CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Ein Update zur Email-(Un)Sicherheit

oder: warum wir alle S/MIME nutzen sollten

Ben Stock

CISPA Helmholtz Center for Information Security

EDV Gerichtstag – 11.9.2024

About: ben

- Leitender Wissenschaftler am CISPA
- Forschungsbereich: **Web**-Sicherheit, **benutzbare** Sicherheit, **Netzwerk**-Sicherheit

- Lehrbeauftragter an der Universität des Saarlandes für Netzwerk- und Websicherheit
- **Sehr erfreut, heute mal aus dem "Elfenbeinturm" der Forschung berichten zu können**
- (obligatorisch: Folien tragen CISPA-Logo, stellen aber nicht Meinung meines Arbeitgebers dar)

Wer hat den Begriff schon mal gehört?

DNS

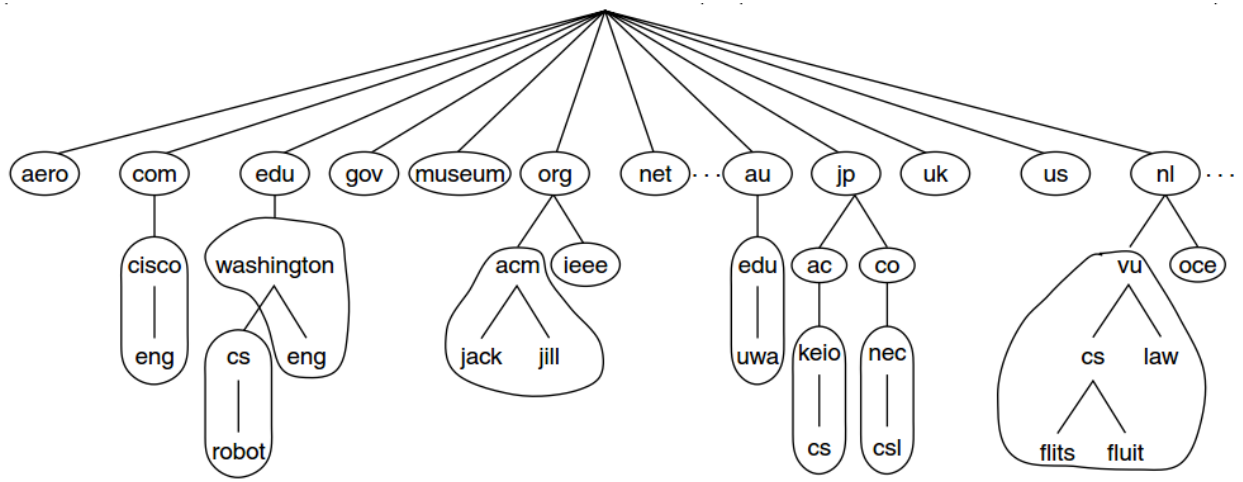
DNSSEC

Email

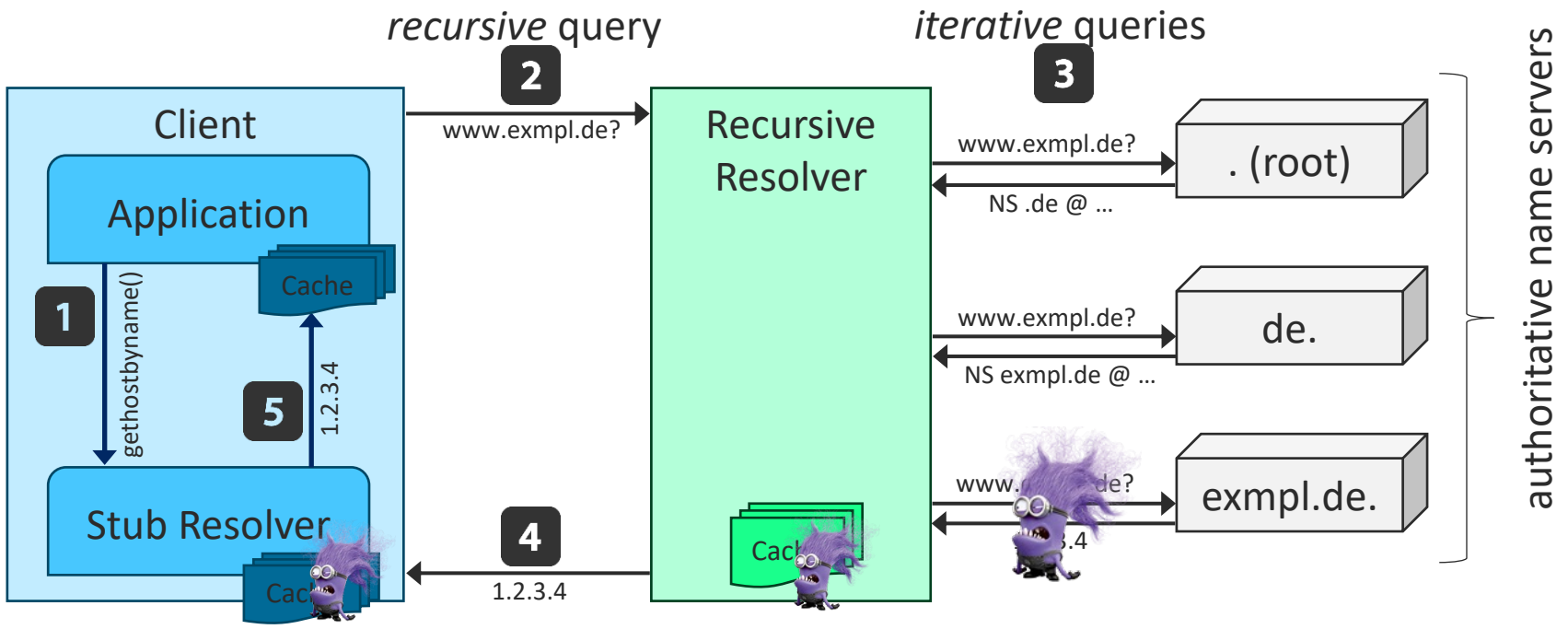
TLS

Domain Name System (DNS)

