

kivitendo, E-Mail und die Archiv-Pflicht



E-Mail Ursprung



1970

Geschlossene Netze

Extra einfach (Simple Mail Transfer Protocol)

==> nur in der Uni verwenden!!!

E-Mail Garantie:

Zustellung nicht garantiert

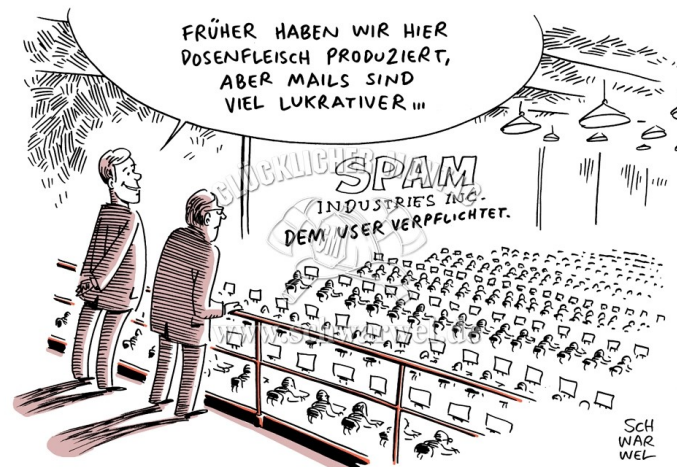
Absender nicht fälschungssicher

Lesbar für alle Internet-Postboten (Postkarte)



Bitte erneut ziehen, um die nächste Portoerhöhung zu sehen.

© Gätz Wiedenroth - www.sh-wiedenroth-kanikatur.blogspot.de



SCH
WAR
WEL



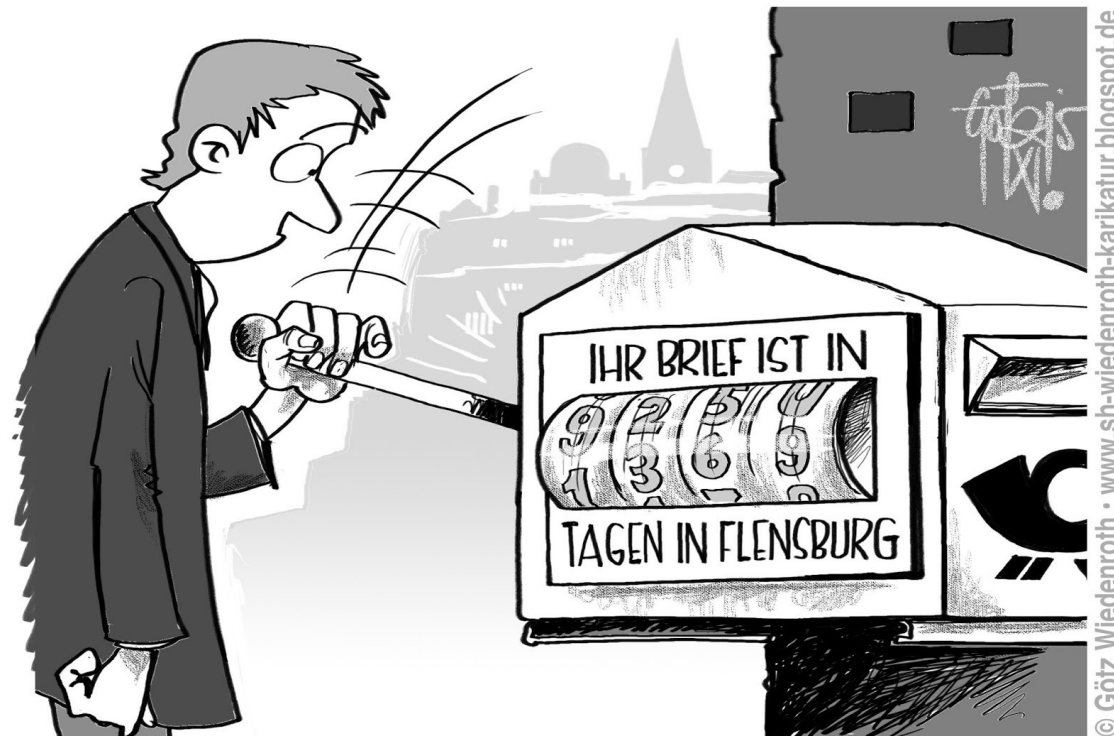
ICH HABE AUS VERSEHEN ENNIGE
WICHTIGE E-MAILS GELOSCHT,
KÖNNEN SIE MIAL NACHSCHAUEN,
OB SIE BEI IHNEN NOCH
GESPEICHERT SIND.

