Veranstaltungsreihe

Ich hab' doch nichts zu verbergen...
Der gläserne Bürger: Wieviel Daten braucht der Staat?

15. Mai bis 3. Juli 2008

Veranstalter sind:

- der Arbeitskreis Vorratsdatenspeicherung Göttingen
- der Chaostreff Göttingen
- die Basisgruppe Jura an der Georg-August-Universität Göttingen

Sicheres E-Mailen

Damit der Briefträger nicht mitliest: verschlüsseln und signieren, GnuPG, S/MIME, Thunderbird Enigmail

Stefan Teusch

Chaostreff Göttingen

29. Mai 2008, Göttingen

Inhalt

Gliederung

Brief

Ein Brief ist ein Blatt Papier mit:

- Empfängeradresse
- Absenderadresse
- Ort, Datum und Betreffzeile
- Anrede
- Inhalt: Text, Bilder etc.
- Unterschrift

Auf dem Umschlag findet sich:

- Empfängeradresse
- Absenderadresse
- Briefmarke mit Poststempel

E-Mail

E-Mail

Eine **E-Mail** ist ein elektronischer Text, der von einem Absender-Rechner zu einem Empfänger-Rechner gesendet wird.

Der Aufbau orientiert sich am physischen Brief, aber:

- Umschlag und Inhalt sind (ASCII-)Texte
- Umschlag existiert nur während des Transports

$\Rightarrow$ Der Schutz für den Inhalt fehlt!

E-Mail

E-Mail

Eine **E-Mail** ist ein elektronischer Text, der von einem Absender-Rechner zu einem Empfänger-Rechner gesendet wird.

Der Aufbau orientiert sich am physischen Brief, aber:

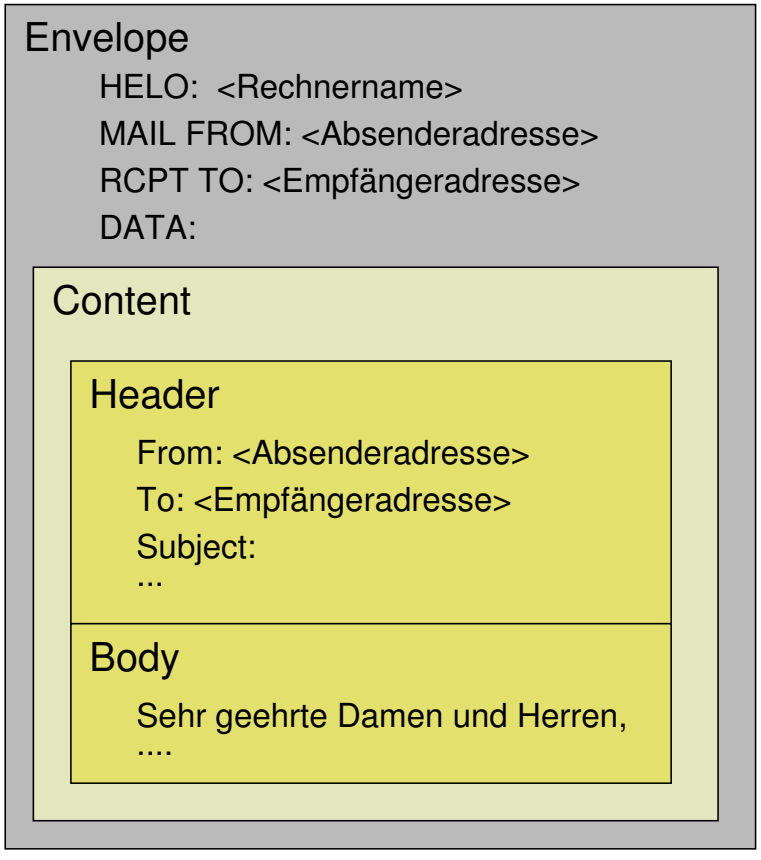
- Umschlag und Inhalt sind (ASCII-)Texte
- Umschlag existiert nur während des Transports

$\Rightarrow$ Der Schutz für den Inhalt fehlt!

