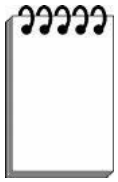
Modul 4: IPsec – Teil 1

Teil 1:

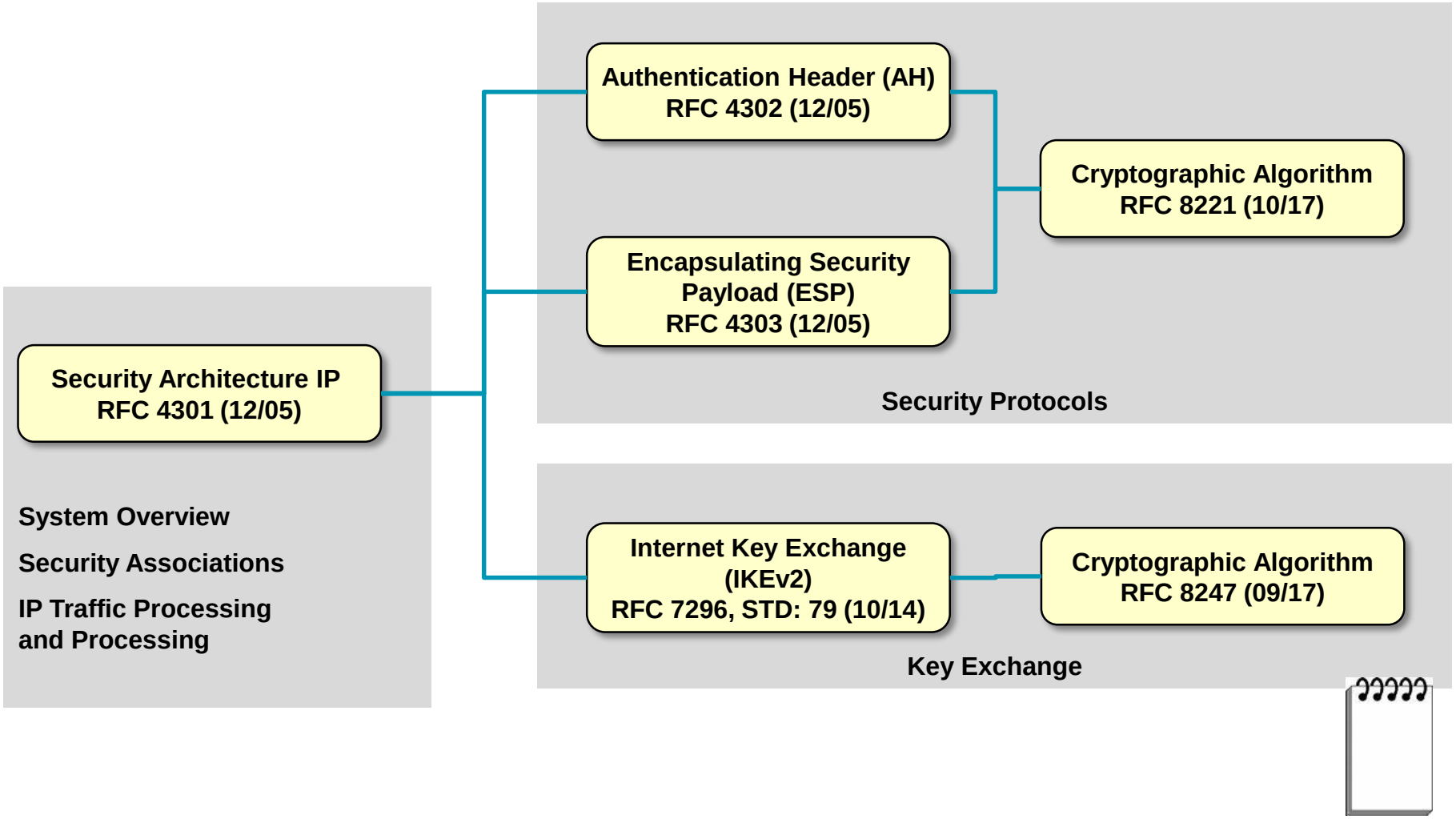
- Transport- und Tunnelmode
- Authentication Header
- Encapsulating Security Payload
- IPsec Architektur (Security Association, SAD, SPD),

Teil 2:

- Das IKE-Protokoll



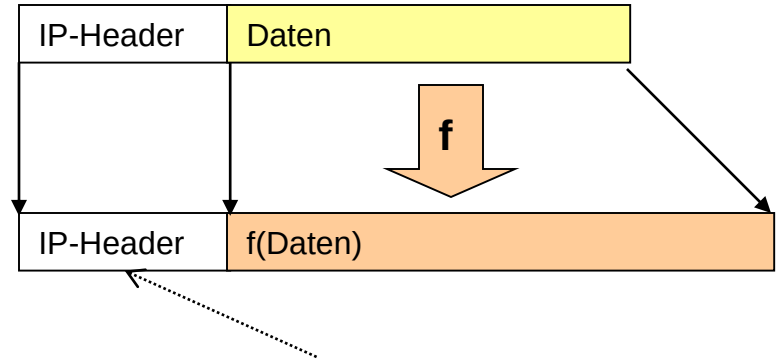
Struktur der IPsec-relevanten RFCs



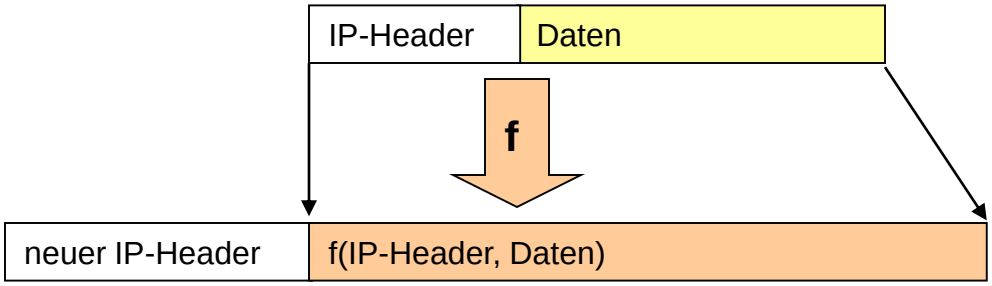
IPSec Überblick

- 2 Modi:
  - Transport-Mode (=Original-Header) → nur E-E
  - Tunnel-Mode (=gekapselt): ermöglicht den Aufbau virtueller Netze → E-E, E-G / G-G
- Authentication Header (AH): für Integrität + Authentizität
- Encapsulating Security Payload (ESP): für Vertraulichkeit + implizite Authentizität
- Security Assosiation (SA): *"Verbindungskontext"*
  - Security parameter index (SPI): dient der Identifikation des Verbindungskontextes
  - Security policy database (SPD):
    regelt die Anwendung des richtigen Verbindungskontextes
  - SA database (SAD):
    dynamisches Repository für Verbindungskontexte
- Management von Sicherheitsassoziationen (Internet Key Exchange, IKE)
  - Internet Security Association and Key Management Protocol (ISAKMP):
    Abstrakte Protokollbasis zum Etablieren von SAs
  - Oakley: Schlüsselaustausch basierend auf Diffie-Hellmann
  - Domain of Interpretation (DOI):
    konkrete Spezifikation der vereinbarten Parameter und Konventionen