E-Mail Garantie:

Zustellung nicht garantiert

Absender nicht fälschungssicher

Lesbar für alle Internet-Postboten (Postkarte)



© Götz Wiedenroth • www.sh-wiedenroth-karikatur.blogspot.de

Bitte erneut ziehen, um die nächste Portoerhöhung zu sehen.

SMTP Antwort 250

Zustellung ohne Relay

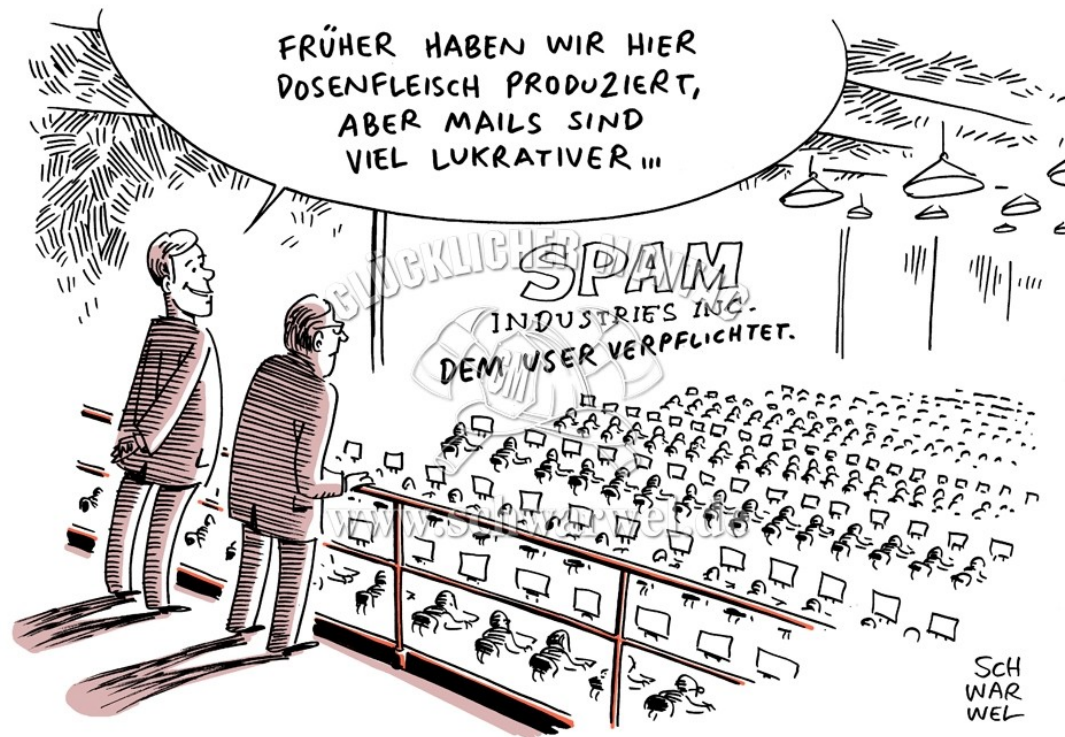
SMTP 250 → Übergabe an Posteingang

E-Mail Garantie:

Zustellung nicht garantiert

Absender nicht fälschungssicher

Lesbar für alle Internet-Postboten (Postkarte)



