Die Rolle von Verschlüsselung, digitalen Signaturen und digitalen Zertifikaten beim E-Commerce

Arno Hornberger
a_hornbe@informatik.uni-kl.de

Seminarvortrag im Sommersemester 2001

Arbeitsgruppe
Datenbanken und Informationssysteme

Universität Kaiserslautern

Inhalt

- Sicherheit und E-Commerce
- Rolle von Unterschriften
- Kryptographische Verfahren
- Digitale Signaturen
- Digitale Zertifikate
- Trustmodelle
- Signaturgesetz

- Zusammenfassung

Sicherheit und E-Commerce

- Einige Merkmale von E-Commerce
  - Räumliche Distanz
  - Anonymität
  - Spontaneität
  - Erreichbarkeit
  - Markttransparenz

- Neben vielen Vorteilen auch Sicherheitsrisiken
  - für Verkäufer
  - für Kunden

- Risiken durch zeitliche Trennung von Warenübergabe und Bezahlung in Verbindung mit Anonymität der Teilnehmer

- Problem: Wer kann haftbar gemacht werden und unter welchen Umständen?

  ⇨ enge Verknüpfung mit gesetzlichen Vorgaben

Rechtssicherheit durch Verträge

- Unterschrift macht Dokument zur Urkunde
- hoher Beweiswert von Urkunden
- Verträge als Form von Urkunden

  ⇨Rechtssicherheit durch Verträge

- Verträge als wichtiges Instrument wirtschaftlicher Aktivität
- elektronische Verträge als Voraussetzung für Rechtssicherheit beim E-Commerce
- zentrale Rolle der Unterschrift
- Funktionen der Unterschrift
  - Identifikationsfunktion
  - Echtheitsfunktion
  - Abschlußfunktion
  - Warnfunktion

- Ziel: elektronische Nachbildung der Funktionen der Unterschrift als *digitale Signatur*

Kryptographische Verfahren zur Realisierung digitalen Signaturen

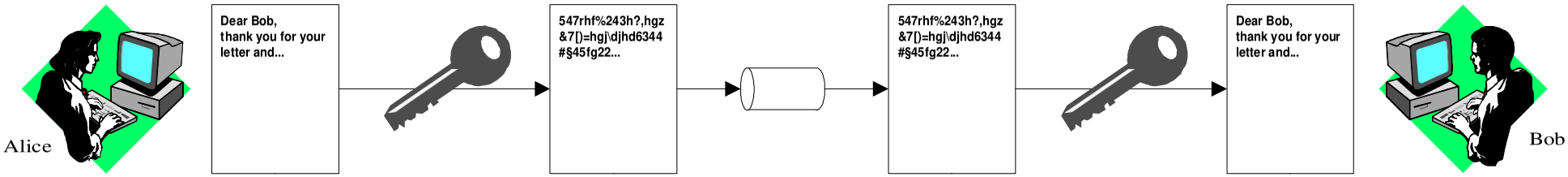
- Kryptographie als Wissenschaft von der Datenverschlüsselung unter Zuhilfenahme mathematischer Verfahren
- Kryptographische Verfahren

  ...zur Verschlüsselung von Daten
  ...als Kernelement digitaler Signaturen
  ...zur Gewähr von Sicherheit durch Geheimhaltung

- Verwendung von Zahlen/Zeichenketten als Schlüssel
- Einfaches Sender-Kanal-Empfänger-Modell
- Systematisierung in
  - schwache und starke
  - symmetrische und asymmetrische

  Verfahren
- Abhängigkeit der Stärke von Schlüsselgüte und gewähltem Verfahren
- Entwicklung fortgeschrittener Verfahren durch Mathematik und Computertechnik begünstigt

Symmetrische Verfahren (1)



- einfachstes Verfahrensschema
- historische Verfahren (<1970) alle symmetrisch
- Verwendung des gleichen Schlüssels zum Verschlüsseln und Entschlüsseln
- Einigung über benutzten Schlüssel notwendig (sicherer Kanal)
- bedeutende Vertreter: DES (1974), IDEA (1990), Blowfish (1994), CAST

Symmetrische Verfahren (2)

