Grundlagen des Datenschutzes und der IT-Sicherheit (11)

Vorlesung im Sommersemester 2007
an der Universität Ulm
von Bernhard C. Witt

Grob-Gliederung zur Vorlesung

Topics zum Datenschutz:
- Geschichte des Datenschutzes
- Datenschutzrechtliche Prinzipien
- Vertiefung in ausgewählten Bereichen
- Verwandte Gebiete zum Datenschutz

Topics zur IT-Sicherheit:
- Einflussfaktoren zur IT-Sicherheit

→ **Mehrseitige IT-Sicherheit**
- Risiko-Management
- Konzeption von IT-Sicherheit

Festgestellte Schadensfälle

Schäden durch	2002	2004	2006
Unfälle (menschl. bzw. techn. Versagen)	79%	73%	70%
Angriffe (ungezielt bzw. gezielt)	43%	60%	43%

Quelle: <kes>-Sicherheitsstudien

- mehr Schäden durch Unfälle zu verzeichnen als durch Angriffe
- (mehrseitige) IT-Sicherheit hat beides zu berücksichtigen
- Ursachenermittlung ergibt differenziertes Bild (Mehrfachnennungen waren möglich; bei <kes> in einer Tabelle aufgelistet)

Ursachen von Schadensfällen durch unabsichtliche Ereignisse

Ursachen unabs. Gefahr	1998	2000	2002	2004	2006
Fehler eigener Mitarbeiter	49%	52%	30%	51%	49%
Fehler durch Externe	7%	6%	9%	15%	30%
höhere Gewalt	5%	5%	3%	8%	12%
Software-bedingte Defekte	35%	30%	19%	43%	46%
Hardware-bedingte Defekte	23%	23%	15%	38%	45%
Dokumentations-bed. Defekte	7%	11%	3%	17%	20%

Quelle: <kes>-Sicherheitsstudien

Ursachen von Schadensfällen durch Angriffe

Formen erlittener Angriffe	1998	2000	2002	2004	2006
Malware (Vir., Würm., Troj.Pf.)	31%	29%	25%	54%	35%
unbefugte Kenntnisnahme	10%	11%	6%	9%	12%
Hacking	-----	-----	8%	9%	12%
Manipulation z. Bereicherung	2%	2%	2%	8%	11%
Sabotage (inkl. DoS-Attacken)	0%	2%	2%	8%	10%

Quelle: <kes>-Sicherheitsstudien

→ Schadensfälle gegen Safety als auch gegen Security aufgetreten

Formen der Angriffe via Internet

Angriffe aus dem Internet	1998	2000	2002	2004
Hacking des Rechners	16%	21%	43%	40%
Beeinträchtigung der Verfügbarkeit	5%	8%	29%	27%
unbefugtes Lesen von Daten	14%	15%	19%	23%
Veränderung von Daten	5%	6%	7%	11%
Abhören von Verbindungsdaten	4%	6%	9%	9%
kein Angriff registriert	61%	59%	57%	45%

Quelle: <kes>-Sicherheitsstudien (2006 leider nicht abgefragt)

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
- 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

Gründe für Ausfallzeiten

hinsichtlich unbeabsichtigter Ereignisse:

- zu 39 % **Hardware**-Fehler
  (davon 51 % Plattenspeicher)
- zu 31 % Fehler & Abstürze in **Software**-Programmen
  (davon 62 % Betriebssystem)
- zu 18 % **Bedienungsfehler**
- zu 12 % **externe Fehlerquellen** wie Stromausfall & Wasserschaden

  Quelle: Jochen Sommer: IT-Servicemanagemet mit ITIL und MOF, 2004

→ leider keine absolute Angabe der durchschnittlichen Ausfallzeit & keine Angabe zu angriffsbedingten Ausfallzeiten

Ausfall der Verfügbarkeit durch Angriffe

Dauer von Ausfallzeiten:

- zu 32,5 % 0 h
- zu 27,8 % < 4 h
- zu 13,4 % [4 .. 8] h
- zu 8,6 % (8 .. 24] h
- zu 5,3 % (1 .. 3] d
- zu 2,3 % > 3 d
- zu 10,2 % kein Kommentar