Behauptung:

Eine E-Mail ist eine elektronische Version einer Postkarte (mit Absenderadresse).

Aufbau einer E-Mail



Umschlag (Envelope) mit

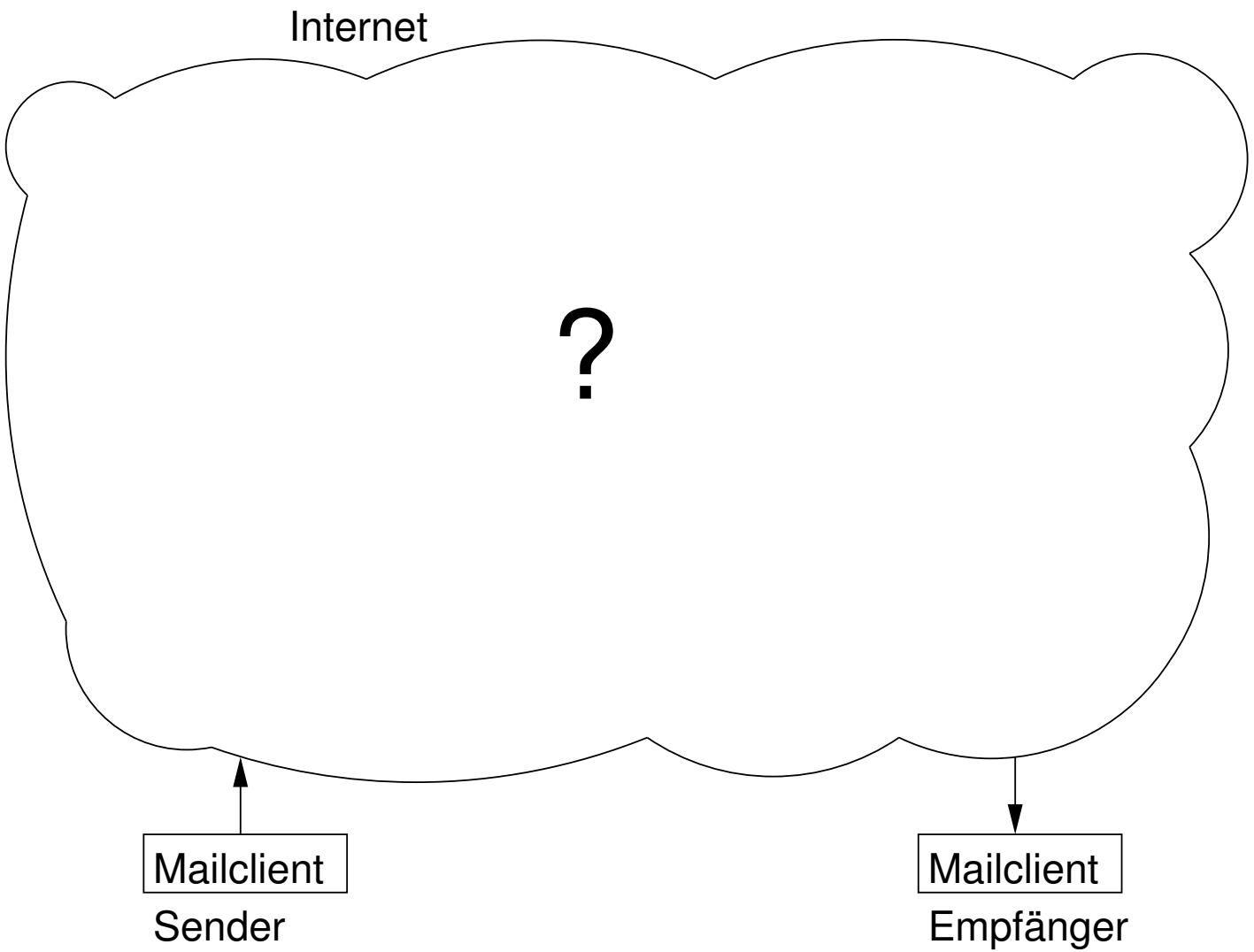
- Transportinformation

Inhalt (Content)

