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

Vorlesung im Sommersemester 2019

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

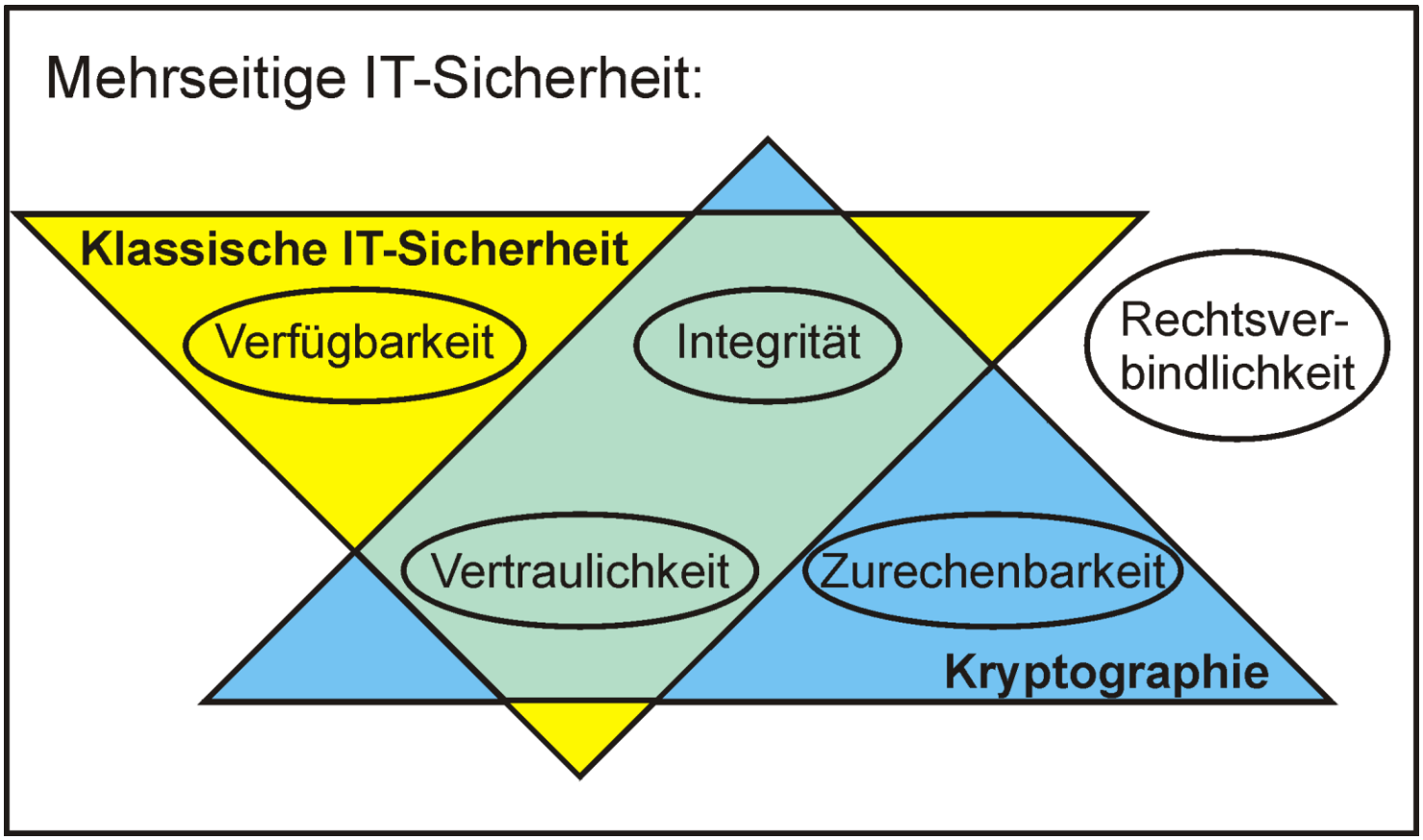
Mehrseitige IT-Sicherheit:

- 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
  → Sicherheit der Systeme
- **Beherrschbarkeit** = keine unzulässige Beeinträchtigung von Rechten oder schutzwürdigen Belangen der Betroffenen durch Vorhandensein oder Nutzung von IT-Systemen
  → Sicherheit vor den Systemen

Mehrseitige IT-Sicherheit (2)



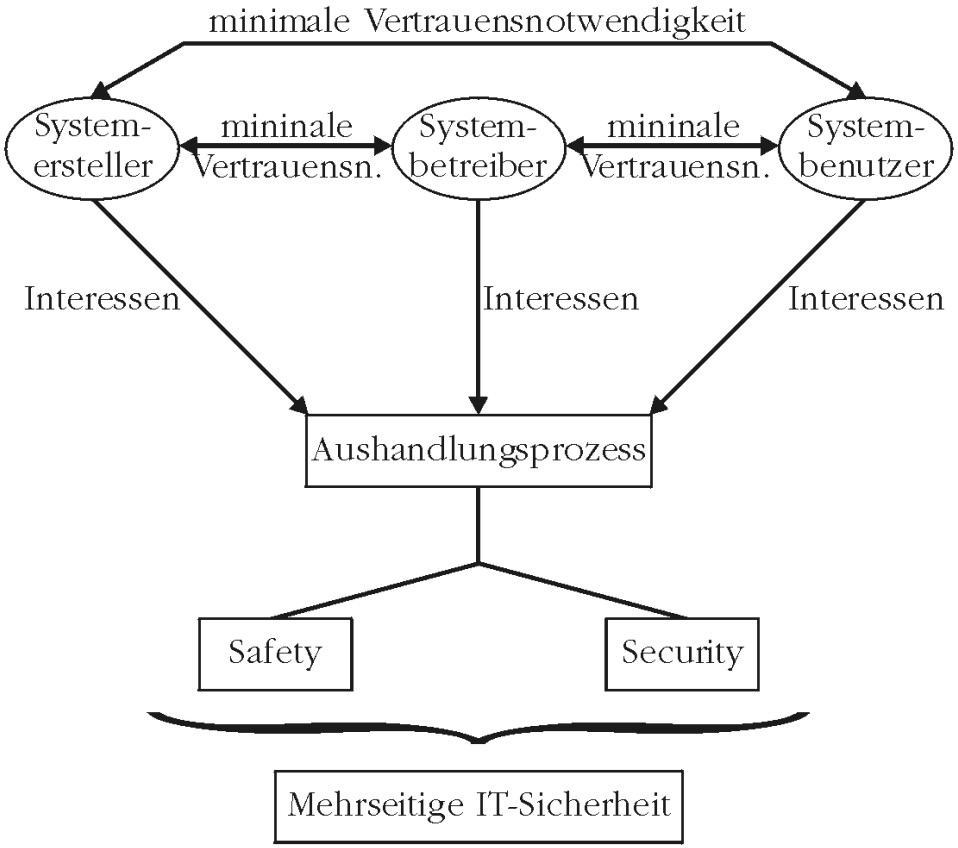
Mehrseitige IT-Sicherheit (3)

