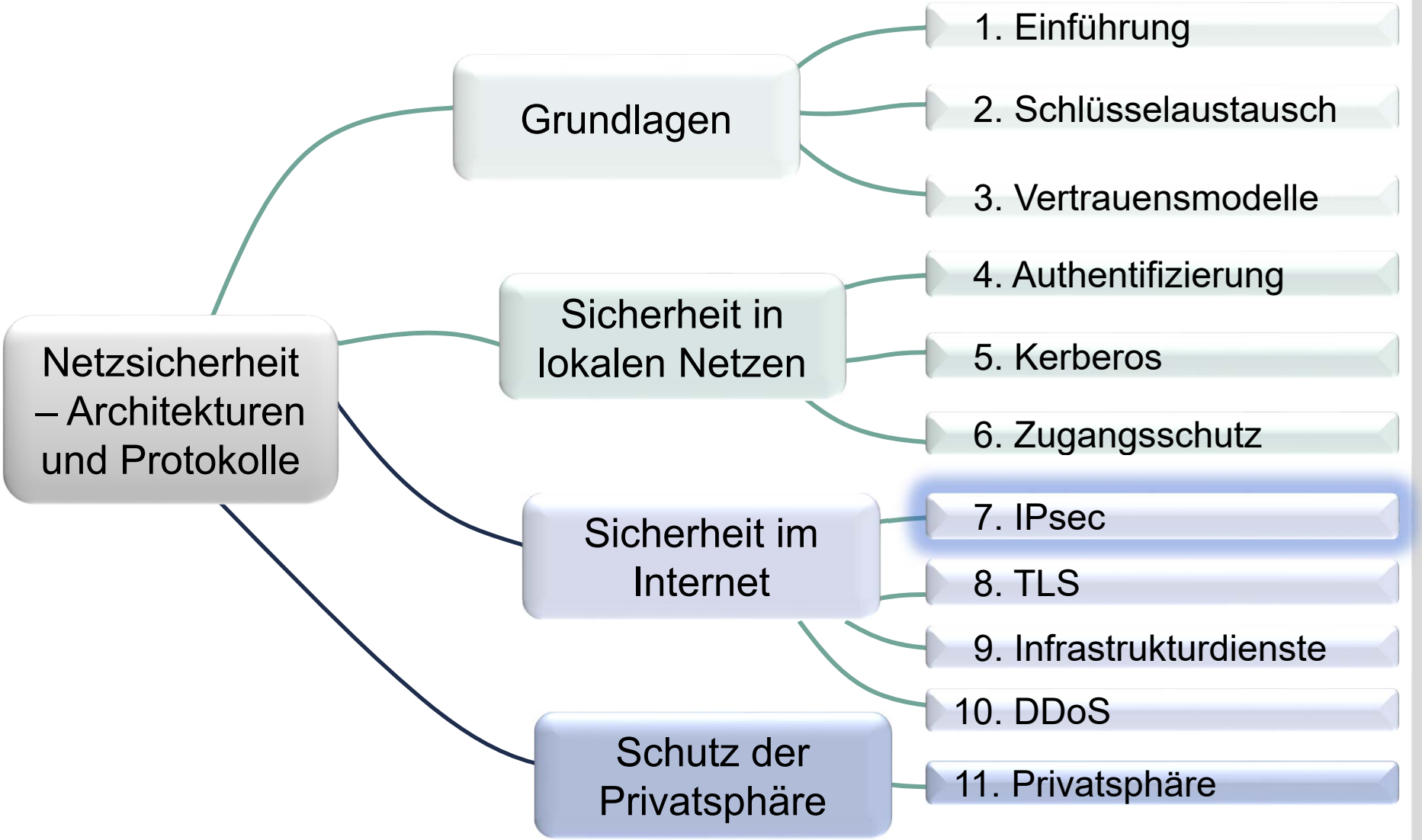
Vorlesung Netzsicherheit
Kapitel 7 – IPsec

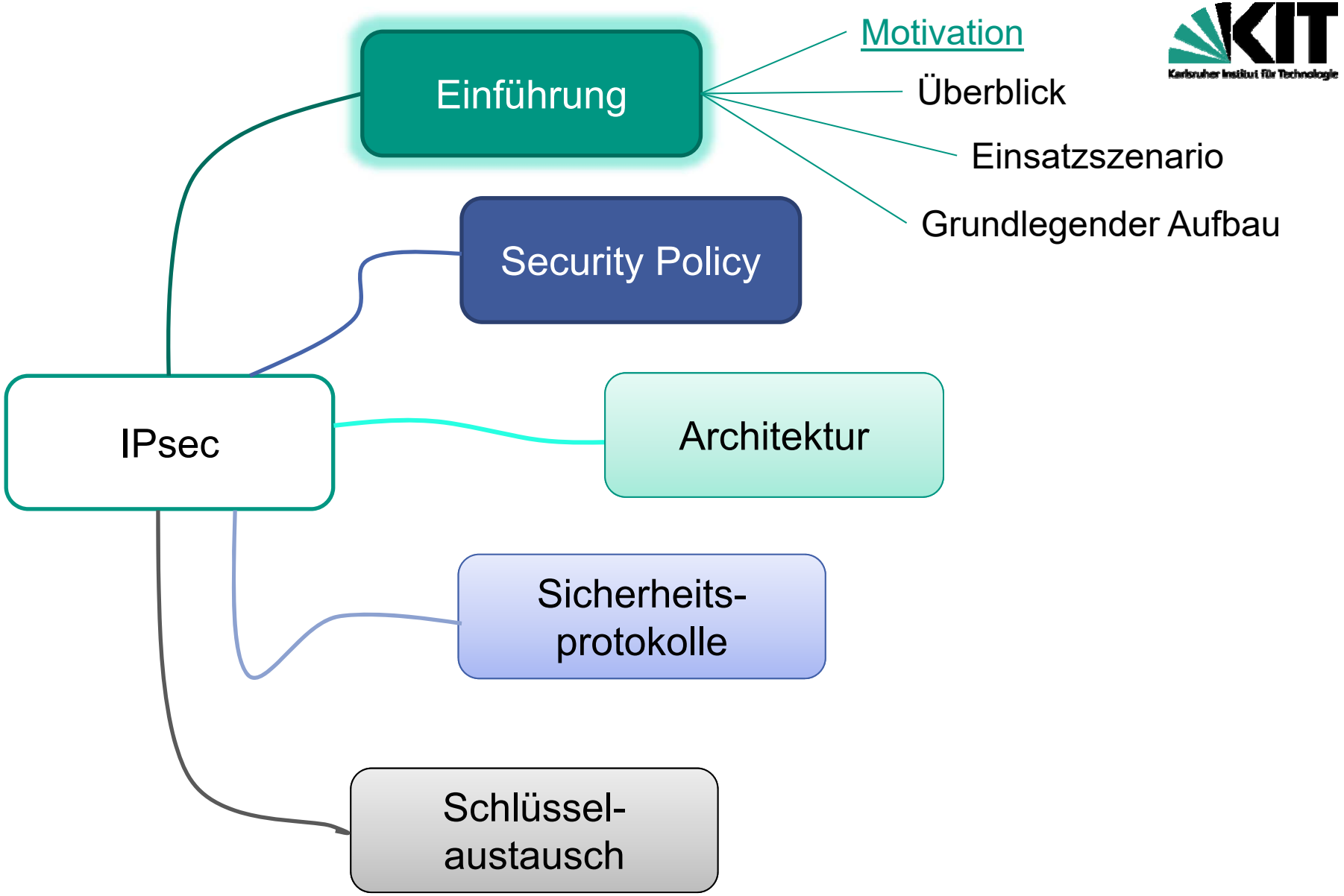
PD Dr. Ingmar Baumgart, PD Dr. Roland Bless, Matthias Flittner, Prof. Dr. Martina Zitterbart
baumgart@fzi.de, [bless, flittner, zitterbart]@kit.edu

Institut für Telematik, Prof. Zitterbart

© Peter Baumung

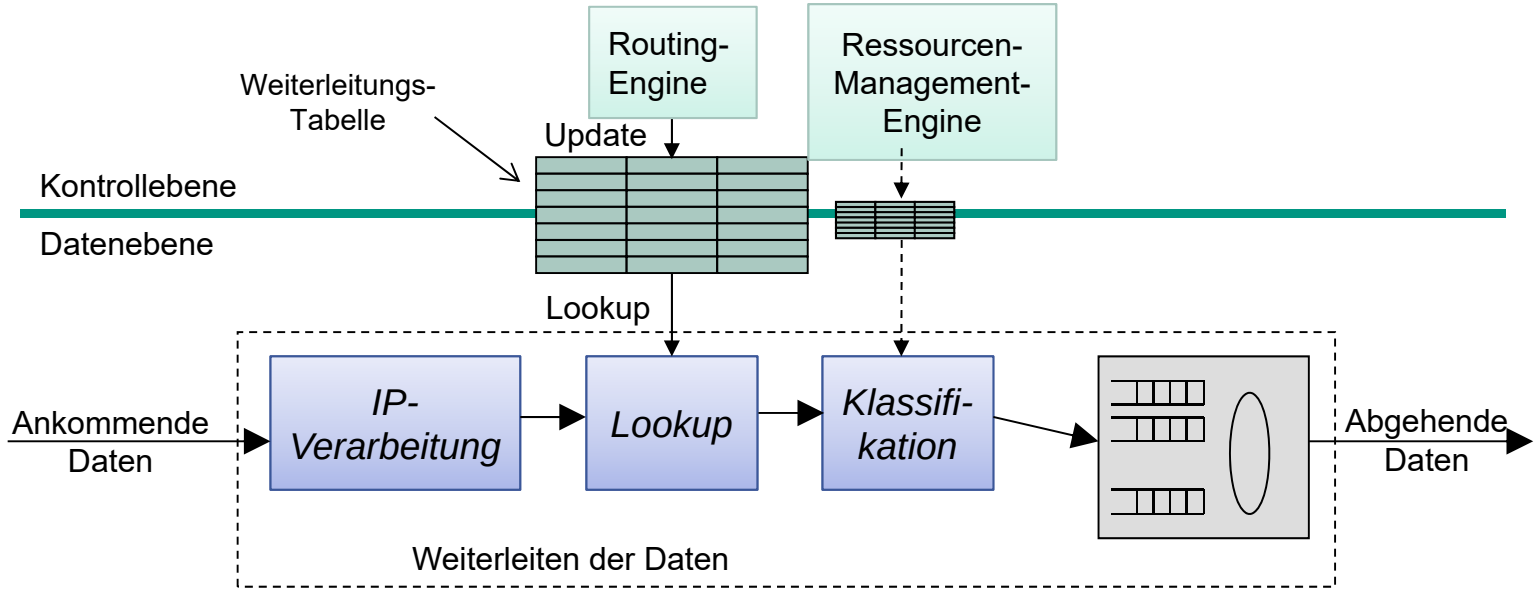
Inhalte der Vorlesung



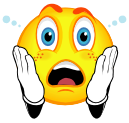

Einführung
Motivation
Überblick
Einsatzszenario
Grundlegender Aufbau
Security Policy
IPsec
Architektur
Sicherheits-
protokolle
Schlüssel-
austausch

Motivation

- Das Internet Protocol (IP)
  - Bietet einen unzuverlässigen Ende-zu-Ende Dienst (Best-Effort)
    - Kein IP-basierter Kontext in End- und Zwischensystemen, keine Verbindungen
  - Verantwortlich für das Weiterleiten von Datagrammen auf Schicht 3



→ Keine Maßnahmen zur Unterstützung von Sicherheit

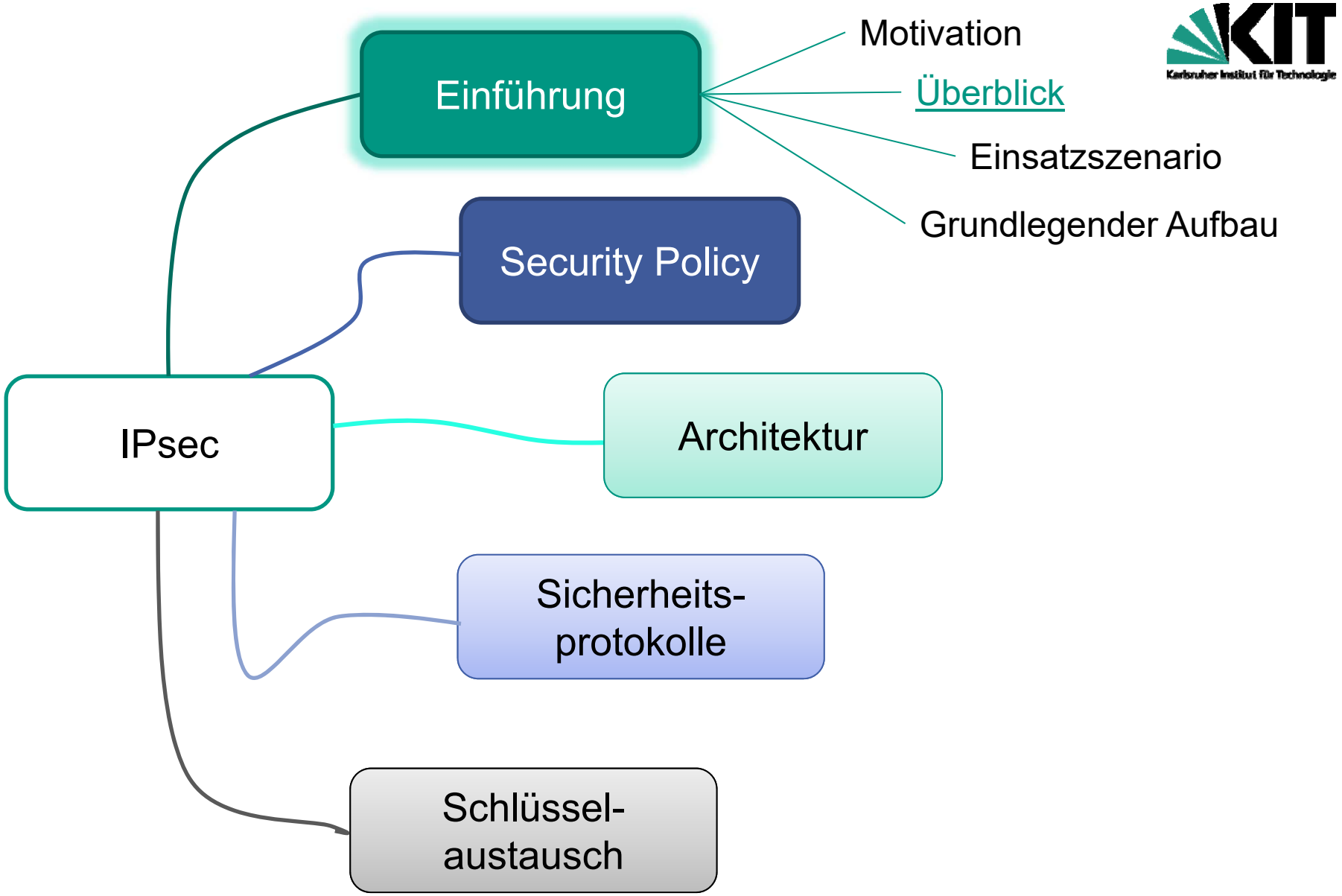


Beispiele für mögliche Angriffe

- Mitlesen von IP-Paketen
  - Eavesdropping
  - Passiver Angriff
- Falschangabe von IP-Adressen
  - IP–Spoofing
  - Aktiver Angriff
- Veränderung von IP-Paketen
  - Man-in-the-Middle
  - Aktiver Angriff
- Wiedereinspielen von IP-Paketen
  - Replay
  - Aktiver Angriff

Sicherheitsmängel bei IP

- Authentizität und Datenintegrität
  - Paket tatsächlich von angegebenem Sender gesendet?
  - Ist Inhalt unverfälscht?
  - Ist Zieladresse tatsächlich das ursprüngliche Ziel?
- Vertraulichkeit
  - Wurde Paket vom Angreifer gelesen?
- Schutz vor Wiedereinspielen
  - Aktuelles Paket oder Wiedereinspielung von Angreifer?


Einführung
Motivation
Überblick
Einsatzszenario
Grundlegender Aufbau
Security Policy
IPsec
Architektur
Sicherheits-
protokolle
Schlüssel-
austausch

IPsec = IP Security

- Ziel
  - Umsetzung von Schutzzielen für den Verkehr auf Schicht 3
    - … also für IP-Datenströme
      - Sowohl für IPv4 als auch für IPv6
      - Unabhängig vom Transportprotokoll

- Vorteile
  - Stellt Sicherheit unabhängig von Anwendungen bereit
    - IPsec sichert auch Anwendungen, die selbst Sicherheit ignorieren
    - Anwendungssoftware muss nicht geändert werden
  - Kann für Nutzer transparent sein
    - Nutzer müssen Sicherheitsmechanismen nicht kennen
    - Kein Schlüsselmaterial pro Nutzer, damit auch kein Widerrufen von Schlüssel erforderlich wenn Nutzer Organisation verlässt
  - Kann Sicherheit für individuelle Nutzer bereitstellen
    - Z.B. für Außenmitarbeiter

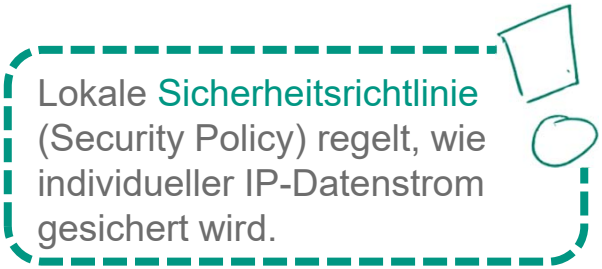
IPsec = IP Security

- 1994 initiiert durch das Internet Architecture Board
  - Ursache: Steigende Anzahl von Angriffen (IP-Spoofing …)
  - Ergänzung zu IPv4 (optional)
  - Bei IPv6 integraler Bestandteil

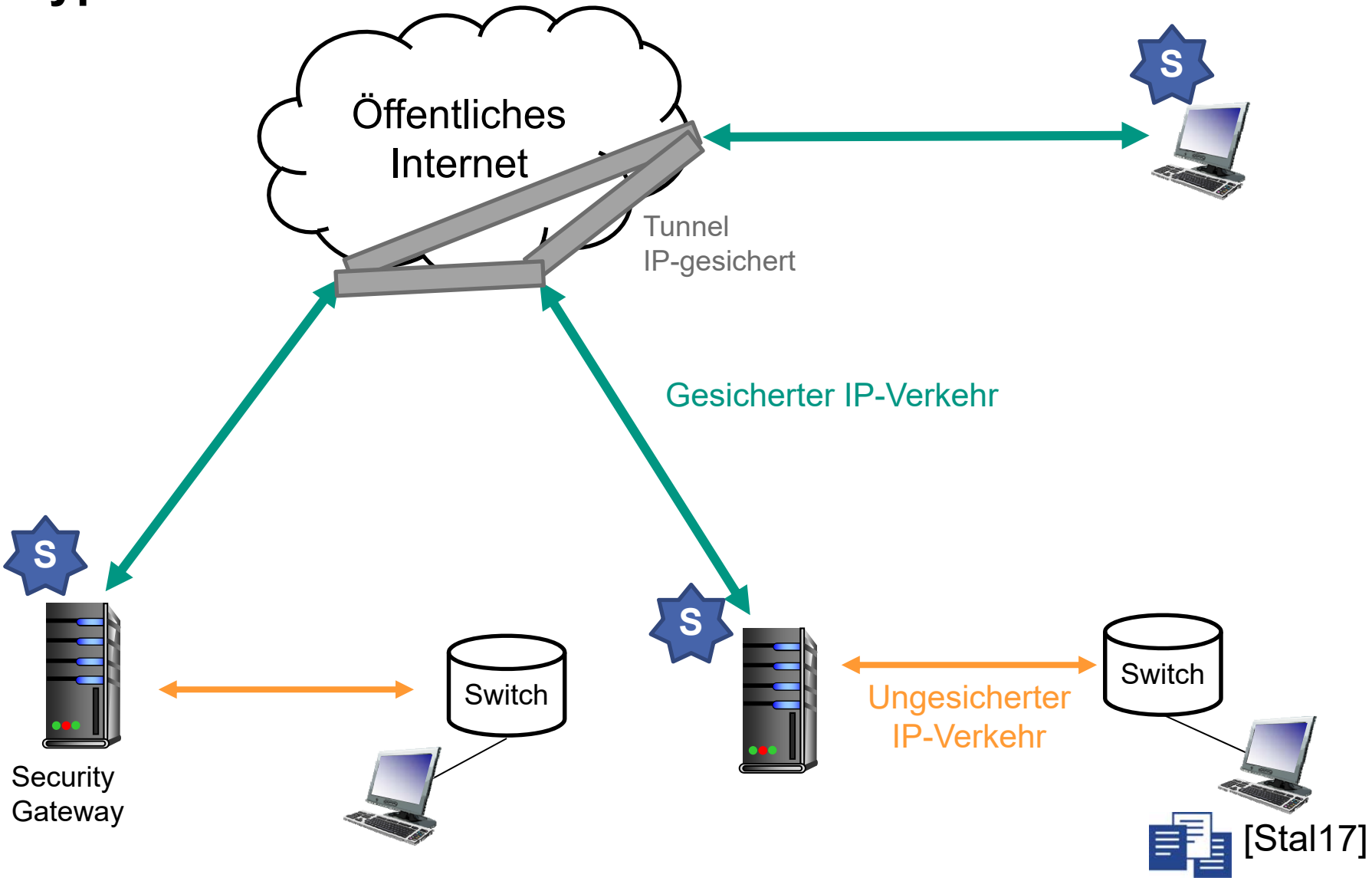
IPsec-Schutzziele

- Klassische Schutzziele
  - Integrität und Authentizität der Daten
    - Durch MAC
  - Vertraulichkeit
    - Durch Verschlüsselung

- Weitere Schutzziele
  - Zugangskontrolle
    - Authentifizierung
    - Grundlegende Filter-Funktionalität
  - Schutz vor Wiedereinspielen
    - Durch Sequenznummern
  - Schutz vor Verkehrsanalyse
    - Durch Padding und Dummy-Pakete



Typisches Einsatzszenario von IPsec



Typisches Einsatzszenario von IPsec

- Unternehmen hat lokale Netze an verschiedenen Standorten
  - Lokale Netze ungesichert
  - Verkehr von/zu anderen Lokationen über IPsec geschützt
  - IPsec auch für einzelne Nutzer von außen möglich

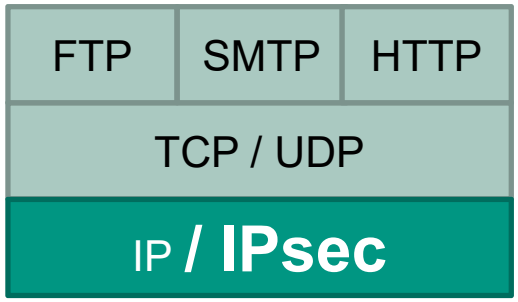
- 

  - … kennzeichnet Systeme, die IPsec implementieren müssen

- IPsec häufig für VPNs (Virtual Private Networks) genutzt

Einordnung in den Protokollstack

- Protokollstack



  - Nutzung
    - Durch alle oberhalb von IP angesiedelten Protokolle
    - Für IP selbst
    - Transparent für Anwendungen
  - Typischerweise Bestandteil des Betriebssystems