DNS ist nicht fälschungssicher

www.sparkasse.de ==> www.cima.ky

Quick Links ▼

The Latest ▼



84 °F

12:28:34 pm EST



Search

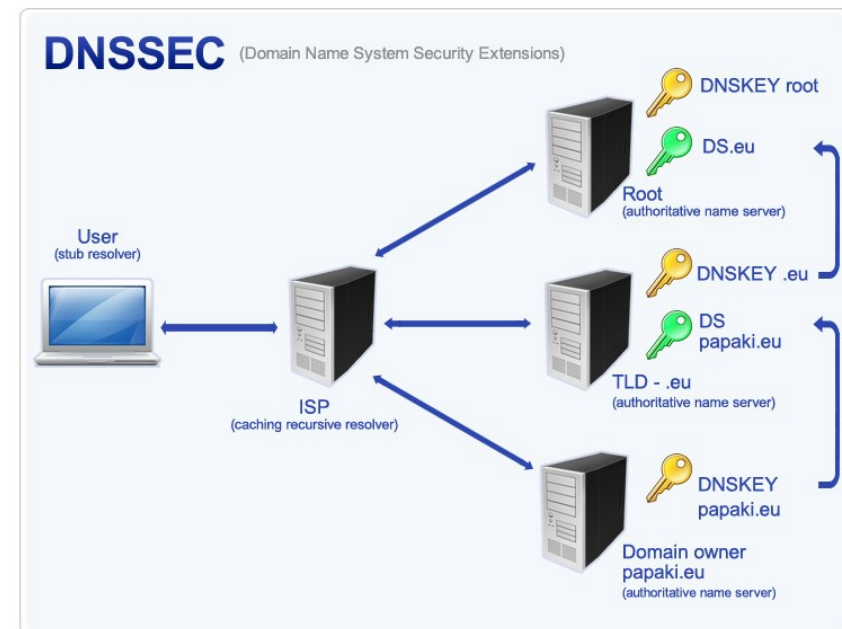


Cayman Islands Monetary Authority

DNSSEC


Prinzipielles Problem gelöst

Technisch komplexer zu implementieren

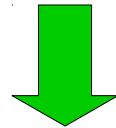


DNSSEC für https

Search: My Add-ons Available Add-ons

 **DNSSEC**
Check the DNSsec status of every website you browse. [More](#)

www.sparkasse.de



  https://www.sparkasse.de 300%   DNS 

 www.sparkasse.de
secure by DNSSEC

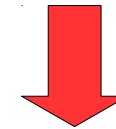
Domain **www.sparkasse.de** is properly secure through DNSSEC.

You can learn more about [DNSSEC on Wikipedia](#).

Https ohne DNSSEC ...



www.deutsche-bank.de

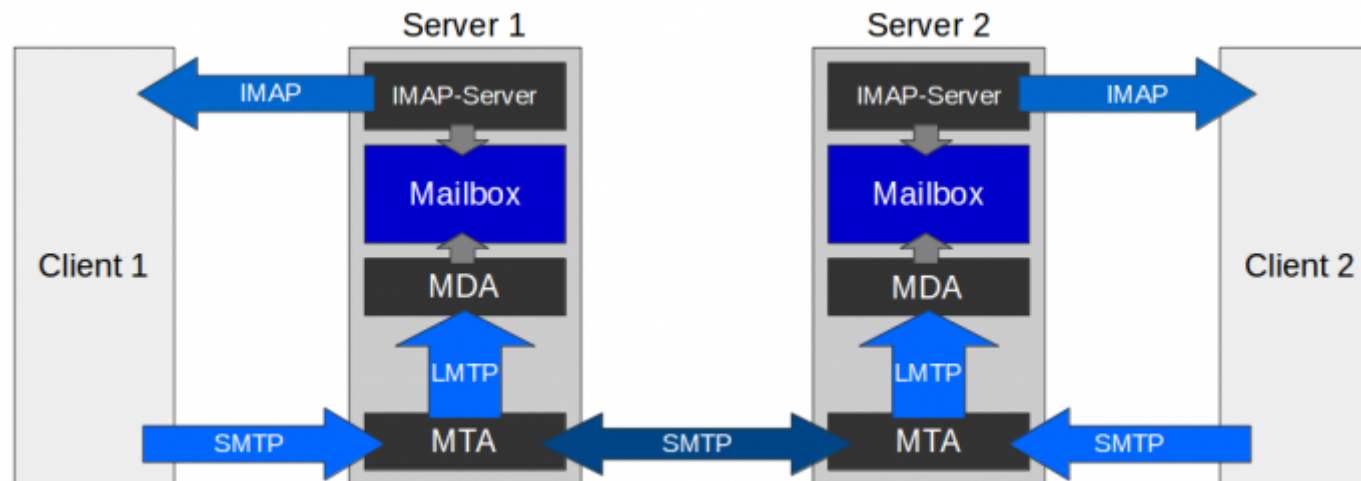
A screenshot of a web browser displaying a security warning. The address bar shows the URL "https://www.deutsche-bank.de/pk.html". A red "DNS" indicator is visible in the address bar. A warning box is overlaid on the page, containing a red "X" icon and the text: "www.deutsche-bank.de not secure by DNSSEC". Below this, it states: "Domain www.deutsche-bank.de is not secure through DNSSEC. Your connection is prone to man-in-the-middle attacks." and "You can learn more about [DNSSEC on Wikipedia](#)." The background of the browser shows the Deutsche Bank Konzern website with navigation links like "Privatkunden", "Vermögende Kunden", and "Geschäft".