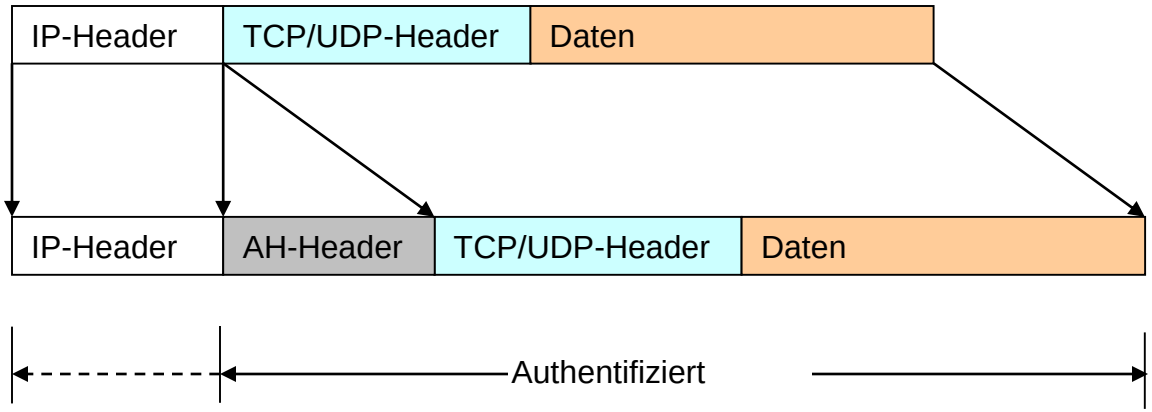
Transport- und Tunnelmode

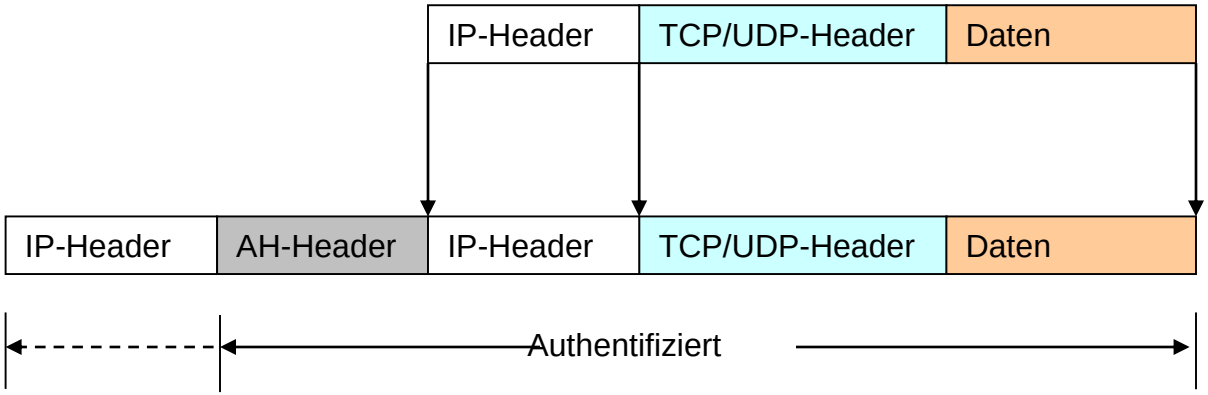


nur Länge modifiziert

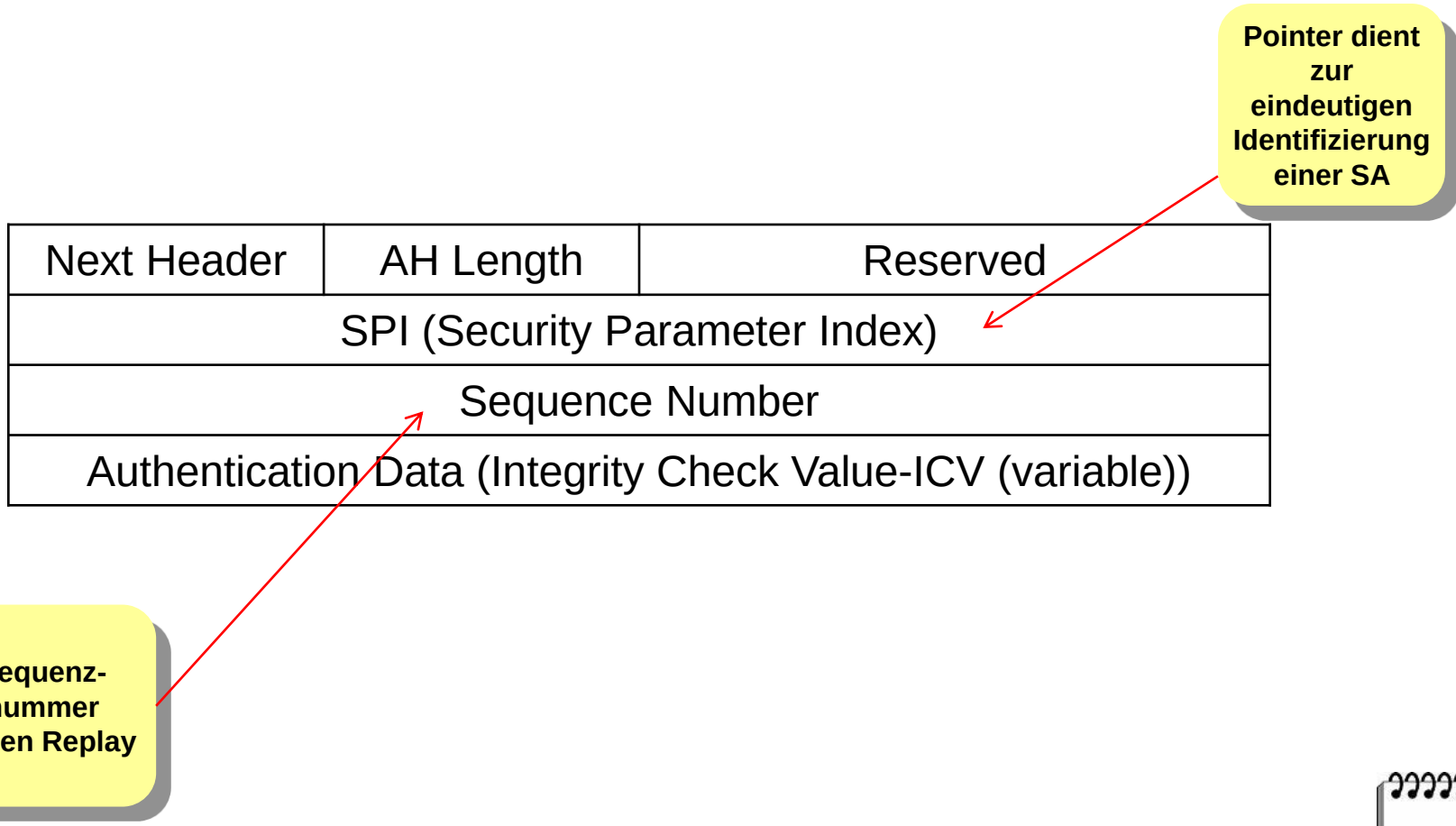


AH im Transport Mode / AH im Tunnel Mode





Aufbau des IPsec AH-Header-Formats (RFC4302, 12/05)



HMAC für AH-Authentifizierung

Variante 1:

- **MAC = H(*key* ‖ *message*)**

Variante 2:

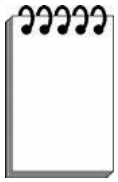
- **MAC = H(*message* ‖ *key*)**

Variante 3:

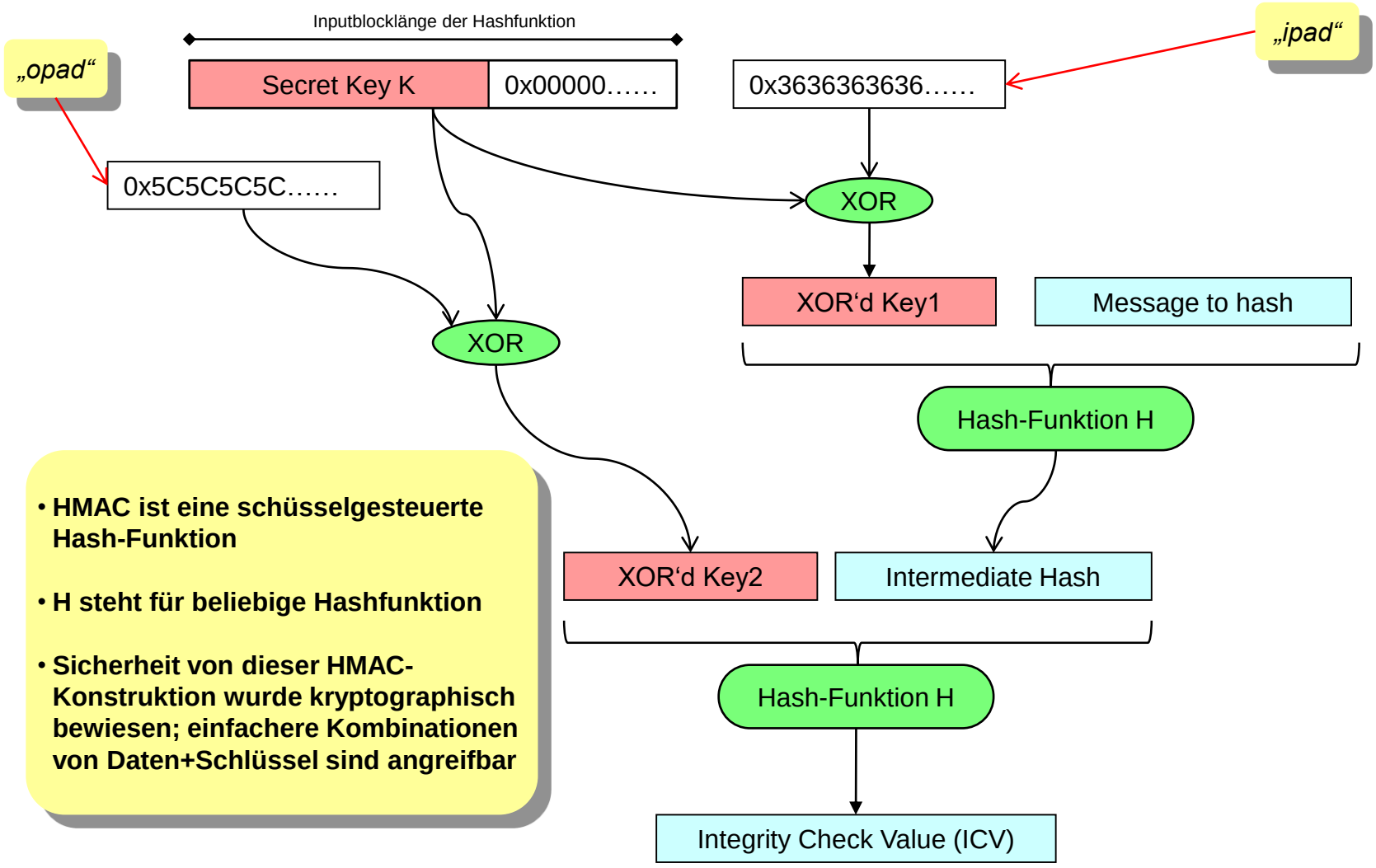
- **MAC = H(*key* ‖ *message* ‖ *key*)**

Variante 4:

- **H(*key1* ‖ H(*key2* ‖ *message*))**



HMAC für AH-Authentifizierung nach RFC 2104 (Updated by: RFC 6151)



- **HMAC ist eine schüsselgesteuerte Hash-Funktion**
- **H steht für beliebige Hashfunktion**
- **Sicherheit von dieser HMAC-Konstruktion wurde kryptographisch bewiesen; einfachere Kombinationen von Daten+Schlüssel sind angreifbar**

Empfehlungen des BSI zu AH

Aus Technische Richtlinie TR-02102-3 (Version 2018-01)
Kryptographische Verfahren: Empfehlungen und Schlüssellängen

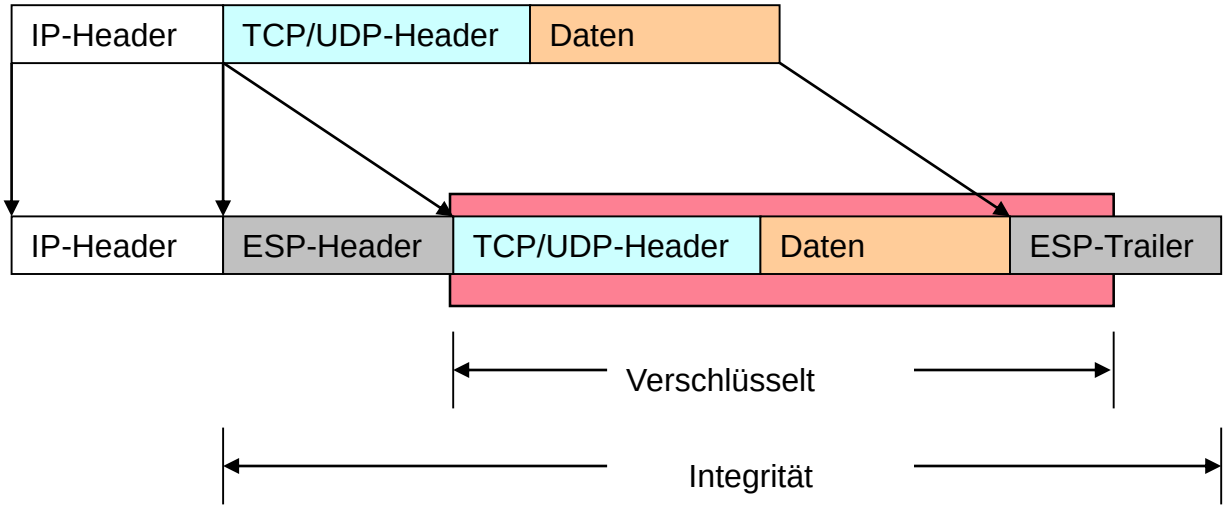
Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)

