



Sichere Email: PGP & S/MIME

Gerald Haider

Josef Schachinger

[Gliederung]

- Einleitung/Geschichtliches
- Verschlüsselungsverfahren Algorithmen
- Einbettung in Mails
- Schlüsselverwaltung
- Einsatz in der Praxis
- Sicherheitsrisiken
- Zusammenfassung

[Warum PGP – S/MIME ?]

- Vertraulichkeit
 - Geheimhaltung gegenüber Dritter
 - Verschlüsseln
- Integrität
 - Ausschließbarkeit von Manipulationen an den Daten
 - Fingerprint durch Hashwert (=> signieren)
- Authentizität
 - Überprüfbarkeit der Herkunft
 - signieren
- Verbindlichkeit
 - Nichtabstreitbarkeit der Herkunft
 - signieren

[Geschichtliches zu PGP]

- Erfinder Phil Zimmerman
- 1991 erste Version veröffentlicht
- war aufgrund von Exportbeschränkungen illegal
- 1997 übernommen von NAI (Network Associates)
- 1997 OpenPGP von PGP V 5 abgeleitet

[Geschichtliches zu S/MIME]

- S/MIME Version 1, spezifiziert im Jahr 1995 von RSA Security, Inc.
- S/MIME Version 2, März 1998
RFC 2311 und RFC 2312
- Version 3 im Juli 1999 veröffentlicht