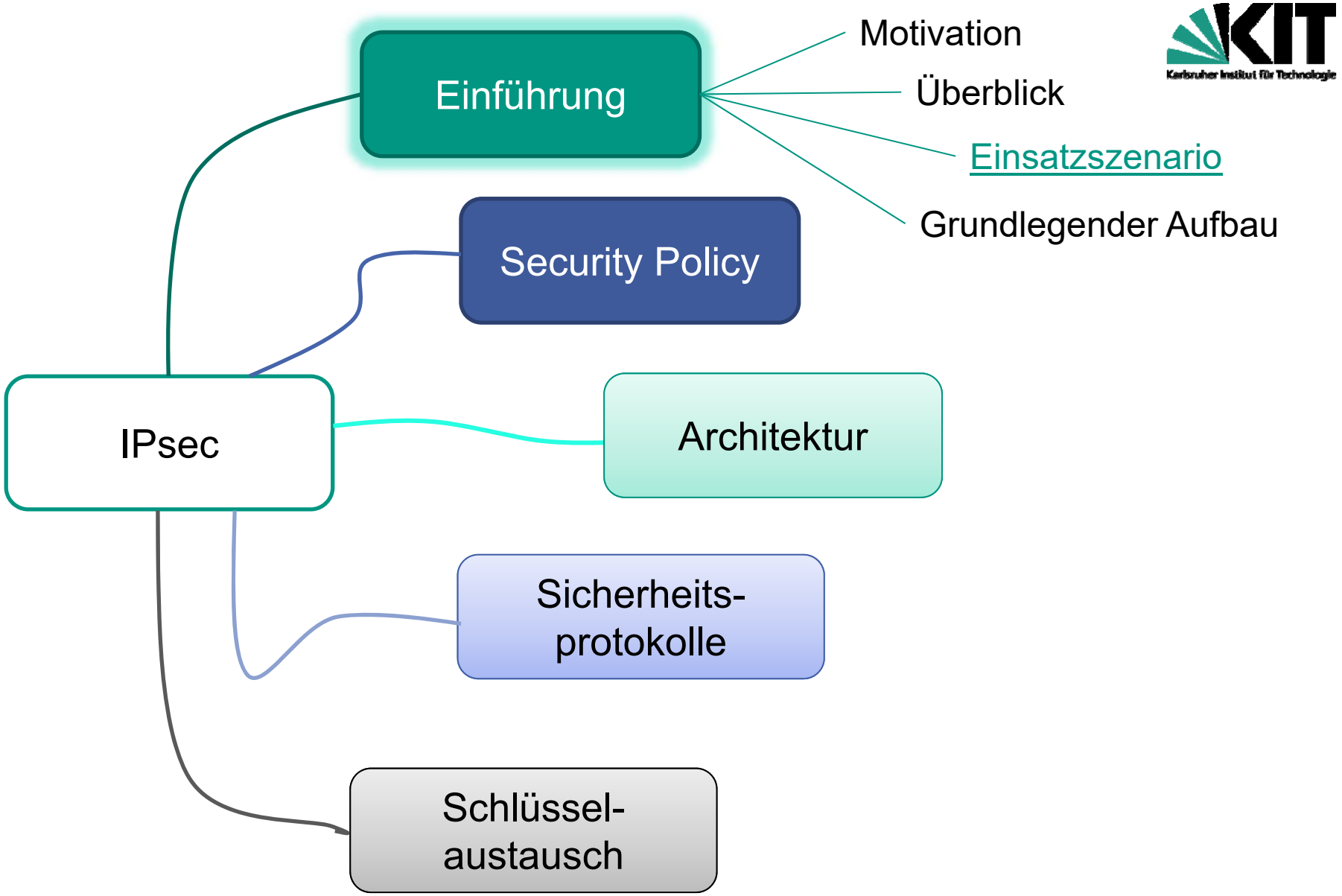
Definition von IPsec

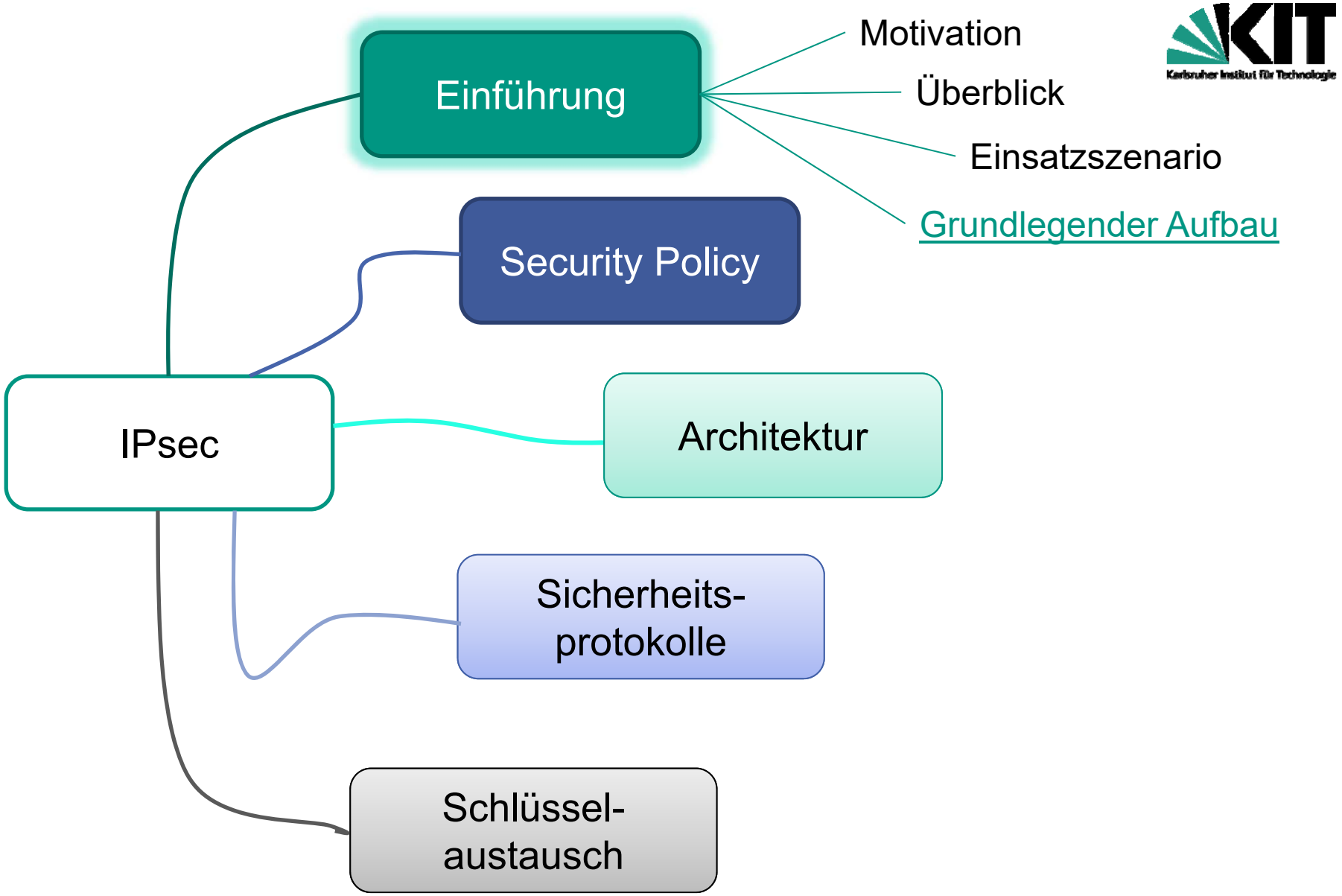
- Vielzahl von RFCs
  … insgesamt ziemlich unübersichtlich

- Beispiele
  - RFC 4301: Security Architecture for IP
  - RFC 4302: IP Authentication Header (AH)
  - RFC 4303: IP Encapsulating Security Payload (ESP)
  - RFC 7296: Internet Key Exchange (IKEv2) Protocol

- Überblick über aktuelle RFCs
  - RFC 6071: IP Security and Internet Key Exchange Document Roadmap

- Aktuell: IPsecv3 und IKEv2


Einführung
Motivation
Überblick
Einsatzszenario
Grundlegender Aufbau
Security Policy
IPsec
Architektur
Sicherheits-
protokolle
Schlüssel-
austausch


Einführung
Motivation
Überblick
Einsatzszenario
Grundlegender Aufbau
Security Policy
IPsec
Architektur
Sicherheits-
protokolle
Schlüssel-
austausch

Grundlegende Komponenten von IPsec

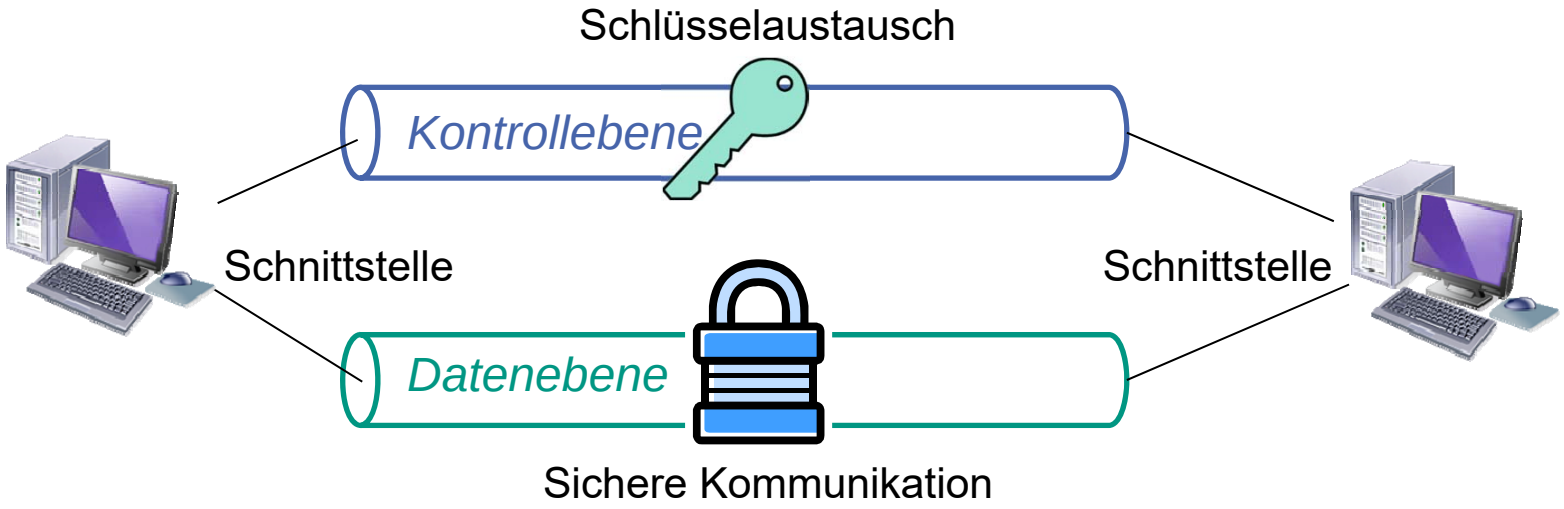
- Schlüsselaustausch
  - Internet Key Exchange (IKE)

- Protokolle zur sicheren Kommunikation
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

- „Datenbanken“ für
  - Sicherheitsrichtlinien (SPD)
  - Sicherheitsassoziationen (SAD)

Kontroll- und Datenebene

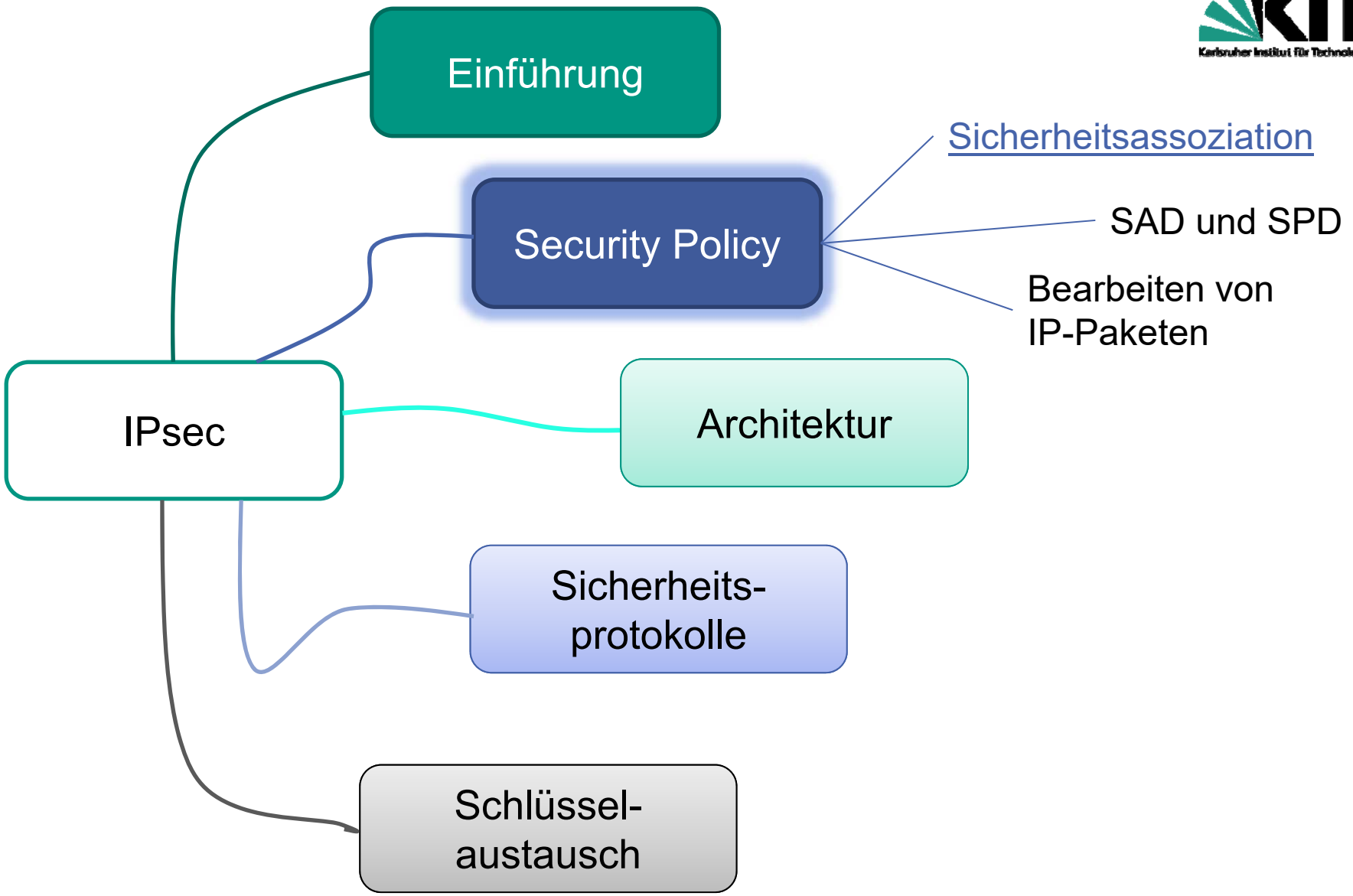
- Entkopplung von Schlüsselaustausch und Sicherung
  - Kontrollebene: Aushandlung wie und mit welchen Schlüsseln zu schützen ist
  - Datenebene: Schutz der „Nutzdaten“ aus höheren Schichten



Eigenschaften

- Auswahl von Sicherheitsprotokoll
- Bestimmen der zu nutzenden Algorithmen
- Installation des erforderlichen Schlüsselmaterials

- Zwei Übertragungsmodi
  - Tunnel-Modus
    - Schützt das gesamte IP-Paket
  - Transport-Modus
    - Schützt primär höhere Schichten


Einführung
Security Policy
Sicherheitsassoziation
SAD und SPD
Bearbeiten von IP-Paketen
IPsec
Architektur
Sicherheits-protokolle
Schlüssel-austausch

Security Policy

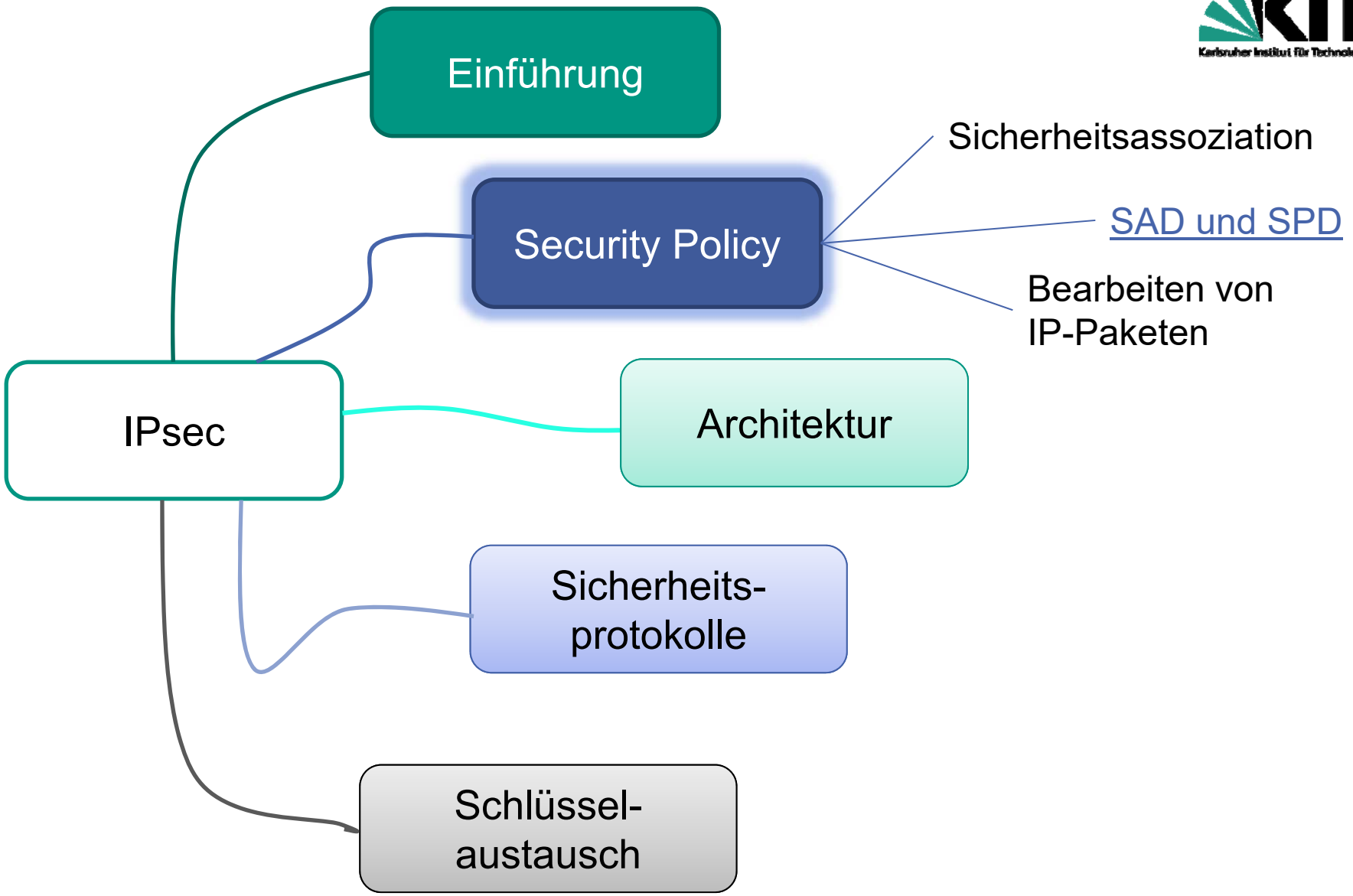
- Flexibilität bei IPsec
  - Kommunikationspartner können entscheiden welche Sicherheitsanforderungen an einen IP-Datenstrom gestellt werden
    - Kommunikationspartner vereinbaren hierzu Security Policy
    - Security Policy wird für jedes IP-Paket angewandt

Sicherheitsassoziation

- Security Association (SA)
  - Unidirektionale Sicherheitsassoziation („Verbindung“) zwischen zwei IP-Instanzen
    - Falls bidirektional notwendig müssen zwei SAs aufgebaut werden
    - Ausnahme: IKE-SA
  - Nutzt entweder AH- oder ESP-Protokoll
  - Eindeutige Identifikation einer SA (pro System)
    - Security Parameter Index (SPI)
      - 32 Bit Integer, nur lokal signifikant
      - Wird im Kopf von AH und ESP übertragen
    - IP-Zieladresse
    - Genutztes Sicherheitsprotokoll (AH oder ESP)

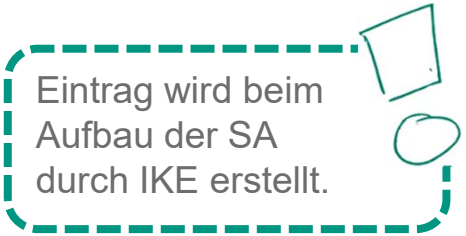
Sicherheitsassoziation

- SA zwischen folgenden Instanzen möglich
  - Endsystem – Endsystem
  - Endsystem – Zwischensystem
  - Zwischensystem – Zwischensystem


Einführung
Security Policy
Sicherheitsassoziation
SAD und SPD
Bearbeiten von IP-Paketen
IPsec
Architektur
Sicherheits-protokolle
Schlüssel-austausch

„Datenbank“ der Sicherheitsassoziationen (SAD)

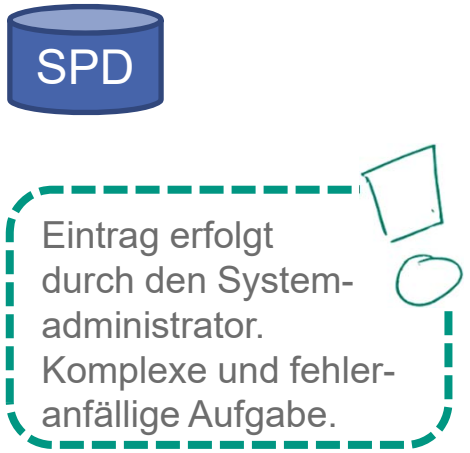
- Aufgabe
  - Hält Parameter aktiver gesicherter IP-Datenströme
- Parameter
  - Security Parameter Index (SPI)
  - Sequenznummer
  - Flag das anzeigt ob Sequenznummernüberlauf SA beendet
  - Fenster zum Schutz gegen Wiedereinspielen
  - AH- oder ESP-Informationen
    - Schlüssel etc.
  - Lebenszeit der SA
    - in Bytes oder Zeiteinheiten gemessen
    - Soft-Lifetime (Warnung), Hard-Lifetime (SA deaktiviert)
  - IPsec Übertragungsmodus
  - Pfad MTU
    - für Fragmentierung notwendig, bzw. Verhinderung der Fragmentierung



„Datenbank“ der Policies (SPD)

- Richtlinien nach denen der Verkehr zu schützen ist
  - Für welche Partnerinstanzen müssen Sicherheitsassoziationen mit welchen Parametern ausgehandelt werden?
  - Zu sendende Pakete werden gemäß SPD auf SA abgebildet

- „Datenbank“ der Policies (SPD)
  - Eintrag enthält eine Reihe sogenannter Selektoren
    - Quell- und Ziel-IP-Adresse
    - Quell- und Ziel-Port
    - Protokoll der nächsten Schicht
  - Behandlung des IP-Pakets
    - BYPASS, PROTECT, DISCARD
    - Protokoll
    - Übertragungsmodus



Beispiel einer SPD eines Endsystems

Protokoll	Quell-IP	Quell-Port	Ziel-IP	Ziel-Port	Aktion	Kommentar
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Fehlernachricht
*	1.2.3.101	*	**1.2.3.0/24**	*	PROTECT: ESP, Transport-Mode	Verschlüsselter Intranet-Verkehr
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP, Transport-Mode	Verschlüsselt zum Server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS, doppelte Verschlüsselung vermeiden
*	1.2.3.101	*	**1.2.4.0/24**	*	DISCARD	Geschütztes LAN (DMZ)
*	1.2.3.101	*	*	*	BYPASS	Internet

