TeleTrusT EBCA
European Bridge Certificate Authority

TeleTrusT-EBCA "PKI-Workshop"

Berlin, 22.06.2017

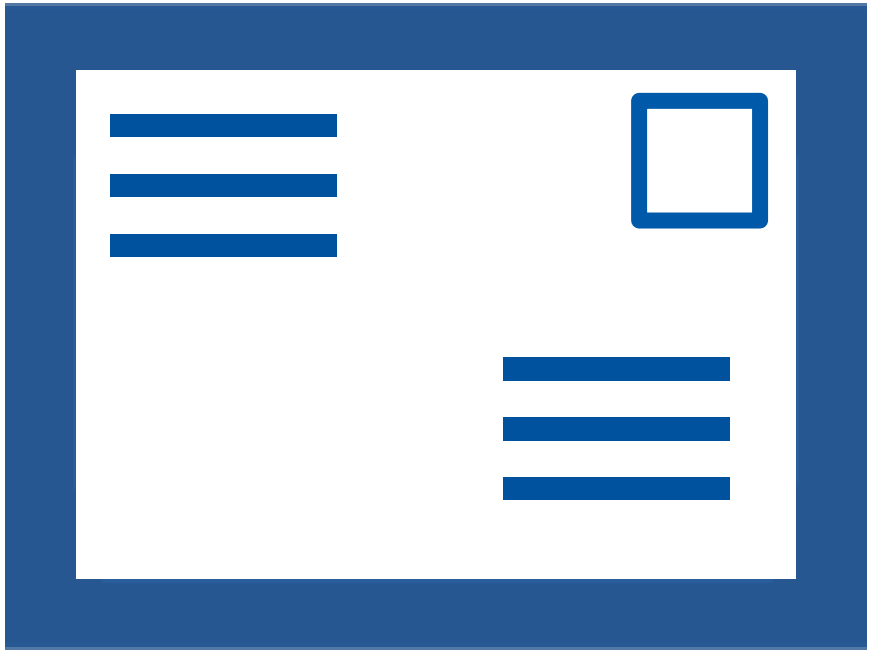
Aktuelle Standards zum besseren E-Mail-Schutz: DMARC, DKIM, SPF