- Briefkopf (Header)
  - Transportprotokoll mit Zeitstempeln
  - Angabe Absender und Empfänger
  - Betreffzeile (Subject)
- Brief (Body)
  - Text der Mail
  - Anhänge, z.B. ein Bild

Gliederung

Mysterium



E-Mail-Protokolle

Protokoll

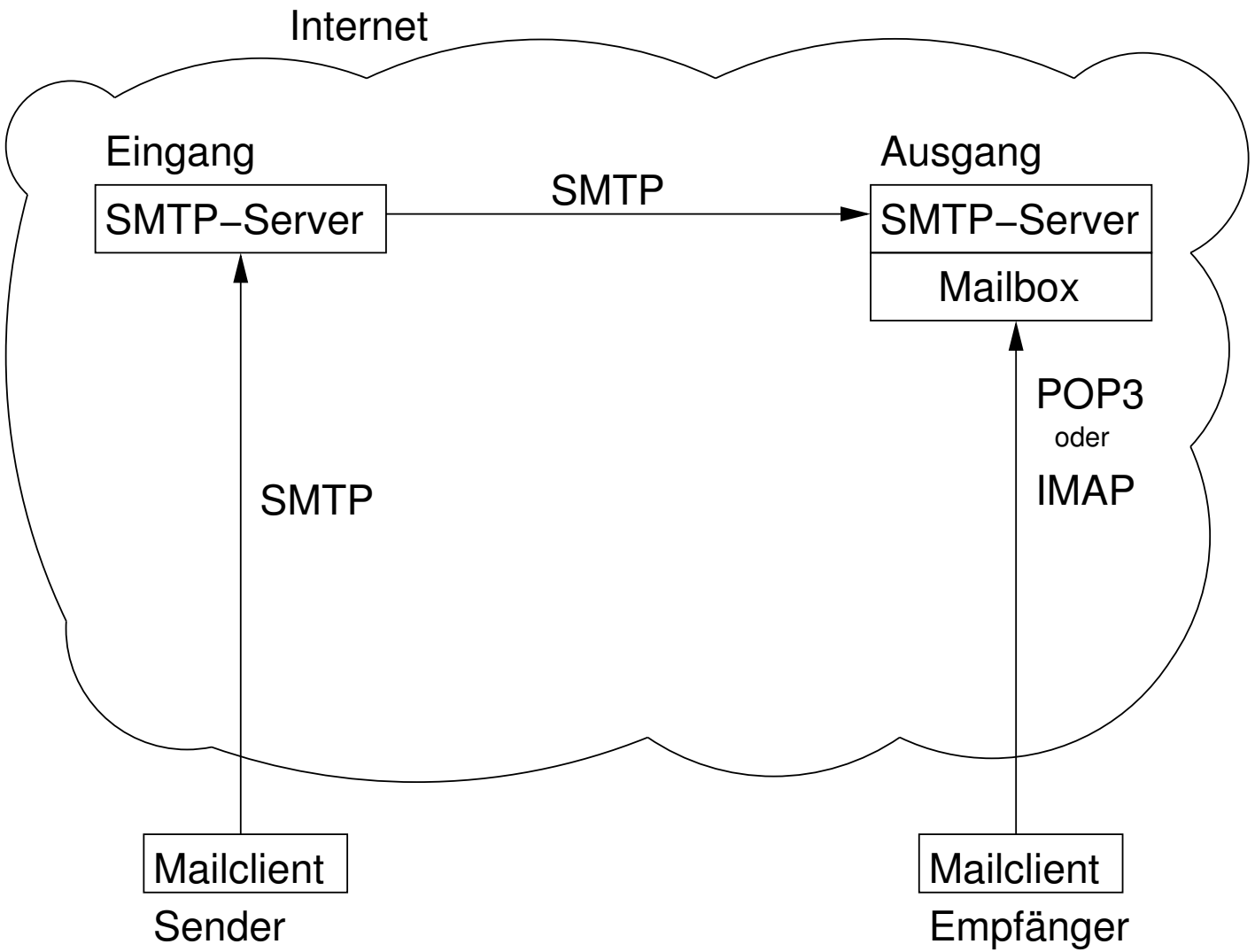
Ein **Protokoll** ist ein Regelwerk, das die Kommunikation zwischen Rechner beschreibt.