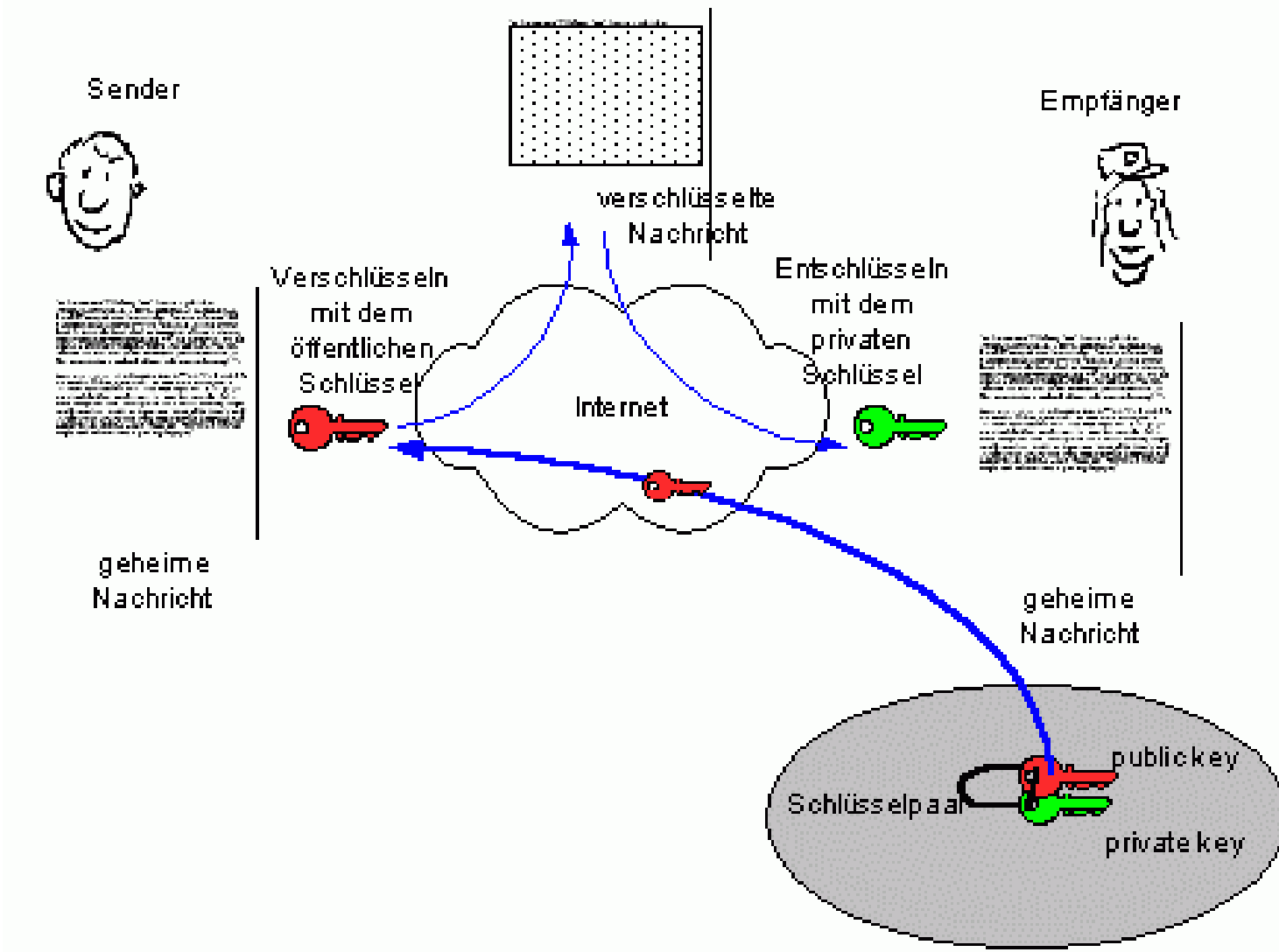
Verschlüsselungsverfahren - symmetrisch

- Symmetrisch – gleicher Schlüssel zum Ver- und Entschlüsseln
- Problematik sicherer Schlüsselübergabe
- Einfaches Beispiel:
 - Caesar's Verschlüsselung
- Aktuelle Algorithmen:
 - CAST, IDEA, 3DES

Verschlüsselungsverfahren – asymmetrisch I

- Jeder Benutzer hat ein Schlüsselpaar
 - öffentlicher Schlüssel für jedermann zugänglich
 - privater Schlüssel muss geheim gehalten werden
- höherer Rechenaufwand als symmetrische Verfahren
- Problematik der Echtheit des öffentlichen Schlüssels

Verschlüsselungsverfahren – asymmetrisch II



Verschlüsselungsverfahren – asymmetrisch III

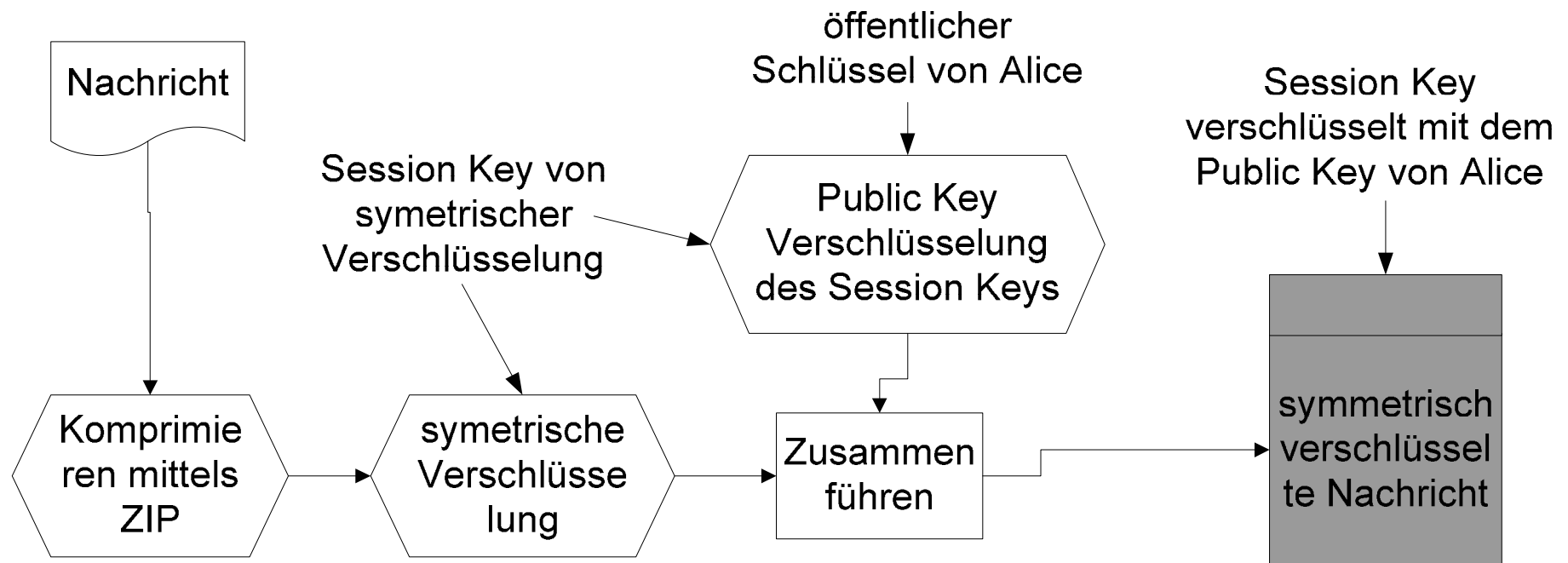
- Aktuell eingesetzte Algorithmen:
 - Diffie-Hellman - ElGamal
 - RSA
- Einfaches Beispiel:
 - Merkel-Hellmann Verfahren