Definition 10: Mehrseitige IT-Sicherheit

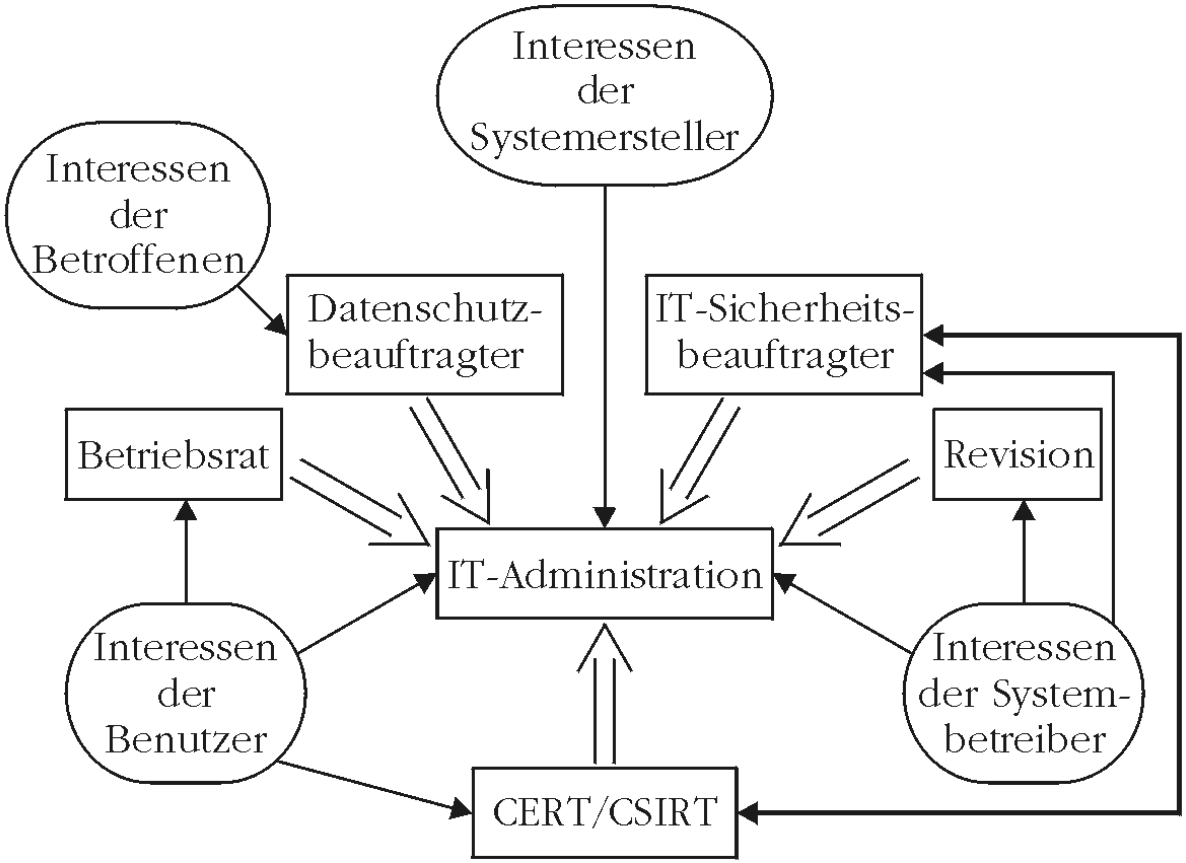
Schutz von Hardware, Software und Daten vor Gefährdungen vereinbarter Verfügbarkeit, Integrität, Vertraulichkeit, Zurechenbarkeit und Rechtsverbindlichkeit

- 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**: Vereinbarte (!) IT-Sicherheit mit minimalen (!) Annahmen über andere (d.h.: möglichst wenig Vertrauen in andere setzen müssen)

Mehrseitige IT-Sicherheit (4)



Akteure zur IT-Sicherheit



Klassische IT-Sicherheit vs Mehrseitige IT-Sicherheit

Klassische IT-Sicherheit:

- **Verfügbarkeit**
- **Integrität**
- **Vertraulichkeit**

→ Vermeidung unzureichender Beeinträchtigungen der IT-Systeme, Daten, Funktionen und Prozesse in Bestand, Nutzung oder Verfügbarkeit

→ Verlässlichkeit der IT-Systeme

→ Sicherheit der Systeme

Mehrseitige IT-Sicherheit:

- klassische IT-Sicherheit
- ergänzt um **weitere Sicherheitsziele** (Zurechenbarkeit & Rechtsverbindlichkeit)

→ Berücksichtigung der Interessen aller Beteiligten

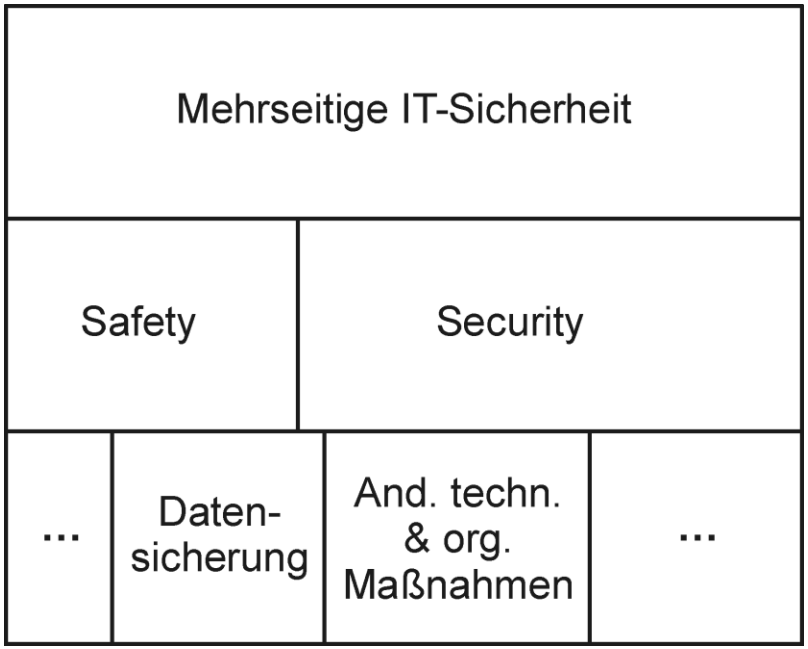
→ Verlässlichkeit und Beherrschbarkeit der IT-Systeme

→ Sicherheit der Systeme und vor den Systemen

Abgrenzung zwischen IT-Sicherheit & Datensicherheit

- Schutz vor unbeabsichtigten Ereignissen: **Safety**
  ≠ Safety-Begriff im Sinne des Schutzes vor Personenschaden!
- Schutz gegen beabsichtigte Angriffe: **Security**