  Quelle: InformationWeek: „IT-Security 2004“

→ im Schnitt ca. 6 h Ausfallzeit durch erfolgreiche **Angriffe** auf die Verfügbarkeit von Server, Anwendungen und Netzwerken

Dauer bestimmter Ausfallzeiten:

- 47,8 h Virus-/Wurm-Infektion
- 35,7 h Hoax
- 24,6 h Fehlalarm
- 16,4 h Spyware-Befall
- 3,1 h Online-Angriff
- 1,8 h Phishing

  Quelle: <kes>-Sicherheitsstudie 2006

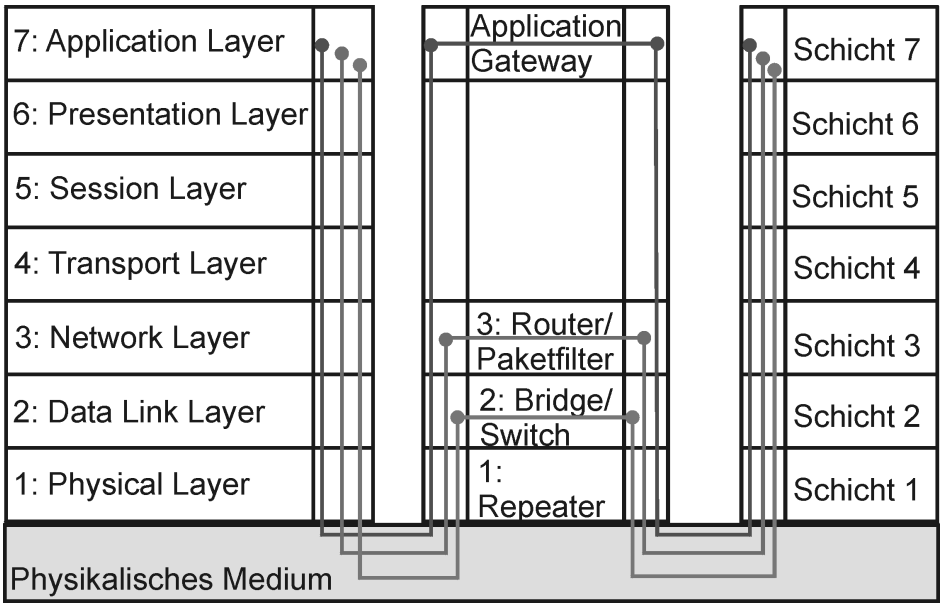
→ Abschätzung für den konkret eingetretenen **Einzelfall**

Verlust der Vertraulichkeit

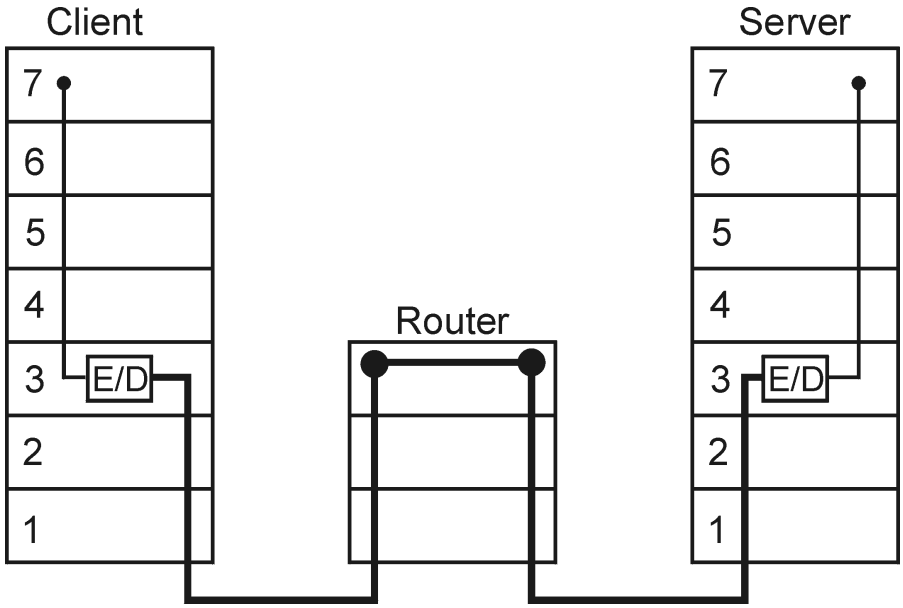
unbefugte Zugriffsart	bekannt	vermutet
Verlust mobiler IT-Systeme	27%	9%
Einbruch in Gebäude	17%	1%
Missbrauch durch Berechtigte	3%	15%
Verlust von Speichermedien	7%	5%
Abhören von Kommunikation	1%	8%
Online-Angriff	2%	4%
sonstiger Weg	2%	1%