Verschlüsselungsverfahren – hybride Verfahren

- Hybride – Kombination aus symmetrisch und asymmetrisch
- Geschwindigkeitsvorteil der symmetrischen Verfahren
- „Einfachheit“ bzw. Sicherheit des Schlüsselaustausches von asymmetrischen Verfahren

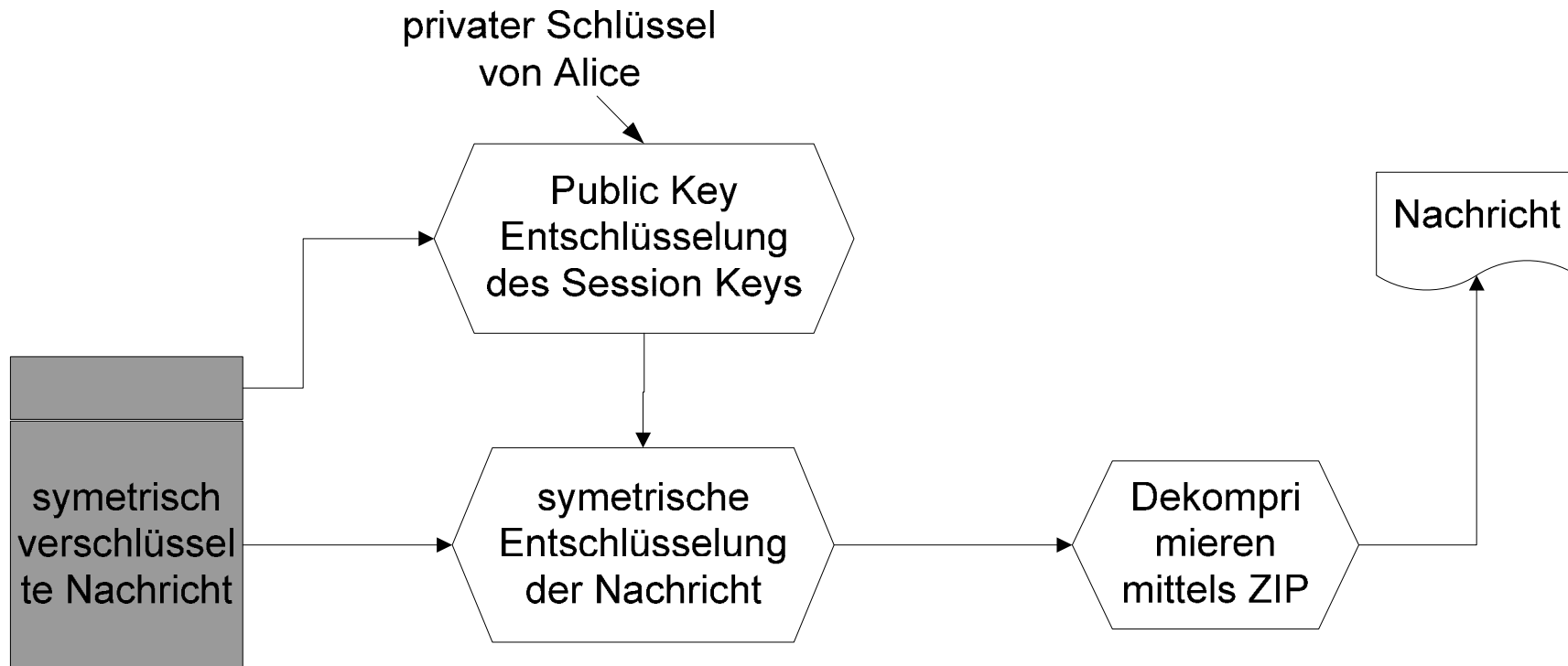
Verschlüsselungsverfahren – hybrides Verfahren bei PGP I

■ Verschlüsseln



Verschlüsselungsverfahren – hybrides Verfahren bei PGP II

■ Entschlüsseln



[Fingerprinting - Hash Verfahren]