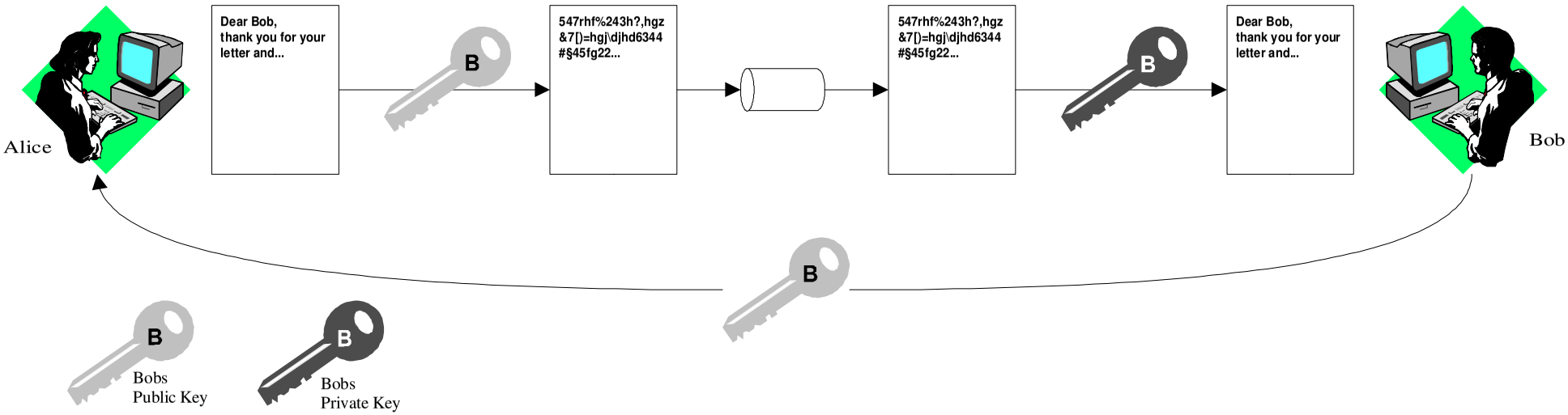
■ Vorteile:

- ➢ hohe Geschwindigkeit
- ➢ geringer Verfahrensaufwand
- ➢ gut geeignet zur Archivierung

■ Nachteile:

- ➢ Sicherheitsrisiko durch Notwendigkeit des Schlüsseltransfers
- ➢ große Angriffsfläche für Schlüsseldiebe (zwei Personen)
- ➢ nicht geeignet für digitale Signaturen

Asymmetrische Verfahren (1)



- relativ junge Verfahren (>1970)
- asymmetrische Verfahren als Ansatz zur Lösung des Hauptproblems symmetrischer Verfahren
- Aufteilung des Schlüssels in privaten und öffentlichen Teil
- öffentlicher Schlüsselteil frei verfügbar

Asymmetrische Verfahren (2)

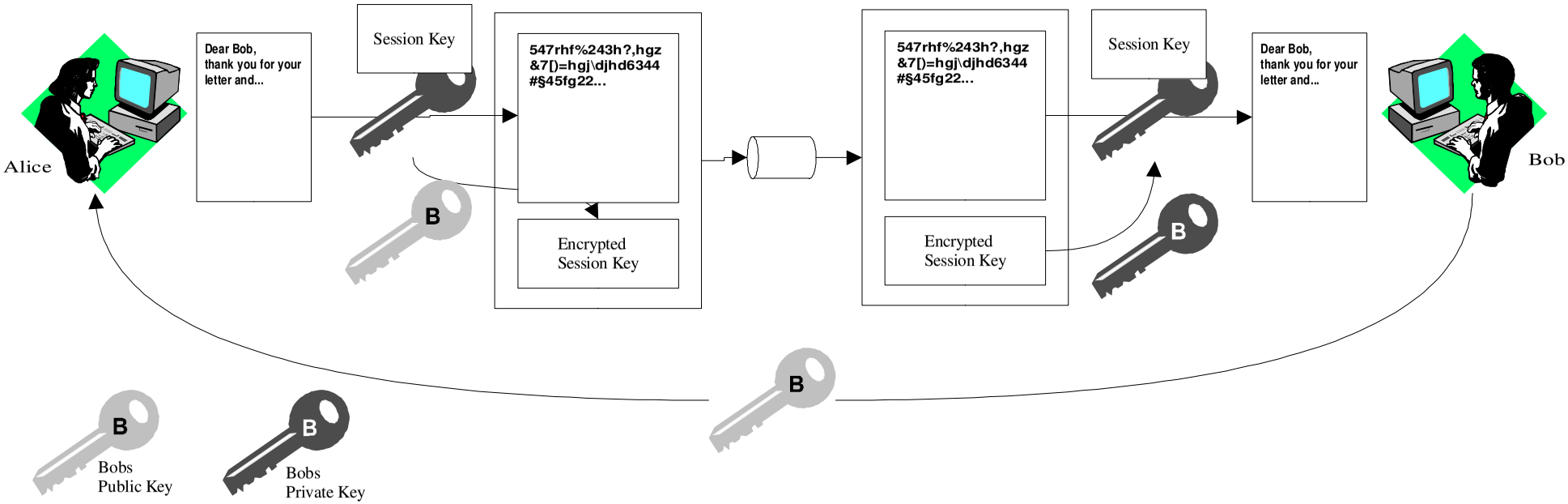
- mit öffentlichem Schlüssel verschlüsselte Botschaft kann nur mit privatem Schlüssel entschlüsselt werden
- Notwendigkeit von Schlüsselverzeichnissen (Public-Key-Server)
- bedeutende Vertreter: DH (1976), RSA (1978)

