Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

IPSec Verschlüsselung

- Vorlesung -

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

IPSec Verschlüsselung
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- IPSec Header
- IPSec Schlüsselmanagement
- Protokollmitschnitt
- Zusammenfassung

IPSec Verschlüsselung
→ Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- Einleitung
- IPSec Header
- IPSec Schlüsselmanagement
- Protokollmitschnitt
- Zusammenfassung

Ziele und Ergebnisse der Vorlesung
→ IPSec Verschlüsselung

- Gutes Verständnis für die **Cyber-Sicherheitsmechanismen** von IPSec.
- Erlangen der Kenntnisse über die verschiedenen **IPSec-Header** und das zentrale **Schlüsselmanagement** von IPSec.
- Gewinnen von praktischen Erfahrungen durch die Betrachtung eines **Protokollmitschnittes**.

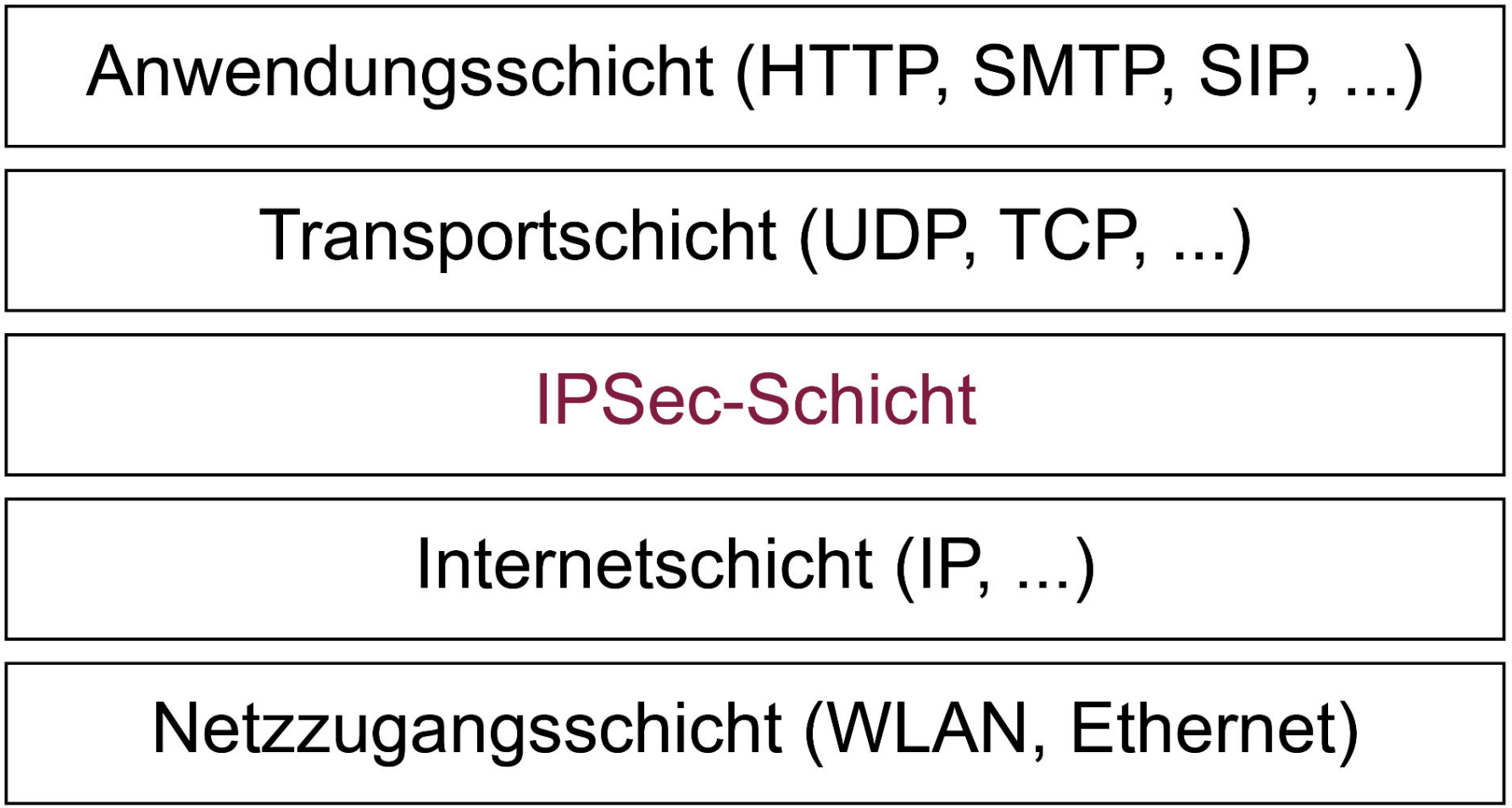
IPSec Verschlüsselung
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- **Einleitung**
- IPSec Header
- IPSec Schlüsselmanagement
- Protokollmitschnitt
- Zusammenfassung

Einleitung
→ Einordnung (1/2)

- IPSec := Internet Protocol Security
- Weiterentwicklung des IP-Protokolls (IP).
- Entwickelt von der Internet Engineering Task Force (IETF).
- Arbeitet direkt auf der Vermittlungsschicht.
- IPSec war als Feature in IPv6 gedacht und ergänzt aber auch das bestehende IPv4 Protokoll um wichtige Cyber-Sicherheitsfunktionen.

Einleitung
→ Einordnung (2/2)



Einleitung
→ Cyber-Sicherheitsfunktionen (1/2)

- **Verschlüsselung** schützt die Vertraulichkeit der übertragenen Daten
  (Jedes Paket kann verschlüsselt werden.)

- **HMAC-Funktion** sorgt für die Authentizität, Unversehrtheit der übertragenen Daten
  (Jedes Paket kann gegen Manipulation geschützt und auf die Echtheit überprüft werden.)

- **Anti-Replay-Mechanismus** schützt vor unberechtigter Wiedereinspielung von übertragenen Daten
  (Jedes Paket kann vor Wiedereinspielung geschützt werden.)

Einleitung
→ Cyber-Sicherheitsfunktionen (2/2)

- **Authentifikation** gewährleistet die Eindeutigkeit und Echtheit der Kommunikationspartner
  (Die Kommunikationspartner können authentifiziert werden.)

- **Tunneling** verschleiert den Datentransfer für definierte Aspekte
  (Die IP-Kommunikation kann gegen einen gewissen Grad der Verkehrsflussanalyse geschützt werden.)

IPSec Verschlüsselung
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- **IPSec Header**
- IPSec Schlüsselmanagement
- Protokollmitschnitt
- Zusammenfassung

IPSec Header
→ Erweiterung von IP (1/2)

- Einfügen von Erweiterungs-Header in die IP Pakete.

- In den IPSec-Headern sind nur minimal notwendige Informationen für die Kommunikationsendpunkte untergebracht:
  - Verweise auf spezielle Datenbanken.
  - Security Associations → Security-Management.

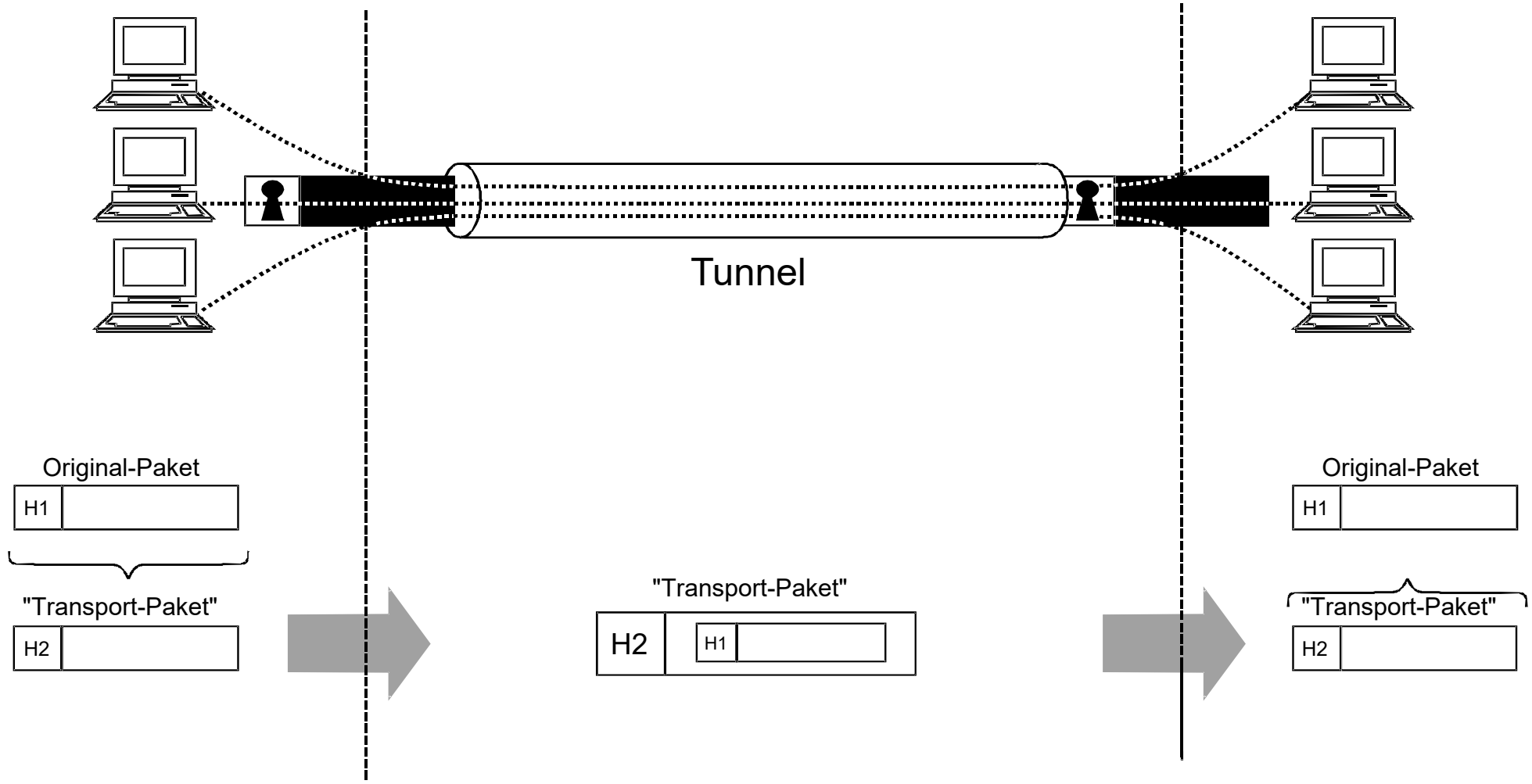
- **Authentication Header (AH, RFC 2402)**
  - Datenunversehrtheit
  - Authentifikation
  - Anti-Replay Service (Optional)

IPSec Header
→ Erweiterung von IP (2/2)

- **Encapsulated Security Payload (ESP, RFC 2406)**
  - Datenunversehrtheit und Authentifikation (Optional)
  - Anti-Replay Service (Optional)
  - Verschlüsselung (Optional)

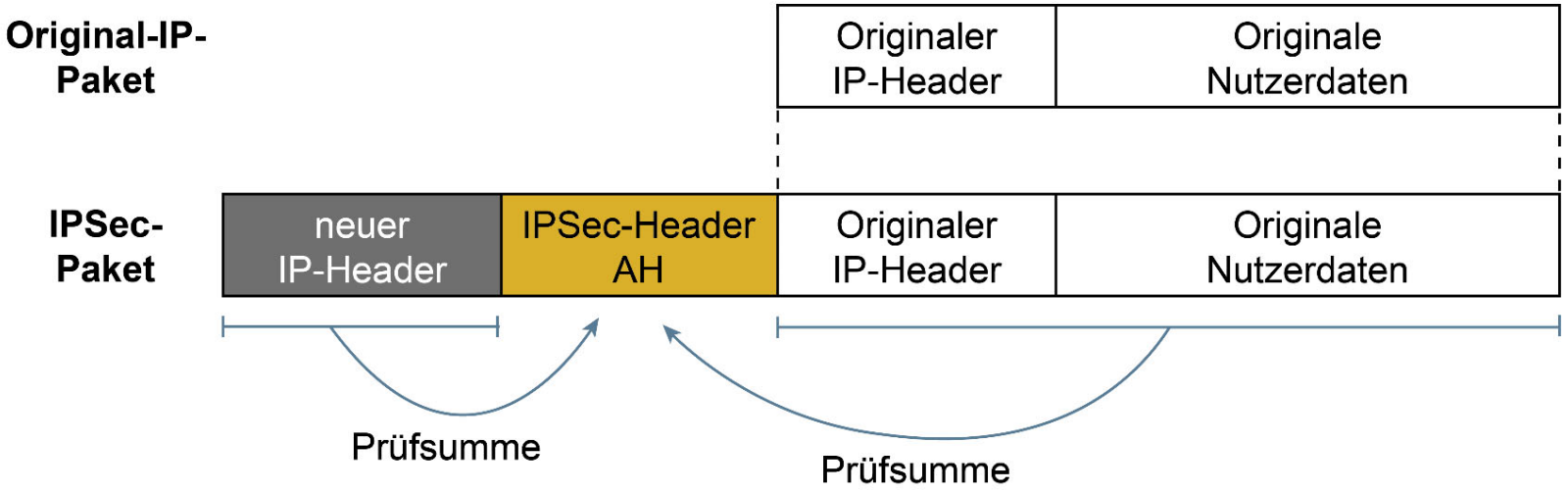
- Diese zusätzlichen IPSec-Header können in verschiedenen Modi verwendet werden:
  - **'Transportmode'**= Verschlüsselung der Nutzdaten
  - **'Tunnelmode'** = Verschlüsselung des IP-Headers und der Nutzdaten

IPSec Tunneling
→ Idee



IPSec Header
→ Authentication Header (AH)

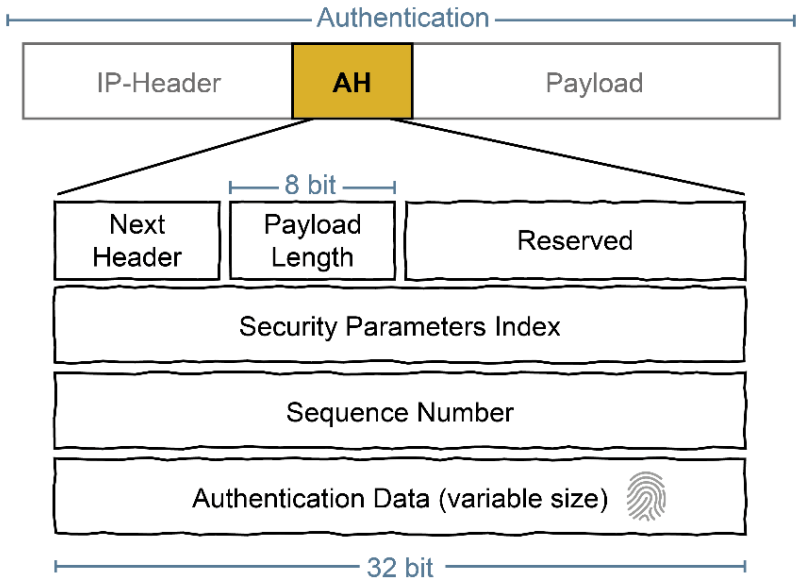
- AH im Tunnel-Mode:



- AH sorgt für eine starke Integrität und Authentizität der IP Pakete.
- Über das gesamte IP Paket und das Authentication-Feld selbst wird ein HMAC berechnet.
  - Felder, die während des Transportes modifiziert werden sind nicht inbegriffen (TTL, TOS, Flags und Header Checksum).
  - Ende-zu-Ende Überprüfung.

