Netzsicherheit SS 2003

# IPSec

Benedikt Gierlichs

gierlichs@itsc.rub.de

Marcel Selhorst

selhorst@crypto.rub.de

Lehrstuhl für Kommunikationssicherheit

Betreuer: Ahmad-Reza Sadeghi

# - Gliederung -

1. Motivation
2. Grundlagen der IP-Sicherheit
3. Die Funktionalität von IPSec
4. Selektoren, SPI, SPD
5. Sicherheitsassoziationen (SA, SADB, ISAKMP)
6. Modi
7. Authentication Header / Encapsulated Security Payload
8. Die Sicherheit von IPSec
9. RFCs

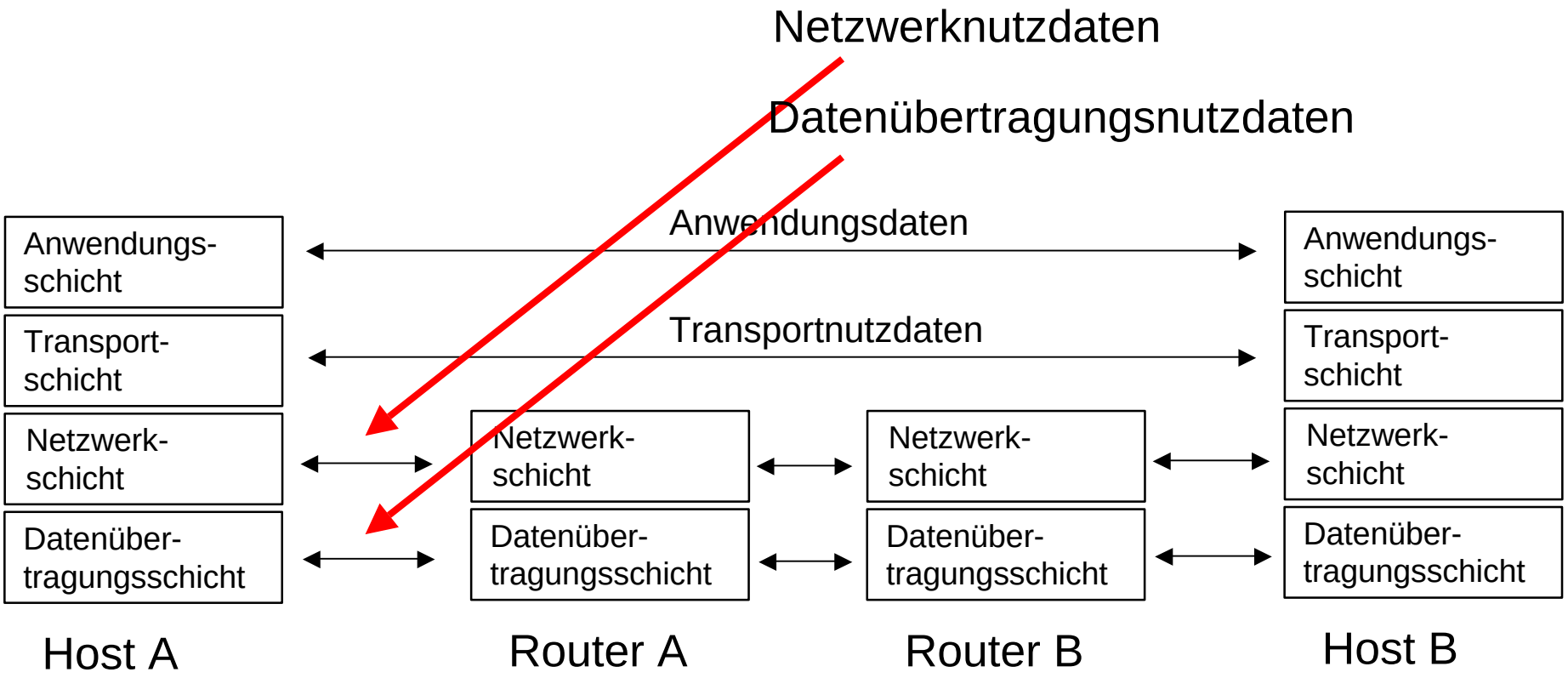
# - Motivation -

- IPv4 stellt IP-Pakete nur zu
- Internetwachstum wirft 2 Probleme auf:
  - Zu kleiner Adressraum (32bit)
  - Keine Sicherheitsaspekte berücksichtigt
- Planung von IPv6
  - Größerer Adressraum (128bit)
  - Standardmäßig eingebaute IP-Sicherheit
- **IPSec**
  - 1992: IETF Arbeitsgruppe
  - 1995: erste RFCs
  - 1998: überarbeitete RFCs