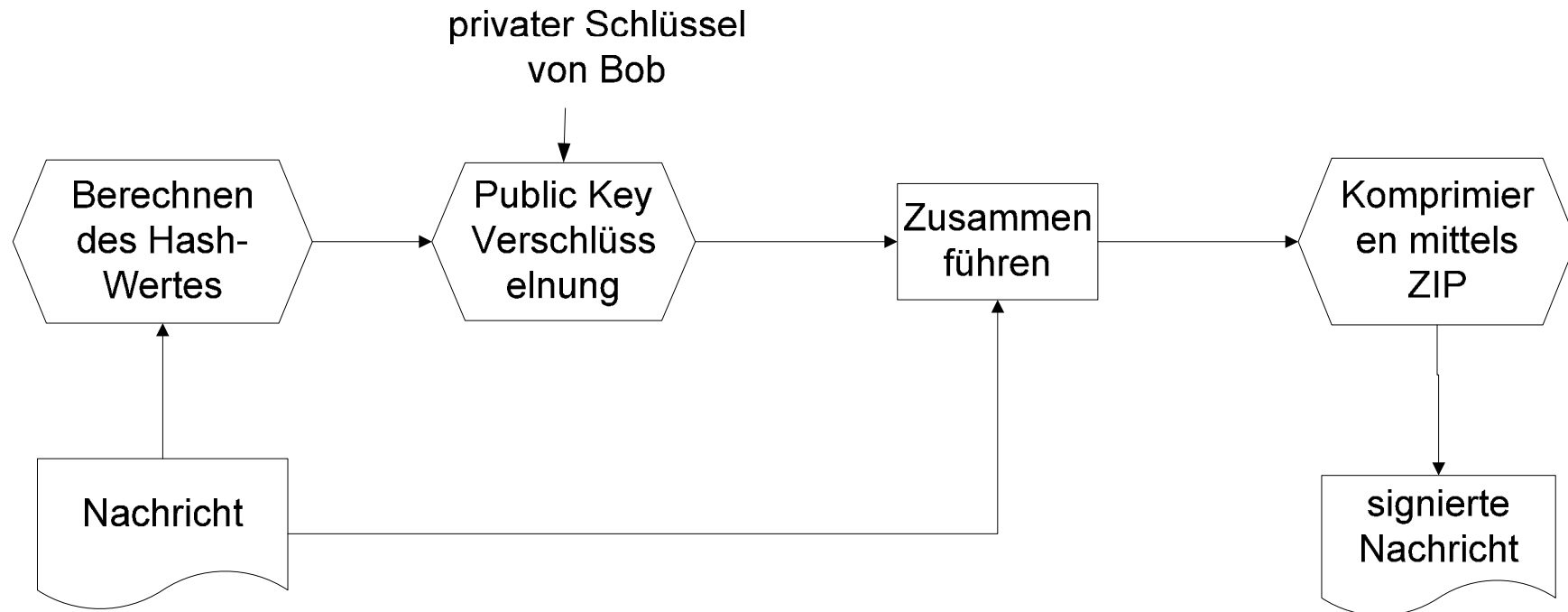
- Verfahren zum Erstellen von Fingerprints von Daten
- jegliche Änderung an den Originaldaten verursacht eine Änderung des Hash Wertes
- Beispiele für Hashing Algorithmen
 - MD4, MD5, SHA1

[Digitale Unterschriften]

- Berechnen eines Hash Wertes über die Nachricht
- zum Erzeugen der digitalen Unterschrift werden:
 - der Hash Wert
 - ein aktueller Timestampmit dem privaten Schlüssel des Unterzeichners verschlüsselt

