Kryptografische Verfahren für sichere E-Mail

Roadshow Sicheres Internet

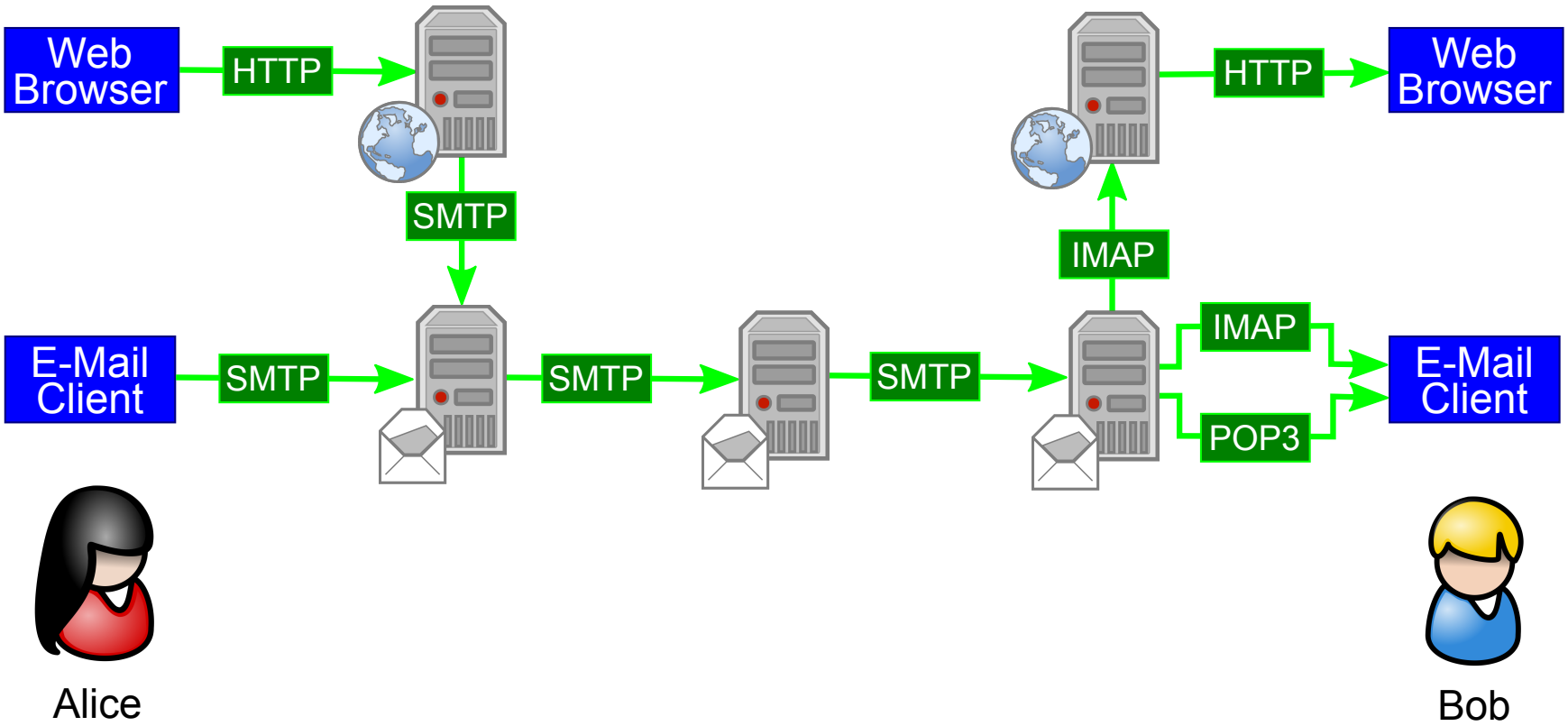
Prof. Dr. Christoph Karg

Hochschule Aalen
Studiengang Informatik

28. November 2013

E-Mail Kommunikation