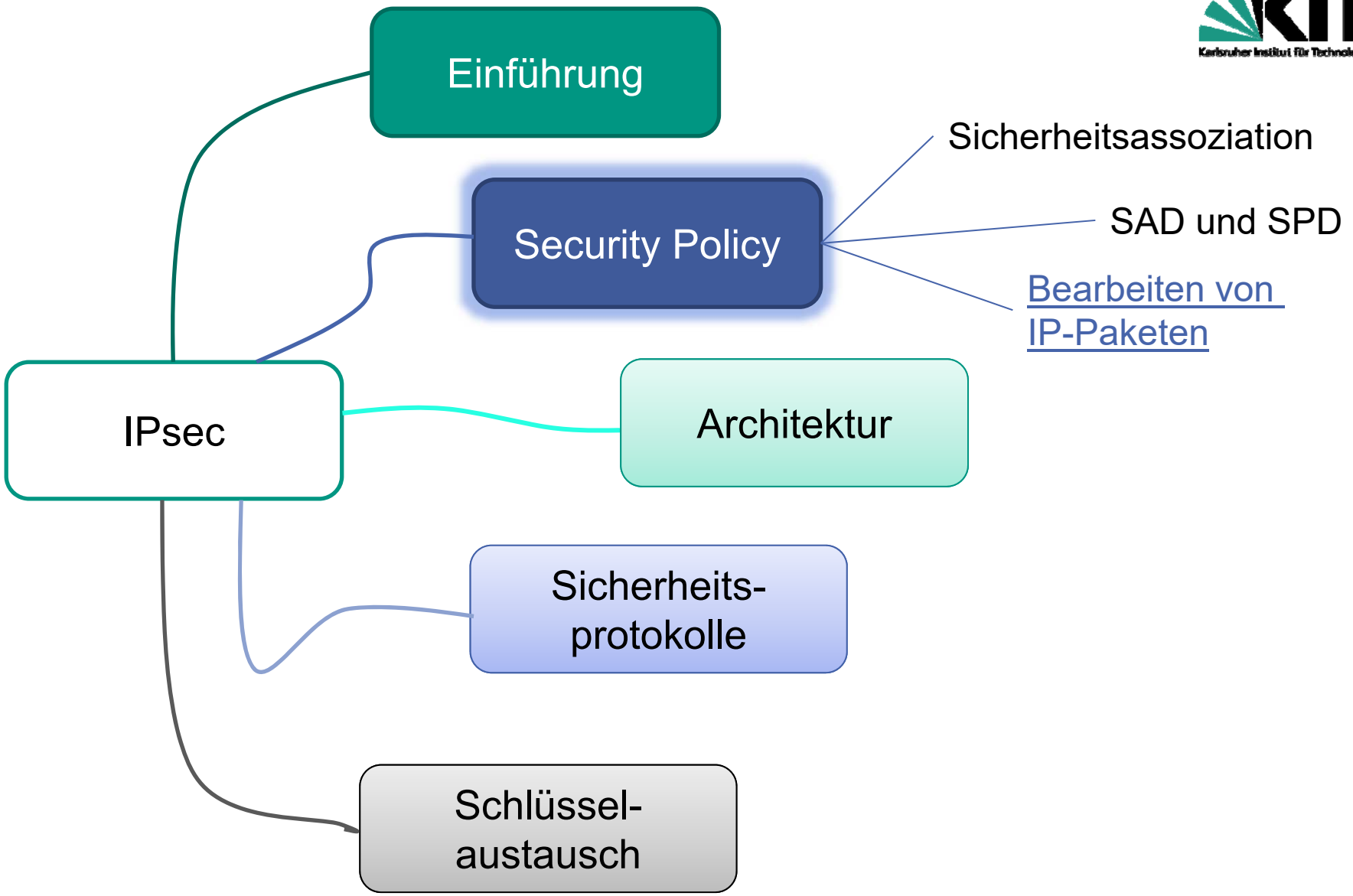

[Stal17]

Beispiel

- Zugrunde liegendes Szenario
  - Lokale Konfiguration mit zwei Netzen
    - Basisnetz: 1.2.3.0/24
    - Geschütztes Netz (DMZ): 1.2.4.0/24
      - Durch Firewalls vom Rest getrennt
  - SPD eines Endsystems mit IP 1.2.3.101

- Richtlinien
  - Zeile 1: IKE-Verkehr (Port 500) wird nicht durch IPsec geschützt
  - Zeile 2: ICMP-Verkehr wird nicht geschützt und weitergeleitet
  - Zeile 3: Verkehr ins sichere Netz wird geschützt
  - Zeile 4: Verbindungen zum Server im sicheren Netz werden geschützt
  - Zeile 5: Zugriff auf bestimmten Rechner in geschütztem Netz, Verkehr ist bereits durch TLS (Port 443) geschützt
  - Zeile 6: Verworfen, da Ziel im geschützten Netz
  - Zeile 7: Verkehr ins Internet

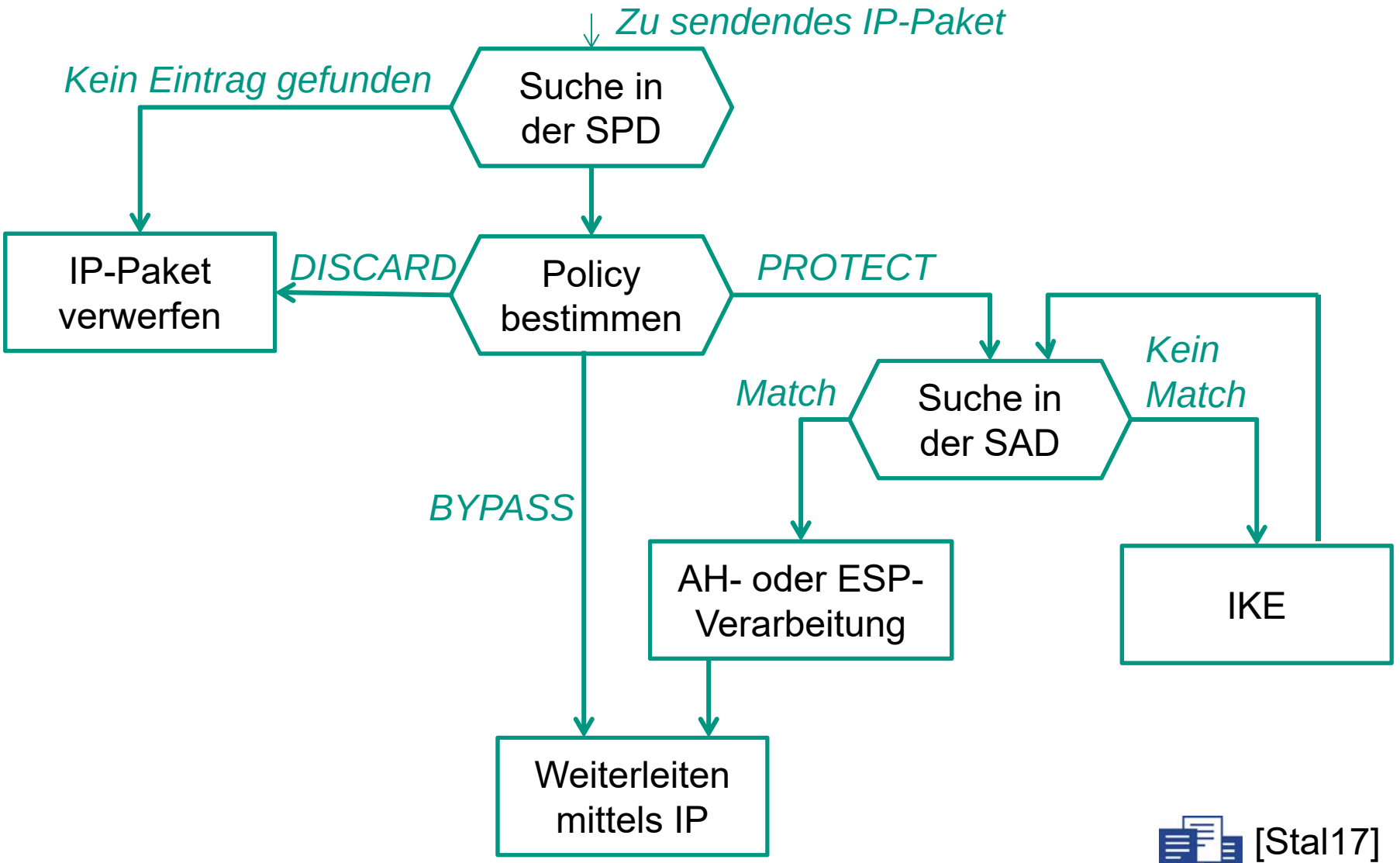
[vgl. Kapitel TLS]


Einführung
Security Policy
Sicherheitsassoziation
SAD und SPD
Bearbeiten von IP-Paketen
IPsec
Architektur
Sicherheits-protokolle
Schlüssel-austausch

Bearbeiten von IP-Paketen

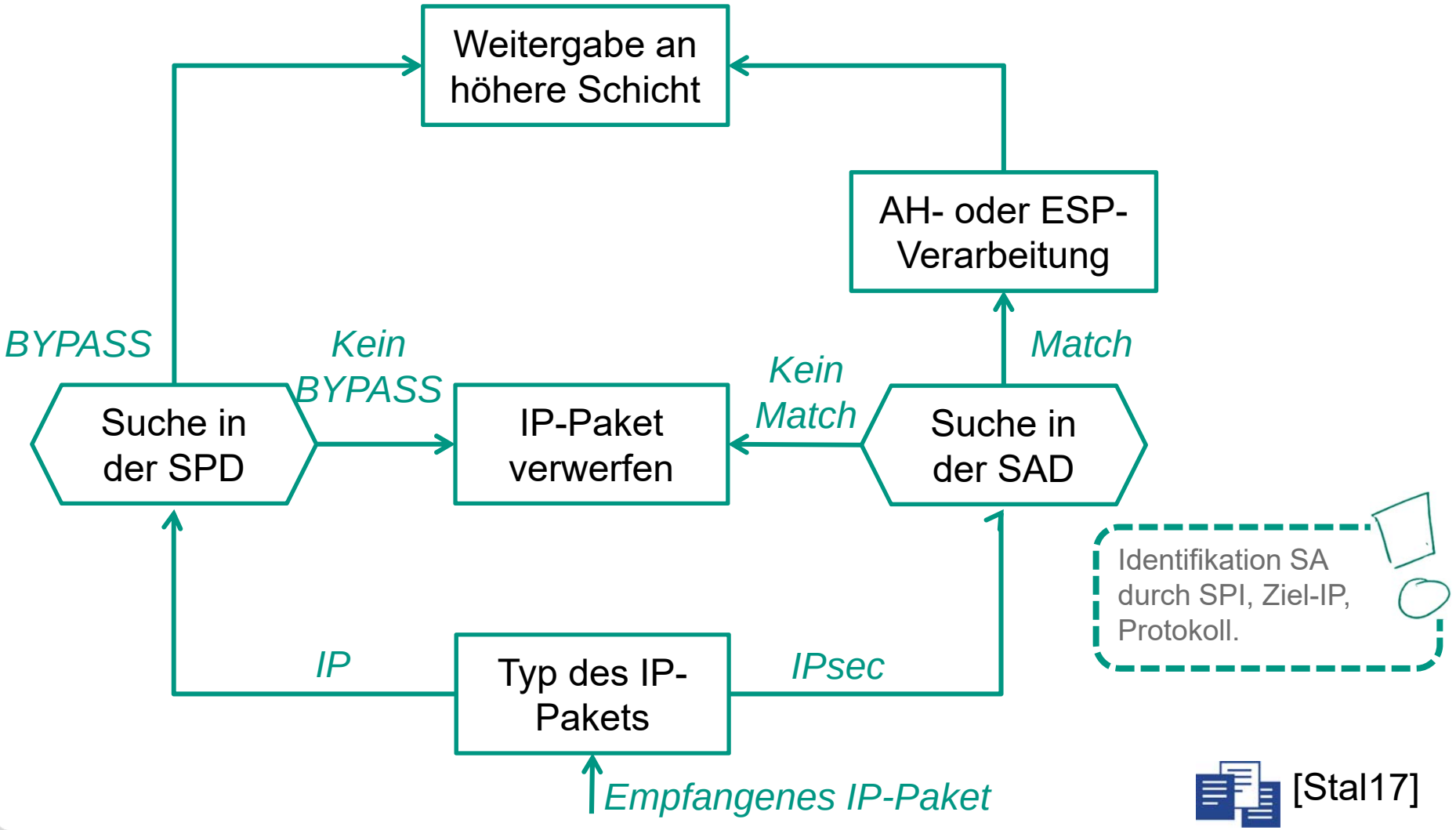
- Klassifikation
  - *Welche IP-Pakete sollen wie geschützt werden?*
- Selektoren für ausgehende IP-Pakete
  - Quell- und Zieladresse (IPv4 oder IPv6)
  - Schicht-4-Protokoll (TCP oder UDP), Quell- und Zielports
  - Name (nur auf Endsystem verfügbar)
    - Voll qualifizierter DNS-Benutzername (z.B.: administrator@tm.kit.edu)
    - X.500 Name
- Selektoren für eingehende IP-Pakete
  - Zieladresse (IPv4 oder IPv6)
  - Sicherheitsprotokoll (AH oder ESP)
  - SPI (Security Parameter Index)
- Klassifikation anhand der *Security Policy Database* (SPD)
  - Festlegung der Verarbeitungsstrategien

Bearbeiten zu sendendes IP-Paket

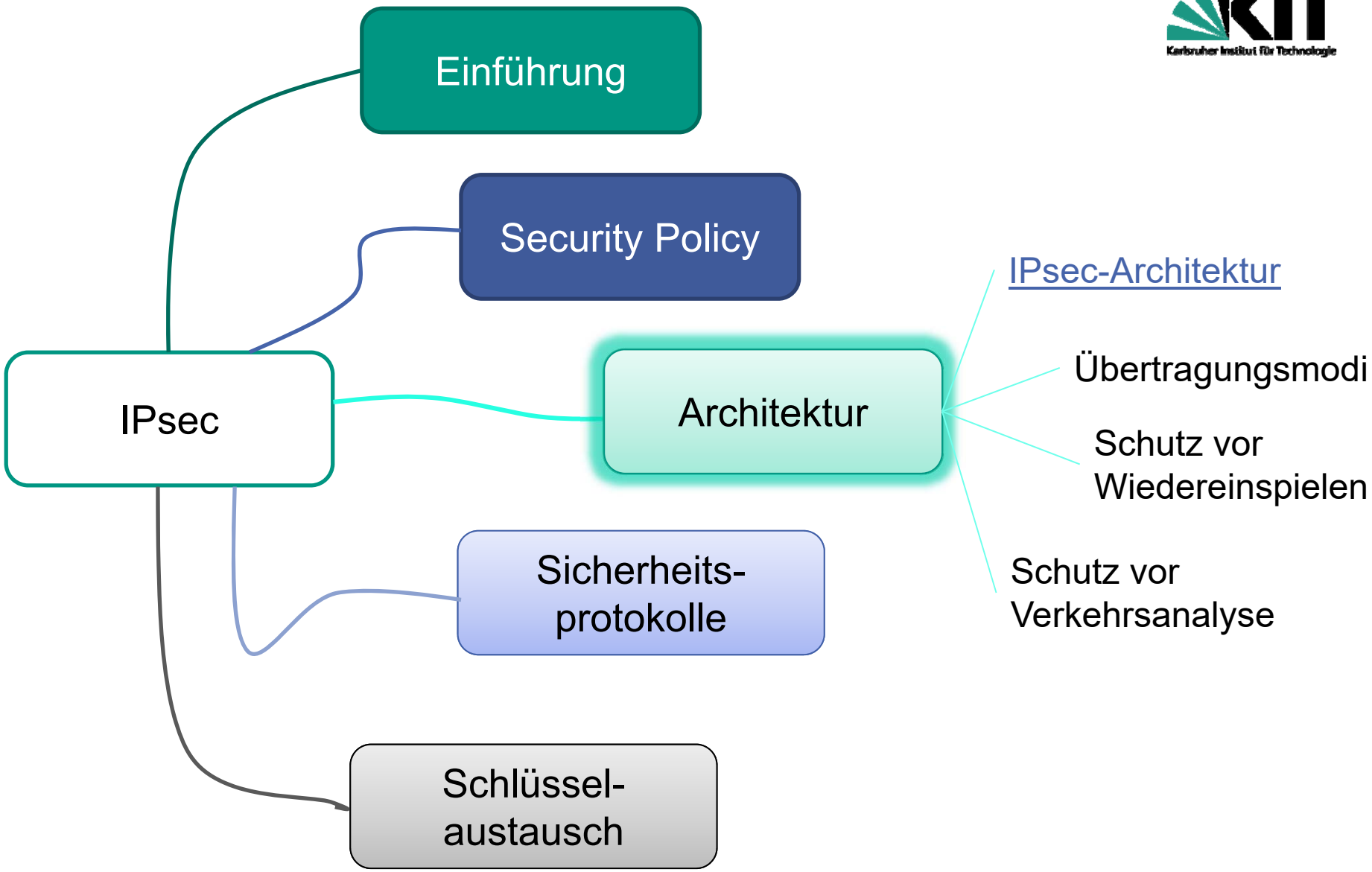


[Stal17]

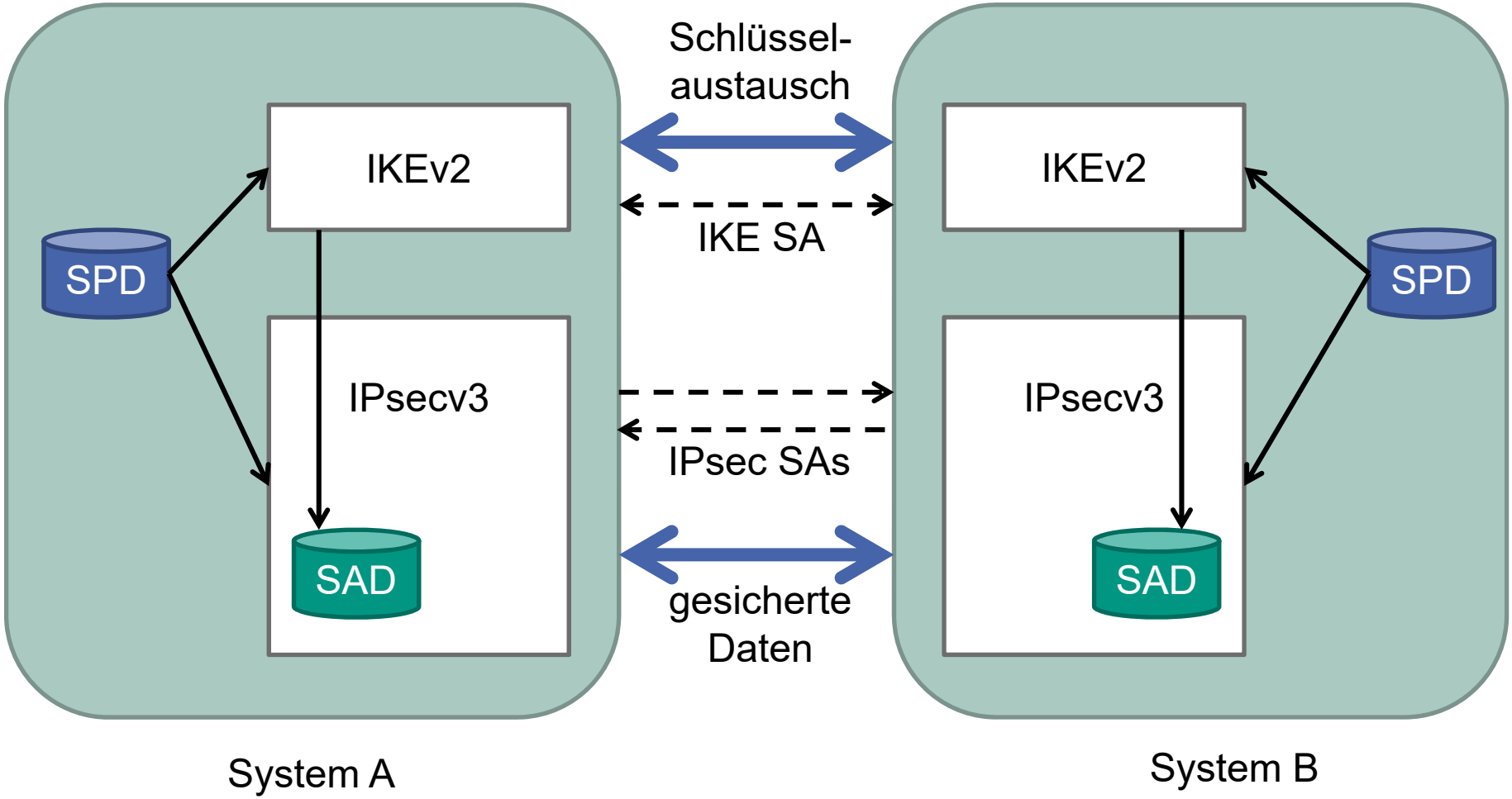
Bearbeitung empfangenes IP-Paket



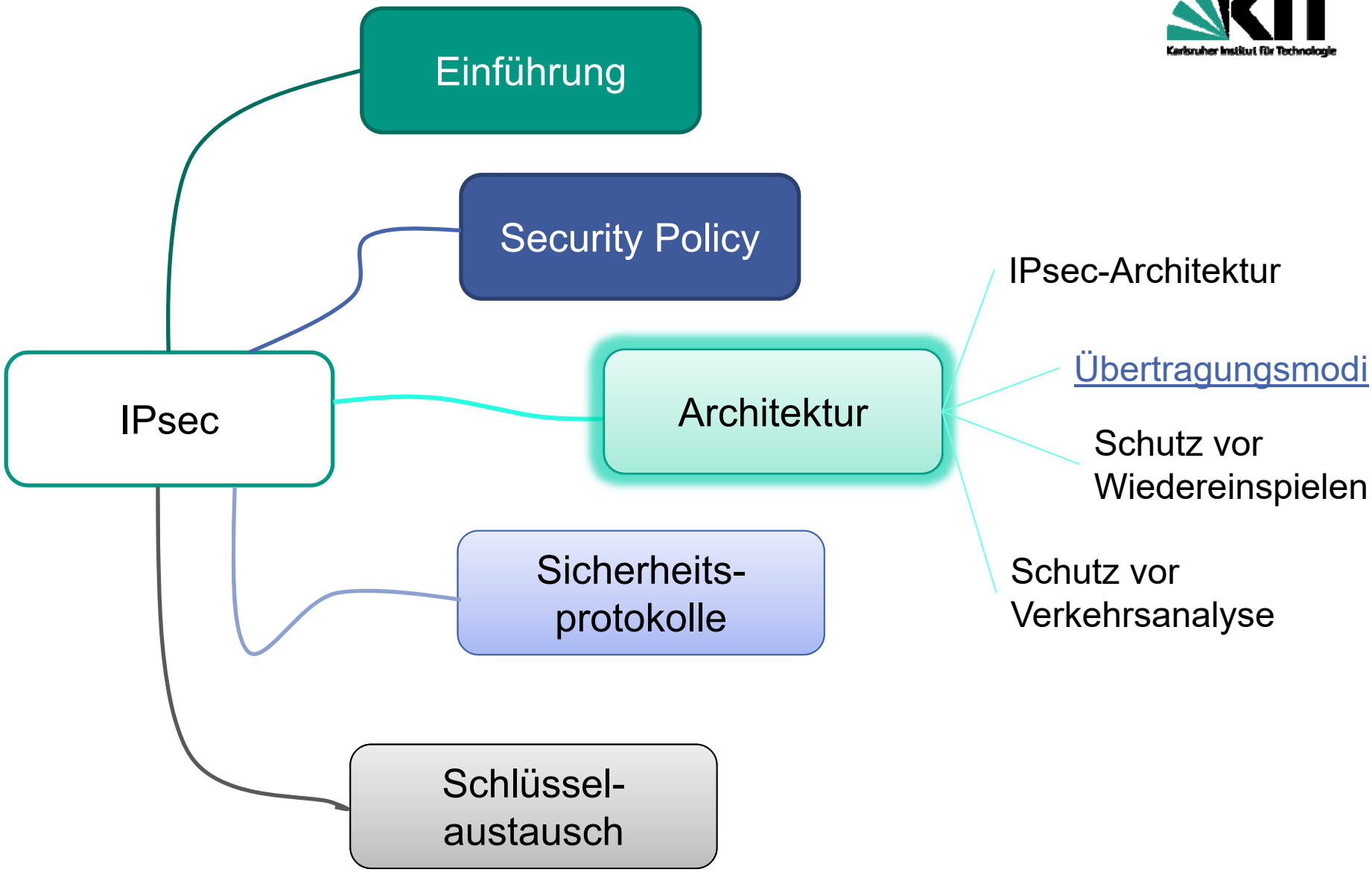
[Stal17]