DANE = DNSSEC über SMTPS

Einfacher als über https,
da SIMPLE Mail Transfer Protocol ?

DANE = DNSSEC über SMTPS

Komplexer:
Kommunikationspartner
mindestens 4



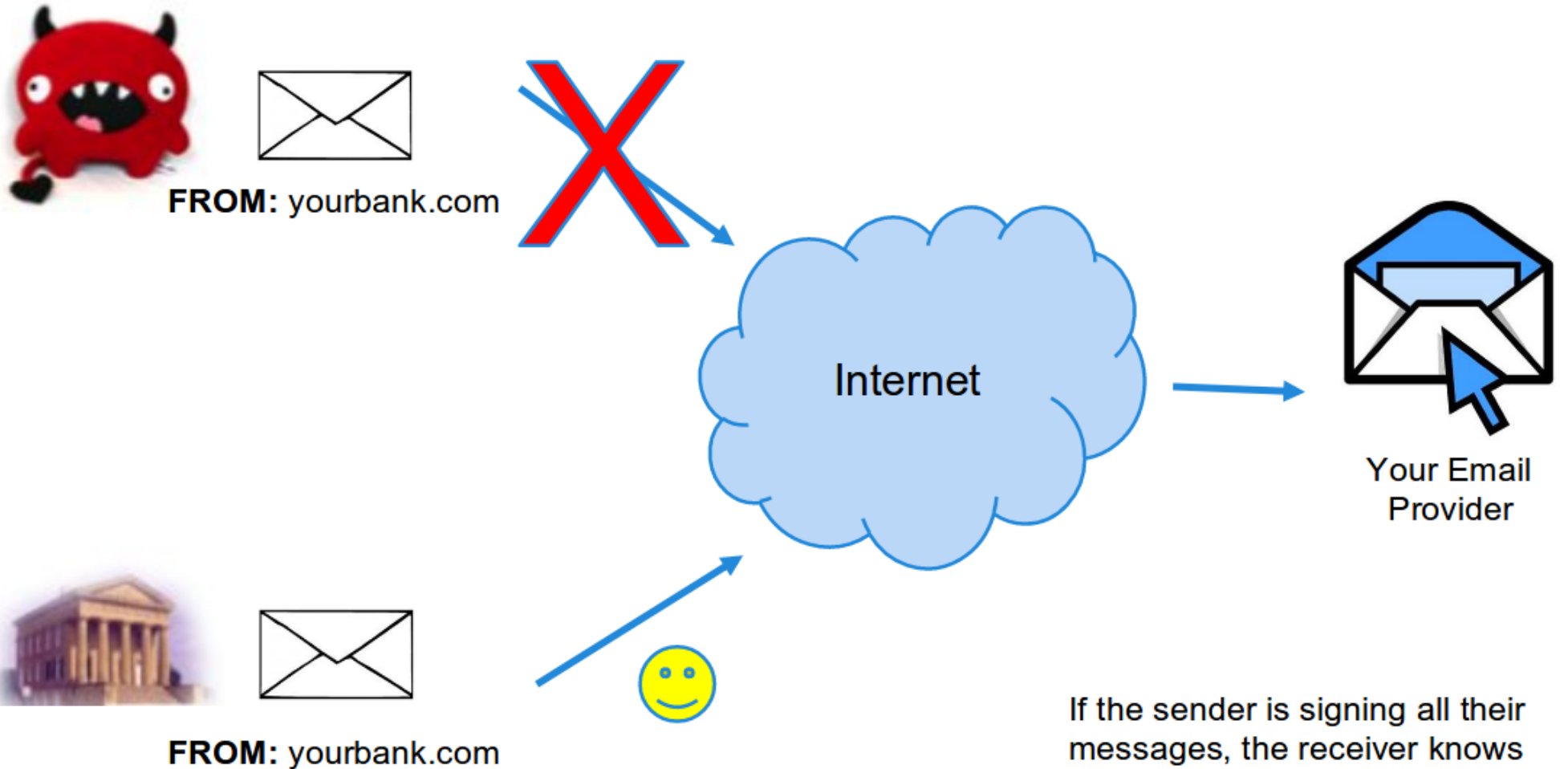
Zustellung nicht garantiert

Absender nicht fälschungssicher

Lesbar für 2 Internet-Postboten (Postkarte)