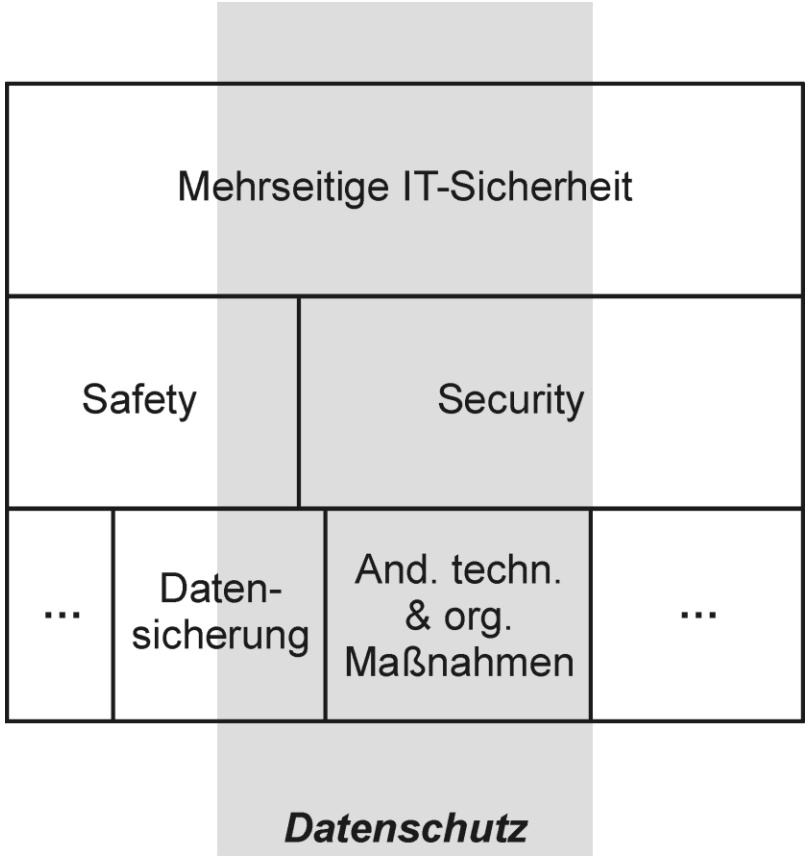
→ **IT-Sicherheit = Safety + Security**



Abgrenzung zwischen IT-Sicherheit & Datensicherheit

Zusammenhang zwischen mehrseitiger IT-Sicherheit und Datenschutz:

- Überschneidung bei der Verarbeitung personenbezogener Daten
- **Schwerpunkt liegt auf Security**



Sicherheitsziele im Vergleich

	Vertraulich-keit	Integrität	Verfügbar-keit	Authentizität	Verbindlich-keit
Mehrseitige IT-Sicherheit	**X**	**X**	**X**	X	X
EU-DSGVO	**X**	**X**	**X**		(X)
IT-Sicher-heitsgesetz	**X**	**X**	**X**	X	
MaRisk	**X**	**X**	**X**	X	
IT-Grund-schutz	**X**	**X**	**X**		
ISO/IEC 27001	**X**	**X**	**X**	(X)	
V-Modell XT	**X**	**X**	**X**		X

Ziele mehrseitiger IT-Sicherheit (1)

Definition 11: Verfügbarkeit (availability)

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

- → **ISO/IEC 27000**: property of being accessible and usable upon demand by an authorized entity
- → 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** (parallele Systeme) durch:

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

$$\text{Verfügbarkeit}_{\text{bauungleich}} = 1 - \Pi\ (1 - \text{Verfügbarkeit}_{\text{normal}} \text{ der Komponente i})$$

- 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

Berechnung der Verfügbarkeit (3)

Berücksichtigung **Gesamtverfügbarkeit** durch:

Verfügbarkeit IT-Verbund = Π (Verfügbarkeit aller IT-Komponenten)

- Die Einzelverfügbarkeiten werden also miteinander multipliziert
- Je komplexer ein IT-Verbund also ist, desto ausfallanfälliger ist er insgesamt, wenn er keinerlei Redundanzen aufweist
- Im Zuge einer Parallel-Schaltung von IT-Systemen wird die Nicht-Verfügbarkeit eines IT-Systems ggf. durch eine vorhandene Verfügbarkeit eines anderen IT-Systems ausgeglichen (vorausgesetzt, das redundante IT-System ist tatsächlich aktiver Teil des Clusters und nicht nur als Cold-Stand-by konzipiert)
- Bei Hochverfügbarkeit muss Redundanz standort-übergreifend realisiert sein

Ziele mehrseitiger IT-Sicherheit (2)

Definition 12: Vertraulichkeit (confidentiality)

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

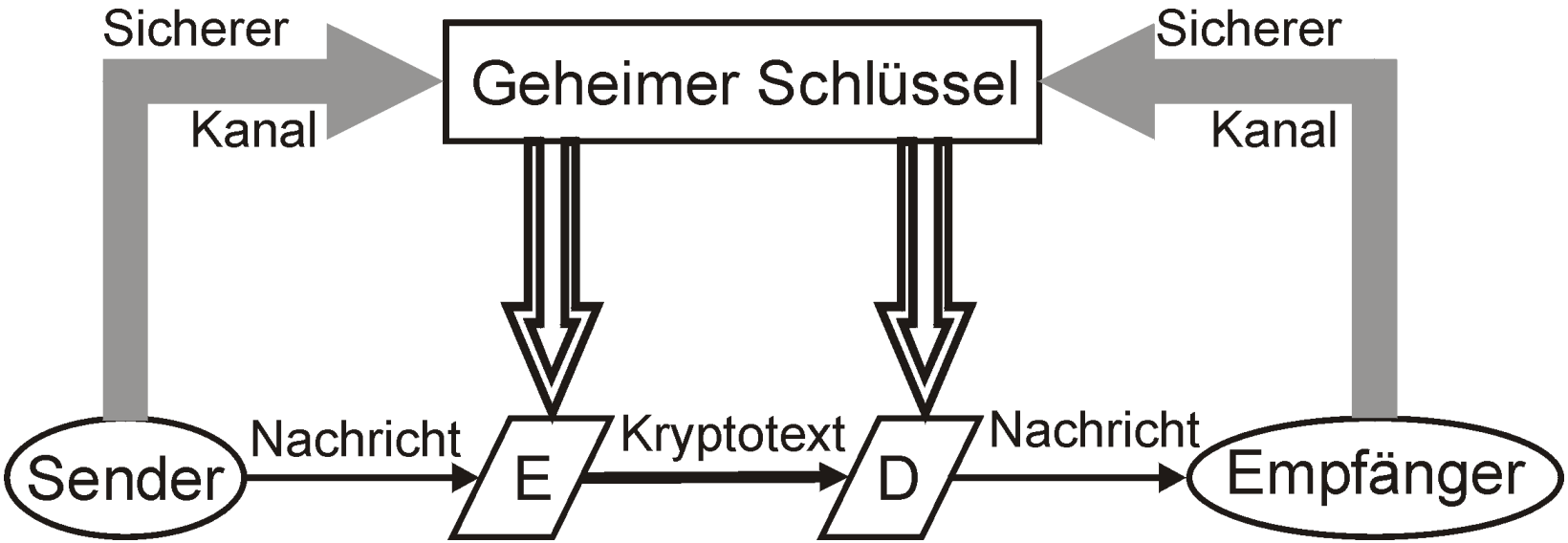
→ **ISO/IEC 27000**: property that information is not made available or disclosed to unauthorized individuals, entities, or processes