- E-Mail senden:
  - SMTP (Simple Mail Transfer Protocol)
- E-Mail empfangen:
  - POP3 (Postoffice Protocol Version 3)
  - IMAP (Internet Message Access Protocol)

Der Weg vom Sender zum Empfänger

1. E-Mail wird auf einem E-Mail-Klienten geschrieben
2. Übergabe der E-Mail an den SMTP-Server
3. Transport von einen SMTP-Server zum anderen
4. Einordnung der Mail in die “Mailbox” (Postfach) des Empfängers
5. Abruf der Mail durch den Empfänger mittels
   - POP3: Download der E-Mail auf den (heimischen) PC
   - IMAP: Verwaltung der E-Mail auf dem Server

Applikationsschicht

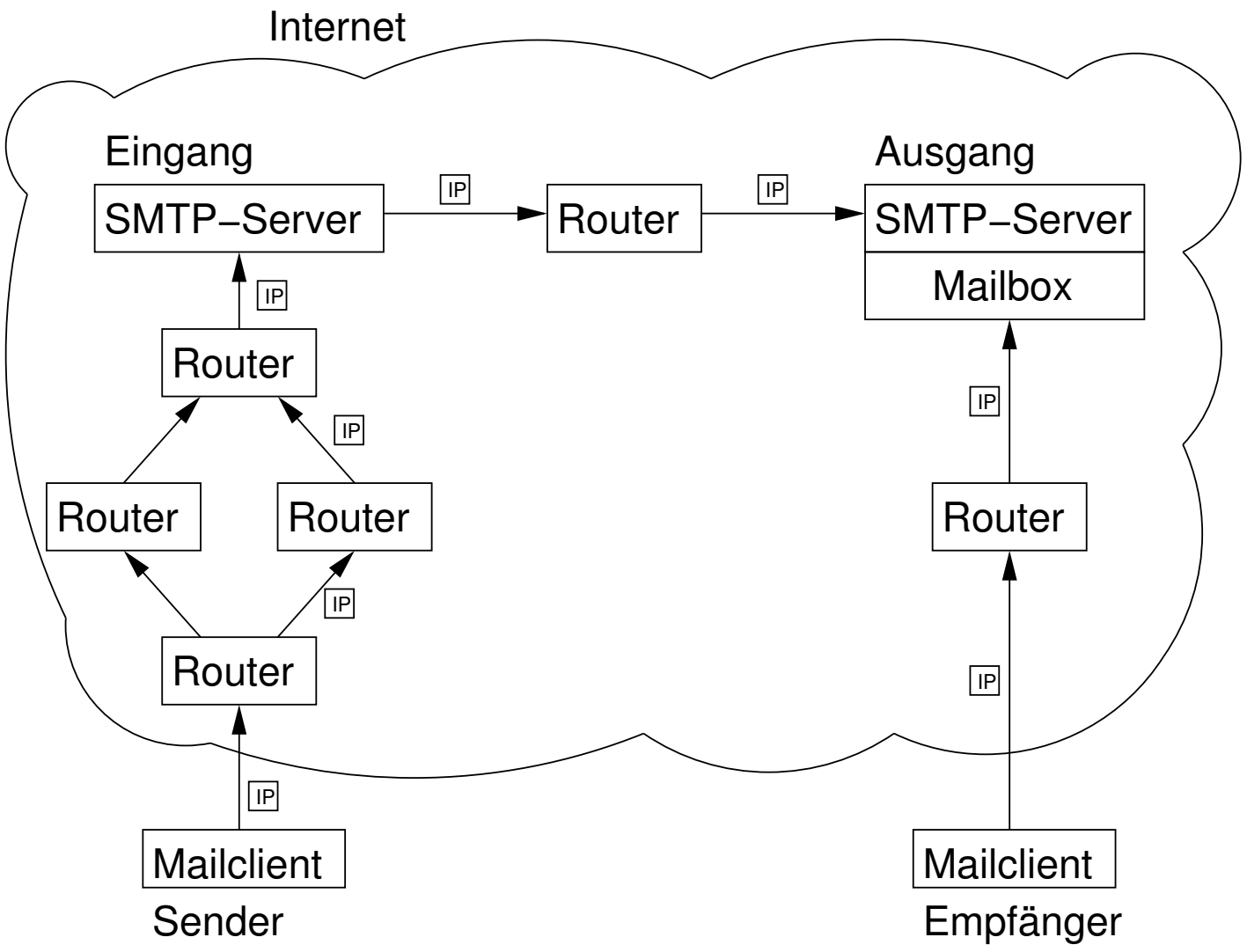


Vermittlung der E-Mail mittels IP

IP (Internet Protocol)

- Paketorientierte Vermittlung von Daten
- Sender und Empfänger werden über IP-Adressen identifiziert
- Wegewahl und Weiterleitung erfolgt durch Router
- Kein vorgeschriebener Weg der IP-Pakete

Vermittlungsschicht



Gefahren

Für die Transportstationen (Router, SMTP-Server, Mailbox) gilt:

- E-Mail ist lesbar und damit kopierbar
- E-Mail ist veränderbar
- E-Mail ist fälschbar