# - Schutzziele (allgemein) -

- Vertraulichkeit — Zugang zu Daten nur für Befugte
- Integrität — Manipulation der Daten während der Übertragung muss erkennbar sein
- Authentifizierung — Quelle ist diejenige, die sie zu sein vorgibt
- Verbindlichkeit — Empfänger kann beweisen, die Nachricht vom Sender erhalten zu haben
- Verfügbarkeit — System muss zu einem vorgegebenen Zeitpunkt in einem funktionsfähigen Zustand sein

# - Einordnung in den TCP/IP-Stapel -

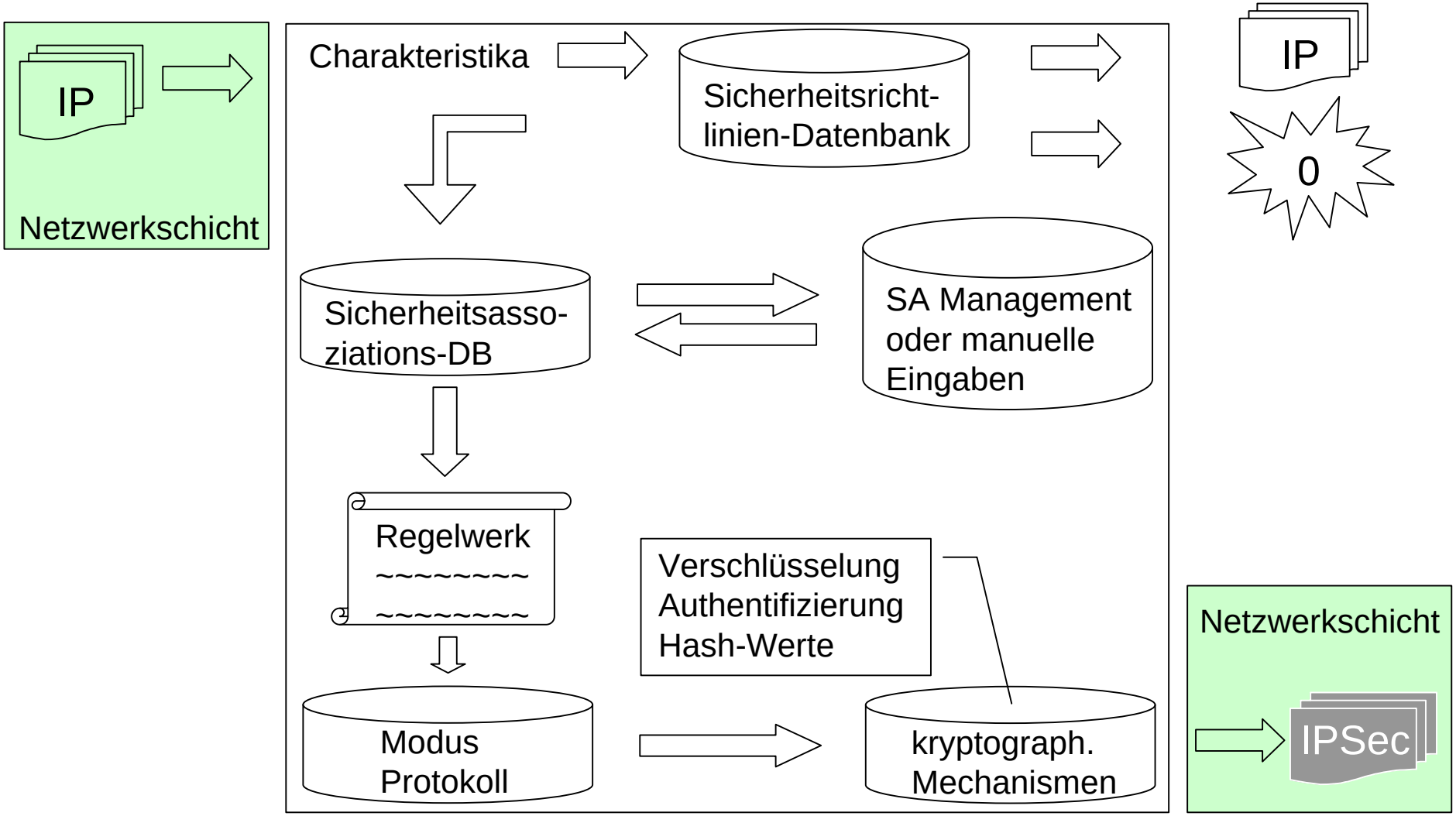


# - Einordnung in den TCP/IP-Stapel -

## Einbettung von Sicherheit in welche Schicht?

| | |
|---|---|
| Anwendungsschicht: | **Nein,** umfangreiche Modifikationen an jeder Anwendung erforderlich |
| Transportschicht: | **Nein,** gibt es als Transport Layer Security (TLS), allerdings anderer Kontext (Anwendung/Nutzer) |
| Netzwerkschicht: | **Ja,** da nur geringfügige Änderungen am TCP/IP-Stapel nötig und größtmöglicher Sicherheitsumfang |
| Datenübertragungs-schicht: | **Nein,** da sie nur für physikalische Verbindung zwischen zwei Hosts in Frage kommt |