Quelle: <kes>-Sicherheitsstudie 2006

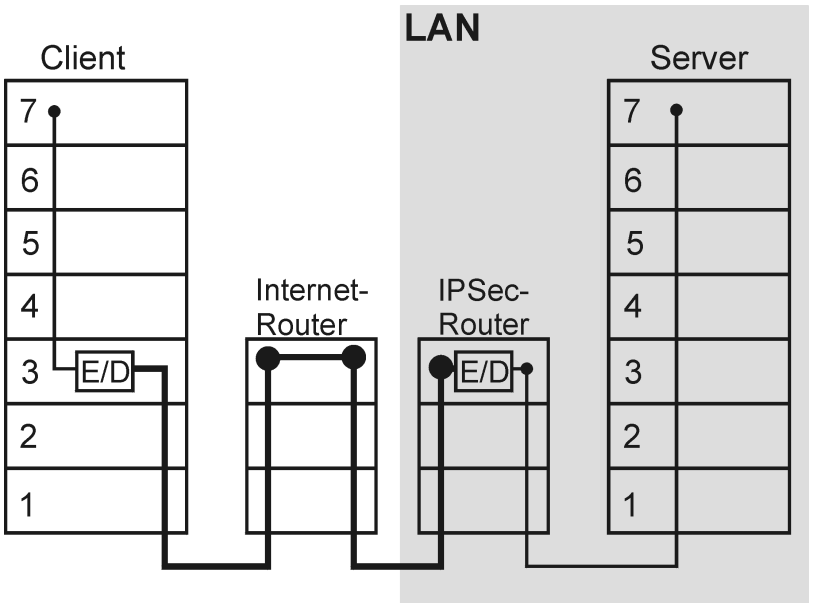
Kommunikationsbeziehungen beim ISO/OSI-Referenzmodell



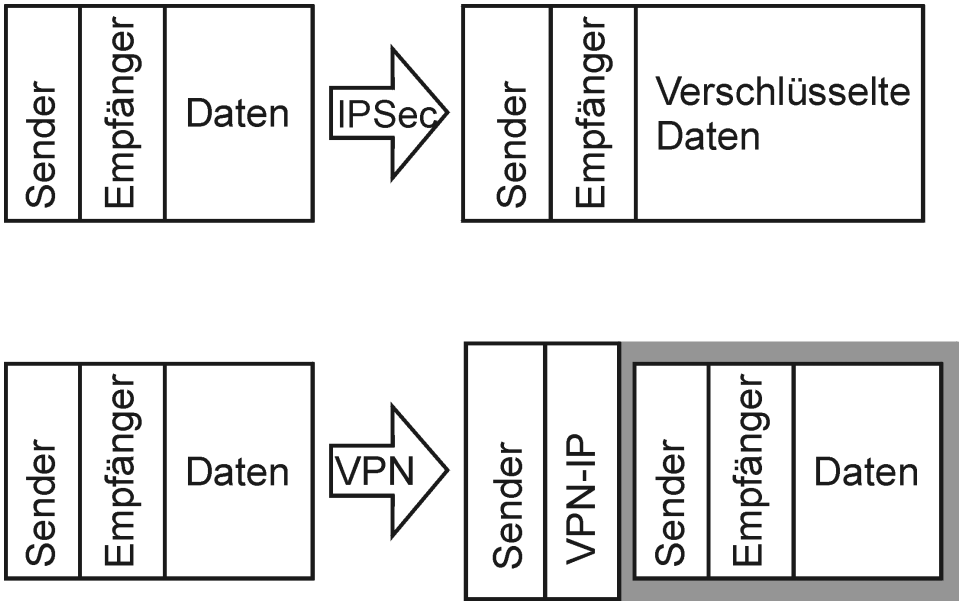
Kommunikation via IPSec: Ende-zu-Ende-Verschlüsselung



