Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 2b)

Vorlesung im Sommersemester 2011

an der Universität Ulm

von Bernhard C. Witt

2. Grundlagen der IT-Sicherheit

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes	✓	Anforderungen zur IT-Sicherheit
✓	Datenschutzrechtliche Prinzipien	➔	Mehrseitige IT-Sicherheit
✓	Technischer Datenschutz		Risiko-Management
✓	Kundendatenschutz		Konzeption von IT-Sicherheit

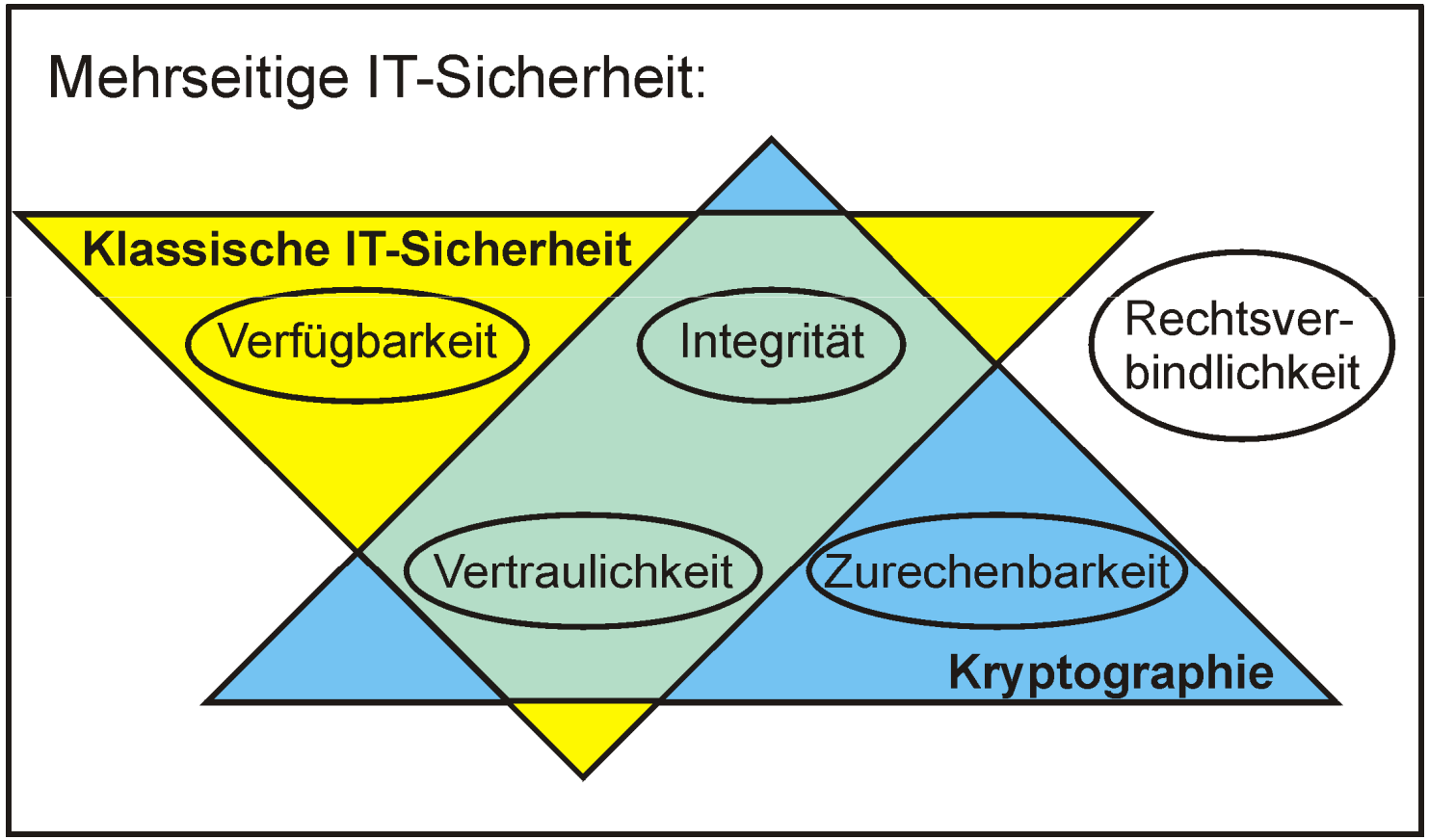
Mehrseitige IT-Sicherheit:

- Kennzeichen mehrseitiger IT-Sicherheit
- Ziele mehrseitiger IT-Sicherheit
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
  - Zurechenbarkeit
  - Rechtsverbindlichkeit

Mehrseitige IT-Sicherheit (1)

- 1997: „Duale“ bzw. „Mehrseitige“ IT-Sicherheit entwickelt vom Ladenburger Kolleg „Sicherheit in der Kommunikationstechnik“
- Erweiterung der klassischen Sicherheitsziele, die der Verlässlichkeit der IT-Systeme dienen, um Komponenten zur Beherrschbarkeit der IT-Systeme (→ Integration der Betroffenensicht) → komplementäre Sicht
- **Verlässlichkeit** = keine unzulässige Beeinträchtigung der IT-Systeme, Daten bzw. Funktionen/Prozessen im Bestand, ihrer Nutzung oder ihrer Verfügbarkeit
- **Beherrschbarkeit** = keine unzulässige Beeinträchtigung von Rechten oder schutzwürdigen Belangen der Betroffenen durch Vorhandensein oder Nutzung von IT-Systemen

Mehrseitige IT-Sicherheit (2)



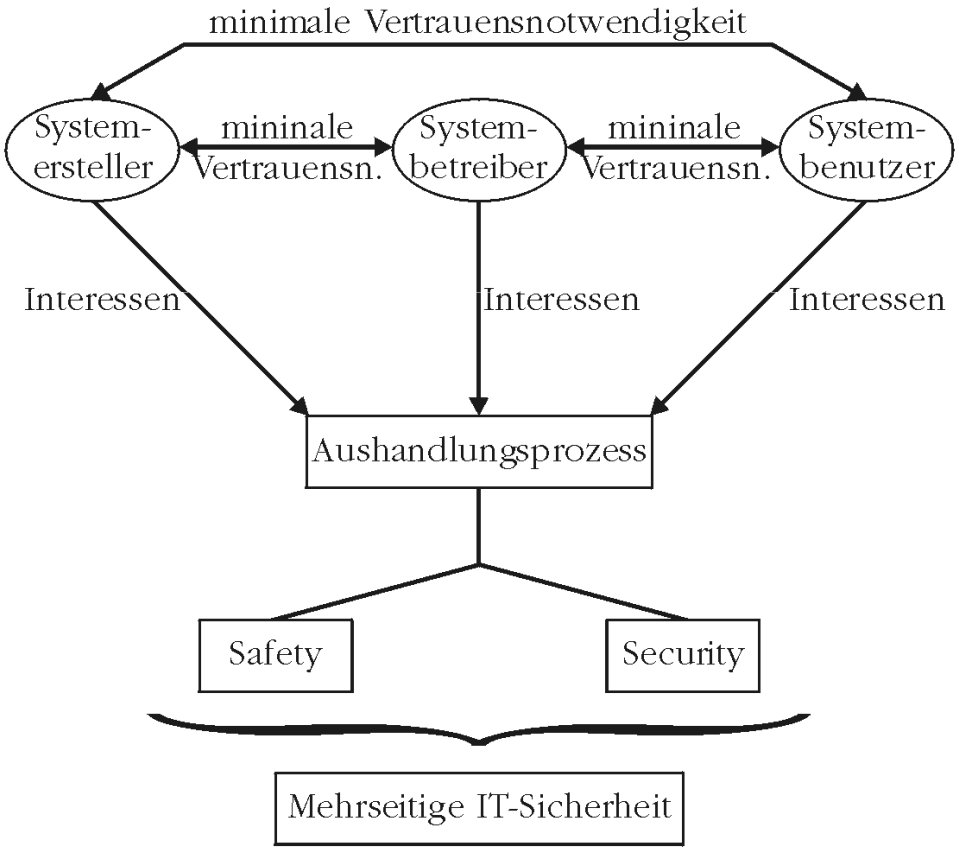
Mehrseitige IT-Sicherheit (3)

