

# IT-Sicherheit

- Sicherheit vernetzter Systeme -

## Kapitel 2: Grundlagen



## Kapitel 2: Inhalt

1. Überblick über die OSI-Sicherheitsarchitektur
2. ISO/OSI Referenzmodell
3. OSI Sicherheitsarchitektur
  1. Sicherheitsdienste
  2. Sicherheitsmechanismen
4. OSI Sicherheitsmanagement
5. Unterscheidung Security versus Safety

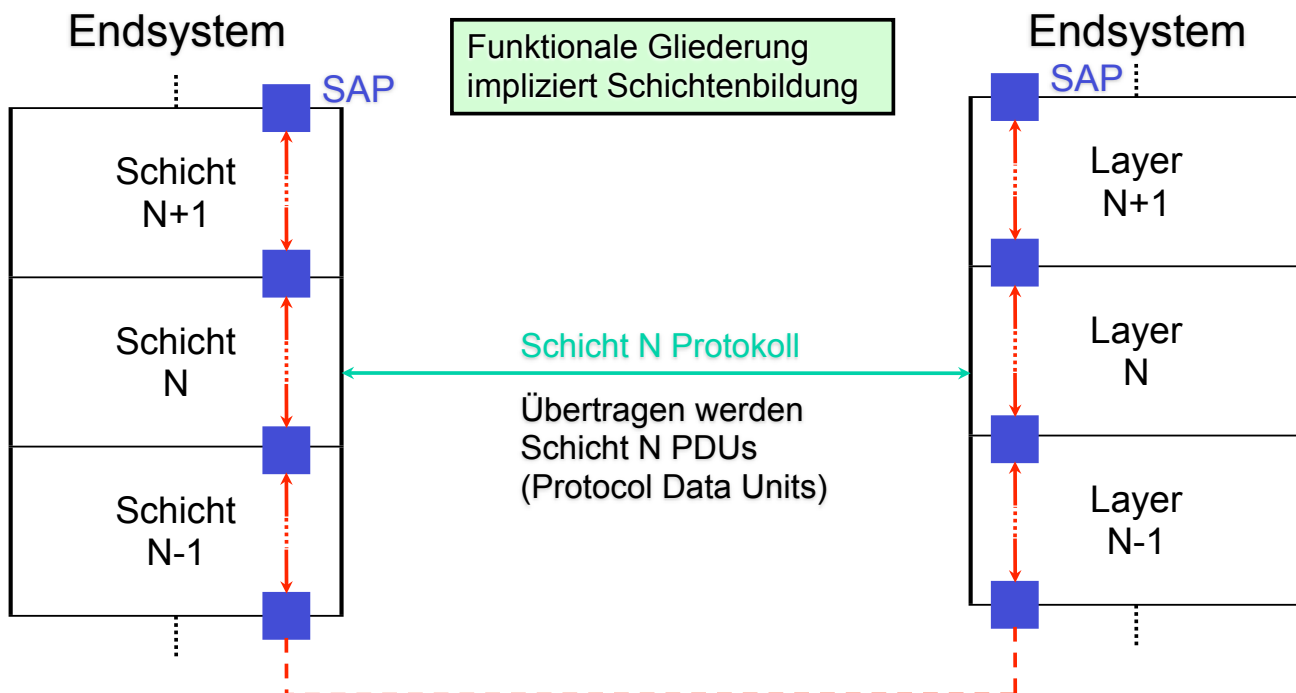


# OSI Security Architecture: Überblick

- Standardisiert von der International Standardization Organization (ISO) 1988 und der International Telecommunication Union (ITU) 1991
- Dokumente:
  - ISO: ISO-7498-2; ISO-10181-1 bis -7 (Security Framework); ISO-11586-1 bis -6 (Upper Layer Security)
  - ITU: ITU-T X.800 – X.830
- Fokus liegt auf verteilten / vernetzten Systemen
- Beschreibung von Sicherheitsdiensten (Security Services), Sicherheitsmechanismen,.....
- Baut auf dem Open System Interconnection Reference Model (ISO/OSI-RM) auf