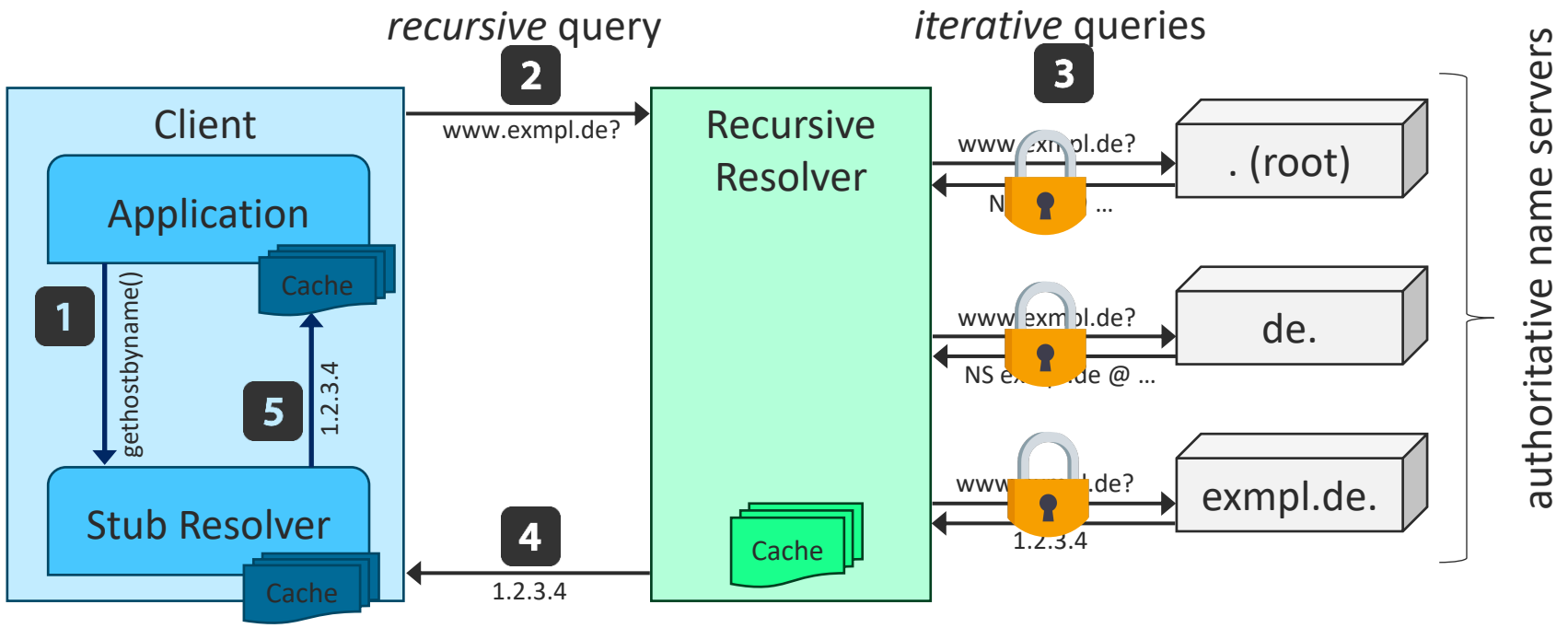
- Menschen können sich Namen leichter merken als Zahlen
  - Google.de statt 142.250.184.195 oder gar 2a00:1450:4001:830::2003
- Hierarchie von Root zu spezifischeren Zonen
  - Verschiedene Einträge pro Domain
  - A/AAAA Record: IP-Adresse zur Domain
  - MX Record: **M**ail e**X**change (zuständiger Mailserver)



Domain Name System (DNS)

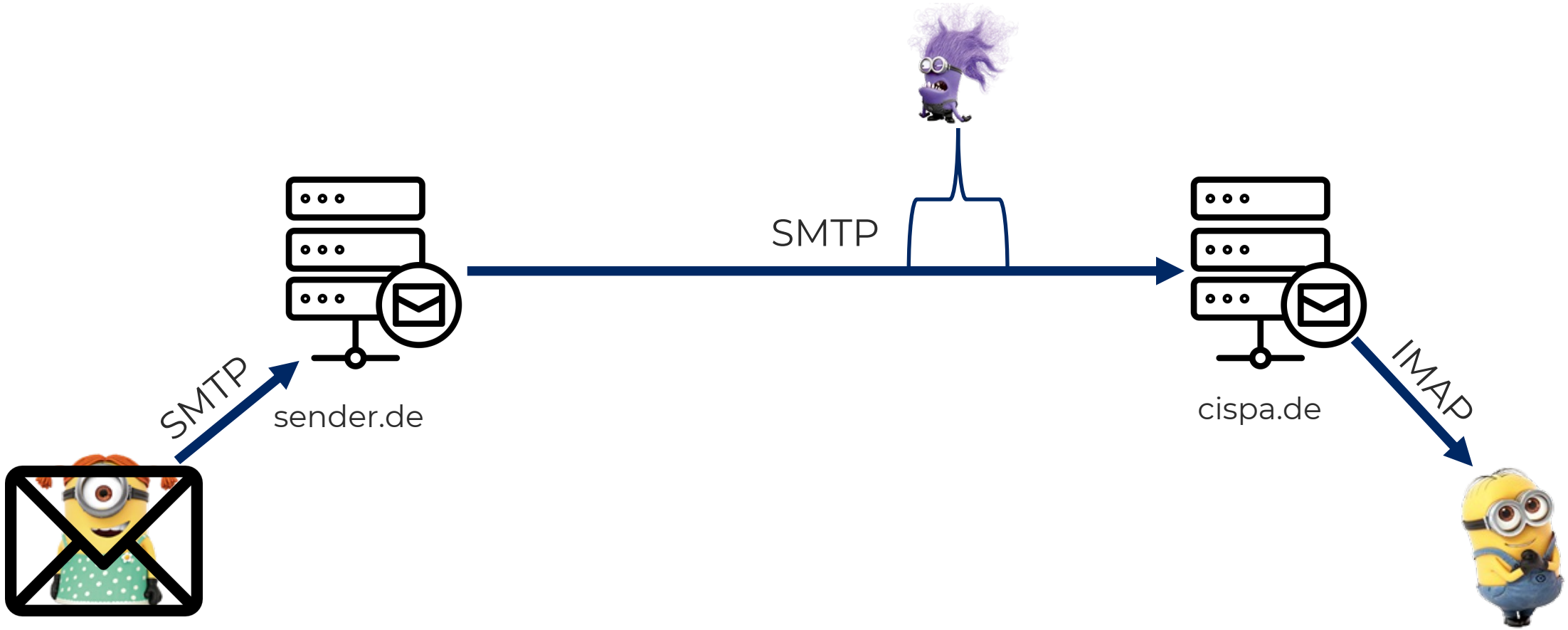


DNS Security Extensions (DNSSEC)