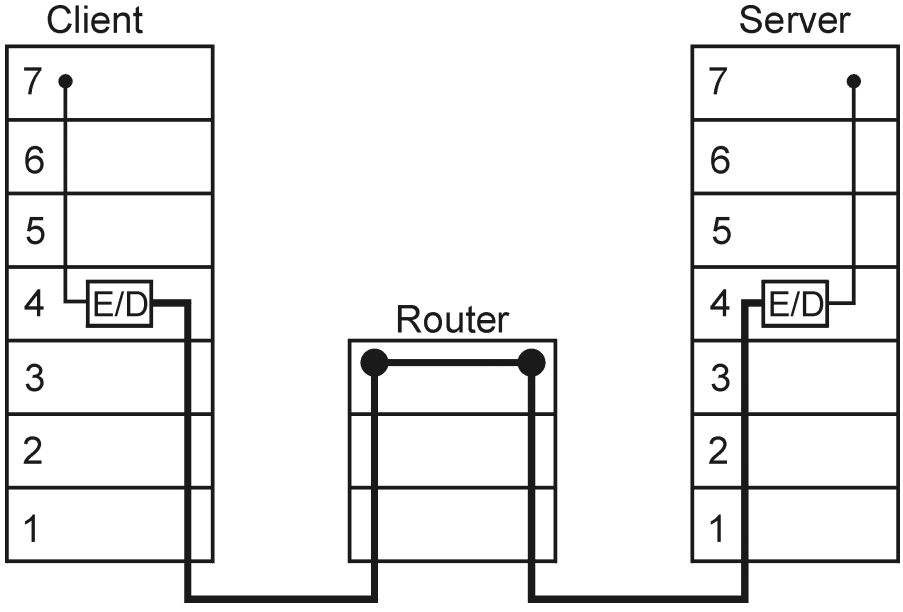
Kommunikation via VPN: Verbindungsverschlüsselung