Einführung
Security Policy
IPsec
Architektur
IPsec-Architektur
Übertragungsmodi
Schutz vor Wiedereinspielen
Schutz vor Verkehrsanalyse
Sicherheits-protokolle
Schlüssel-austausch

IPsec-Architektur



[Stal17]


Einführung
Security Policy
IPsec
Architektur
IPsec-Architektur
Übertragungsmodi
Schutz vor Wiedereinspielen
Schutz vor Verkehrsanalyse
Sicherheits-protokolle
Schlüssel-austausch

Übertragungsmodi

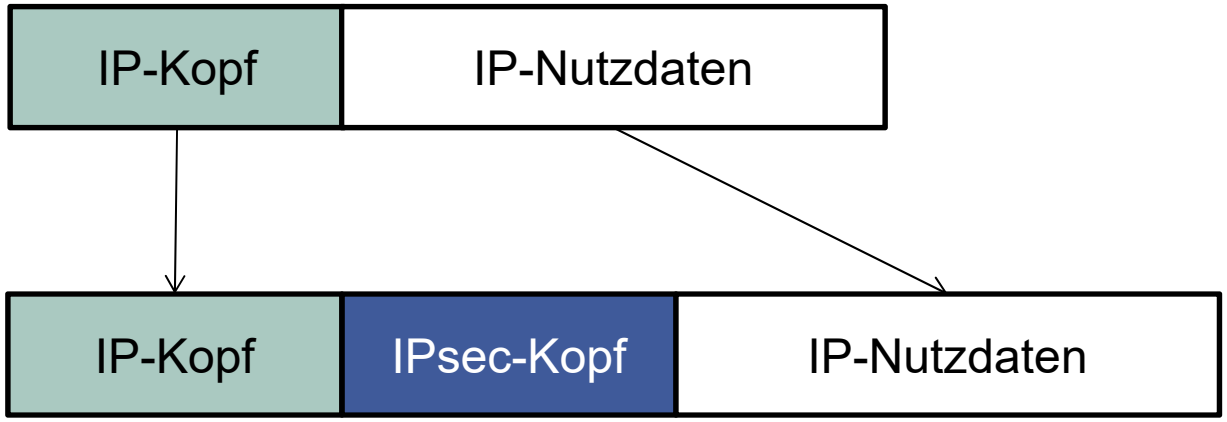
- Zwei Übertragungsmodi
  - Transport-Modus
  - Tunnel-Modus

… es lassen sich folgende Endpunkte unterscheiden

- Kommunikationsendpunkt
  - Quell- und Zielsystem der ausgetauschten IP-Pakete
- Kryptografischer Endpunkt
  - Endpunkte der Sicherheitsprotokolle
    - Also von AH und ESP

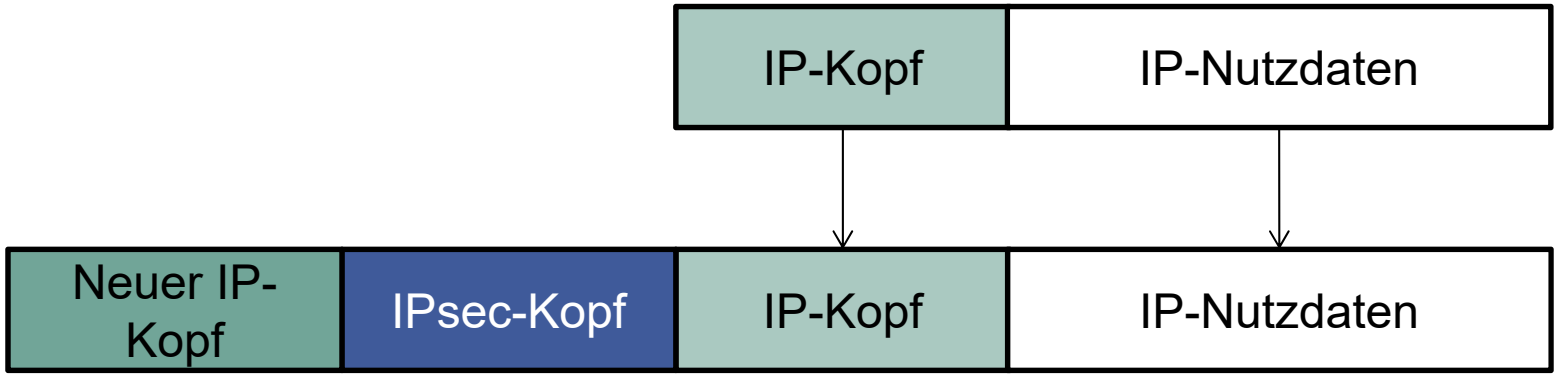
Übertragungsmodi

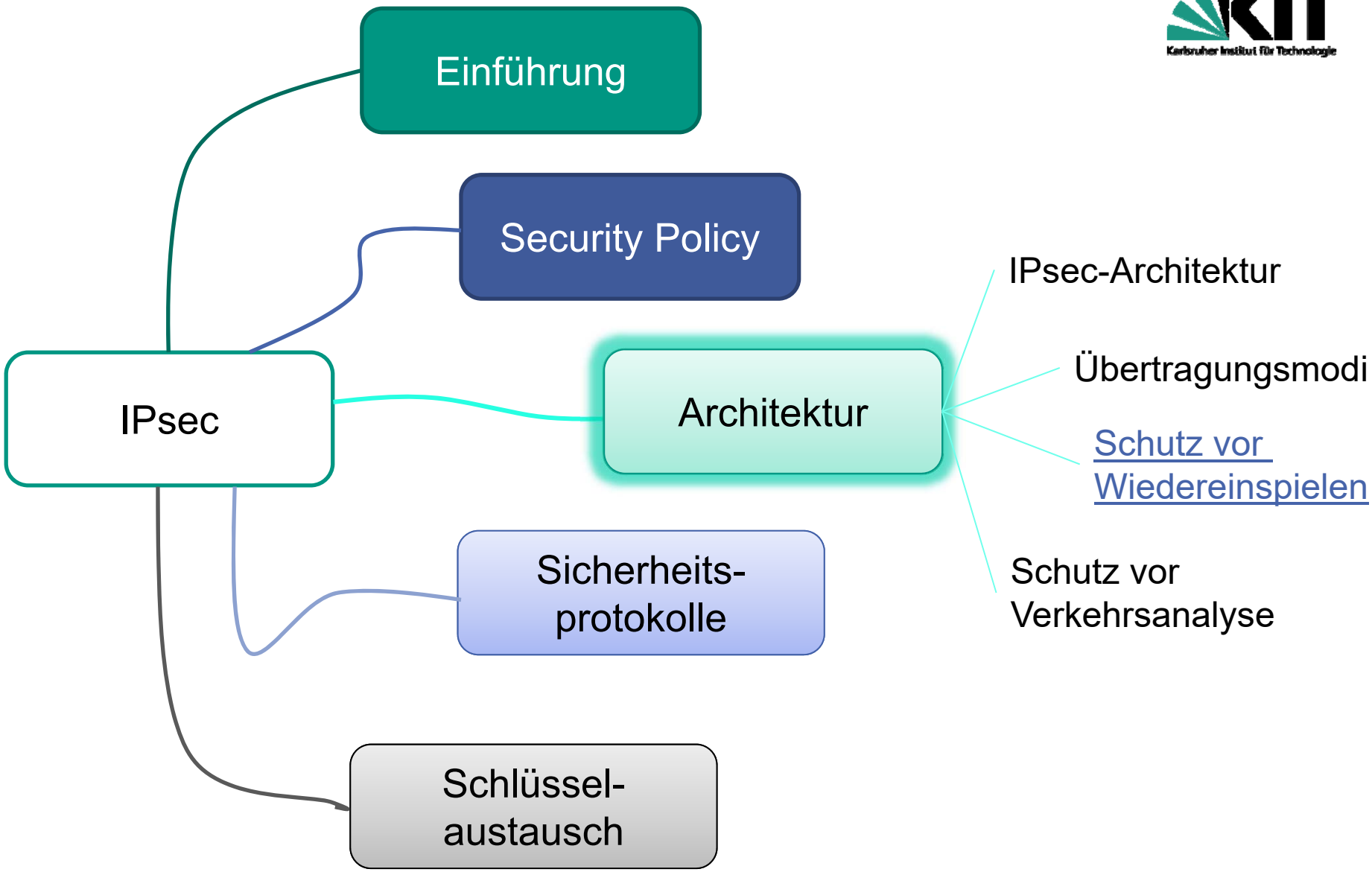
- Transport-Modus
  - Einsatz zwischen Kommunikationsendpunkten
    - Können sowohl im Endsystem als auch im Zwischensystem sein
    - Kryptografischer Endpunkt stimmt mit Kommunikationsendpunkt überein
  - Schützt die Nutzdaten



Übertragungsmodi

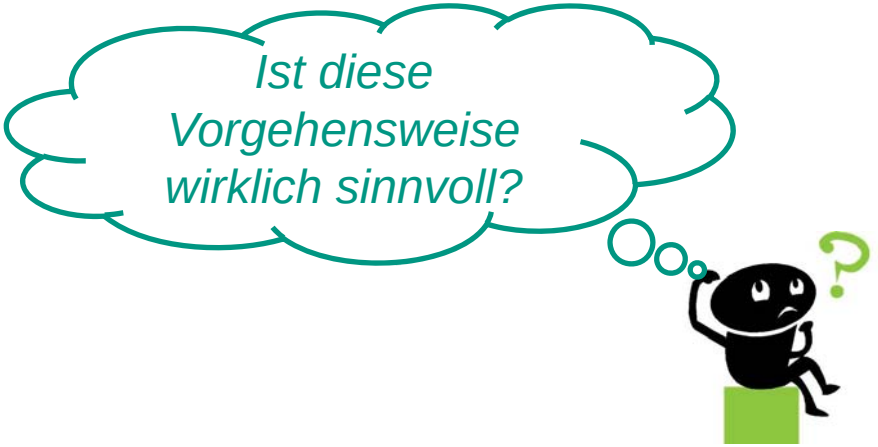
- Tunnel-Modus
  - Einsatz zwischen beliebigen Systemen
    - Oft ist ein Endpunkt *kein* Kommunikationsendpunkt
  - IP-in-IP-Kapselung
    - Schützt gesamtes IP-Paket
    - Router auf dem Weg haben keinen Zugriff auf Original-IP-Kopf
  - Anwendung
    - Security-Gateway als Stellvertreter für Endsysteme eines Netzes
    - Nutzung von privaten IP-Adressen




Einführung
Security Policy
IPsec
Architektur
IPsec-Architektur
Übertragungsmodi
Schutz vor Wiedereinspielen
Schutz vor Verkehrsanalyse
Sicherheits-protokolle
Schlüssel-austausch

Schutz vor Wiedereinspielen

- Verwendung von Sequenznummern
  - Eindeutig und monoton wachsend
    - Pro gesendetem Paket um Eins erhöht
  - Benachrichtigung bei Sequenznummernüberlauf
    - Falls gefordert, Neuaushandlung des Schlüsselmaterials
- Hypothetisches Empfängerverhalten
  - Sequenznummer echt größer als letzte empfangene?
    - Ja: Paket akzeptieren und Sequenznummer speichern
    - Nein: Paket verwerfen



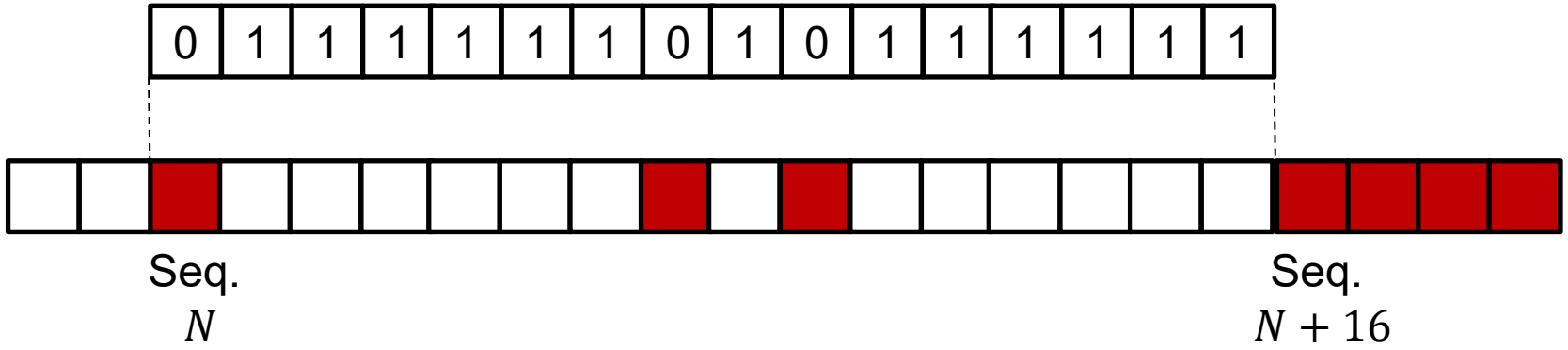
Schutz vor Wiedereinspielen

- Fenstermechanismus
  - Bereich von Sequenznummern, die akzeptiert werden - Sliding Window
- Fenstermanagement
  - Fenstergröße: W
    - Empfohlene Größe: $\mathrm{W} = 64$
  - Oberes Ende
    - Höchste empfangene Sequenznummer
  - Unteres Ende
    - $Oberes\ Ende\ - W + 1$
- Empfang eines Pakets
  - Sequenznummer größer als höchste bisher empfangene
    - Akzeptieren (nach Authentizitätsprüfung)
    - Fenster verschieben
  - Sequenznummer im Fensterbereich und noch nicht erhalten
    - Akzeptieren (nach Authentizitätsprüfung)
    - Sequenznummer als empfangen markieren
  - Sequenznummer im Fensterbereich und bereits erhalten
    - Paket verwerfen
  - Sequenznummer kleiner als unteres Ende
    - Paket verwerfen

[Scha14]

Schutz vor Wiedereinspielen

- Beispiel
  - Empfangsfenster der Größe 16
  - Nicht empfangenes Paket rot markiert

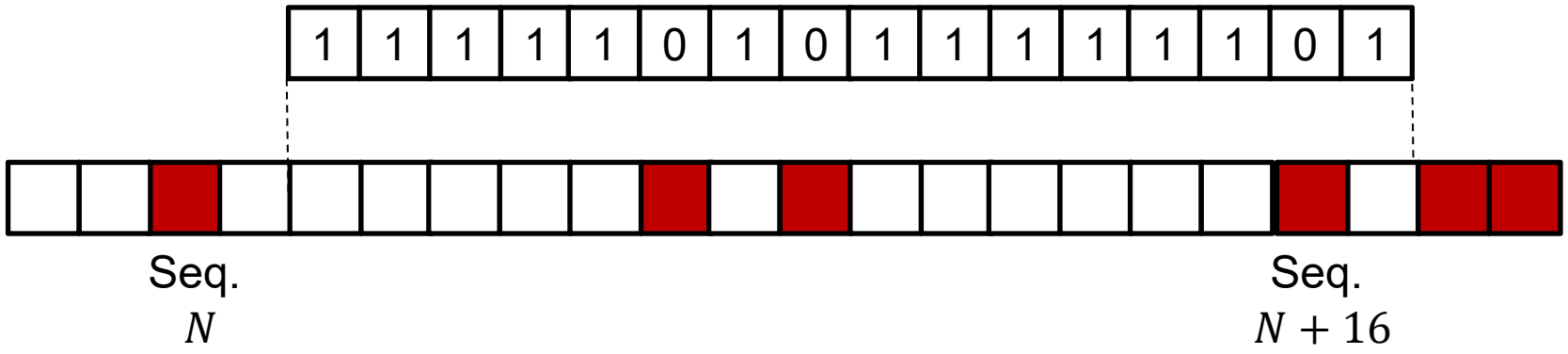


  - Höchstes empfangenes Paket habe Sequenznummer $N + 15$
  - Letztes empfangenes Paket$N\ + 13$
  - Paket mit Sequenznummer N kann noch empfangen werden

[Scha14]

Schutz vor Wiedereinspielen

- Beispiel fortgesetzt
  - Paket mit Sequenznummer N wurde nicht empfangen
  - Paket mit Sequenznummer $N + 17$ wird empfangen
  - Fenster wird um zwei Stellen verschoben

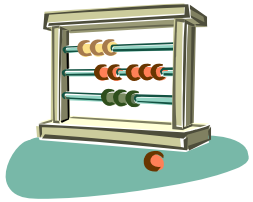


  - Paket mit Sequenznummer N muss nun bei Empfang verworfen werden

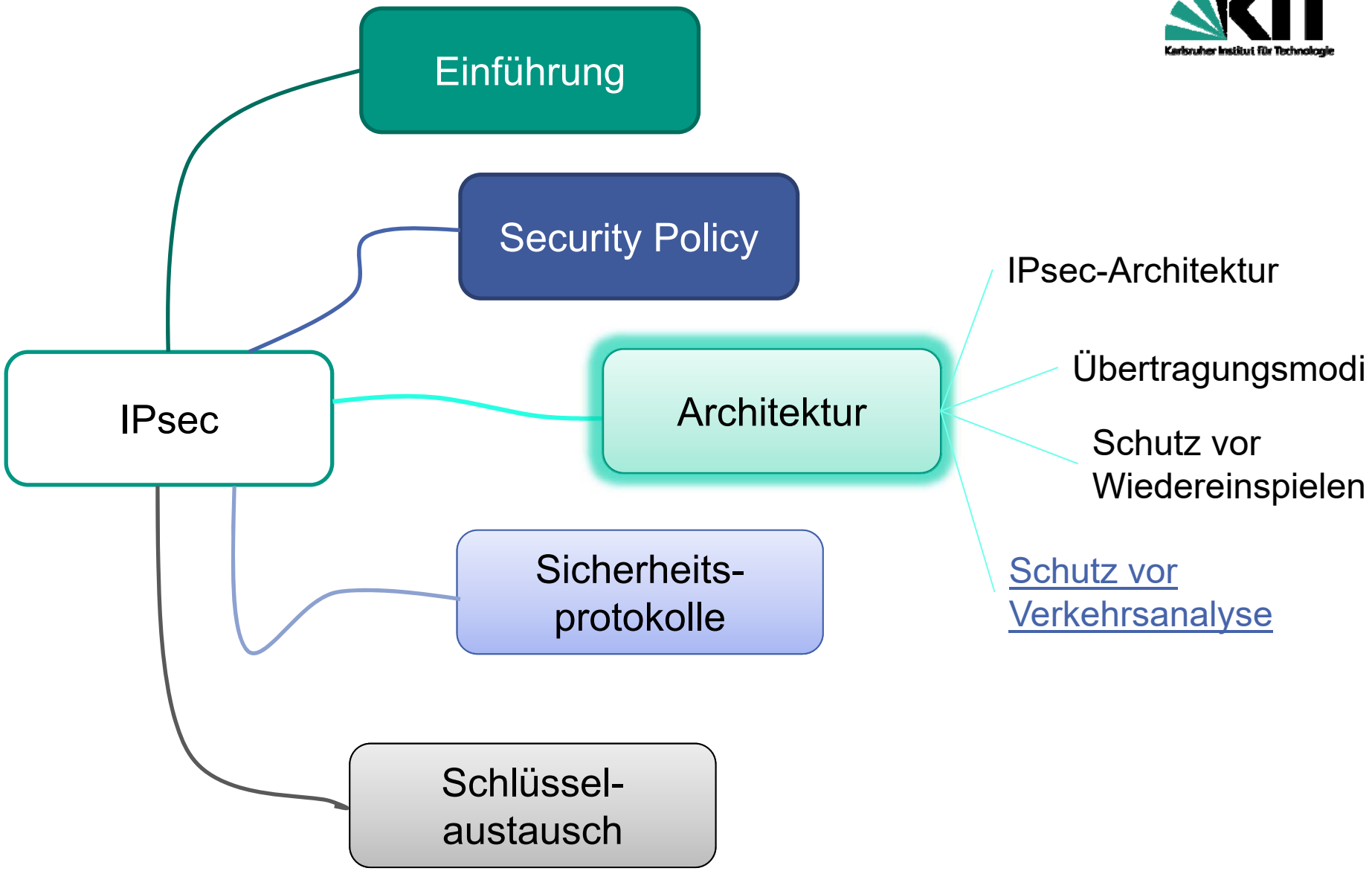
[Scha14]

Zur Sequenznummer

- IPsec-Paket hat 32-Bit-Sequenznummer
  - Reicht für etwa 4 Milliarden Pakete
  - Für schnelle Netze zu wenig
    - Datenrate = 10Gbit/s und Pakete von 1 KByte
    - → ca. 1 Millionen Pakete pro Sekunde
    - → Überlauf in ca. 1,12 Stunden

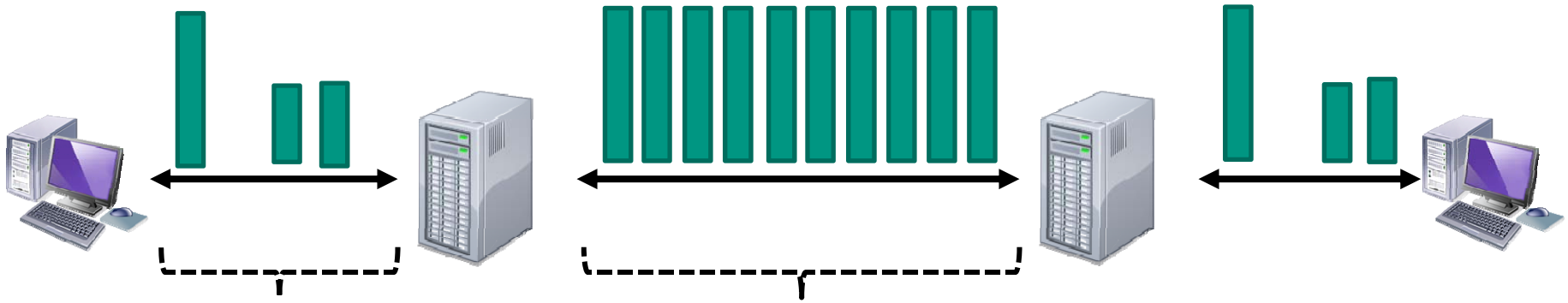


- Extended Sequence Number (ESN): 64 Bit
  - Für Abwärtskompatibilität können allerdings nur 32 Bit im Kopf stehen
  - Lösung
    - Untere 32 Bit der Sequenznummer werden übertragen
    - Obere 32 Bit der Sequenznummer nur in der SA geführt
    - Die kompletten 64 Bit werden bei Berechnung der Authentifizierungsdaten eingerechnet und somit in den Schutz aufgenommen


Einführung
Security Policy
IPsec
Architektur
IPsec-Architektur
Übertragungsmodi
Schutz vor Wiedereinspielen
Schutz vor Verkehrsanalyse
Sicherheits-protokolle
Schlüssel-austausch