- **Vorteile:**
  - Sicherheitsrisiko durch Schlüsseltransfer nicht gegeben
  - Eignung für digitale Signaturen

- **Nachteile:**
  - hoher Verschlüsselungs und Verfahrensaufwand
  - Problem der sicheren Zuordnung zwischen öffentlichem Schlüssel und Eigentümer

Hybride Verfahren (1)

- kombinierter Einsatz von symmetrischen und asymmetrischen Verfahren
- hohe Verschlüsselungsraten bei großer Sicherheit



Hybride Verfahren (2)

- Anwendung im weit verbreiteten PGP
- Einsatz hybrider Verfahren bei SSL

Vorteile:

- Vereinigung der Geschwindigkeit symmetrischer Verfahren mit Public-Key-Eigenschaften von asymmetrischen Verfahren
- sicherstes Verfahrensschema zur effektiven verschlüsselten Kommunikation

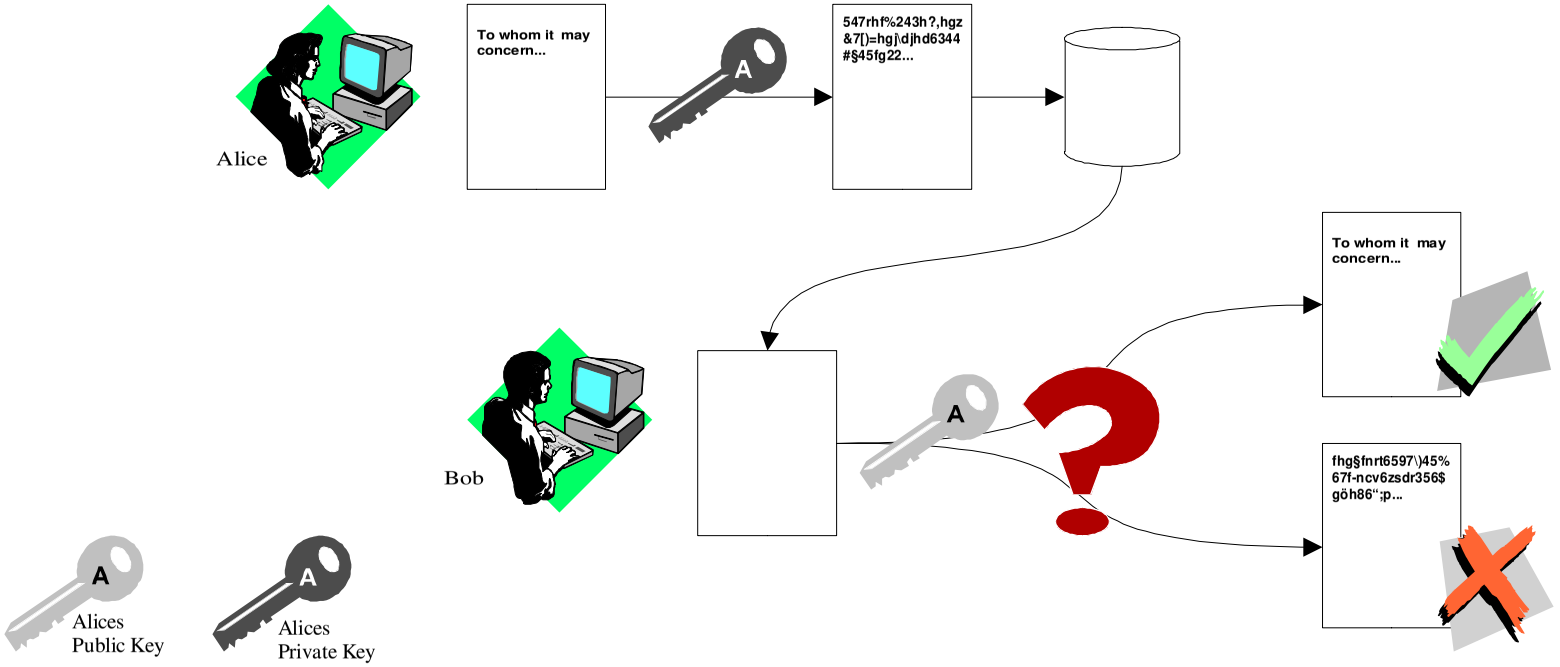
Nachteile:

- hoher Verfahrensaufwand
- Problem der sicheren Zuordnung zwischen öffentlichem Schlüssel und Eigentümer

Digitale Signaturen (1)

- Spezielle Anwendung asymmetrischer Verfahren zur Realisierung einer digitalen Signatur
- Funktionen der Unterschrift müssen elektronisch nachgebildet werden

Erster Ansatz:



Digitale Signaturen (2)

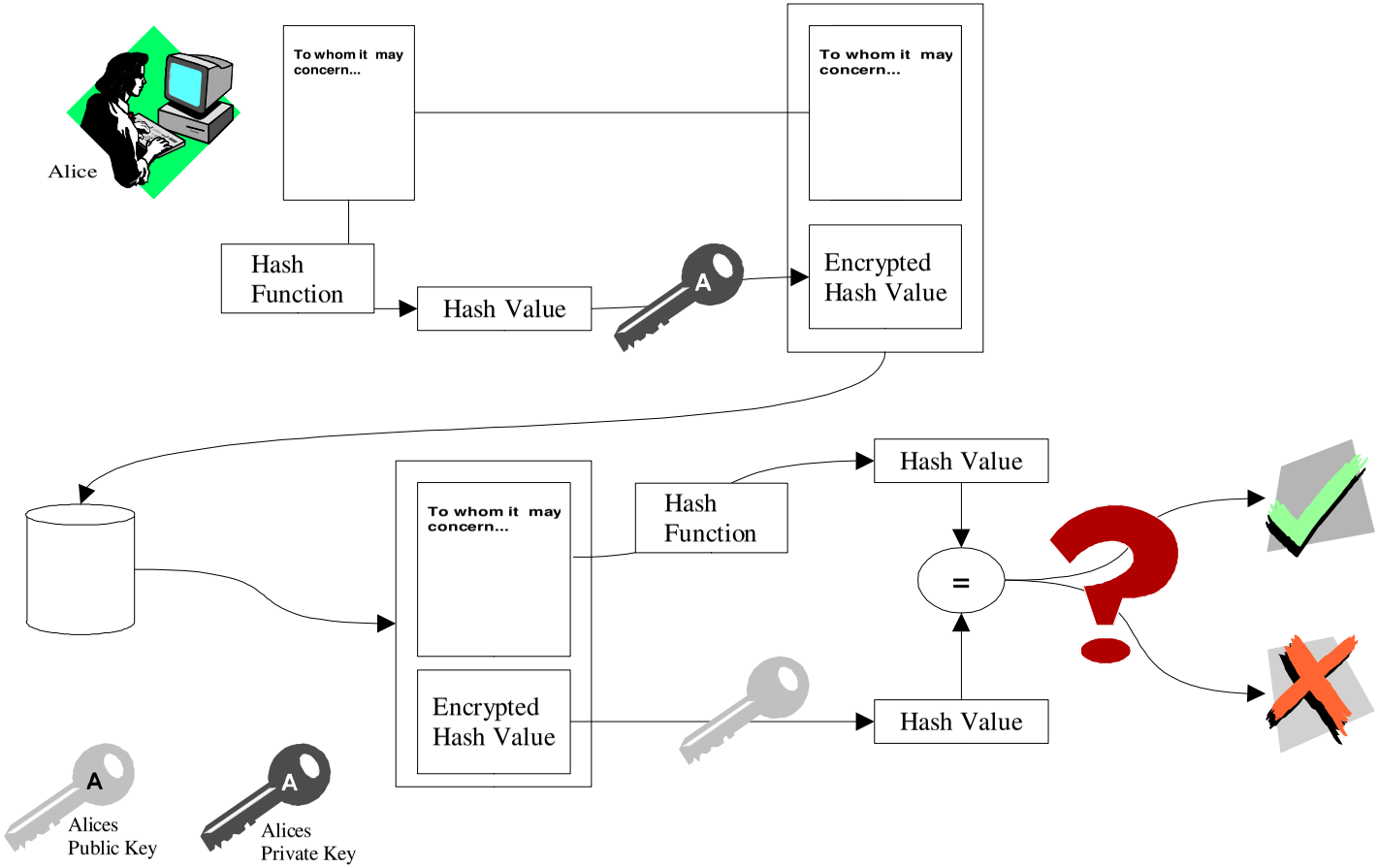
- Verschlüsselung des zu signierenden Dokuments mit privatem (!) Schlüssel
- Bestätigung der Authentizität durch korrekte Entschlüsselung mit öffentlichem Schlüssel

