Sichere E-Mail

Pragmatische Lösungsansätze für die Wirtschaft

31. BremSec Forum

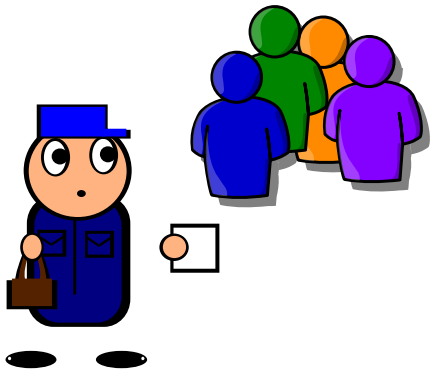
25.09.2013
Robert M. Albrecht
Dr. Matthias Renken

Übersicht

- Wer sollte E-Mails schützen?
- Angriffsmuster auf E-Mails
- Lösungsansätze
- Was brauchen Sie?

E-Mail ist von Haus aus unsicher

- Wir wissen: E-Mail ist offen wie eine Postkarte.
- Reaktion:
  - „Ich habe nichts zu verbergen.“
  - „Wir haben keine sensiblen Daten.“
  - „Wir verschicken keine Kundendaten per Mail.“
  - „Wir haben einen eigenen Mail-Server.“
  - „Wer sollte uns schon ausspionieren?“

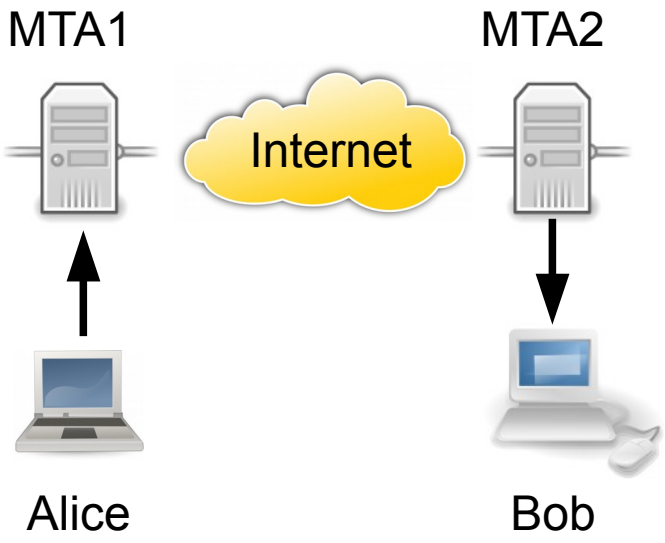


Wer sollte E-Mails schützen?

- Sensible Daten sind
  - Personenbezogene (BDSG, besonders §3(9))
  - Firmeninterna
- E-Mails werden seit Jahren in großem Umfang abgefangen und ausgewertet.
- Persönliche Kompromittierung und Industriespionage sind möglich.
- Seit Prism, Tempora etc. kann dies keiner mehr leugnen.

Angriffsmuster E-Mail

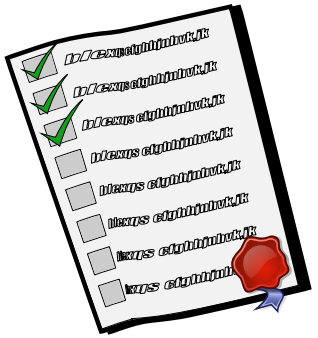
- Auf dem Weg zwischen Sender und Empfänger durchläuft eine E-Mail viele Zwischenstationen
- Mögliche Agriffsziele:
  - Userclient
  - Verbindung User-MTA
  - Verbindung MTA1-MTA2
  - MTA-Server selbst



→ Zu Sichern sind:
- Client
- Übertragungsweg
- Mail-Server

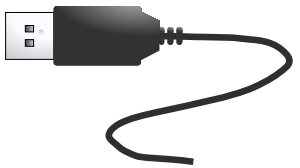
Lösungsansatz 1- Policy

- Rein organisatorischer Ansatz
- Festlegen einer E-Mail Policy
  - Wer darf wann was an wen per Mail verschicken?
- Voraussetzung ist vorherige Datenklassifikation
- Möglichkeiten zur Kontrolle der Policy einplanen
- Keine Investitionen in Hard- oder Software notwendig.



Lösungsansatz 2- TLS

- Umstellen der Postausgangs- und Eingangsserver auf TLS
- Einfachste technische Lösung
- Verursacht i.d.R. keine Kosten.
- Für den Nutzer vollkommen transparent.
- E-Mail Provider muss dieses Verfahren beherrschen.
- Sichert nur den Übertragungsweg.