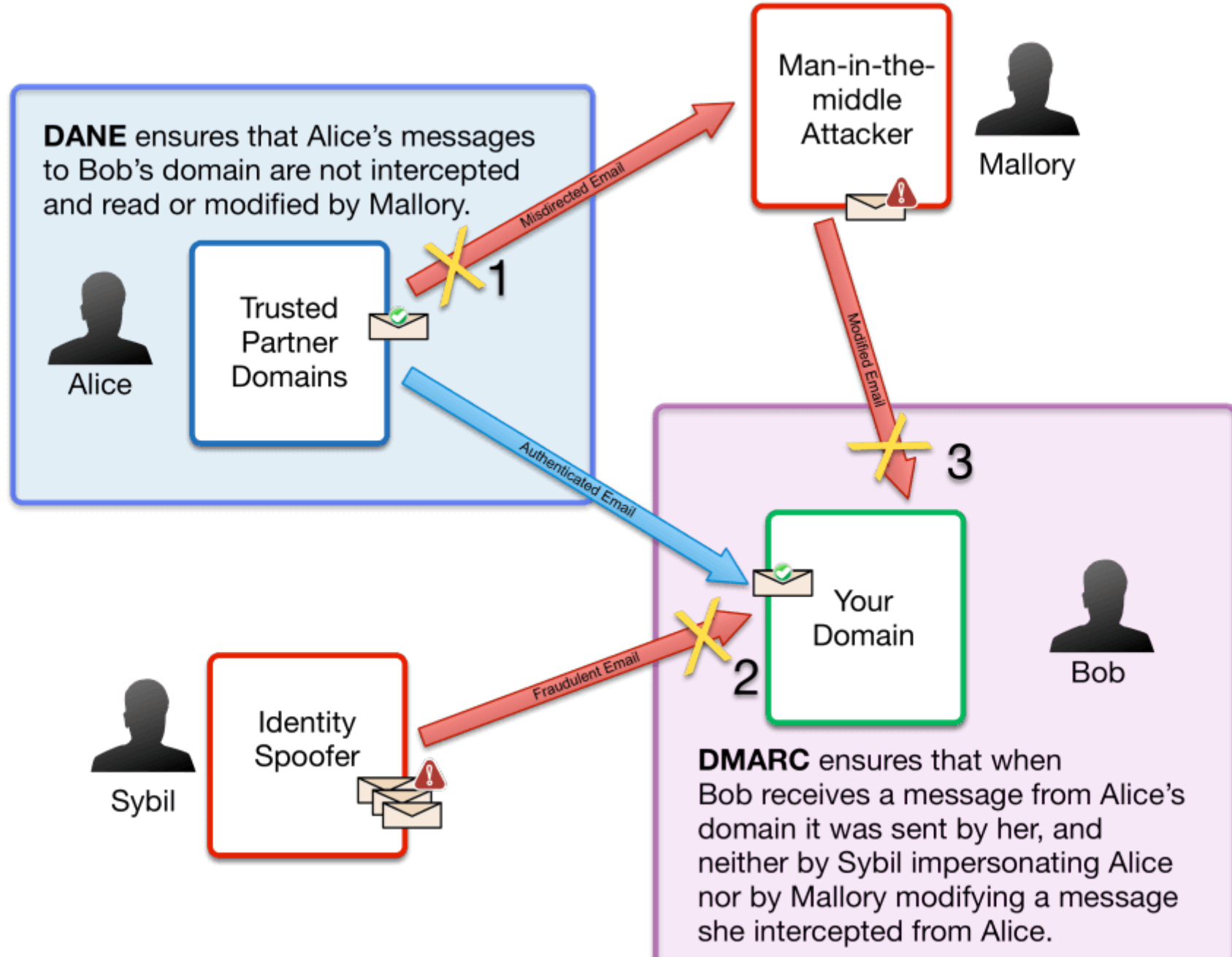
DMARC

Senders authenticate ALL mail and tell that to receivers



If the sender is signing all their messages, the receiver knows unsigned messages are phishing

DANE + DMARC



TLS Policy level !



