

E-Mail made in Germany: Was steckt da steckt da was dahinter?

→ **Helein Support**

- IT-Consulting und 24/7 Linux-Support mit 25 Mitarbeitern
- Eigener Betrieb eines ISPs seit 1992
- Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

→ Mailserver-Spezialisten seit 1992

→ 24/7-Notfall-Hotline: 030 / 40 50 5 - 110

- 25 Spezialisten mit LPIC-2 und LPIC-3
- Für alles rund um Linux & Server & DMZ
- Akutes: Downtimes, Performanceprobleme, Hackereinbrüche, Datenverlust
- Strategisches: Revision, Planung, Beratung, Konfigurationshilfe

Kill den Mythos 1:

Was hat DE-Mail mit (IT-) Sicherheit zu tun?

Wofür ist DE-Mail da?

- DE-Mail stellt die Identität der Beteiligten sicher
- DE-Mail bietet die Möglichkeit, den Zugang einer E-Mail zu beweisen.
- DE-Mail ist vor allem ein juristisches Konstrukt mit fragwürdigem Nutzen für den Bürger.
 - DE-Mail-Mails wirken Kraft Gesetzesdeefinition wie eine Postzustellungsurkunde
 - Für den Bürger ist ein schlecht gepflegter DE-Mail-Account sehr problematisch!

Bietet DE-Mail wenigstens eine sichere Verschlüsselung?

- DE-Mail bietet keine Ende-zu-Ende-Verschlüsselung auf Basis von nutzerindividuellen Schlüsseln.
- Stattdessen wird von Station zu Station verschlüsselt.
 - Auf dem jeweiligen Speicherserver liegt die E-Mail entschlüsselt im Klartext herum.
 - Von der Qualität so wie SSL/TLS.
 - „Lawful interception“ ist also Tür und Tor geöffnet.
- DE-Mail hat nichts mit (Daten-) Sicherheit zu tun.

Was hat DE-Mail mit Sicherheit zu tun?

Nichts.

Kill den Mythos 2:

**„E-Mail made in Germany“ macht E-Mails
jetzt sicher**

Der lange Weg zu „E-Mail made in Germany“

- Seit > 15 Jahren wird über sichere SSL/TLS-Verbindungen kommuniziert
- Jahrelang wurde „den Großen“ angekreidet, dass Sie kein oder nur sehr lückenhaft SSL/TLS anbieten
- Oft noch nicht einmal POP3/IMAP/SMTP-Verbindungen mit Passwörtern verschlüsselt

EMIG: Was ist letzten Sommer geschehen?

- SSL/TLS wurde aktiviert
 - smtp_use_tls=yes
 - smtpd_use_tls=yes

- Und dann war da noch:
 - cat \$\$\$ >> /dev/marketing
 - cat \$\$\$ >> /dev/marketing
 - cat \$\$\$ >> /dev/marketing
 - cat \$\$\$ >> /dev/marketing

Was taugt „E-Mail made in Germany“?

- E-Mail made in Germany ist ein genialer Marketing-Trick
 - Zur rechten Zeit am rechten Ort mal richtig fix gewesen! Respekt.
- Technisch ist es nichts anderes als
20 Jahre nach allen anderen aktivieren auch web.de, GMX, T-Online
und Freenet die üblichen Technologien wie SSL/TLS.
 - *Aber da man es doch ganz bestimmt noch mehr geben?*
Nein, gibt (zurzeit zumindest) nicht.
 - *Aber was wie eine Verifizierung der Gegenstelle?*
Nein. An Konzept wird noch überlegt...
 - *Aber dann kann ein man-in-the-middle das ja aufbohren?*
→ Ja. Kann er.

Aber bei EMIG sind meine Mails sicher verschlüsselt.