IPSec Header
→ Beschreibung des IPSec-Headers „AH“

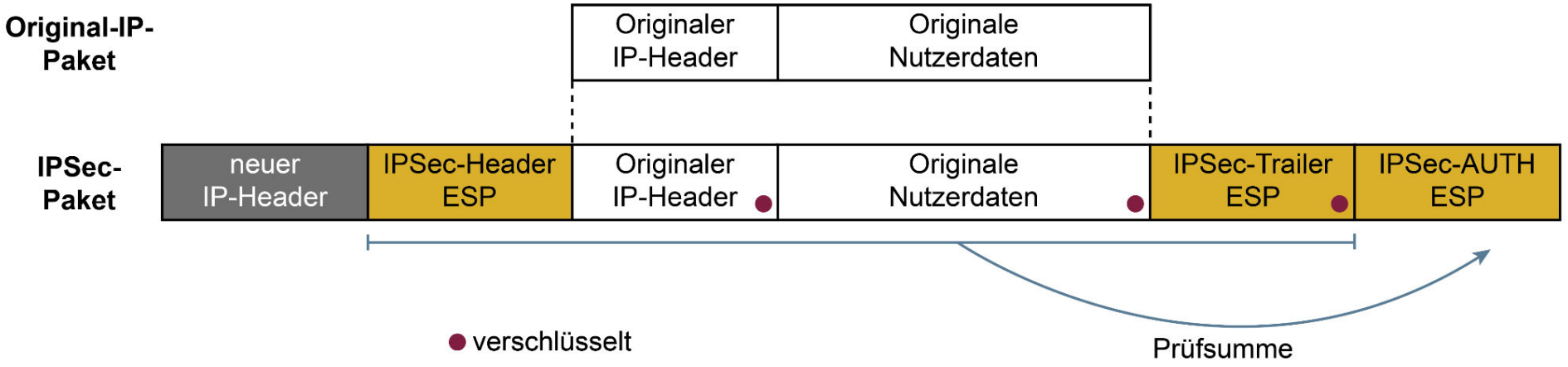
- **Next Header** (8-Bit): Datentyp der nächsten Daten hinter dem AH.
- **Payload Length** (8 Bit): Länge des AH in 32-bit Worten.
- **Reserved**: Zukünftige Funktionen.



- **SPI** (32 Bit): Beliebiger Wert, der in Kombination mit der Ziel IP-Adresse und dem „AH“ eindeutig die Security Association für dieses Paket definiert.
- **Sequence Number** (32 Bit): Zähler gegen Replay-Angriffe.
- **Authentication Data** (ganzzahliges Vielfaches von 32 Bit): Ergebnis vom HMAC.

IPSec Header
→ Encapsulated Security Payload (ESP)

- ESP im Tunnel-Mode:

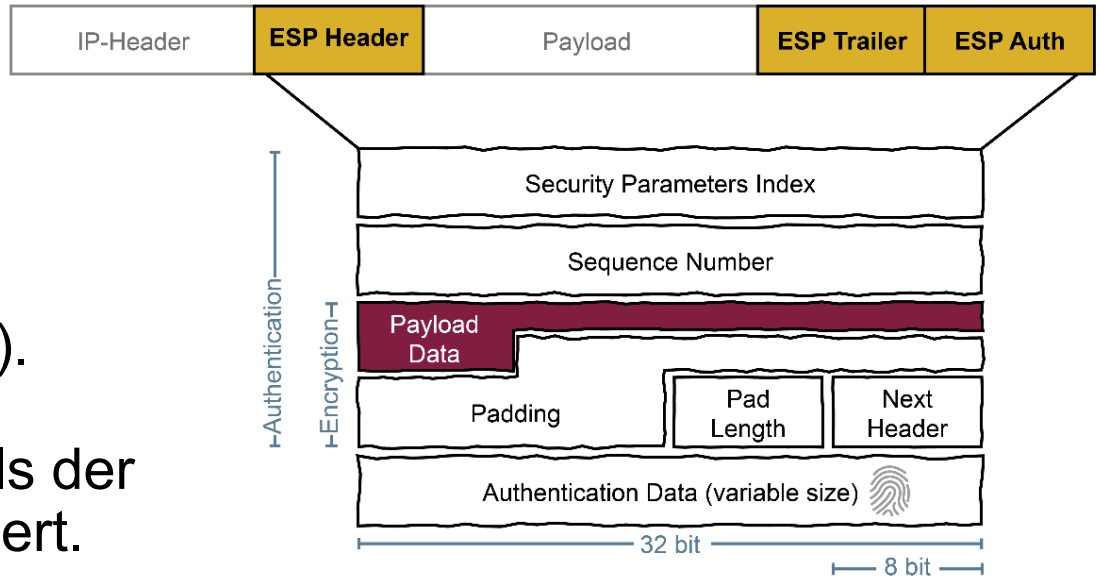


- Verschlüsselung des IP-Headers und der Nutzdaten mit einem symmetrischen Verschlüsselungsverfahren (z.B. AES).

- Keine Integrität und Authentizität des „Outer IP-Headers“.

IPSec Header
→ Beschreibung des IPSec-Headers „ESP“

- **SPI** (32 Bit): Beliebiger Wert, der in Kombination mit der Ziel IP-Adresse und dem „ESP“ eindeutig die Security Association definiert.
- **Sequence Number** (32 Bit): Zähler gegen Replay-Angriffe.
- **Payload Data** (variable Länge): Beinhaltet das originale IP-Paket (evtl. Initialization Vector zu Beginn).
- **Padding** (0-255 Byte)**:** Auffüllen falls der Verschlüsselungs-Mode dies erfordert.

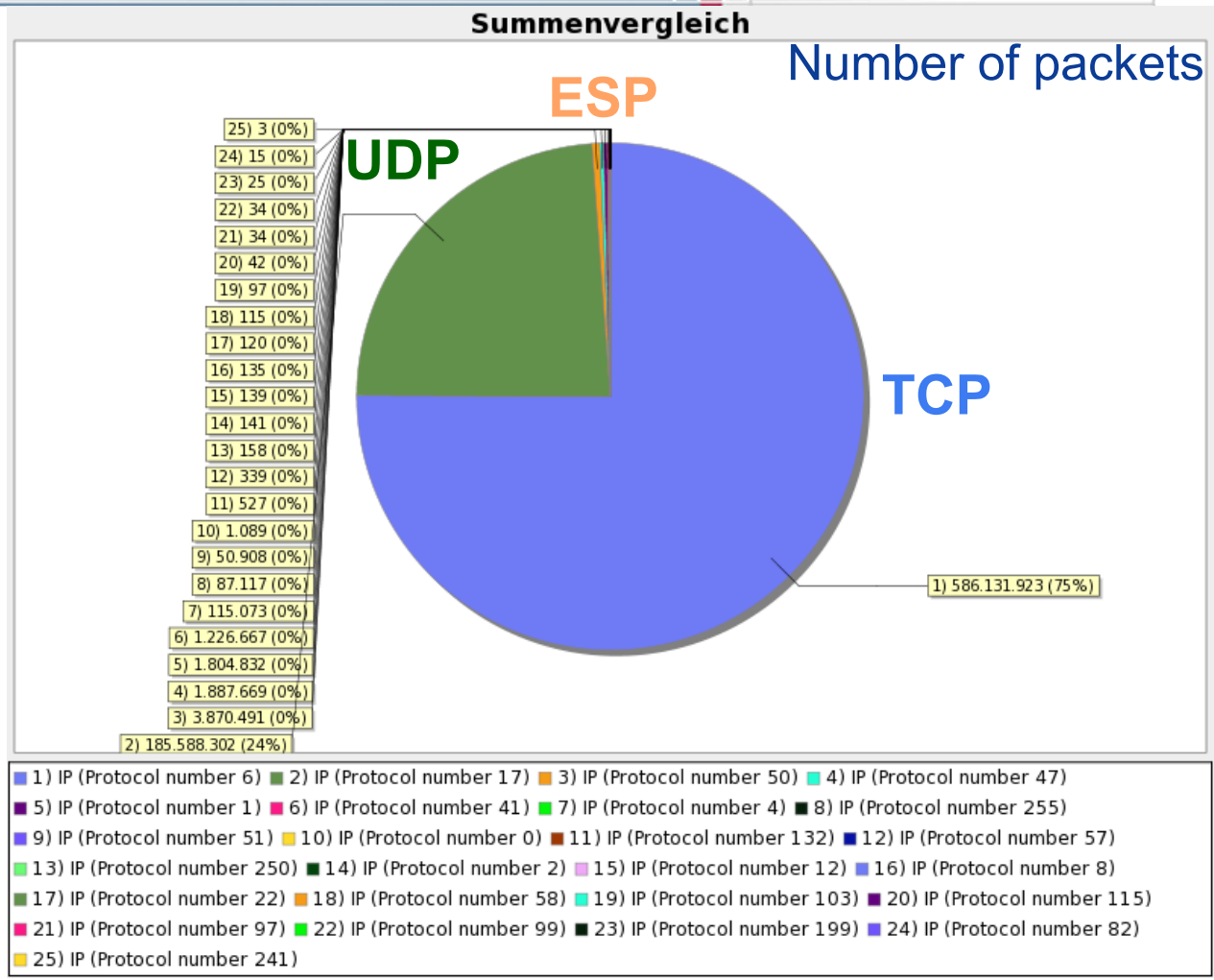


- **Pad Length**: Anzahl an Bytes für das Padding.
- **Next Header** (8-Bit): Datentyp der nächsten Daten hinter dem ESP.
- **Authentication Data** (ganzzahliges Vielfaches von 32 Bit): Ergebnis vom HMAC.

IPv4 Header „Protocol“-field → TOP25

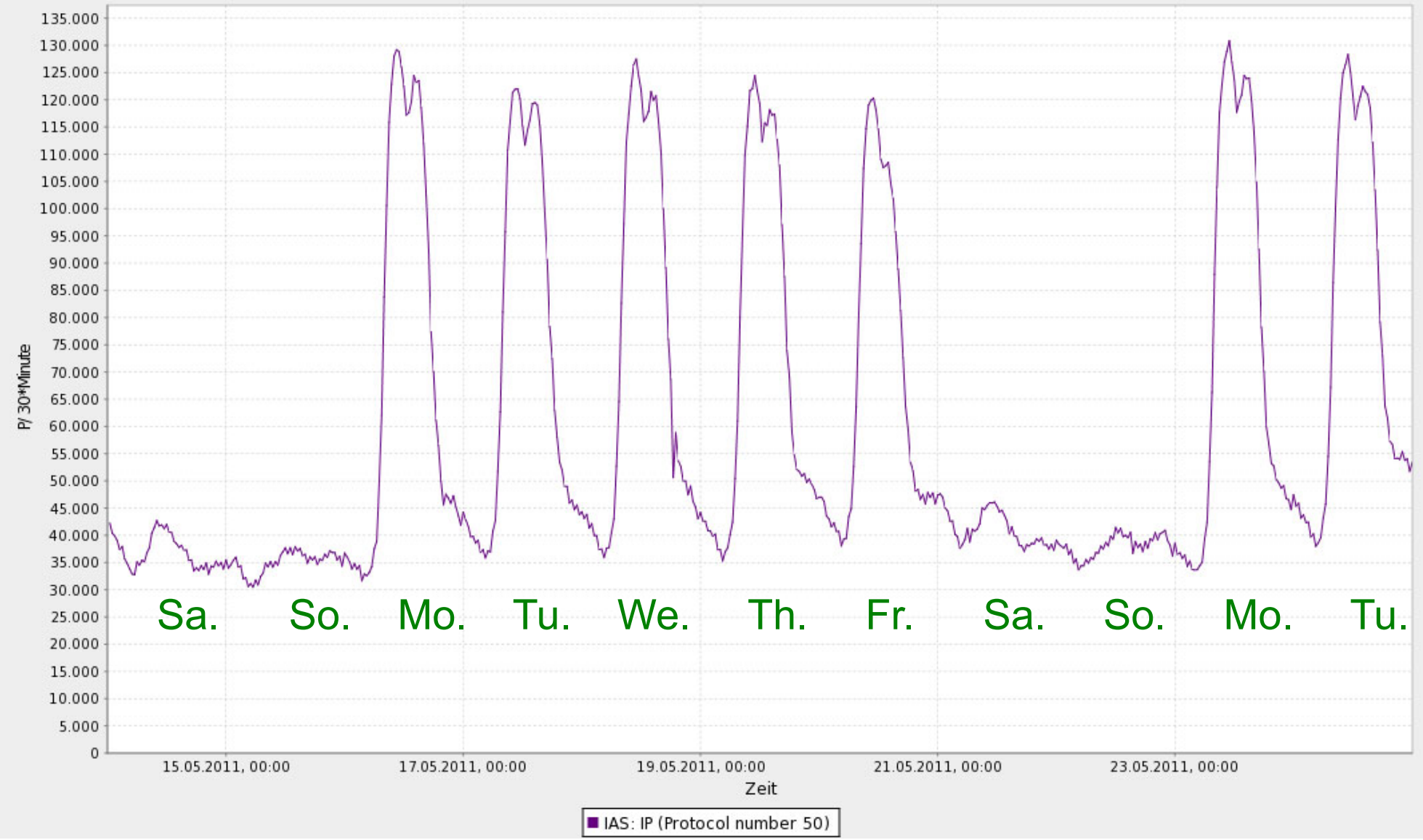
Häufigkeit

- **75% TCP – (6)**
- **24% UDP – (17)**
- **<1% ESP (0,5%) – (50)**
- <1% GRE (0,24%) – (47)
- <1% ICMP (0,23%) – (1)
- <1% IPv6 Encapsulation - (41)
  (6over/to4 = 0,157%)
- <1% IPv4 Encapsulation
- <1% Reserved
- **<1% Authentication H. (0,007%)**
- <1% IPv6 Hop-by-Hop Option
- <1% SCTP
- <1% SKIP
- <1% Unassigned (199, 250, 241)
- <1% PUP
- <1% EGP
- <1% XNS-IDP
- <1% IPv6-ICMP
- <1% PIM



- <1% L2TMP
- <1% ETHERIP
- <1% any private encription scheme
- <1% SECURE-VMTP

„Protocol“-field 50 (IPSec → ESP)
→ User behavior



→ IPSec more common in the business environment

IPSec Header
→ Anti-Replay Service (1/2)

- Schutz vor unberechtigter Wiedereinspielung von alten IP-Paketen.
- Optional sowohl beim Authentication Header und Encapsulated Security Payload nutzbar.
- Standardmäßig ist der Anti-Replay Service aktiviert.
- Verwendung der Sequence Number (SN) in den entsprechenden Headern.
- SN ist ein 32-Bit-Feld, das einen steigenden Zählerwert enthält.