- Zugangsdaten des Mailabrufs sind abgreifbar
- Kommunikationspartner (Mail-Adressen) sind erkennbar
- Kommunikationspartner (IP-Adressen) sind erkennbar

Gefahren

Für die Transportstationen (Router, SMTP-Server, Mailbox) gilt:

- E-Mail ist lesbar und damit kopierbar
- E-Mail ist veränderbar
- E-Mail ist fälschbar
- Zugangsdaten des Mailabrufs sind abgreifbar
- Kommunikationspartner (Mail-Adressen) sind erkennbar
- Kommunikationspartner (IP-Adressen) sind erkennbar

Hinweis

IP kennt keine vorgeschriebenen Wege, d.h. der Transport über die EU ist möglich.

Möglichkeiten der Gefahrenabwehr

Die E-Mail und ihr Transport kann geschützt werden durch:

1. Verschlüsselung der Protokolle SMTP, POP3 und IMAP
2. Verschlüsselung der E-Mail selbst
3. Digitale Signatur

Möglichkeiten der Gefahrenabwehr

Die E-Mail und ihr Transport kann geschützt werden durch:

1. Verschlüsselung der Protokolle SMTP, POP3 und IMAP
2. Verschlüsselung der E-Mail selbst
3. Digitale Signatur

Achtung

Verschlüsselung bietet keine Möglichkeit Verbindungsdaten, deren Protokollierung und deren Speicherung zu vermeiden!