# - Die Funktionalität von IPSec -



# - Selektoren, SPI, SPD -

Charakteristika:

- **Quelle:** Selektoren
  - Quell- und Ziel-IP-Adresse
  - evtl.Transportprotokoll
  - evtl. Quell- und Zielport

- **Ziel:** SPI ( Security Parameter Index )
  - wird im IPSec-Header übertragen und ist pro Paket eindeutig

SPD (Security Parameter Index):

- entscheidet anhand der Charakteristika ob discard, bypass oder apply

# - Sicherheitsassoziation -

## Sicherheitsassoziation:

- stellt „Vertrag“ zwischen Hosts dar
- legt Modus und Sicherheitsstufe fest
- unidirektional, pro Verbindung und Richtung eine SA notwendig
- manuell erstellt / gelöscht oder dynamisch mittels ISAKMP / IKE

## Sicherheitsassoziationsdatenbank:

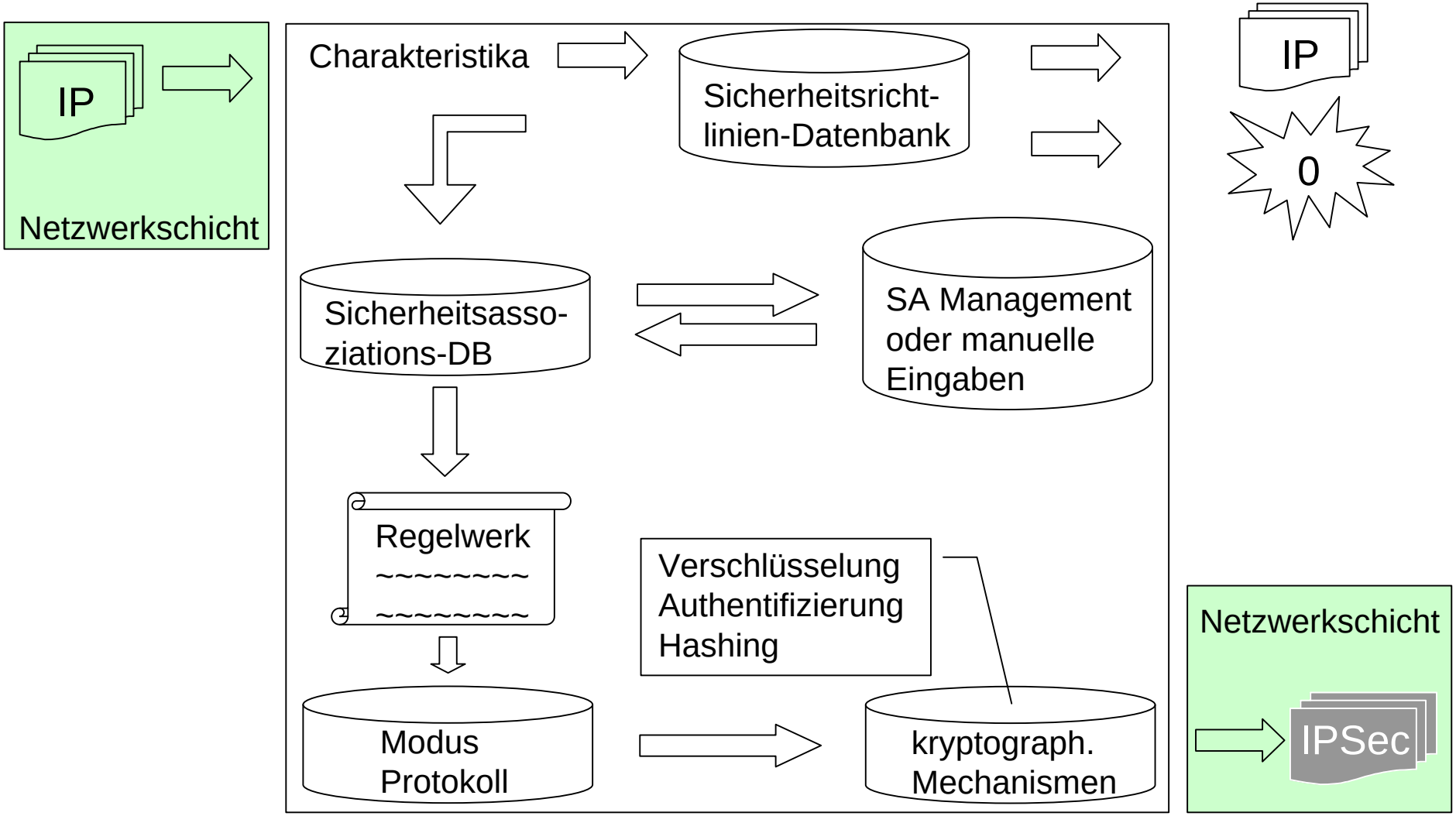
- speichert die SAs

## ISAKMP / IKE

(Internet Security Association & Key Management Protocol /Internet Key Exchange):

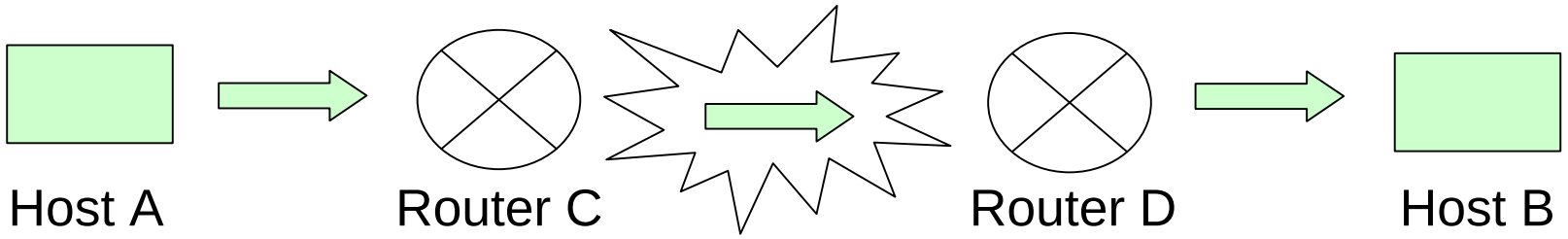
- Verwaltung der Sicherheitsassoziationen
- Schlüsselverwaltung
- bei Bedarf: „Unterprotokoll“ für Schlüsselaushandlung, z.B. IKE

# - Die Funktionalität von IPSec, blackbox -

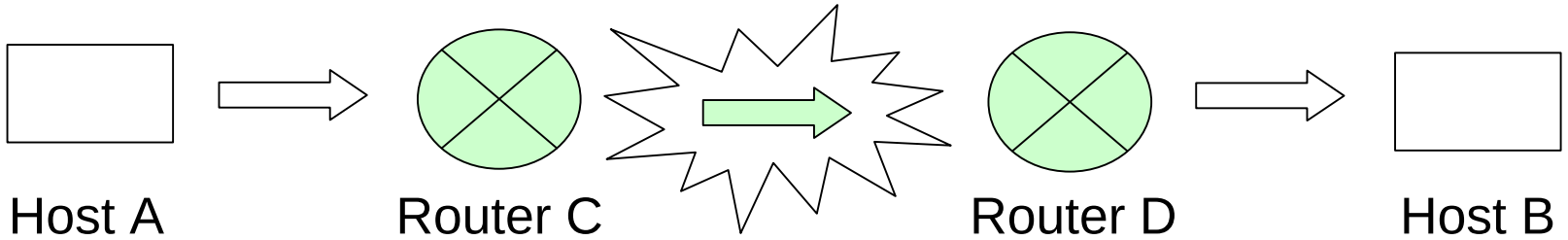


# - Modi -

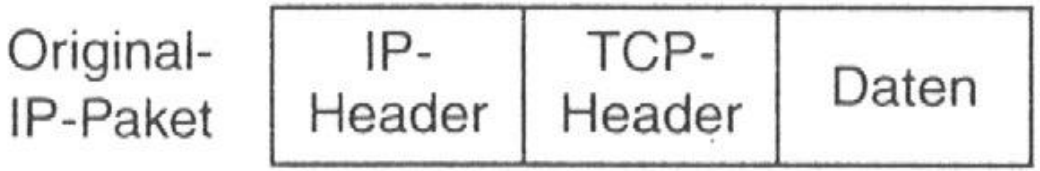
- Transport Modus (Host)
  - Kommunikationsendpunkt = IPSec-Endpunkt