## Prinzip des OSI-Referenzmodell



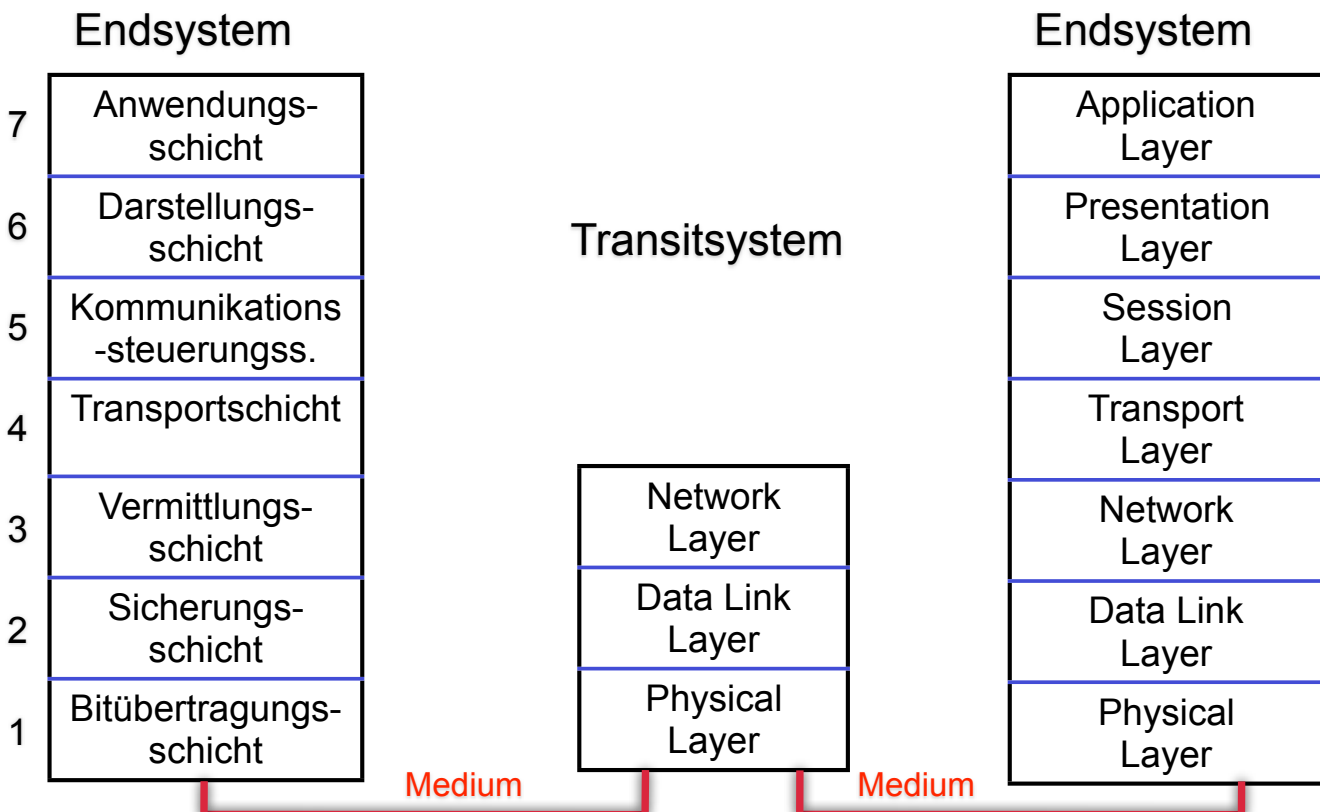
SAP = Service Access Point  
(Dienstzugangsschnittstelle)