→ kein unbefugter Informationsgewinn

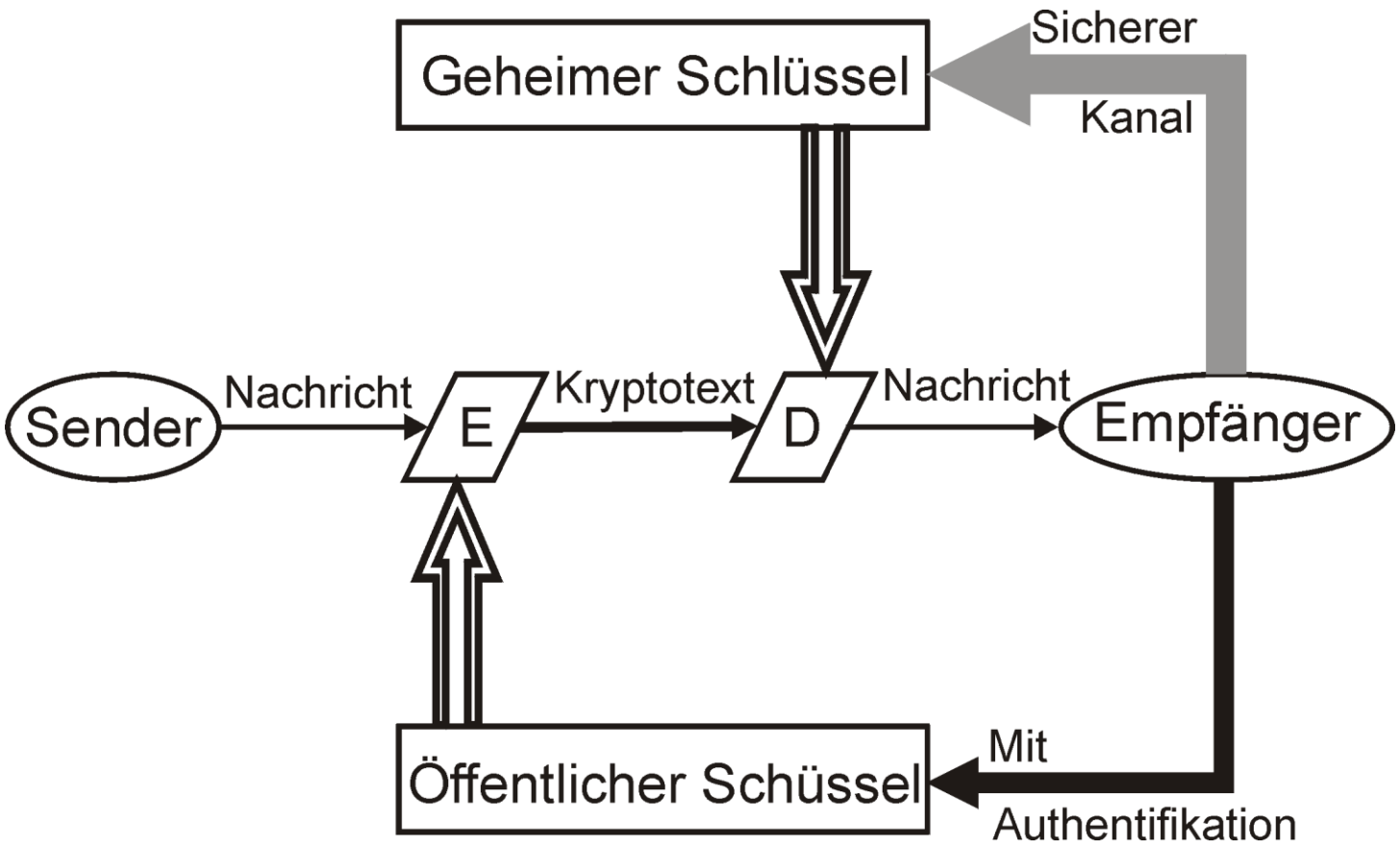
→ Daten für Unbefugte nicht zugänglich (auch nicht über verdeckte Kanäle)

→ ergänzt durch Anonymität/Pseudonymität, Unbeobachtbarkeit & Verdecktheit aus Kommunikationstechnik

Symmetrische Verschlüsselung



Asymmetrische Verschlüsselung



Vergleich der Verschlüsselungen

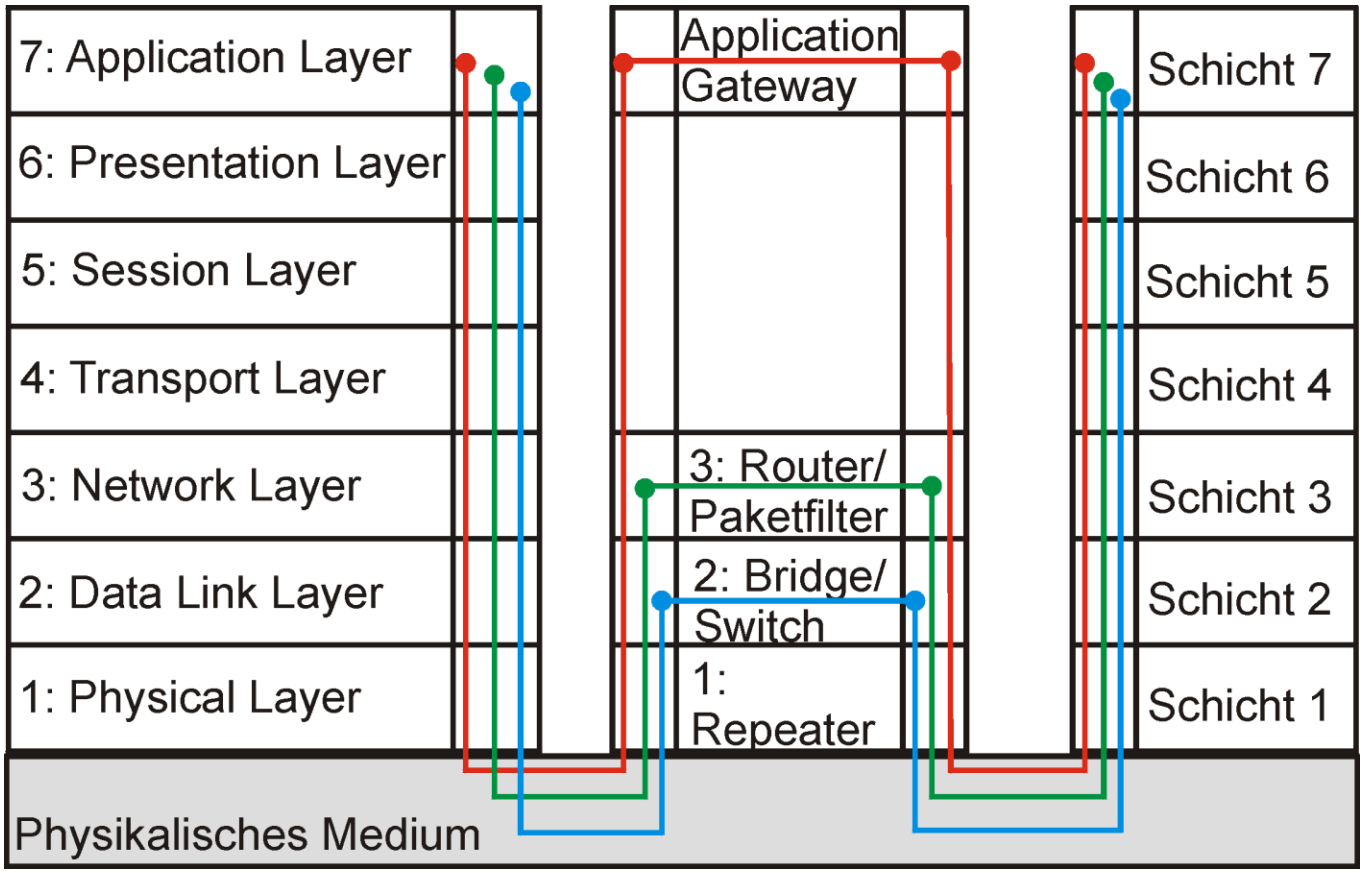
Symmetrisch:

- 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**

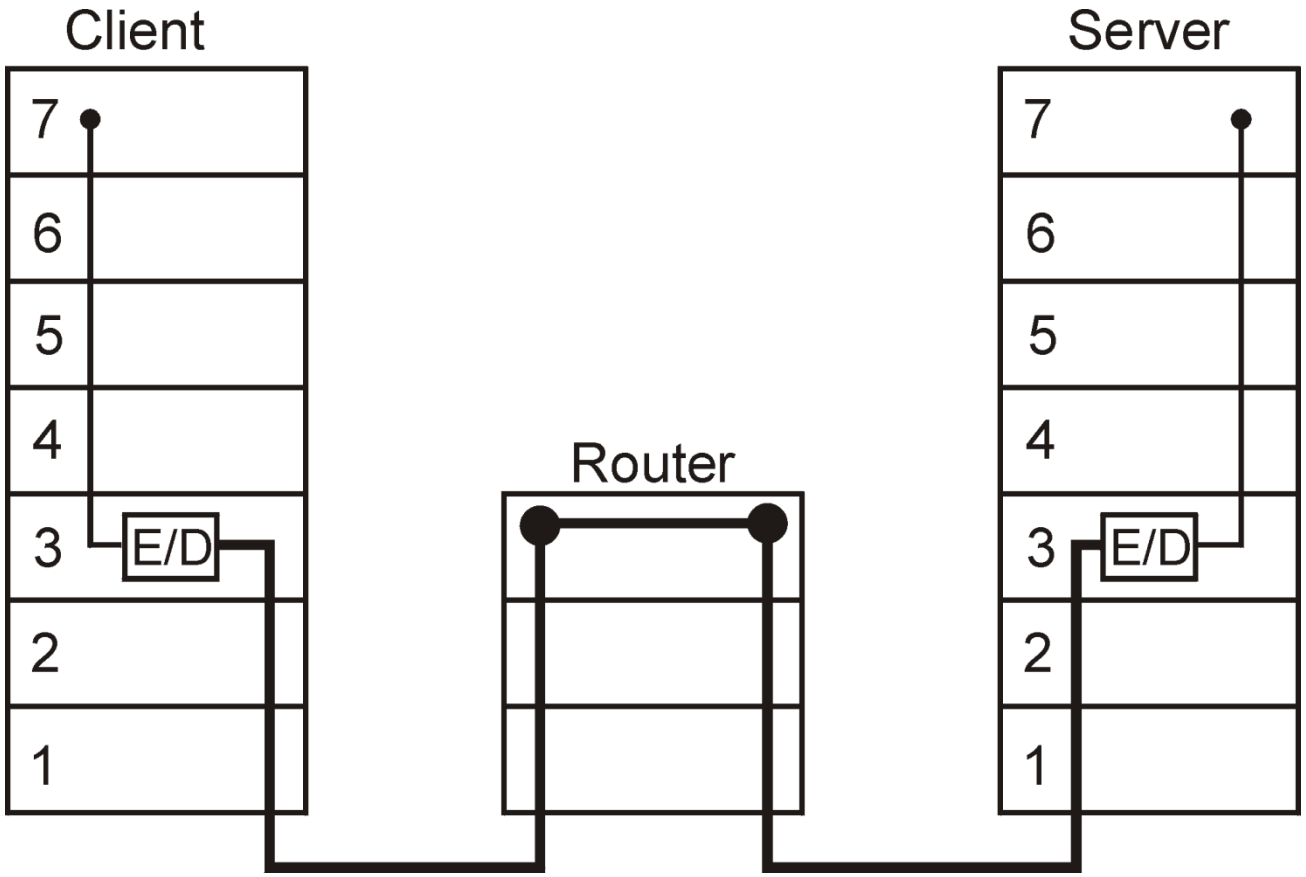
Asymmetrisch:

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

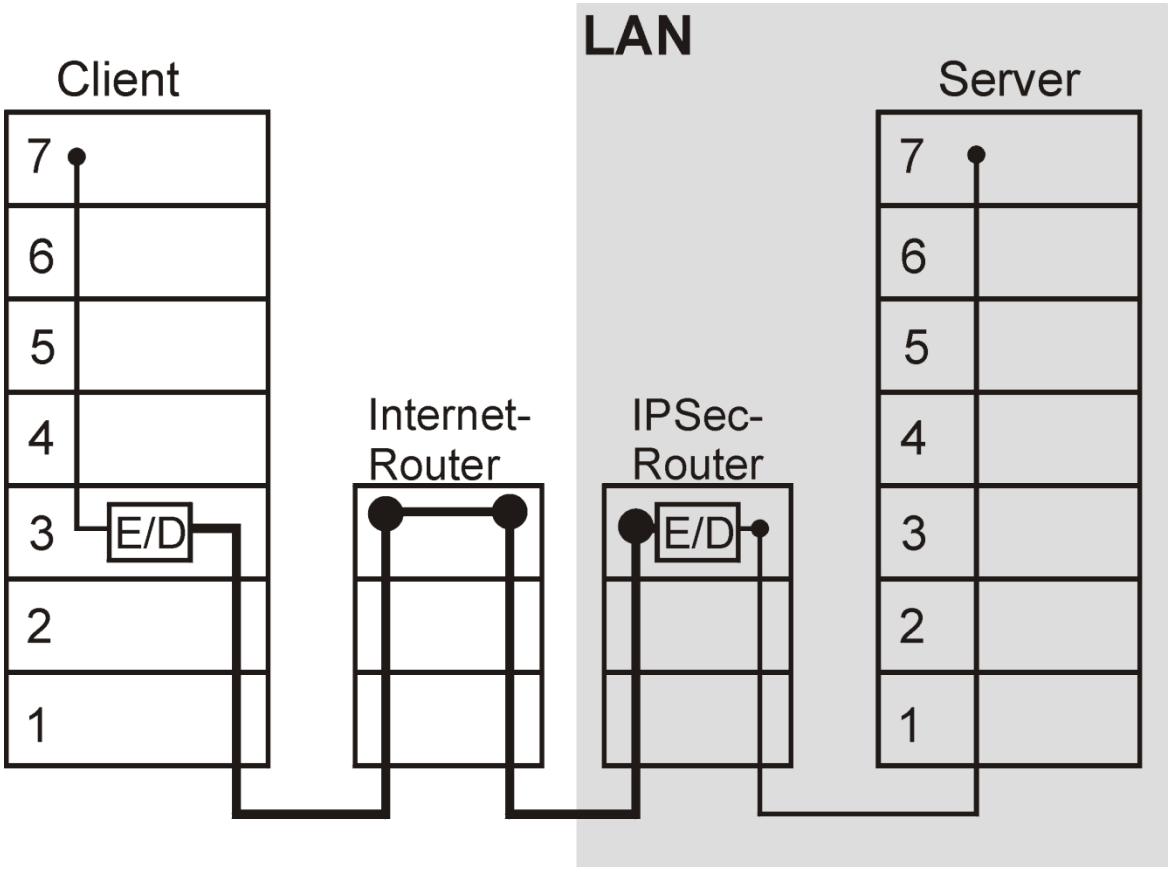
Kommunikationsbeziehungen beim ISO/OSI-Referenzmodell