~~Opportunistic Encryption~~ ==> dane-only (postfix)

```
ww postfix/smtpd[30126]: SSL_accept:unknown state  
ww postfix/smtpd[30126]: Anonymous TLS connection established from mani-gmbh.com[78.94.216.132]:  
25: (0.0000000 seconds)
```



```
www postfix/smtp[1363]: Verified TLS connection established to mani-gmbh.com[78.94.216.132]:25:
```


DNSSEC + DANE + DMARC

Zustellung nicht garantiert

Absender nicht fälschungssicher

Lesbar von 2 Mailserver

Mail-Inhalt änderbar von 1 Mailserver

Ist das kompliziert ?



2 Mailsysteme sauber konfigurieren

S/MIME ist komplizierter



2 bis n E-Mail-Clients sauber konfigurieren

Anwender statt Admins

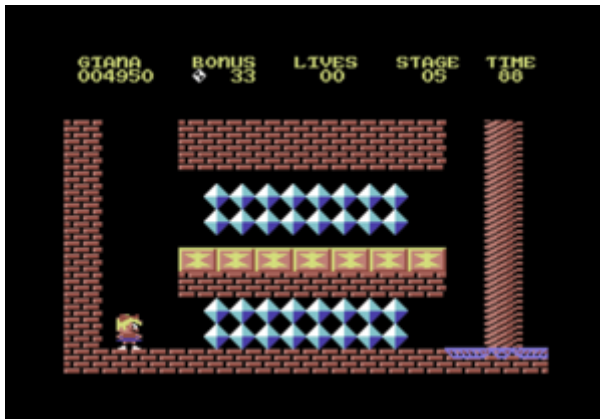
E-Mail Inhalt nicht vom Mail-Server lesbar!

DMARC Bonus Level!



Lass das SYSTEM für DICH arbeiten!

=> DMARC Reports



POKE	8257,173	\$2041,\$ad	unendlich Leben
POKE	7450,000	\$1d1a,\$00	unendlich Zeit

Forensic reports



dmARC:mani-gmbh.com

Find Problems

Solve Email Delivery Problems

dmARC

```
v=DMARC1; p=reject; rua=mailto:jan@kivitendo-premium.de; ruf=mailto:jan@kivitendo-premium.de; adkim=s;
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. TagValue can be 'none', 'quarantine', or 'reject'.
rua	mailto:jan@kivitendo-premium.de	Receivers	List of URIs for receivers to send XML feedback to. URIs are required to be added in the format of 'mailto:address@example.com'.
ruf	mailto:jan@kivitendo-premium.de	Forensic Receivers	List of URIs for receivers to send Forensic reports to. URIs are required to be added in the format of 'mailto:address@example.com'.
adkim	s	Alignment Mode DKIM	Specifies 'Alignment Mode' for DKIM signatures. (r) is for Relaxed which allows authenticated DKIM d=domains that share a common organizational domain with an email's header-From:domain to pass the DMARC test. (s) is for Strict which requires an exact match between the DKIM d=domain and an email's header-From:domain.

Google nimmt uns ernst



Report domain: mani-gmbh.com Submitter: google.com Report-ID: 17441977297364766276	• noreply-dmarc-support@google.com	🕒 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 7072486405678875019	• noreply-dmarc-support@google.com	🕒 08.04.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 8032220609918980985	• noreply-dmarc-support@google.com	🕒 07.04.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 5782097968926327304	• noreply-dmarc-support@google.com	🕒 06.04.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 5782097968926327304	• noreply-dmarc-support@google.com	🕒 06.04.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 13944197070428369070	• noreply-dmarc-support@google.com	🕒 05.04.2018 01:59
Report Domain: mani-gmbh.com Submitter: linkedin.com Report-ID: linkedin.com!mani-gmbh.com!...	• dmarc-noreply@linkedin.com	🕒 04.04.2018 03:54
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 10332821968924008207	• noreply-dmarc-support@google.com	🕒 04.04.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 3194592486335932801	• noreply-dmarc-support@google.com	🕒 02.04.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 4697112794643702766	• noreply-dmarc-support@google.com	🕒 01.04.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 9557856697709970997	• noreply-dmarc-support@google.com	🕒 31.03.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 17005031185293755742	• noreply-dmarc-support@google.com	🕒 30.03.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 15251217910160330796	• noreply-dmarc-support@google.com	🕒 29.03.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 3525423924520179440	• noreply-dmarc-support@google.com	🕒 28.03.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 9386553787978527608	• noreply-dmarc-support@google.com	🕒 27.03.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 9386553787978527608	• noreply-dmarc-support@google.com	🕒 27.03.2018 01:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 13303724525520866413	• noreply-dmarc-support@google.com	🕒 24.03.2018 00:59
Report Domain: mani-gmbh.com Submitter: reports.emailsrvr.com Report-ID: 2e554713-03e2-48e1-b67...	• DMARC Report	🕒 23.03.2018 15:31
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 17972920182058677170	• noreply-dmarc-support@google.com	🕒 23.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 17972920182058677170	• noreply-dmarc-support@google.com	🕒 23.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 14780722788844192050	• noreply-dmarc-support@google.com	🕒 22.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 3169408436169373306	• noreply-dmarc-support@google.com	🕒 21.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 16929208747754981275	• noreply-dmarc-support@google.com	🕒 20.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 2274477045940943690	• noreply-dmarc-support@google.com	🕒 19.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 11774656908058422774	• noreply-dmarc-support@google.com	🕒 17.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 1934194240188115639	• noreply-dmarc-support@google.com	🕒 16.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 17116385866862796890	• noreply-dmarc-support@google.com	🕒 15.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 12916069625462425106	• noreply-dmarc-support@google.com	🕒 14.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 5752584320956015753	• noreply-dmarc-support@google.com	🕒 13.03.2018 00:59
Report Domain: mani-gmbh.com Submitter: linkedin.com Report-ID: linkedin.com!mani-gmbh.com!...	• dmarc-noreply@linkedin.com	🕒 11.03.2018 01:46
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 12998912288839001279	• noreply-dmarc-support@google.com	🕒 10.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 11006338593611260851	• noreply-dmarc-support@google.com	🕒 09.03.2018 00:59
Report domain: mani-gmbh.com Submitter: google.com Report-ID: 7879554137709056177	• noreply-dmarc-support@google.com	🕒 07.03.2018 00:59

Google-Einstufung: Quarantäne!