Lösungsansatz 3 - Dateiverschlüsselung

- Sensible Daten werden in einem separaten Dokument gespeichert
- Dokument wird verschlüsselt und als Anhang versendet.
- Zwischen Sender und Empfänger muss ein Passwort vereinbart werden.
- Freeware wie 7-Zip kann eingesetzt werden.
- Sichere Ende-zu-Ende Verschlüsselung.
- Geeignet für kleinere Nutzergruppen.

Lösungsansatz 4 - Webmail

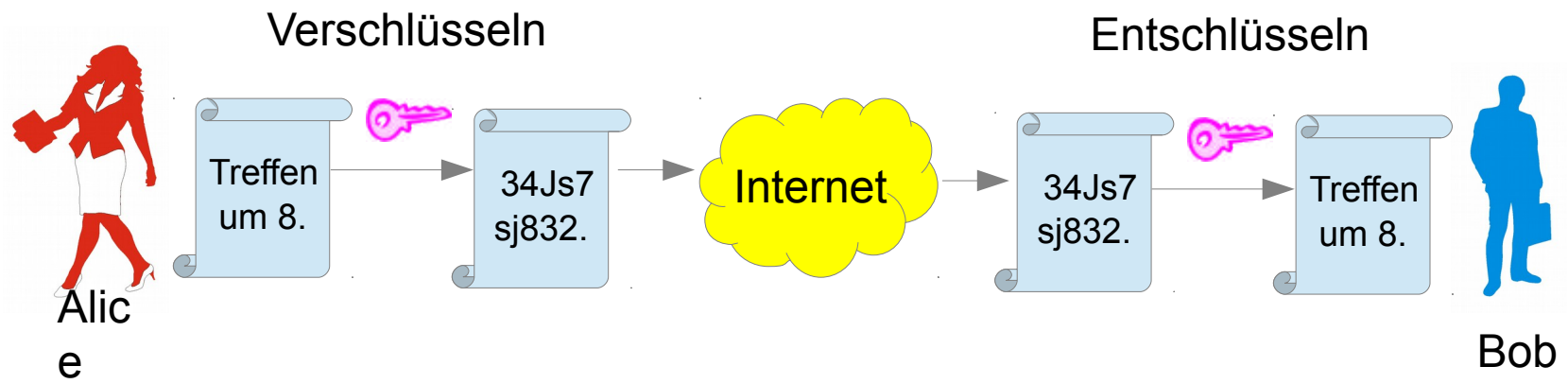
- Ein eigener Webmail-Server wird betrieben.
- Zugang ist nur über https erlaubt.
- Transportweg und Server sind unter eigener Kontrolle.
- Verwendbar für kleinere und mittlere Gruppen.
- Es muss kein Schlüssel vorab ausgetauscht werden.
- Geeignet für alle Endgeräte mit Internetbrowser.
- Investitionen in eigenen Mail-Server erforderlich.

Lösungsansatz 5 - De-Mail

- Das Gesetz reguliert die Zulassung und die Arbeit so genannter De-Mail-Diensteanbieter, das heißt der Anbieter von „Diensten auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen“, § 1 Abs. 1 De-Mail-Gesetz vom vom 28.4.2011
- Webbasierte Anwendung im Internet
- Deutscher Alleingang, international nicht brauchbar
- Betreiber kann Inhalte lesen, aber eine zusätzliche Ende2Ende-Verschlüsselung der Benutzer ist ausdrücklich erlaubt und wird technisch nicht behindert.
- Anbieter: Deutsche Telekom, 1und1 (GMX), ...

Exkurs: Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird für die Ver- und Entschlüsselung der gleiche Schlüssel verwendet.



Problem: Schlüsselverteilung bei mehreren Anwendern

Exkurs: Asymmetrische Verschlüsselung

- Für die Ver- und Entschlüsselung werden unterschiedliche Schlüssel verwendet.
- Jeder Nutzer benötigt dafür ein Schlüsselpaar

Alic
e

p

Privater Schlüssel (private key)

o

Öffentlicher Schlüssel (public key)