Sören Beiler, Net at Work

Absenderreputation

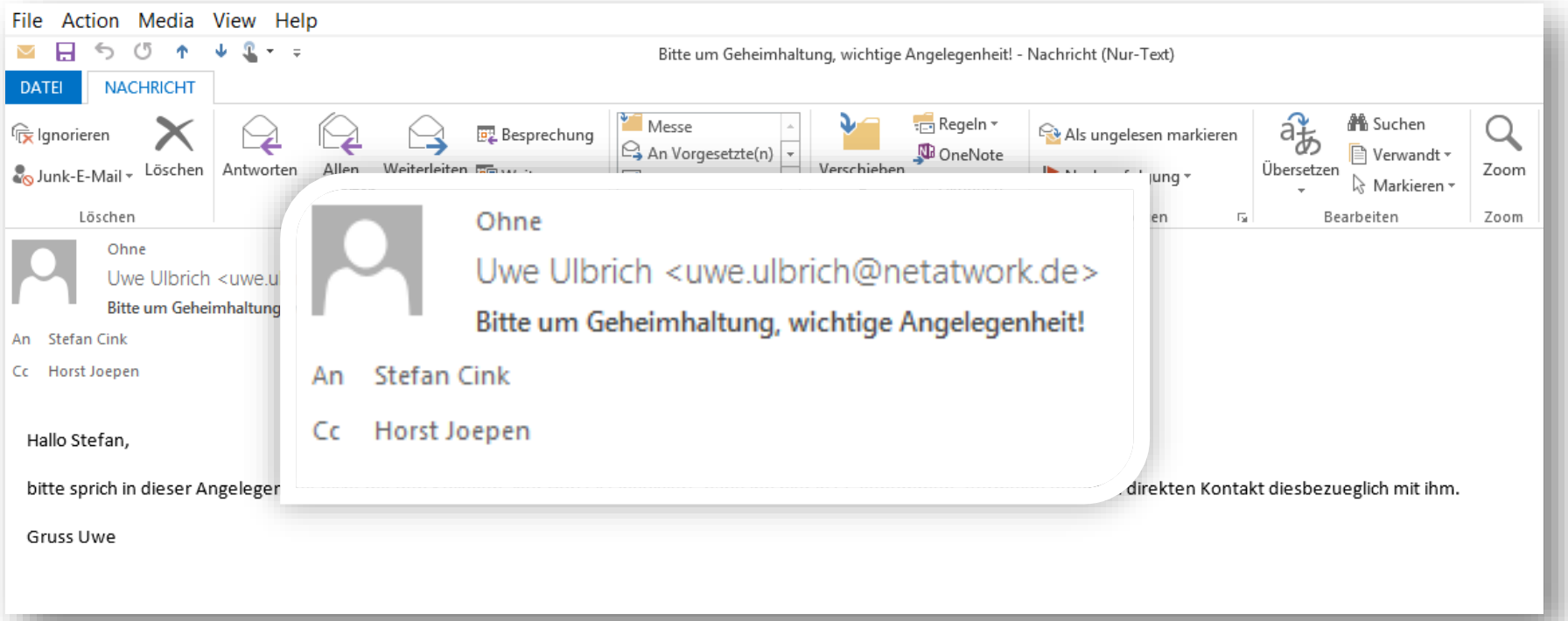
Envelope Sender vs. Body from

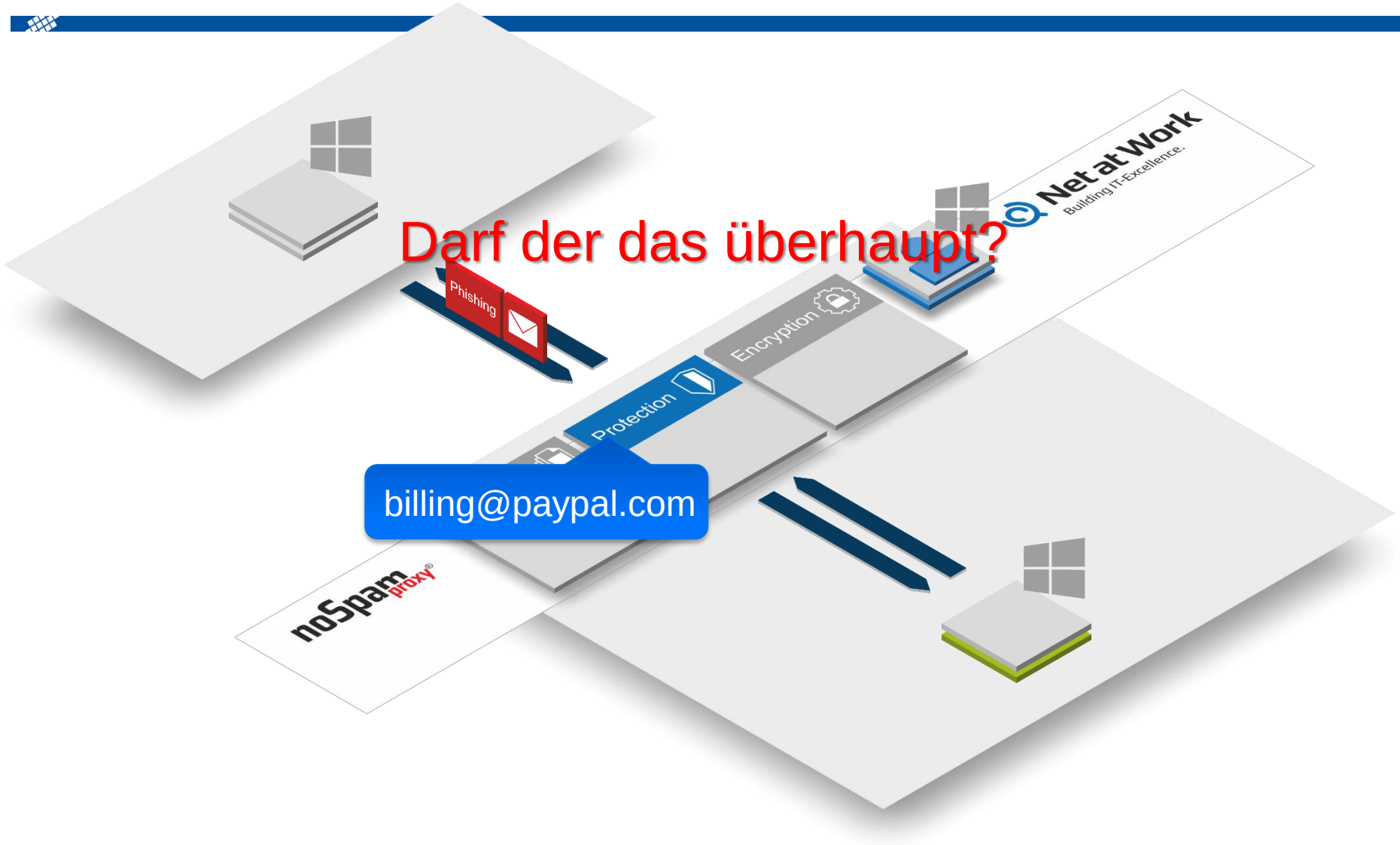
TeleTrusT EBCA
European Bridge Certificate Authority