```
- <row>
  <source_ip>151.84.197.169</source_ip>
  <count>8</count>
  - <policy_evaluated>
    <disposition>quarantine</disposition>
    <dkim>fail</dkim>
    <spf>fail</spf>
    - <reason>
      <type>forwarded</type>
      - <comment>
        looks forwarded, downgrade to quarantine with phishing warning
      </comment>
    </reason>
  </policy_evaluated>
</row>
```

Thunderbird Plugins

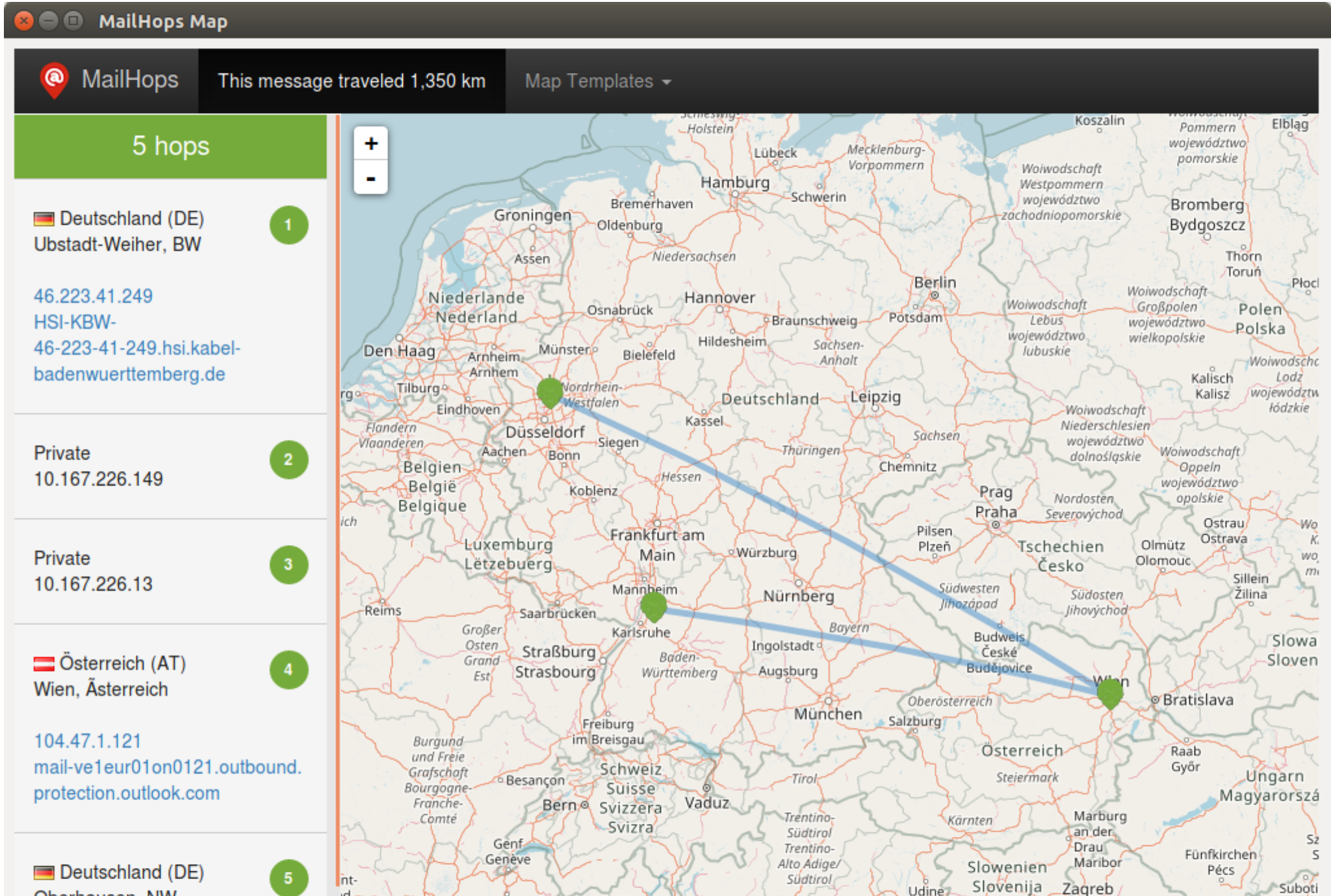


Mailhops

Check DKIM

rspamdspamness

MailHops GEO-IP



E-Mails sind Geschäftsdokumente (ca. 2006)

E-Mails inkl. Eingangsrechnung

Verfahrensdokumentation

Konsequenzen



E-Mails prinzipiell 10 Jahre aufbewahren
Rechnungs-E-Mails anders bearbeiten

IMAP only



Versehentlich Löschen!

Technisches Backup aller Mails SMTP

Schreibgeschütztes Postfach

Mail-Archiv 3. Anbieter mit Signatur

Verfahrensdokumentation kivitendo

Prozesse müssen dokumentiert sein,
Dritt-Anbieter Zertifikat reicht nicht aus!

GMV sagt:



Geschäftswichtige Daten schnell und einfach
Auffinden!

GMV (Gesunder Menschen-Verstand)

google sagt:



Gib mir alle DATEN und ich finde alles!

