Vorlesung (WS 2014/15)

Sicherheit: Fragen und Lösungsansätze

Dr. Thomas P. Ruhroth

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

“Sicherheitsprotokolle“

**[mit freundlicher Genehmigung basierend
auf einem Foliensatz von
Prof. Dr. Claudia Eckert (TU München)]**

Literatur:

Claudia Eckert: IT-Sicherheit: Konzept - Verfahren - Protokolle, 7., überarb. und erw. Aufl., Oldenbourg, 2012.

E-Book: http://www.ub.tu-dortmund.de/katalog/titel/1362263

Prüfungen

- 12.Feb
- 26. Feb
- 2. März
- 23. März
- Bitte beachten Sie die Hinweise zur Anmeldung:
  - https://www-secse.cs.tu-dortmund.de/secse/pages/teaching/allgemeineInfo/pruefungsanmeldung_de.shtml

Agenda

- Kommunikationsprotokoll
  - IPSec
- Anwendungsprotokolle
  - DNSSEC
  - PGP

- Zusammensetzung von Sicherheitsbausteinen zu Anwendungsprotokollen verstehen.

IPsec

6.2 IPsec

IPsec (IETF-Standard)

Standardprotokoll für Schicht 3

6.2.1 Ipsec-Grundlagen

- **Sicherheitsarchitektur** für Internetprotokolle, seit 1995 verschiedene RFCs: 4302 (AH), 4303 (ESP), 4306 (IKE) …
- optionaler Einsatz im IPv4 und verpflichtend für Ipv6
- 2 Modi: Transport und Tunnel-Modus (insbes. bei VPN)

Ziel: Gewährleistung von Schutzzielen auf IP-Ebene

- Authentizität des Datenursprungs
- Vertrauliche Datenübertragung (Payload)
- Integrität u. Schutz vor Replay-Attacken
- Schlüsselmanagement: Erneuerung, Austausch

IPsec in a Nutshell

IPsec in a Nutshell

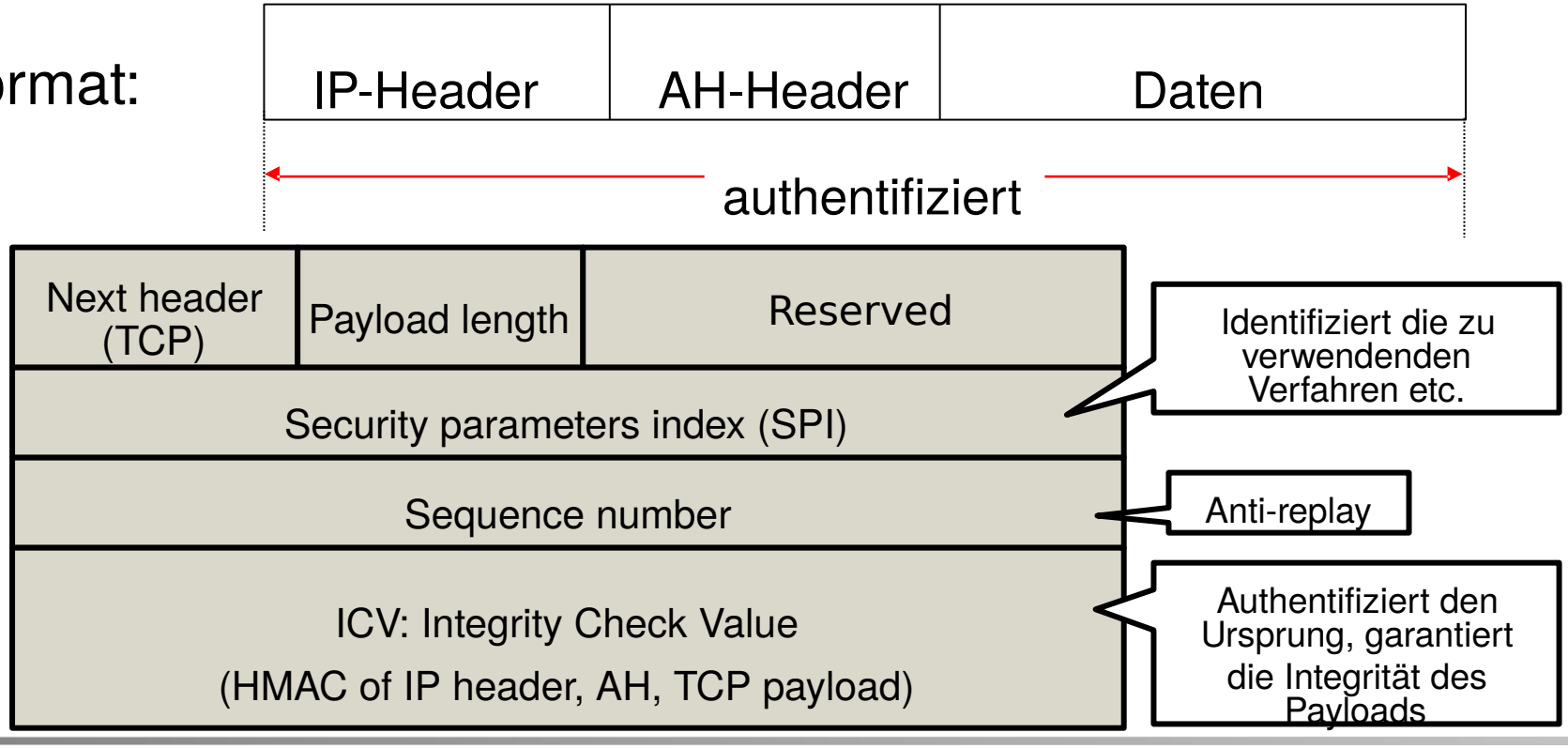
- **Protokolle:**
  - AH und ESP: Integrität, Vertraulichkeit angewandt auf einzelne IP-Pakete
  - IKE: Aushandeln der Verfahren und Schlüssel
- **Regelwerk (Policy):** muss konfiguriert werden
  - welche Pakete, von wem, zu wem, mit welchen Verfahren
  - Security-Policy-Database (SPD) (pro Ipsec-Rechner)
- **Speicherung der Sicherheitsparameter:**
  - Security-Association (SA): Verfahren, Schlüssel, ….
  - Verfahren, Schlüssel pro ‚Verbindung‘ : Zustand in IP!
  - Inbound, Outbound-Datenbanken

