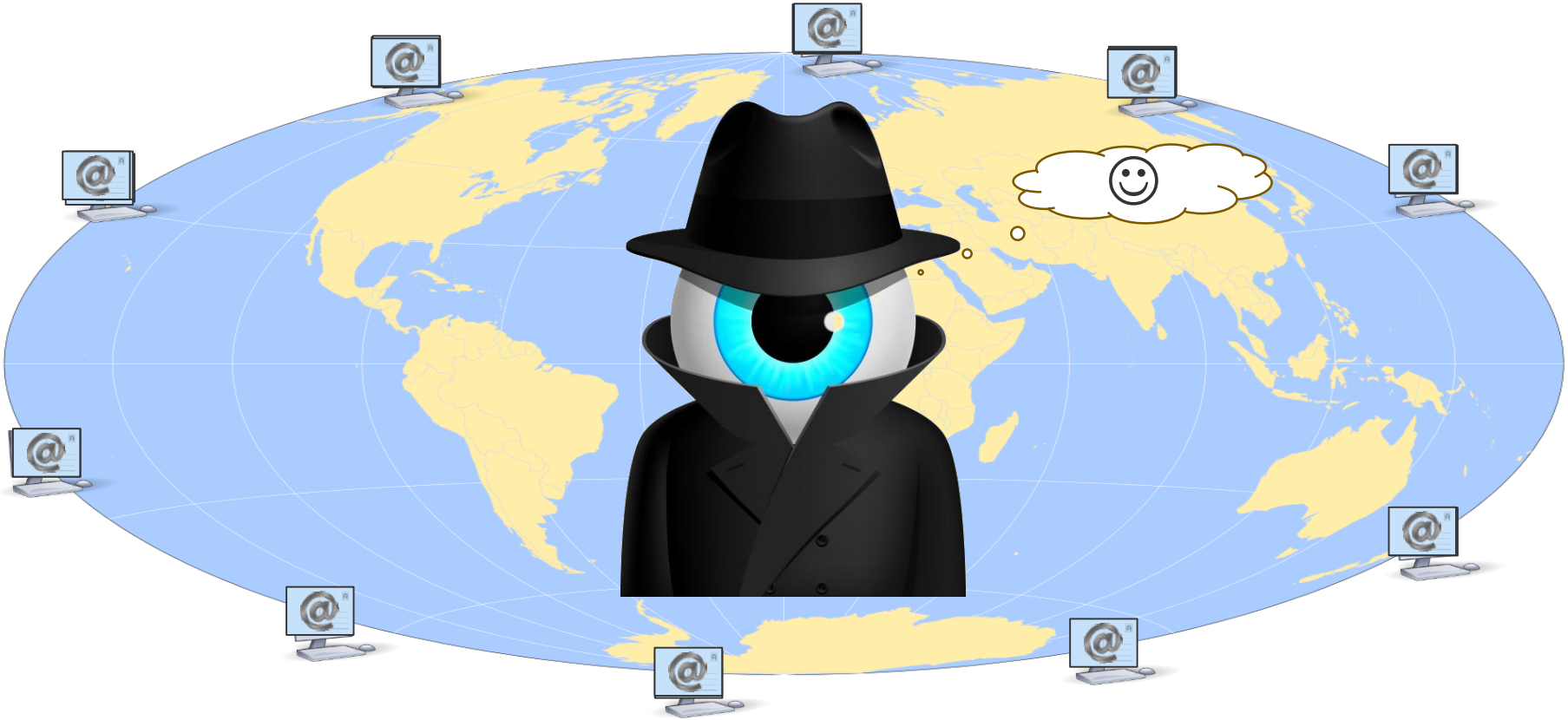
SICHERE E-MAIL

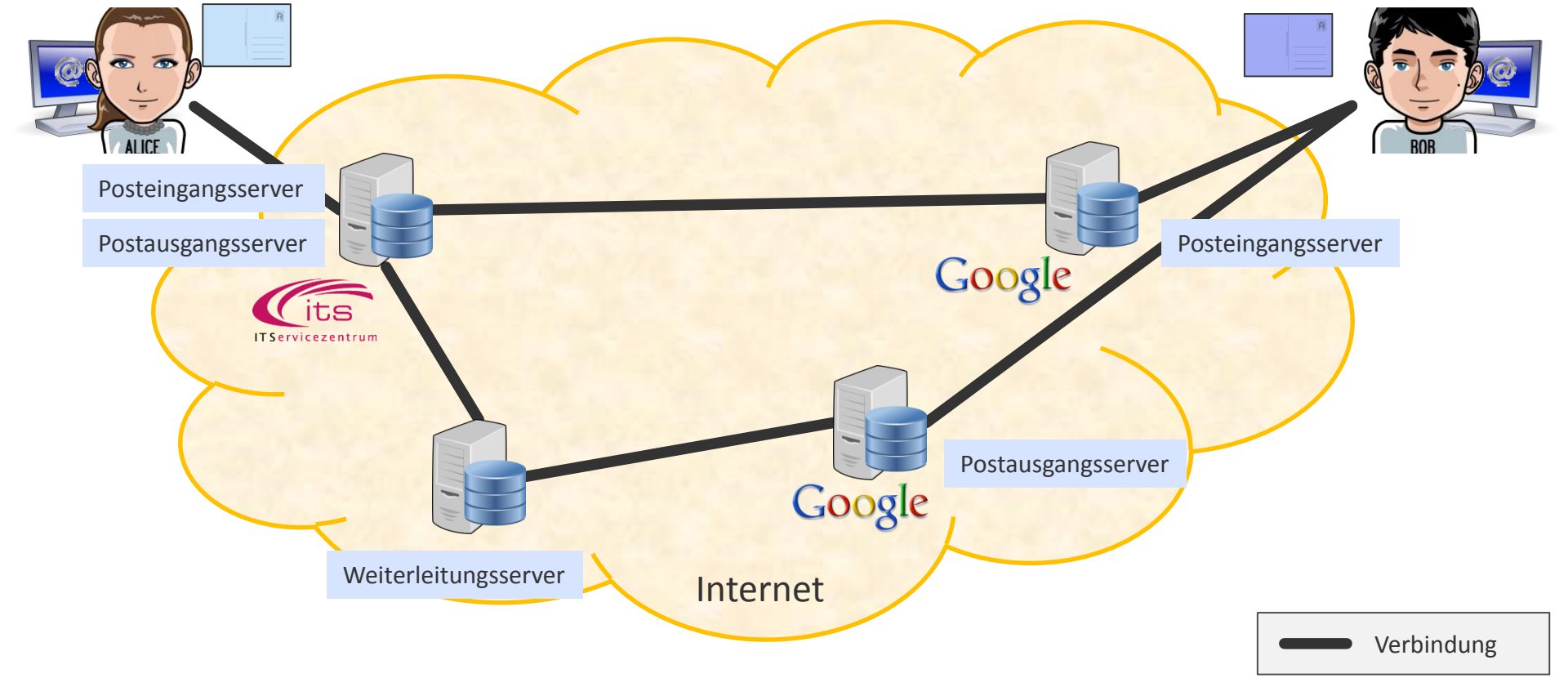
Prof. Arno Wacker
Angewandte Informationssicherheit
Universität Kassel