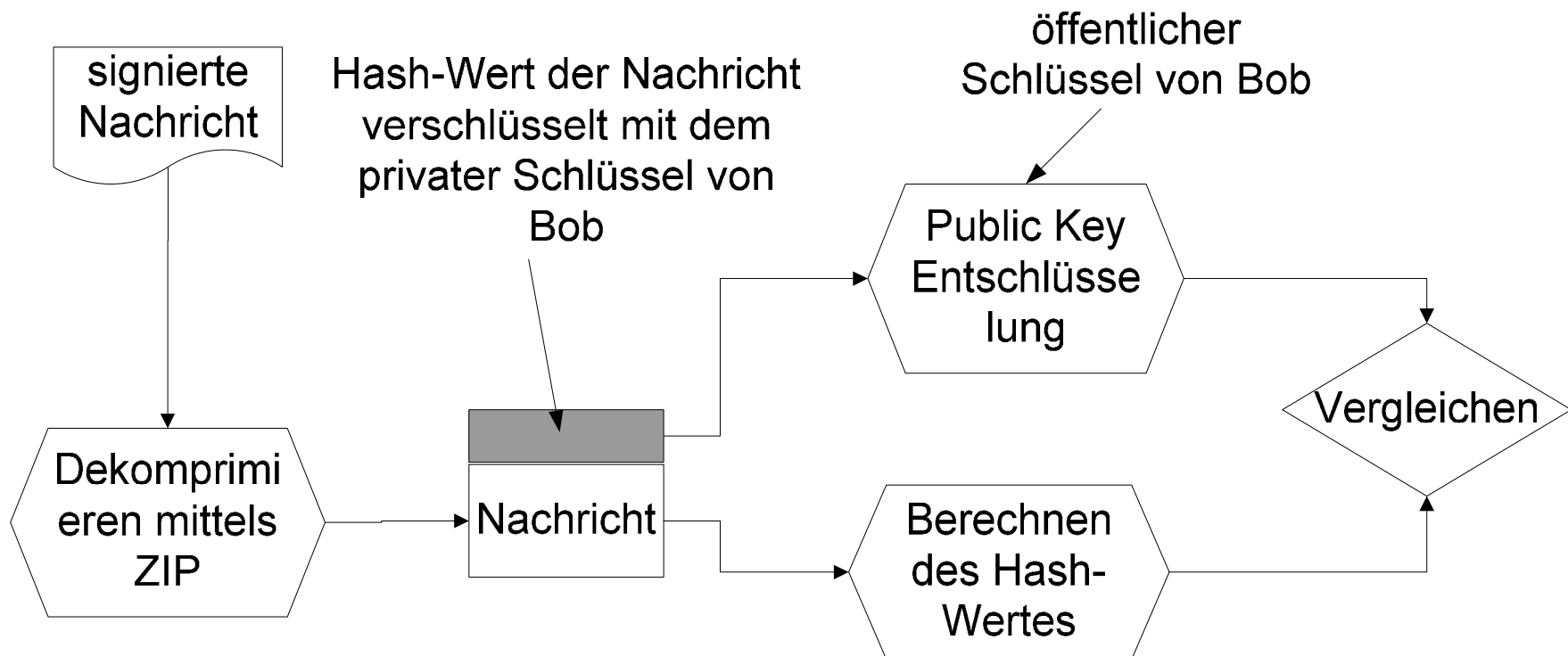
Digitale Unterschrift am Beispiel von PGP I

■ Erzeugen der Signatur



Digitale Unterschrift am Beispiel von PGP II

■ Überprüfen der Signatur



[Einbettung in Mails - Probleme]

- ursprünglicher Standard: RFC 822
 - nur 7 Bit ASCII Zeichensatz möglich
 - keine Umlaute bzw. Binärdaten
- MIME – Multipurpose Internet Mail Extension
 - erlaubt codierte Binärdaten (base64 encoding)

[Einbettung in Mails - PGP]

- Einbettung als 7 Bit ASCII Code
 - Text in normalen ASCII
 - Signatur in base64 encoding
- Einbettung mittels verschiedener MIME Content Types
 - z.B: application/pgp-signature

[Einbettung in Mails – S/MIME]

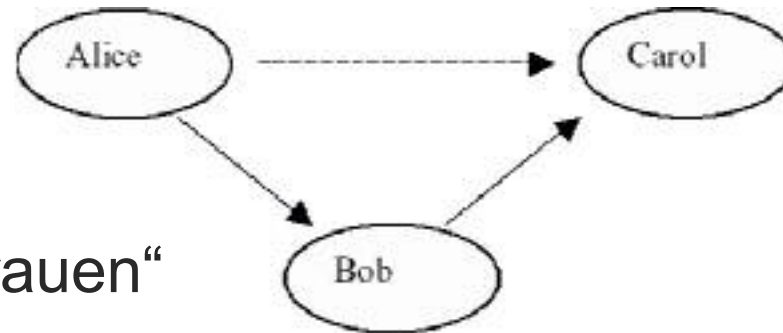
- S/MIME – Content Types
 - Enveloped data
 - Signed data
 - Clear-signed data
 - Signed and enveloped data

[Schlüsselverwaltungssysteme I]

- Problem bei asymmetrischer Verschlüsselung:
 - Verifikation der Echtheit des öffentlichen Schlüssels
- Bob will Alice verschlüsselt schreiben:
 - wie kann Bob feststellen das der ihm vorliegende öffentliche Schlüssel wirklich von Alice stammt?