Logischer Datenfluss

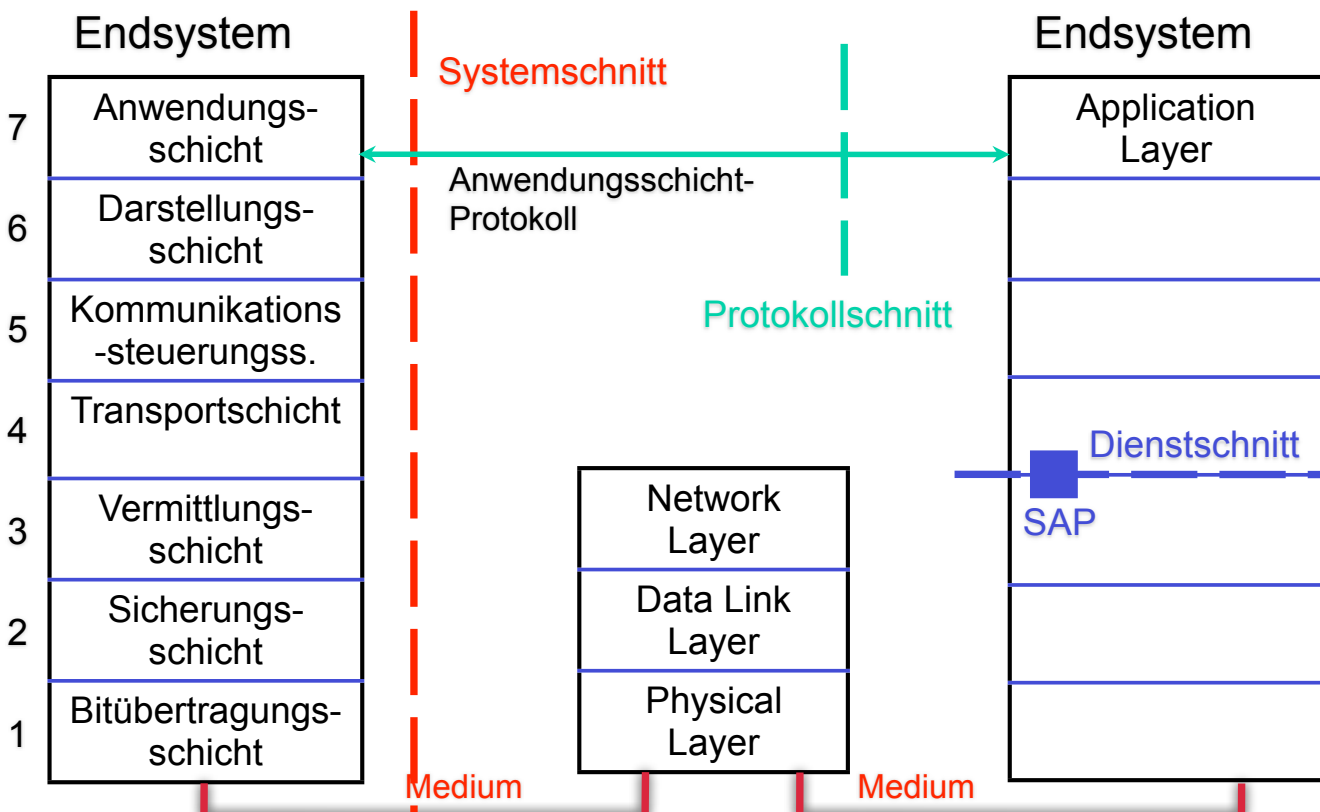
Physischer Datenfluss



# OSI Referenzmodell: Schichten



# OSI Referenzmodell: Schnittbildung



# OSI Security Architecture: Überblick

- Beschreibung von Sicherheitsdiensten (Security Services) und Sicherheitsmechanismen
- Beziehungen zwischen Services, Mechanismen und den Schichten
- Platzierung von Services und Mechanismen
- Security Management
- Hintergrundinformation
  - Bedrohungen und Angriffe
  - Security Policy
  - Grundlegende Mechanismen
- Fokus der Sicherheitsarchitektur
  - Sicherheitsbedürfnisse von verteilten / vernetzten Systemen
  - Betrachtet **keine** Host- oder Betriebssystem-Sicherheit



# OSI Security Architecture: Dienste

- **Authentisierung (Authentication):**  
Jede Entität kann zweifelsfrei identifiziert werden
  - Peer Entity Authentication:  
Gegenseitige Authentisierung von zwei oder mehr Kommunikationspartnern
  - Data Origin Authentication:  
Identifikation des Senders bzw. des Autors einer Nachricht
- **Zugriffskontrolle (Access Control):**  
Schutz vor unberechtigter Nutzung von Ressourcen
- **Vertraulichkeit (Data Confidentiality):**  
Schutz der Daten vor unberechtigter Offenlegung
  - Connection confidentiality:  
Alle (N-) User Daten einer (N-) Verbindung
  - Connectionless confidentiality:  
Alle (N-) User Daten einer einzelnen (N-) SDU (Service Data Unit)
  - Selective field confidentiality:  
Bestimmte Felder der User Daten
  - Traffic flow confidentiality:  
Schutz vor Verkehrsflussanalyse. (Wer kommuniziert mit wem in welchem Umfang und zu welcher Zeit?)