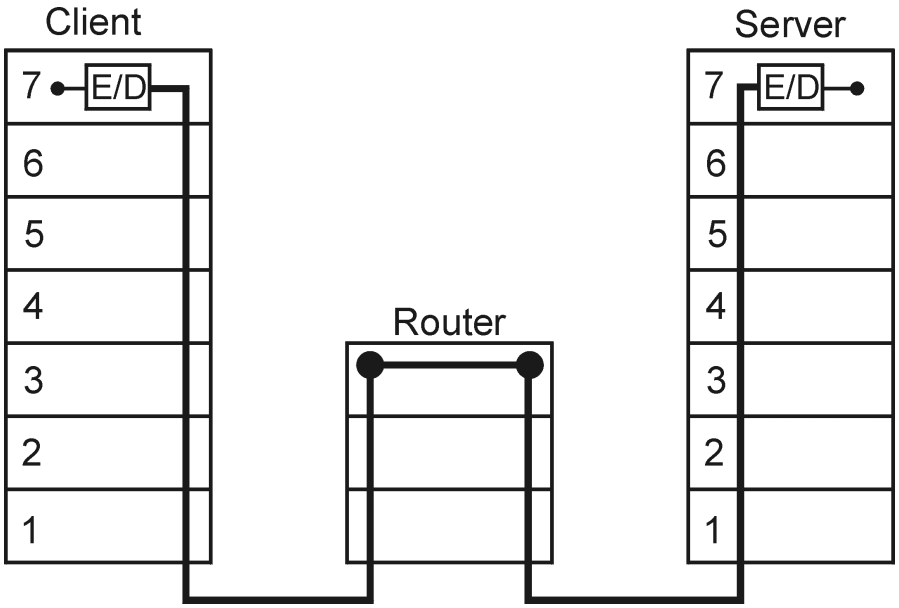
Unterschied zwischen IPSec & VPN



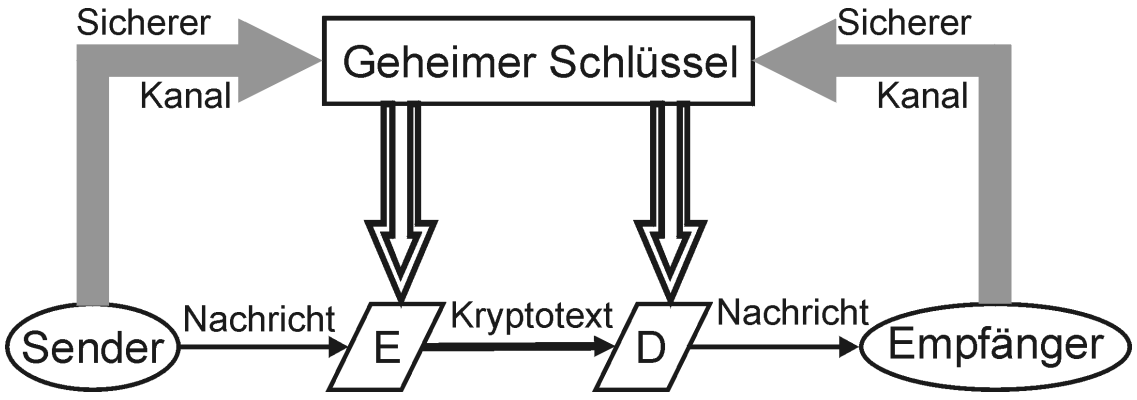
Kommunikation via SSL/TLS: Ende-zu-Ende-Verschlüsselung



Kommunikation via SSH: Ende-zu-Ende-Verschlüsselung



Symmetrische Verschlüsselung

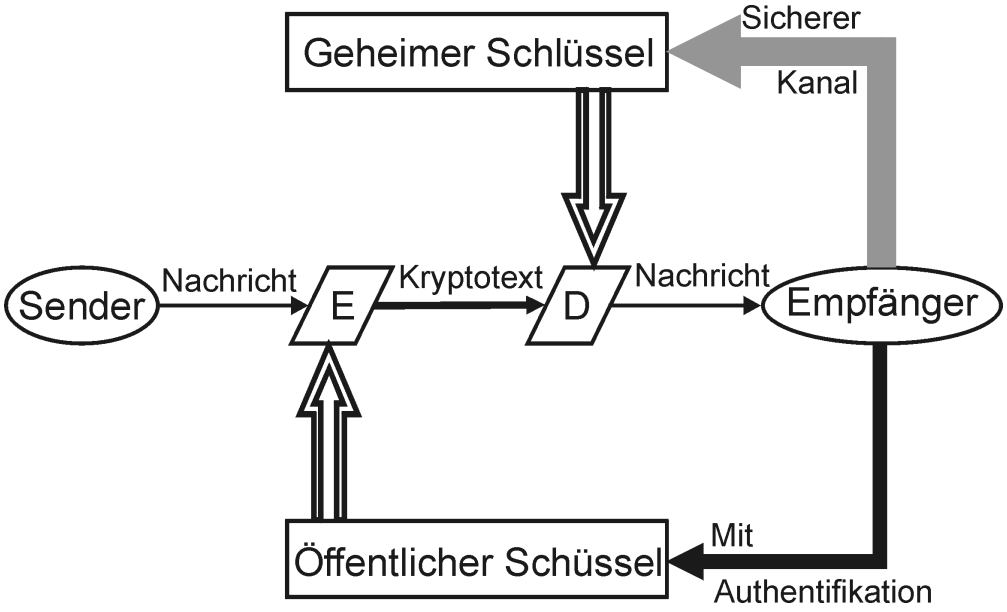


Beispiel: Symmetrische Verschlüsselung

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**

Zum Vergleich symmetrischer zu asymmetrischer Verschlüsselung

Gemäß Primzahlensatz gilt für die Primzahl-Anzahl:

$(n/[\ln(n)+2]) < \pi(n) < (n/[\ln(n)-4])$

→ $\pi(n) \approx [n/\ln(n)]$

- im Intervall [1 .. 1024] → $\pi(n) \approx 148$ (Primzahlen)
- im Intervall [1 .. 2048] → $\pi(n) \approx 269$ (Primzahlen)
- im Intervall [1 .. 3072] → $\pi(n) \approx 382$ (Primzahlen)
- im Intervall [1 .. 4096] → $\pi(n) \approx 492$ (Primzahlen)

beim Vergleich mit Bits ist zu beachten, dass jedes Bit den Wert 0 oder 1 annehmen kann