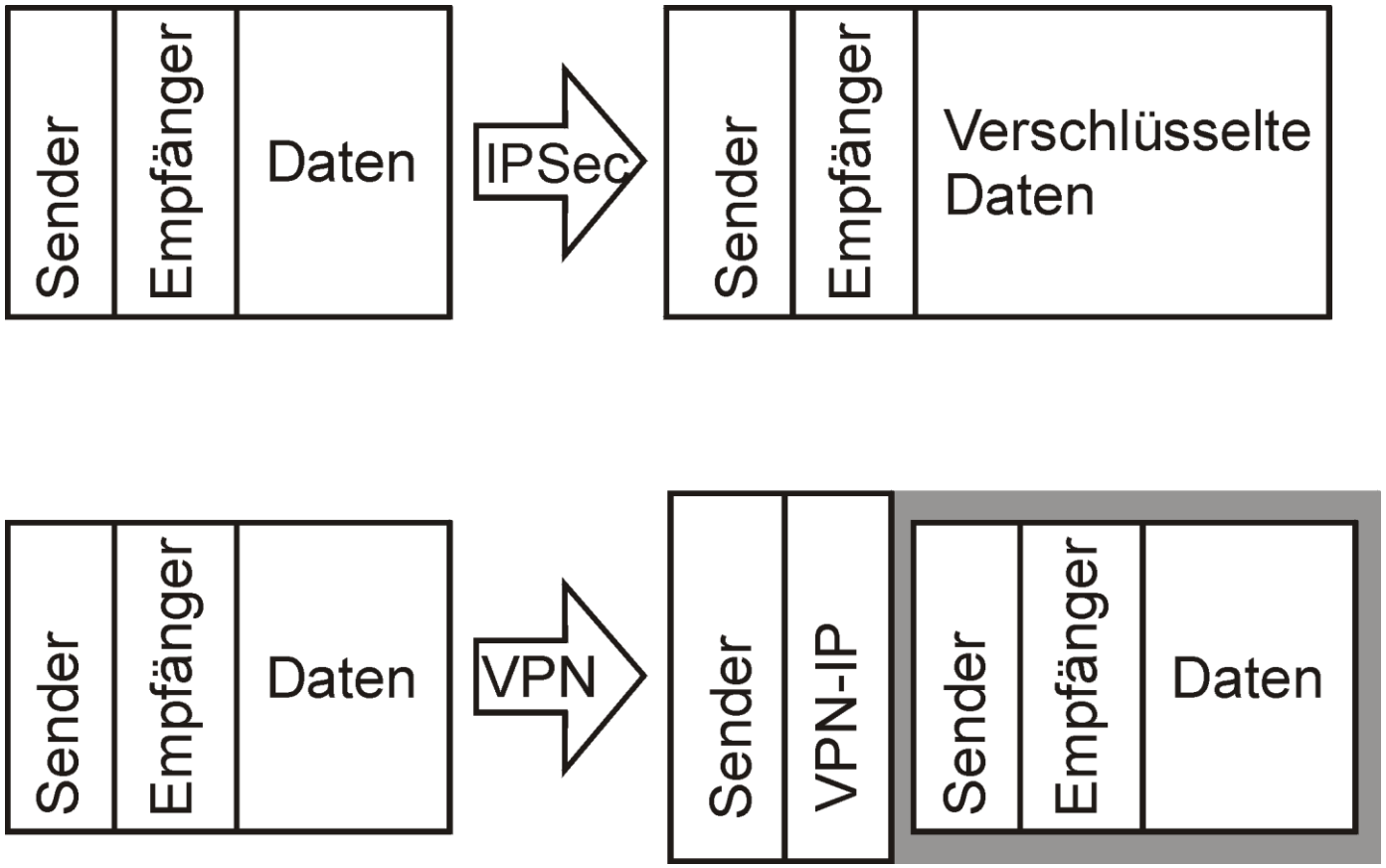
Kommunikation via IPSec: Ende-zu-Ende-Verschlüsselung