Nachteile:

- Einheit von Signatur und zu signierendem Dokument
- hoher Verschlüsselungsaufwand
- Problem der unsicheren Zuordnung von Schlüssel und Eigentümer

Digitale Signaturen (3)

Zweiter Ansatz:



Digitale Signaturen (4)

- Generierung eines Hashwertes aus zu signierendem Dokument
- Verschlüsselter Hashwert als digitale Signatur
- hohe Anforderungen an die Hashfunktion
- Hash-Funktionen bei PGP: MD5, SHA-1

Vorteile:

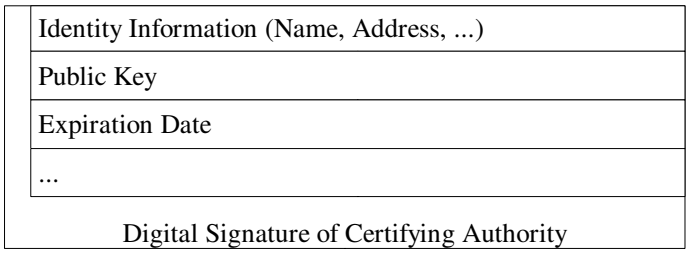
- logische Trennung von Signatur und zu signierendem Dokument
- geringer Verschlüsselungsaufwand

Nachteil:

- Problem der unsicheren Zuordnung von Schlüssel und Eigentümer noch immer nicht gelöst