Definition 11: Mehrseitige IT-Sicherheit

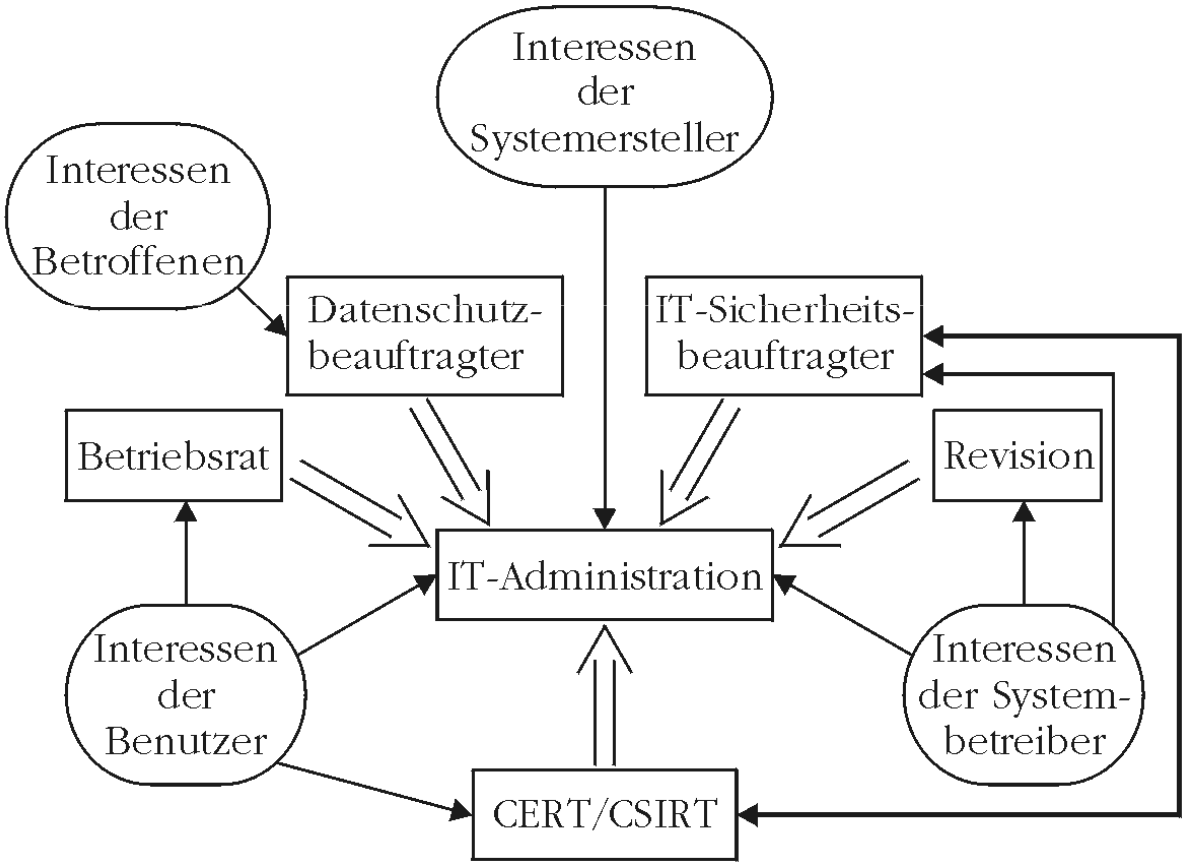
Schutz von Hardware, Software und Daten vor Gefährdungen vereinbarter Verfügbarkeit, Integrität, Vertraulichkeit, Zurechenbarkeit und Rechtsverbindlichkeit

- Mehrseitige IT-Sicherheit erfordert die Einbeziehung der Schutzinteressen aller Beteiligten:
  - → Formulierung der spezifischen Sicherheitsinteressen
  - → Erkennen der zu lösenden Schutzkonflikte
  - → Aushandlung zur Auflösung dieser Konflikte
  - → Durchsetzung eigener Sicherheitsinteressen (Kompromiss)
- **Grundsatz**: Sicherheit mit minimalen Annahmen über andere (d.h.: möglichst wenig Vertrauen in andere setzen müssen)

Mehrseitige IT-Sicherheit (4)



Akteure zur IT-Sicherheit



Ziele mehrseitiger IT-Sicherheit (1)

Definition 12: Verfügbarkeit (availability)

Gewährleistung, dass das IT-System (für befugte Nutzer) zugänglich und funktionsfähig ist

→ Prozessausführung in vorgesehener Weise zum geplanten Zeitpunkt im vorgegebenen Zeitrahmen

→ Sicherung vor Ausfällen und ungewolltem Verlust

→ betrifft auch die Vollständigkeit des Datenbestands (Nutzdaten, Passwortdaten, Konfigurationsdaten & Protokolldaten)