[Schlüsselverwaltungssysteme II]

- Web of Trust



- Gegenseitiges „Vertrauen“

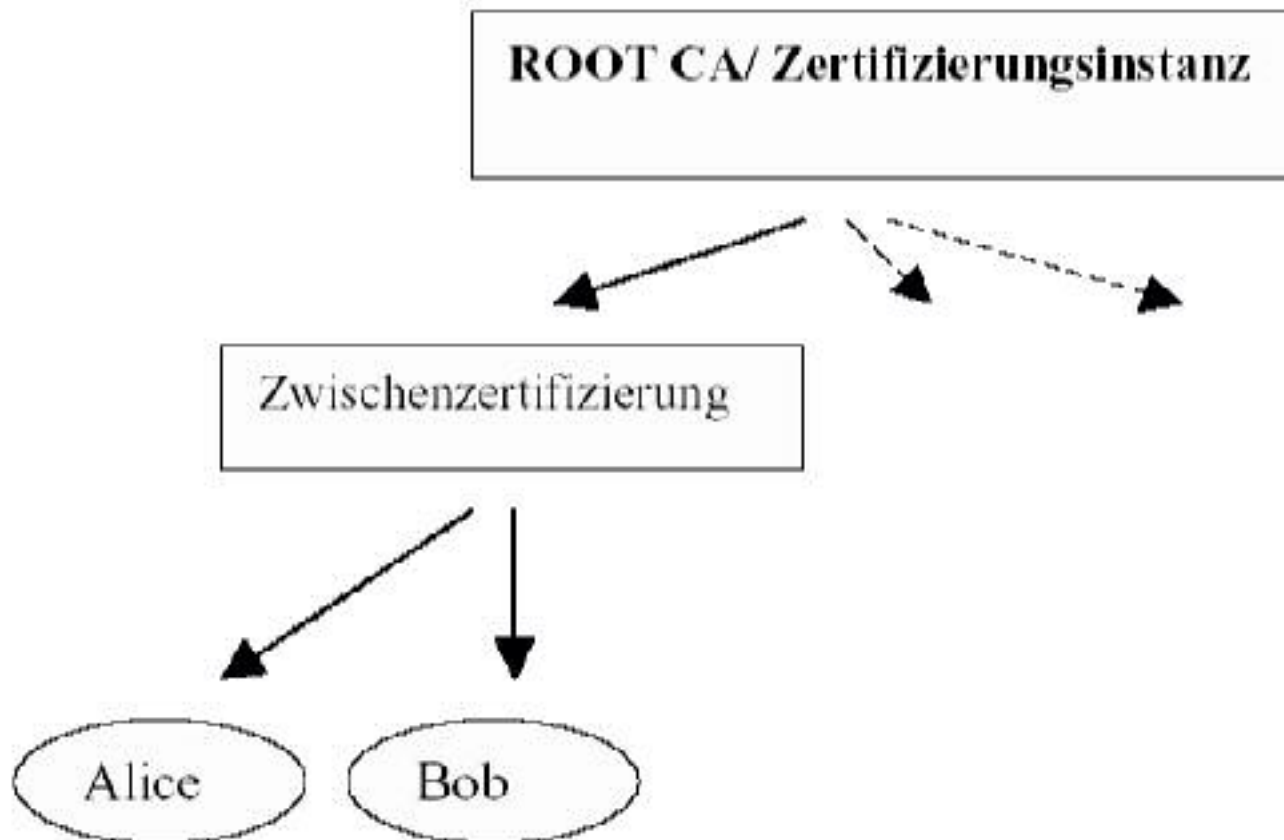
- Bob vertraut Alice und Carol vertraut Bob!

- Grad des Vertrauens kann weiter erhöht werden durch:

- Fingerprint Vergleich muss über ein sicheres Medium erfolgen.
- Veröffentlichung auf „relativ“ fälschungssicheren Medien (c't)

[Schlüsselverwaltungssysteme II]

- Certification Chain



[Sicherheitsrisiken I]

- Kompromittierte Passphrasen oder private Schlüssel
- Veränderter öffentlicher Schlüssel
- Rückstände von gelöschten Dateien
- Viren und Trojanische Pferde
- Auslagerungsdateien

[Sicherheitsrisiken II]

- Tempest-Angriffe
- Gefälschte Zeitmarkierungen
- Mehrbenutzer Systeme
- Datenverkehrsanalyse
- Kryptoanalyse

[Zusammenfassung]

- moderne Verschlüsselung basiert auf hybriden Techniken
- Hauptproblem nach wie vor der Schlüsselaustausch
- Verschiedene Ansätze zum Schlüsselaustausch, Web of Trust, Certification Chain