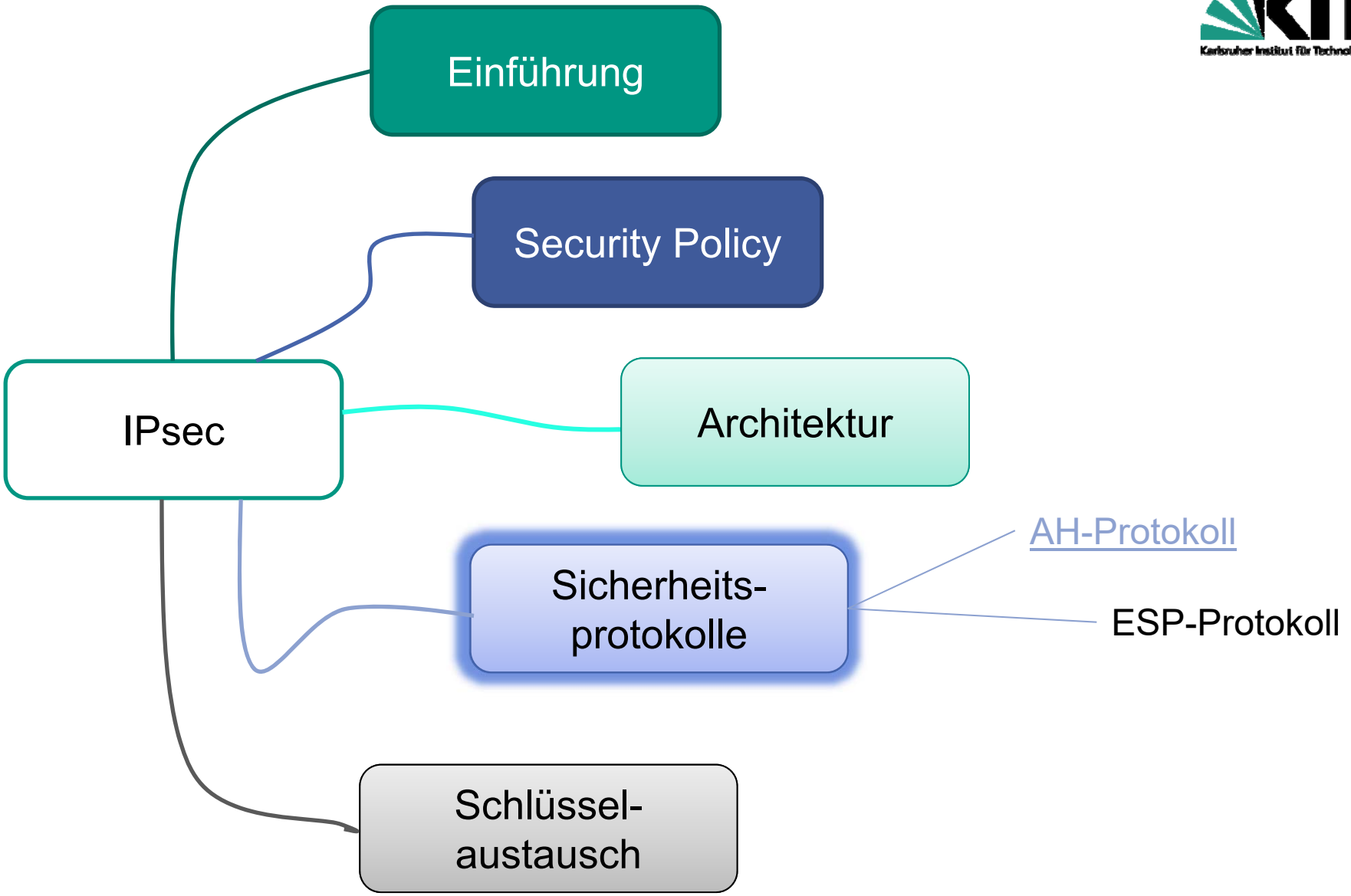
Schutz vor Verkehrsanalyse

- Idee: keine Informationen mittels Größe und Frequenz der Pakete verraten
  - Padding auf bis zu 64k Größe eines Pakets
  - Dummy-Pakete einfügen
    - Gekennzeichnet durch Protokollnummer 59
- Englische Bezeichnung: Traffic Flow Confidentiality



Pakete sind zufällig in Zeit und Größe

Pakete sind uniform in Zeit und Größe


Einführung
Security Policy
IPsec
Architektur
Sicherheits-
protokolle
AH-Protokoll
ESP-Protokoll
Schlüssel-
austausch

Sicherheitsprotokolle

- Authentication Header (AH)
  - Integrität
  - Authentizität
  - Zugangskontrolle
  - Schutz vor Wiedereinspielen

[RFC4302]

- Encapsulating Security Payload (ESP)
  - … wie oben, plus
  - Vertraulichkeit
  - Schutz vor Verkehrsanalyse

[RFC4303]

AH-Protokoll

- Hauptsächliches Ziel
  - Abwehr von Address-Spoofing-Angriffen

- Schutzziele
  - Integritätsschutz der übertragenen Daten
  - Authentizitätsschutz der übertragenen Daten
  - Schutz vor Wiedereinspielen

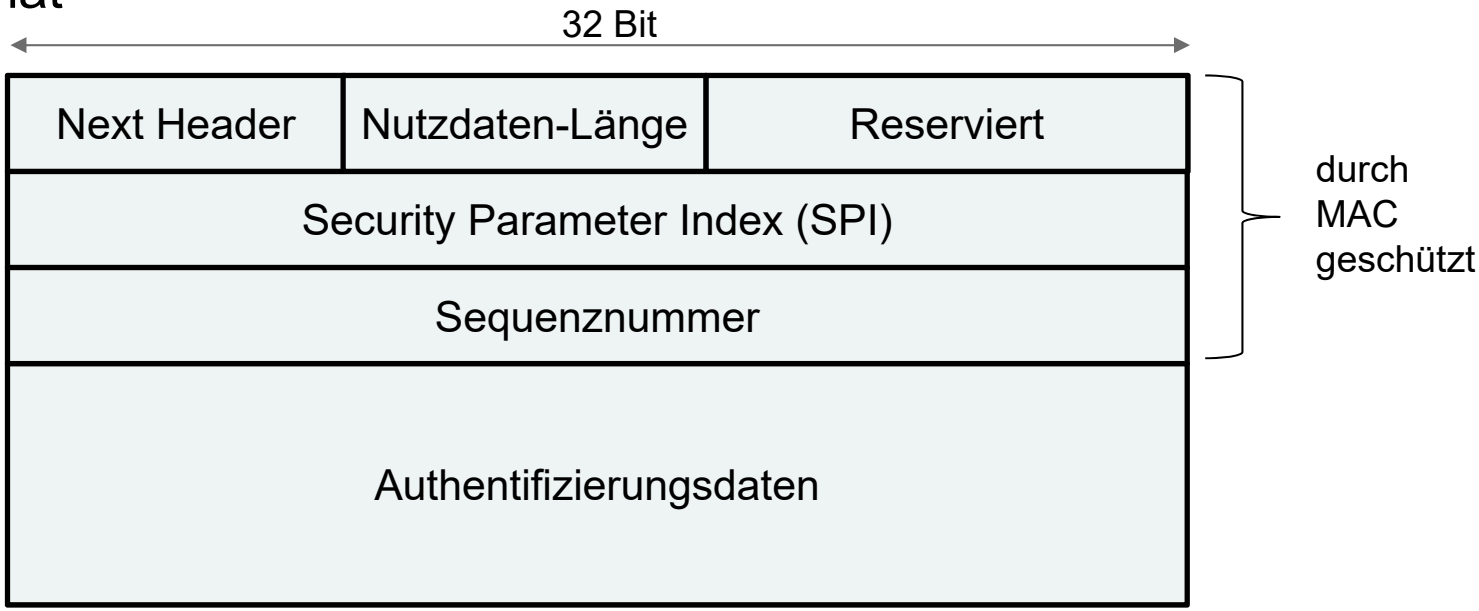
- Kryptographischer Baustein
  - Message Authentication Code (HMAC)

- Voraussetzung
  - Gemeinsamer geheimer Schlüssel

… seit IPsecv3 nur noch optional

Kopf eines AH-Pakets

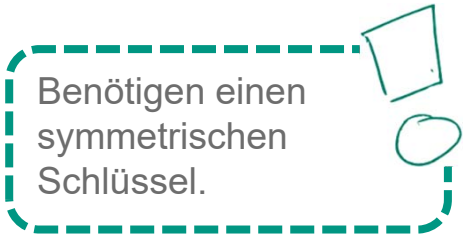
- Ziel
  - Transport der für die Bereitstellung der Schutzziele erforderlichen Information
- Format



- Anmerkung
  - Protokollnummer des AH-Protokolls: 51

Felder des AH-Kopfs

- Next Header
  - Übernimmt die Rolle des Protokollfelds im IP-Kopf
- Reserviert
  - Für zukünftige Nutzung reserviert. Hat den Wert Null
- Security Parameter Index (SPI)
  - Identifiziert im Ziel-Adresse Eintrag in SAD
    - … muss beim Einrichten der SA ausgetauscht werden
    - Dient der Zuordnung von Schlüsselmaterial und weiterem Zustand
- Sequenznummer
  - Sequenznummer für jede Dateneinheit erhöht
    - … wird bei Einrichten einer SA auf Null gesetzt
- Authentifizierungsdaten
  - Variable Länge
  - Mindestens anzubietende Verfahren
    - HMAC-MD5 und HMAC-SHA-1



MAC-Berechnung

- Berechnet über
  - Unveränderliche Felder im vorangehenden IP-Kopf
    - Veränderliche Felder werden auf Null gesetzt
  - AH Kopf
    - Mit Null initialisiert
  - Nutzdaten nach AH-Kopf
  - Die oberen 32 Bits der erweiterten Sequenznummer

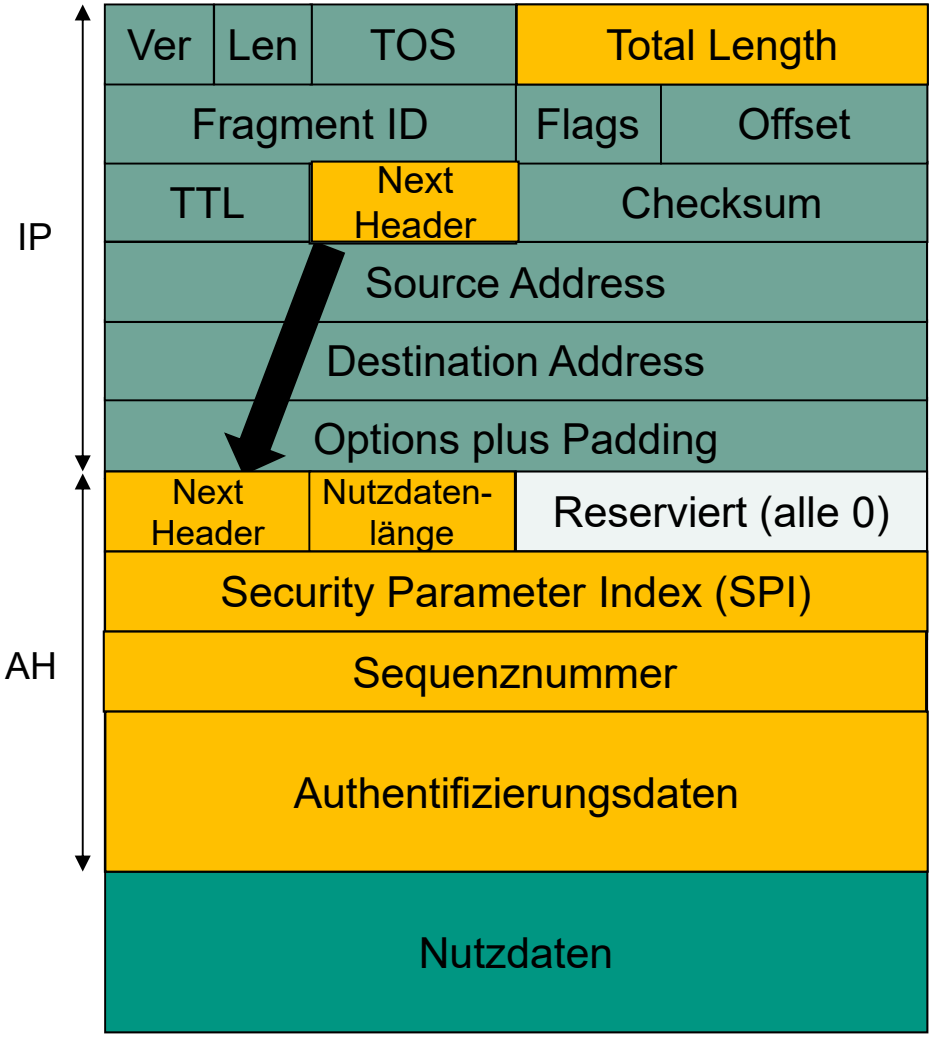
- Gegeben
  - K: geheimer Schlüssel zwischen Sender und Empfänger
  - m: zu sichernde Nachricht

$$HMAC(m) = H(K \oplus opad \mid H(K \oplus ipad \mid m))$$

- Zu beachten
  - Fragmentierung darf erst nach Berechnung der Authentifizierungsdaten erfolgen

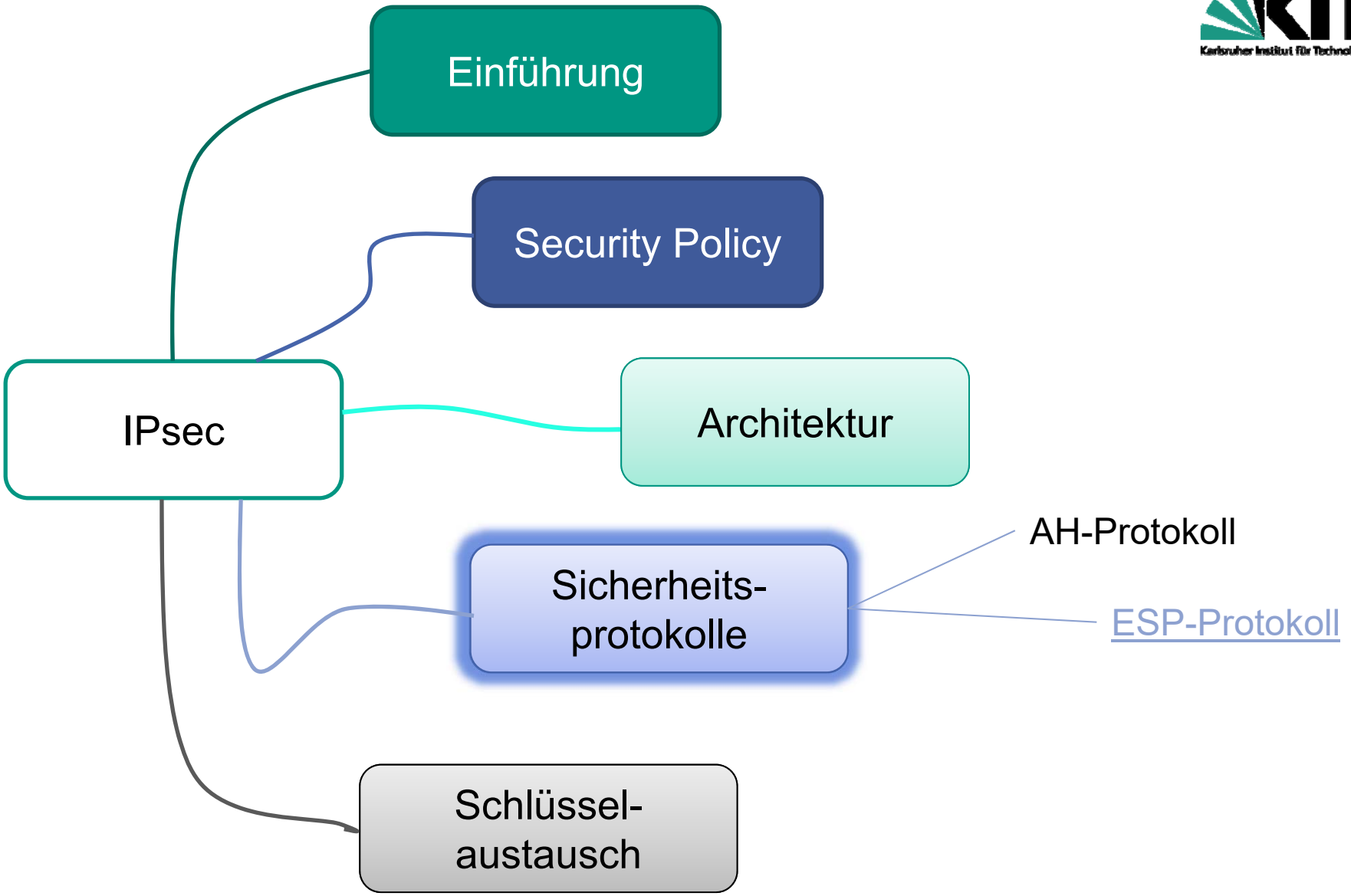
Erstellen des AH-Pakets

- IPv4-AH-Transport-Modus
  1. Einfügen des AH-Kopfs
  2. Setzen der Felder „Next Header“- und „Nutzdaten-Länge“
  3. Setzen des SPI für die gewählte SA
  4. Setzen der Sequenznummer
  5. Ändern des IP „Next Header“-Felds und der „Total Length“
  6. Berechnung der Authentifizierungs-Daten
  7. Fragmentieren, wenn nötig



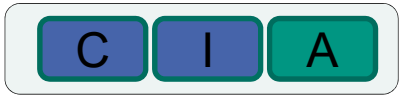
Überprüfen beim Empfänger

Ver	Len	TOS	Total Length
Fragment ID		Flags	Offset
TTL	51 (AH)	Checksum	
Source Address			
Destination Address			
Options plus Padding			
Next Header	Nutzdaten-länge	Reserviert (alle 0)	
Security Parameter Index (SPI)			
Sequenznummer			
Authentifizierungsdaten			
Nutzdaten			


Einführung
Security Policy
IPsec
Architektur
Sicherheits-
protokolle
AH-Protokoll
ESP-Protokoll
Schlüssel-
austausch

ESP-Protokoll

- Schutzziele
  - … wie AH, plus
  - Vertraulichkeit
  - Schutz vor Verkehrsanalyse



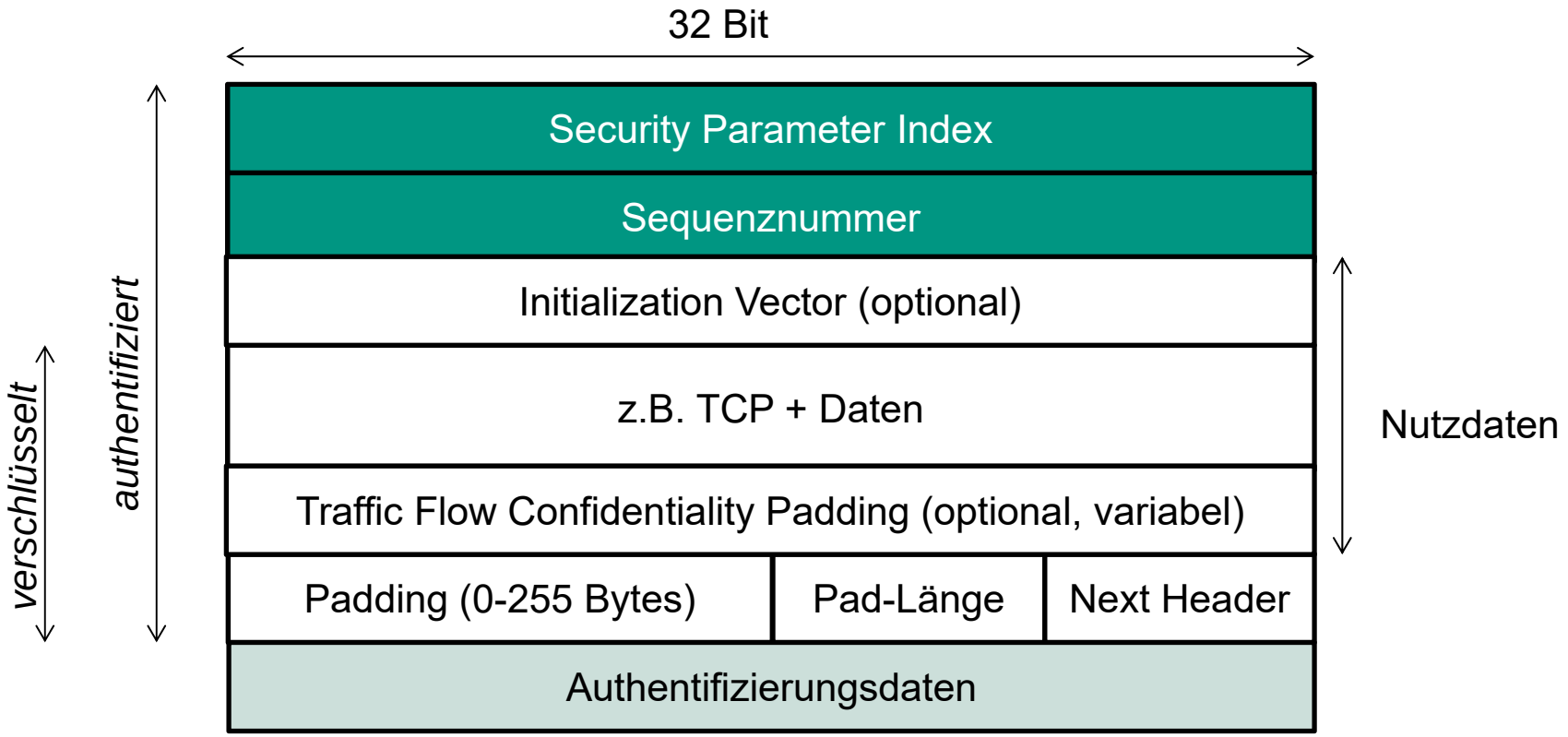
- Umgesetzte Menge an Schutzzielen abhängig von
  - Ausgewählten Optionen bei Etablierung der SA
  - Lokation der Implementierung (z.B. Endsystem, Gateway)

ESP-Protokoll

- Verwendung verschiedener kryptographischer Bausteine
  - Message Authentication Code
    - Mindestens HMAC-MD5 und HMAC-SHA-1
  - Verschlüsselungsverfahren
    - Mindestens Triple-DES im CBC-Modus, AES-CBC-128 und ESP-NULL
  - Kombinierte Verschlüsselung u. Authentifizierung
    - Z.B. GCM (Galois/Counter Mode)