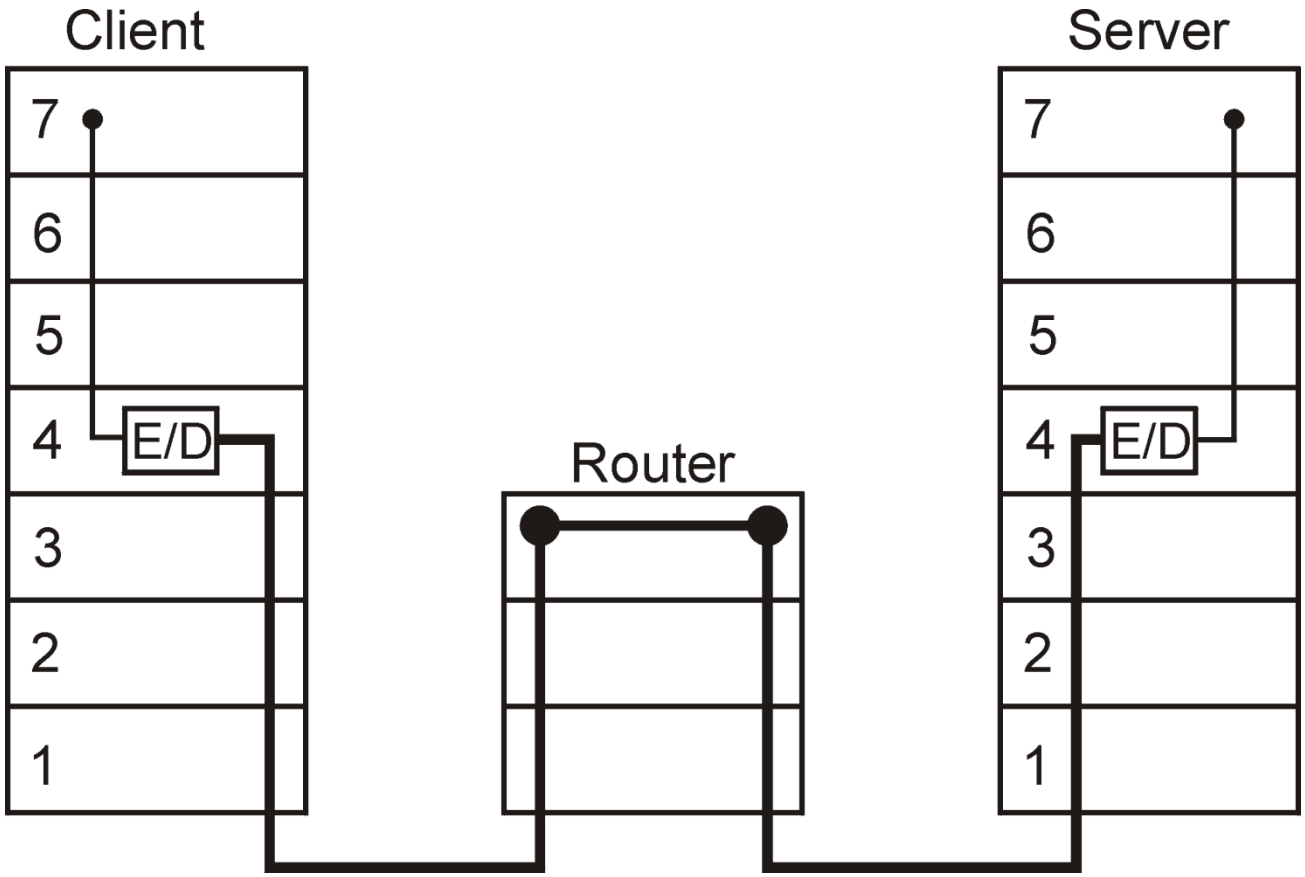
Kommunikation via VPN: Verbindungsverschlüsselung



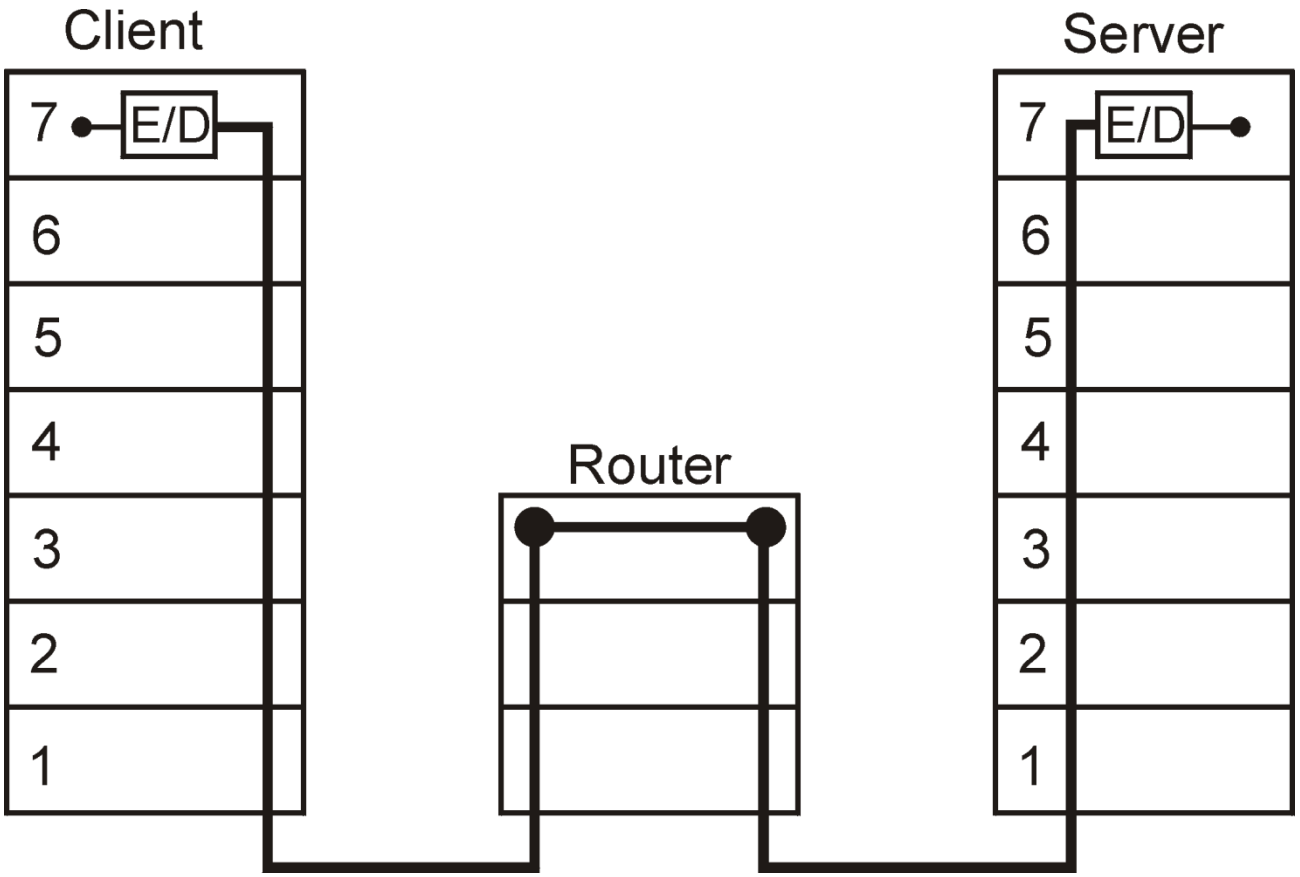
Unterschied zwischen IPSec & VPN



Kommunikation via SSL/TLS: Ende-zu-Ende-Verschlüsselung



Kommunikation via SSH: Ende-zu-Ende-Verschlüsselung



Ziele mehrseitiger IT-Sicherheit (3)

Definition 13: Integrität (integrity)

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

- → **ISO/IEC 27000**: property of protecting the accuracy and completeness of assets
- → 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 Zutritts-/Zugangs-/Zugriffsrechten für Identität

Ziele mehrseitiger IT-Sicherheit (4)

Definition 14: Zurechenbarkeit (accountability)