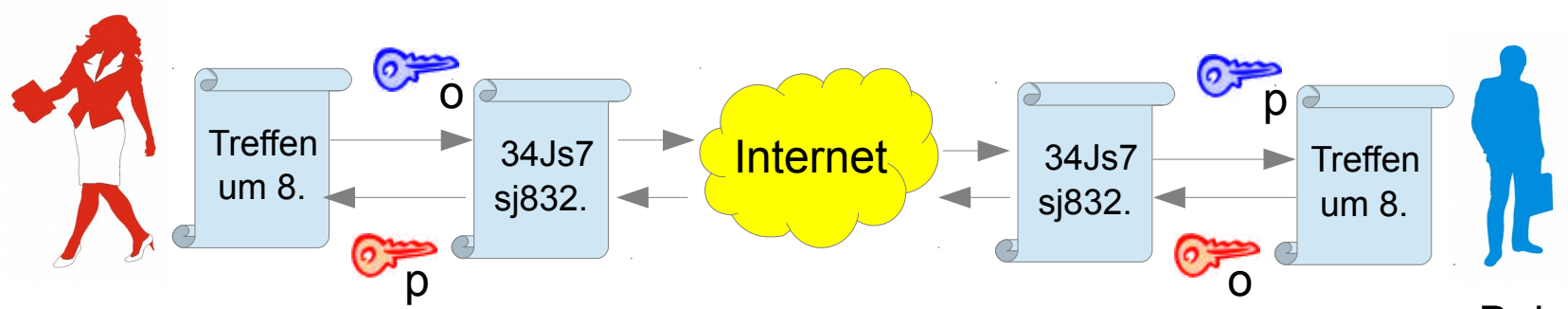
p

o

Bob

Exkurs: Asymmetrische Verschlüsselung

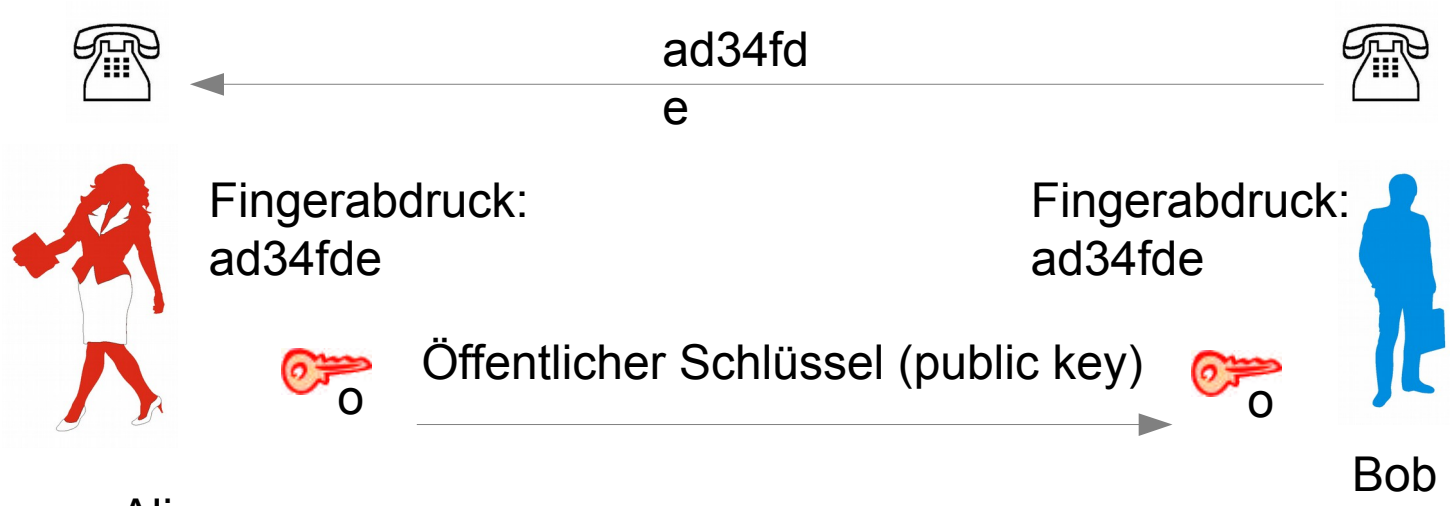
Zum Verschlüsseln wird der öffentliche Schlüssel des Empfängers genutzt, zum Entschlüsseln der private.



Kein Problem bei der Schlüsselverteilung, aber woher weiß Bob, dass er wirklich Alices Schlüssel benutzt?