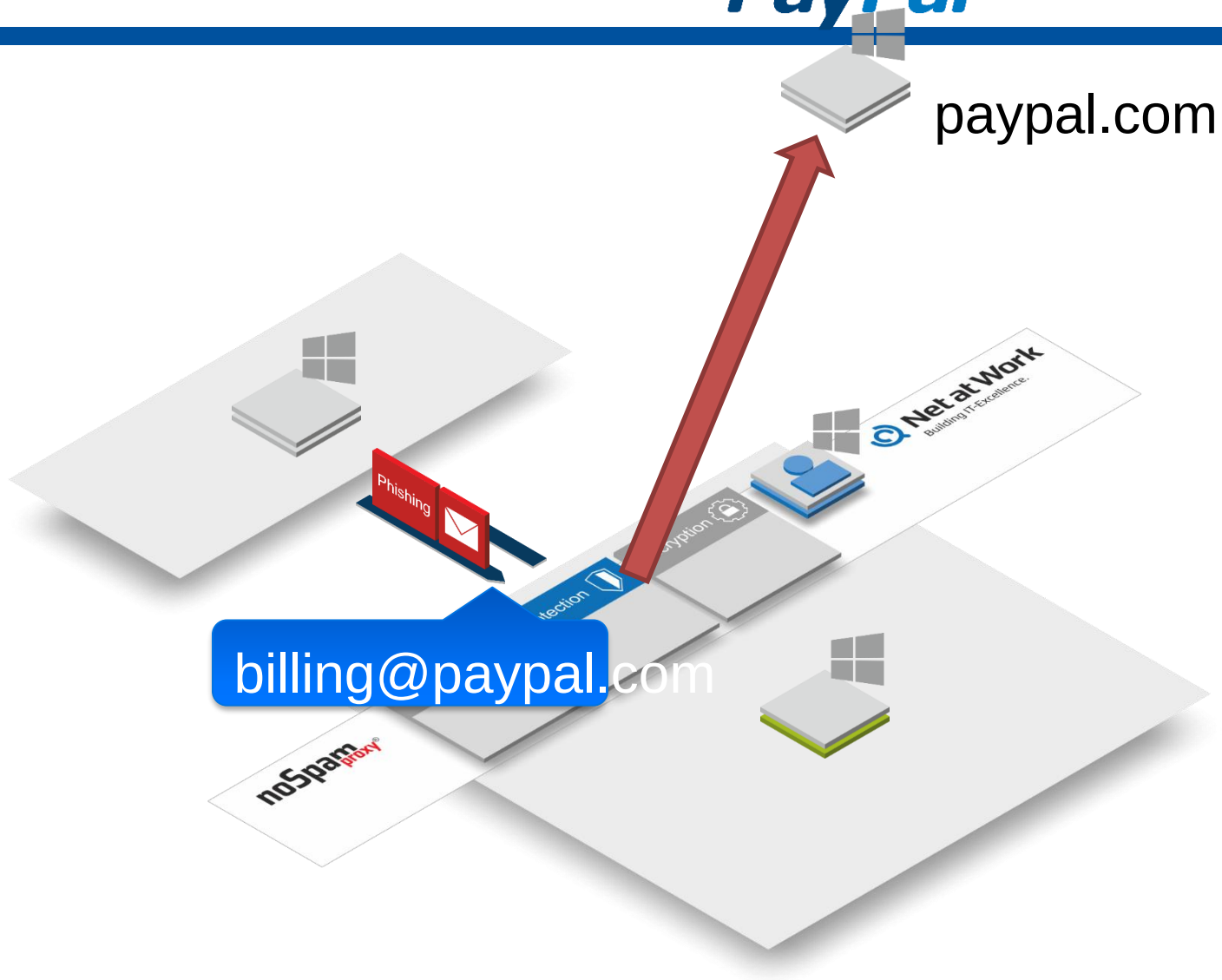
Envelope Sender vs. Body from

TeleTrusT EBCA
European Bridge Certificate Authority





PayPal™

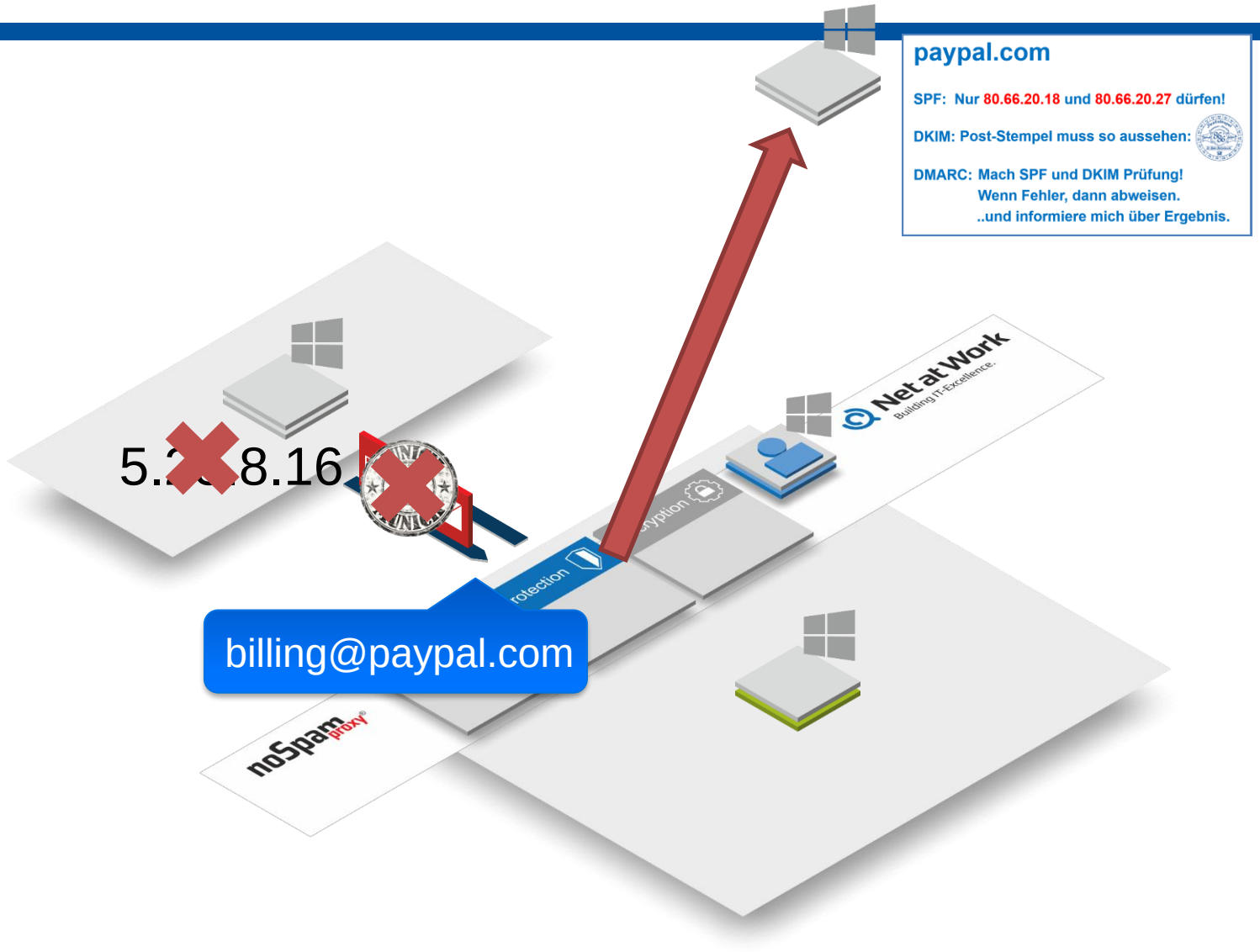


paypal.com

SPF: Nur 80.66.20.18 und 80.66.20.27 dürfen!

DKIM: Post-Stempel muss so aussehen:

DMARC: Mach SPF und DKIM Prüfung!
Wenn Fehler, dann abweisen.
..und informiere mich über Ergebnis.