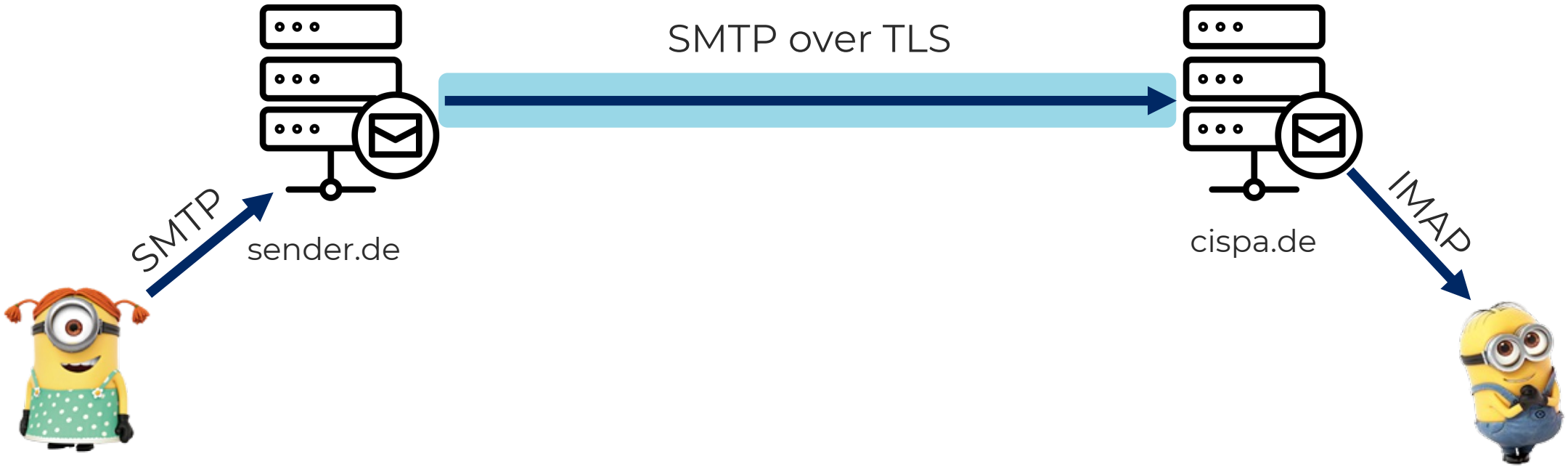
- Authoritative Nameserver signieren ihre Antworten, Recursive Resolver prüfen bevor sie im Cache landen