Exkurs: Fingerabdruckprüfung

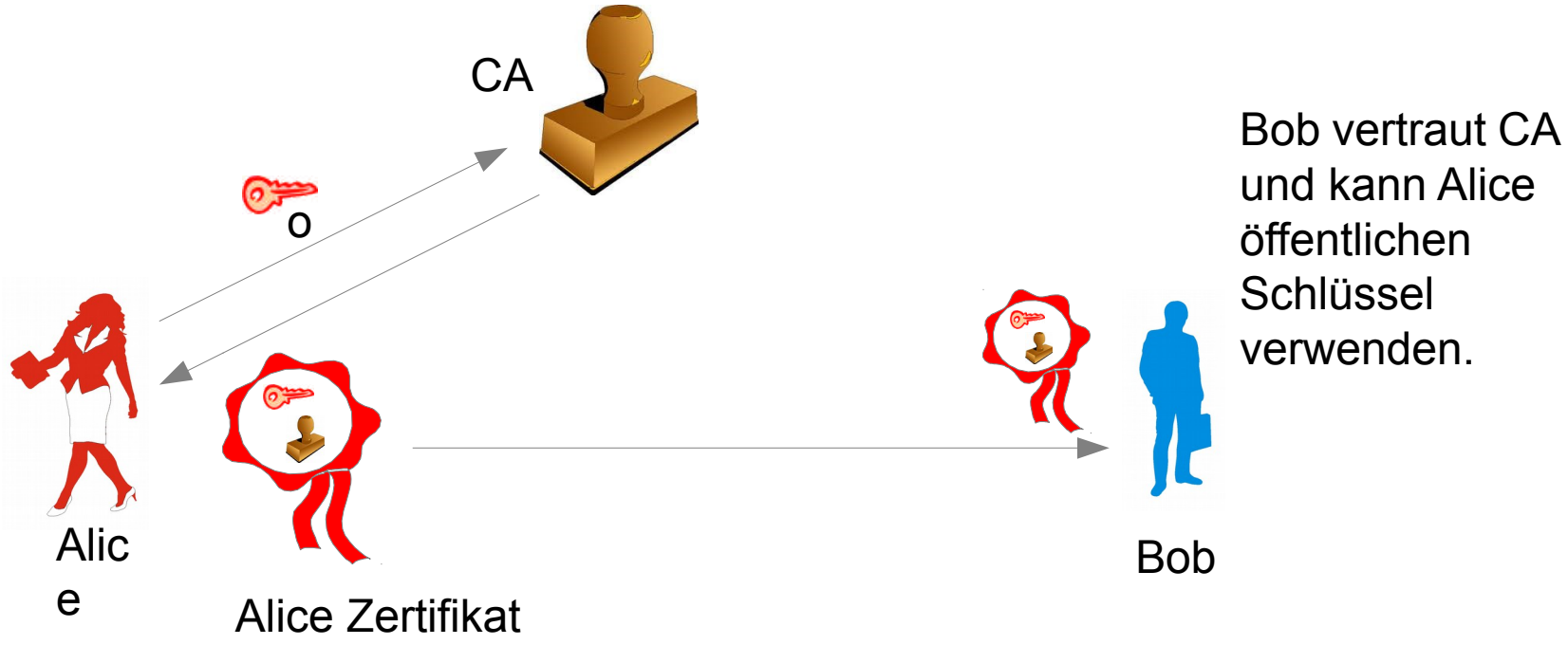
- Jedem Schlüssel ist ein eindeutiger Fingerabdruck (fingerprint) zugeordnet, der z.B. über Telefon geprüft werden kann.



Leider unpraktisch bei vielen und unbekannten Kontakten.

Exkurs: Public-Key-Infrastructure (PKI)

- Certification Authorities (CA) sind „Passämter“ für Schlüssel.
- Macht aus einem öffentlichen Schlüssel ein Zertifikat.

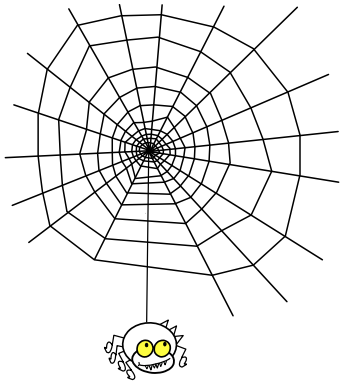


Bob vertraut CA und kann Alice öffentlichen Schlüssel verwenden.