E-Mail Kommunikation – Technische Sichtweise



Sichere E-Mail

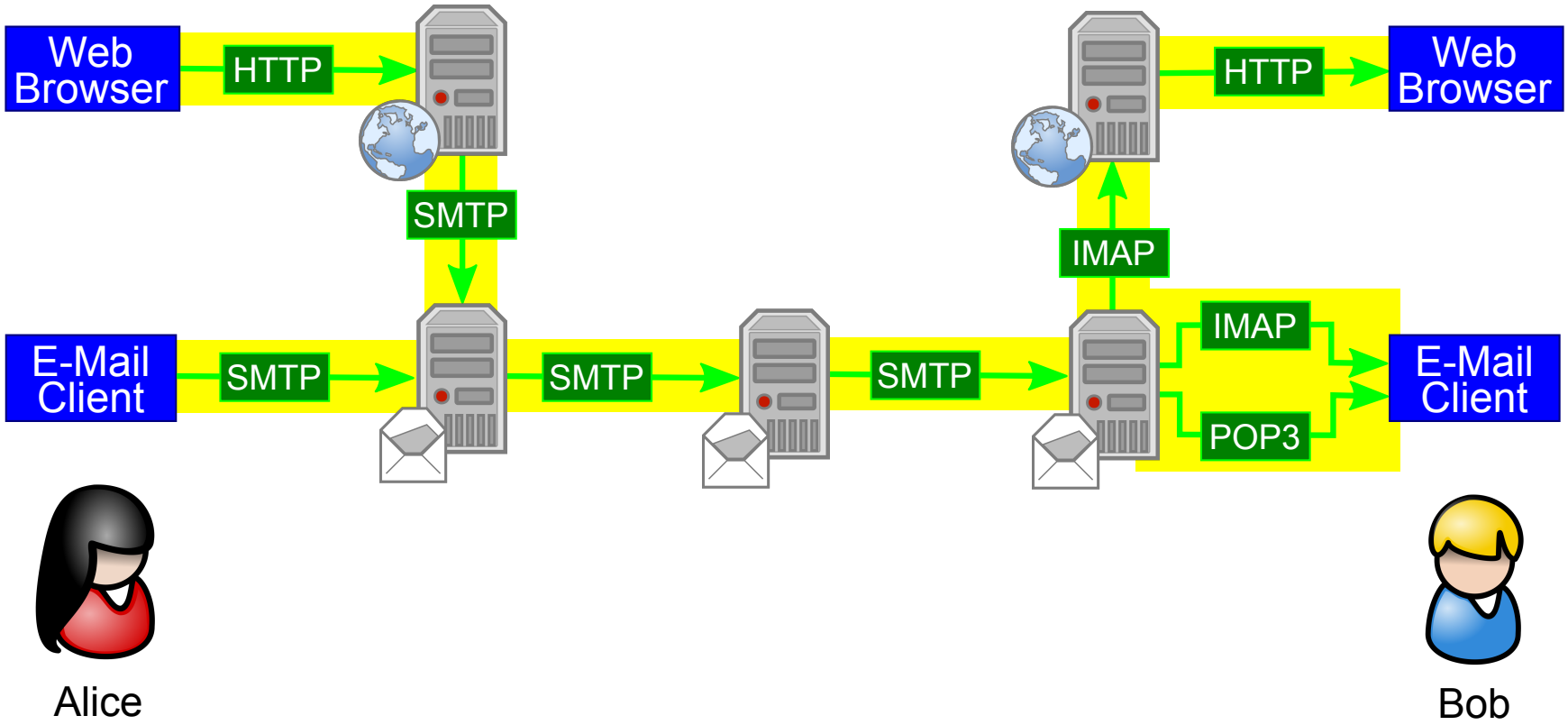
Anforderungen:

- Vertraulichkeit
- Authentizität & Integrität
- Verbindlichkeit

Zu untersuchende Aspekte:

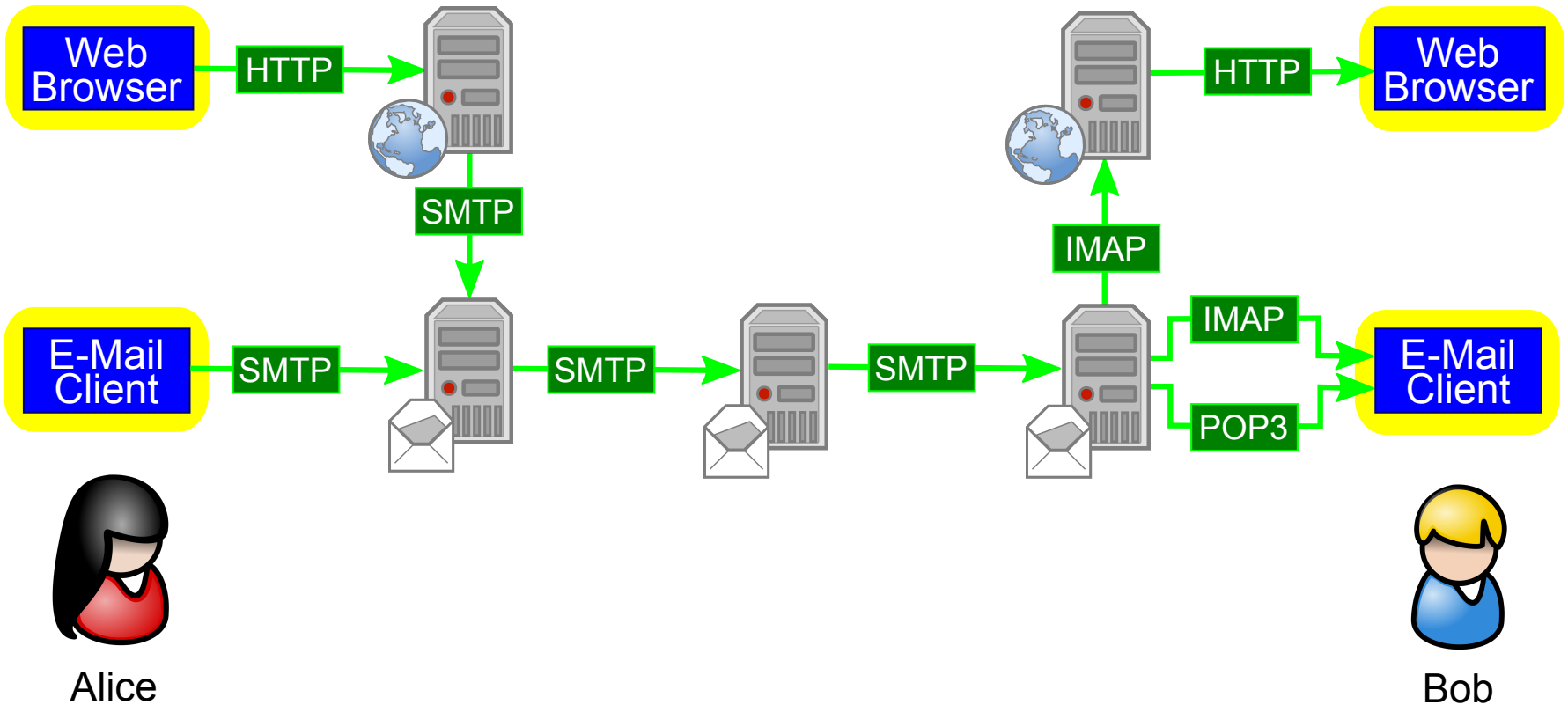
- Übertragung einer E-Mail
- Zugriff auf eine E-Mail
- Speicherung/Archivierung einer E-Mail
- Ende-zu-Ende-Sicherheit