IPSec Header
→ Anti-Replay Service (2/2)

- **Initiator:**
  - Bei der IPSec-Initialisierung wird von Initiator SN = 0 gesetzt
  - Das erste Paket wird mit SN = 1 gesendet
  - Das Feld wird vor dem Versand jedes weiteren Paketes um 1 erhöht

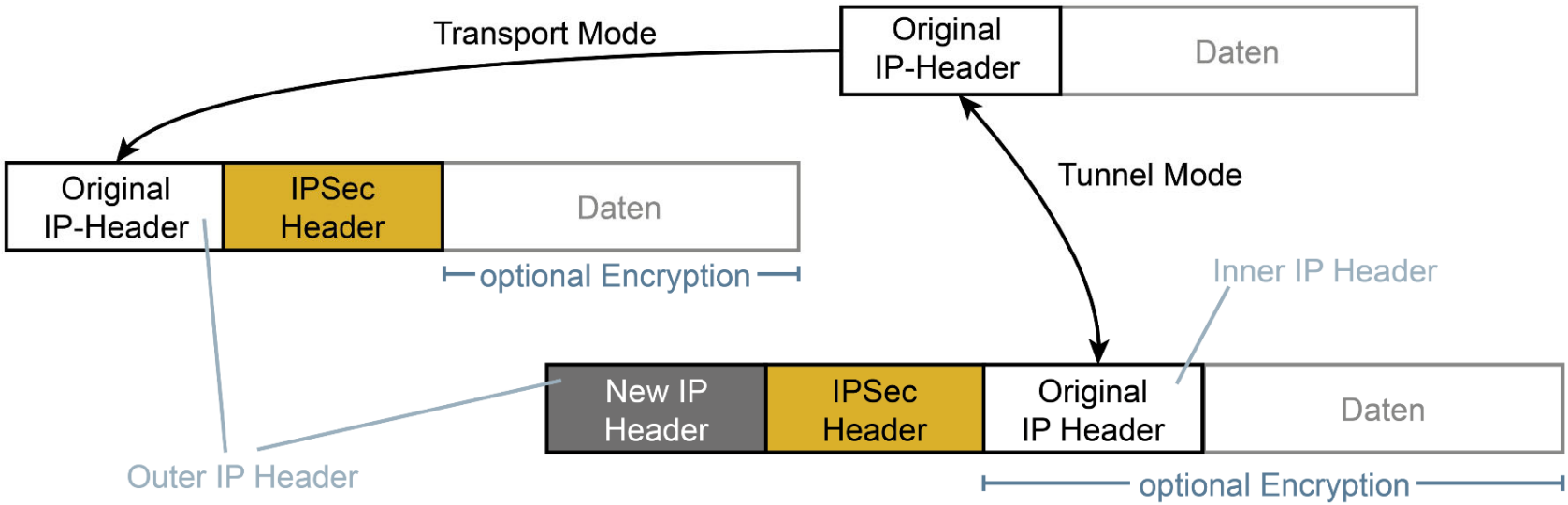
- **Receiver:**
  - Überprüft, ob die SN in der richtigen Reihenfolge ist.
  - Mit Hilfe eines „Sliding Window“ wird entschieden, ob ein Paket mit einer bestimmten Sequenznummer angenommen oder verworfen wird. Die Größe eines Sliding Windows ist z.B. 32.
  - Damit wird das unberechtigte Wiedereinspielen von alten Paketen in einer Security Association (AS) unterbunden.

IPSec Header
→ Security Association (SA)

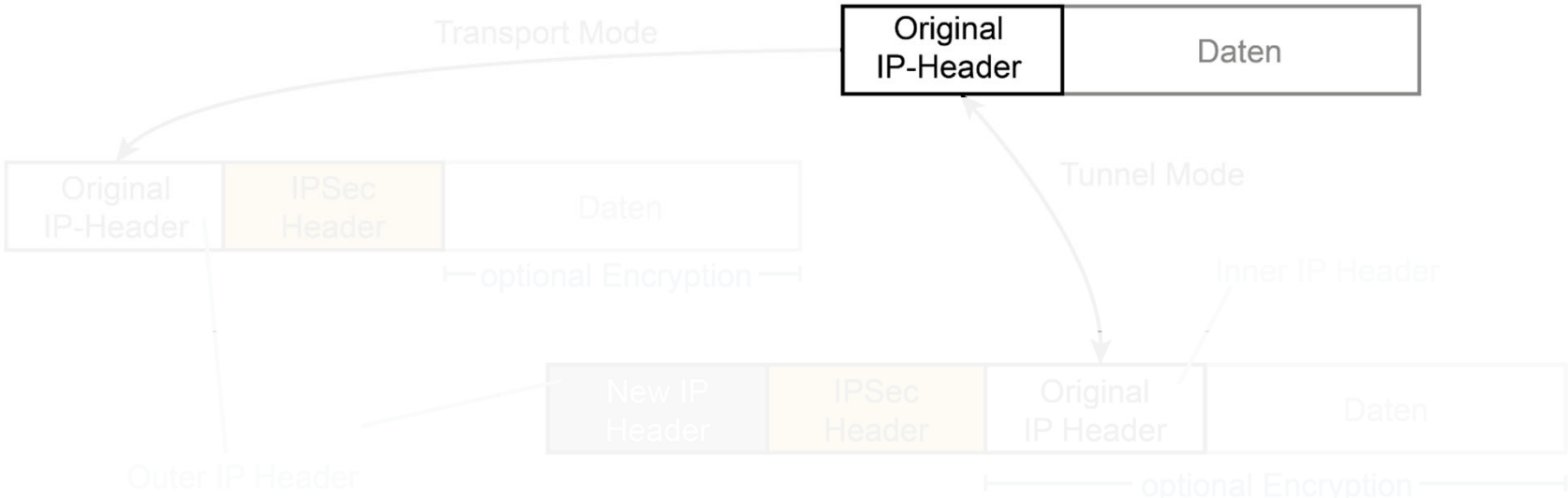
- IPSec Header enthalten keine direkten Informationen über die zur Absicherung zu verwendenden Algorithmen, Schlüssellängen, ...

- **SPI** und **Ziel-Adresse** definieren eindeutig eine/mehrere **SA**.
  - Security Parameter Index (SPI)
  - genutzter IPSec-Service (AH oder ESP oder beide)
  - Modus (Transport oder Tunnel)
  - Quell- & Ziel-IP-Adresse, evtl. Adresse des Gateways
  - evtl. genutzte Protokolle, Quell- & Zielportnummer
  - genutzte Algorithmen & Schlüssel für die Security Association
  - Sequenznummer
  - Dauer der Gültigkeit der Security Association (kann über einen längeren Zeitraum sein!)
  - Statusinformation der Anti-Replay-Windows

IPSec Header
→ Transport- und Tunnelmodus



IPSec Header
→ Transport- und Tunnelmodus



IPSec Header
→ Transportmodus

- Kann nur mit IPSec-Clients umgesetzt werden.
- Er ist nicht für IPSec-Gateway verfügbar.
- Wenn ein IPSec-Gateway im Transportmodus arbeitet, fungiert es als IPSec-Client, d.h.der Datenverkehr ist dann für sich selbst bestimmt.
- Im Transportmodus wird der IPSec-Header nach dem IP-Header und vor einem Protokoll der oberen Schicht (z. B. TCP, UDP, ICMP usw.) eingefügt.
- Bei 1:n- oder m:n-Verschlüsselung mit IPSec-Client kommt nur der Transportmodus zum Einsatz.

IPSec Header
→ Tunnelmodus (1/2)

- Der **Tunnelmodus** gilt für IPSec-Client/-Gateway und IPSec-Gateways.

- Ein IPSec-Gateway unterstützt nur den Tunnelmodus.
  - Die äußeren IP-Quell- und -Zieladressen identifizieren die "Kommunikationsendpunkte" des Tunnels.
  - Die innere IP-Quell- und -Zieladresse identifiziert den ursprünglichen Absender und Empfänger des Datagramms.

- Ermöglicht die Verwendung öffentlicher IP-Adressen im neuen äußeren IP-Header, während die vorhandenen privaten IP-Adressen des ursprünglichen Pakets beibehalten werden.

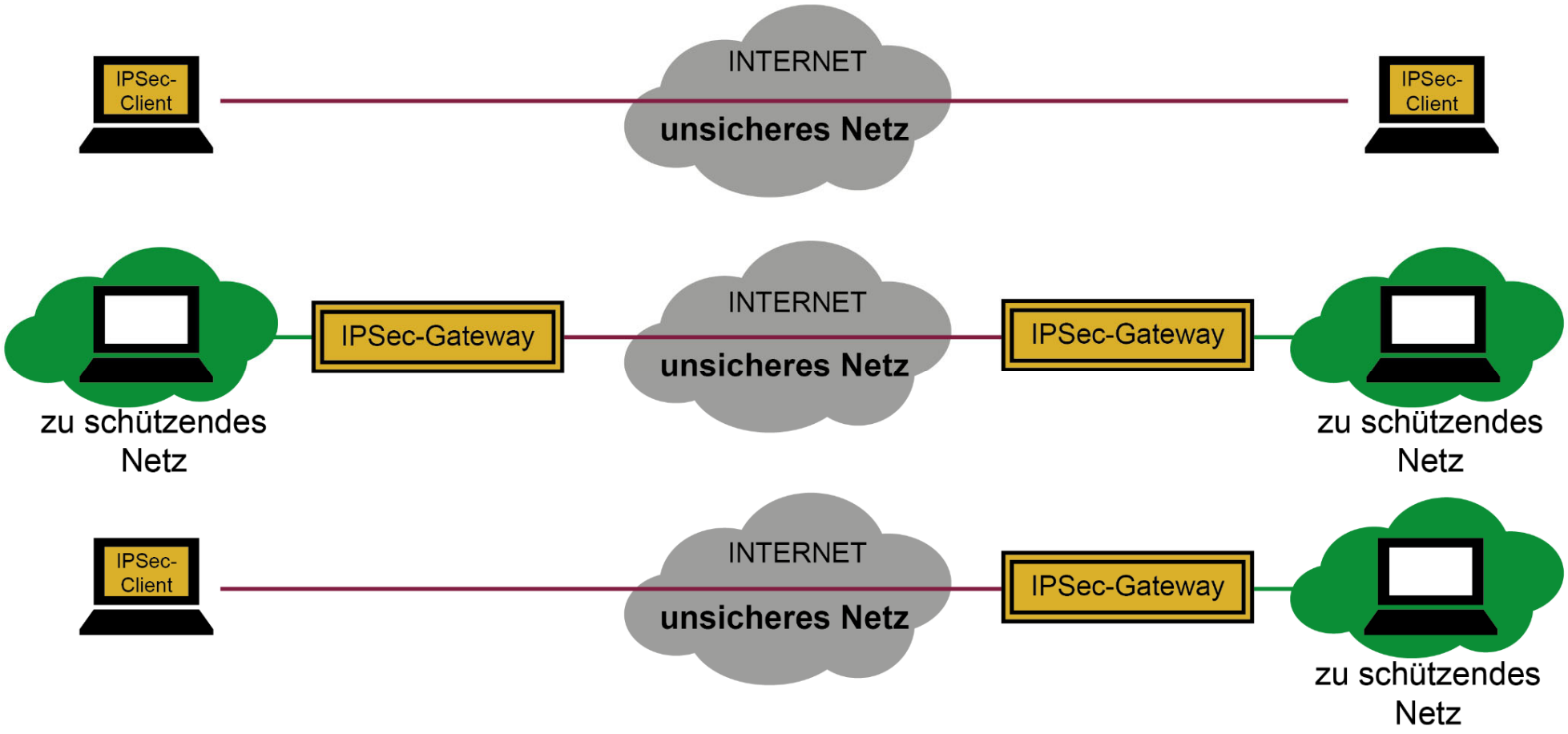
IPSec Header
→ Tunnelmodus (2/2)

- Der öffentliche IP-Header wird dann vom empfangenden IPSec-Gateway gelöscht, und das ursprüngliche Paket wird im **Intranet** entsprechend dem privaten IP-Header weitergeleitet.

- Das ursprüngliche IP-Paket wird am Ende des Tunnels außer dem TTL-Feld, das dekrementiert wird, und dem Checksum-Feld, das aufgrund der TTL-Änderung neu berechnet wird, nicht geändert.