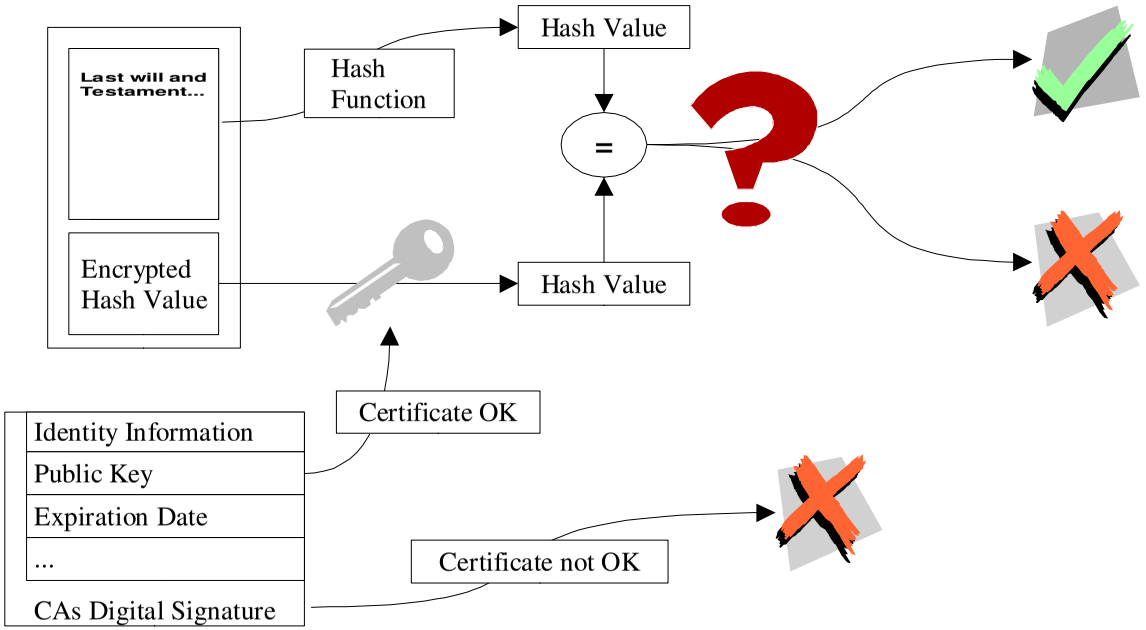
Digitale Zertifikate (1)

- Ermöglichung einer sicheren Zuordnung zwischen öffentlichem Schlüssel und Eigentümer
- Voraussetzung zur Erfüllung der Identifikationsfunktion
- Hinzuziehen einer vertrauenswürdigen Partei



- vertrauenswürdige Partei bestätigt durch digitale Signatur Identität und öffentlichen Schlüssel des Zertifikatinhabers
- öffentlicher Schlüssel der vertrauenswürdigen Partei muß als sicher gelten
- digitales Zertifikat als "elektronischer Personalausweis"
- Zertifikatausstellung nach Authentisierung und Vorlage eines öffentlichen Schlüssels
- Bedarfsweise Übermittlung durch Zertifikat-inhaber oder durch Zugriff auf Zertifikatsserver

Digitale Zertifikate (2)



- Zertifikatsprüfung wie bei Prüfung digitaler Signaturen
- erfolgreiche Zertifikatsprüfung bestätigt den öffentlichen Schlüssel des Zertifikatinhabers

Digitale Zertifikate (3)

- Aufnahme weiterer Informationen in das digitale Zertifikat:
  - Verfalldatum
  - Ausstelldatum
  - Seriennummer
  - Informationen über Aussteller
  - Art des öffentlichen Schlüssels
  - ...

- X.509 als wichtiger Standard für digitale Zertifikate
- große Verbreitung von PGP-Zertifikaten

Trustmodelle (1)

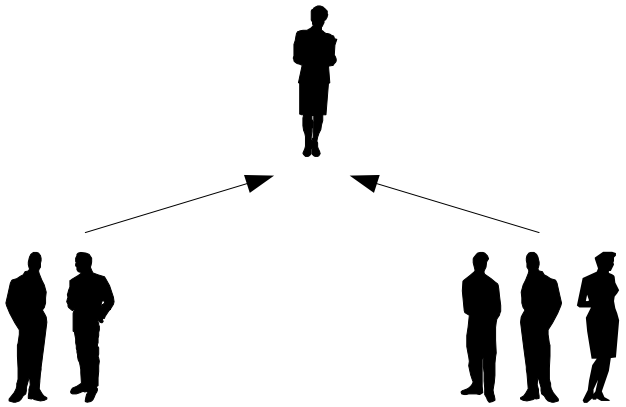
- Zertifikatausstellung setzt prinzipiell lediglich asymmetrisches Schlüsselpaar und Fähigkeit zum digitalen Signieren voraus
- Zertifizierung kann auch verkettet (in "Zertifizierungspfaden") erfolgen
- es ergeben sich verschiedene Zertifizierungsszenarien (Trustmodelle)

Direct Trust

- Trustpartner kennen sich und haben öffentliche Schlüssel selbst ausgetauscht
- keine Relevanz von Zertifikaten

Trustmodelle (2)