Übertragung einer E-Mail



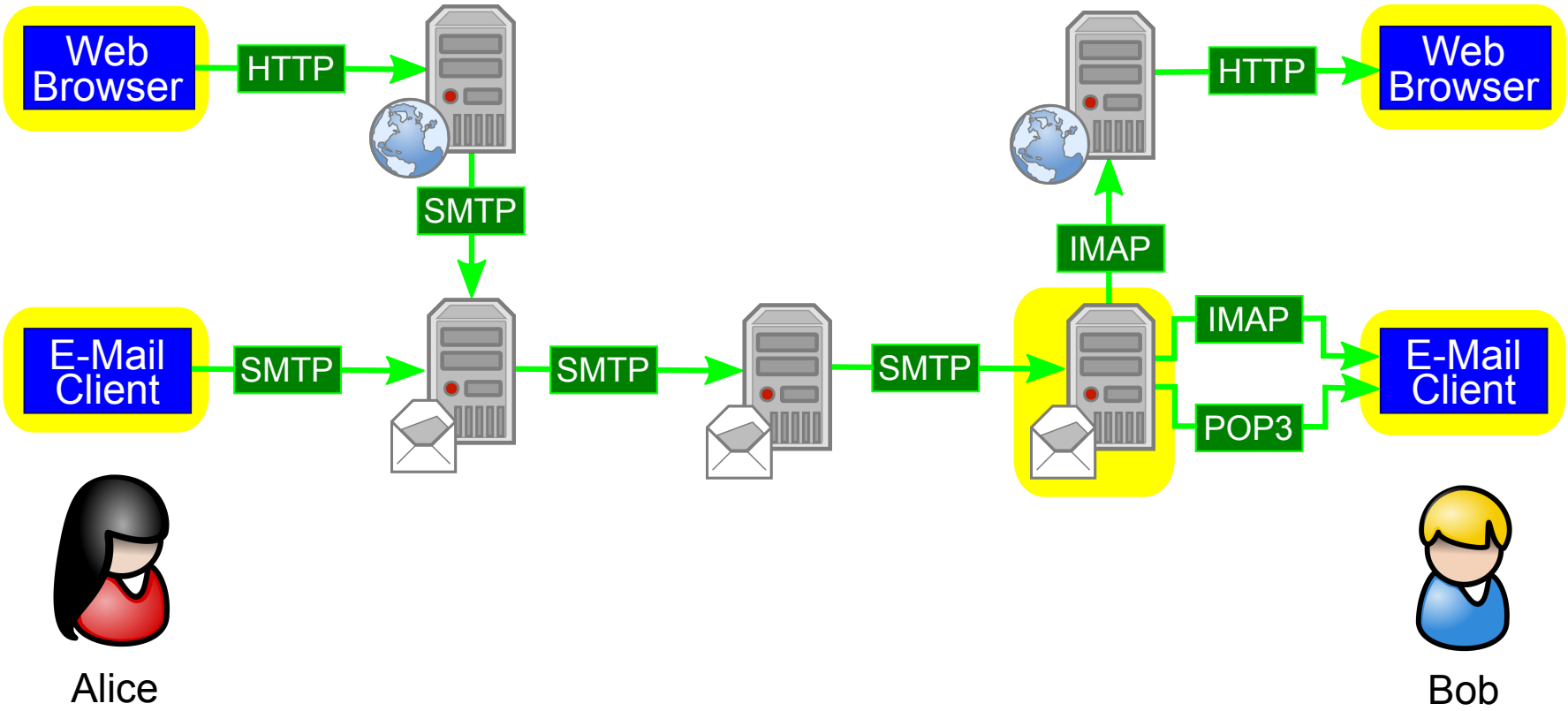
Frage: Wie schützt man E-Mails während der Übertragung?