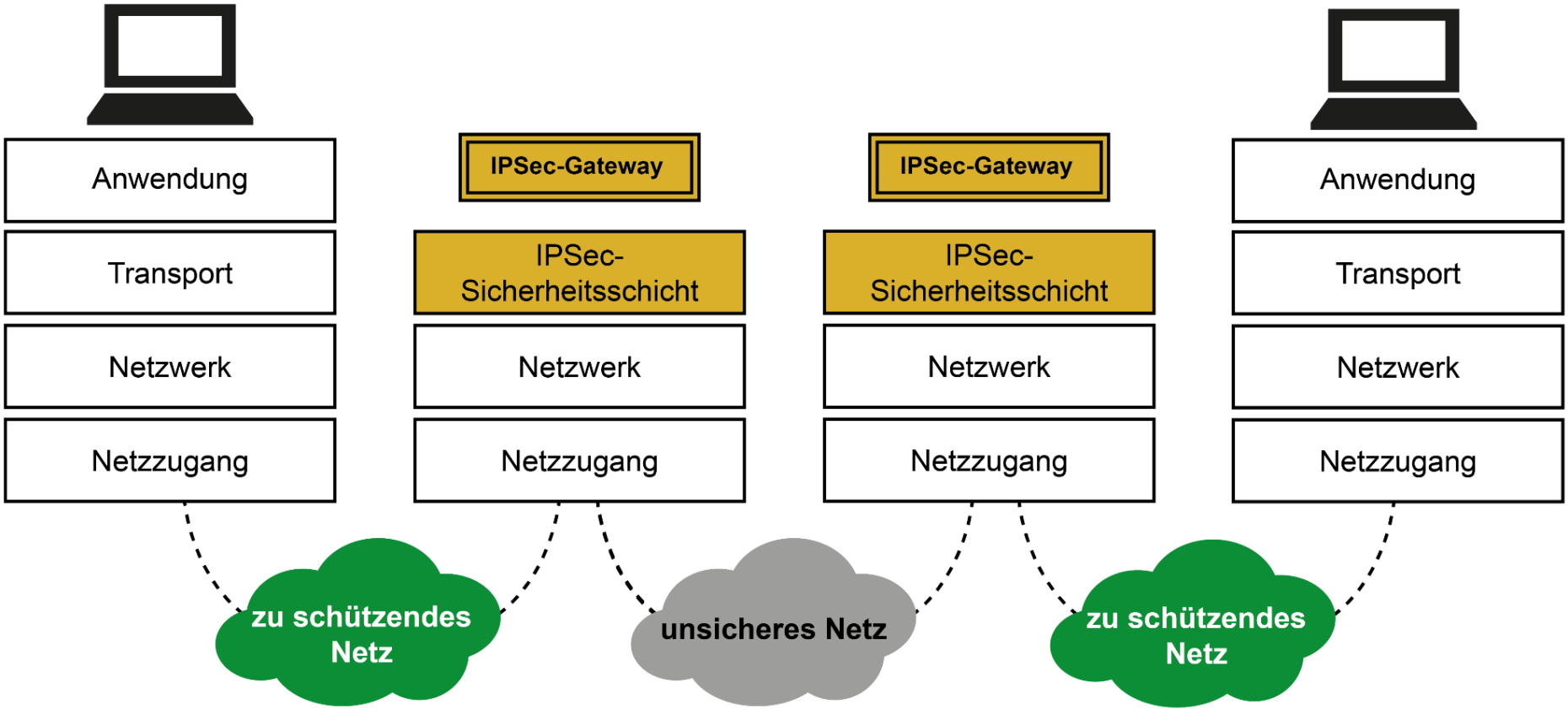
- Bei 1:1-Verschlüsslung, die beispielsweise zwischen zwei Firewall-Systemen oder sonstigen Security-Gateways eingerichtet werden, wird immer der Tunnelmodus genutzt.
  - Damit bleiben die echten IP-Adressen der Kommunikations-Partner einem Angreifer verborgen.

IPSec Header
→ Realisierungsformen



IPSec Header
→ Realisierungsformen

IPSec Header
→ IPSec-Gateway



IPSec Header

→ Vorteile einer IPSec-Gateway-Lösung (1)

- Unabhängigkeit von IT-Systemen (Server, PC, Notebook, Tablets, Smartphone, Wearable, …) und deren Betriebssystemen (Android, iOS, LINUX, Windows, …).

- Einrichtung von Cyber-Sicherheitsfunktionen zwischen IT-Systemen, in die ansonsten keine Cyber-Sicherheitsfunktionen integriert werden könnten (z.B. Terminals).

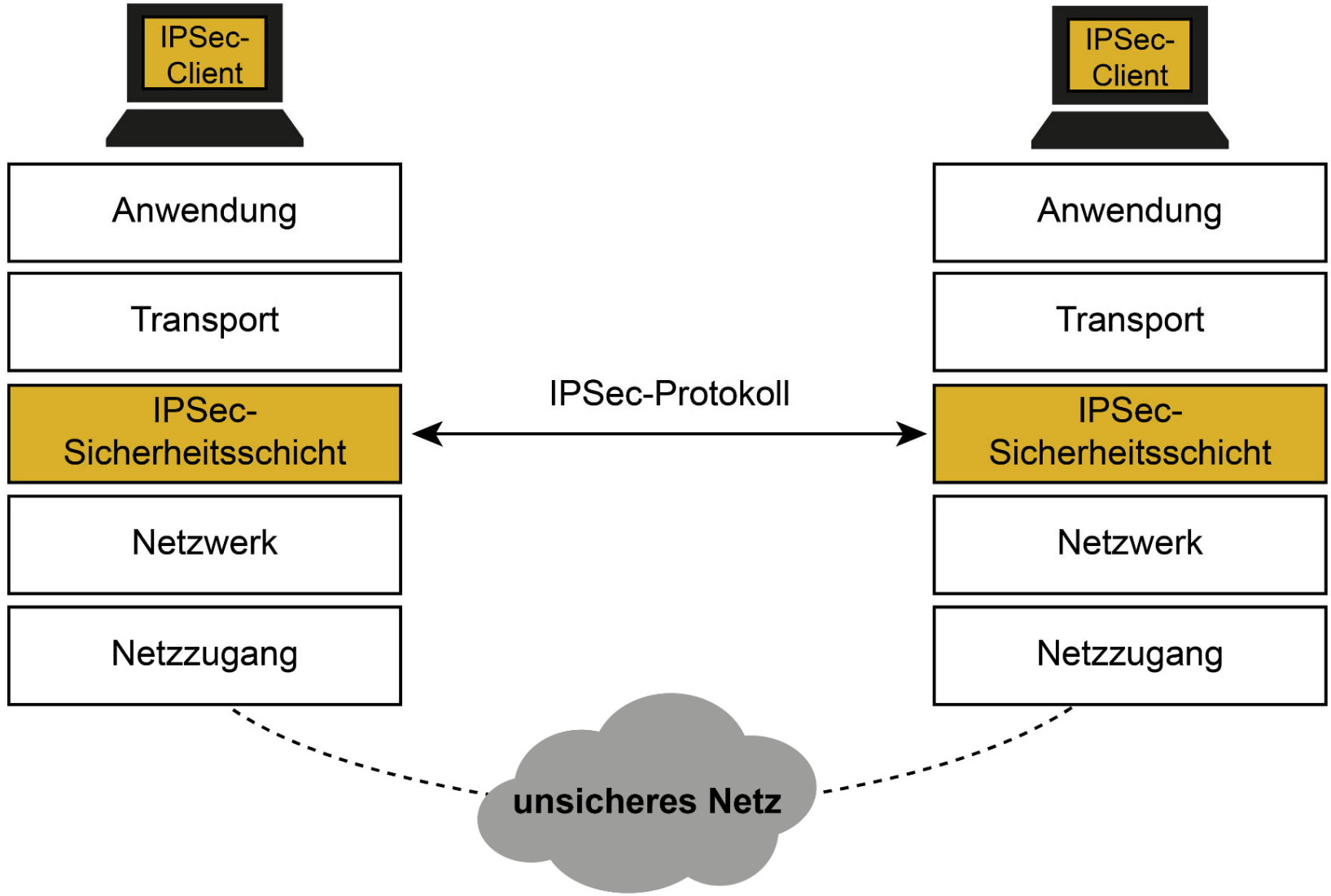
- Verringerung des Aufwandes: Bei heterogenen IT-Systemen kann immer das gleiche IPSec-Gateway verwendet werden.

IPSec Header

→ Vorteile einer IPSec-Gateway-Lösung (2)

- Vergleichsweise leichter „sicher“ zu realisieren als spezielle Software-Lösungen in IT-Systemen
- Immer ansprechbar, und damit einfacher zu managen.
- Hinsichtlich der Sicherheitsqualität unabhängig von anderen Systemkomponenten → Cyber-Sicherheit ist anwendungsunabhängig.

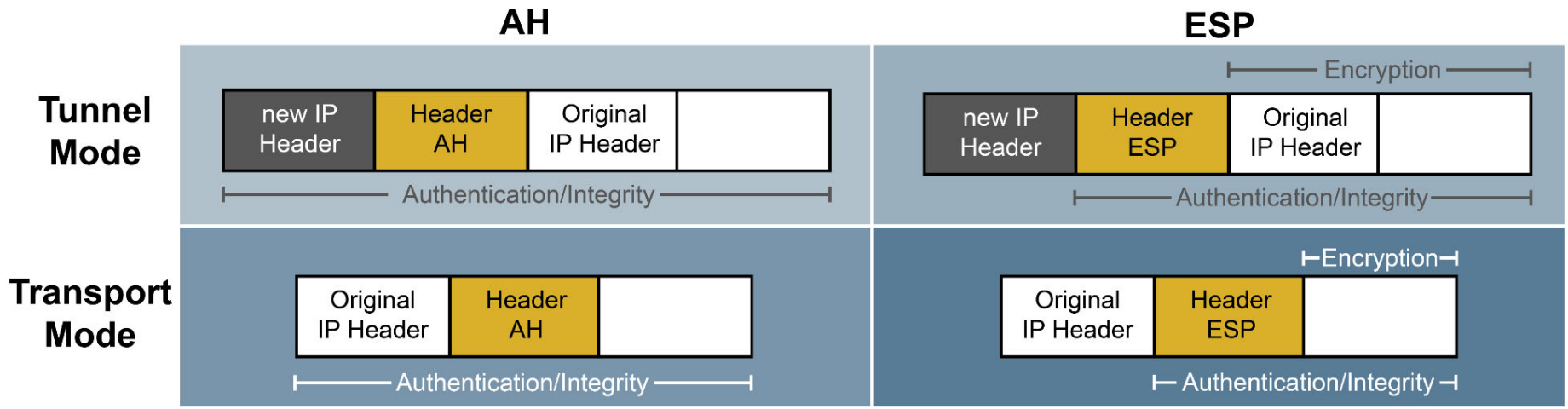
IPSec Header
→ IPSec-Client



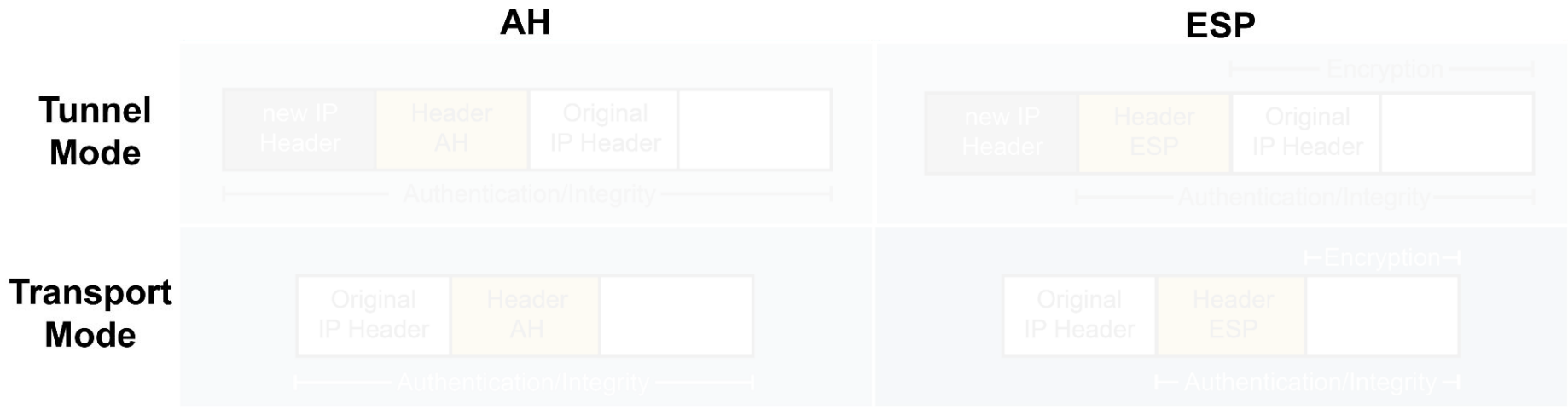
IPSec Header
→ Vorteile einer IPSec-Client-Lösung

- Kostengünstiger als die IPSec-Gateway-Lösung.
- Bietet End-to-End-Sicherheit.
- Kann mobil und flexibel verwendet werden.
- Eine Person, ein Nutzer, kann authentisiert werden.

IPSec Header
→ Header und Mode Kombinationen



IPSec Header
→ Header und Mode Kombinationen



IPSec Verschlüsselung
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- IPSec Header
- **IPSec Schlüsselmanagement**
- Protokollmitschnitt
- Zusammenfassung

IPSec Schlüsselmanagement
→ Manual Keying (1/2)

- Notwendige Schlüssel werden entweder von einem der Kommunikationspartner oder einem zentralen Management generiert.
- Schlüssel werden auf einem sicheren Weg zu allen beteiligten Kommunikationspartnern (IPSec-Client und IPSec-Gateways) übertragen.
- Da der Schlüssel vertraulich sein muss, kann dieser Vorgang sehr aufwendig sein.

IPSec Schlüsselmanagement
→ Manual Keying (2/2)

- Nutzung der PKI-Infrastruktur der TPMs kann das „Manual Keying“ vereinfachen.

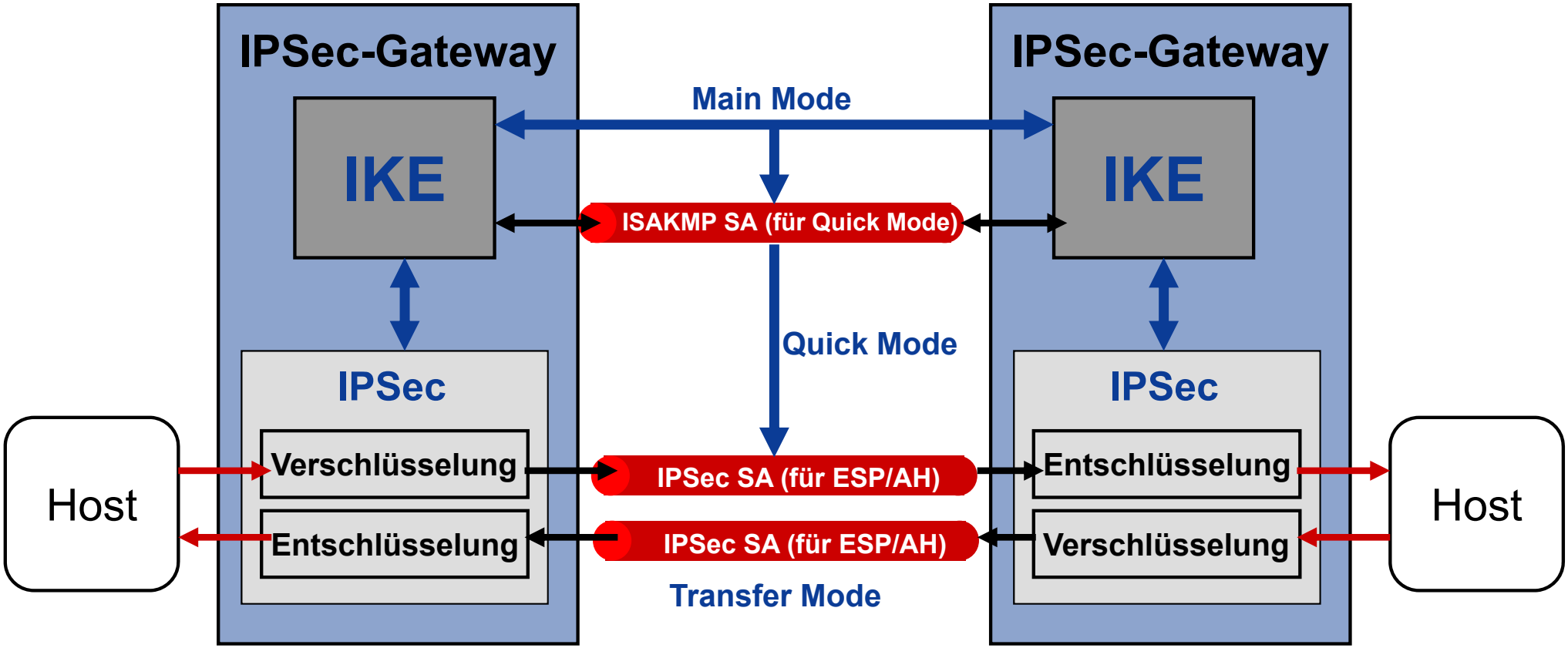
- Die Schlüssel werden mit den Public-Keys der TPMs verschlüsselt und erst im TPM wieder entschlüsselt.