Bekannte CA sind VerySign, Thawte, Teletrust

Lösungsansatz 5 – PGP/GPG

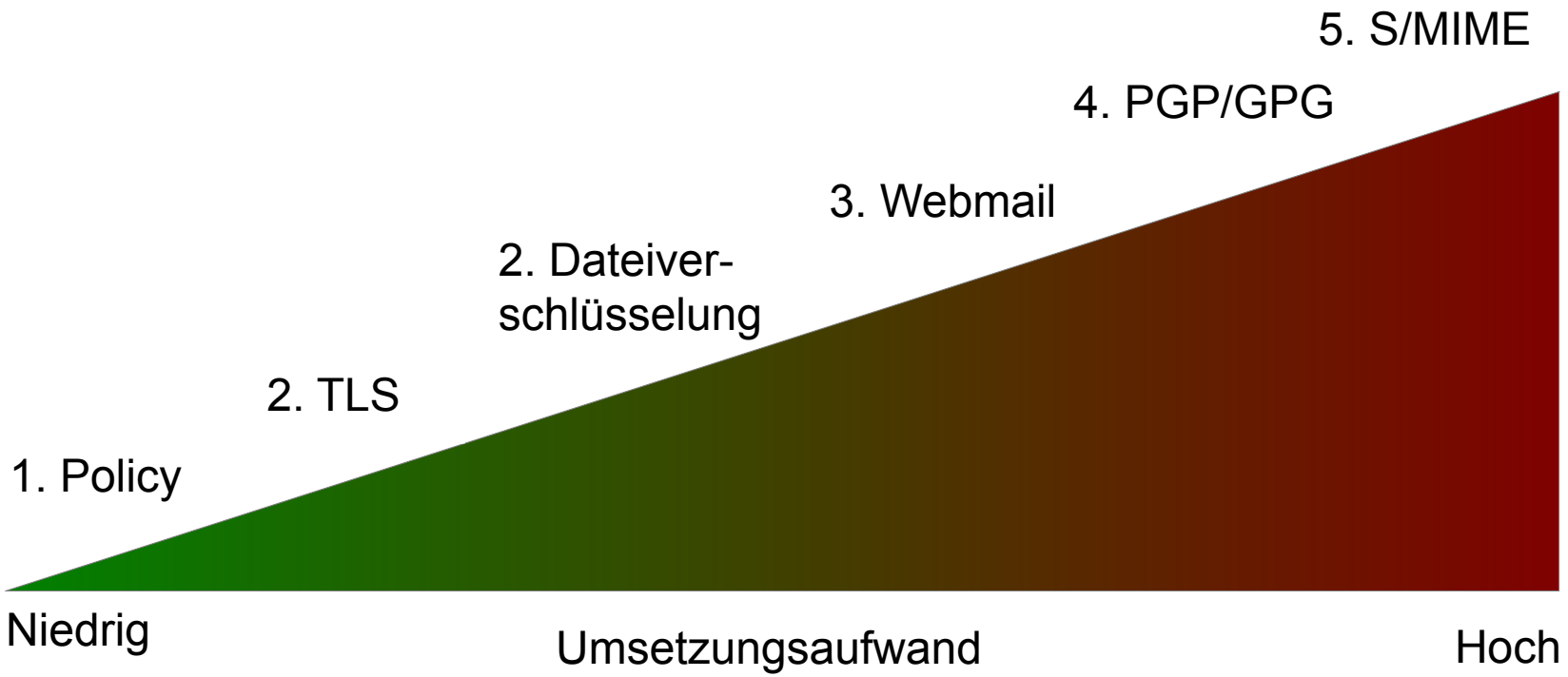
- Asymmetrisches Verfahren, basiert auf Fingerabdruckprüfung und Web of Trust.
- PGP (Pretty-good-Privacy, kostenpflichtig) und freie Alternativen wie GPG (Gnu Privacy Guard)
- Sichere Ende-zu-Ende Verschlüsselung
- Benötigt PGP Installation und Plugin für verwendete E-Mail Clients.
- Für jeden Nutzer muss ein Schlüsselpaar generiert und verwaltet werden.



Lösungsansatz 6 – S/MIME

- Asymmetrisches Verfahren, basiert auf Public-Key-Infrastructure
- Sichere Ende-zu-Ende Verschlüsselung
- Keine separate Software auf den Clients erforderlich, jedes gängige Mail-Programm beherrscht das Verfahren.
- Für jeden Nutzer muss ein Schlüsselpaar generiert und verwaltet werden.
- Aufbau oder Nutzung einer PKI erforderlich.
- Transparente Anwendung
- Für mittlere bis größere Unternehmen geeignet.

Lösungsansätze im Vergleich



Was brauchen Sie?

- In welchem Umfang wird E-Mail für vertrauliche Daten heute eingesetzt?
- Welche Verfahren setzen Sie ein?
- Was benötigen Sie, um besser zu werden?

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:
Robert M. Albrecht
robert.albrecht@pmbremen.de

Dr. Matthias Renken
matthias.renken@pmbremen.de