Gliederung

Verschlüsselung

Asymmetrische Verschlüsselung besteht aus einen Schlüsselpaar:

- Private Schlüssel bleibt unter Verschluss
- Öffentliche Schlüssel erhält Kommunikationspartner

	Öffentliche Schlüssel	**Private Schlüssel**
Absender	Verschlüsseln	-
Empfänger	-	Entschlüsseln

Signaturen

Signatur

Eine **Signatur** ist eine digitale Unterschrift zur Prüfung:

- der Identität des Absenders (Authentifizierung)
- auf evtl. Modifikationen der E-Mail (Integrität)

	Öffentliche Schlüssel	**Private Schlüssel**
Absender	-	Signieren
Empfänger	Signatur püfen	-

Beglaubigungsverfahren

1. Vergleich des Fingerabdrucks
2. Beglaubigungsverfahren (Zertifizierungen)

Beglaubigung

Der öffentliche Schlüssel wird durch einen vertrauenswürdigen Dritten signiert. Dieser Dritte "verbürgt" sich für die Identität des Schlüsselinhalbers.

Prinzipielle Möglichkeiten:

- Hierarchische Struktur mit einer obersten Zertifizierungsstelle.
- "Jeder signiert jeden." $\Rightarrow$ Netz des Vertrauens *(Web of Trust)*

(X.509-)Zertifikatsbasierte Verschlüsselung

X.509 ist ein “Verpackungs”-Standard für einen öffentlichen Schlüssel

- Eigentümer erstellt ein Schlüsselpaar
- Zertifikat ist ein durch eine Zertifizierungstelle beglaubigter öffentliche Schlüssel mit zusätzlichen Informationen
  - Zertifizierung ist i. A. kostenpflichtig
  - CAcert (`http://www.cacert.org`) ist eine freie Zertifizierungsstelle
- Verwendung für Computer und Personen
- E-Mailerweiterung: S/MIME (Secure/Multipurpose Internet Mail Extensions)

OpenPGP

OpenPGP (Pretty Good Privacy) und GnuPG

- Internet-Standard für Verschlüsselungs-Software
- Verwendung von asymmetrischen Verschlüsselungsverfahren
- Implementiert als GnuPG (Open Source)
- Freie Benutzung: Jeder darf und kann ein eigenes Schlüsselpaar erstellen
- Verwendet ein *Web of Trust*
- Verteilung der Schlüssel über Keyserver

Gliederung

Verschlüsselung der Protokolle SMTP, POP3 und IMAP

- Verschlüsselung der Protokolle (SMTP, POP3, IMAP) mittels:
  - SSL (Secure Socket Layer)
  - TLS (Transport Layer Security)
- Verhindert Mitlesen und Manipulationen der Mail ausschließlich während des Transports zum STMP-Server bzw. von der Mailbox
- Wichtiger: Mitlesen der Zugangsdaten während des Transports