IKE
→ Verschiedenen Modi und Phasen: Übersicht

- IKE = Protokoll, um eine sichere ISAKMP- u. IPSec-SA zu etablieren
- **Basiert auf UDP, Port 500 (Quelle und Ziel)**
- Zwei Phasen:
  - 1 - Main Mode/Aggressive Mode
  - 2 - Quick Mode

Exchange Mode	IKE Phase	No. of Mesg's	Agree On Key	Authent. IDs	Conceal IDs	No. of Proposals
Main	1	6	Yes	Yes	Yes	Multiple
Aggressive	1	3	Yes	Yes	No	Only One; No DH Group
Quick	2	3	Yes	Yes	No	Multiple

IPSec und IKE
→ Übersicht und Zusammenhang



- **Main Mode:** Aufbau der ISAKMP SA sowie **Policy Absprachen** und **Authentikation**
- **Quick Mode:** Aufbau der IPSec SA sowie **Mode/Protokoll (AH, ESP) Absprache** und **Key-Management**
- **Transfer Mode: Sicherung der IP-Pakete** mit AH/ESP und Anti-replay Service

IPSec Schlüsselmanagement
→ Security Policy Database (SPD)

- In der SPD ist beispielsweise hinterlegt, wie die Verbindung zwischen den Kommunikationsendpunkten gesichert werden soll.
- Zur Aushandlung der Schlüssel wird meist IKE verwendet.
- Ein Eintrag in der SPD ist „zustandslos“.
- Definition des Sicherheitsstandards:
  - Quell- & Ziel-IP-Adressen
  - Quell- & Zielportnummer
  - Protokoll (UDP, TCP, ...)
  - eine Liste mit den zugelassenen Algorithmen
  - falls notwendig: Beschreibung des Tunnelendpunktes
  - Informationen über das Anti-Replay-Window und der maximalen Lebensdauer der SA´s

IPSec Schlüsselmanagement

→ Security Association Database (SAD) (1)

- In der SAD werden SA zwischen den Kommunikationsendpunkten der IPSec-Verbindung verwaltet.
- Die Einträge in der SAD verändern sich öfter, anders als bei der SPD.
- Die Einträge der SA enthalten die Schlüssel mit der entsprechenden Lebensdauer.
- AH und ESP haben eigene Einträge in der SA der SAD.
- Eine SA wird über das IKE-Protokoll angelegt und für nur eine Kommunikationsrichtung genutzt: Sender und Empfänger haben darin die entsprechenden Schlüssel und Verfahren.
- Wenn AH und ESP gleichzeitig verwendet werden, sind vier Einträge in der entsprechenden SA vorhanden.

IPSec Schlüsselmanagement

→ Security Association Database (SAD) (2)

Für jede SA werden folgende Parameter festgelegt:

- **Identifier:**
  - Ziel-IP-Adressen oder Ranges
  - IPSec-Header (AH oder ESP)
  - Security Parameter Index (SPI)
- **Parameter:**
  - Algorithmen für die Authentifikation und Verschlüsselung
  - Lebensdauer der Security Association (SA)
  - Tunnel oder Transport-Mode
  - Anti-Replay-Service
  - Link mit der Policy in der SPDSA´s

IPSec Schlüsselmanagement

→ Security Association Database (SAD) (3)

- Der SPI zusammen mit der IP-Adresse des Kommunikationsendpunkt identifiziert die entsprechenden SA.
  - Diese Informationen stehen im IP- und IPSec-Header.

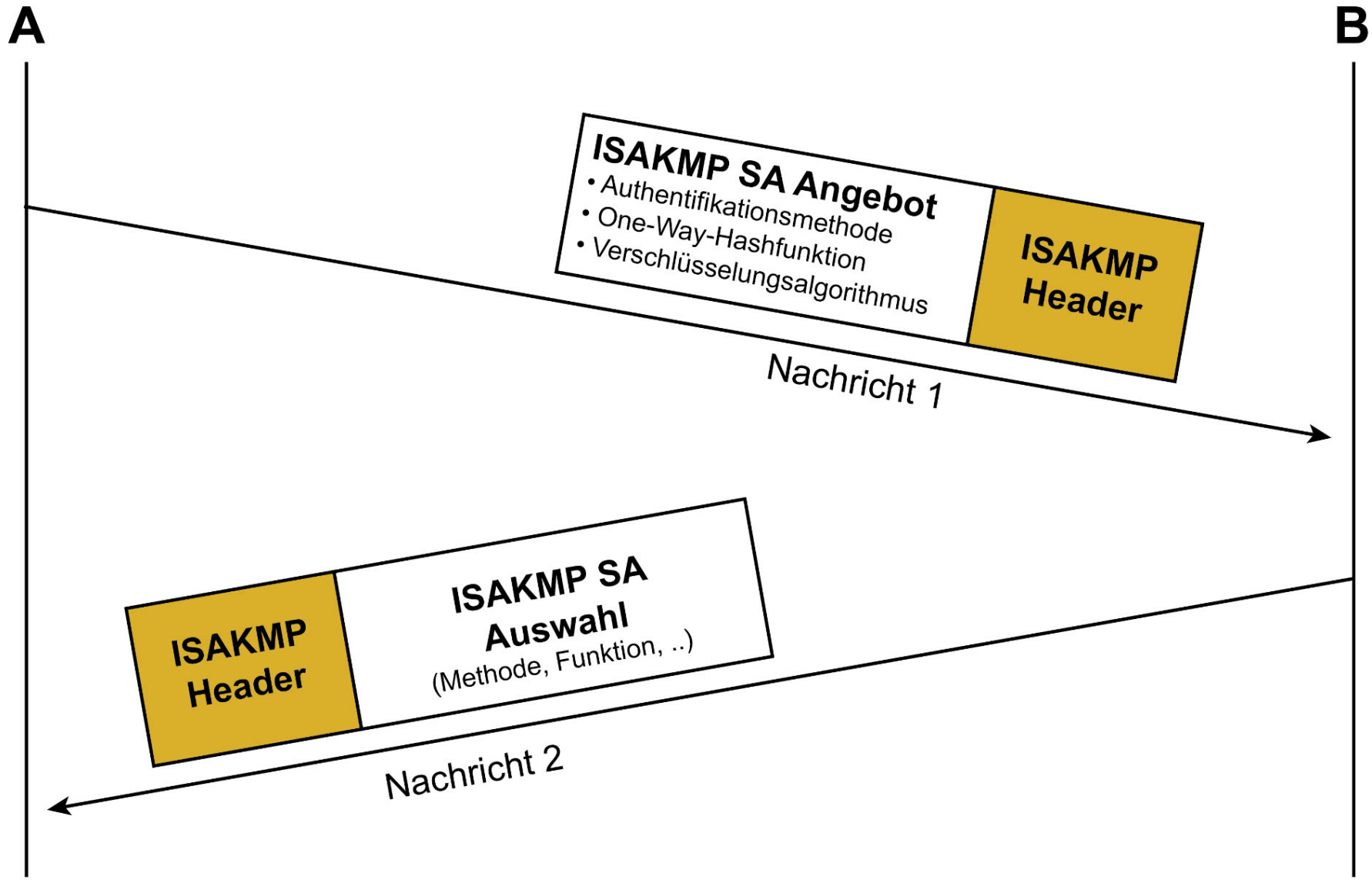
IPSec Schlüsselmanagement

→ Verschiedenen Modi und Phasen von IKE (1)

- Es werden zwei Phasen von Security Association durchgeführt:
  - **Phase 1 (P1) - Main Mode/Aggressive Mode**
  - **Phase 2 (P2) - Quick Mode**
    - Basic Quick Mode
    - Perfect Forward Secrecy

IPSec Schlüsselmanagement

→ P1: IKE Main Mode – Aushandeln der Basis-Algorithmen (1)



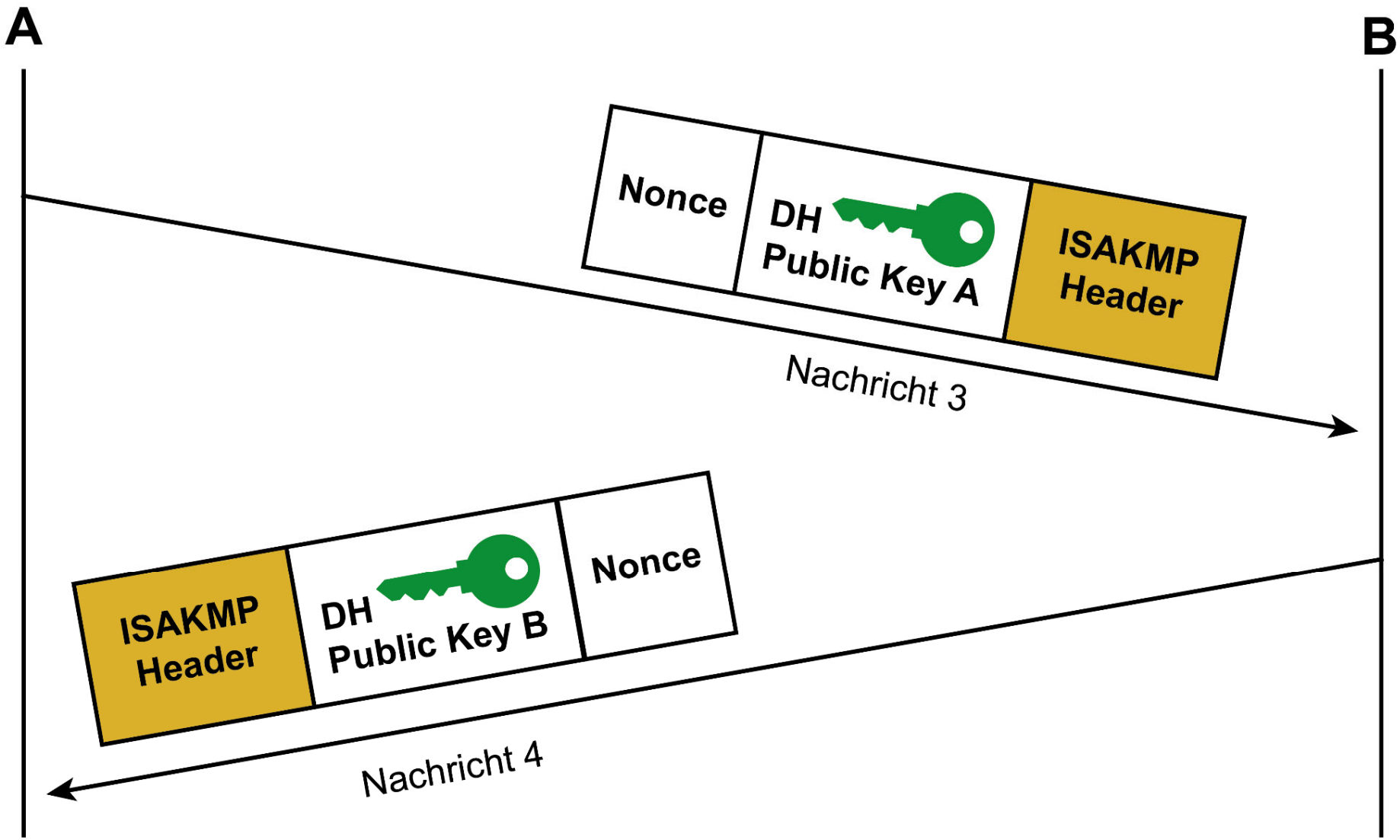
IPSec Schlüsselmanagement

→ P1: IKE Main Mode – Aushandeln der Basis-Algorithmen (2)

- Authentifikationsmethoden sind z.B. auf der Basis einer PKI oder Pre-Shared Key (PSK)
- One-Way-Hashfunktionen sind z.B. SHA512, SHA384, SHA256, …
- Verschlüsselungsalgorithmen sind z.B. AES-256-GCM, AES-256-CBC, … DES
- DH Group (für p) sind z.B. Group20 (384-Bit Elliptic Curve), Group19, Group14, …. Group1 (768 Bit)

IPSec Schlüsselmanagement

→ P1: IKE Main Mode – Umsetzung des Diffie-Hellman-Verfahrens



IPSec Schlüsselmanagement

→ Berechnungen des Diffie-Hellman Shared Secrets (1)

- Diffie-Hellman Shared Secrets := DDHS

- **Kommunikationspartner A:**
  - DHSS = DH Public Key B $^{\text{DH Private Key A}}$ mod p

- **Kommunikationspartner B:**
  - DHSS = DH Public Key A $^{\text{DH Private Key B}}$ mod p

- **DH Private Key X:**
  - Ist der geheime Schlüsselteil des Kommunikationspartner X.