- Tunnel Modus (Gateway)
  - Kommunikationsendpunkt ≠ IPSec-Endpunkt



# - Modi -



# - Modi, Vergleich -

Transportmodus:

- Ziel ist ein Host – Ende zu Ende
- Nur Daten aus oberen Schichten geschützt
- IP-Header unverändert, ungeschützt

Tunnelmodus:

- Ziel ist ein Gateway – Verbindung
- Neuer IP-Header bis zum Ende des Tunnels
- Komplettes Original-IP-Paket wird verkapselt
  - Schutz des Headers (Integrität, Auth., Verschl.)
  - „Anonymisierung“ der Quell- und Zieladresse

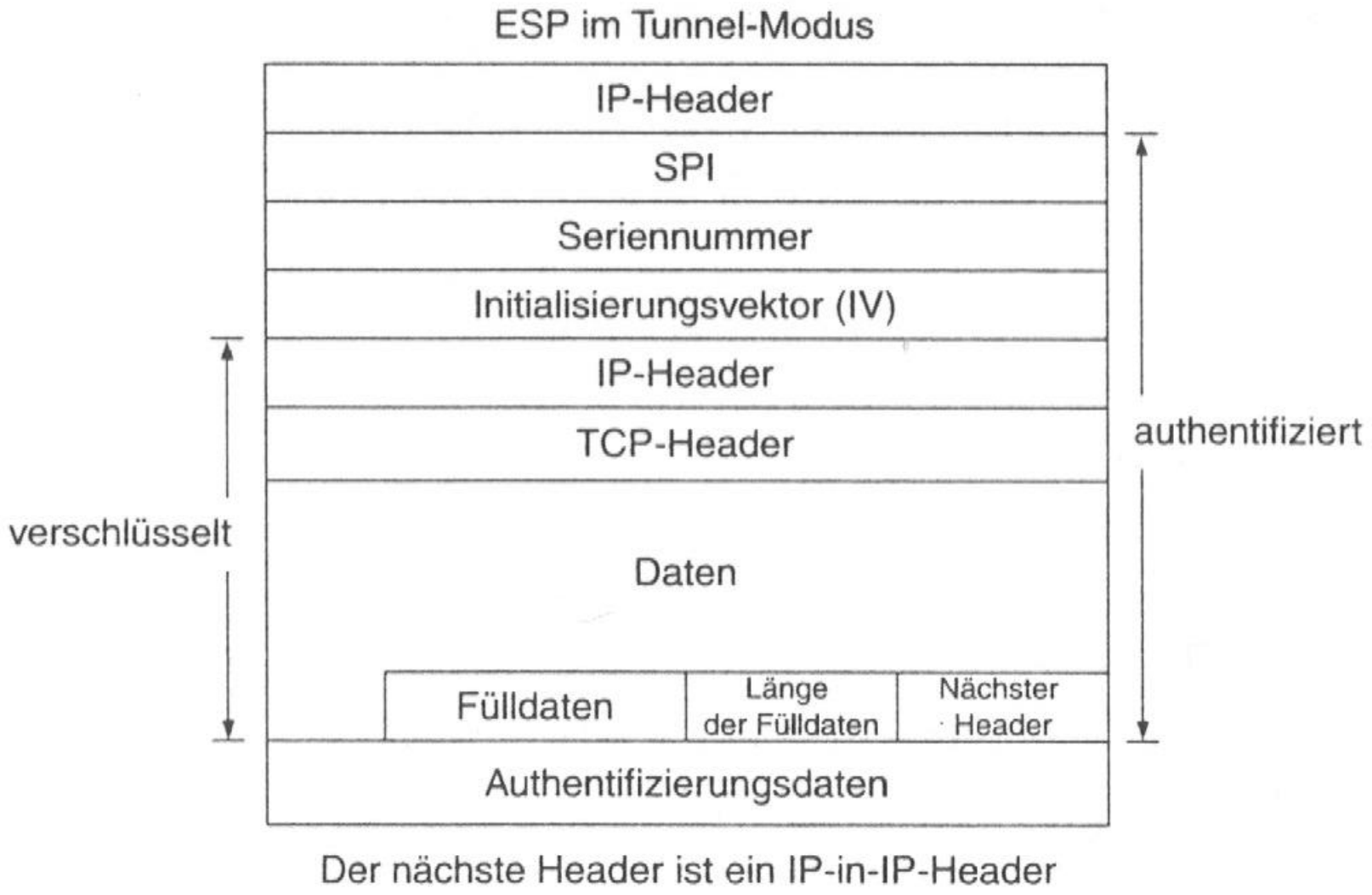
# - Encapsulated Security Payload -

- Sicherheitsdienste:
  - Verschlüsselung
  - Authentifizierung der Datenquelle
  - Integrität der Daten