ZKI-Frühjahrstagung 2016

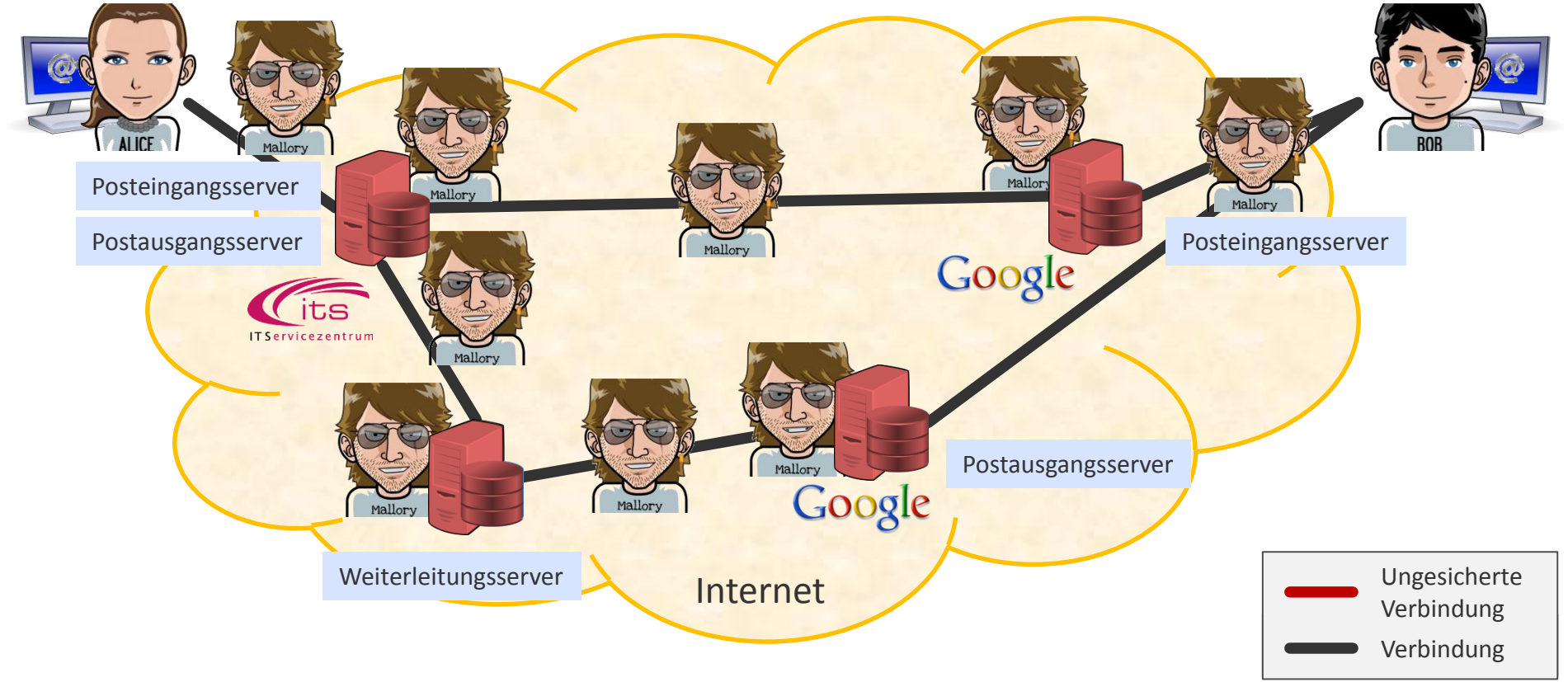
08. März 2016



Wie funktioniert E-Mail?



Wer kann meine E-Mail lesen?