IPSec Schlüsselmanagement

→ Berechnungen des Diffie-Hellman Shared Secrets (2)

- Aus dem gemeinsamen Shared Secret DDHS werden drei weitere geheime Schlüssel abgeleitet:

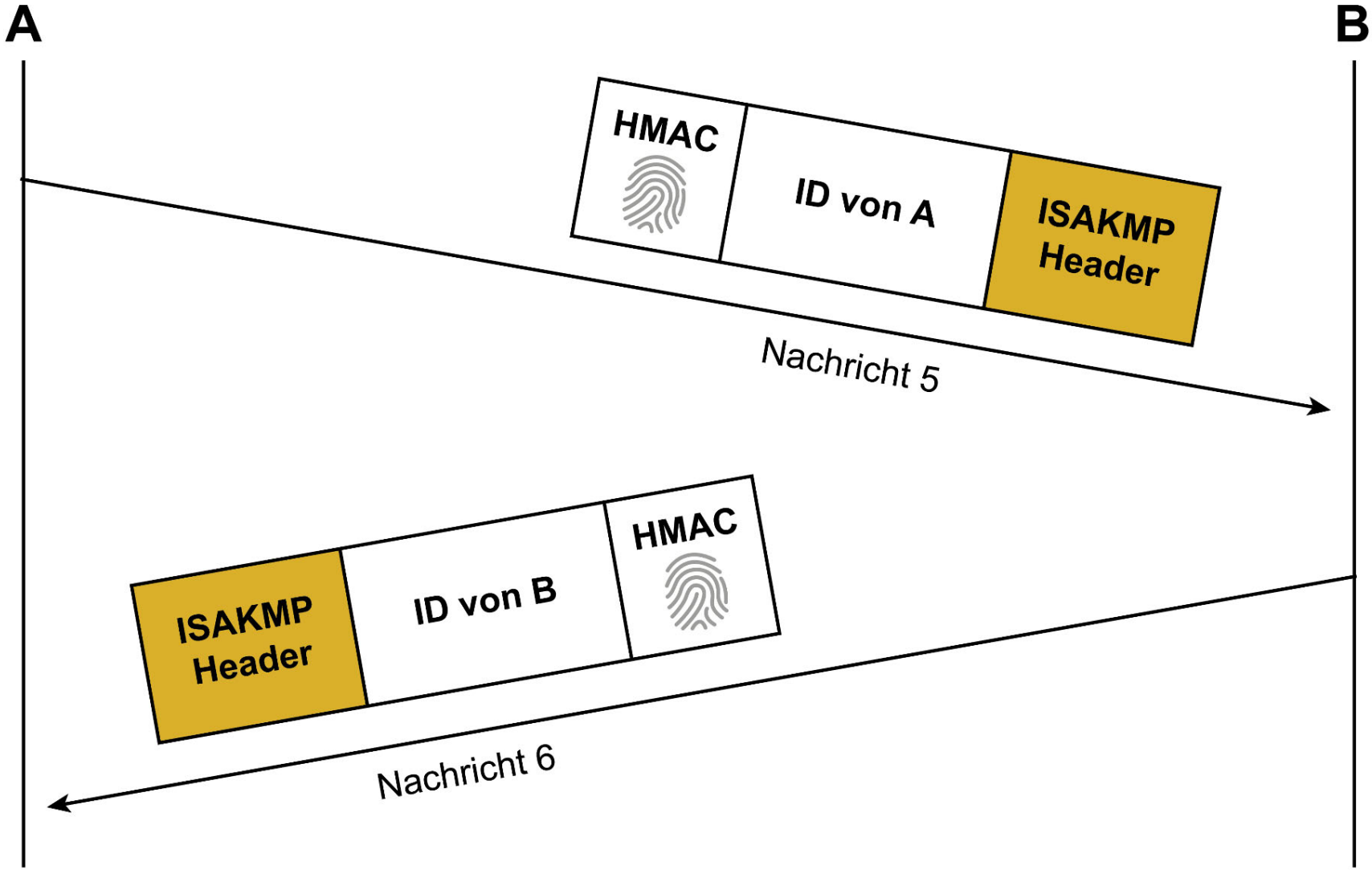
- **1.) Derivation Key**
  Der Derivation Key wird für die Sicherheit des Quick Modes verwendet.

- **2.) Authentication Key**
  Der Authentication Key wird als Sitzungsschlüssel für die Authentizität der Protokollelemente im Schritt 3 verwendet.

- **3.) Encryption Key**
  Der Encryption Key wird als Sitzungsschlüssel für die Verschlüsselung der Protokollelemente im Schritt 3 verwendet.

IPSec Schlüsselmanagement

→ P1: IKE Main Mode – Authentifikation der Kommunikationspartner



IPSec Schlüsselmanagement
→ Pre-Shard-Secret Authentifizierung

HMAC = KH (PSK, Nonce || DHPK || ID || K-Profil)

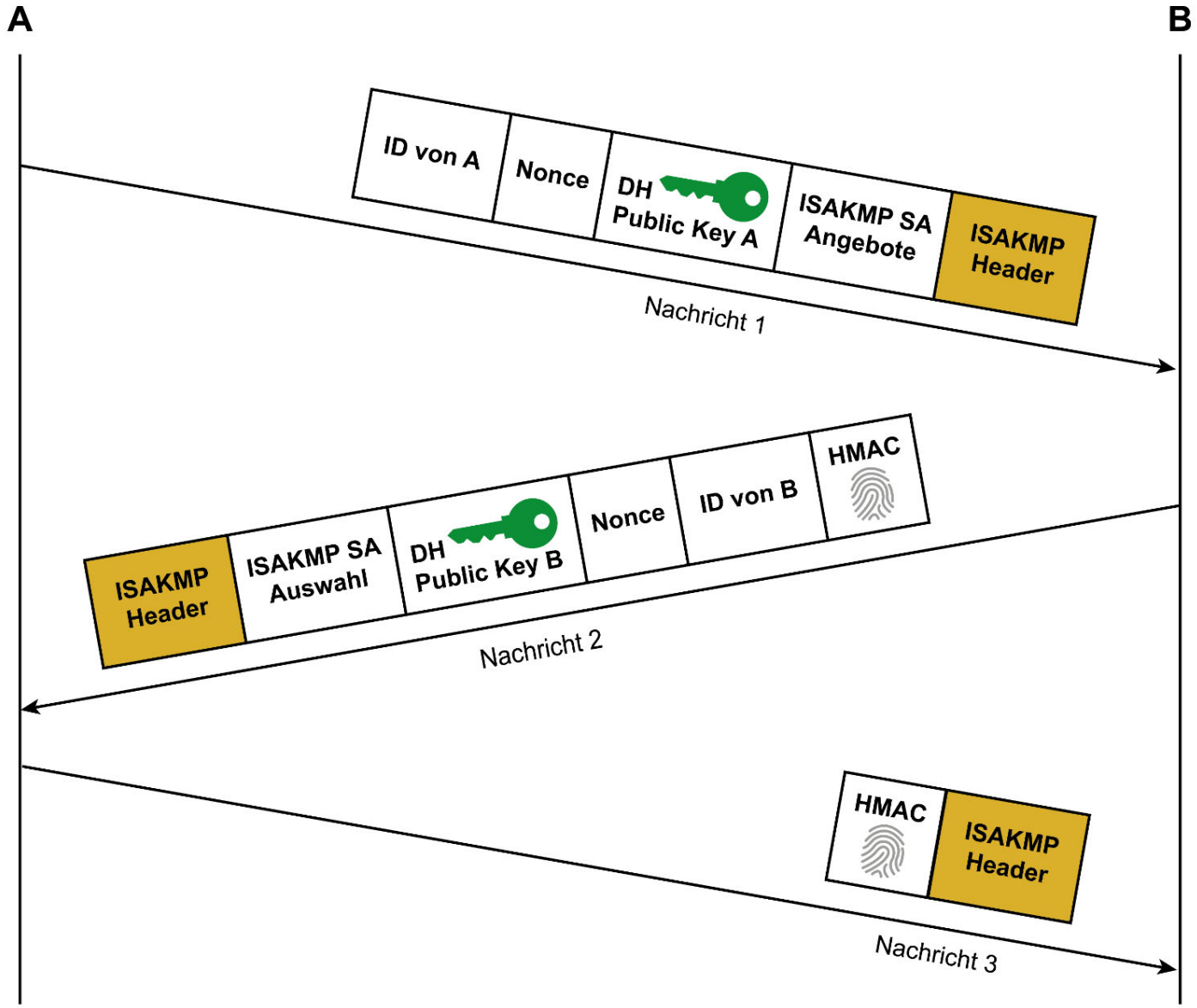
- **KH** = “Keyed-Hashing for Message Authentication”-Verfahren; HMAC-Verfahren
- **PSK** = Pre-Shared Key (geheimer Schlüssel) der Kommunikationspartner
- **Nonce** = jeweilige Zufallszahl der Kommunikationspartner
- **DHPK** = öffentliche Diffie-Hellman Schlüssel des Kommunikationspartners
- **ID** = ID des Kommunikationspartners (A und B)
- **K-Profil** = ausgewähltes Krypto-Profil (aus Nachricht 2)

IPSec Schlüsselmanagement
→ Digitale Signatur Authentifizierung

HMAC = S (KH (DHSS, Nonce || DH PK || ID || K-Profil), GSX)

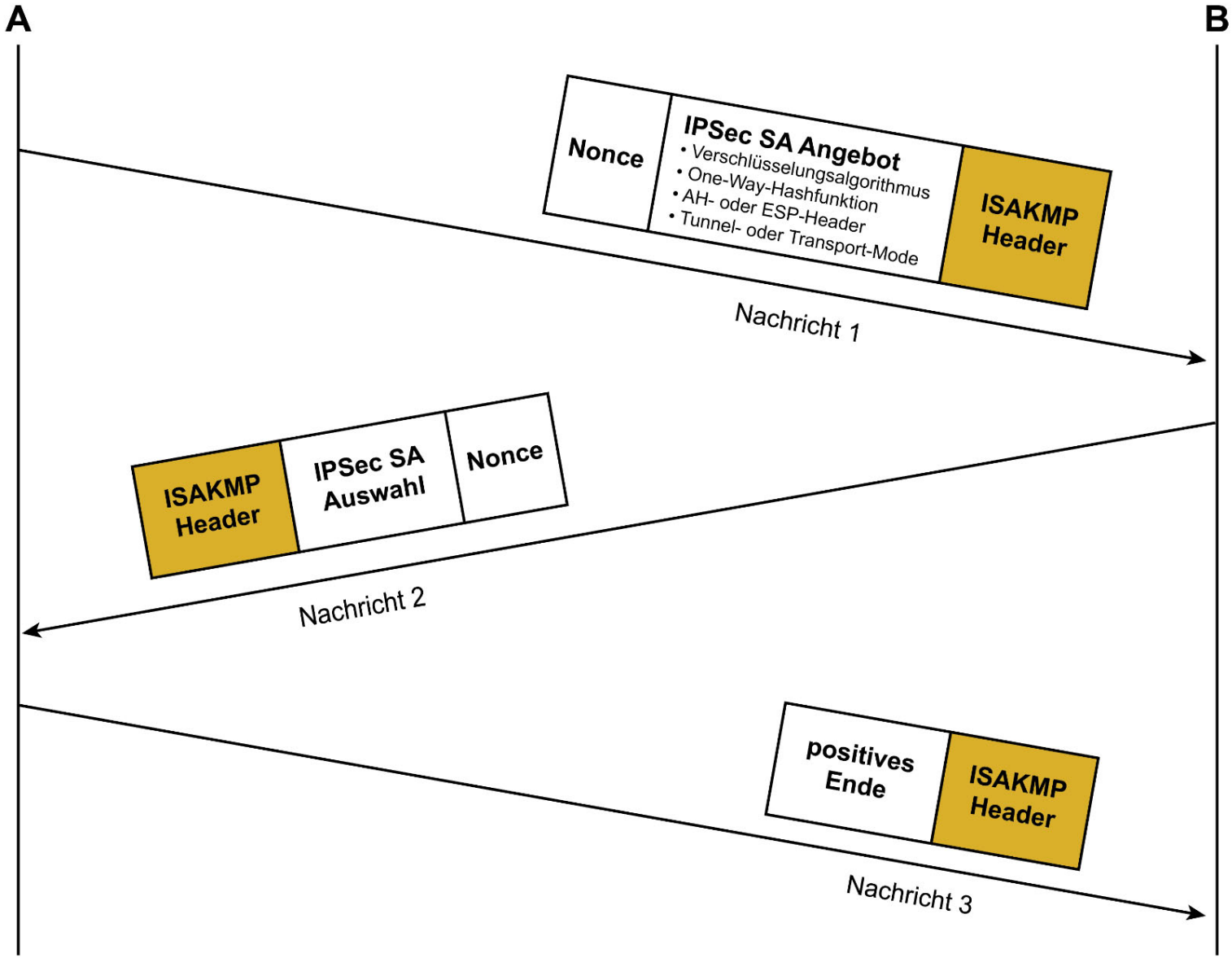
- **S** = Signaturfunktion (z.B. RSA-Verfahren)
- **GSX** = geheimer Schlüssel des Kommunikationspartners X (A oder B)
- **KH** = “Keyed-Hashing for Message Authentication”-Verfahren; HMAC-Verfahren
- **DHSS** = Diffie-Hellman Shared Secret (geheimer Schlüssel aus Schritt 2)
- **Nonce** = jeweilige Zufallszahl der Kommunikationspartner
- **DHPK** = öffentliche Diffie-Hellman Schlüssel des Kommunikationspartners
- **ID** = ID des Kommunikationspartners (A und B)
- **K-Profil** = ausgewähltes Krypto-Profil (aus Nachricht 2)