Lfd. Nr.	*Verfahren*	*IANA-Nr.*	*Spezifiziert in*	*Verwendungs-zeitraum*
1	AUTH_HMAC_SHA1_96	2	[RFC2404]	2018+
2	AUTH_AES_XCBC_96	5	[RFC3566]	2024+
3	AUTH_AES_CMAC_96	8	[RFC4494]	2024+
4	AUTH_HMAC_SHA2_256_128	12	[RFC4868]	2024+
5	AUTH_HMAC_SHA2_384_192	13		2024+
6	AUTH_HMAC_SHA2_512_256	14		2024+

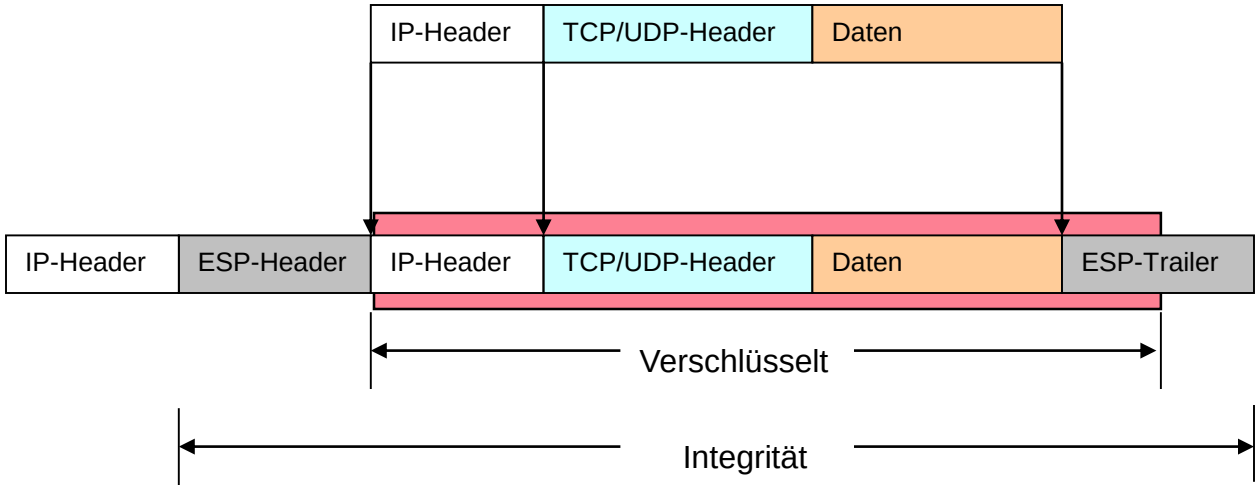
Tabelle 9: Integritätsschutz der AH-Pakete

- **Berechnung des Integrity Check Values (ICV)**
- **Für Neuentwicklungen wird eines der auf SHA-2 basierenden Verfahren (Nr. 4-6) in Tabelle 9 empfohlen.**

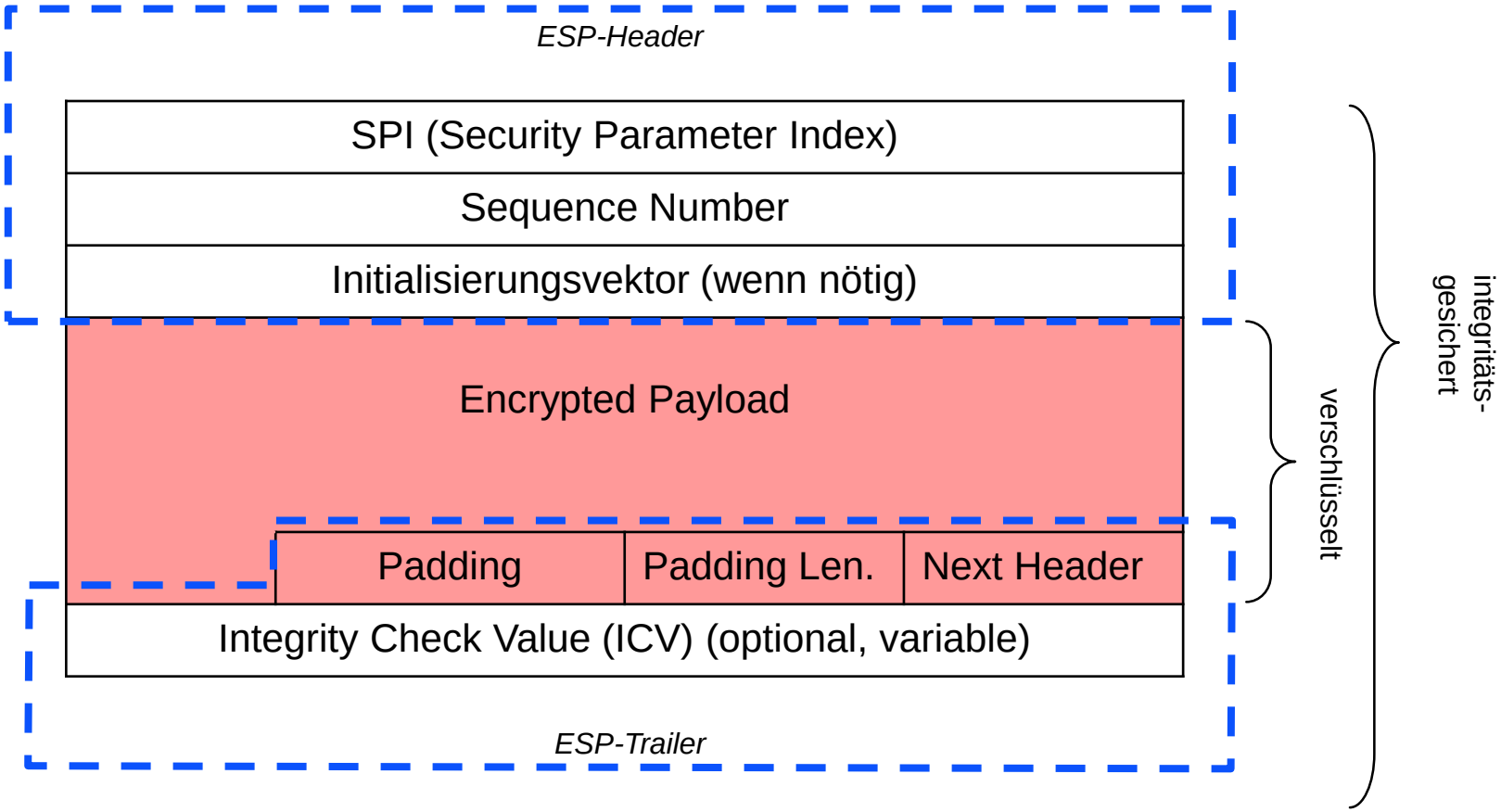
ESP (Encapsulating Security Payload) im Transport Mode