Schreibgeschütztes Postfach

Postfächer nach Lieferanten

Verknüpfung Mail mit Kreditorenbuchung

Indizierung der E-Mail plus Anhang

Verfahrensdoku als Arbeitsanweisung

Schreibgeschütztes Postfach

Postfächer nach Lieferanten

Verknüpfung Mail mit Kreditorenbuchung

Indizierung der E-Mail plus Anhang

Verfahrensdoku als Arbeitsanweisung

- E-Mail-Archiv ausgehende Mails
- WebDAV für digitalen Beleg
- kivi-DMS für digitalen Beleg
- verknüpfte Belege mit E-Mail-Archiv

E-Mail

<input type="checkbox"/>	Verschickt am	Betreff	Status	Von
<input type="checkbox"/>	23.02.2018 16:04:46	<u>Brief so und so nicht weiter</u>	failed	"" <jan@richardson-bueren.de>
<input type="checkbox"/>	23.02.2018 14:42:20	<u>Brief</u>	failed	"" <jan@richardson-bueren.de>

Verknüpfungen hinzufügen

Verknüpfungen löschen

Verknüpfung Mail mit Kreditorenbuchung

- E-Mail-Archiv + eingehende Mails
- Verknüpfte Belege + eingehende Mails
- Vorfilter simpel mit SMTP / Sieve
- Rechnungserkennung mit Buchungsvoralgen

Indizierung der E-Mail plus Anhang

- pdf2totxt
- Indizierung mittels IMAP-Plugin