Zugriff auf eine E-Mail



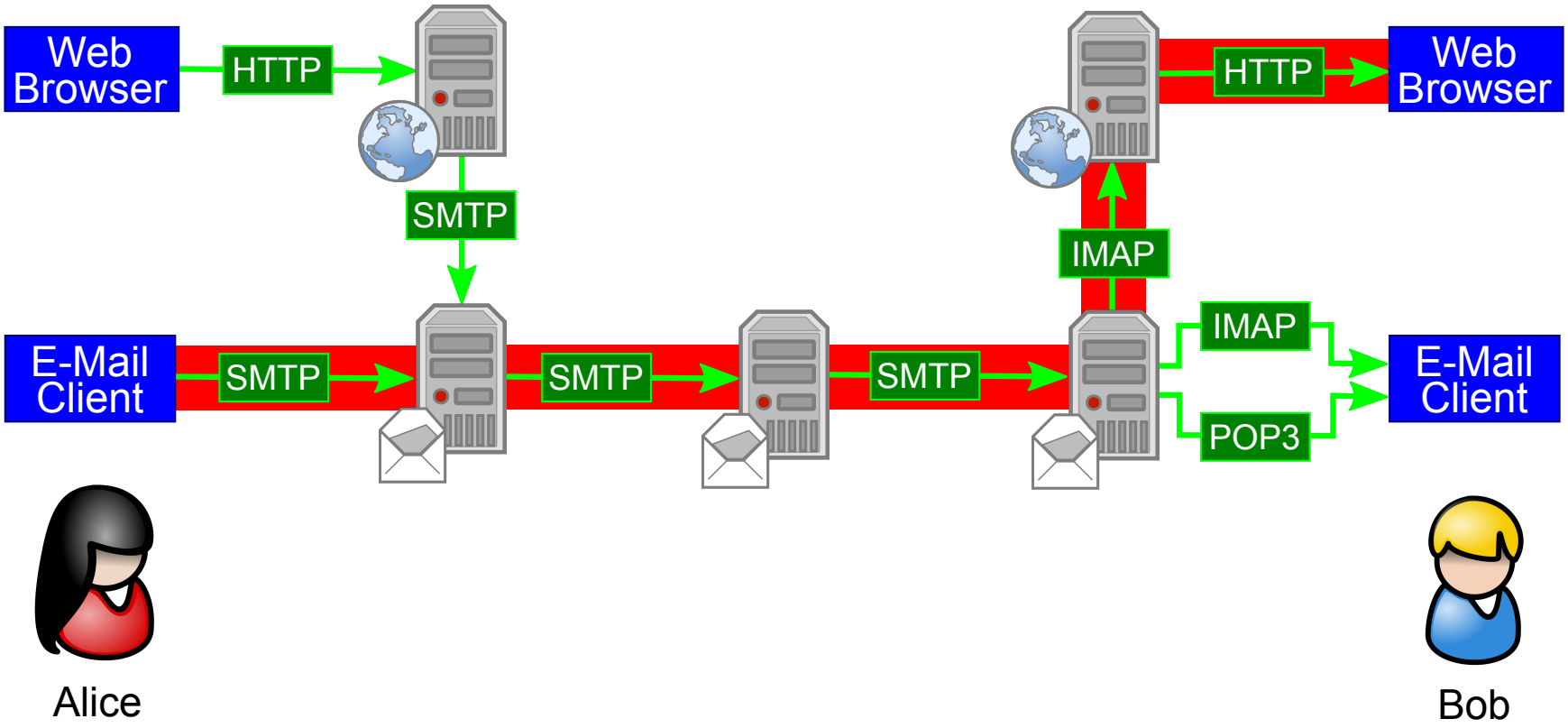
Frage: Wie schützt man den Inhalt einer E-Mail während des Schreibens/Lesens?