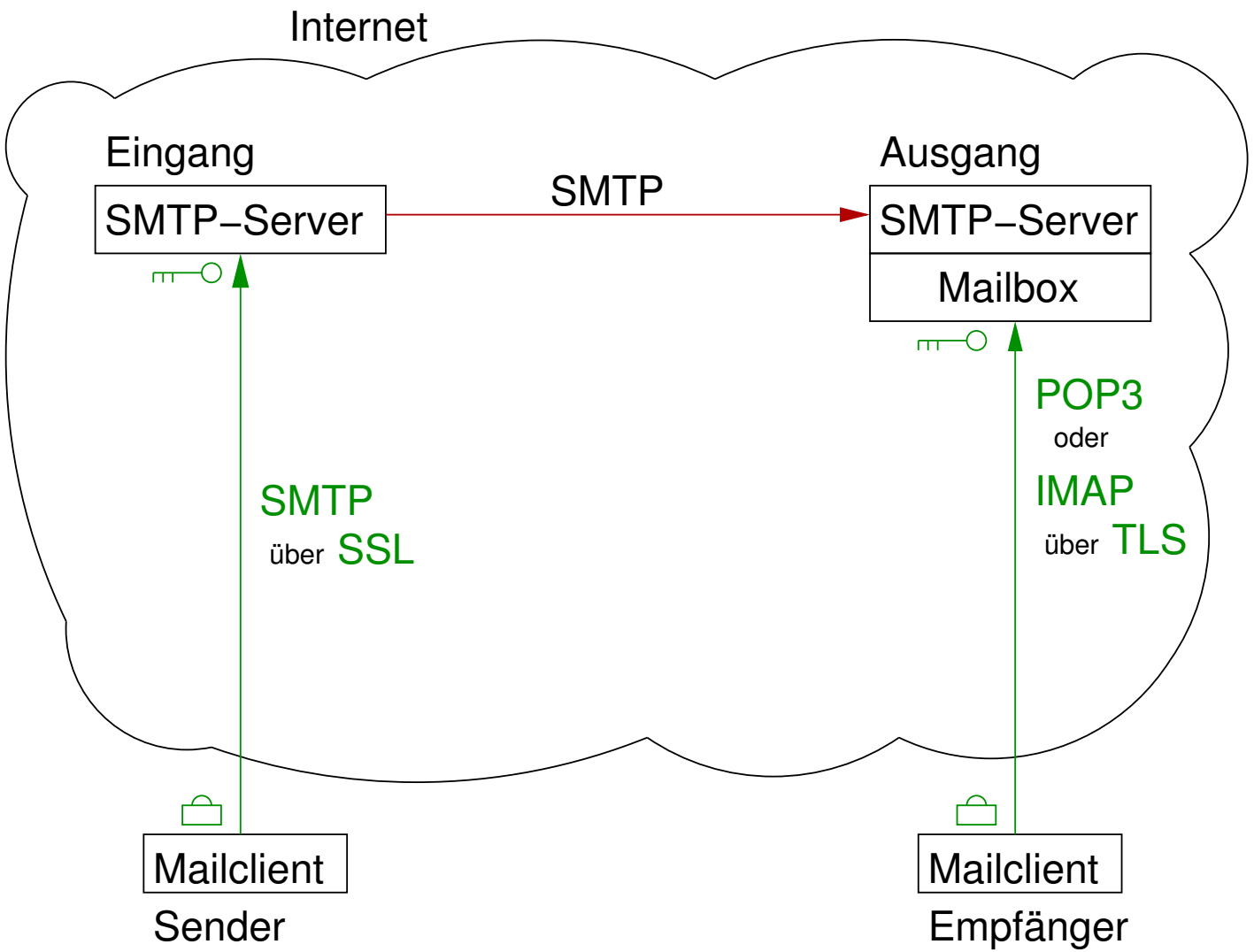
Verschlüsselung der Protokolle SMTP, POP3 und IMAP

- Verschlüsselung der Protokolle (SMTP, POP3, IMAP) mittels:
  - SSL (Secure Socket Layer)
  - TLS (Transport Layer Security)
- Verhindert Mitlesen und Manipulationen der Mail ausschließlich während des Transports zum STMP-Server bzw. von der Mailbox
- Wichtiger: Mitlesen der Zugangsdaten während des Transports

Achtung

- Während des Aufenthalts auf dem SMTP-Server oder der Mailbox ist die Mail nicht geschützt
- Die Protokolle (SMTP, POP3, IMAP) und die Verbindungspartner (IP-Adressen) sind erkennbar.

Applikationschicht: SMTPs, POP3s und IMAPs



Verschlüsselung von E-Mail

Durch Verschlüsseln bzw. Signieren von E-Mail wird

- Inhalt geschützt (Vertrautheit oder Intimität)
- Absender durch Signatur verifiziert (Authentizität)
- Modifikation des Inhalts ausgeschlossen (Integrität)
  - Eine Veränderung kann festgestellt werden, aber nicht was geändert wurde.