# OSI Security Architecture: Dienste (Forts.)

## ■ Datenintegrität (Data Integrity):

Erkennung von Modifikationen, Einfügungen, Löschungen, Umordnung, Duplikaten oder Wiedereinspielung von Daten

- Connection Integrity with/without Recovery
- Selective Field Connection Integrity
- Connectionless Integrity
- Selective Field Connectionless Integrity

## ■ Verbindlichkeit (Non-repudiation):

Niemand kann das Senden oder Empfangen der Daten leugnen

- With proof of origin:  
Sender kann das Senden nicht leugnen; Empfänger kann beweisen welchen Ursprung die Daten haben
- With proof of delivery:  
Empfänger kann Empfang nicht leugnen; Sender kann die Auslieferung beweisen



## Fokus der Sicherheitsdienste

Authentication	Peer Entity
	Data Origin
Access Control	
Data Confidentiality	Connection
	Connectionless
	Selective field
	Traffic flow
Data Integrity	Connection
	Connectionless
	Selective field
	Recovery
Non-Repudiation	Proof of origin
	Proof of delivery

- Betrachtet werden **keine** Host- oder Betriebssystem-Sicherheit
- Fehlende bzw. nicht explizit spezifizierte Security Services:
  - **Identifikation (Identification);**  
Personalisierung:  
Zweifelsfreie Verbindung zwischen digitaler ID und Real World Entity (Person oder Organization)
  - **Autorisierung (Authorization):**  
Erteilung von Rechten an Entities
  - **Zurechenbarkeit (Accountability)**
  - **Anonymität (Anonymity)** (außer bei Traffic Flow Confidentiality)
  - (Verfügbarkeit (Availability))
  - **Ressourcenbeschränkung (Resource constraints)**



# OSI Security Architecture: Mechanismen

- Unterscheidung in:
  - spezifische (specific)
  - durchgängige (pervasive)
- Sicherheitsmechanismen
- Specific Security Mechanisms
  - Verschlüsselung (Vertraulichkeit)
    - Symmetrisch
    - Asymmetrisch
  - Digitale Signatur (Verbindlichkeit)
  - Zugriffskontrolle
    - Zugriffskontrolllisten, -matrizen
    - "Wissen und/oder Besitz"
    - Capabilities, Tickets
  - Prüfsummenverfahren (Integrität)
  - Notariatsfunktionen
- Austausch von Authentisierungs-  
informationen; nutzt ggf.
  - Verschlüsselung und
  - Digitale Signatur
- Traffic Padding, Anonymisierung  
(zur Verhinderung von Verkehrs-  
flussanalysen)
- Kontrolle des Routing-Verfahrens
- Pervasive Security Mechanisms
  - Vertrauenswürdige Funktionen
  - Security Labels zur (Sensitivitäts-)  
Klassifikation der Daten
  - Eventmechanismen
  - Auditing und Logging
  - Recovery Mechanismen
    - Unmittelbar, kurz- und  
langfristig