Speicherung einer E-Mail



Frage: Wie schützt man gespeicherte E-Mails?

Ende-zu-Ende-Sicherheit

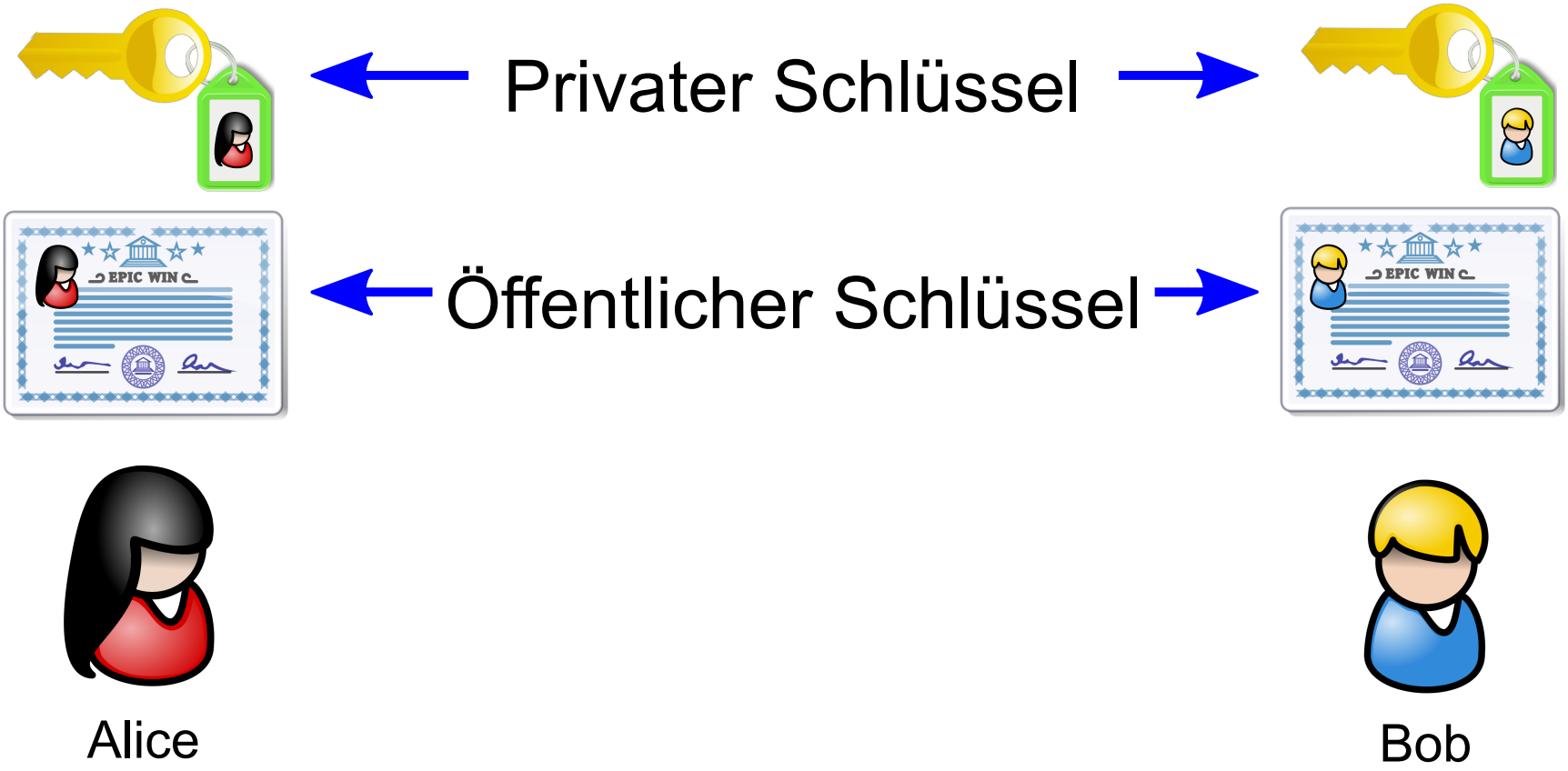


Anforderung: Nur der Empfänger der E-Mail ist in der Lage, deren Inhalt zu lesen.