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

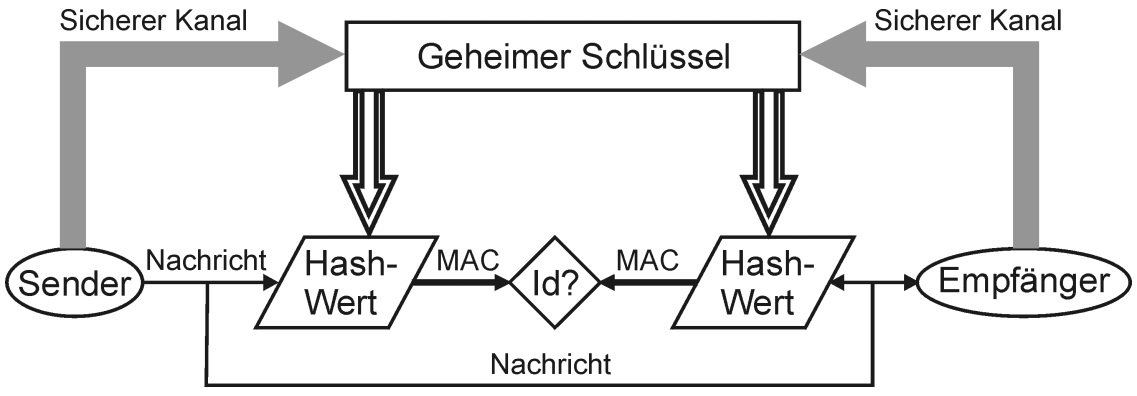
Hinweis:

Authentisierung = Nachweis einer Identität

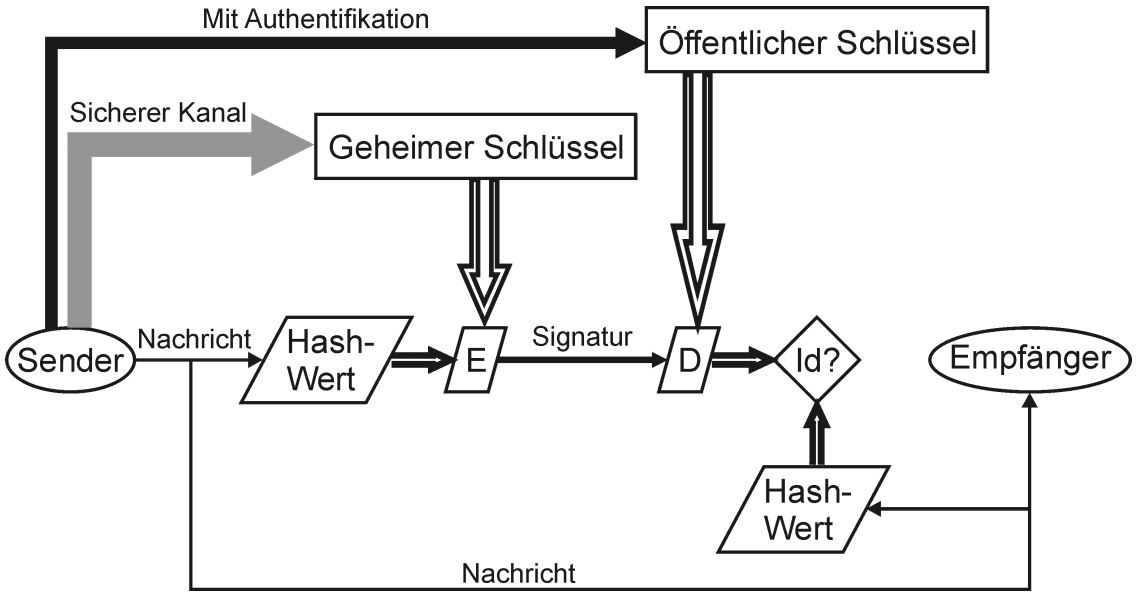
Authentifizierung = Überprüfung einer Identität

Autorisierung = Gewährung von Zutritts-/Zugangs-/Zugriffsrechten

Symmetrische 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)