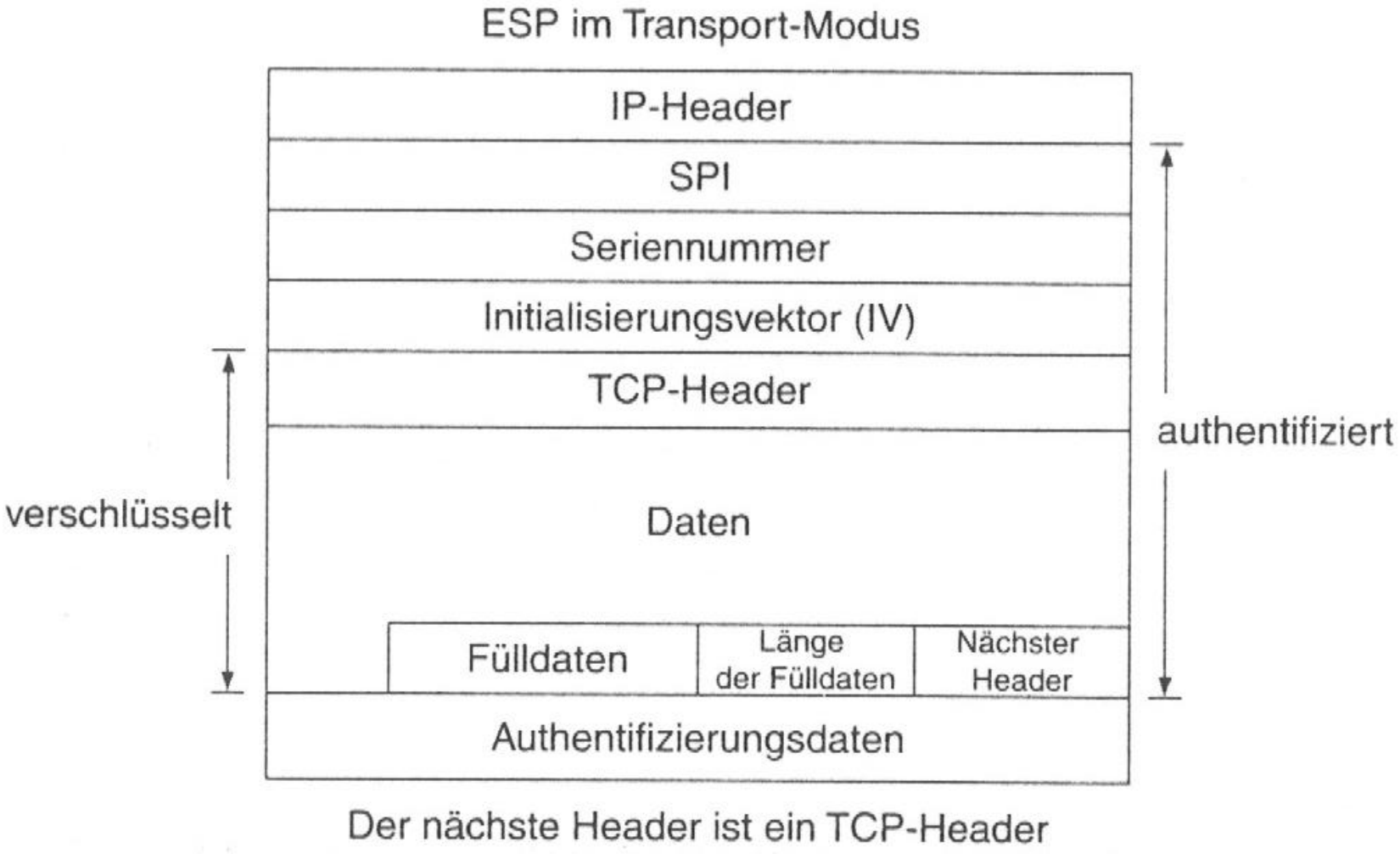
- Original-Paket wird verschlüsselt und in ein Neues eingepackt
  - von ESP-Header und ESP-Trailer umfasst