Unter der Motorhaube

Sender Policy Framework (SPF)

netatwork.de

A	www.netatwork.de	80.66.20.21
A	mail.netatwork.de	80.66.20.22
MX	netatwork.de	mail.netatwork.de
TXT	netatwork.de	v=spf1 +MX -All

Domain Key Identified Mail (DKIM)

netatwork.de

A	www.netatwork.de	80.66.20.21
A	mail.netatwork.de	80.66.20.22
MX	netatwork.de	mail.netatwork.de
TXT	netatwork.de	v=spf1 +MX -All
TXT	selektor._domainkey.netatwork.de	v=DKIM1; p=123; s=email; t=s

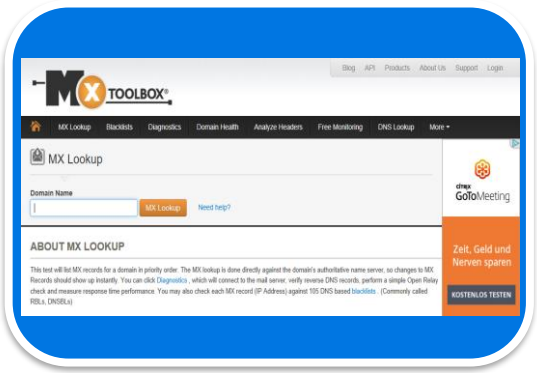
Absenderreputation

Domain-based Message Authentication, Reporting and Conformance (DMARC)

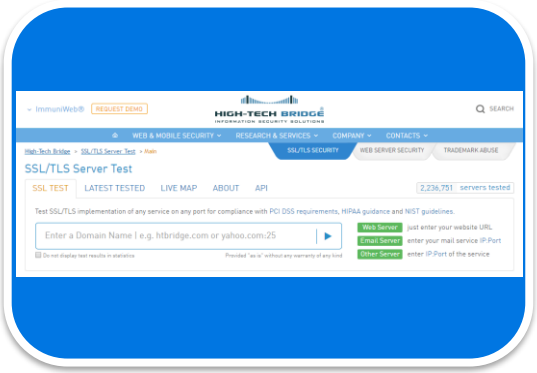
```
v=DMARC1;
        p=none;
        rua=mailto:dmarc_rua@netatwork.de;
        ruf=mailto:dmarc_ruf@netatwork.de;
        fo=1;
        adkim=s;
        aspf=s;
        rf=afrf;
        sp=none
```

Welche Tools gibt es?

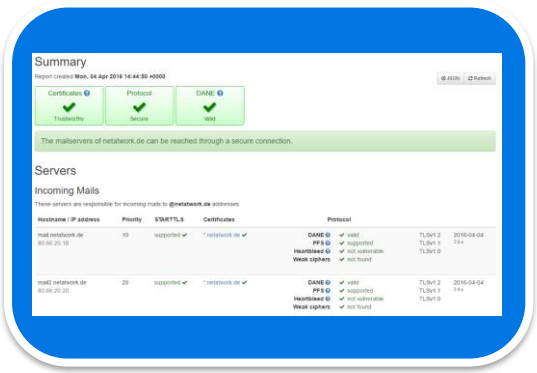
TeleTrusT EBCA
European Bridge Certificate Authority



MXToolbox.com



HighTech Bridge



ssl-tools.net

Immer für Sie da:

Sören Beiler
Presales Consultant
e: soeren.beiler@netatwork.de
t: +49 5251 304676

Workshop: Ergebnisse

TeleTrusT EBCA
European Bridge Certificate Authority

Was hindert mich am Einsatz von SPF und DMARC ?

- Angst, dass Mails verloren gehen
- Unklarheit der Admins oder Mailadmins, welche Server bereits im Namen der eigenen Domain E-Mails versenden dürfen
- Zuständigkeiten sind nicht immer geklärt, wenn z.B. das Marketing Newsletter Versender beauftragt die dann im eigenen Namen E-Mails versenden

Vorteile:

- Weniger Spam
- Steigerung der eigenen Reputation
- eigene Mails mit generischem Inhalt landen nicht mehr so schnell in einem Junk Ordner beim Empfänger
- Auswertung über den Missbrauch der eigenen Domain über die Aggregate Reports die um Zuge der Umsetzung der DMARC Policy an den Inhaber der Domain versendet werden
- bei "DMARC light" bekommt der Admin zunächst einen Überblick über die eingesetzten Mailserver und kann diese dann in den SPF einfließen lassen

Implementierung:

- zunächst sollte SPF und DMARC light eingesetzt werden um sich im klaren über alle erlaubten Hosts zu werden
- wenn möglich sollte die eigenen DNS Zone immer per DNSSEC geschützt sein
- alle beteiligten Mail Admins sollten "mit ins Boot" geholt werden um hier Fehler zu vermeiden
- nach einer Übergangsfrist von der Light Variante das System dann auf strict stellen