- EMIG macht (jetzt endlich) SSL, andere Provider machen das auch.
- Mails von EMIG an EMIG werden mit SSL verschlüsselt
- Mails von EMIG an andere werden mit SSL verschlüsselt
- Mails von anderen an EMIG werden mit SSL verschlüsselt
- Mails von anderen an andere werden mit SSL verschlüsselt

- Muß ich zu EMIG gehen damit ich SSL-verschlüsselte Mails habe?
 - Nein. Man muß zu einem Anbieter gehen, der Verschlüsselung ernst nimmt.
 - Idealerweise auf technischer Ebene, statt nur im Marketing

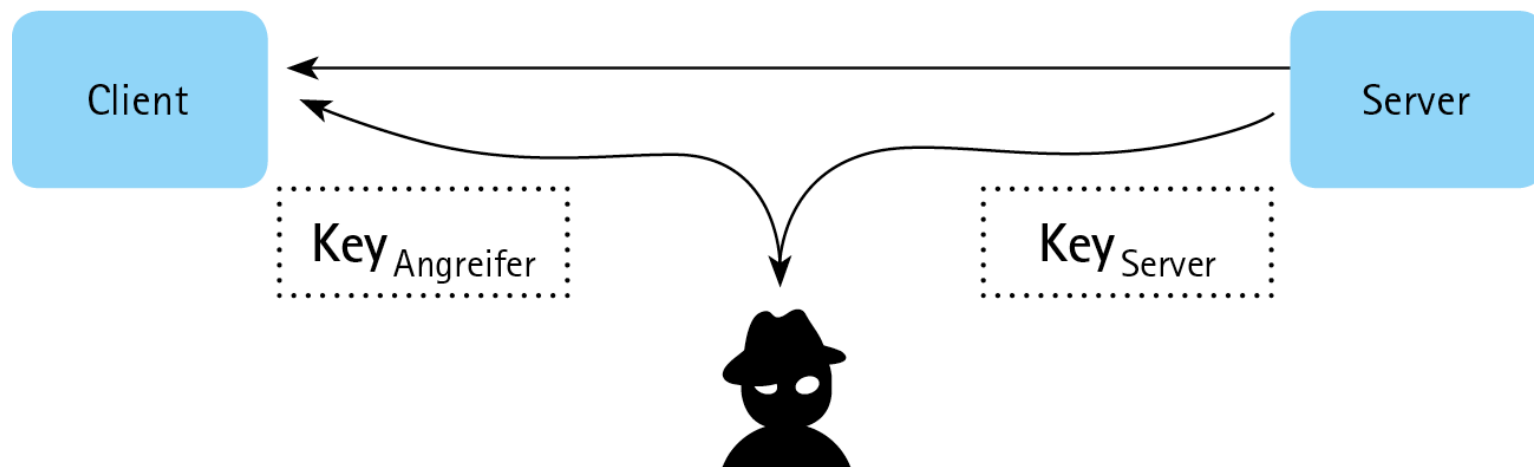
EMIG: Technische Lösung oder reines Marketing?

- Die Frage ist: Wer darf bei EMIG mitmachen?
 - Lange wurden alle anfragenden hingehalten, seit letzter Woche tut sich etwas
- Wird es eine integrative Initiative, die die Sicherheit erhöht und andere ISPs mitmachen läßt?
- Oder wird eine ausschließende Abgrenzung betrieben, um möglichst gut ein (scheinbares) Alleinstellungsmerkmal vermarkten zu können?
- Was ist mit ausländischen Providern?