Email – Angreifer

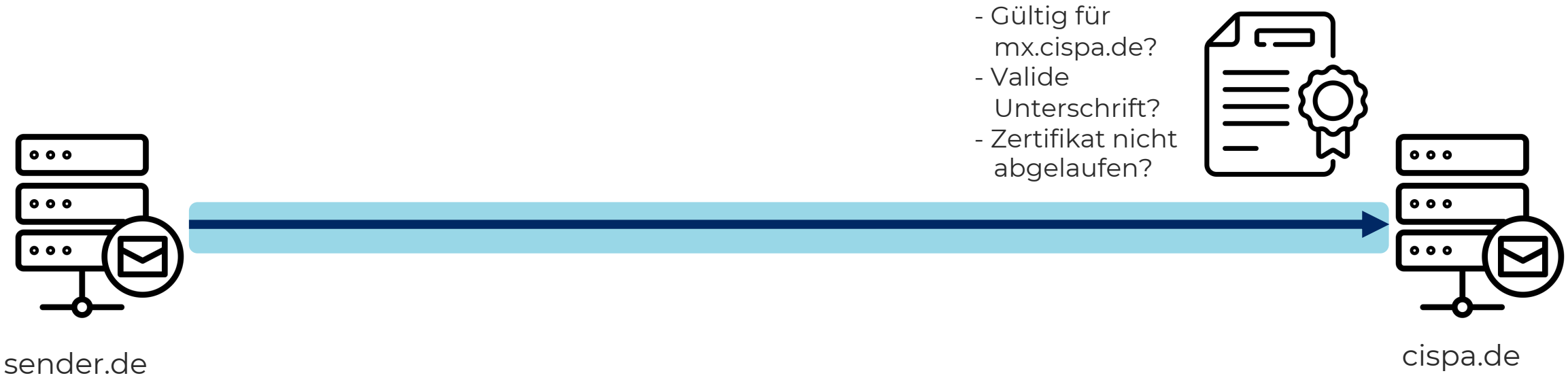


Von: Alice@sender.de
An: Bob@cispa.de

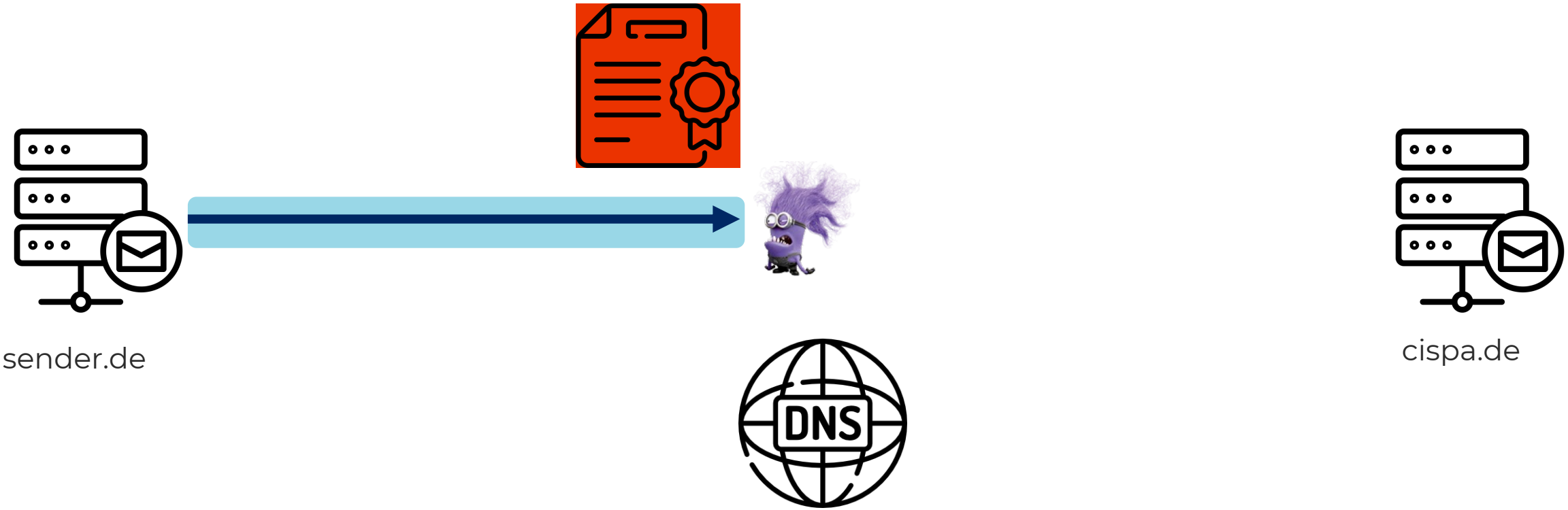
Email – SMTP over TLS / STARTTLS



Email – SMTP over TLS / STARTTLS



Email – SMTP over TLS / STARTTLS

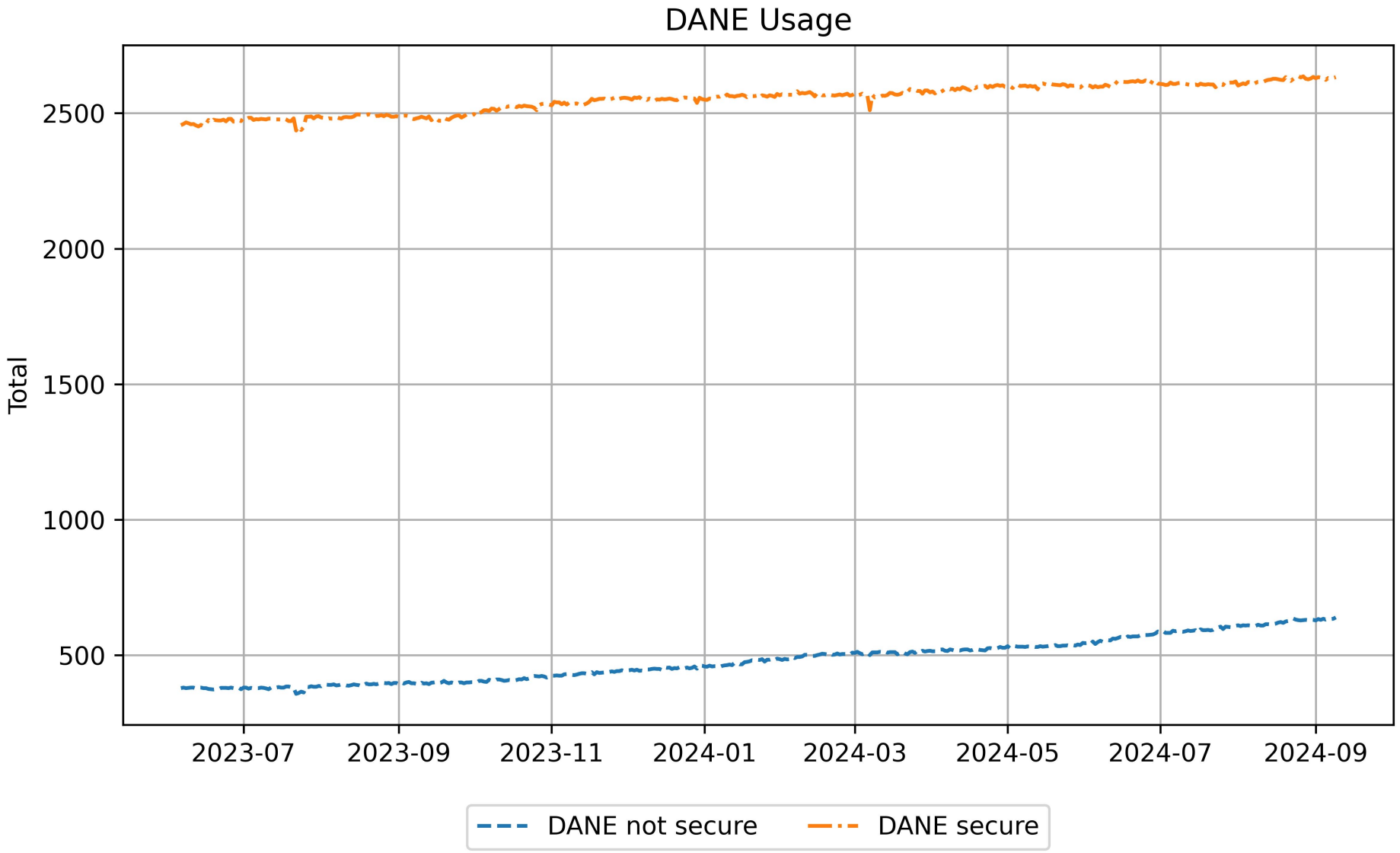