6.2.2 IP-Protokollerweiterungen: AH und ESP

Authentication-Header-Protokoll (AH) RFC 4302

- Authentizität, Integrität des Datenursprung und Payloads
- Verhinderung von Replay-Attacken über Sequenznummern

Format:

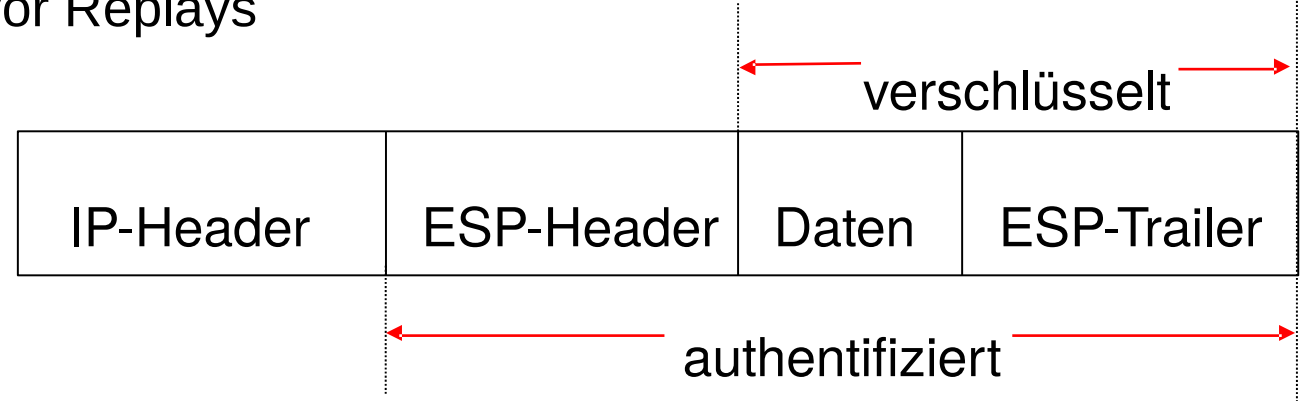


ESP

Encapsulating Security-Payload (ESP) RFC 4303

- Vertraulichkeit der Daten des IP-Datenpakets, Symmetrische Blockchiffre, auch NULL-Algorithmus zulässig
- Authentisierung des Payloads mittels HMAC
- (optional) Schutz vor Replays

Format:



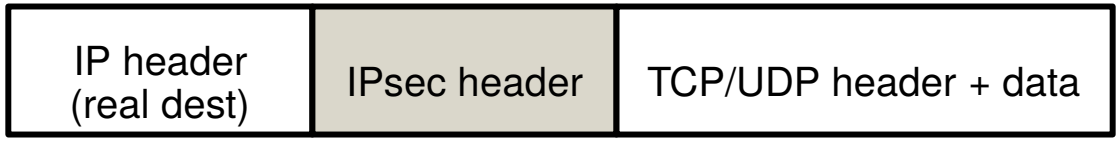
Durch die Nutzung von IPsec wird ein **IP-Paket verändert**:

- zusätzliche Header
- Verschlüsseln und/oder Hashen der Daten (Payload)

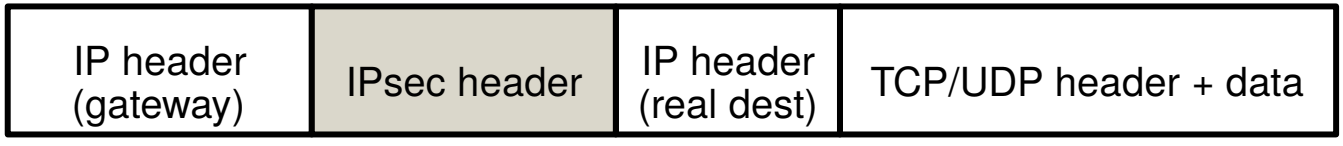
IPsec-Modi

IPsec-Modi: Transport und Tunnel-Modus

- Transport-Modus: Absichern des Payloads, **Konsequenz?**



- Tunnel-Modus: Einkapseln sowohl des IP-Headers als auch des Payloads in Ipsec-Paket



