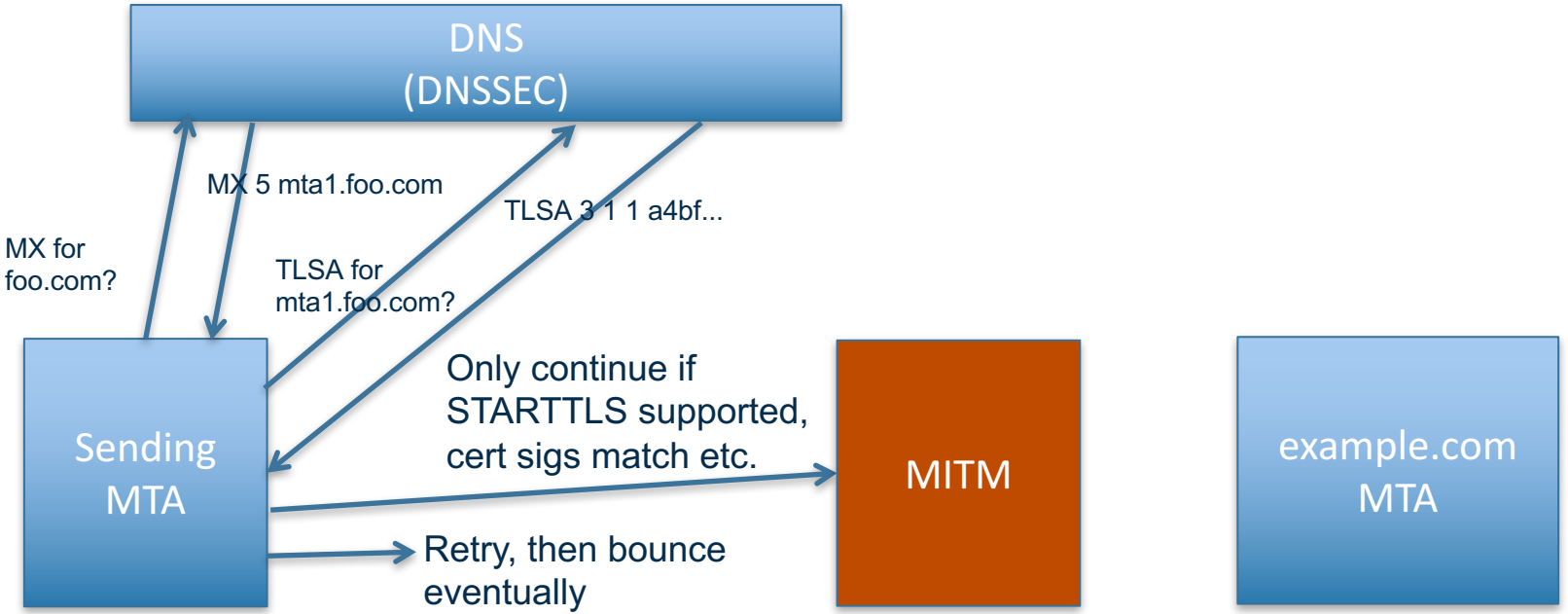
- DANE is used in conjunction with SMTP & TLS to fully secure mail delivery

- DANE addresses vulnerabilities discussed earlier:
  - Authenticate presented certificates using DNSSEC signed TLSA record
  - ***Use presence of a TLSA record to prevent downgrade (you must encrypt)***

DANE in Action (normal)



DANE in Action (MITM)



Operational Issues with DNSSEC/DANE

- DNSSEC is perceived as difficult to implement and administer
- This may have been true previously but not today
- Zone signing, Key generation, signature rollover etc. is all automated
  - Signing a zone ‘one command’ with some nameservers
- Transferring DS record to registrar for signing by parent zone is typically still manual
- DNSSEC Validation has been difficult until recently
- However this has also changed
  - Resolvers: Unbound, PowerDNS, Bind
  - Stub Resolver Libraries: GetDNS
- DANE seen as not currently suitable for use by browsers/clients
- C.f. Certificate Transparency from Google

What do I need to implement this?

Software

- DNSSEC Compliant DNS Server
- DANE-Compliant MTA (sending only)
  - All TLS-capable MTAs are DANE capable by default

Operational

- DNS
  - DNSSEC Signed Email Domains
  - TLSA Records for your mail servers
  - TES records for membership lookup
- MTA
  - Policy to allow local overrides
- WebMail recipient lookup javascript