## Beziehung zwischen Service und Mechanismus

TABLE 1/X.80

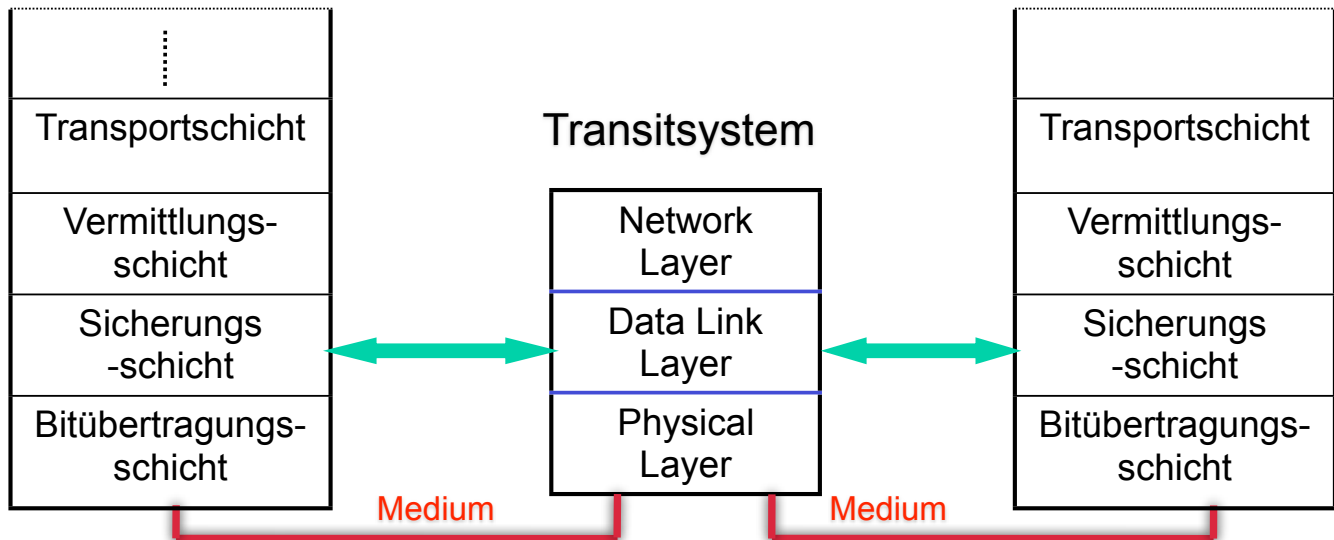
Illustration of relationship of security services and mechanism

Mechanismus	Enciphermen	Digitale Signatur	Access control	Data integrität	Authentisierungs- austausch	Traffic padding	Routing control	Notariats- funktion
Peer entity authentication	Y	Y	.	.	Y	.	.	.
Data origin authentication	Y	Y	.	.	.	.	.	.
Access control service	.	.	Y	.	.	.	.	.
Connection confidentiality	Y	.	.	.	.	.	Y	.
Connectionless confidentiality	Y	.	.	.	.	.	Y	.
Selective field confidentiality	Y	.	.	.	.	.	.	.
Traffic flow confidentiality	Y	.	.	.	.	Y	Y	.
Connection Integrity with recover	Y	.	.	Y	.	.	.	.
Connection integrity without recover	Y	.	.	Y	.	.	.	.
Selective field connection integrity	Y	.	.	Y	.	.	.	.
Connectionless integrity	Y	Y	.	Y	.	.	.	.
Selective field connectionless integrity	Y	Y	.	Y	.	.	.	.
Non-repudiation. Origin	.	Y	.	Y	.	.	.	Y
Non-repudiation. Delivery	.	Y	.	Y	.	.	.	Y



# Mechanismen auf unterschiedlichen Schichten

- Was ist die zu authentisierende/sichernde Entität?
- Wie weit reicht der Sicherheitsmechanismus?  
Bsp. Verschlüsselung auf Schicht 2 (Sicherheitsschicht)  
d.h. jedes Transitsystem muss entschlüsseln



# Vorschlag einer Zuordnung der Services auf Layer

TABLE 2/X.80

Illustration of the relationship of security services and layer

Service	Layer						
	1	2	3	4	5	6	7
Peer entity authentication	.	.	Y	Y	.	.	Y
Data origin authentication	.	.	Y	Y	.	.	Y
Access control service	.	.	Y	Y	.	.	Y
Connection confidentiality	Y	Y	Y	Y	.	Y	Y
Connectionless confidentiality	.	Y	Y	Y	.	Y	Y
Selective field confidentiality	.	.	.	.	.	Y	Y
Traffic flow confidentiality	Y	.	Y	.	.	.	Y
Connection Integrity with recover	.	.	.	Y	.	.	Y
Connection integrity without recover	.	.	Y	Y	.	.	Y
Selective field connection integrity	.	.	.	.	.	.	Y
Connectionless integrity	.	.	Y	Y	.	.	Y
Selective field connectionless integrity	.	.	.	.	.	.	Y
Non-repudiation Origin	.	.	.	.	.	.	Y
Non-repudiation. Deliver	.	.	.	.	.	.	Y

Y Yes, service should be incorporated in the standards for the layer as a provider option.