- Schutz vor Replay-Attacken durch Seriennummern

# - ESP im Tunnel-Modus -



# - ESP im Transport-Modus -

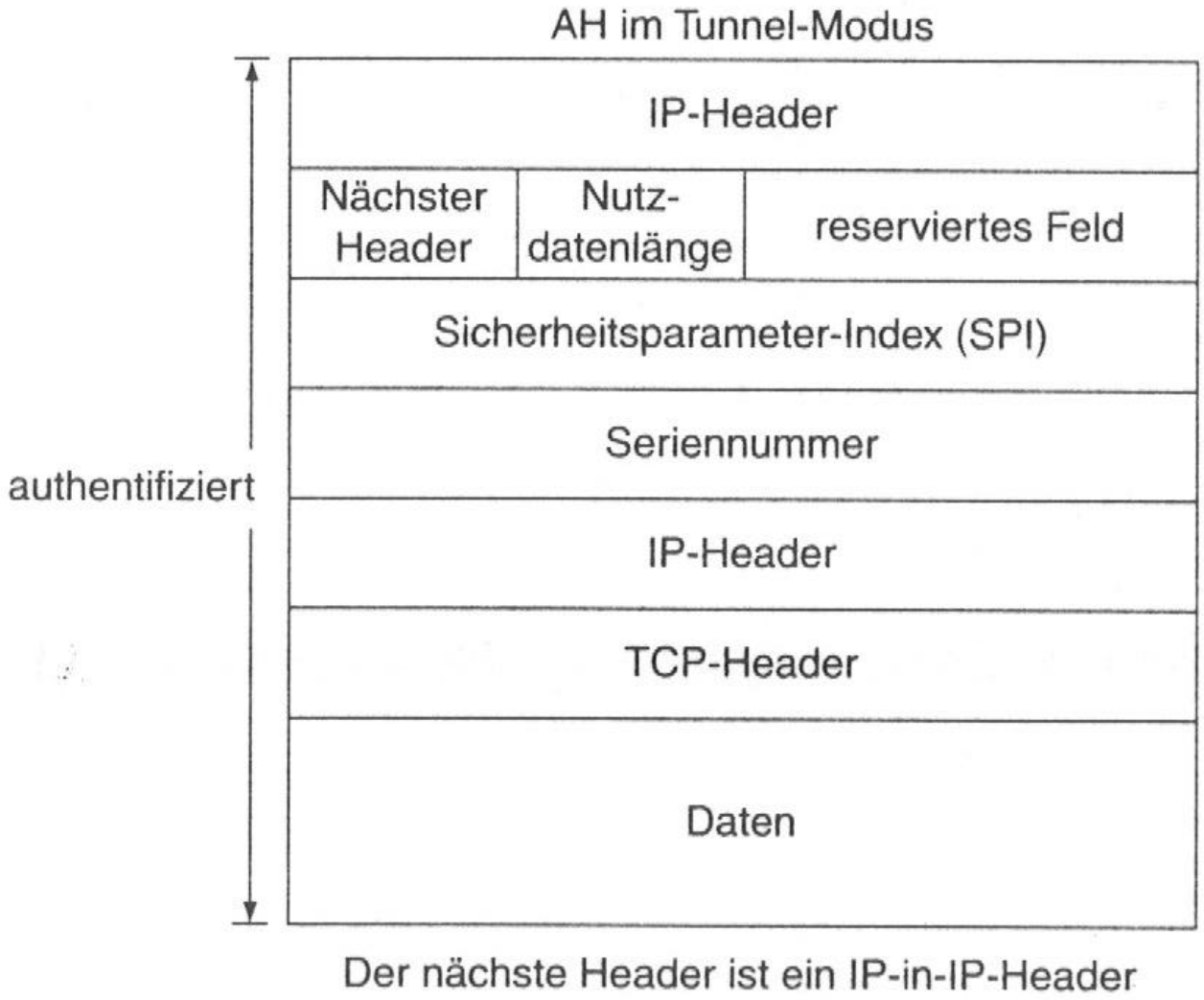


# - Authentication Header -

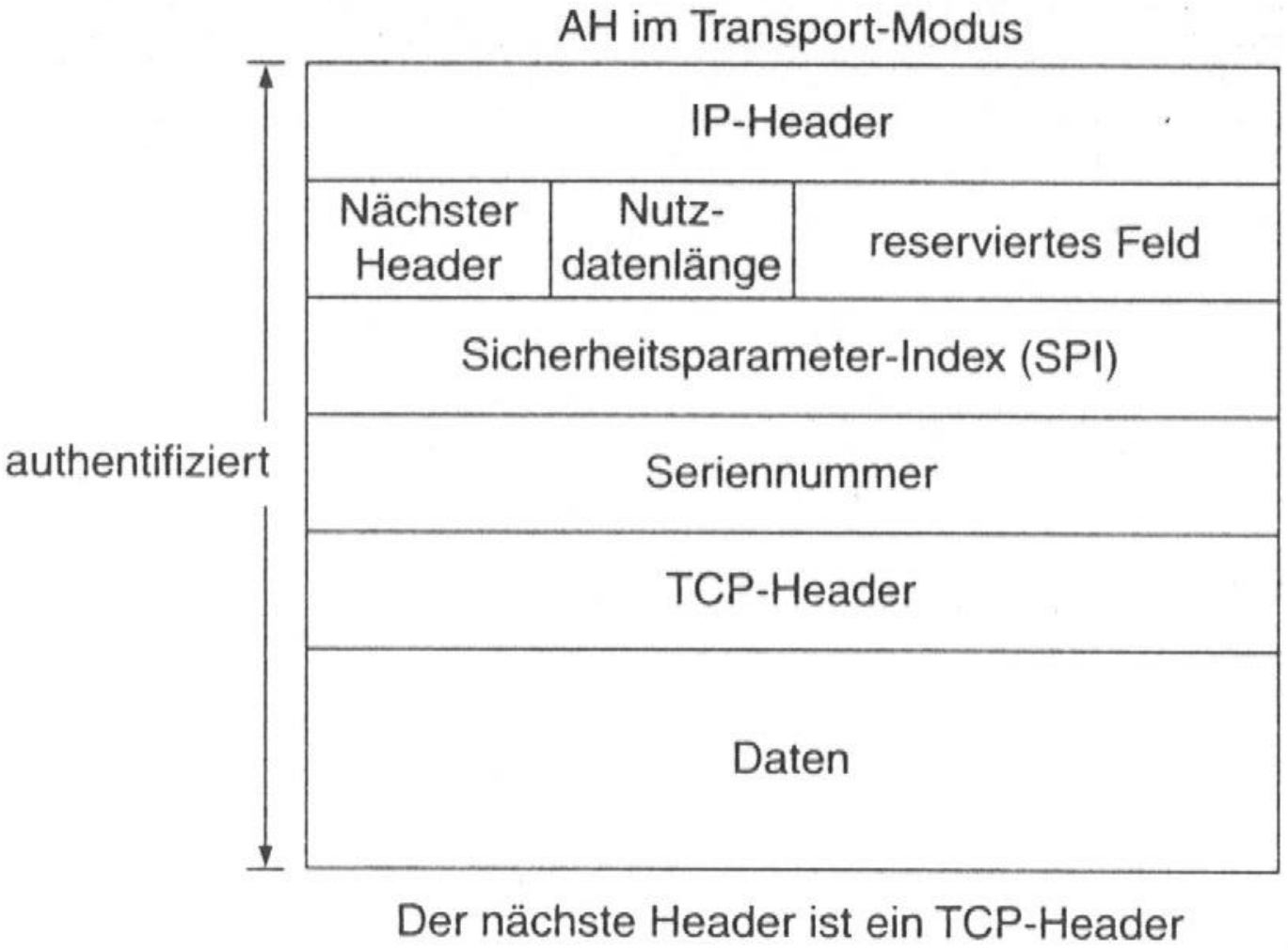
- Sicherheitsdienste:
  - Authentifizierung der Datenquelle
  - Integrität der Daten

- Original-Paket wird um AH-Header erweitert

# - AH im Tunnel-Modus -



# - AH im Transport-Modus -



# - ESP vs. AH -

- ESP bietet Vertraulichkeit durch Verschlüsselung
- AH fügt lediglich AH-Header ein,
  geringerer Overhead als bei ESP
- Beide bieten Authentifizierung der Datenquelle und
  Integrität

# - Varianten -

- ESP und AH können kombiniert werden
  - Jeweils eine SA erforderlich: SA-Bundle
  - SAs im Bundle können unterschiedliche Endpunkte haben

- Viele Kombinationen möglich, Beispiele:
  - AH (ESP(Original-Paket)): Authentifizierung berücksichtigt mehr Felder
  - ESP(AH(Original-Paket)): Authentifiziert den Quelltext

# - Sicherheit / Zukunft -

- Nach Schneier / Ferguson das momentan beste verfügbare IP-Sicherheits-Protokoll
- Auf Grund zu vieler Optionen / Flexibilität zu komplex → Komplexität vs. Sicherheit! (Komitee-Arbeit)
- Zu viele Modi → AH und Transport-Modus „überflüssig“
- Durch symm. Krypto. und CBC schnell und „sicher“
- Austauschbare Algorithmen für Zukunft
- Gute Zukunftschancen wg. Multicast, PCP usw.

# - RFCs -

- 2401: Security Architecture for the Internet Protocol
- 2402: IP Authentication Header
- 2406: IP Encapsulating Security Payload
- 2408: ISAKMP
- 2409: IKE

- Weitere auf **http://www.ietf.org/html.charters/ipsec-charter.html**

# Danke für die Aufmerksamkeit!