- Voraussetzung
  - Gemeinsamer geheimer Schlüssel

Felder eines ESP-Pakets

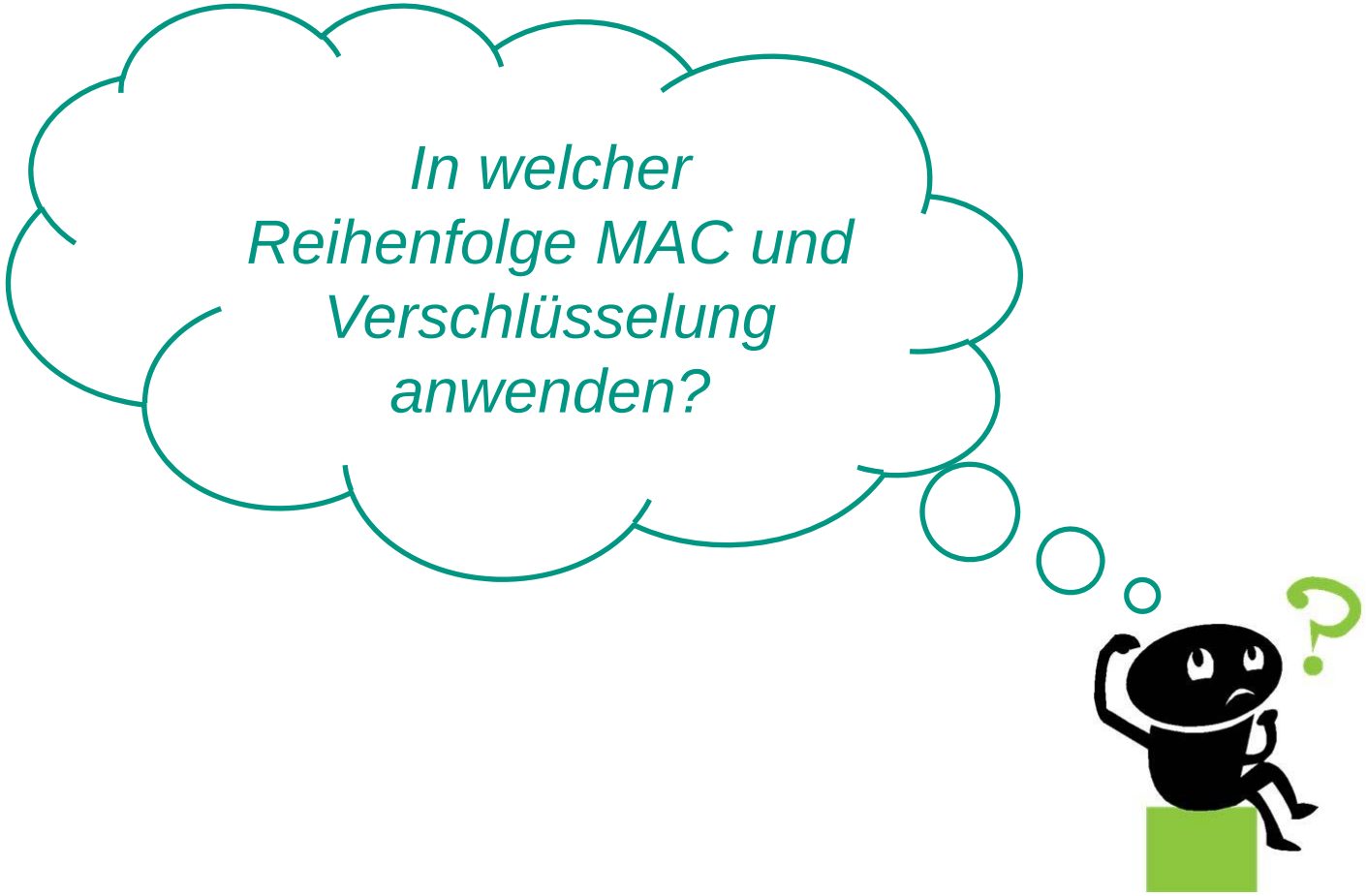


- Anmerkung
  - ESP-Protokollnummer: 50

Format eines ESP-Pakets

- ESP-Kopf
  - Security Parameter Index (SPI)
  - Sequenznummer
  - Initialisierungsvektor (IV)
    - In den Nutzdaten platziert
- ESP-Anhang
  - TFC-Padding
    - Im Tunnel-Modus möglich; in den Nutzdaten platziert
  - Padding
    - Ausrichten von Feldern (z.B. Pad-Länge und Next Header)
    - Blockgröße für Verschlüsselungsverfahren erreichen
  - Länge des Paddings
  - Next Header
- ESP-Auth
  - Authentifizierungsdaten

Entwurfsentscheidung



Alternative 1

- Erst verschlüsseln, dann authentifizieren (Encrypt-than-MAC, EtM)
  - Vorgehensweise beim Empfänger
    - Prüft zunächst die Authentizität
    - Entschlüsselt nur authentifizierte Pakete
    - Schnelles Verwerfen nicht-authentifizierter Pakete
    - Entschlüsselung und Authentifizierung kann parallel erfolgen
  - Vorteil: DoS-Angriff eingeschränkt
  - Beachten: Authentifizierungsdaten nicht verschlüsselt, deshalb keyed authentication algorithm erforderlich
  - Stand der Forschung: In Theorie EtM besser als MtE
- Trend: beides kombinieren

Alternative 2

- Erst authentifizieren, dann verschlüsseln (Mac-than-Encrypt, MtE)
  - Nachteil beim Empfänger: Teure Entschlüsselung immer erforderlich
  - Vorteil: MAC nicht direkt angreifbar, da verschlüsselt
  - Schneier, Ferguson: „Authentizität wichtiger als Vertraulichkeit“
  - Horton-Prinzip
    - „You should authenticate what you mean, not what you say“
      - Quelltext authentifizieren, nicht verschlüsselten Text

ESP im Transport-Modus

- Vorgehensweise
  - Quelle
    - Dateneinheit der höheren Schicht plus ESP-Anhang verschlüsseln
    - Resultierende verschlüsselte Information ersetzt ursprüngliche Daten
    - Authentifizierungsdaten anhängen, falls ausgewählt
  - Router
    - Greift nur auf IP-Kopf und Erweiterungsköpfe zu
  - Senke
    - Verarbeitung von IP-Kopf und Erweiterungsköpfen
    - Auswertung SPI … entschlüsseln

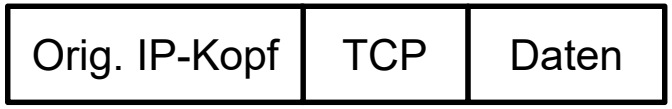
- Schutzziele
  - Schützt Verbindungen zwischen Endsystemen
  - Vertraulichkeit der Daten für alle darüber angesiedelten Protokolle
  - Aber: Verkehrsanalyse möglich
  - Felder im IP-Kopf *nicht* authentifiziert (Unterschied zu AH!)

ESP im Tunnel-Modus

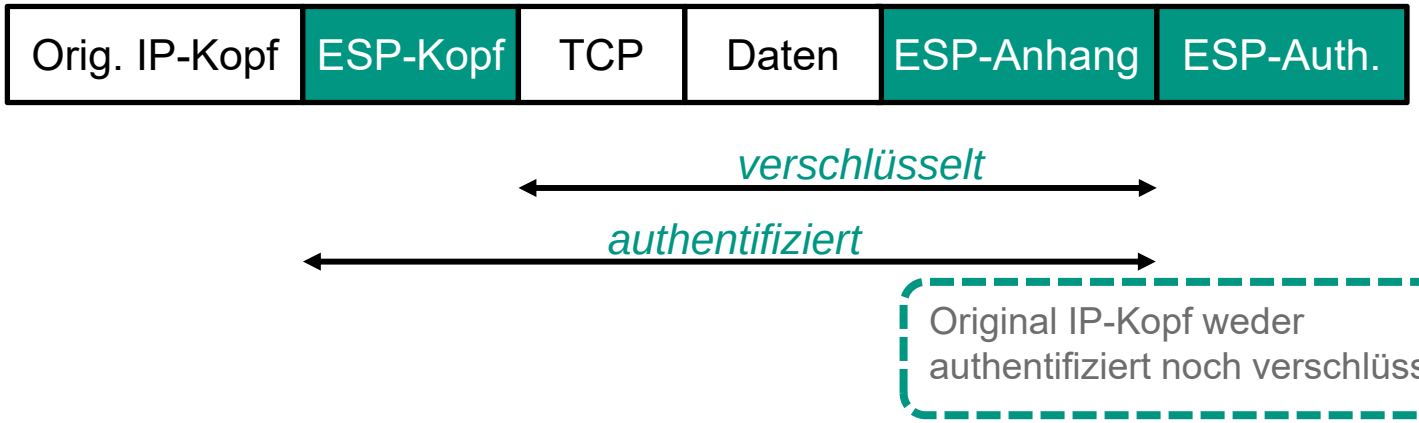
- Vorgehensweise
  - Quelle
    - ESP-Kopf wird vorangestellt
    - Verschlüsselung des Pakets (inkl. originalem IP-Kopf) und ESP-Anhang
    - Authentifizierungsdaten anhängen, falls ausgewählt
    - Neuen Kopf voranstellen, mit ausreichend Information für Routing
  - Router
    - Greift auf neuen Kopf zu, auch Hop-by-Hop Optionen etc.
  - Senke
    - Verarbeitung von IP-Kopf und Erweiterungsköpfen
    - Auswertung SPI … entschlüsseln
- Schutzziele
  - Schützt Netzwerk vor externen Netzen
    - Verschlüsselung nur zwischen
      - Externem Endsystem und Sicherheits-Gateway
      - Sicherheits-Gateways
  - Verkehrsanalyse wird eingeschränkt

ESP-Paket bei IPv4

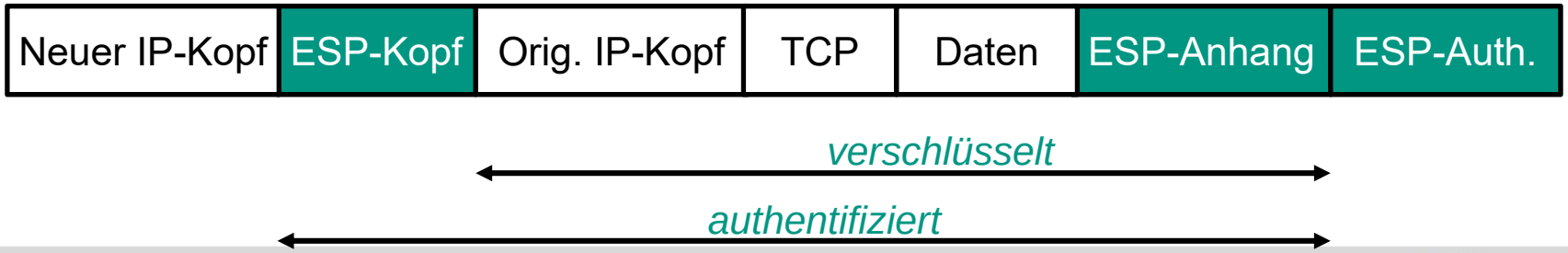
- IPv4-Paket



- ESP im Transport-Modus



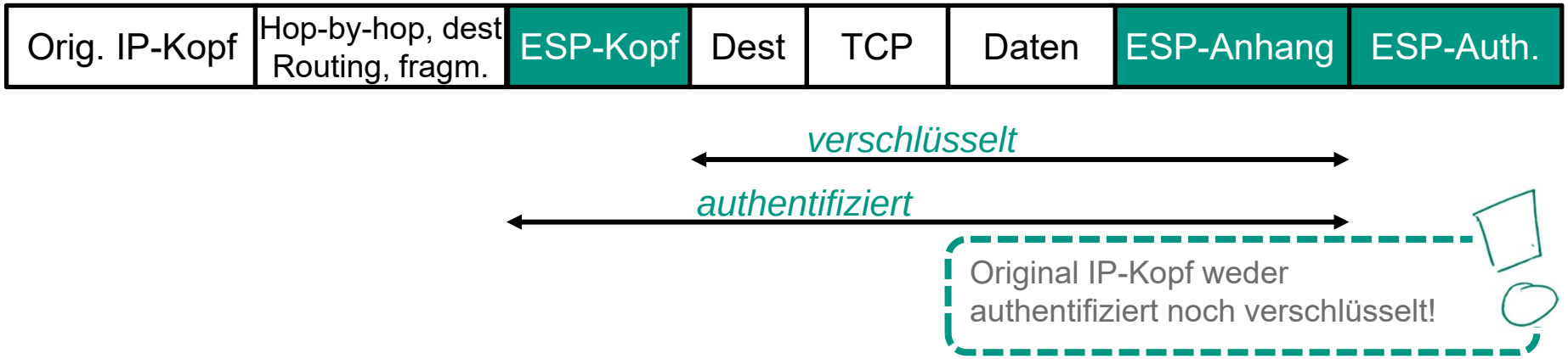
- ESP im Tunnel-Modus



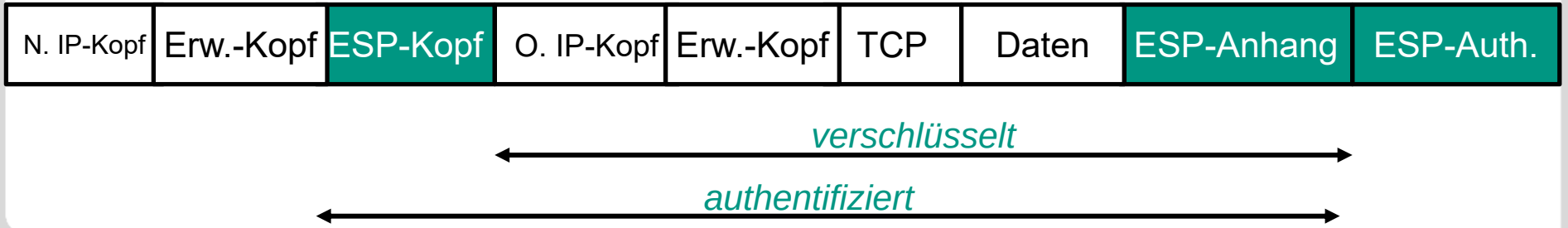
ESP-Paket bei IPv6

- IPv6-Paket

- ESP im Transport-Modus



- ESP im Tunnel-Modus



Viele Detailprobleme, u.a.

- IPsec und NAT
  - UDP-Einkapselung: Kapselung von IKE und IPsec in UDP
    - UDP-Port 4500
  - AH authentifiziert IP-Kopf
    - Änderungen am äußeren IP-Kopf machen Paket ungültig
    - IPsec muss Änderungen vorher in die Authentifizierungsdaten einberechnen
      - IKEv2 kann mittels NAT-Traversal die notwendigen Daten bestimmen

[RFC3948]

- IPsec und Firewalls
  - häufiger Firewall Selektor: Portnummer
    - bei ESP ist jedoch die Schicht-4 Portnummer verschlüsselt

Viele Detailprobleme, u.a.

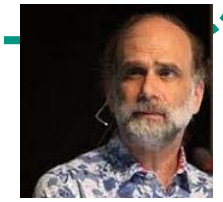
- Einträge in SDP
  - Wechselwirkungen und Zusammenhänge verteilter Systeme müssen verstanden werden
  - Konfigurationsfehler einfach
    - Zwischen Maschine A und B: ESP, Transportmodus ohne Authentifikationsanteil, keine zusätzliche Absicherung mittels Tunnel-Modus
      - Spoofing-Angriffe möglich
      - Unautorisierte Modifikation möglich
      - → Gilt dann für alle Anwendungen die darüber laufen

Viele Detailprobleme, u.a.

- IPsec-Köpfe vergrößern Paket
  - Ggfs. Fragmentierung notwendig
  - MTU-Wert des Pfads muss bestimmt werden!
    - Wer tut dies? Sicherheit?
  - Zuerst fragmentieren oder zuerst IPsec?
    - Erster Fall: Kenntnis der Pfad-MTU notwendig
    - Zweiter Fall: DoS möglich

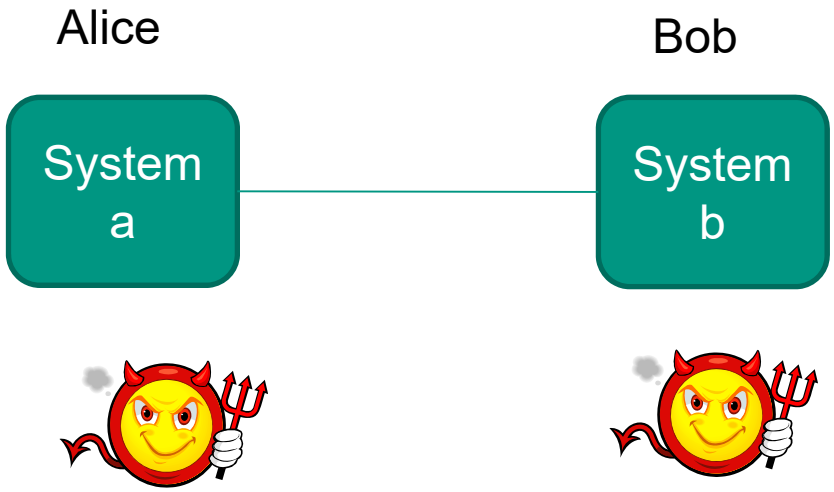
Wichtiger Kritikpunkt: **Komplexität**!
Erschwert korrekte Implementierung.
Außerdem: schlechte Dokumentation erschwert Nachvollziehen von Entwurfsentscheidungen.
Und: Auf AH und Transportmodus kann man im Prinzip komplett verzichten.

„IPsec was a great dissapointment to us. Given the quality of the people that worked on it and the time that was spent on it, we expected a much better result.“
Ferguson, Schneier, 1999



Cut-and-Paste-Angriff

- Situation
  - ESP, hostbasierte Verschlüsselung, keine Integritätssicherung
  - Autorisierte Nutzer Alice und Bob
  - Mallory hat Zugang zu Sa (oder Sb)



Cut-and-Paste-Angriff

- Ablauf

1. Alice sendet Nachricht X zu Bob: vertraulich, TCP

2. M hört Nachricht X ab und zeichnet sie auf
3. M verschickt UPD-Paket von Sa an sich selbst
   - Mit den gleichen Schlüssel verschlüsselt wie in (1)

4. M ersetzt seine verschlüsselten Daten durch die von Alice (Cut-and-Paste), schickt Paket direkt an Sb mit sich als Empfänger

5. Sa entschlüsselt Paket

Cut-and-Paste-Angriff

- Konsequenzen
  - ESP-Protokoll mit Authentifikation kombinieren
  - Möglichst auf hostbasierte Schlüsselvergabe verzichten

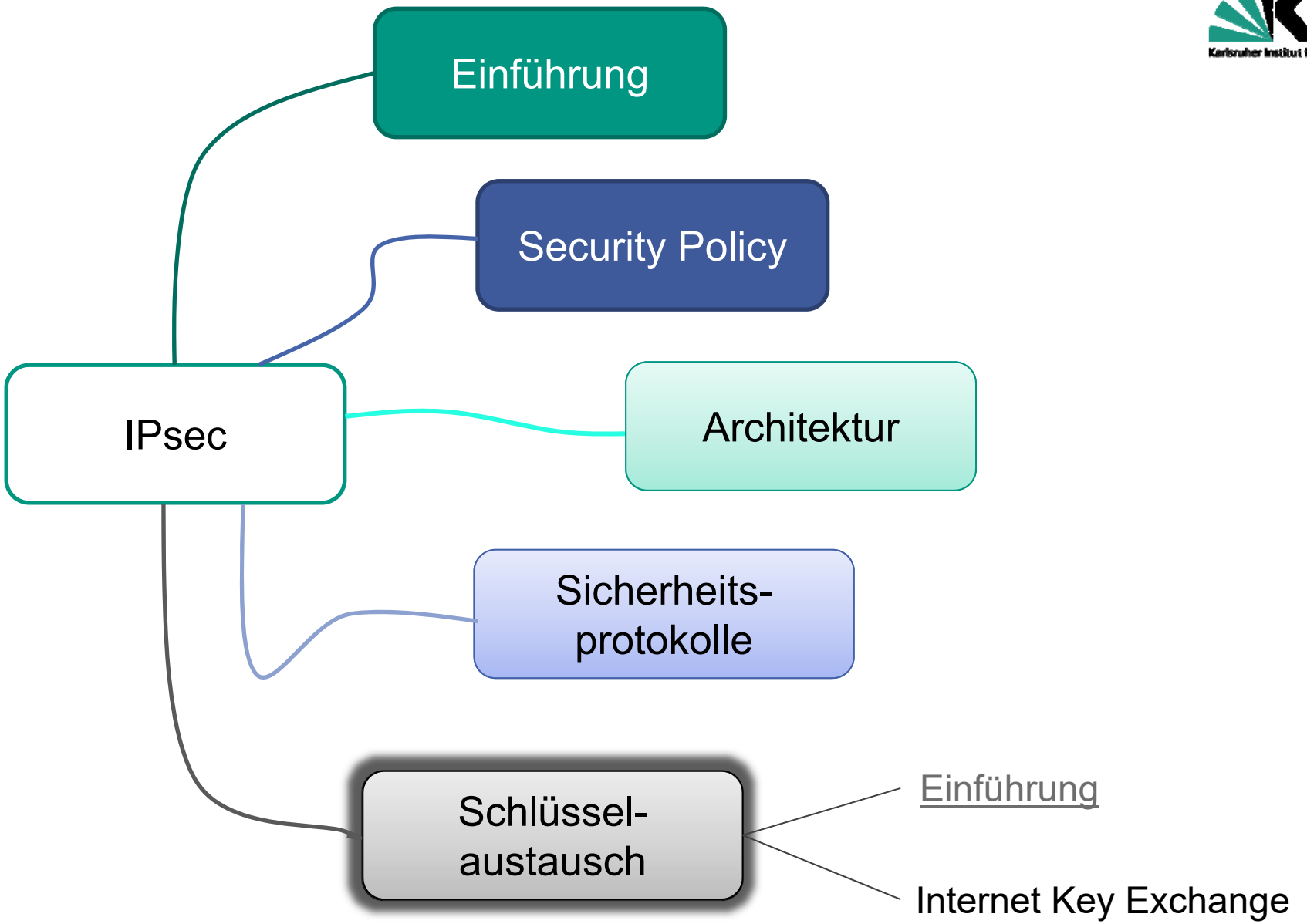
Session Hijacking

- Ähnlich wie Cut-and-Paste

1. Mallory fängt Nachricht von Alice an Bob ab

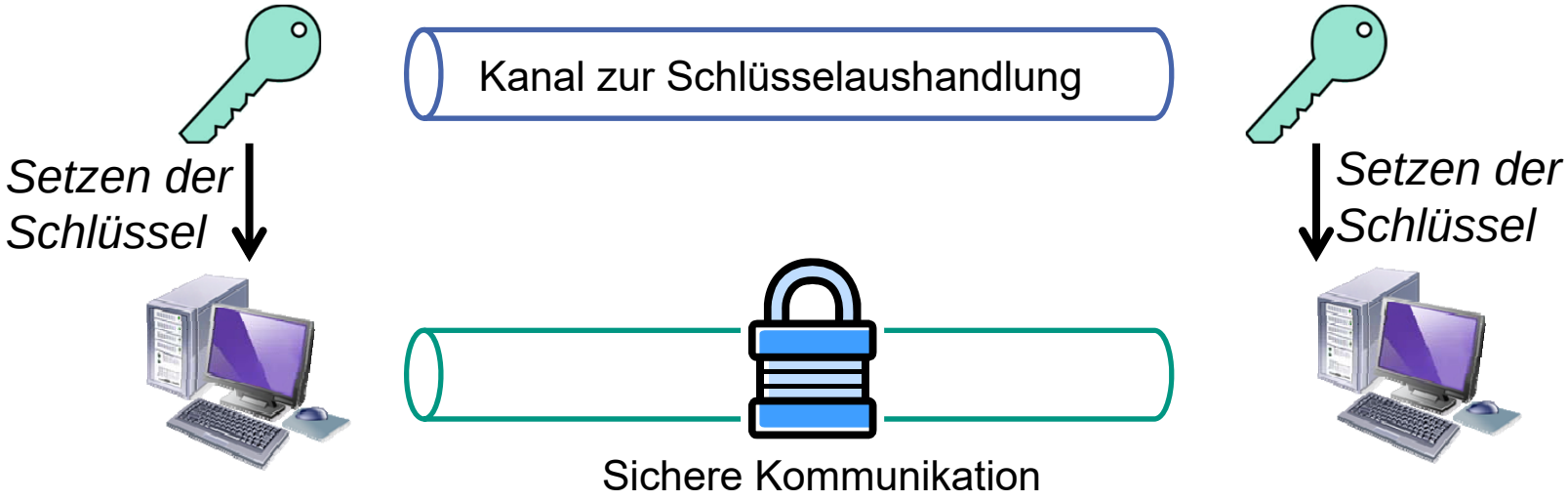
2. Paket von Mallory über Sa und Sb and Mallory

3. Modifizierte Nachricht zu Bob


Einführung
Security Policy
IPsec
Architektur
Sicherheits-
protokolle
Schlüssel-
austausch
Einführung
Internet Key Exchange

Einführung

- Erinnerung Entwurfsentscheidung
  - Entkopplung von Schlüsselaustausch und Sicherung



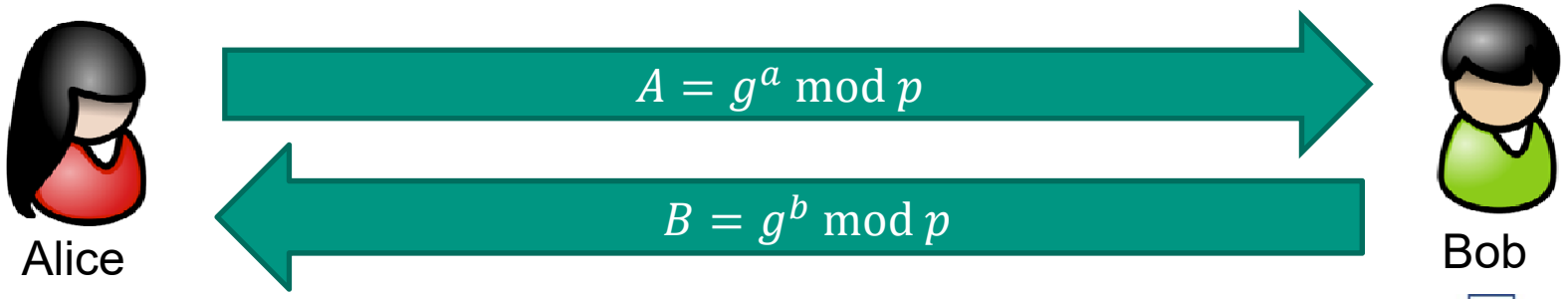
- Schlüsselaustausch-Protokoll erforderlich
  - Authentifizierung des Kommunikationspartners
  - Aushandlung der Austausch-/Sicherungsverfahren für den Kanal
  - Erzeugung gemeinsamer Schlüssel

Wie Schlüssel austauschen?