Berechnung der Verfügbarkeit (1)

$$\text{Verfügbarkeit einer IT-Komponente} = \frac{(\text{vereinbarte Servicezeit} - \text{Ausfallzeit})}{\text{vereinbarte Servicezeit}} \text{ [in \%]}$$

$$\text{Verfügbarkeit eines Dienstes} = \frac{\text{MTBF}}{(\text{MTBF} + \text{MTTR})}$$

Hinweis:

- MTBF = "mean time between failures" (= Gesamtbetriebszeit / Gesamtzahl aufgetretener Fehler); MTTR = "mean time to repair“ (= Gesamtreparaturzeit / Gesamtzahl aufgetretener Fehler)
- bei der vereinbarten Servicezeit (wie auch der Gesamtbetriebszeit) werden vereinbarte Wartungszeiten nicht berücksichtigt, da Systemausfälle in diesem Zeitraum ausdrücklich durch die getroffene Vereinbarung abgedeckt sind („geplante Nichtverfügbarkeit“)

Berechnung der Verfügbarkeit (2)

Berücksichtigung **technischer Redundanzen** durch:

$$\text{Redundanz-Verfügbarkeit} = 1 - (1 - \text{Verfügbarkeit}_{\text{normal}})^{\text{Anzahl}}$$

- besonders kritische IT-Systeme können durch technische Redundanz eine deutlich höhere Verfügbarkeit erhalten (Parallelität statt Seriellität!)
- die Angabe von Verfügbarkeiten ist vor allem im Rahmen von **Service Level Agreements** (SLAs) wichtig; Ausfallzeiten (durch unbeabsichtigte Ereignisse & Angriffe) sind teuer
- bei Auftreten von Ausfallzeiten hängt einiges davon ab, welche „Reaktionszeiten“ (bis wann wird auf die Meldung reagiert?) und „Problembeseitigungszeiten“ (bis wann ist das gemeldete Problem behoben?) mit einem entsprechenden Serviceunternehmen vereinbart wurden

Ziele mehrseitiger IT-Sicherheit (2)

Definition 13: Vertraulichkeit (confidentiality)

Gewährleistung, dass die Daten des IT-Systems nur durch befugte Nutzer interpretiert werden

- → kein unbefugter Informationsgewinn
- → Daten für Unbefugte nicht zugänglich (auch nicht über verdeckte Kanäle)
- → ergänzt durch Anonymität/Pseudonymität, Unbeobachtbarkeit & Verdecktheit aus Kommunikationstechnik

Ziele mehrseitiger IT-Sicherheit (3)

Definition 14: Integrität (integrity)

Gewährleistung, dass die Daten des IT-Systems nur durch befugte Nutzer verändert werden

- → Vorliegen korrekter (= originalgetreuer und unverfälschter) und aktueller Daten
- → Feststellbarkeit von Manipulationen (Datenqualität)
- → zielt auf die Vollständigkeit des Datenbestandes ab
- → Anforderungen an disaster recovery

Sicherung der Integrität

- Ein Nachweis von Integrität erfolgt z.B. mittels Authentifizierungs-mechanismen
- Ebenso im Einsatz vor allem zur Vermeidung ungewollter Manipulationen: fehlerkorrigierender Code & verschiedene Fehlermeldeverfahren
- Die Zuverlässigkeit von IT-Komponenten kann durch entsprechende Zertifikate (Common Criteria) nachgewiesen werden
- Protokollierungen erforderlich für Datenqualität
- Revisionssicherheit z.B. durch Abspeichern auf nur einmal beschreibbaren Datenträgern