Warum SSL/TLS aber nicht ausreicht

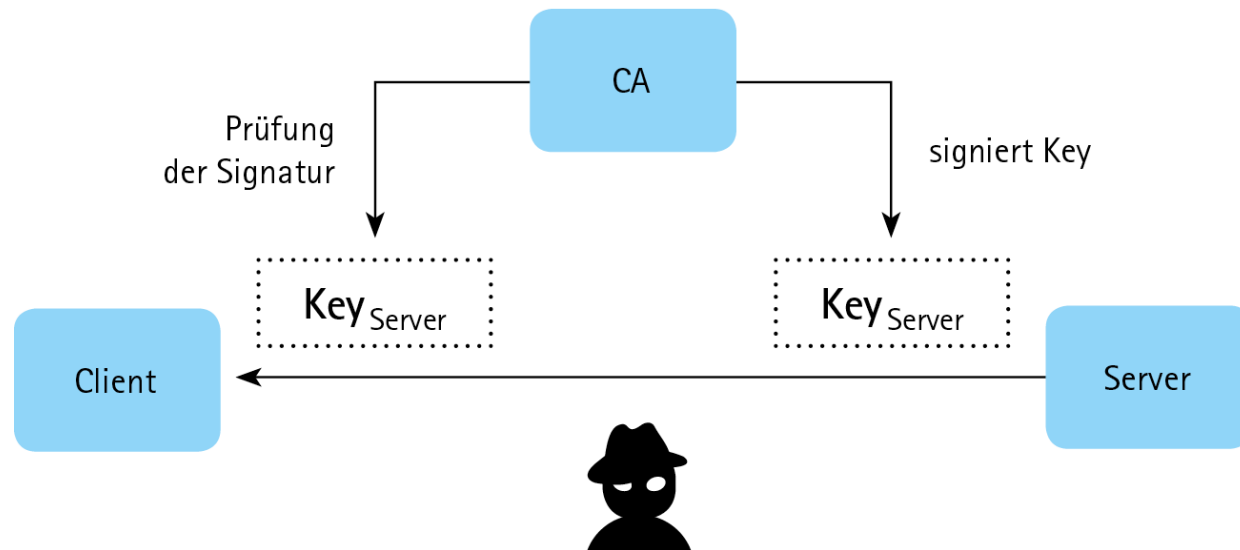
Warum SSL/TLS nicht ausreicht

→ Ein man-in-the-middle könnte das SSL-Zertifikat austauschen.



Warum SSL/TLS nicht ausreicht

→ Darum braucht man eine CA.



→ Welcher CA kann man trauen?

Warum SSL/TLS nicht ausreicht

- Mit welchen Servern rede ich?
 - Über DNS-Poisoning könnten andere MX-Records untergeschoben werden.
 - Kann ich mich ohne DNSsec auf das DNS verlassen?
- Viele Provider haben nur selbstsignierte Zertifikate.
 - Kann man ändern, muß man dann aber auch!
- Was ist, wenn kein SSL/TLS möglich ist? Was ist, wenn der MitM das SSL-Announcement unterdrückt?
 - Dann normalerweise Fallback auf Klartextübertragung
- SSL/TLS ist nur Nexthop-Verschlüsselung. Danach liegt die Mail zunächst wieder im Klartext vor (siehe DE-Mail)
 - Kann man seinem Provider trauen?

Warum SSL/TLS trotzdem sinnvoll und gut ist

- Es schützt vor ungewollten Mitlesern
- Es erhöht den Aufwand für jemanden, der mitlesen will
- Es ist eine selbstverständliche Grundabsicherung
- Das Problem: Es ist halt immer nur optional. Ein MitM kann SSL unterdrücken.
 - Hier eventuell Vorteil von EMIG
 - Dafür gibt es neuerdings jedoch auch DANE TLS
- Rund 40% unserer SMTP-Verbindungen laufen über SSL/TLS
 - Das ist deprimierend. Warum?!

Demnächst kommt DANE TLS

- Wie gesagt: Ein MitM könnte SSL-Announcements unterdrücken
- Die CA könnte unterwandert sein.
- DANE TLS führt neue TLSA-Records ein (TLS association), die definieren, welche Zertifikate der Client akzeptieren darf.
 - Die Zertifikate einer bestimmten CA
 - Bestimmte genannte Zertifikate
 - Zertifikate, die von einem bestimmten Vertrauensanker abstammen
- Der TLSA-Record wird dann für `_25._tcp.example.com` definiert
 - Also individuell pro Dienst/Port

Probleme von DANE TLS

- DNS selbst wäre durch einen MitM leicht angreifbar
 - Die TLSA-Records könnten unterdrückt und ausgetauscht werden
 - Anschließend wäre der Client wieder blind und naiv wie früher
- Also: Absicherung der DNS-Records über DNSsec
 - Theoretisch: Kein Problem. „Muß man nur machen“
 - Praktisch: DNSsec hat sich bis heute nicht flächendeckend durchgesetzt. Zahlreiche Fallstricke, komplexeres Handling der Records, große Sorgfalt notwendig.
 - DANE TLS sorgt im Prinzip für den ersten flächendeckenden Einsatz von DNSsec!
- Problem: Hohe Latenz bei Überprüfung der zahlreichen DNSsec-RR
 - Schwierig bei HTTP, XMPP & Co!