Verschlüsselung von E-Mail

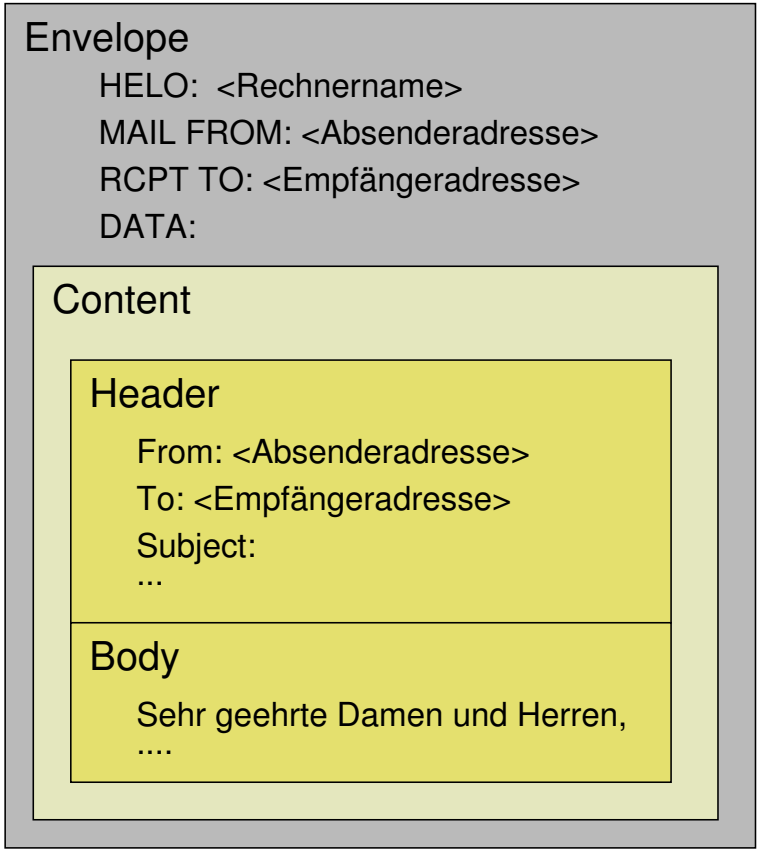
Durch Verschlüsseln bzw. Signieren von E-Mail wird

- Inhalt geschützt (Vertrautheit oder Intimität)
- Absender durch Signatur verifiziert (Authentizität)
- Modifikation des Inhalts ausgeschlossen (Integrität)
  - Eine Veränderung kann festgestellt werden, aber nicht was geändert wurde.

Achtung

Verschlüsselung schützt nur den Inhalt (Body) der E-Mail; nicht den Header (inkl. Subject, Empfänger- und Absenderadresse). Anhänge sind i. A. separat zu verschlüsseln!

Nicht-verschlüsselte Anteile der E-Mail



- Umschlag (Envelope) muss für die Mailzustellung lesbar sein
- Briefkopf (Header)
  - "Transportprotokoll wird durch Mailserver erweitert, d. h. muss veränderbar sein"
  - Absender, Empfänger, Subject sind damit ungeschützt
- Brief (Body)
  - Text wird verschlüsselt
  - Anhänge werden anschließend angehängt

Gliederung

Demonstration

Die verwendeten Programme:

- Thunderbird (`http://www.mozilla-europe.org/de/products/thunderbird/`)
- Enigmail (`http://enigmail.mozdev.org/home/index.php`)
- GnuPG (`http://www.gnupg.org/`)
- S/MIME (Funktion ist im Thunderbird integriert.)

Gliederung

Fazit zur Diskussion

Verschlüsseln und signieren

- schützt den Inhalt.
- authentifizieren den Absender.
- kann Modifikationen erkennen.

Verbleibende Probleme:

- Verschlüsselung ist aufwendig und muss konsequent betrieben werden.
- Mailverschlüsselung funktioniert nicht einseitig.
- Es werden nicht alle Bestandteile der E-Mail verschlüsselt.
- IP-Adressen sind erkennbar.
- Mailserver protokollieren Verbindungen.

Vielen Dank.