Wie Schlüssel sicher über ungesicherten Kanal austauschen? Manuell oder über Protokoll?

Schon bekannt: Diffie-Hellman-Austausch

- Vorbereitung
  - Alice und Bob einigen sich auf eine große Primzahl p
  - Beide wählen gemeinsam Element g nach best. Rechenvorschrift
  - → p und g sind *öffentlich* bekannt
- Schlüsselaustausch
  - Alice wählt Zufallszahl a mit $2 \leq a \leq p-2$ und berechnet
    - $\boldsymbol{A = g^a \bmod p}$ *… öffentlicher Schlüssel von Alice*
  - Bob wählt Zufallszahl b mit $2 \leq b \leq p-2$ und berechnet
    - $\boldsymbol{B = g^b \bmod p}$ *… öffentlicher Schlüssel von Bob*
  - → a und b werden *nicht* bekannt gegeben



[DiHe76]

Schon bekannt: Diffie-Hellman-Austausch

- Berechnung des gemeinsamen geheimen Schlüssels K
  - Alice und Bob berechnen jeweils
    - Alice: $K = B^a \bmod p = \left(g^b\right)^a \bmod p = g^{ab} \bmod p$
    - Bob: $K = A^b \bmod p = (g^a)^b \bmod p = g^{ab} \bmod p$

→ *Alice und Bob sind nun im Besitz eines gemeinsamen geheimen Schlüssels K*

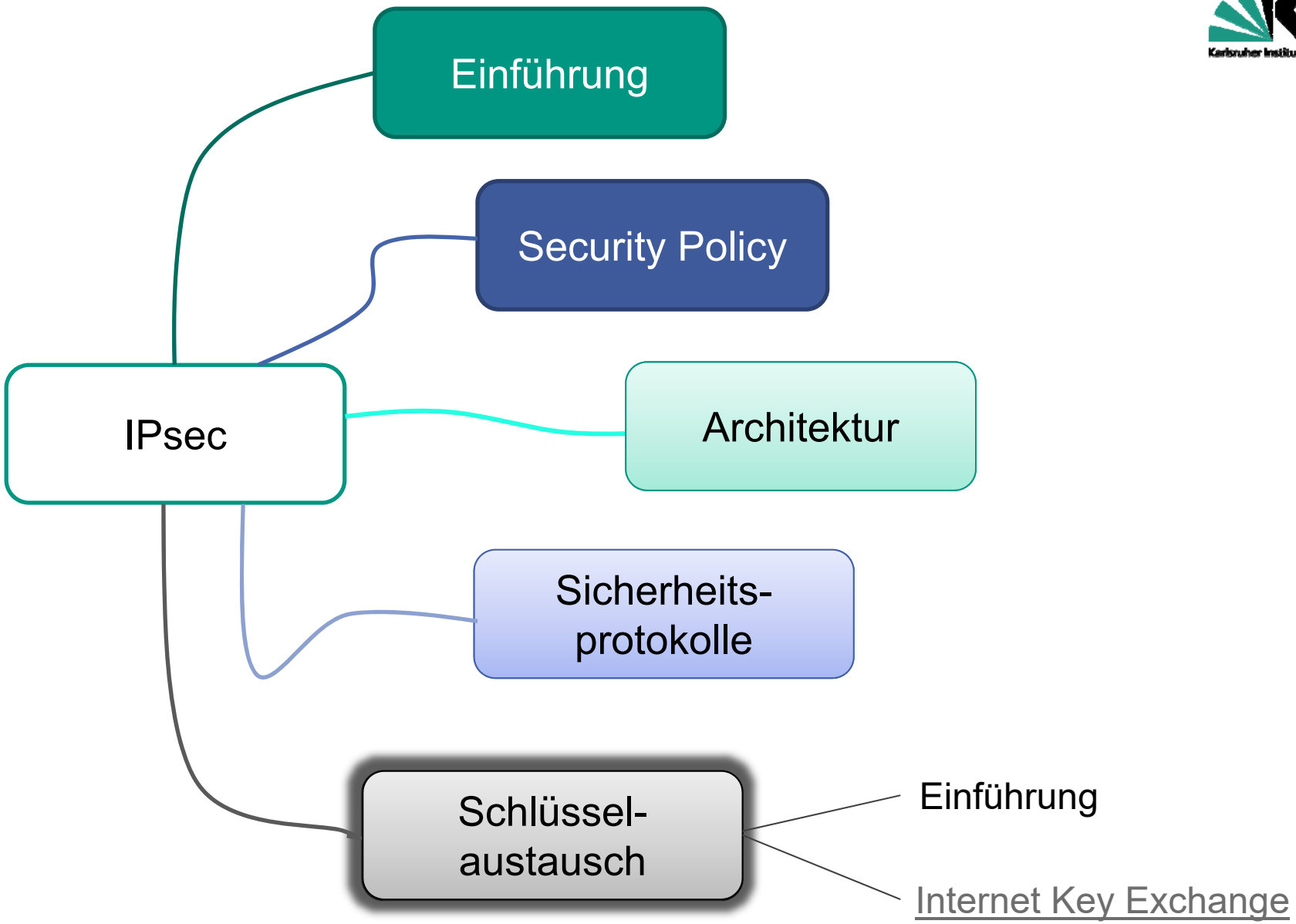
… gemeinsamer geheimer Schlüssel wird nicht über Kanal gesendet!

- K stellt Sitzungsschlüssel dar

Diffie-Hellman-Austausch

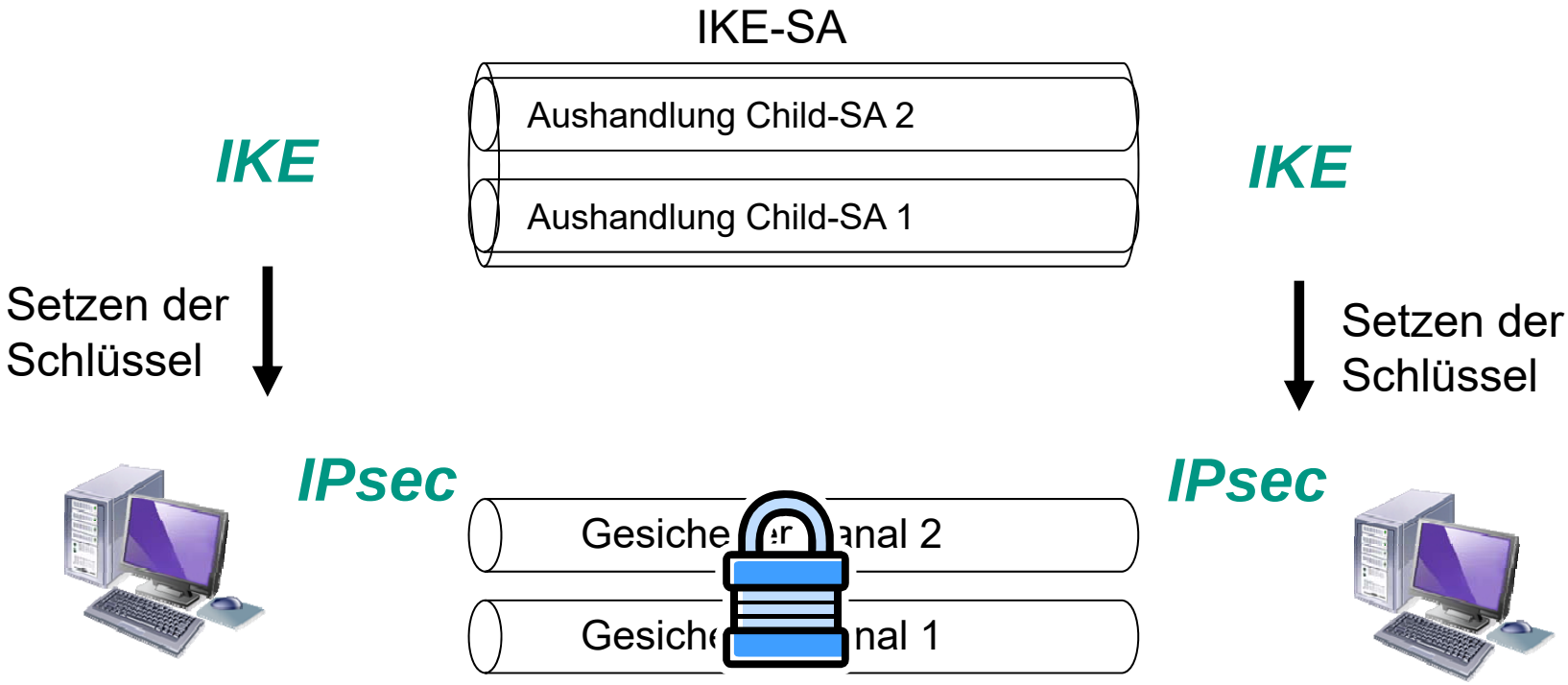
- Vorteile
  - Gemeinsame Geheimnisse werden nur erzeugt wenn benötigt
  - Keine Infrastrukturunterstützung erforderlich
    - Lediglich Diffie-Hellmann-Gruppe muss bekannt sein
  - Geheime Zufallszahlen werden am Ende der Kommunikation gelöscht

- Nachteile
  - Anonymer Schlüsselaustausch
    - keine Authentifizierung der Kommunikationspartner
  - Man-in-the-Middle-Angriff möglich
  - Rechenintensiv
    - also anfällig gegen DoS-Angriffe


Einführung
Security Policy
IPsec
Architektur
Sicherheits-
protokolle
Schlüssel-
austausch
Einführung
Internet Key Exchange

Internet Key Exchange (IKE)

- Ziel
  - Sichere Aushandlung von IPsec-Parametern
- Hier betrachtet
  - IKEv2



Internet Key Exchange

- Aufbau eines gesicherten Kanals (IKE-SA)
  - Definition von Formaten der Pakete
  - Gegenseitige Authentifizierung
  - Diffie-Hellman-Austausch zum Erzeugen eines gemeinsamen Geheimnisses

- Aushandlung des IPsec-Schlüsselmaterials pro SA
  - Wahl der zu verwendenden Verfahren
  - Generierung der Schlüssel

Initialer Austausch

(1) Aufbau der IKE-SA

- Austausch von
  - Kryptographischen Algorithmen und Sicherheitsparametern
  - Nonce
  - DH-Werten (g^a, g^b)

→ Alle nachfolgenden Nachrichten-Austausche erfolgen über IKE-SA

- Sind geschützt durch
  - Verschlüsselung und
  - Daten-Authentifizierung

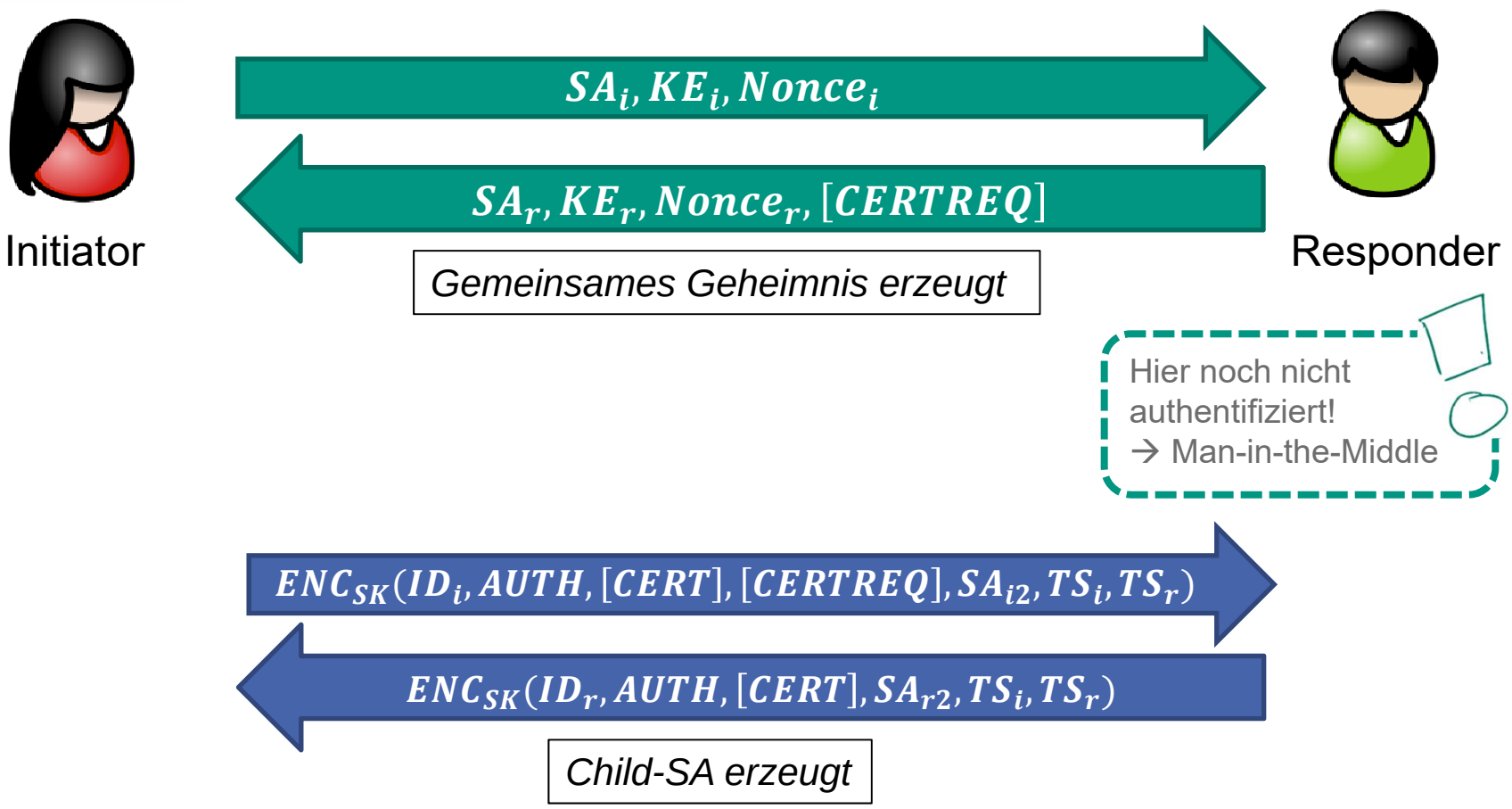
Initialer Austausch

(2) Authentifizierung der Kommunikationspartner, Aufbau erste Child-SA

- Authentifizierung IKE SA
  - Überprüfung der Identitäten
  - Integritätsprüfung des DH-Austausches
- Aushandlung Child-SA
  - Auswahl von Algorithmen
  - Austausch von Traffic-Selektoren
    - Beschreiben den zu schützenden Verkehr
      - z.B: TCP / IP1:Port1 → IP2:Port2
      - z.B: UDP / IP-Range:* → IP-Range:*
  - Austausch von Zertifikaten

→ Eintrag in SAD; Nutzung für IPsec-Verkehr

Initialer Austausch



Initialer Austausch

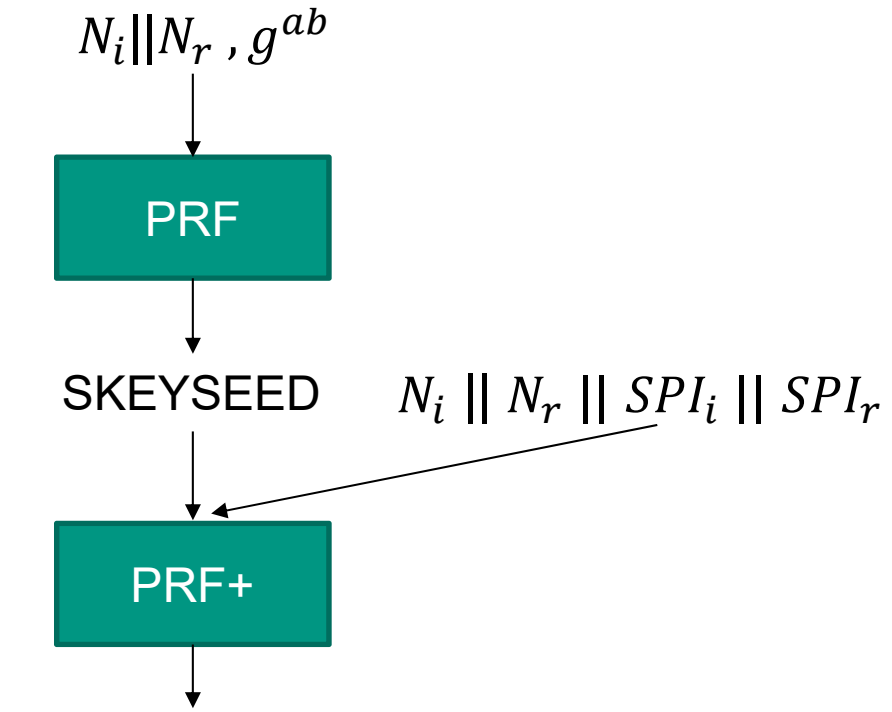
- Erläuterung der Nachrichtenfelder der ersten beiden Nachrichten
  - SA_i: Unterstütze Algorithmen für IKE-SA, DH-Gruppe,
  - SA_r: Ausgewählte Algorithmen für IKE-SA
  - KE_i und KE_r: Diffie-Hellman-Werte des Initiators bzw. Responders
  - $Nonce_i$ und $Nonce_r$: Zufallszahlen des Initiators bzw. Responders
  - CERTREQ: Optionale Anforderung eines Zertifikats

Initialer Austausch

- Schlüsselerzeugung mittels DH-Verfahren unter Verwendung der beiden Nonces
  - SK: Seeded Key, Seed wird aus Nonces berechnet
- Es werden *unterschiedliche* Schlüssel für Verschlüsselung und zur Integritätssicherung pro Kommunikationsrichtung erzeugt
  - Insgesamt sieben Schlüssel
    - Zwei (Initiator, Responder) für Verschlüsselung
    - Zwei (Initiator, Responder) für Berechnung Nachrichtenauthentisierungswerte
    - Zwei (Initiator, Responder) für Authentisierung beim initialen IKE-Austausch
    - Einer zur Ableitung von Schlüsselmaterial für die „eigentlichen“ SAs

Initialer Austausch

- Schlüsselerzeugung



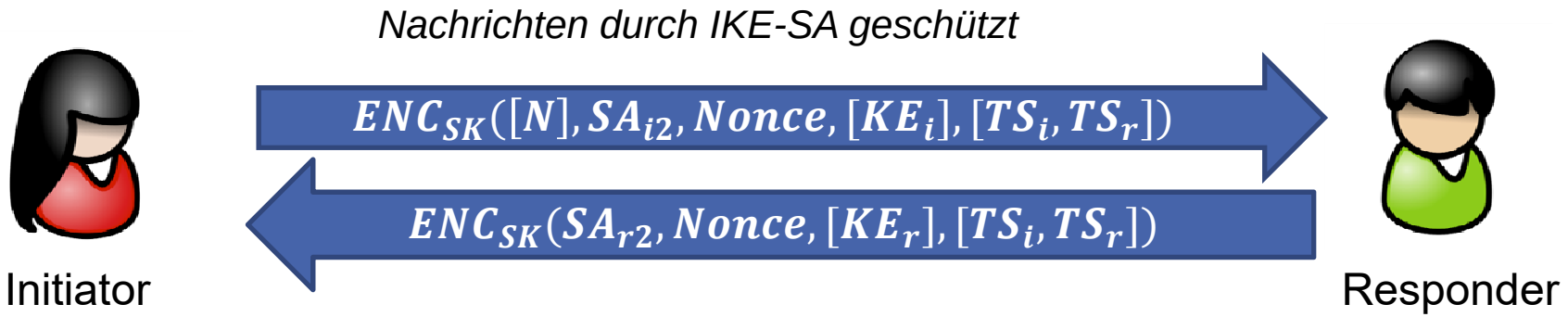
T1 = PRF(K, S || 1)
T2 = PRF(K, T1 || S || 2)
T3 = PRF(K, T2 || S || 3)
…

Initialer Austausch

- Erläuterung der Nachrichtenfelder der Nachrichten 3 und 4
  - ID_i und ID_r : Identifikator des Initiators bzw. Responders
  - $AUTH$: Authentifizierungsdatenstruktur
    - Authentifizierung der Kommunikationsteilnehmer aufgrund eines gemeinsamen symmetrischen Geheimnisses oder mit Hilfe von Public-Key Kryptografie bzw. Zertifikaten
    - Berechnet über Nachricht 1 bzw. 2 um Downgrade-Angriffe zu erkennen, z.B. signierter Hash über ausgetauschte Nachrichten

- Authentifizierung abgeschlossen, ab jetzt Aushandlung der Child-SAs
  - $CERT$ und $CERTREQ$: Optional falls Authentifizierung mit Zertifikaten durchgeführt werden soll
  - SA_{i2} und SA_{r2}: Vorgeschlagene bzw. ausgewählte Algorithmen
  - TS_i und TS_r : Traffic-Selektoren

Aufbau einer (weiteren) Child-SA



- Aushandlung der Child-SA
  - Hier wieder Vorschläge und Auswahl
  - Traffic-Selektoren, falls neue SA
    - Bei Rekeying nicht notwendig

- N: Notify (Benachrichtigungs-Payload)

Initialer Austausch und DoS

Initiator

(1) $SA_i, KE_i, Nonce_i$

$N\ (Cookie)$

(2) *Responder vermutet DoS Angriff und/oder Spoofing*

Responder

(3) $N(Cookie), SA_i, KE_i, Nonce_i$

Kryptografische Berechnungen bei Responder ab jetzt

$SA_r, KE_r, Nonce_r, [CERTREQ]$

Gemeinsames Geheimnis erzeugt

$ENC_{SK}(ID_i, AUTH, [CERT], [CERTREQ], SA_{i2}, TS_i, TS_r)$

$ENC_{SK}(ID_r, AUTH, [CERT], SA_{r2}, TS_i, TS_r)$

Initialer Austausch und DoS

- Ziel: DoS-Angriff erschweren
- Maßnahme: Verwendung von Cookies

- Ablauf
  - Nachricht 1 wie bisher
  - Falls Responder DoS-Angriff vermutet
    - Nachricht 2: Notify (N) mit Cookie
      - Cookie: 1–64 Oktette lang, von Responder beliebig wählbar (siehe nächste Folie)
    - Nachricht 3: Initiator muss mit Cookie antworten
  - weiter: wie bisher

- Ergebnis
  - Kryptografische Berechnung erst nach Nachricht 3, eine Nachricht reicht nicht mehr um Aufwand beim Responder zu erzeugen
  - Zustand muss erst nach Nachricht 3 gehalten werden
  - Spoofing ist nicht mehr möglich

Initialer Austausch und DoS

- Erzeugen des Cookies, Vorschlag nach IKEv2
  - $Cookie = < ID > \mid Hash(Nonce_i \mid IP_i \mid SPI_i \mid < secret >)$
- Tabelle von Geheimnissen