Inhalt

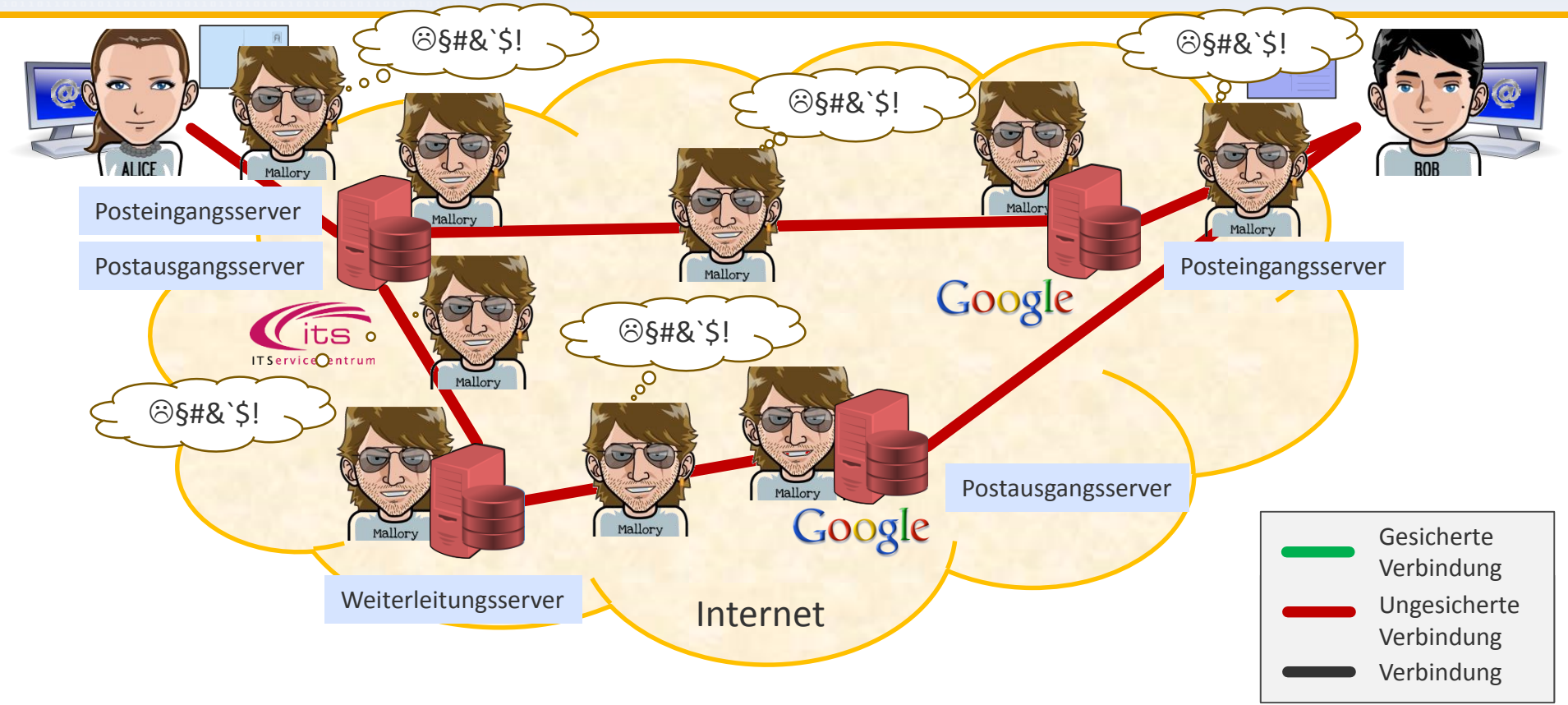
- **Motivation:** Warum wir sichere E-Mail verwenden sollten
- **Die Funktionsweise von sicherer E-Mail**
  - Transportverschlüsselung
  - Ende-zu-Ende Verschlüsselung
- **Herausforderungen & Lösungsansätze**
- **Fazit**

Transportverschlüsselung: Verwendung von SSL/TLS

- **Zwischen Client und Server**
  - Betreiber muss es anbieten (IMAP**S**, PO3**S**, SMTP**S** , HTTP**S**)
  - Benutzer kann/muss es selbst einschalten (Auswahl von SSL/TLS)
- **Zwischen den Servern**
  - Wird i.d.R. automatisch aktiviert, wenn von beiden Seiten unterstützt
  - Bei Inkompatibilität wird stillschweigend die Sicherung abgeschaltet
  - Benutzer hat keinen Einfluss darauf
- **Beispiele**
  - „E-Mail Made in Germany“
  - De-Mail (ohne die aktuell diskutierte PGP-Verschlüsselung)