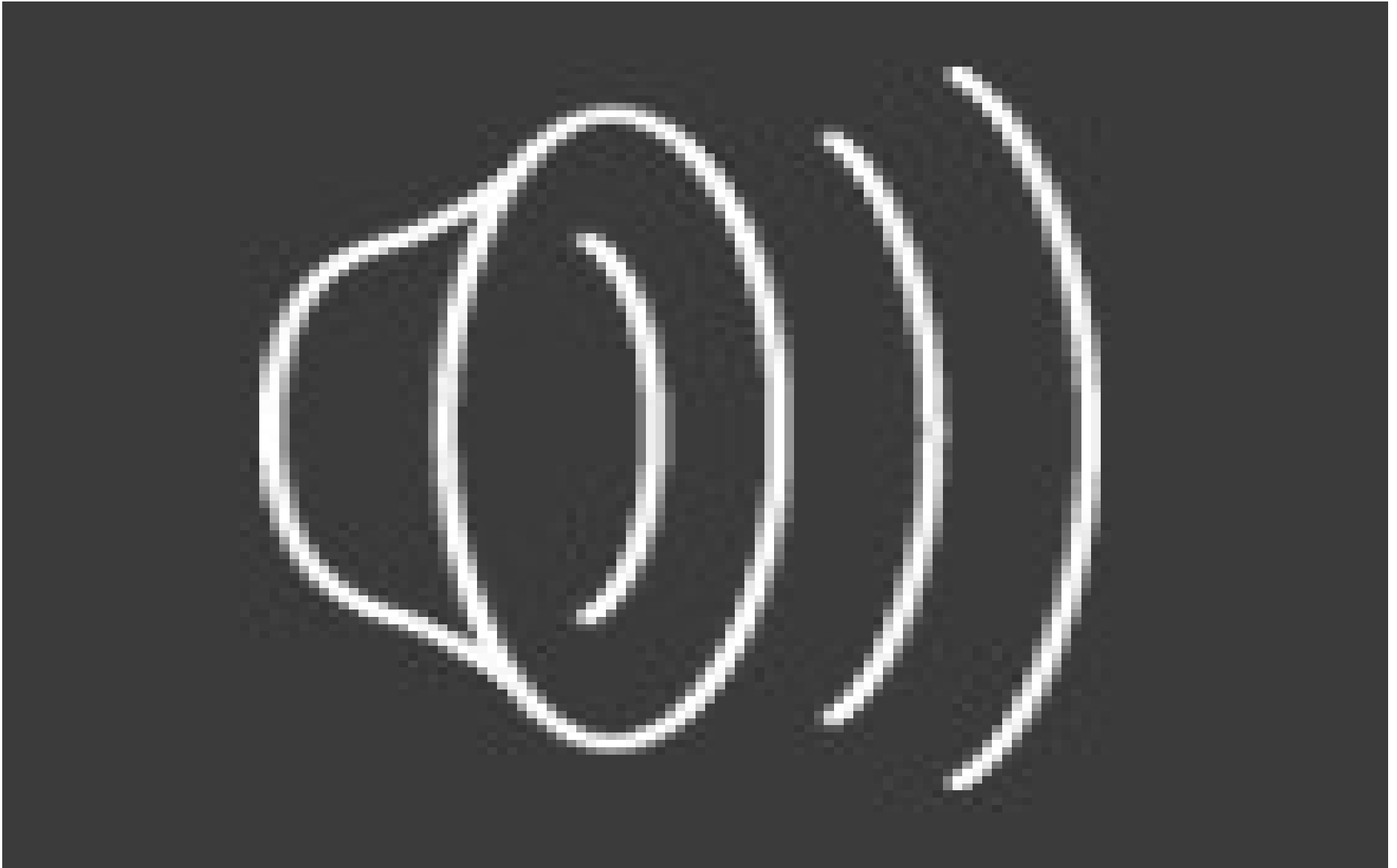
DANE TLS und E-Mail made in Germany

- Wenn DANE TLS eingeführt ist:
Was bringt dann noch EMIG?