sender.de

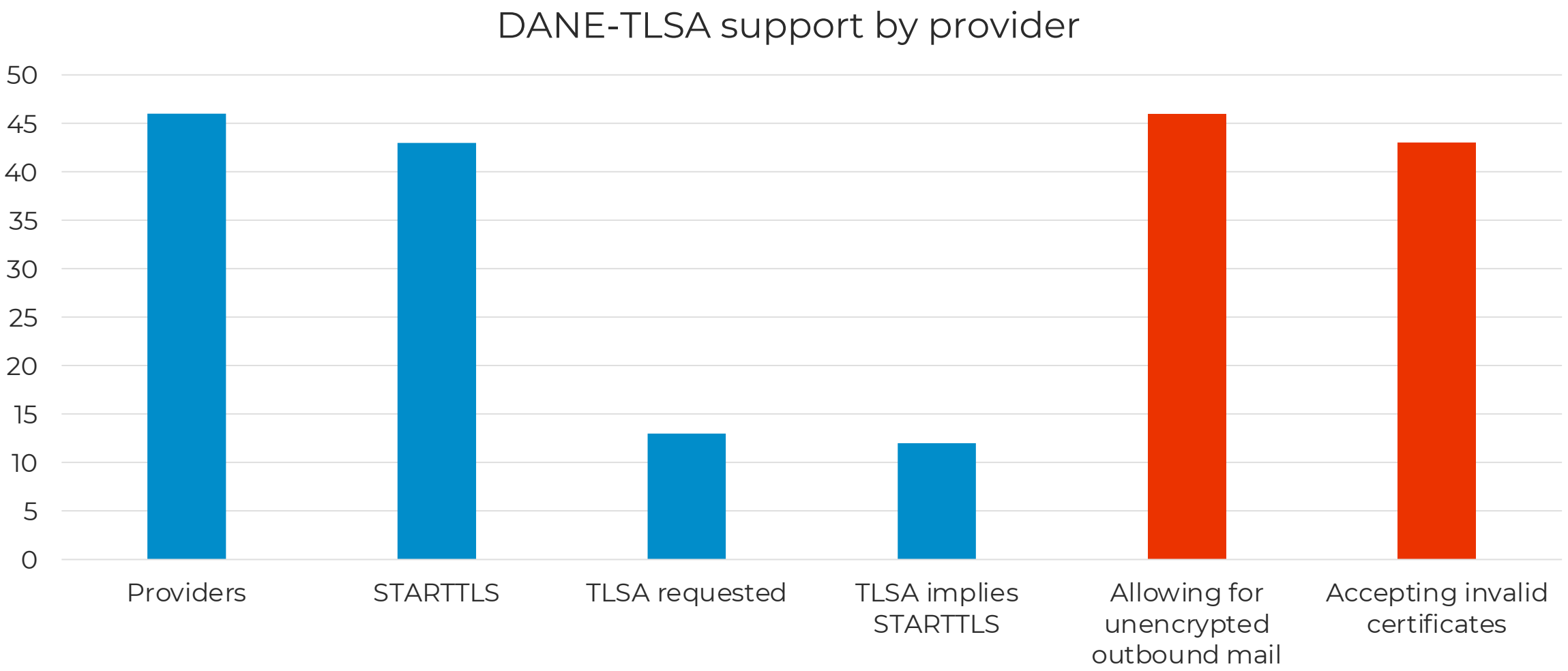
cispa.de

DANE-**TLSA** für mx.cispa.de
- spezifiziert erlaubtes Zertifikat
- wenn vorhanden: TLS **muss** genutzt werden und nur mit dem **korrekten** Zertifikat
- erfordert **DNSSEC** Signatur

DANE Nutzung über die Zeit (Top 1M Domains)