De-Mail

Auswirkung der Transportverschlüsselung



Ende-zu-Ende-Sicherung

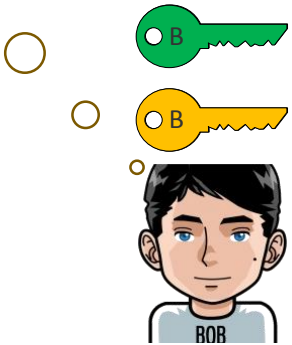
- **Bisher: Sicherung der Transportwege (Transportverschlüsselung)**
  - Auf jedem Server liegt der Klartext vor
  - Manipulation der Daten, z.B. des Absendernamens, möglich (SPAM...)
- **Besser: Sicherung des Mailinhaltes (Ende-zu-Ende)**
  - Verschlüsselung der Daten und Signierung durch den Absender
    - Daten sind auf dem gesamten Übertragungsweg nie unverschlüsselt
    - Identität des Absenders und Integrität des Inhalts kann überprüft werden
  - Unabhängig von der Sicherung des Transportweges
  - Zwei Möglichkeiten (beides anerkannte Standards)
    - S/MIME – Secure / Multipurpose Internet Mail Extensions (1995, RFC 2633)
    - OpenPGP – Pretty Good Privacy (1998, RFC 2440)

Grundlage: Asymmetrische Kryptographie – Verschlüsseln

Eine vertrauliche Nachricht an Bob verschlüssele ich mit Bobs **öffentlichem** Schlüssel.

Eine vertrauliche Nachricht für mich entschlüssele ich mit **meinem privaten** Schlüssel.

Nachricht



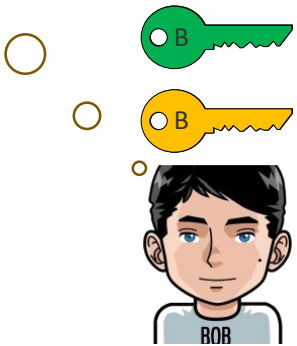
Öffentlicher Schlüssel
Privater/geheimer Schlüssel

Grundlage: Asymmetrische Kryptographie – Signieren

Zum Unterschreiben verwende ich **meinen privaten** Schlüssel.

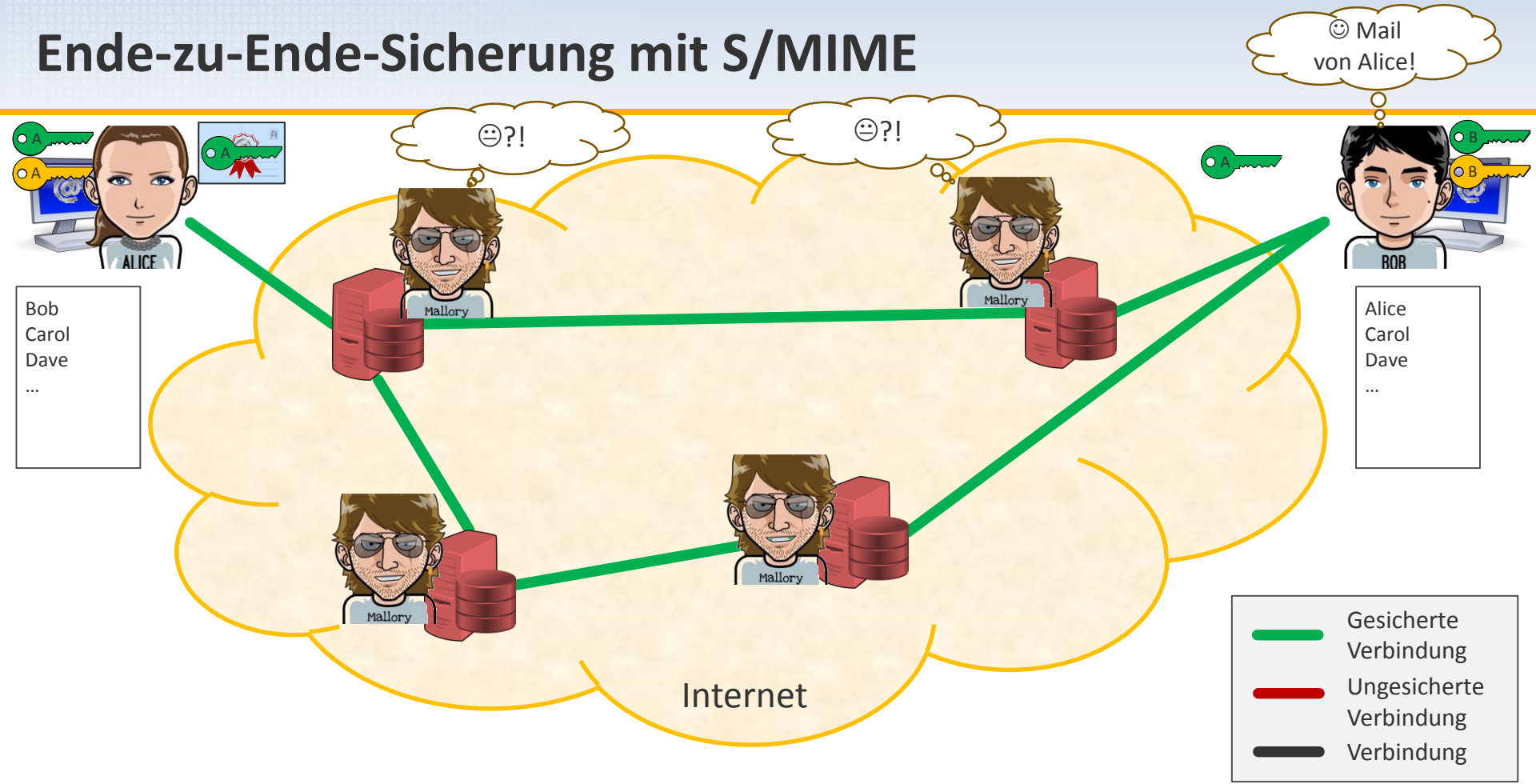
Zum Überprüfen, ob die Nachricht von Alice kommt, verwende ich Alices **öffentlichen** Schlüssel.