ESP im Tunnel Mode



Aufbau des IPsec ESP-Header-Format (RFC4303, 12/05)



Empfehlungen des BSI zu ESP

Aus Technische Richtlinie TR-02102-3 (Version 2018-01)
Kryptographische Verfahren: Empfehlungen und Schlüssellängen

- **Neuerungen 2017: Erhöhung der Bitlängen von RSA, DH und DSA auf 3000 Bit ab 2023**
- **Neuerung 2018: Anpassung der Verwendungszeiträume**

Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)

Lfd. Nr.	*Verfahren*	*IANA-Nr.*	*Spezifiziert in*	*Bemerkungen*	*Verwendungszeitraum*
1	ENCR_AES_CBC	12	[RFC3602]	Muss mit einem Verfahren aus Abschnitt 3.3.2 kombiniert werden.	2024+
2	ENCR_AES_CTR	13	[RFC3686]		
3	AES-GCM with a 16 octet ICV	20	[RFC4106]	Bei Verwendung der Betriebsart GCM kann ein separater Integritätsschutz der ESP-Pakete entfallen.	2024+
4	AES-GCM with a 12 octet ICV	19			

Tabelle 7: Verschlüsselung der ESP-Pakete

Empfehlungen des BSI zum Integritätsschutz von ESP-Paketen.

Aus Technische Richtlinie TR-02102-3 (Version 2018-01)
Kryptographische Verfahren: Empfehlungen und Schlüssellängen

Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)

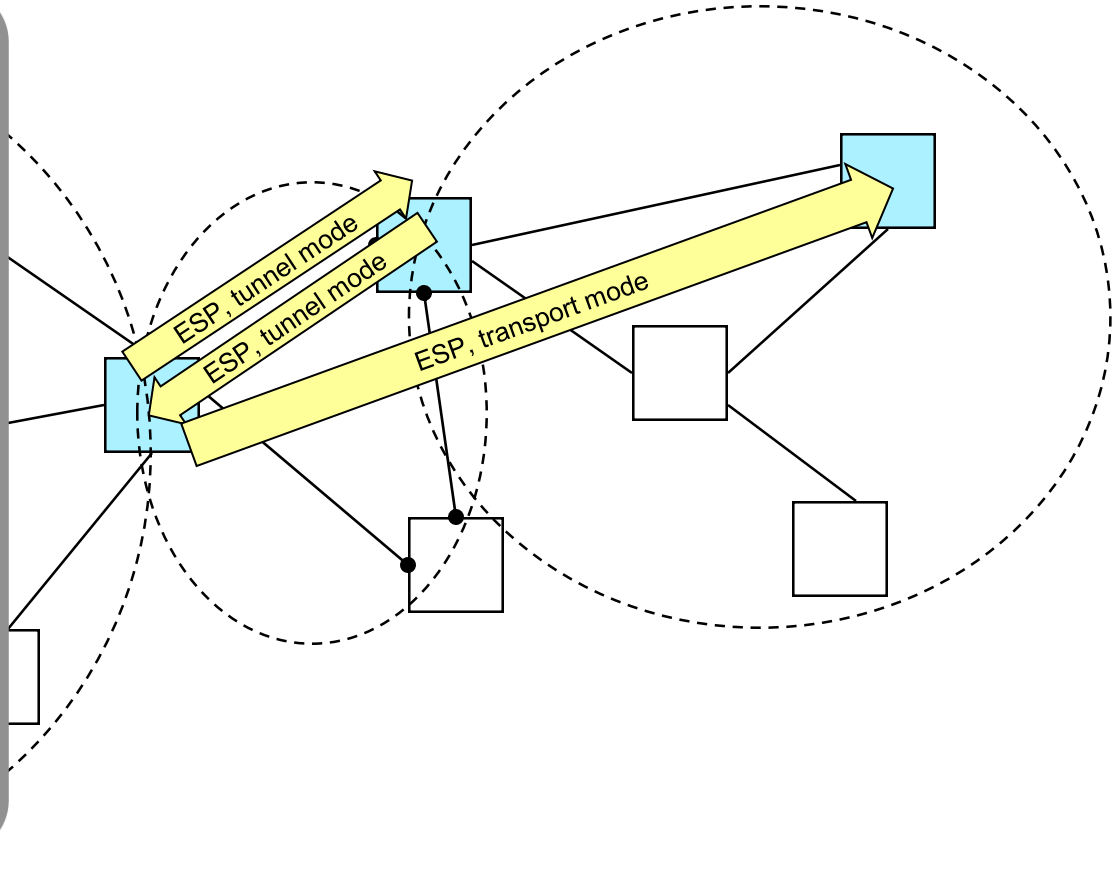
Lfd. Nr.	*Verfahren*	*IANA-Nr.*	*Spezifiziert in*	*Verwendungs-zeitraum*
1	AUTH_HMAC_SHA1_96	2	[RFC2404]	2018+
2	AUTH_AES_XCBC_96	5	[RFC3566]	2024+
3	AUTH_AES_CMAC_96	8	[RFC4494]	2024+
4	AUTH_HMAC_SHA2_256_128	12	[RFC4868]	2024+
5	AUTH_HMAC_SHA2_384_192	13		
6	AUTH_HMAC_SHA2_512_256	14		