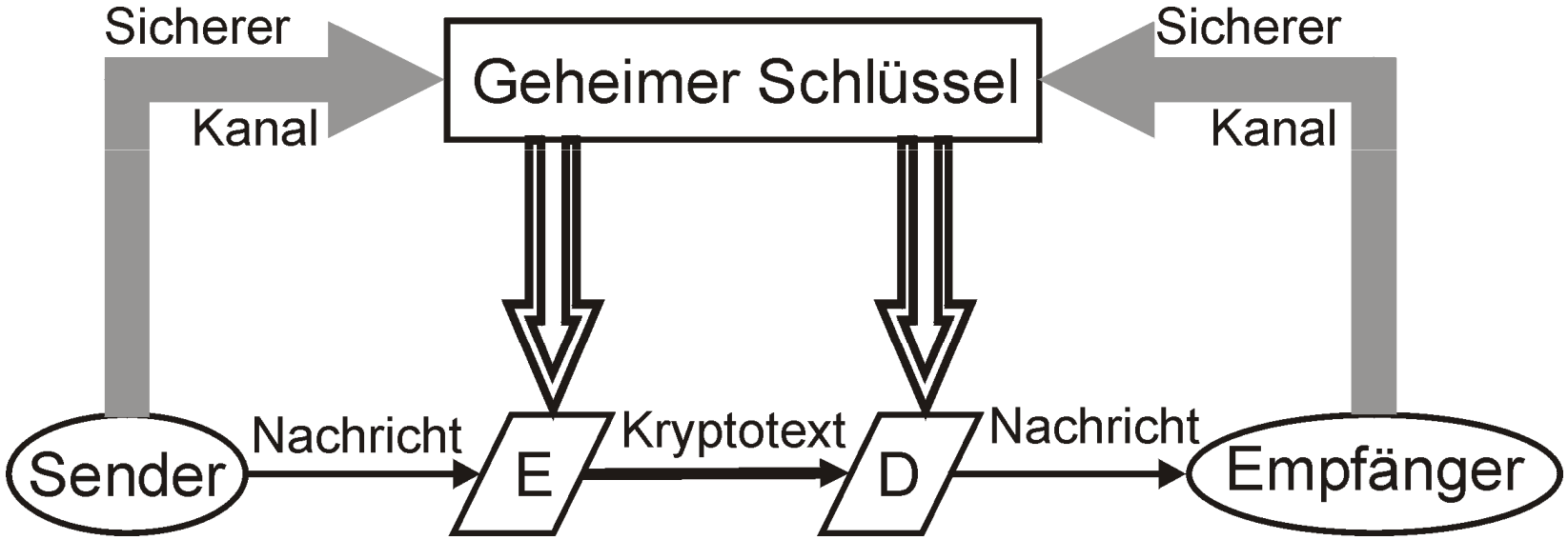
Hinweis:

Authentisierung = Nachweis einer Identität

Authentifizierung = Überprüfung einer Identität

Autorisierung = Gewährung von Zutritts-/Zugangs-/Zugriffsrechten

Symmetrische Verschlüsselung

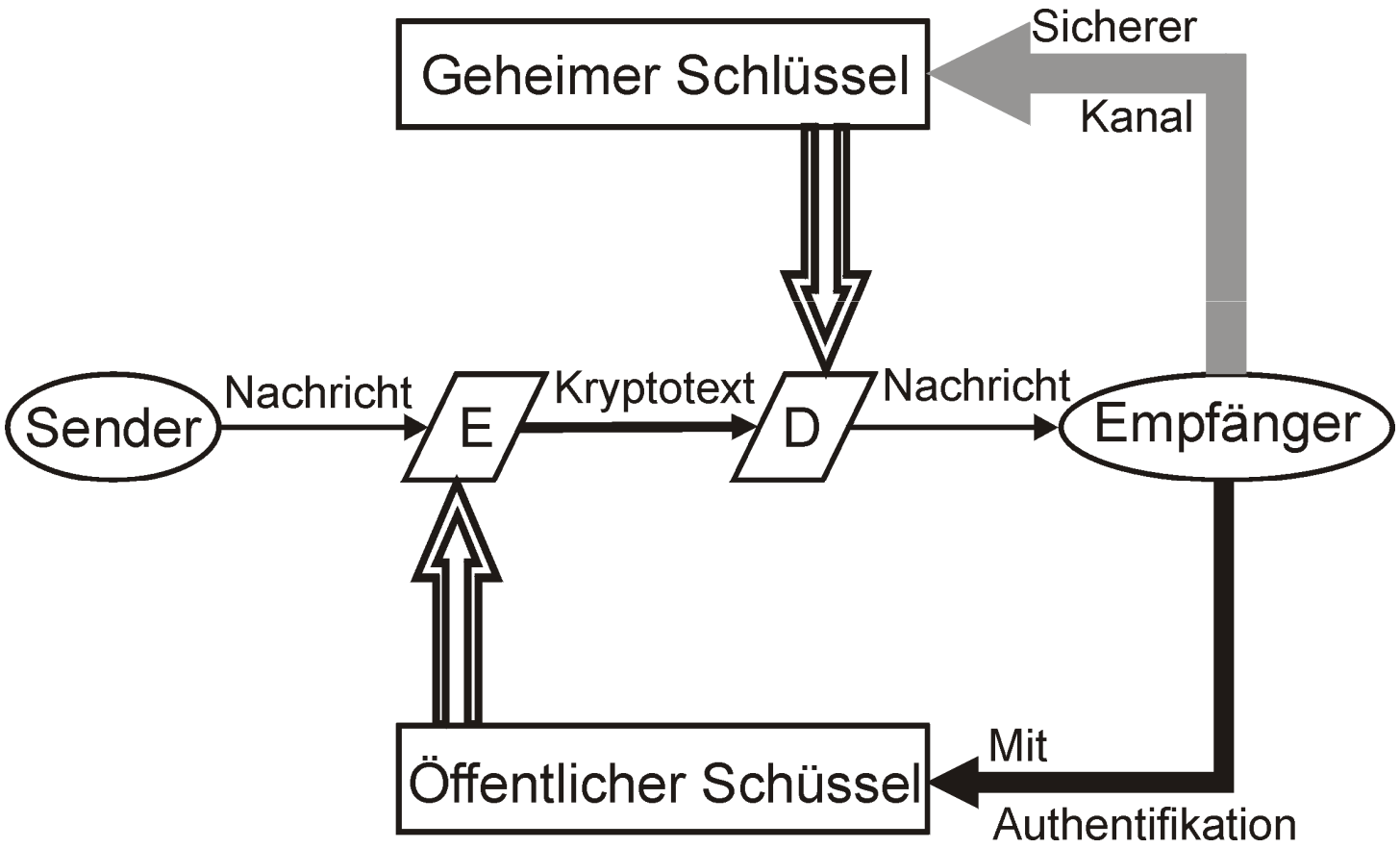


Beispiel: Symmetrische Verschlüsselung

Sender:					
Klartext:	1	0	1	1	
+ Schlüssel:	1	1	0	1	[XOR]
= Chiffre:	0	1	1	0	

Empfänger:					
Chiffre:	0	1	1	0	
- Schlüssel:	1	1	0	1	[XOR]
= Klartext:	1	0	1	1	

Asymmetrische Verschlüsselung



Beispiel: Asymmetrische Verschlüsselung (1)

Verfahren nach Rivest, Shamir und Adleman (RSA):

Ausgangspunkt für Empfänger (!):

- wähle zwei Primzahlen p + q; z.B. p=3 und q=7
- berechne das Produkt dieser Primzahlen und dessen Eulerschen Funktionswert;
  $n=p*q=3*7=21$ und $\varphi(n)=(p-1)*(q-1)=2*6=12$
- wähle zufällig den geheimen Dechiffrierschlüssel d, für den gilt: $ggT(d, \varphi(n))=1$; z.B. d=5
- berechne den zu d gehörenden öffentlichen Chiffrierschlüssel e, für den gilt: $d*e \equiv 1 \bmod \varphi(n)$; $5*e \equiv 1 \bmod 12 \rightarrow e=17$ ($5*17=85=7*12+1$); Anm: empfohlen sind e=3, e=17, e=65537
- veröffentliche n und e

Beispiel: Asymmetrische Verschlüsselung (2)

Sender: (e=17, n=21)			
Klartext:	10	11	
Chiffre:	19	2	$c_i=(m_i)^e \bmod n$

Empfänger: (d=5, n=21)			
Chiffre:	19	2	
Klartext:	10	11	$m_i=(c_i)^d \bmod n$

Vergleich der Verschlüsselungen

Symmetrisch:

- Gängige Verfahren:
  one-time-pad, AES, DES,
  Triple-DES
- Typische Schlüssellänge:
  128 – 256 Bit-Schlüssel „auf absehbare Zeit“ sicher
- Performanz:
  mind. um Faktor 100
  schneller als asymmetrisch
- Ziel:
  Sicherung d. **Vertraulichkeit**

Asymmetrisch:

- Gängige Verfahren:
  RSA, ElGamal
- Typische Schlüssellänge:
  1024 – 4096 Bit-Schlüssel
  (entspricht etwa 128 – 256 Primzahlen)
- Performanz:
  stark vereinfachter Schlüsselaustausch
- Ziel:
  Sicherung d. **Vertraulichkeit**