Nachricht

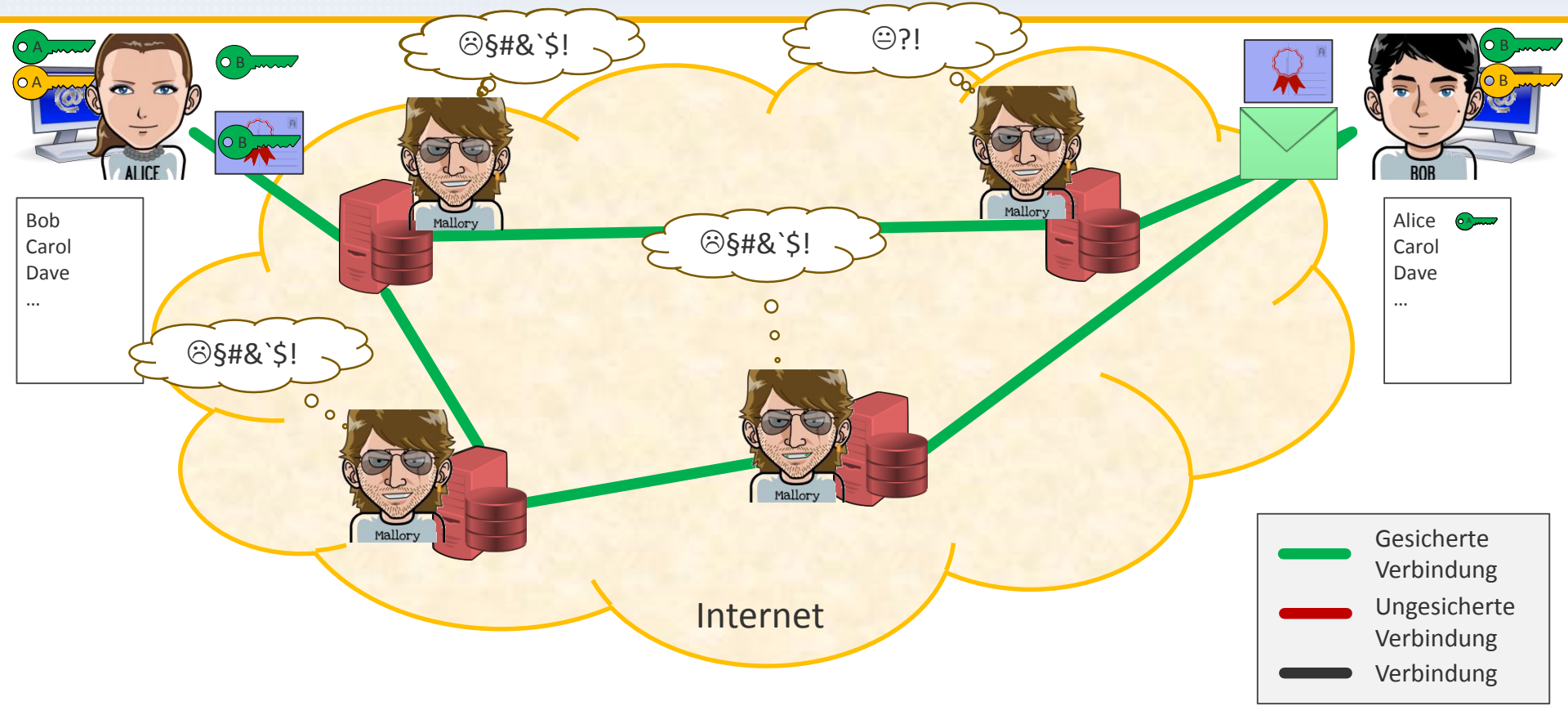


Öffentlicher Schlüssel
Privater/geheimer Schlüssel

Ende-zu-Ende-Sicherung mit S/MIME



Ende-zu-Ende-Sicherung mit S/MIME



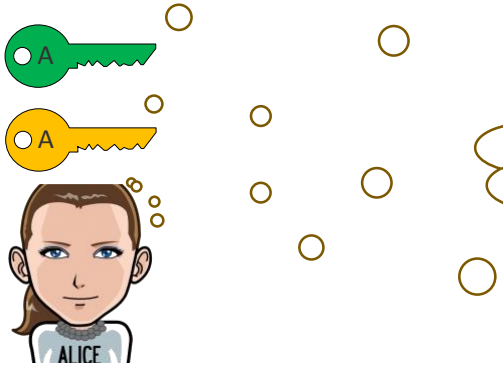
Ende-zu-Ende-Sicherung mit S/MIME – Zertifikate / PKI

- **Problem: „Man-in-the-Middle“**
  - Bob benötigt Alices öffentlichen Schlüssel
  - Mallory könnte diesen bereits auf dem Weg abfangen und ersetzen
  - Danach könnte er alles entschlüsseln und somit mitlesen
- **Lösung: Zertifikate mit einer „Public Key Infrastructure“ (PKI)**
  - „Certification Authority“ (CA)
    - Der öffentliche CA-Schlüssel ist wohlbekannt und in den E-Mail-Programmen integriert
    - Die CA unterschreibt mit ihrem privaten Schlüssel den öffentlichen Schlüssel der Teilnehmer/E-Mail-Nutzer
  - Öffentliche Schlüssel werden nur akzeptiert, wenn sie von einer CA unterschrieben sind

Ende-zu-Ende-Sicherung mit S/MIME – Zertifikate / PKI

Zunächst generiere ich mir ein Schlüsselpaar.

Den öffentlichen Schlüssel lasse ich nun von der CA unterschreiben.



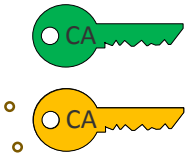
Der unterschriebene öffentliche Schlüssel ist mein Zertifikat.

Das kann jeder mit dem wohlbekannten öffentlichen Schlüssel der CA überprüfen.

Identifikation bitte!

Hier ist mein Personalausweis.

OK!