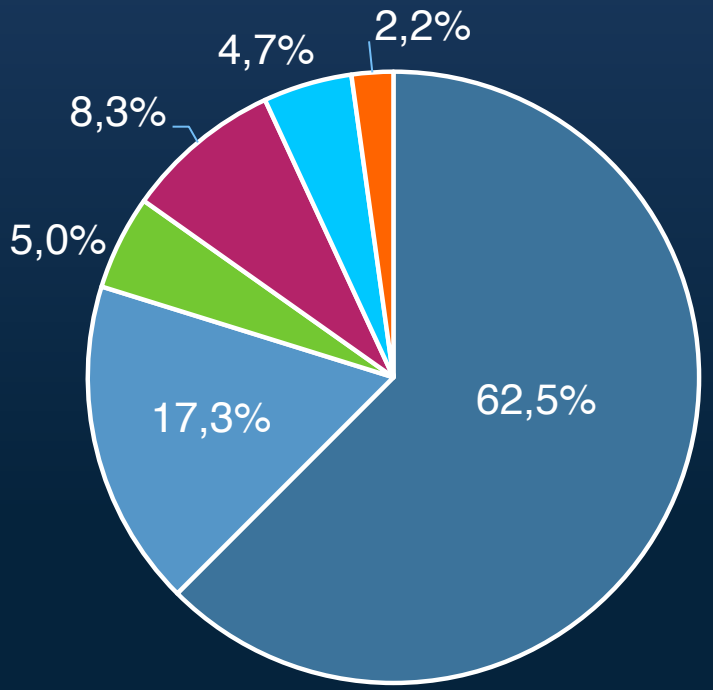
protocol	dnssec	dane	starttls	auth	spf
TLSv1.2	-	-	ok	ok	mx
TLSv1.2	-	-	ok	ok	ip4:64.233.160.0/19
TLSv1.2	-	-	ok	ok	ip4:74.125.0.0/16
TLSv1.2	-	-	ok	ok	ip4:74.125.0.0/16
TLSv1.2	-	-	ok	ok	ip4:74.125.0.0/16
TLSv1.2	-	-	ok	ok	ip4:74.125.0.0/16
TLSv1.2	-	-	ok	ok	?all
TLSv1.2	-	-	ok	ok	?all
TLSv1.2	-	-	ok	ok	?all
TLSv1.1	-	-	ok	false	~all
TLSv1.1	-	-	ok	false	~all
TLSv1.1	-	-	ok	false	~all
TLSv1.1	-	-	ok	false	~all
TLSv1.1	-	-	ok	false	~all
TLSv1.1	-	-	ok	false	~all
TLSv1.1	-	-	ok	false	~all
TLSv1.2	-	-	ok	ok	ip4:208.80.152.0/22
TLSv1.2	-	-	ok	ok	ip4:208.80.152.0/22
STARTTLS NOT SUPPORTED					-all
STARTTLS NOT SUPPORTED					-all
STARTTLS NOT SUPPORTED					ip4:61.208.132.13
TLSv1.1	-	-	ok	ok	ip4:23.103.128.0/19
TLSv1.2	-	-	ok	ok	~all
TLSv1.2	-	-	ok	ok	~all
socket timeout					~all
TLSv1.1	-	-	ok	ok	ip4:23.103.128.0/19

The **TES test tool**

- Tests your domain name for email support, STARTTLS, TLS version, unencrypted auth, DNSSEC, DANE and SPF
- Will be made public shortly on the TES website
- In Dec 2016, we ran a test scan of the top 1000 domain names by Web traffic

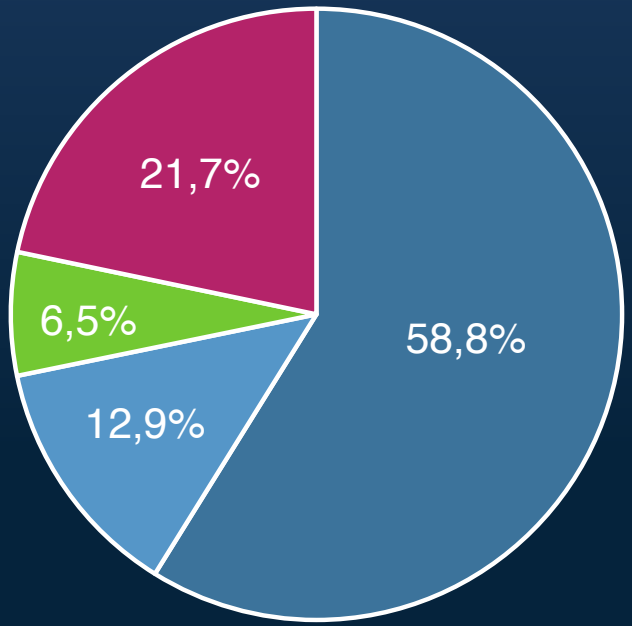
Stay Open. OX

Domains supporting encrypted mail



Stay Open. OX

TLS support on mail servers



- TLS 1.2
- TLS 1.1
- TLS 1.0
- No TLS support

~90% of those supporting TLS do not offer authentication before STARTTLS

DNSSEC and DANE support

DNSSEC

- Deployed by 15 domains
- 1,9% of domains having email
- 2,4% of domains supporting TLS

DANE

- Deployed by 3 domains
- 0,3% of domains having email
- 0,4% of domains supporting TLS

The three lonely heroes: comcast.net, web.de and gmx.net

Thank you

https://tesmail.org/

info@tesmail.org

Stay Open. OX

Stay Open.