Geschachtelte Tunnels sind möglich

Beispiel: Sichere Verbindung über eine Firewall:

- Äußerer Tunnel durch das Internet zum Gateway (Firewall)
- Zugriff auf Server hinter der Firewall:
  - innerer Tunnel, um die Verbindung von der Firewall zum Server abzusichern

6.2.3 Datenstrukturen und Datenbanken

Security-Association-Datenstruktur (SA)

- SAs werden in den SA-Datenbanken von A bzw. B verwaltet
- eine SA enthält alle benötigten Informationen für IPsec- Verbindung zwischen zwei Rechnern A und B
- SAs haben nur unidirektionale Gültigkeit
- für jedes Protokoll (AH/ESP) wird eine eigene SA benötigt
- SAs werden vorab idR über IKE ausgehandelt und erstellt
- Eine SA wird beim erstmaligen Verbindungsaufbau angelegt

SPI:

- jedes IPsec Paket enthält einen Index (SPI), der auf einen SA-Eintrag in der SA-DB des Empfängers verweist
- diese SA enthält die notwendigen Verarbeitungsinformationen

Eine SA enthält u.a. folgende Informationen:

- IP-Adresse des Empfängers
- AH-Informationen:
  - Algorithmus, Schlüssel, Schlüssellebenszeit
- ESP-Informationen:
  - Algorithmen, Schlüssel, Initialwerte, Lebenszeiten, …
- Lebenszeit der SA: Zeitintervall oder Bytecounter, nach dem die SA erneuert oder terminiert werden muss und Angabe, welcher dieser Aktionen auszuführen ist
- Sequenzzähler (ab IKEv2 64 Bit, vorher 32 Bit) AH bzw. ESP
- Modus: Transport oder Tunnel
- Anti-Replay-Window, um einkommende Replays zu erkennen
- Security-Level (z.B. für Multi-level sichere Systeme)

Security-Policy-Database

Security-Policy-Database: Pro IPsec-Rechner eine SPD:

- eine SPD legt Regeln für den Umgang mit IP-Paketen fest
  - individuelle Regeln für eingehende (inbound) und
  - für ausgehende Pakete (outbound)
- jede Regel wird über einen Selektor spezifiziert:
  - ein Selektor ist für ein IP-Paket anzuwenden, wenn die Einträge des IP Pakets mit den Selektorfeldern matchen
  - ist ein Selektor anwendbar (match), dann enthält die SPD die mit dem IP-Paket durchzuführende Aktion

From	To	Protocol	Port	Policy
1.1.1.1	2.2.2.2	TCP	80	Transport ESP with 3DES

Selektoren

Selektoren, die einen SPD-Eintrag bestimmen: u.a.

- die IP-Adresse bzw. Adressbereiche oder Wildcard des Empfängers bzw. des Senders
- Sender-, Empfänger-Ports bzw. Liste von Ports oder Wildcard
- Name: z.B. DNS-Name, X.500 Distinguished Name,
- Unterschied zwischen outbound/inbound Paketen:
  - bei ausgehenden Paketen werden beim Anwenden der Regel die erforderlichen SAs (AH, ESP) etabliert (IKE)
  - inbound Paketen: Paket verwerfen, falls keine SA vorhanden
- **Aktionen:** bypass: direktes Weiterleiten des Pakets
  - apply: IPsec muss angewandt werden, Verweis auf SA
  - discard: das Paket muss vernichtet werden

Ablauf

Ablauf beim Versand eines IPsec-Pakets von A nach B

- A sucht SA für Verbindung mit B in SA-Datenbank von A
- A verwendet die dort angegebenen Informationen: Verschlüsselung, Hashen, MAC berechnen, …
- Aus SA-Eintrag: SPI zum Empfangen des Pakets in SA_DB_B
- A trägt in IPsec-Header diesen SPI ein

SPD von A:

From	To	Protocol	Port	Policy
1.1.1.1	2.2.2.2	TCP	80	Transport ESP with 3DES

Ausgehende SA-DB von A:

From	To	Protocol	SPI	SA-Eintrag
1.1.1.1	2.2.2.2	ESP	10	3DES key

Fazit IPsec

Fazit IPsec:

- Konfigurieren von IPsec-Policies ist sehr komplex
  - fehleranfällig: viele Optionen, viele Freiheitsgrade
  - ggf. Nutzung schwacher Modi, unsichere Auswahl
- Konfigurierungsvarianten führen zu Interoperabilitätsproblemen
- IKE-Pakete werden über UDP übertragen: unzuverlässig und wird von einigen Firewalls blockiert (ggf. kein Aushandeln mögl.)
- Interworking von IPsec und Firewalls ist problematisch Aber: bei korrekter Nutzung hoher Sicherheitsgrad erreichbar

DNSSEC

DNS-Security-Extensions

DNS-Security-Extensions (DNSSEC)

DNS ist eine der wichtigsten Internetdienste:

- Umsetzung von Domain-Namen in IP-Adressen anhand der Domain-Hierarchie.
- 13 Root-Server A bis M bilden Wurzel der Hierarchie, verteilt auf derzeit 376 physische Server (Instanzen) weltweit

DNS :

- Globale, verteilte Datenbank
- zur Abfrage von Informationen

  entlang der Domain-Hierarchie

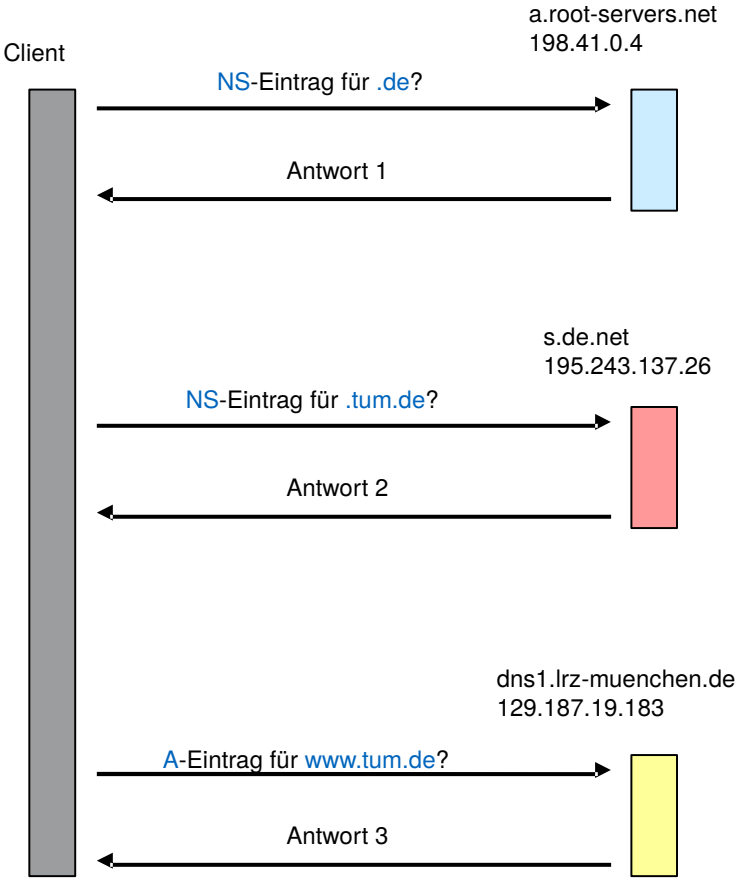
DNS-Root-Server-Instanzen weltweit

Quelle:root-servers.org

Beispiel

Auflösung von www.tum.de in IP-Adresse

Drei Anfragen erforderlich



Antwort 1

```
;; AUTHORITY SECTION:
de.          IN  NS a.nic.de.
de.          IN  NS c.de.net.
de.          IN  NS f.nic.de.
de.          IN  NS l.de.net.
de.          IN  NS s.de.net.
de.          IN  NS z.nic.de.

;; ADDITIONAL SECTION:
a.nic.de. IN   A   194.0.0.53
c.de.net.  IN  A   208.48.81.43
f.nic.de.  IN  A   81.91.164.5
l.de.net.  IN  A   77.67.63.105
s.de.net.  IN  A   195.243.137.26
z.nic.de. IN   A   194.246.96.1
```

Zuständige Nameserver

Zugehörige IP-Adressen

Antwort 2

```
;; AUTHORITY SECTION:
tum.de.  IN  NS  dns1.lrz-muenchen.de.
tum.de.  IN  NS  dns3.lrz-muenchen.de.
tum.de.  IN  NS  dns2.lrz-muenchen.de.

;; ADDITIONAL SECTION:
dns1.lrz-muenchen.de.  IN  A  129.187.19.183
dns2.lrz-muenchen.de.  IN  A  141.40.9.211
dns3.lrz-muenchen.de.  IN  A  193.136.2.123
```

Antwort 3

```
;; ANSWER SECTION:
www.tum.de.                IN  CNAME  tum.www.ze.tu-muenchen.de.
tum.www.ze.tu-muenchen.de. IN  CNAME  tum.www.ze.tum.de.
tum.www.ze.tum.de.         IN  CNAME  portal.mytum.de.
portal.mytum.de.           IN  A      129.187.39.2
```

Aliase für Domain-Namen

IP-Adresse des Hosts

Problem

Problem: DNS-Anfragen und Antworten sind ungeschützt!