.

\* It should be noted, with respect to layer 7, that the application process may, itself, provide security services.



# OSI Security Management

## ■ OSI unterscheidet drei (Sicherheits-)Management-Kategorien:

### 1. **System Security Management:**

- Management des gesamten verteilten (OSI-) Systems
- **Nicht** das System im Sinne von Endsystem oder Betriebssystem

### 2. **Security Service Management:**

- Management von dedizierten Sicherheitsdiensten

### 3. **Security Mechanism Management:**

- Management von spezifischen Sicherheitsmechanismen



## 1. System Security Management Functions

### ■ Policy Management

- Aktualisierung
- Konsistenzprüfung und Überwachung
- Wartung

### ■ Interaktion mit anderen OSI-Mgmt. Funktionen

### ■ Event Handling

- Reporting
- Planung und Fortschreibung
- Analyse

### ■ Audit Management

- Auswahl von zu loggenden Events
- Aktivierung, Deaktivierung (entfernter) Logs
- Sammlung und Auswertung

### ■ Recovery Management

- Erkennung und Report von Angriffen und Angriffsversuchen
- (Reaktions-) Regeln für Administratoren





## 2. Security Service Management Functions

- Auswahl von Sicherheitsdiensten für jedes Ziel (Target) (Anforderungsanalyse)
- Auswahl, Wartung und Aktualisierung von Regeln / Policies für die gewählten Dienste
- Installation / Aktivierung entsprechender Mechanismen zur Realisierung der Dienste
- Aufruf der entsprechenden Funktionalität durch das Sicherheitsmanagement (-system)
- Interaktion mit anderen Management Funktionen



## 3. Security Mechanism Management Functions

- Schlüsselmanagement
    - Personalisierung
    - Schlüsselerzeugung
    - Schlüsselverteilung
    - Widerruf von Schlüsseln
  - Kryptographie-Management
  - Mgmt. der digitalen Signatur
  - Zugriffskontrollmanagement
  - Integritätsmanagement
  - Authentisierungsmanagement
- Interaktion mit dem Schlüsselmanagement
  - Einrichtung und Initialisierung der Verfahren
  - Auswahl und Nutzung geeigneter Protokolle zwischen den Kommunikationspartnern (u. ggf. einer Trusted Third Party (TTP) = Notar)
  - Verteilung der Sicherheitsattribute und Informationen
  - Wartung und Betrieb



## 3. Security Mechanism Mgmt. Functions (Forts.)

### ■ Mgmt. der Notariatsfunktion

- Verteilung von Information über Notare
- Protokoll zur Kommunikation mit Notar

### ■ Traffic Padding Management

- Vorspezifizierte Datenraten
- Zufällige Datenraten
- Spezifikation der Nachrichtencharakteristika (z.B. Länge)
- Variation der Spezifikation, z.B. in Abhängigkeit der Zeit

### ■ Routing Control Management

- Klassifikation der Links oder Subnetze nach Vertrauens-Level
- Festlegung der Routing Verfahren entsprechend dieser Klassifikation



## Unterscheidung von Security und Safety

### ■ Beide Begriffe werden mit „Sicherheit“ übersetzt

### ■ Security (Sicherheit)

- Security Engineering
- Security Policies
- Sicherheitsanforderungen:  
Identifikation, Authentisierung, Autorisierung, Zugriffskontrolle,.....
- Sicherheitsmechanismen realisieren Sicherheitsanforderungen
- Auditing und Logging

### Verfügbarkeit (Availability) von Software und Hardware

### ■ Safety (Betriebs-Sicherheit)

- Verfügbarkeit (Availability) / Ausfallsicherheit (Reliability)
- Betriebssicherheit für sicherheitskritische Programme, z.B., Steuerung und Überwachung von Flugzeugen oder (Atom-)Kraftwerken
- Gesundheitliche Sicherheit / Ergonomie