Tabelle 8: Integritätsschutz der ESP-Pakete

- **Für Neuentwicklungen wird eines der auf SHA-2 basierenden Verfahren (Nr. 4-6) in Tabelle 8 empfohlen.**

Security Association (SA)

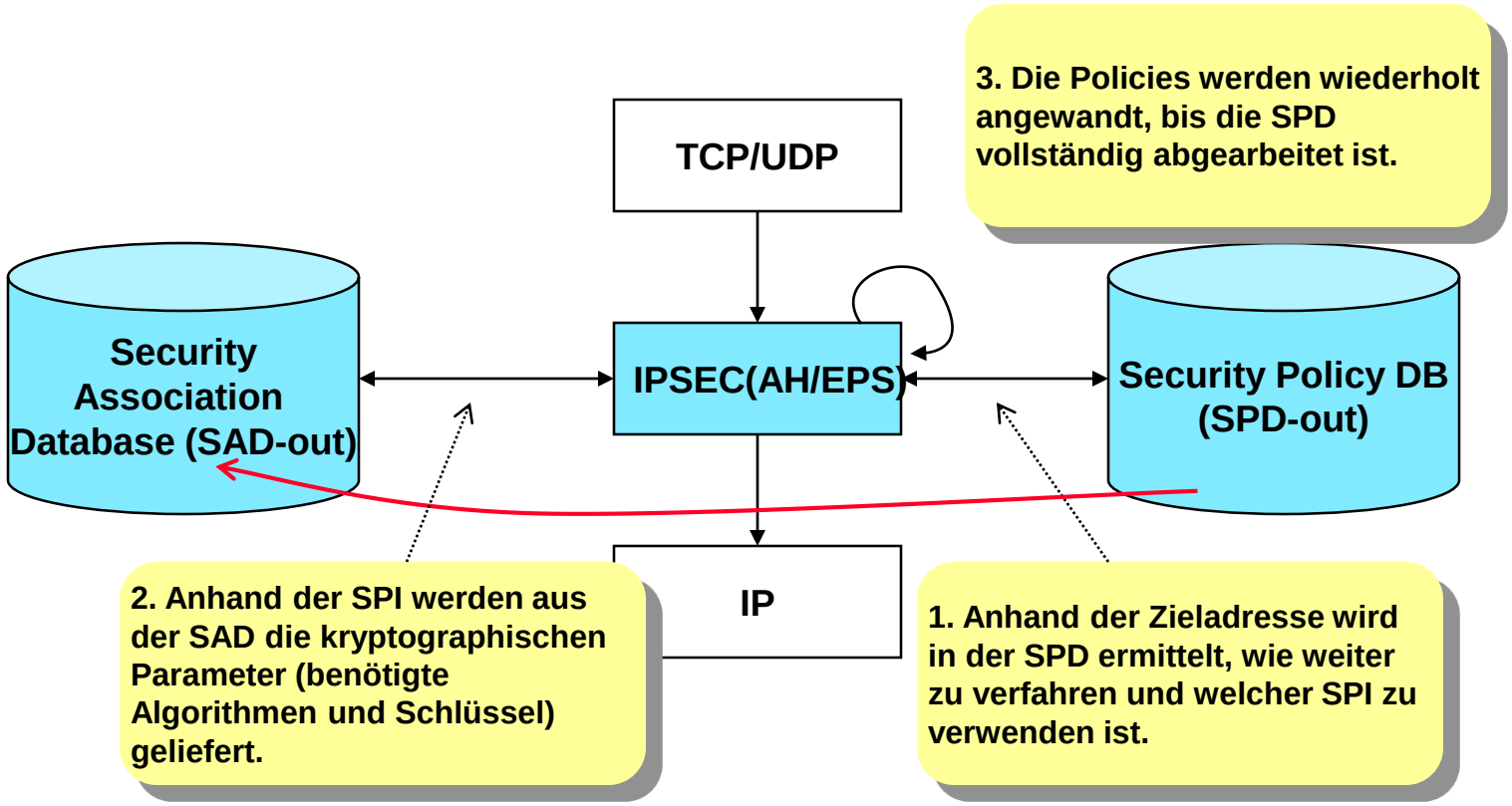
- nur für eine unidirektionale Verbindung
- nur für einen Mechanismus: AH oder ESP
- Ggf. Bündel von SA‘s
- Eindeutige Identifizierung einer SA:
  - Security Parameter Index (SPI)
    - Bitstring mit lokaler Bedeutung
    - SPI Bestandteil von AH- und ESP-Header
    - Verknüpfung mit SA
  - IP-Zieladresse
    - Endbenutzersystem oder Netzwerksystem (Router, Firewall)
    - zur Zeit nur Unicast-Adressen erlaubt
  - Sicherheitsprotokoll-ID: AH- oder ESP-SA