- Distributed-Denial-of-Service-Attacke auf Nameserver
- DNS-Amplification-Angriff
  - Denial-of-Service-Attacke verstärken
- DNS-Spoofing
  - „Umleiten von Namen“
- Cache Poisoning
  - Zusätzliche Daten werden ungeprüft genutzt
- DNS-Framing

DNSSEC, seit 1997 entwickelt! (RFC 4033)

- Etablierung einer globalen PKI entlang der Domain-Hierarchie
- Administrator eines Nameservers signiert die DNS-Einträge in seinem Verwaltungsbereich
- Empfänger prüft digitale Signatur der DNS-Antworten und kann so Manipulationen erkennen

PKI von DNSSEC

Pro Zone zwei Arten von Public-Key-Schlüssel-Paaren:

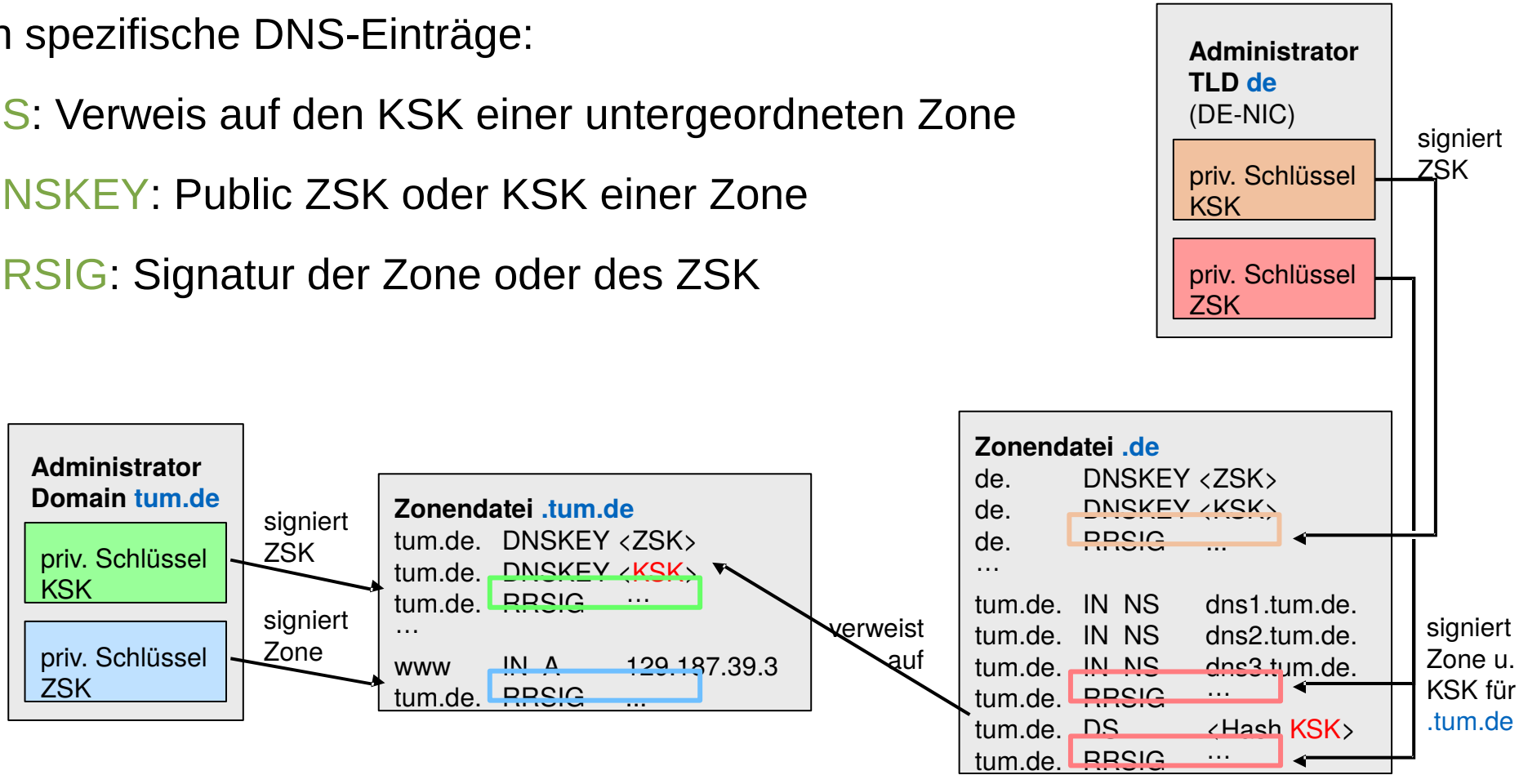
- Key-Signing-Key (KSK), empfohlen 2048 Bit, 2-4 Jahre gültig
- Zone-Signing-Key (ZSK), empfohlen 512 Bit, 1-2 Monate gültig

- ZSK signiert die DNS-Einträge der eigenen Zone
- KSK signiert den Public-ZSK der eigenen Zone
- KSK der übergeordneten Zone signiert den Public-KSK der darunter liegenden Zonen
- Root-Zone selbst ist ebenfalls signiert, Schlüssel wird von VeriSign verwaltet

Signatur und Schlüsselverteilung

Durch spezifische DNS-Einträge:

- DS: Verweis auf den KSK einer untergeordneten Zone
- DNSKEY: Public ZSK oder KSK einer Zone
- RRSIG: Signatur der Zone oder des ZSK



- **Prüfung der Echtheit des Eintrages durch Public Key**
  - **ZSK oder KSK**
- **Häufig auf lokalem DNS**
  - **DO-Bits (DNSSEC OK)**
  - **AD-Bit (Authenticated Data)**

Schlüsselverwaltung

Wozu die Indirektion von KSK und ZSK?