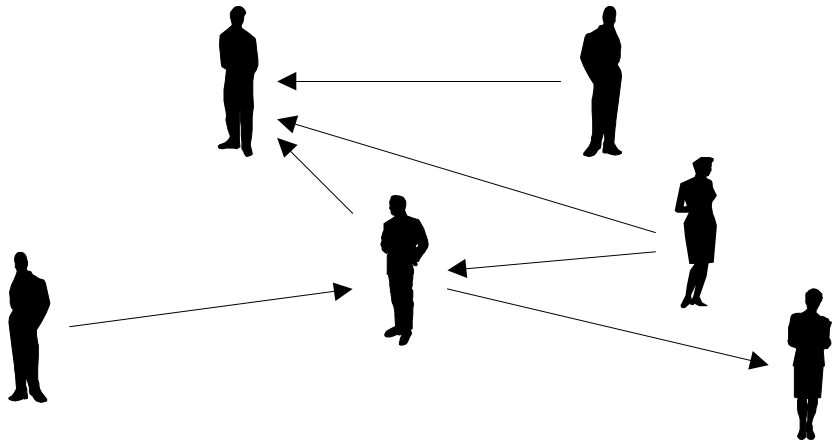
Hierarchical Trust



- zertifizierende Stellen lassen sich in Ebenen einteilen
- jede Stelle kann sich nur bei einer Stelle höherer Ebene zertifizieren lassen
- Vertrauen zu Teilnehmer des Hierarchical Trust durch Direct Trust zur Wurzelinstanz
- Vertrauen als transitive Eigenschaft
- abnehmende Sicherheit bei langen Zertifikatsketten (größte Sicherheit durch flache Hierarchien)

Trustmodelle (3)

Web of Trust



- keine Einschränkungen bei gegenseitiger Zertifizierung
- Verwendung in PGP
- Problem der Speicherung der Zertifikate
- Wie kann ein gültiger Zertifizierungspfad gefunden werden?
- Was passiert bei Invalidierung von Zertifikaten?

Signaturgesetz (1)

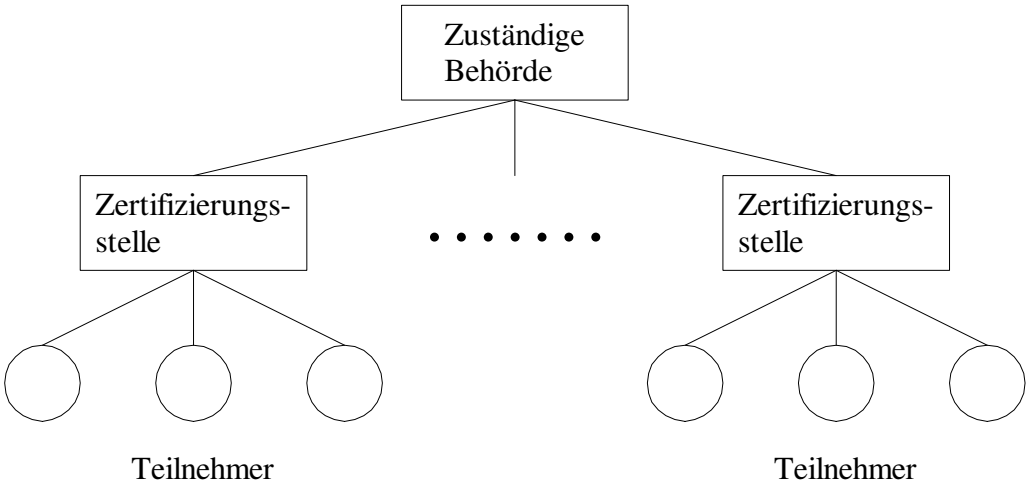
- viele Freiheitsgrade durch verschiedene Trustmodelle, Zertifikatstypen, kryptographische Verfahren
- gesetzliche Regulierung zur Garantie von Sicherheit notwendig
- gesetzliche Regulierung als Voraussetzung zur Gleichstellung der digitalen Signatur mit der eigenhändigen Unterschrift

Signaturgesetz (1997)