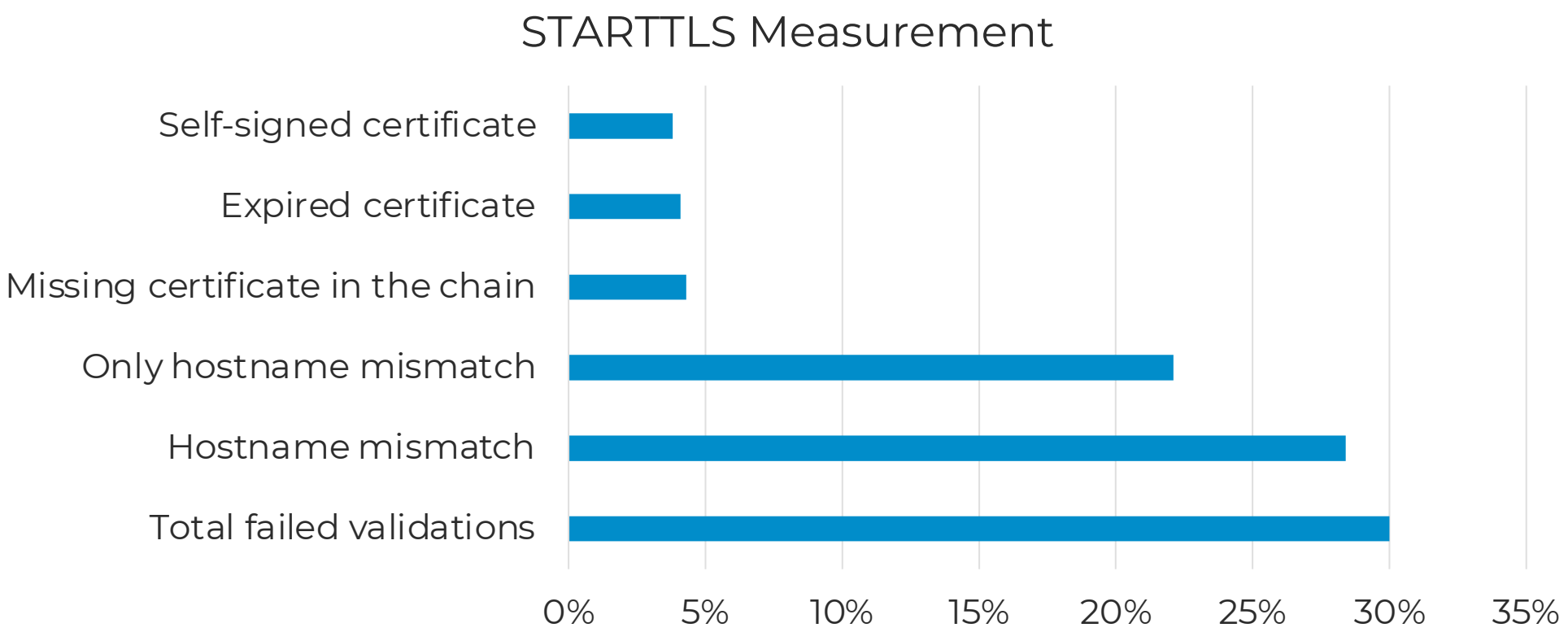


Ergebnisse Provider

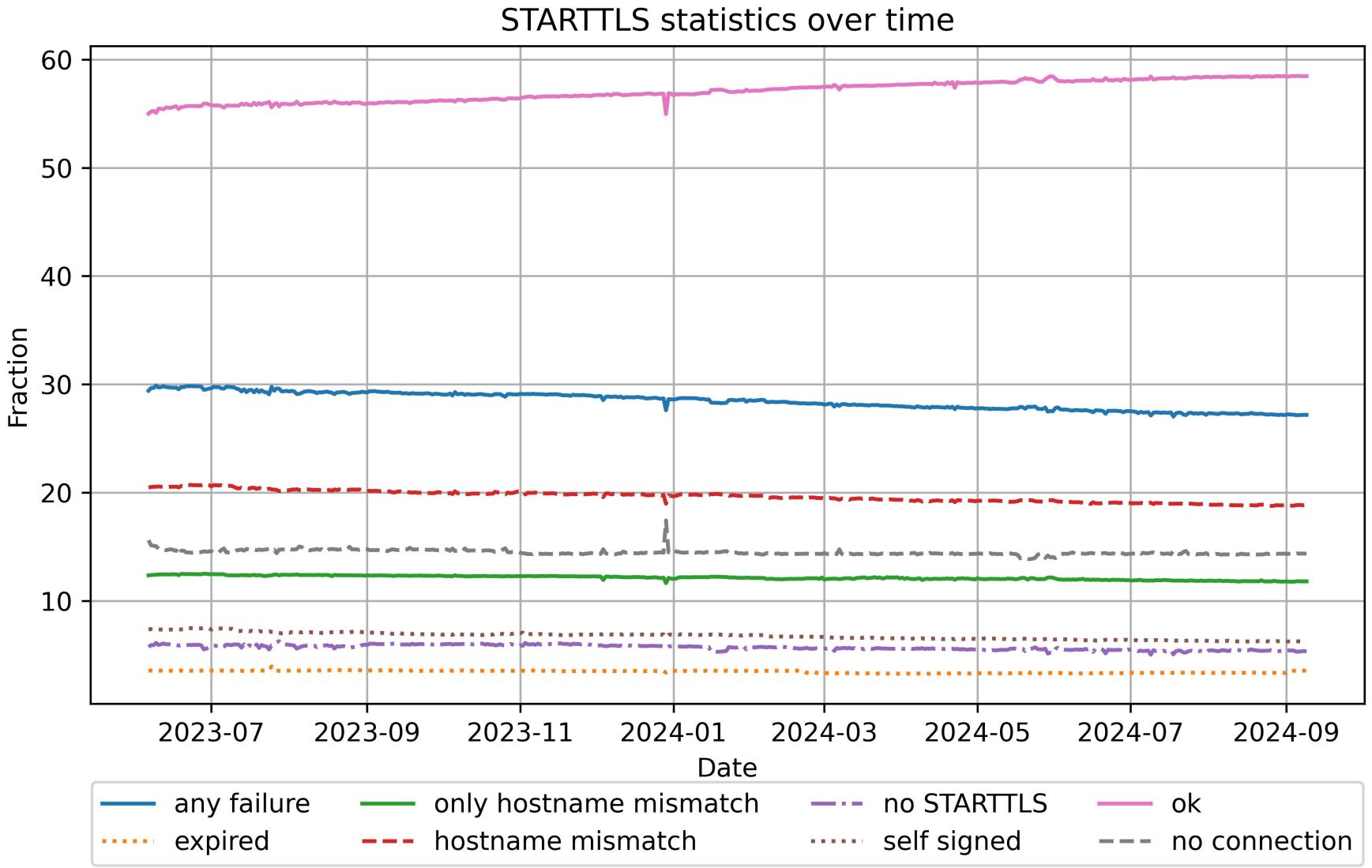


Top 10M Domains (Mai 2023) – MX-Statistiken

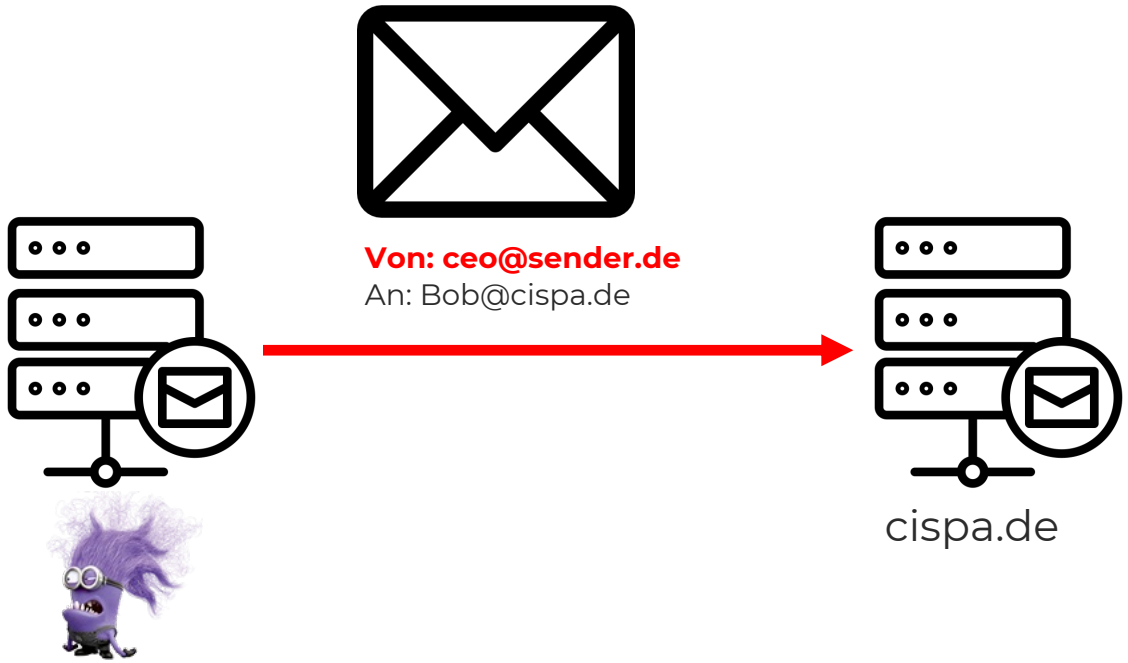
- 30% aller Zertifikate lassen sich nicht validieren



Top 1M Domains – MX Statistiken über Zeit



Email – Spoofing verhindern



- **Sender Policy Framework** (SPF)
  - Sender.de erlaubt explizit eigene MX (DNS-Eintrag)
  - Eingehende Mailserver wenden Regeln an
- **Domain-Keys Identified Mail** (DKIM)
  - Sender.de signiert alle Emails, veröffentlicht Schlüssel per DNS
  - Eingehende Mailserver prüfen Signature
- **Domain-based Message Authentication, Reporting and Conformance** (DMARC)
  - Verpflichtet Mailserver zu SPF/DKIM-Validierung
  - (erlaubt Reporting)

Wieso sollte man das konfigurieren?