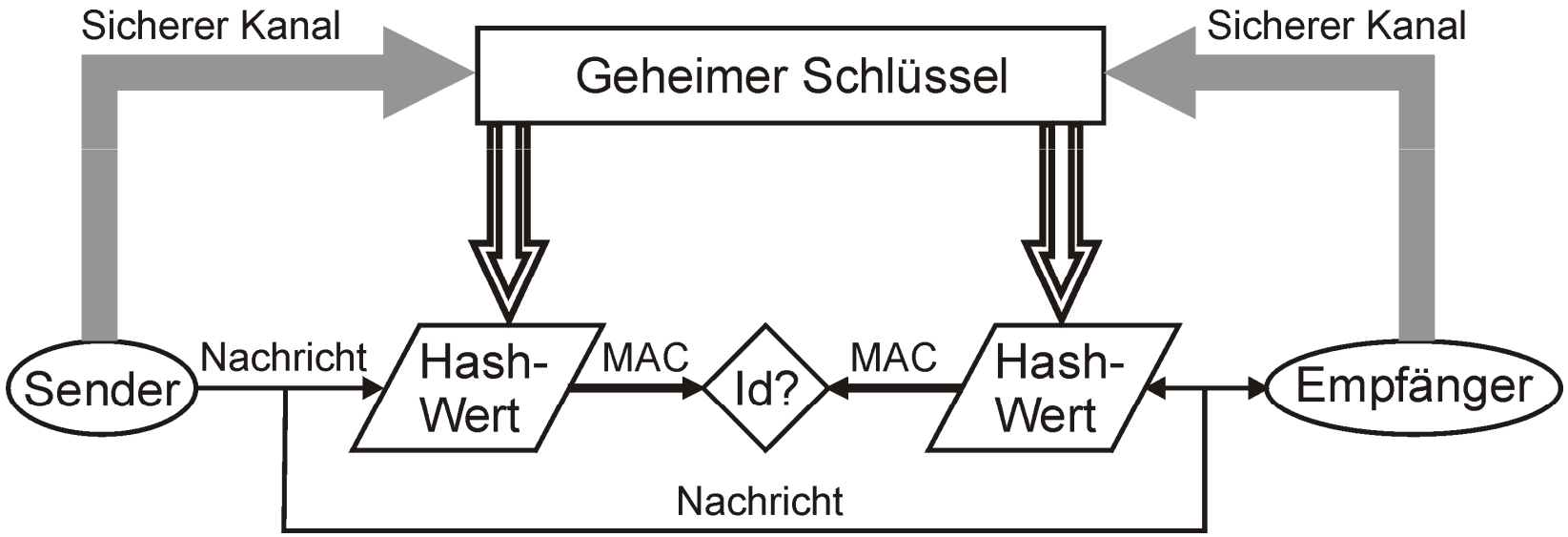
Ziele mehrseitiger IT-Sicherheit (4)

Definition 15: Zurechenbarkeit (accountability)