IPSec Schlüsselmanagement
→ P1: IKE Aggressive Mode



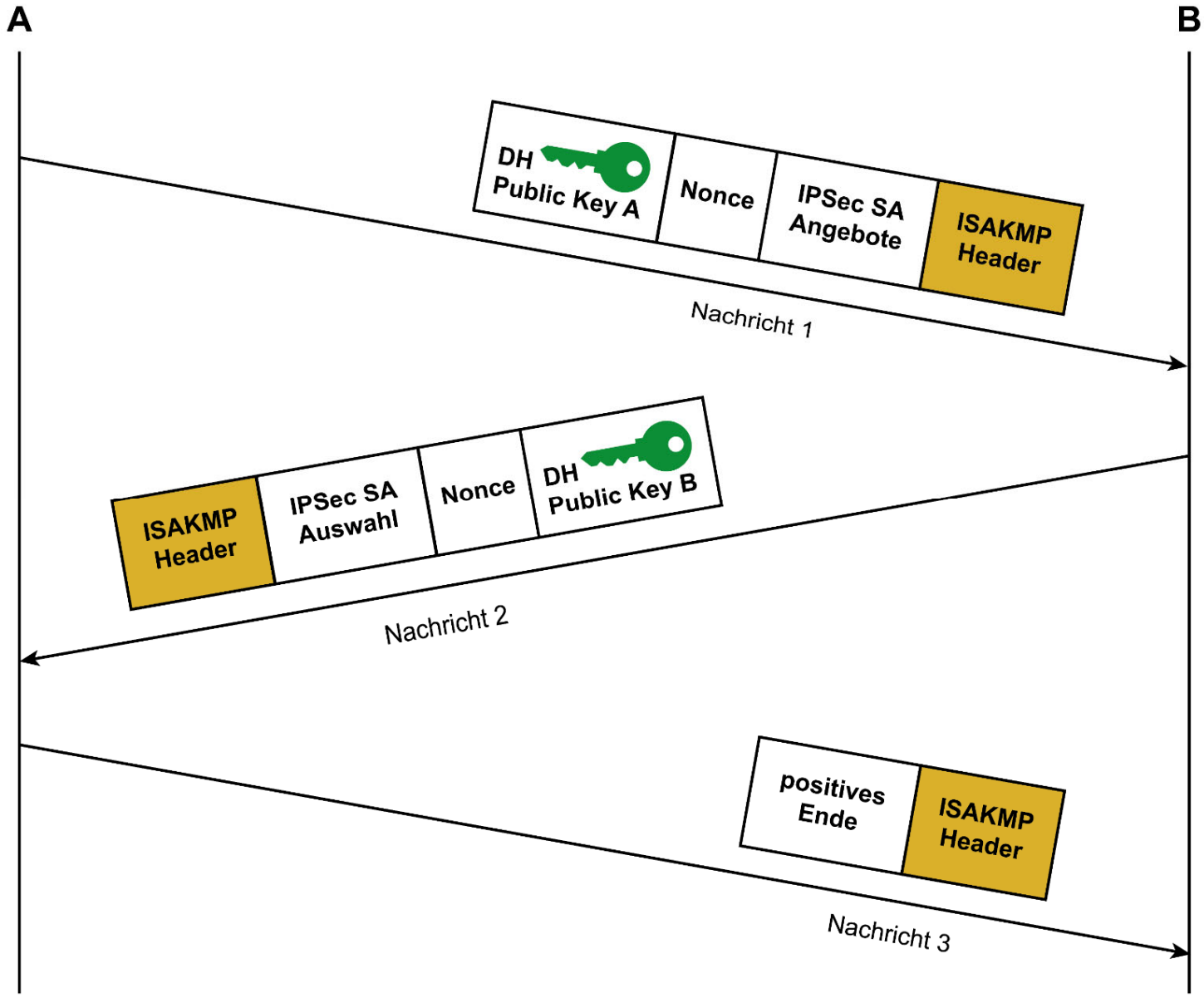
IPSec Schlüsselmanagement

→ P2: Basic Quick Mode - Aufbau der IPSec SA



IPSec Schlüsselmanagement

→ P2: Perfect Forward Secrecy - Aufbau der IPSec SA



IPSec Schlüsselmanagement
→ Berechnung von KEYMAT (1/3)

- KEYMAT ist das Schlüsselmaterial für die Authentizität und Verschlüsselung für die ein- und ausgehenden Kommunikationskanäle im Transfer Mode.

Basic Quick Mode:

KEYMAT = KM (DK, IPSH || SPI || Nonce)

- **KH** = “Keyed-Hashing for Message Authentication”-Verfahren; HMAC-Verfahren
- **DK** = Derivation Key, aus der Phase 1
- **IPSH** = IPSec Header (AH oder ESP)
- **SPI** = Security Parameter Index
- **Nonce** = jeweilige Zufallszahl der Kommunikationspartner

IPSec Schlüsselmanagement
→ Berechnung von KEYMAT (2/3)

Perfect Forward Secrecy:

KEYMAT = KH (DK, DHSS || IPSH || SPI || Nonce)

- **KH** = “Keyed-Hashing for Message Authentication”-Verfahren; HMAC-Verfahren
- **DK** = Derivation Key, aus der Phase 1
- **DHSS** = Diffie-Hellman Shared Secret
- **IPSH** = IPSec Header (AH oder ESP)
- **SPI** = Security Parameter Index
- **Nonce** = jeweilige Zufallszahl der Kommunikationspartner

IPSec Schlüsselmanagement
→ Berechnung von KEYMAT (3/3)

- Aus KEYMAT werden dann 4 weitere Schlüssel erzeugt:
  - Zwei **Authentifizierungsschlüssel** und
  - zwei **Verschlüsselungsschlüssel**

  für eingehende und ausgehende IT-Pakete (Transfer Mode).

IPSec Schlüsselmanagement
→ Perfect Forward Secrecy (PFS) (1)

- PFS ist eine kryptographische Charakteristik, die eine Aussage über die Abhängigkeit von Schlüsseln untereinander trifft.

- Mit aktiviertem PFS sind bei einem kompromittierten Schlüssel (z.B. Derivation Key) alle weiteren nicht gleichzeitig auch kompromittiert, da die Schlüssel nicht voneinander abhängen.

- Dieses kann durch die zusätzliche Aushandlung des Diffie-Hellman Shared Secret, erreicht werden!

IPSec Schlüsselmanagement
→ Perfect Forward Secrecy (PFS) (2)

- Beispiel eines Angriffes, bei dem PFS eine Rolle spielt:
  - Ein Angreifer speichert alle Pakete des Quick Modes sowie alle IP-Pakete, die im Transfer Mode verschlüsselt übertragen worden sind, in einer Datenbank.
    Dann wird der Klartext des „Derivation Keys“ bekannt.
    (Der „Derivation Keys“ seht für einen Angriff zur Verfügung.)

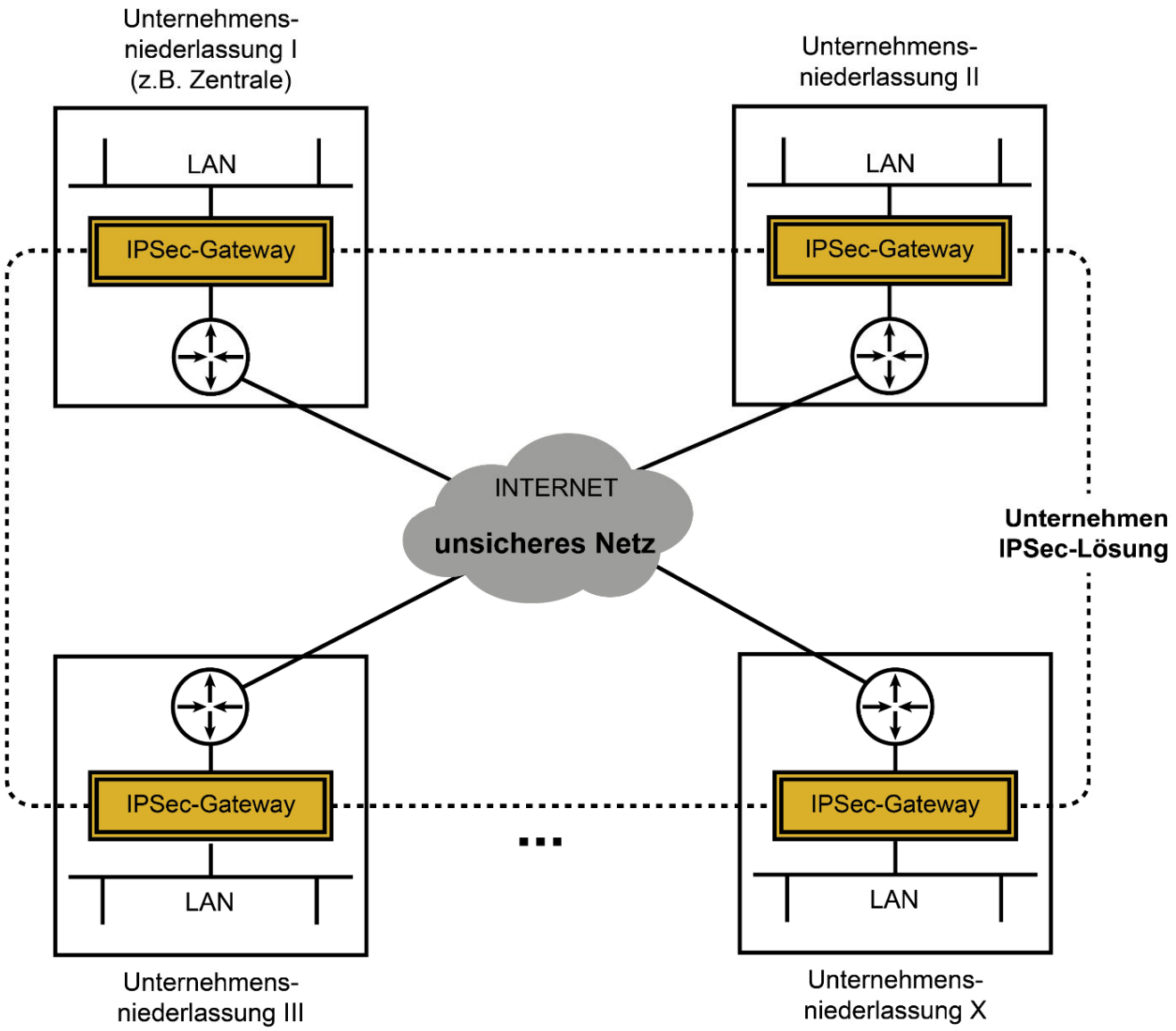
- **A) Basic Quick Mode**
  Mit Hilfe des „Derivation Keys“ kann der Angreifer für alle vergangenen Security Associations die KEYMAT berechnen und damit alle gespeicherten verschlüsselten IP-Pakete im Nachhinein entschlüsseln.

- **B) Perfect Forward Secrecy**
  Auch wenn der „Derivation Key“ bekannt ist, kann der Angreifer die vergangenen KEYMAT nicht berechnen, weil der Angreifer die entsprechenden „Diffie-Hellman Shared Secret“ nicht kennt.

IPSec und IKE
→ Komplexität

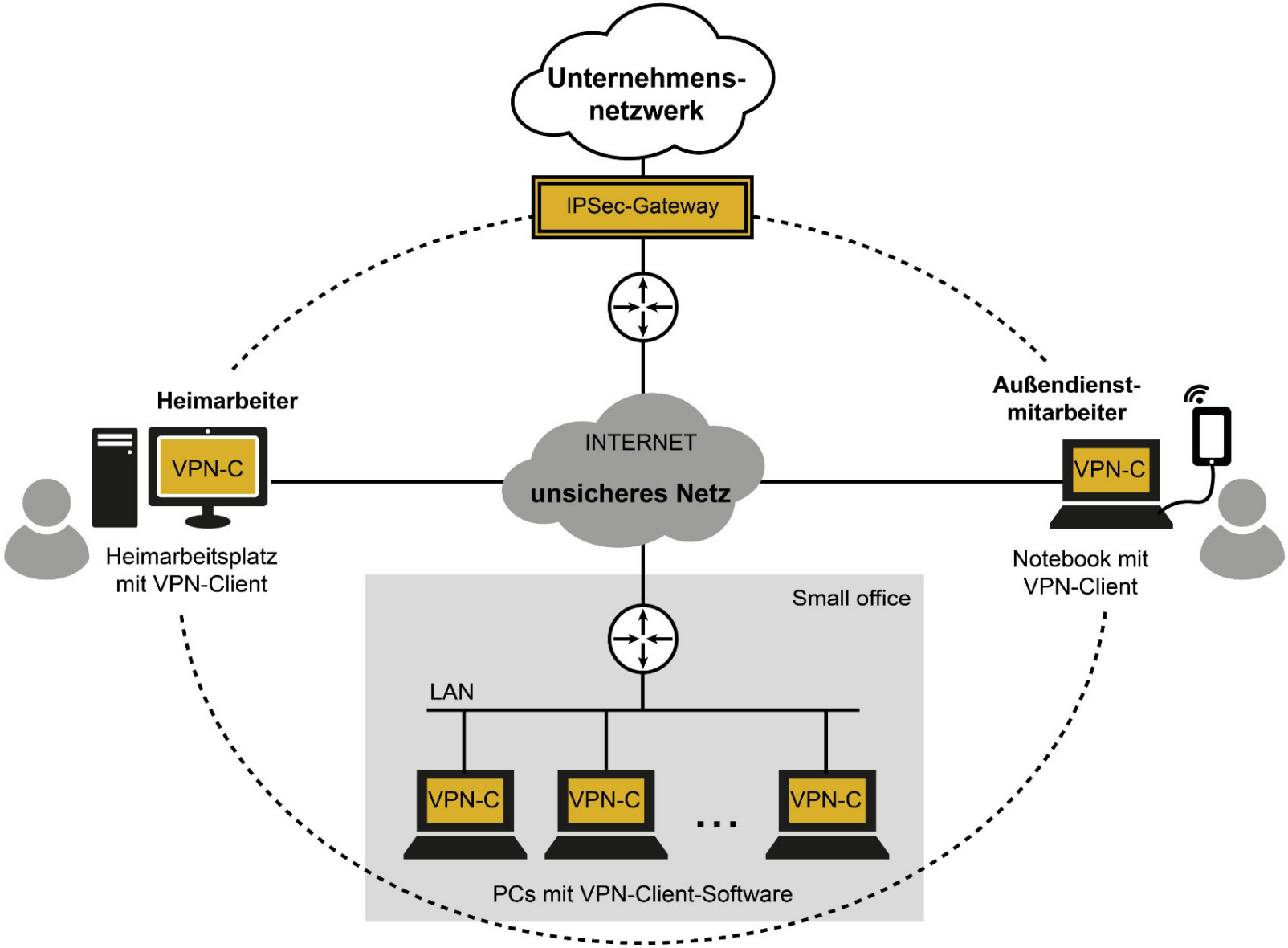
- Die Aufteilung auf zwei verschiedene SAs (Phase 1 und Phase 2) ist einer der Gründe für die Komplexität von IPSec.
- Die Trennung bietet aber auch Vorteile:
  - Der Quick Mode ist sehr schnell, weil **keine** Authentifikation mehr notwendig ist.
  - Der Schlüssel, der im Main Mode für die äußere ISAKMP SA ausgehandelt wurde, kann lange Zeit benutzt werden, weil nur sehr wenige Pakete damit verschlüsselt werden.
  - Die Lifetime der ISAKMP SA kann also wesentlich höher sein als die Lifetime der IPSec SAs.
  - Außerdem kann die ISAKMP SA auch „auf Verdacht“ aufgebaut werden, um die Etablierung von IPSec SAs bei Bedarf zu beschleunigen.