Dein Vortrag

H

heike.hess@telekom.de <heike.hess@telekom.de> Today at 10:45

To: Ben Stock

Hi Ben,

ich bin total sicher, dass dein Vortrag super ist. Wir würden Dir daher gerne noch einen riesigen Bonus zahlen! Passt das für Dich?
LG
Heike

TELEKOM SECURITY
Deutsche Telekom Security GmbH
Heike Heß
Chapter Emergency and Continuity Management
Holzhauser Str. 4-8, 13509 Berlin
+49 30 8353 77577 (Telefon)
+49 160 905 701 91 (Mobil)
E-Mail: heike.hess@telekom.de
www.telekom.com

SPF, DKIM, DMARC (Stand: Anfang 2023)

Provider	SPF veröffentlicht	SPF angefragt	DKIM-signiert	DKIM angefragt	DMARC veröffentlicht	DMARC angefragt
T-Online	nein (inzwischen schon) *	nein	nein	ja	nein	nein
Web.de	ja	ja	ja	ja	ja	ja
Vodafone	ja	ja	ja	ja	ja	nein
Posteo	ja	ja	ja	ja	ja	ja
1und1.de	nein	ja	nein	ja	nein	nein
gmail.com	ja	ja	ja	ja	ja	ja

* Google verlangt entweder DKIM oder SPF

SPF, DKIM und DMARC bei bekannten Providern

Szenario	t-online.de	web.de	vodafone.de	posteo.de	1und1.de
DMARC Reject (kein SPF, kein DKIM)	●	●	●	●	●
DMARC Reject (SPF fail, DKIM fail)	●	●	●	●	●
DMARC Quarantine (SPF fail, DKIM fail)	●	●	●	●	●
DMARC Parent Reject	●	●	●	●	●
Double From	●	●	●	●	●

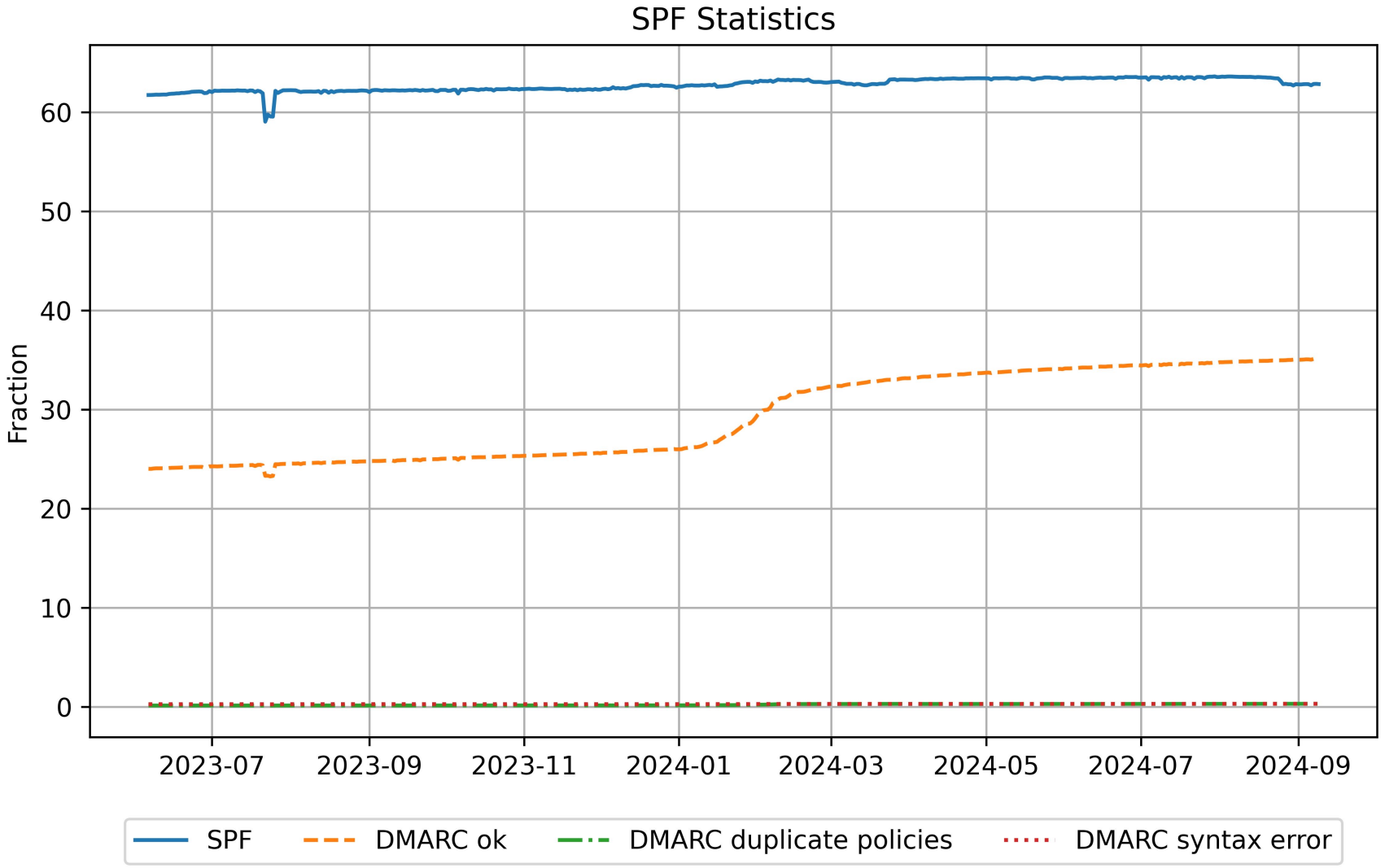
● Zustellung in Inbox ● Ablehnung ● Zustellung in Spam