Die Alternative:

**Echte Ende-zu-Ende-Verschlüsselung
Mit PGP oder S/MIME**

<http://vimeo.com/86736532>



Möglichkeiten und Grenzen von PGP & S/MIME

- Hier kontrollieren Absender und Empfänger die Ver-/Entschlüsselung
- Auch auf den Servern liegt die E-Mail nur verschlüsselt vor
 - Aber: Meta-Daten (=Mailheader) einer E-Mails bleiben unverschlüsselt: Wer redet mit wem wozu.
- Nötig ist die Kombination mehrerer sich überlagernder Mechanismen:
 - Verschlüsselte E-Mails, die über SSL/TLS-Tunnel transportiert werden

Wer ist wer?

- Das Problem: Man muß auch sicherstellen, daß man den richtigen Schlüssel des Empfängers benutzt. Sonst „man in the middle“-Angriffe möglich..
- Andererseits will man auch anonym kommunizieren können.
- PGP: Gegenseitige Unterschriften, ein „web of trust“, kein einzelner Vertrauensanker
 - Achtung, Sozialprofil: Wer kennt wen?
- S/MIME: Zentrale Zertifizierungsstelle, „anchor of trust“.
 - Ist die vertrauenswürdig?

Unser Projekt: mailbox.org

- Wir bieten spezielle Mailadressen, die definitiv nur per SSL/TLS erreichbar sind. Damit kann ein User durch Auswahl seines Mailaliases steuern, wie versandt werden muß.
 - Sichere Mails nicht nur innerhalb EMIG, sondern mit allen!
- Unsere Domain wird über DNSsec abgesichert
 - Sichere MX-Records!
- Als Provider wollen wir informieren, aufklären und auch erziehen.
 - Wir produzieren Stiffilme, leben die Nutzung von PGP vor und pflegen umfangreiche Dokumentation im Support-Bereich
- mailbox.org kann noch viel mehr, aber das müssen Sie selbst entdecken. :-)

→ Snowden sagte im Guardian Chat:

Starke Verschlüsselung ist das einzige, worauf Sie sich verlassen können.

"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."

→ Zeit, das endlich mal anzugehen.

Darum meine Bitte an Sie

- Nutzen Sie die zur Verfügung stehenden Möglichkeiten.
 - Jeder Baustein trägt zur Absicherung bei.
- Verschlüsselung ist weder kompliziert, noch etwas für Klein- oder Großkriminelle.
 - Verschlüsselung ist aber auch nichts für die Marketing-Abteilung!
- Verschlüsselte sichere Kommunikation ist ein Ausläufer des Menschenrechts auf Gedanken- und Meinungsfreiheit. Dieses Recht dürfen wir uns nicht nehmen lassen.

Mailserver-Consultung seit > 20 Jahren

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich über Feedback!



Peer Heinlein

Mail: p.heinlein@heinlein-support.de

Telefon: 030/40 50 51 - 42

- Wenn's brennt:

Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

Und nun...



- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Schauen Sie doch mal vorbei:
 - <https://mailbox.org>
- Und viel Erfolg an der Tastatur...

Bis bald.

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln in Training und [Schulung](#) die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN CONSULTING

Das Backup für Ihre [Linux-Administration](#): LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN ELEMENTS

Hard- und Software-Appliances für [Archivierung](#), [IMAP](#) und [Anti-Spam](#) und speziell für den Serverbetrieb konzipierte Software rund ums Thema E-Mail.