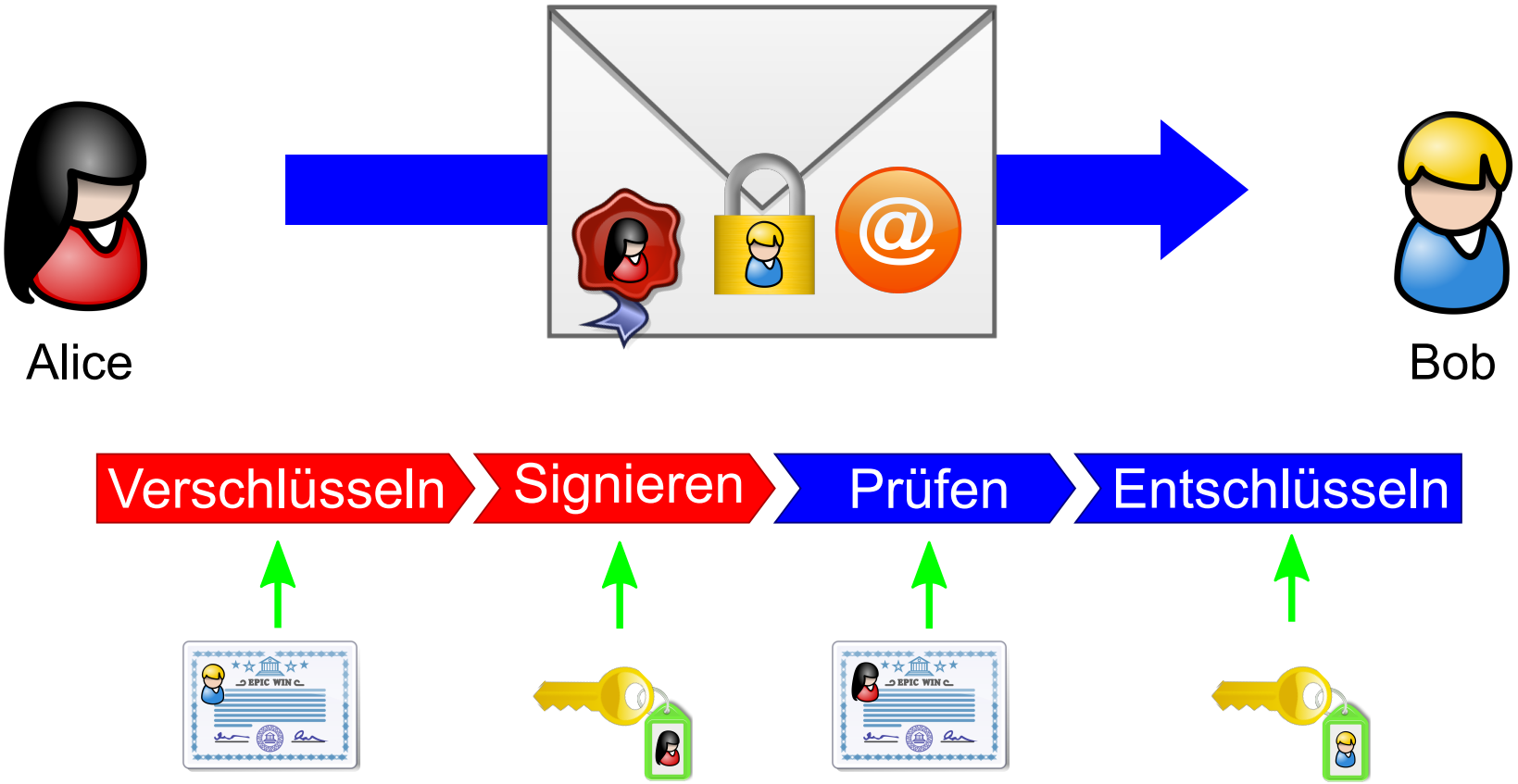
Sicherheitsmechanismen

- Übertragung von E-Mails
  - Einsatz sicherer Varianten von HTTP, IMAP, POP3 und SMTP
  - Server-Zertifikate in Verbindung mit SSL/TLS
- Zugriff auf E-Mails
  - Authentisierung der Nutzer
  - Einspielen sicherheitsrelevanter Updates
  - Arbeit in einer vertrauenswürdigen Umgebung
- Speicherung von E-Mails
  - Verschlüsselung der entsprechenden Datenträger
  - Sichere Aufbewahrung von Backup-Medien
- Ende-zu-Ende-Sicherheit
  - Einsatz von Benutzer-Zertifikaten und den entsprechenden kryptografischen Verfahren

Public Key Kryptosysteme

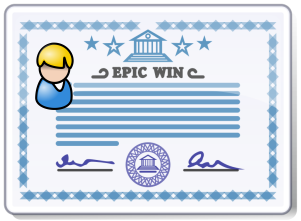


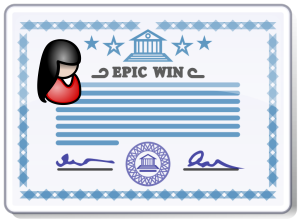
Public Key Kryptosysteme (Forts.)

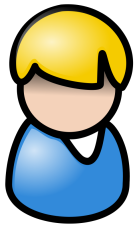


Herausforderung: Echtheit der Nutzerzertifikate

Alice







Bob

Zwei Ansätze

Public Key Infrastrukturen

- Zertifikate auf Basis des X509 Standards
- Hierarchische Struktur für die Prüfung der Echtheit von Zertifikaten
- Beglaubigung der Zertifikate durch eine Certificate Authority (CA)

Web Of Trust

- Pretty Good Privacy (PGP)/GNU Privacy Guard (GPG)
- Gegenseitige Bestätigung der Echtheit der Zertifikate durch die Nutzer
- Qualität eines Zertifikats abhängig vom Vertrauen in die unterzeichnenden Nutzer

Ist De-Mail die Lösung?

Quelle: Telekom

Wissenswertes zu De-Mail

- Projekt des Bundesministerium des Innern
- Ziel: Einführung eines elektronischen Pendants zur Briefpost
- Umsetzung einer Dienstleistungsrichtlinie der EU
- Technische Umsetzung durch De-Mail Diensteanbieter
- Akkreditierung der Anbieter durch das BSI
- Ende-zu-Ende-Verschlüsselung nur optional
  $\rightsquigarrow$ ungeeignet zur Übertragung vertraulicher Daten
- Einschätzung des Chaos Computer Club: „völlig lächerliches Sicherheitsniveau“

Zusammenfassung

- Die Absicherung von E-Mail Kommunikation ist eine komplexe Aufgabe
- Wichtige Aspekte sind:
  - Übertragung der E-Mails
  - Zugriff auf E-Mails
  - Speicherung der E-Mails
  - Ende-zu-Ende-Sicherheit
- Es existieren kryptografische Verfahren, um jeden Aspekt sicherer E-Mail abzudecken

Kontakt

Prof. Dr. Christoph Karg
Hochschule Aalen
Studiengang Informatik
Studienschwerpunkt IT-Sicherheit
Anton-Huber-Straße 25
73430 Aalen
Telefon 07361/576-4205
E-Mail christoph.karg@htw-aalen.de