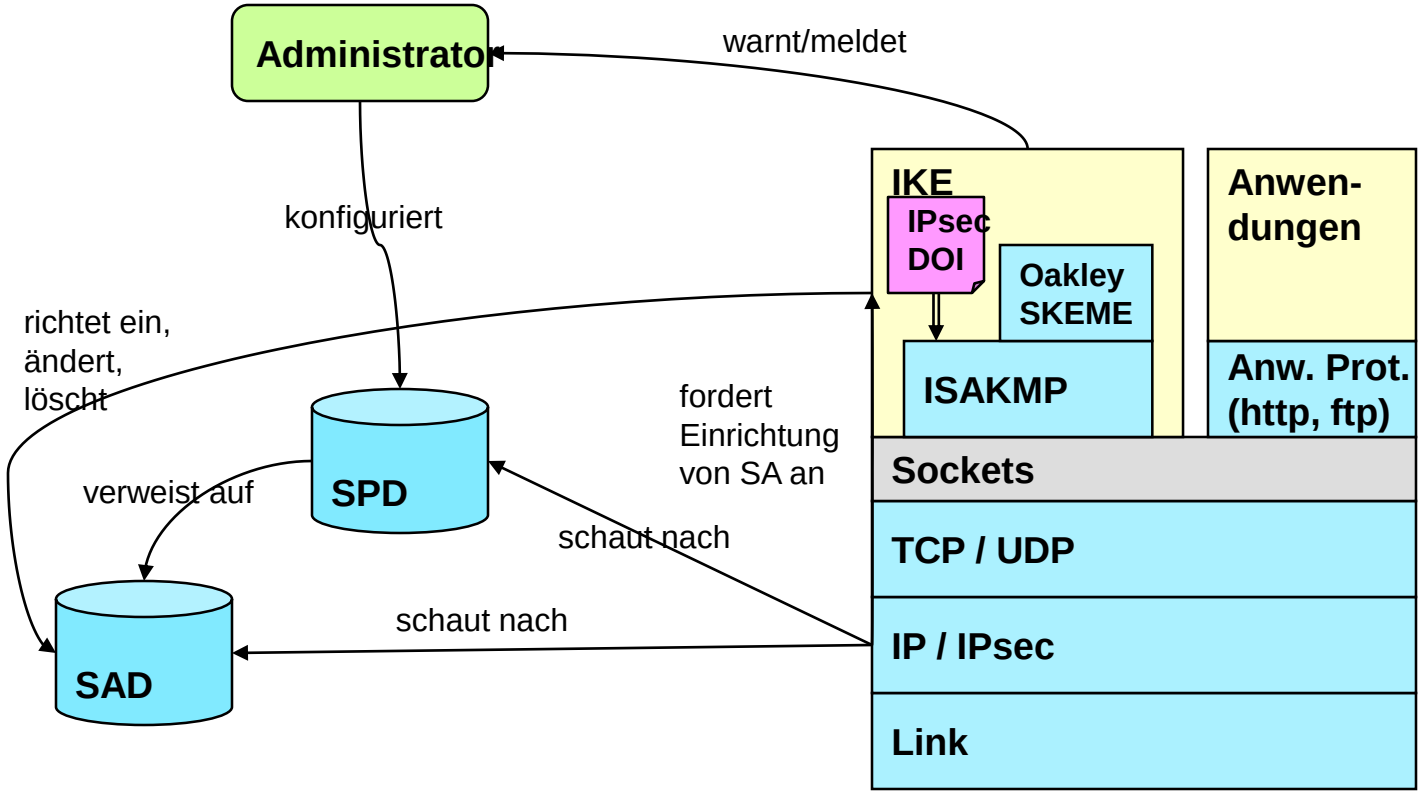
Parameter einer SA

- **Sequence Number Counter:**
  - 32 Bitwert zum Zählen der Pakete mit einer SA
- **Lebensdauer der SA:**
  - Zeitintervall oder Byte-Zähler
- **IPSec Protokoll-Modus:**
  - Tunnel, Transport Modus.
- **AH-Information**
  - Authentifizierungsalgorithmus
  - Schlüssel
  - Lebensdauer des Schlüssels
- **ESP-Information**
  - Verschlüsselungs- und Authentifizierungsalgorithmus
  - Schlüssel
  - Anfangswerte
  - Lebensdauer des Schlüssels

Ablauf: Zu sendendes IP-Paket



Organisation von IPsec



nach: Ghislaine Labouret: Ipsec: a technical overview (Ghislaine.Labouret@hsc.fr)

Komponenten des IPsec-Assoziationsmanagements

- **ISAKMP (Internet Security Association and Key Management Protocol)**

  Meta-Protokoll, das Pakettypen und Formate für den Schlüsselaustausch und das Management von SAs definiert.

  Generische Operationen für Aufbau und Management von SAs.

- **IKE (Internet Key Exchange)**

  Rahmen-Anwendung für das Management der SAs in der SAD und für den Schlüsselaustausch.

  Phase 1: Etablierung eines SAs für IKE

  Phase 2: Etablierung von IPsec SAs