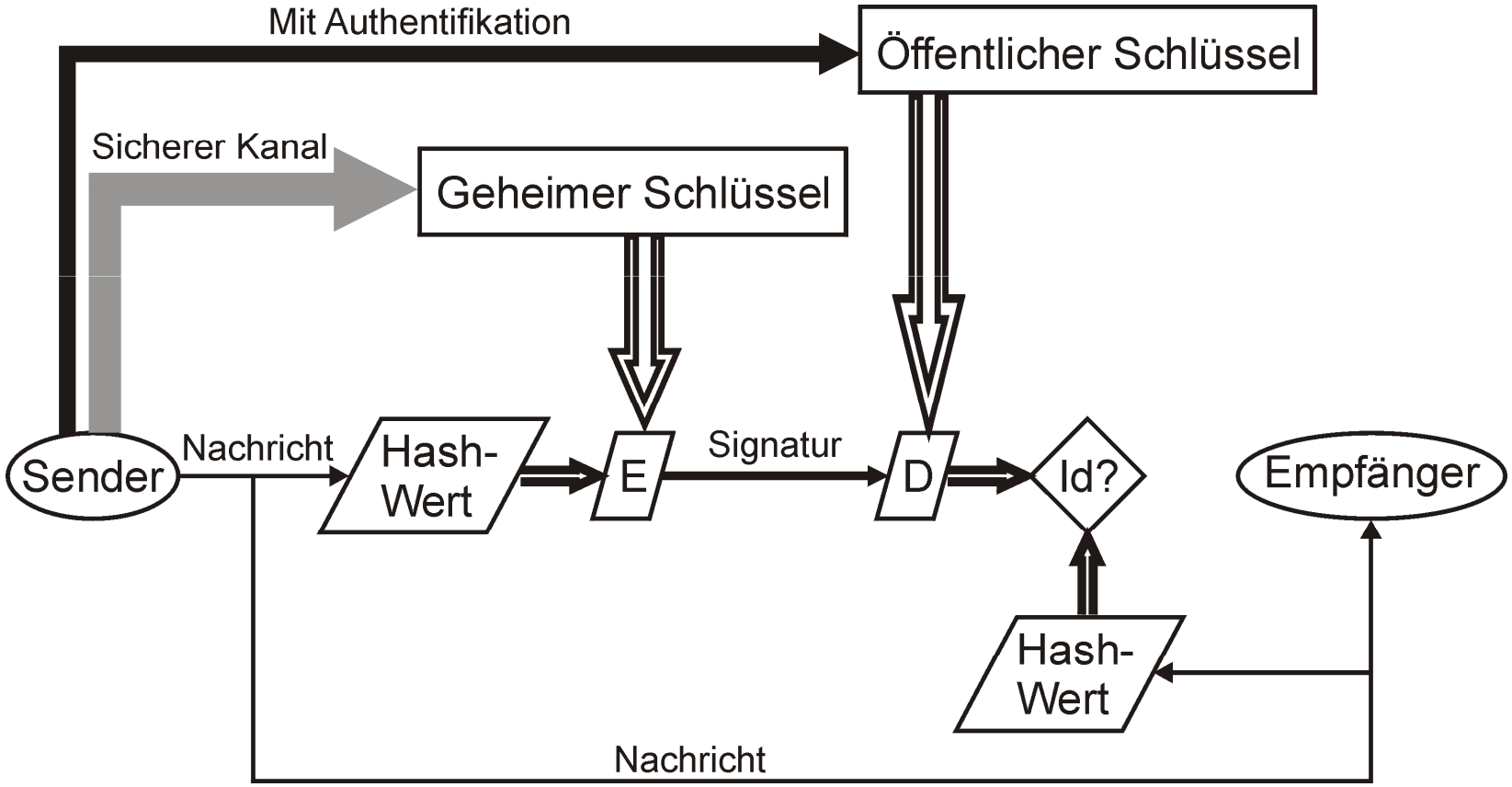
Gewährleistung, dass jederzeit festgestellt werden kann, welcher Nutzer einen Prozess ausgelöst hat

- → Verantwortlichkeit & Authentizität (Glaubwürdigkeit)
- → Diese Daten kommen vom betreffenden Kommunikations-partner
- → Die betreffenden Daten kommen von diesem Kommunikations-partner
- → Kern des Rechtemanagements

Symmetrische Authentifikation: Message Authentication Code



Asymmetrische Authentifikation: Digitale Signatur



Vergleich der Authentifikationen

Symmetrisch:

- Gängige Verfahren:
  SecurID, GSM-Authentikation
- Ziel:
  Sicherung d. **Integrität**
- Key-Recovery sinnvoll:
  Hinterlegung des Entschlüsselungsschlüssels zur Vorbeugung gegen Schlüsselverlust

Asymmetrisch:

- Gängige Verfahren:
  RSA, ElGamal, DSS, DSA
- Ziel:
  Sicherung d. **Integrität** & **Zurechenbarkeit**
- erfüllt Anforderungen zur fortgeschrittenen Signatur nach SigG, sofern geheimer Schlüssel unter alleiniger Kontrolle des Schlüsselinhabers (qualifizierte Signatur, wenn zertifiziert und mit sicherer Einheit erzeugt)

Ziele mehrseitiger IT-Sicherheit (5)

Definition 16: Rechtsverbindlichkeit (legal liability)

Gewährleistung, dass Daten und Vorgänge gegenüber Dritten jederzeit rechtskräftig nachgewiesen werden können

→ Transparenz (Nachvollziehbarkeit)

→ Reversibilität & Verhinderung falschen Abstreitens

→ Nachweis zugesicherter Eigenschaften (assurance)

→ Voraussetzung für Auditierbarkeit

→ Ausgleich für fehlenden klassischen Augenscheinbeweis