Ende-zu-Ende-Sicherung mit S/MIME – Zusammenfassung

- **Jeder Teilnehmer muss sich ein Schlüsselpaar generieren**
  - Der private Schlüssel ist nur dem Besitzer bekannt (auch nicht der CA!)
  - Der öffentliche Schlüssel ist hingegen für jedermann zugänglich
- **Der öffentliche Schlüssel muss von einer Zertifizierungsstelle (CA) unterschrieben werden**
  - Das ergibt das Zertifikat – kann z.B. auch auf der eigenen Webseite veröffentlicht werden
  - Ab Klasse 3 ist eine Identitätsprüfung notwendig
- **Für das Verschlüsseln benötigt man das Zertifikat des Empfängers**
  - Dieses bekommt man automatisch mit der ersten unterschriebenen E-Mail
  - Kann auch manuell installiert werden
  - Es gibt auch Verzeichnisse
  - **Empfehlung:** Verschlüsselung immer verwenden, wenn es geht (d.h. wenn das Zertifikat bekannt ist)
- **Unterschreiben geht immer, da man dabei nur den eigenen privaten Schlüssel benötigt**
  - Nachrichten, die nur unterschrieben sind, bieten keinen Vertraulichkeitsschutz (d.h. Mallory liest mit)
  - Es kann aber sichergestellt (verifiziert) werden, dass die Nachricht nicht verändert wurde
  - Auch Teilnehmer, die S/MIME nicht nutzen, können diese E-Mails problemlos lesen
  - **Empfehlung:** Signieren immer aktivieren, da dadurch das Zertifikat automatisch verteilt wird

Herausforderungen in der Praxis

Technologien sind vorhanden, Benutzbarkeit muss deutlich verbessert werden.

- **Benutzbarkeit der existierenden Software**
  - Anfangshürde ist derzeit zu hoch (Zertifikat beantragen und einrichten)
  - Benutzer haben mehrere Geräte (Verteilung der Zertifikate auf alle Geräte)
  - Im Betrieb z.T. explizites Einschalten der Sicherung notwendig (1 Klick zu viel)
  - Ablauf/Erneuerung der Zertifikate (Altes Zertifikat muss für immer behalten werden)
- **Interoperabilität momentan …**
  - … zwischen Mailclients
    - Beispiel: Korrekte Signaturen aus Lotus werden z.T. in Thunderbird als nicht gültig angezeigt
  - … zwischen den beiden etablierten Standards S/MIME und PGP
    - Ein ewiger Kampf, beide wollen das Gleiche, kritisieren aber das jeweils andere...
    - Konflikte bei der Verwendung beider Standards (z.B. PGP/MIME und S/MIME)

Lösungsansätze

- **Es funktioniert bereits heute in großen Unternehmen**
  - Sichere E-Mail wird den Mitarbeitern ohne Hürde angeboten
  - Gängige Lösungen verwenden zwei Schlüsselpaare (signieren und verschlüsseln)
    - S/MIME-Gateways (d.h. der Benutzer bemerkt davon nichts)
    - Mit Smartcards (privater Schlüssel für das Verschlüsseln auch auf zentralem Server)
    - Plugins für gängige E-Mail-Clients sind z.T. proprietäre Eigenentwicklungen

- **Es soll in Zukunft auch für jedermann verfügbar sein**
  - Automatisierte und kostenlose Zertifikate (direkt während der E-Mail-Einrichtung)
  - Automatisierte Verteilung der Zertifikate auf alle Geräte (z.B. durch einen Clouddienst)
  - Nahtlose und konfliktfreie Integration der beiden Standards in alle Clients
  - Klare und einfache Rückmeldungen an den Benutzer

  ➔ **Für den Nutzer darf es nicht komplizierter werden** („will nur eine E-Mail schreiben“)

Fazit

- Es gibt **gute Gründe,** sichere E-Mail zu verwenden
- Ein **alltagstauglicher** praktischer Einsatz ist machbar

- **Signieren immer**
- **Verschlüsseln, wenn möglich**
- **Wirkungsvoll**
  - Gegen Hacker und neugierige Administratoren
  - Gegen Massendaten-Überwachung und -Spionage

Vielen Dank
für Ihre Aufmerksamkeit!

Prof. Arno Wacker
arno.wacker@uni-kassel.de