IPSec Schlüsselmanagement
→ Unternehmensweite IPSec-Lösung



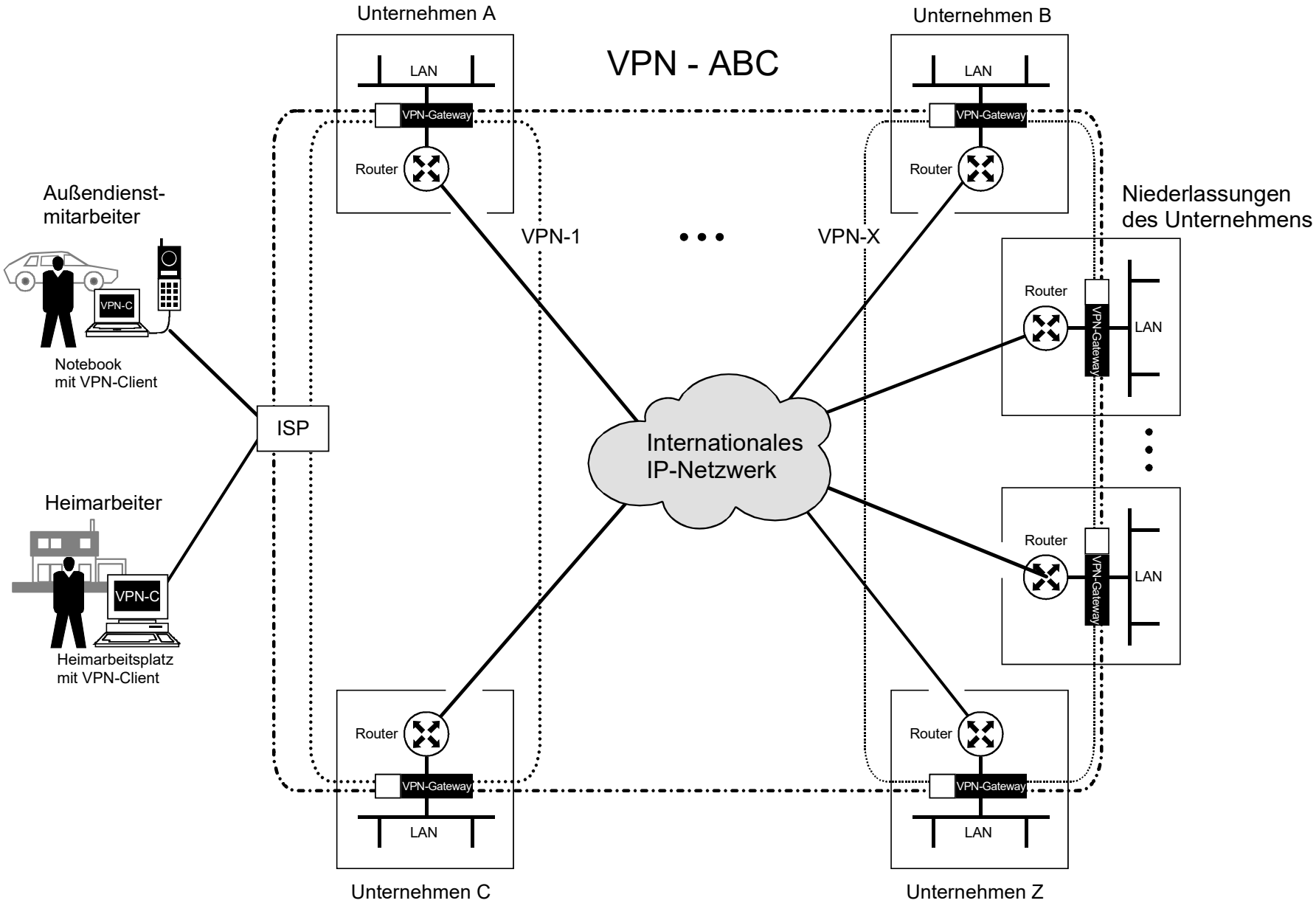
IPSec Schlüsselmanagement

→ Remote-Ankoppelung mit Hilfe einer IPSec-Lösung



IPSec Schlüsselmanagement

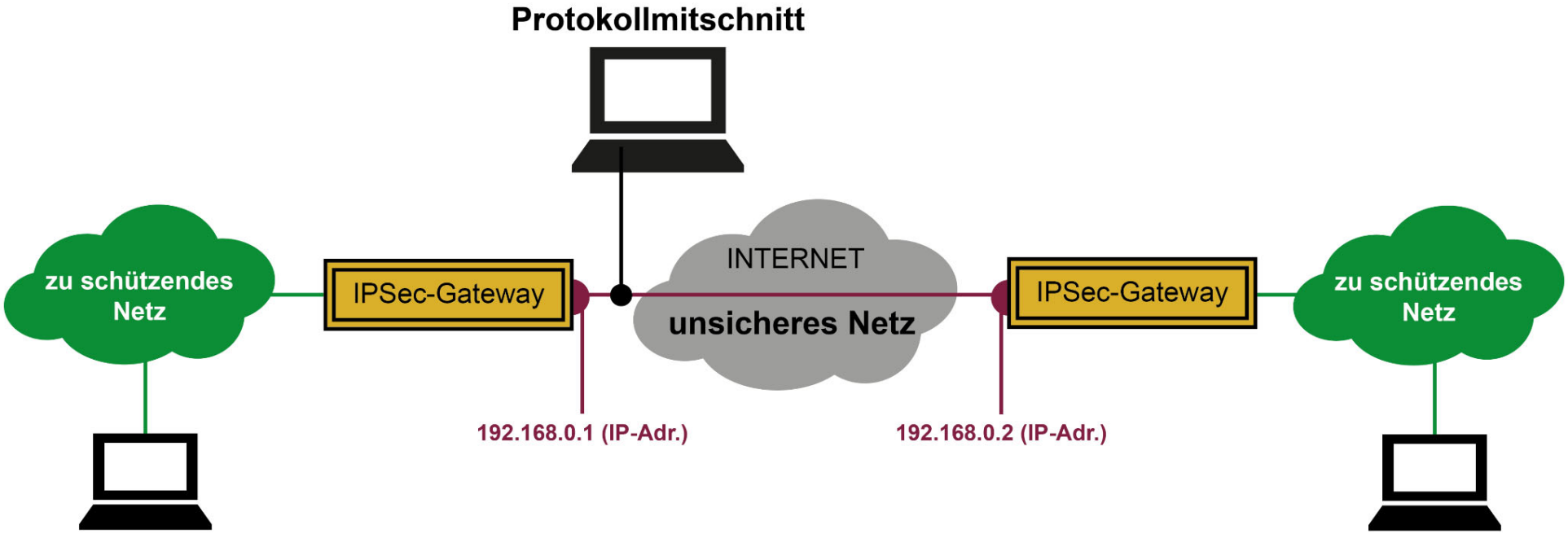
→ IPSec zwischen verschiedenen Unternehmen



IPSec Verschlüsselung
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- IPSec Header
- IPSec Schlüsselmanagement
- **Protokollmitschnitt**
- Zusammenfassung

Protokollmitschnitt
→ Übersicht



Protokollmitschnitt

→ P1: IKE Main Mode – Aushandeln der Basis-Algorithmen (1)

Frame 1: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface 0 **A >>> B**
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
Initiator SPI: a93311f793844263
Responder SPI: 0000000000000000
Next payload: Security Association (1)
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
....0 = Encryption: **Not encrypted**
.... ..0. = Commit: No commit
.... .0.. = Authentication: No authentication
Payload: Security Association (1)
Payload: Proposal (2) # 0
Proposal transforms: 1
Payload: Transform (3) # 1
Transform ID: KEY_IKE (1)
IKE Attribute (t=1,l=2): Encryption-Algorithm: AES-CBC
IKE Attribute (t=14,l=2): Key-Length: 128
IKE Attribute (t=2,l=2): Hash-Algorithm: SHA2-256
IKE Attribute (t=4,l=2): Group-Description: Unknown 31
IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key
IKE Attribute (t=11,l=2): Life-Type: Seconds
IKE Attribute (t=12,l=2): Life-Duration: 3600
...

Protokollmitschnitt

→ P1: IKE Main Mode – Aushandeln der Basis-Algorithmen (1)

Frame 2: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits) on interface 0 **A <<< B**
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Next payload: Security Association (1)
Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
....0 = Encryption: **Not encrypted**
.... ..0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x00000000
Length: 160
Payload: Security Association (1)
Payload: Proposal (2) # 0
Proposal transforms: 1
Payload: Transform (3) # 1
Transform ID: KEY_IKE (1)
IKE Attribute (t=1,l=2): Encryption-Algorithm: AES-CBC
IKE Attribute (t=14,l=2): Key-Length: 128
IKE Attribute (t=2,l=2): Hash-Algorithm: SHA2-256
IKE Attribute (t=4,l=2): Group-Description: Unknown 31
IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key
IKE Attribute (t=11,l=2): Life-Type: Seconds
IKE Attribute (t=12,l=2): Life-Duration: 3600
...

Protokollmitschnitt

→ P1: IKE Main Mode – Umsetzung des Diffie-Hellman-Verfahrens (1)

Frame 3: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0 **A >>> B**
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
....0 = Encryption: **Not encrypted**
.... ..0. = Commit: No commit
.... .0.. = Authentication: No authentication
Payload: Key Exchange (4)
Next payload: Nonce (10)
Payload length: 36
Key Exchange Data: dea402c4acede7f3deaf139fb9be156fba854c7e17d186bc...
Payload: Nonce (10)
Next payload: NAT-D (RFC 3947) (20)
Payload length: 36
Nonce DATA: 26c7cbb0b16c80fccf04292800eee2d9066ec853c1c12cea...
…

Protokollmitschnitt

→ P1: IKE Main Mode – Umsetzung des Diffie-Hellman-Verfahrens (2)

Frame 4: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0 **A <<< B**
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x00
....0 = Encryption: **Not encrypted**
.... ..0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x00000000
Length: 172
Payload: Key Exchange (4)
Next payload: Nonce (10)
Payload length: 36
Key Exchange Data: 7e04039108ed5b48f2631a8c7dbbc2322875f94ad3ed1358...
Payload: Nonce (10)
Next payload: NAT-D (RFC 3947) (20)
Payload length: 36
Nonce DATA: 290c5cdcbc3f9dd9f754be62f30338fa12af070b6fcb3dc5...
...

Protokollmitschnitt

→ **P1: IKE Main Mode – Authentifikation der Kommunikationspartner (1)**

Frame 5: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0 **A >>> B**
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x01
....1 = Encryption: **Encrypted**
.... ..0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x00000000
Length: 124
Encrypted Data (96 bytes)

Protokollmitschnitt

→ **P1: IKE Main Mode – Authentifikation der Kommunikationspartner (2)**

Frame 6: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0 **A <<< B**
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x01
....1 = Encryption: **Encrypted**
.... ..0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x00000000
Length: 92
Encrypted Data (64 bytes)

Protokollmitschnitt

→ **Aufbau der Phase 2 mit der IPSec Security Assoziation - „Basic Quick Mode" Protokolls (1)**

Frame 7: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface 0 **A >>> B**
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Next payload: Hash (8)
Exchange type: Quick Mode (32)
Flags: 0x01
....1 = Encryption: **Encrypted**
.... ..0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x7f1877fd
Length: 188
Encrypted Data (160 bytes)

Protokollmitschnitt

→ **Aufbau der Phase 2 mit der IPSec Security Assoziation - „Basic Quick Mode" Protokolls (2)**

Frame 8: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface 0 **A <<< B**
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Exchange type: Quick Mode (32)
Flags: 0x01
....1 = Encryption: **Encrypted**
.... ..0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x7f1877fd
Length: 188
Encrypted Data (160 bytes)

Protokollmitschnitt

→ **Aufbau der Phase 2 mit der IPSec Security Assoziation - „Basic Quick Mode" Protokolls (3)**

Frame 9: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0 **A >>> B**
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
Initiator SPI: a93311f793844263
Responder SPI: 8ec4e54d335d2687
Exchange type: Quick Mode (32)
Flags: 0x01
....1 = Encryption: **Encrypted**
.... ..0. = Commit: No commit
.... .0.. = Authentication: No authentication
Message ID: 0x7f1877fd
Length: 76
Encrypted Data (48 bytes)

Protokollmitschnitt

→ **Transfer Mode: Sicherung der IP-Pakete mit ESP inklusiv Anti-Replay Service (1)**

Frame 10: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0 **A >>> B**
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
Encapsulating Security Payload
ESP SPI: 0xc9e8cf58 (3387477848)
ESP Sequence: 1

Frame 11: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0 **A <<< B**
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
Encapsulating Security Payload
ESP SPI: 0xca4d2ae5 (3394054885)
ESP Sequence: 1

Frame 12: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0 **A >>> B**
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
Encapsulating Security Payload
ESP SPI: 0xc9e8cf58 (3387477848)
ESP Sequence: 2

Frame 13: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0 **A <<< B**
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
Encapsulating Security Payload
ESP SPI: 0xca4d2ae5 (3394054885)
ESP Sequence: 2

Protokollmitschnitt

→ **Transfer Mode: Sicherung der IP-Pakete mit ESP inklusiv Anti-Replay Service (2)**

Frame 14: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0 **A >>> B**
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
Encapsulating Security Payload
ESP SPI: 0xc9e8cf58 (3387477848)
ESP Sequence: 3

Frame 15: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0 **A <<< B**
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
Encapsulating Security Payload
ESP SPI: 0xca4d2ae5 (3394054885)
ESP Sequence: 3

IPSec Verschlüsselung
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Einleitung
- IPSec Header
- IPSec Schlüsselmanagement
- Protokollmitschnitt
- **Zusammenfassung**

IPSec Verschlüsselung
→ Zusammenfassung (1/2)

- **IPSec** ist der **Standard** für die **Cyber-Sicherheit von IP-Pakten** über unsichere Netze, wie das Internet.
- Der Großteil der Anwendungen liegt im Bereich der sicheren **Kommunikation zwischen Unternehmen** und deren Niederlassungen oder mit anderen Unternehmen.
- Aber auch die **Authentifikation von Mobil-Mitarbeitern** für den sicheren Zugang über das Internet in das Unternehmensnetz und seine Dienste ist ein großer Anwendungsbereich von IPSec.
- Mit der **AH-Datenstruktur** kann gewährleistet werden, dass eine **Manipulation von IP-Daten** auf dem Weg durch das Netzwerk **entdeckt** wird.

IPSec Verschlüsselung
→ Zusammenfassung (2/2)

- Außerdem findet die Authentizität der Pakete statt. Beim den ausschließlichen Einsatz des IPSec-Headers AH wird von IPSec keine Verschlüsselung durchgeführt.

- Mit Hilfe von **ESP** können **Vertraulichkeit der Übertragung**, Authentifikation des Absenders und Integrität der Daten garantiert werden, da neben der Verschlüsselung auch ähnliche Cyber-Sicherheitsmechanismen, wie in AH definiert werden können.

- Im Unterschied zu ESP bezieht sich die Authentizität von AH auch auf den IP-Header, so dass die Kombination von AH und ESP Vorteile im Sicherheitsbereich bietet, allerdings mehr Ressourcen auf den beteiligten IT-Systemen benötigt!

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

IPSec Verschlüsselung

- Vorlesung -

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

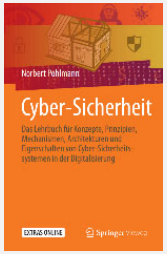
Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

securityNews

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum
- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/
- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019
- https://norbert-pohlmann.com/cyber-sicherheit/



Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/