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

→ **ISO/IEC 27000**: responsibility of an entity for its actions and decisions

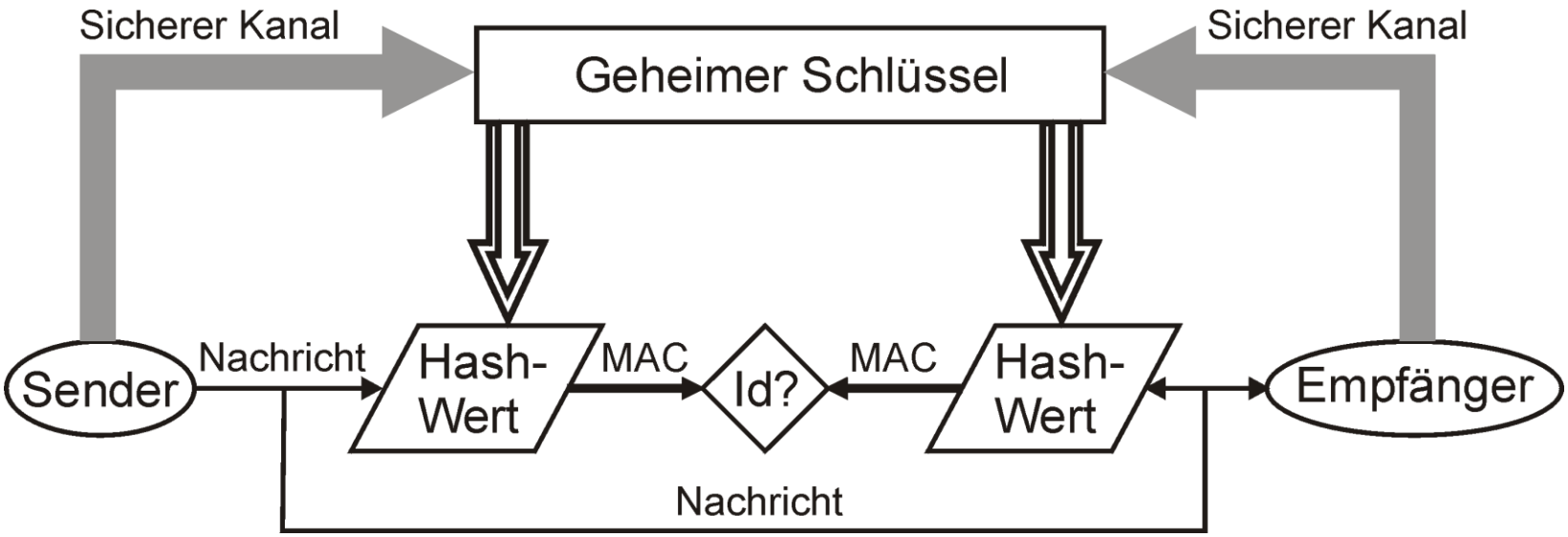
→ Verantwortlichkeit & Authentizität (Glaubwürdigkeit)

→ Diese Daten kommen vom Kommunikationspartner

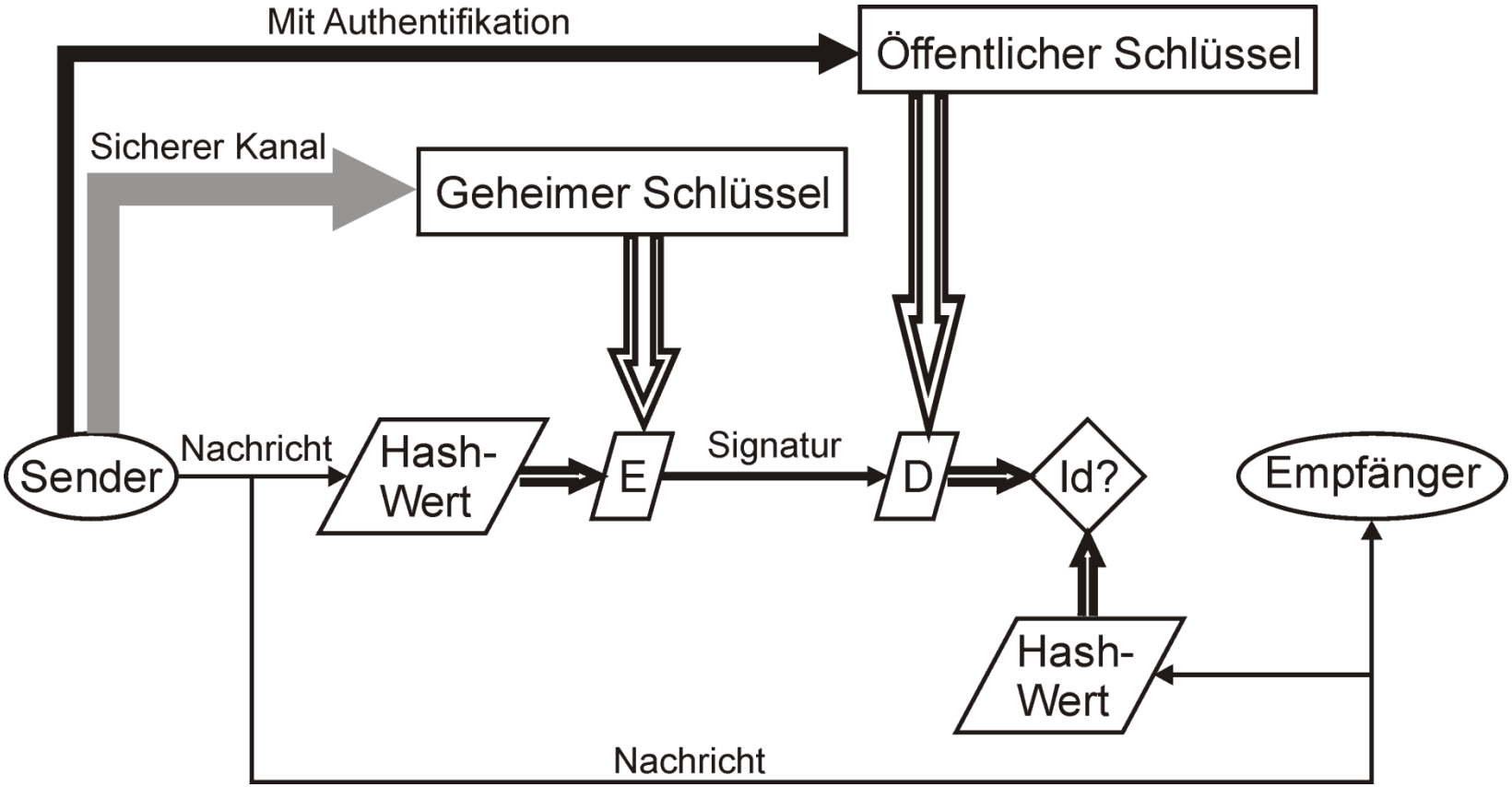
→ Die Daten kommen von diesem Kommunikationspartner

→ Kern des Rechtemanagements

Symmetrische Authentifikation: Message Authentication Code



Asymmetrische Authentifikation: Digitale Signatur



Vergleich der Authentifikationen

Symmetrisch:

- Gängige Verfahren:
  SecurID, GSM-Authenti-
  kation
- Ziel:
  Sicherung d. **Integrität**
- Key-Recovery sinnvoll:
  Hinterlegung des Ent-
  schlüsselungsschlüssels zur
  Vorbeugung gegen
  Schlüsselverlust

Asymmetrisch:

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

Ziele mehrseitiger IT-Sicherheit (5)

Definition 15: 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