SPF, DKIM und DMARC bei bekannten Providern

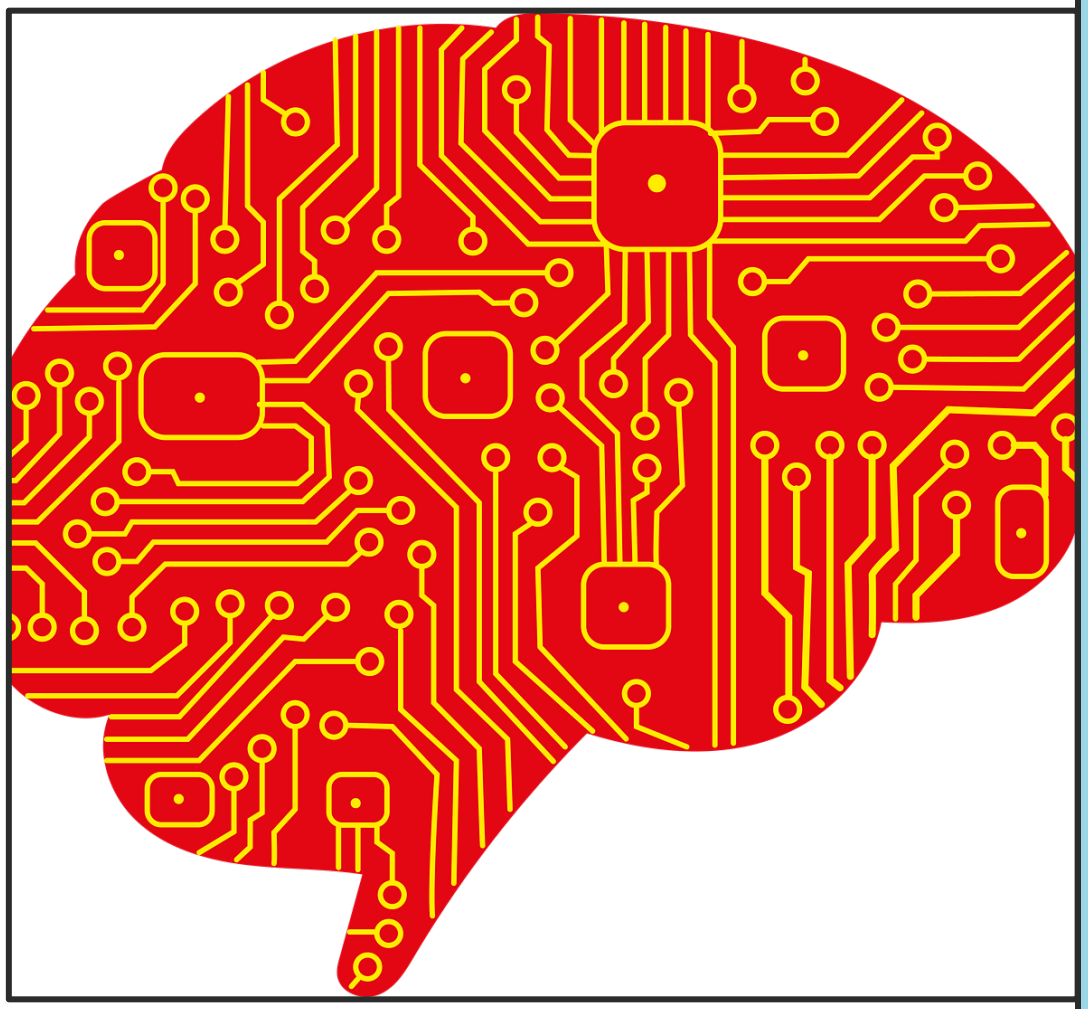
Szenario	t-online.de	web.de	vodafone.de	posteo.de	1und1.de	gmail.com
DMARC Reject (kein SPF, kein DKIM)	●	●	●	●	●	●
DMARC Reject (SPF fail, DKIM fail)	●	●	●	●	●	●
DMARC Quarantine (SPF fail, DKIM fail)	●	●	●	●	●	●
DMARC Parent Reject	●	●	●	●	●	●
Double From	●	●	●	●	●	●

● Zustellung in Inbox ● Ablehnung ● Zustellung in Spam

SPF und DMARC über Zeit (Top 1M Domains)



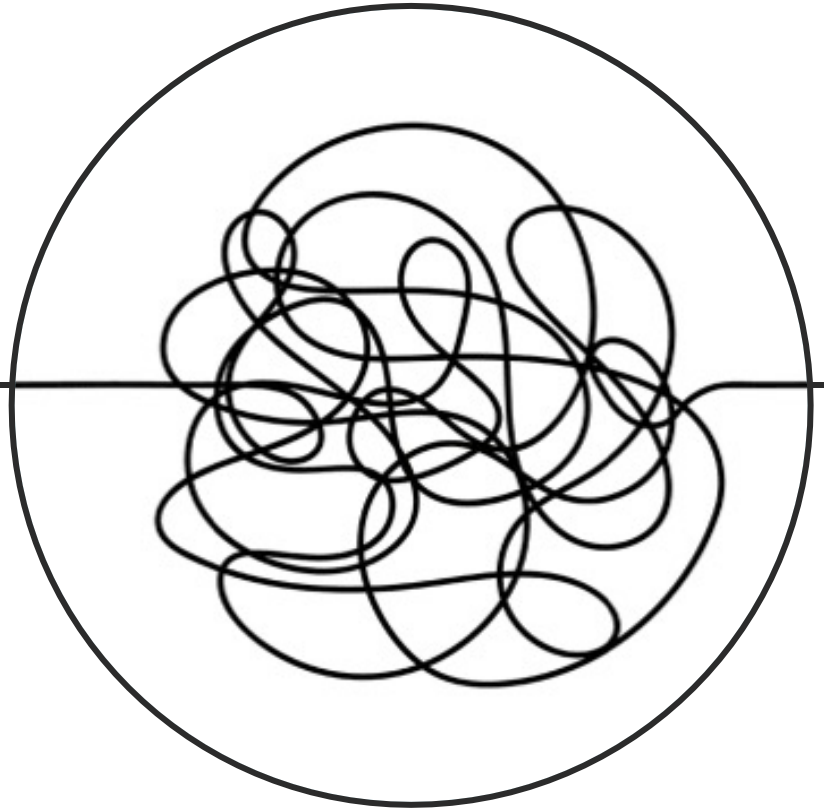
Komplexität bei Emails



- Email wurde ohne Security designed, alles danach sind **optionale Add-Ons**
- Große Player können Änderungen bewirken (z.B. Google mit SPF&DKIM)
  - Nicht so einfach wie im Web
- Fokus auf Kompatibilität mit **allen** Mailservern bedeutet Verlust von Sicherheit bei **vielen**
- (In aller Fairness: Email-Ökosystem wird noch komplexer durch Anti-Spam-Gateways, die SPF/DKIM stören…)

Freue mich auf die Diskussion!

- Email nutzen wir jeden Tag
- Email wurde nicht mit Sicherheit im Hinterkopf entwickelt
  - Aus Sicht des Elfenbeinturms: wegschmeißen, neu machen



- Konsequenzen: viele Mechanismen, um nachträglich Sicherheit hinzufügen
- ➔ extreme hohe Komplexität und Fehleranfälligkeit
- … für Benutzer weder gut zu verstehen noch zu beeinflussen
- **Einzig sichere Option: Ende-zu-Ende Verschlüsselung (S/MIME oder PGP)**