ID	Secret
1057	4711
1058	1234
1059	3344

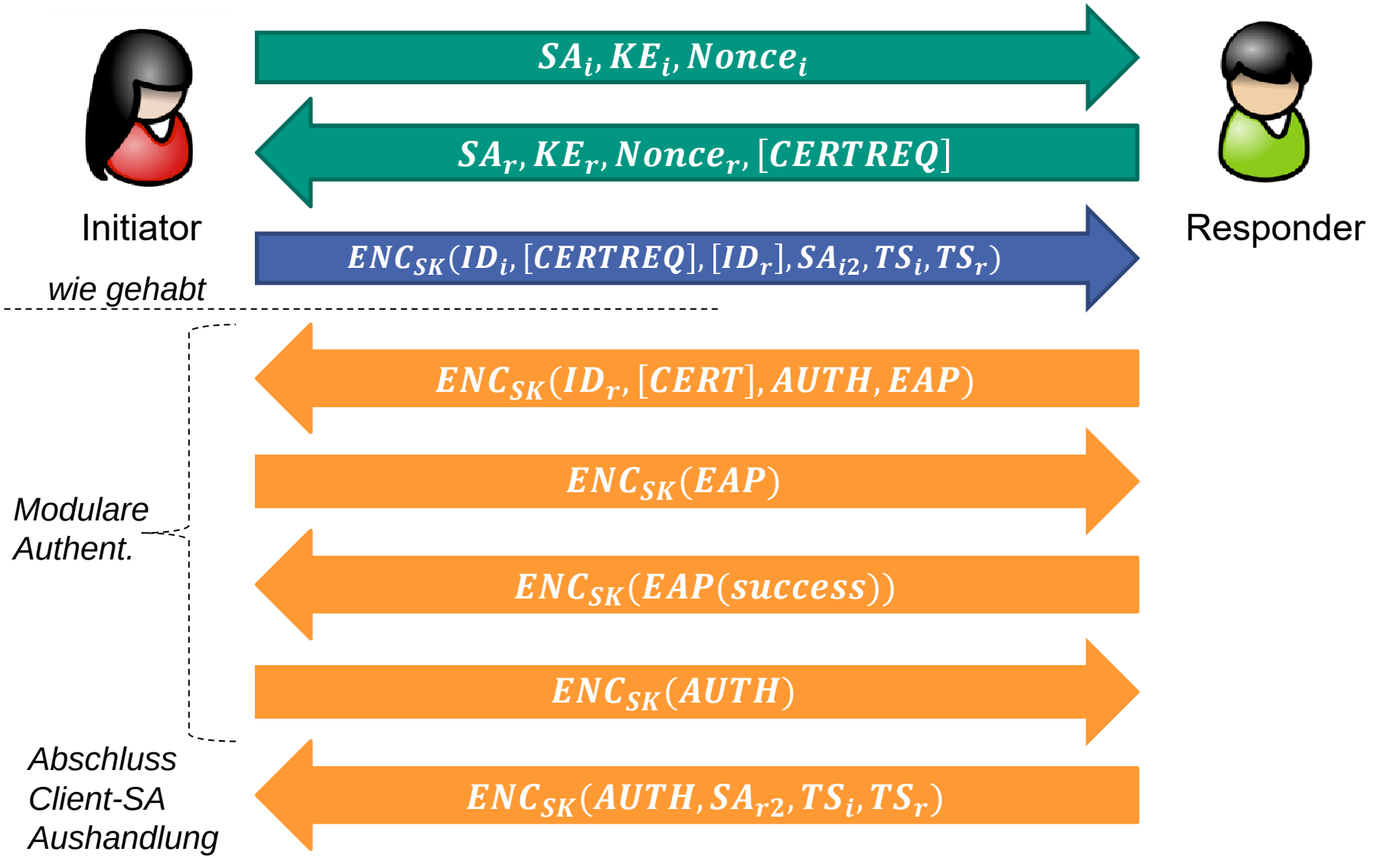
- Vorteile
  - Ändern des Geheimnisses während Angriff möglich

Initialer Austausch und EAP

- Extensible Authentication Protocol (EAP)
  - Sehr verbreitetes Verfahren für modulare Authentifizierung
  - Unterstützt z.B. passwortbasierte, zertifikatsbasierte und SIM-basierte Authentifizierung
- Motivation
  - Authentication „Plug-and-Play“ für IKEv2

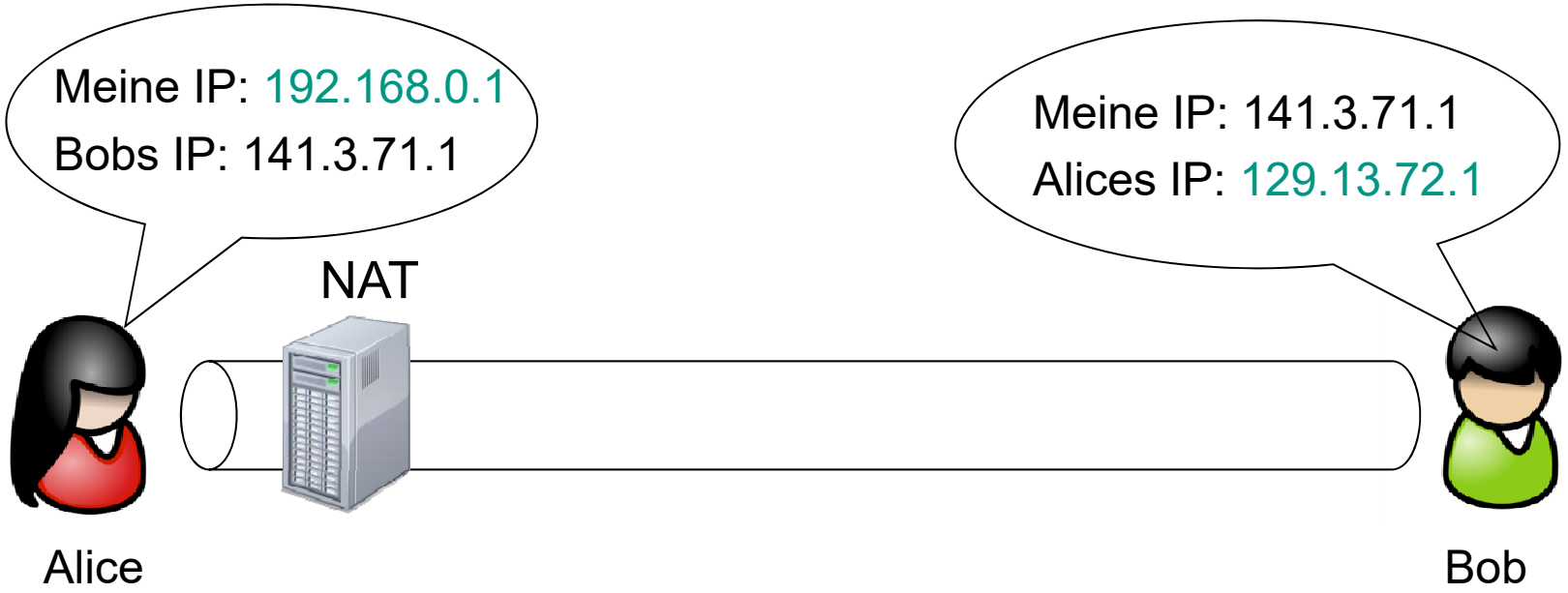
[s. Kapitel Authentifizierung]

Initialer Austausch und EAP



NAT-Traversal

- Network Address Translation (NAT) ändert IP-Adressen/Ports



- Lösung
  - IKEv2 transportiert mittels Notify-Payload den Hash der Adressen (SPI, IP, Port) für beide Seiten (Initiator und Responder)
  - Daraufhin kann Gegenseite NATs erkennen

Sitzungswiederaufnahme

- Problem
  - Sitzungsabbruch
- Szenario: VPN Gateway
  - Potentiell große Zahl verbundener Clients
  - Temporärer Fehler des Gateways oder des Clients

Welche Probleme sehen Sie voraus? Welche Anforderungen stellen Sie?

Sitzungswiederaufnahme

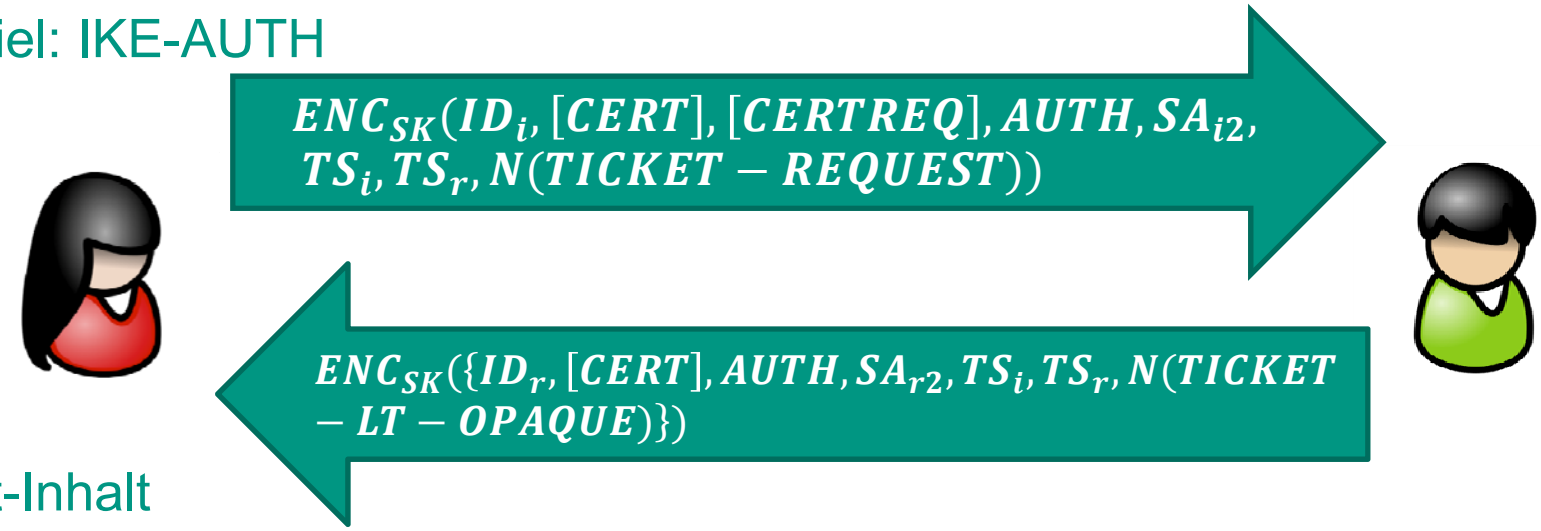
- Ziele
  - Symmetrische Kryptographie um CPU zu schonen
  - Keine negativen Auswirkungen auf die Sicherheit
  - Unterstützung für Cryptographic Agility

- Explizit keine Ziele waren
  - Failover auf Backup Gateway
  - Load Balancing
  - Spezifikation wie Clients erkennen können, dass die Sitzung wieder aufgenommen werden muss

[RFC5723]

Tickets zur Zustandsspeicherung

- Ticket-Anforderung während
  - IKE_AUTH oder Rekeying oder Informational Exchange
- Beispiel: IKE-AUTH

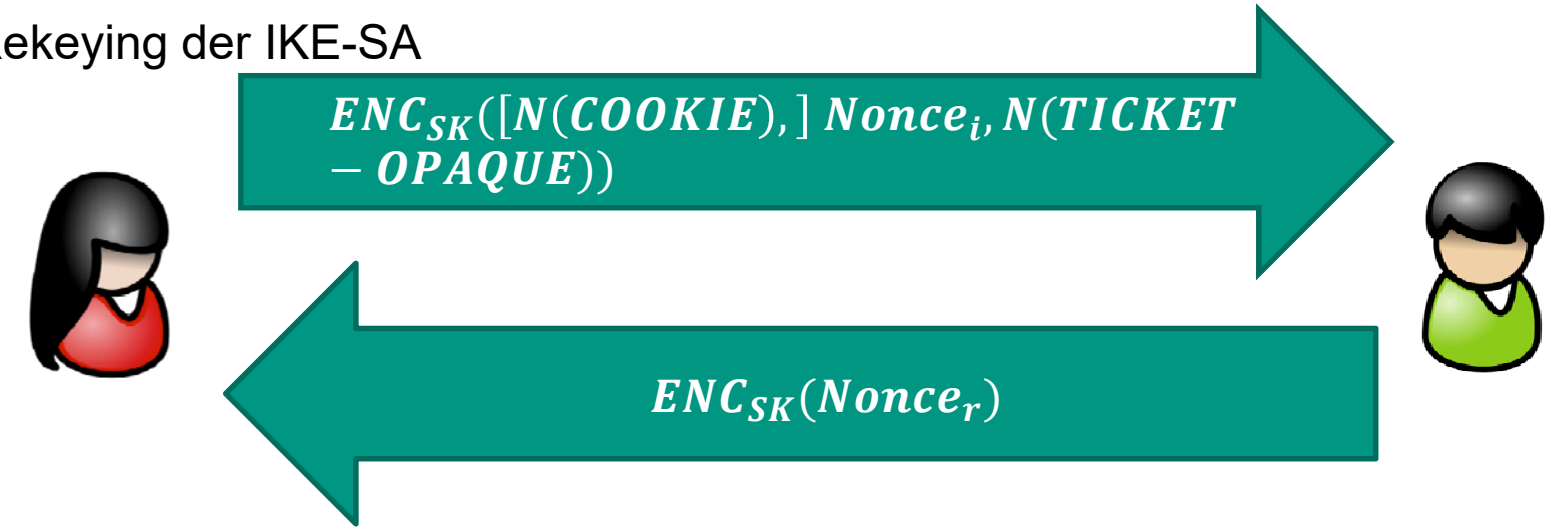


- Ticket-Inhalt
  - Auslagerung zum Peer
  - Nicht-les und –modifizierbar durch Peer
  - Ticket ist nur einmal verwendbar
  - Referenz auf SA-Speicherort, oder
  - SA-Parameter direkt

[RFC5723]

Tickets zur Zustandsspeicherung

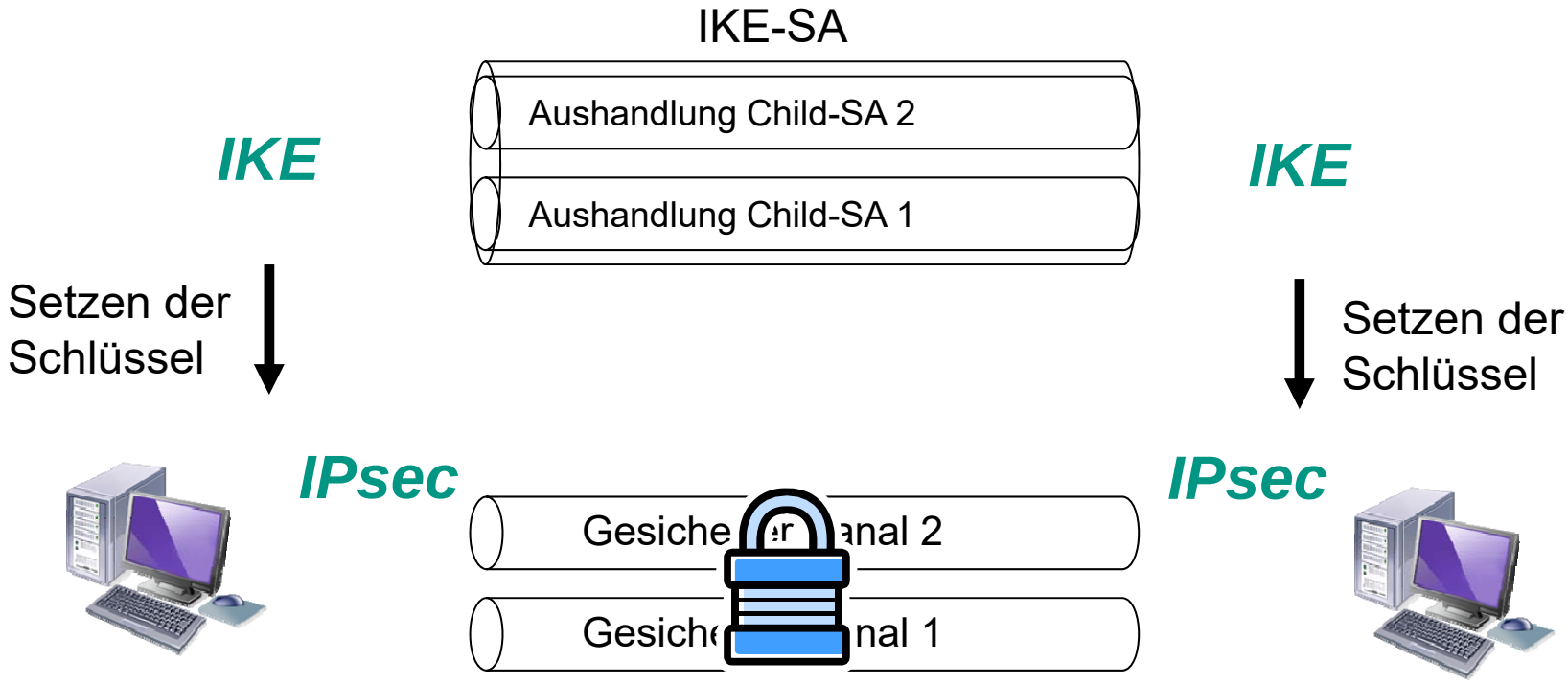
- Sitzungswiederaufnahme
  - Übergabe des Tickets
  - Anschließender IKE_AUTH Austausch
  - Rekeying der IKE-SA



- IKE-Payloads enthalten
  - N(TICKET_REQUEST): Ticket-Anforderung
  - N(TICKET_LT_OPAQUE): Ticket-Übergabe
  - N(TICKET_TICKET_OPAQUE): Ticket-Auslieferung

[RFC5723]

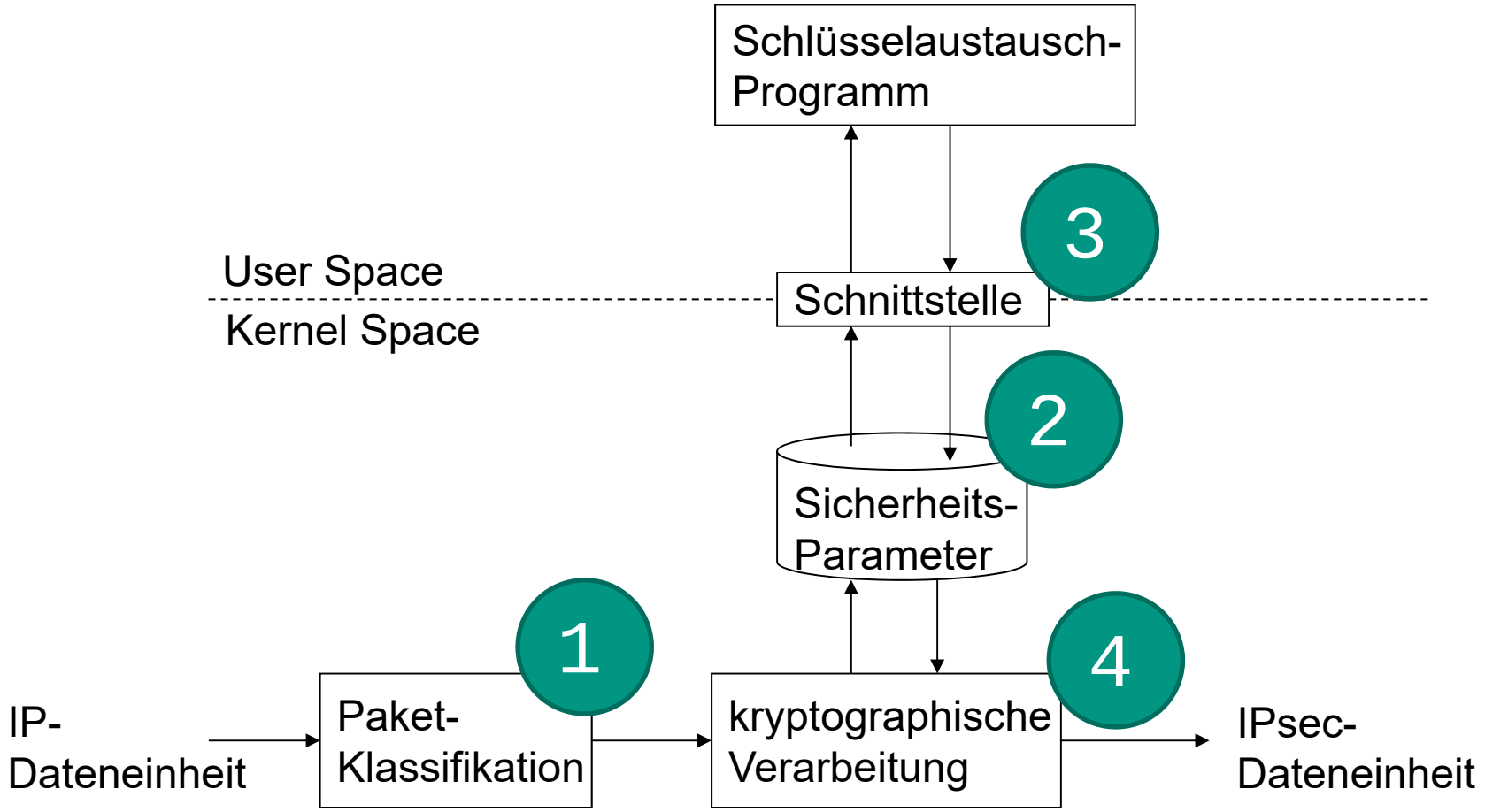
IKE-Zusammenfassung



- Zusammenfassung der Phasen
  - IKE-SA schützt Aushandlung weiterer Schlüssel
  - Child-SA stellt Schlüsselmaterial für Anwendung dar (IPsec)
  - Anwendung (IPsec) sichert den Datenaustausch

IPsec: Zusammenspiel der „Komponenten“

Verarbeitungsschritte einer ausgehenden IP-Dateneinheit



Zusammenfassung IPsec

- Vermittlungsschicht: IPsec
  - Generische Lösung
    - Transparent für die Anwendung … verwendet einfach TCP oder UDP
  - Meist bei *Virtual Private Networks* (VPN) eingesetzt
- Vorgehensweise
  - Sendendes System verschlüsselt Daten in IP-Dateneinheit
  - Authentizität und Integrität mittels kryptografischer Hashfunktionen
  - Vertraulichkeit mittels symmetrischer Verschlüsselung
- Weiteres
  - Hohe Komplexität: AH sowie Transport-Modus werden oft als unnötig bezeichnet
  - Hat Probleme mit NAT-Gateways und Firewalls
    - TCP/UDP-Ports können nicht einfach überschrieben werden
  - Meist nur in Kombination mit Schlüsselaustauschprotokoll wie z.B. IKEv2 sinnvoll

Literatur

[FeSc99] N. Ferguson, B. Schneier; A Cryptographic Evaluation of IPsec“, http://www.counterpane.com/ipsec.html, Feb. 1999

[RFC4301] S. Kent, K. Seo; Security Architecture for the Internet Protocol; Dez. 2005

[RFC4302] S. Kent; IP Authentication Header; Dez. 2005

[RFC4303] S. Kent; IP Encapsulating Security Payload (ESP); Dez. 2005

[RFC4304] S. Kent; Extended Sequence Number (ESN) Addendum …; Dez 2005

[RFC4305] D. Eastlake 3rd; Cryptographic Algorithm Implementation Requirements for ESP and AH; Dez. 2005

[RFC5723] Y. Sheffer, H. Tschofenig; Internet Kex Exchange Protocol Version 2 (IKEv2) Session Resumption; Jan. 2010

[RFC7296] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen; Internet Key Exchange (IKEv2) Protocol; Oct 2014

[Scha03] G. Schäfer; Netzsicherheit; dpunkt.Verlag, 2014

[Stal17] W. Stallings; Cryptography and Network Security, 7th Edition, Prentice-Hall, 2017