- erstmals in Deutschland gesetzliche Regulierung für Einsatz digitaler Signaturen
- spezielle Anforderungen an Zertifikate
- strenge Vorschriften für Zertifizierungsstellen (Genehmigungspflicht)
- Vorgabe des Trustmodells (2-stufig, hierarchisch)
- zentrale Wurzelinstanz
- Signaturgesetz-konforme digitale Signaturen
- keine Gleichstellung mit handschriftlicher Unterschrift („freie Beweiswürdigung“)

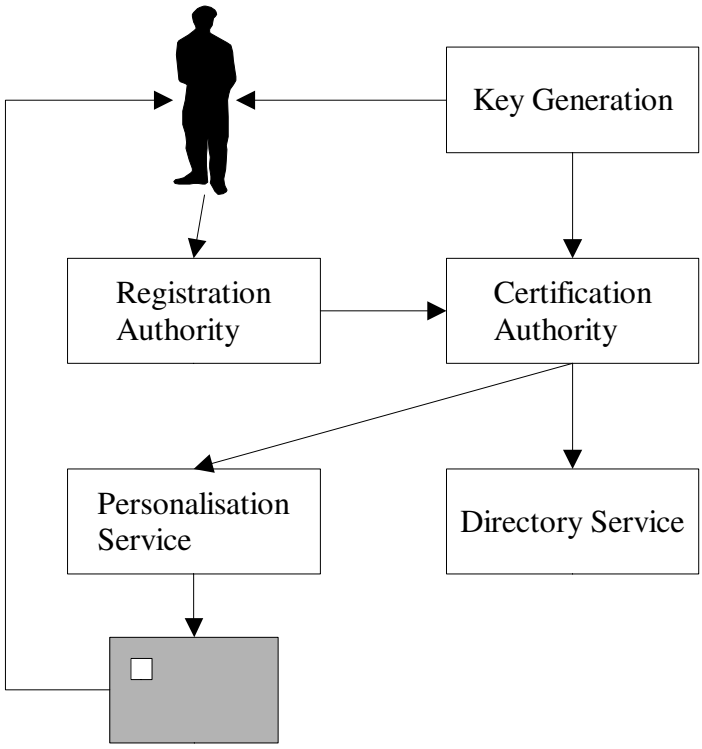
Signaturgesetz (2)

Zertifizierungshierarchie nach Signaturgesetz



Signaturgesetz (3)

- Signaturverordnung regelt Detailanforderungen an Zertifizierungsstellen
- Regulierung der Dienste und des Ablaufs in Zertifizierungsstellen
- Zeitstempeldienste



Nachteile Signaturgesetz (1997):

- hoher Zertifizierungsaufwand (=hohe Kosten)
- lediglich nationaler Ansatz
- freie Beweiswürdigung digitaler Signaturen

Signaturgesetz (4)

- neues Signaturgesetz vom 22. Mai 2001 setzt EU-Richtlinie für "Gemeinsame Rahmenbedinungen für elektronische Signaturen" vom 13.12.1999 in national geltendes Recht um
- europaweite Regulierung des Einsatzes digitaler Signaturen
- Gleichstellung mit ausländischen Signaturen, die die EU-Richtlinien erfüllen
- Einführung von drei Signaturtypen:
  - elektronische Signaturen
  - fortgeschrittene elektronische Signaturen
  - qualifizierte elektronische Signaturen
- Wegfall des Genehmigungsverfahrens (freiwillige Akkreditierung möglich)
- Pflicht zur Deckungsvorsorge in Höhe von jeweils mindestens EUR 250.000 bzw. DM 500.000
- Gleichstellung von qualifizierten elektronischen Signaturen mit der eigenhändigen Unterschrift

Zusammenfassung

- Bedeutung der Unterschrift für Rechtssicherheit
- Schaffung eines digitalen Äquivalents der Unterschrift als Voraussetzung für rechtssicheren E-Commerce
- zentrale Rolle von kryptographischen Verfahren bei der Konstruktion digitaler Signaturen
- Notwendigkeit von digitalen Zertifikaten
- Trustmodelle als Infrastruktur zur Zertifikatsverteilung und zur Bildung von Vertrauen
- Signaturgesetz als Voraussetung zur Schaffung von Rechtssicherheit
- Verunsicherung durch verschiedene Signaturtypen und aufgelockerte Anforderungen an Zertifizierungsstellen
- Gleichstellung von qualifizierten elektronischen Signaturen mit der eigenhändigen Unterschrift