- Kurze Schlüssellängen für ZSK:
  - weniger Rechenaufwand zur Verifikation der Zonendaten
  - weniger Daten bei DNSSEC-Anfragen zu übertragen
  - **Aber:** kurze Schlüssel sind leichter zu knacken
- Lange Schlüssellängen für KSK:
- höherer Aufwand, größeres Datenvolumen, dafür aber mehr Sicherheit.

Konsequenz: langlebige KSKs, die regelmäßig neue kurzlebige ZSKs erzeugen

DNS-Resolver: Cachen verifizierte Public-ZSKs

Fazit DNSSEC

Fazit DNSSEC

- Massivste Änderung des DNS in der Geschichte des Internet
- Root-Zone sowie einige TLDs bereits signiert, Testbetrieb von .de läuft seit 2010
- Kann Spoofing und Poisoning-Angriffe verhindern
- DNSSEC als Security-Enabler:

  Globalen, hierarchischen PKI auch für andere Szenarien interessant, Beispiele?
- **Aber:** Viele Endgeräte und Router nach wie vor nicht DNSSEC-fähig, großer Nachholbedarf seitens der Gerätehersteller

Secure Mail - **Pretty Good Privacy (PGP)**

Secure Mail

Secure Mail am Beispiel Pretty Good Privacy (PGP)

- OpenPGP RFC 2440: Public Domain Software
- verfügbar als Plug-in für Standard E-Mail-Clients oder als eigenständige Software

(Sicherheits-)Dienste von PGP (v8.0.1)

- Verschlüsselung symmetrischer Schlüssel: RSA , ElGamal
- (Mail-)Verschlüsselung: symmetrische Blockchiffre:
  - AES, 3DES, DES, CAST, Twofish
- Datenintegrität und Authentizität: SHA-1, MD5, auch andere
  - Signaturverfahren: RSA, DSA (je 1024 – 4096 Bit)
- Weitere Dienste:
  - Kompression (ZIP-Kompression)

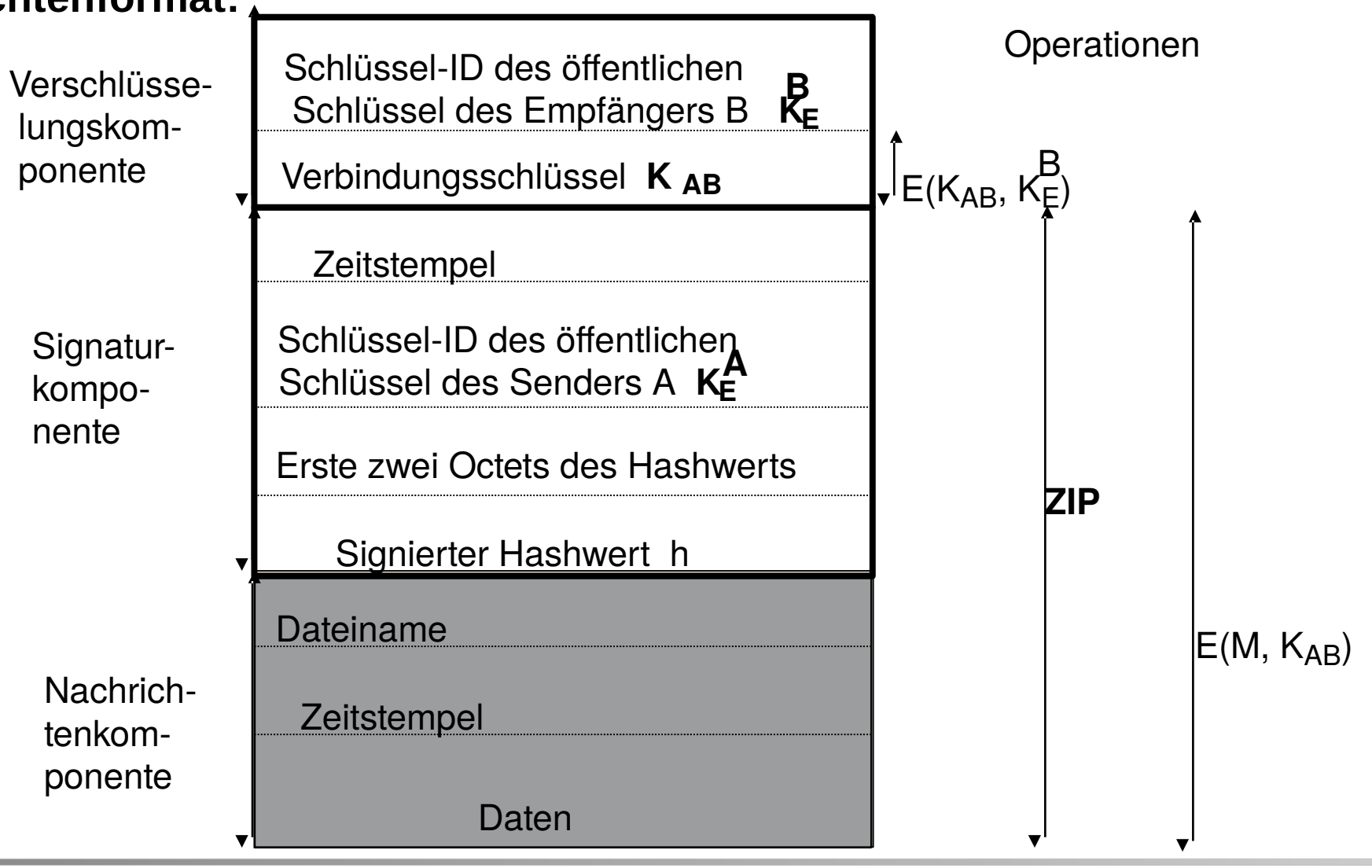
Nachrichtenformat

PGP-Nachricht besteht aus maximal drei Komponenten:

- Nachrichtenkomponente:
  - zu übermittelnde/zu speichernde Daten
- Signaturkomponente: enthält
  - Zeitstempel mit dem Zeitpunkt der Signaturerstellung,
  - den signierten Hashwert und
  - Schlüssel-ID des Signierers
- Verschlüsselungskomponente:
  - verschlüsselter Verbindungsschlüssel (von Sender erzeugt)
  - Schlüssel-ID de(s)r verwendeten Empfänger-Schlüssel(s)

PGP-Nachrichtenformat

PGP-Nachrichtenformat:



Schlüsselverwaltung

Schlüsselverwaltung

Unterschiedliche Schlüssel sind zu verwalten:

- symmetrischer Nachrichtenschlüssel (Einmalschlüssel),
- die öffentlichen Schlüssel von Partnern sowie eigene
- Schlüssel zur verschlüsselten Ablage privater Schlüssel

Pro Benutzer: Sender oder Empfänger:

- sind mehrere asymmetrische Schlüsselpaare möglich

Bei mehreren asymmetrischen Schlüsselpaaren:

- Sender muss den benutzten Schlüssel identifizieren:
- Erzeugen einer Zufalls-ID pro Schlüssel ist zuviel Overhead deshalb: ID ableiten aus Schlüssel
- 64-Bit ID: 64 niedrigwertigsten Bits des öffentlichen Schlüssels; Schlüssel-Id: ID = $K_E \bmod 2^{64}$

Private-Key-Ring

Verwaltung der asymmetrischen Schlüssel in **Key-Rings:**

- Key-Rings sind Dateien
- Private-Key-Ring: Eigene Schlüsselpaare
- Public-Key-Ring: Öffentliche Schlüssel anderer

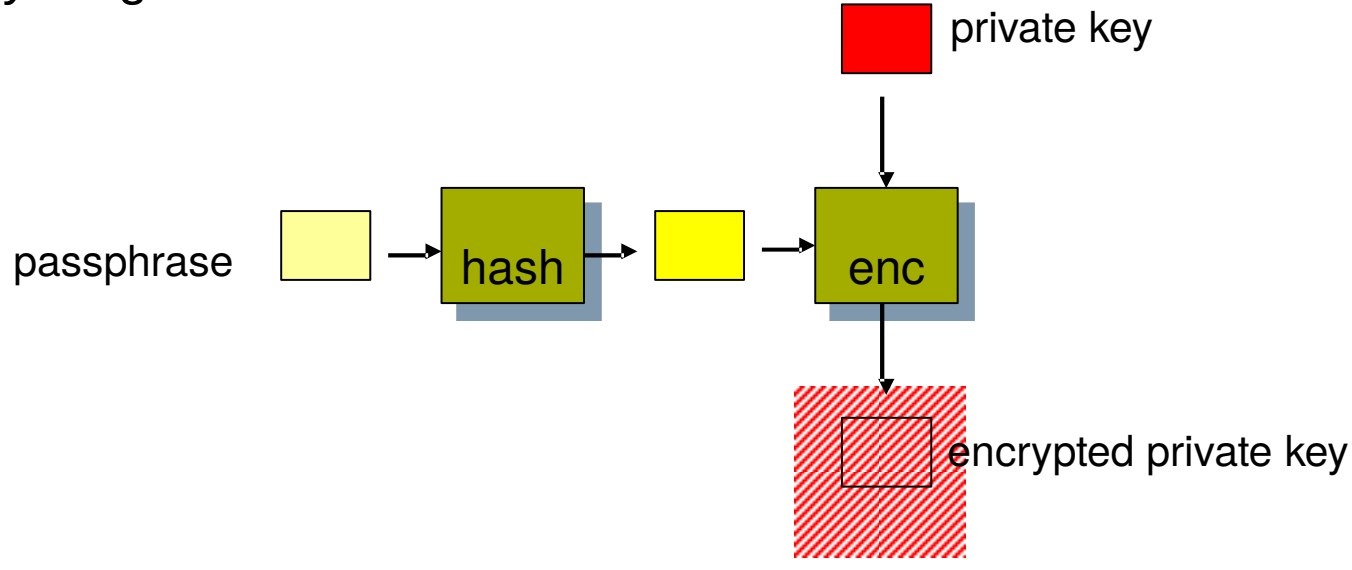
Private-Key-Ring:

- erzeugbar über PGP-Bibliotheksfunktion
- Eintrag in Private-Key-Ring pro asymmetrischem Schlüsselpaar:
  - Zeitpunkt der Schlüsselerzeugung (timestamp)
  - Schlüssel-ID
  - Öffentlicher Schlüssel
  - Verschlüsselter privater Schlüssel
  - Benutzer-ID (z.B. E-Mail-Adresse)

Schutz des Private-Keys

Schutz des Private-Keys:

- Benutzer-definierte Passphrase: Mantra
- 160-Bit SHA-1 Hashwert *H* des Mantras
- Hashwert liefert Schlüsselmaterial für symmetrisches Verschlüsselungsverfahren
- Mit korrekter Passphrase (Passwortbasierter Schutz!) ist Rekonstruktion des Private-Key möglich



Public-Key-Ring

Public-Key-Ring

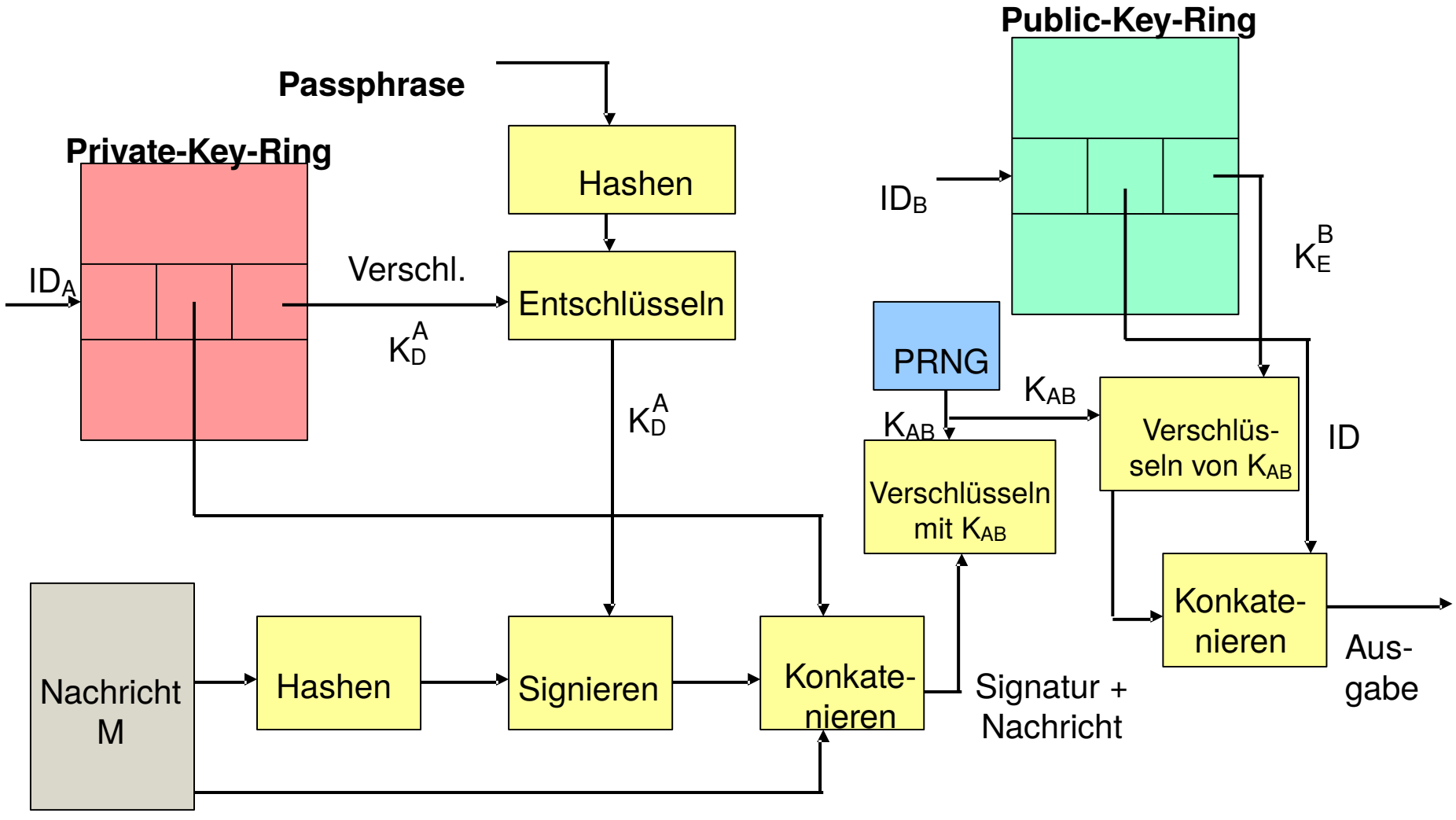
- öffentliche Schlüssel der Kommunikationspartner
- Informationen pro Eintrag:
  - Zeitpunkt der Schlüsselaufnahme in die Datei
  - Schlüssel-ID und zugehöriger öffentlicher Schlüssel
  - ID des Schlüsselbesitzers
  - Key-Legimitation-Field (KLF): Web of Trust
  - Grad des Vertrauens, das der Benutzer in diesen öffentlichen Schlüssel eines anderen Benutzers besitzt.

Symmetrische Verschlüsselungsschlüssel K_{AB}:

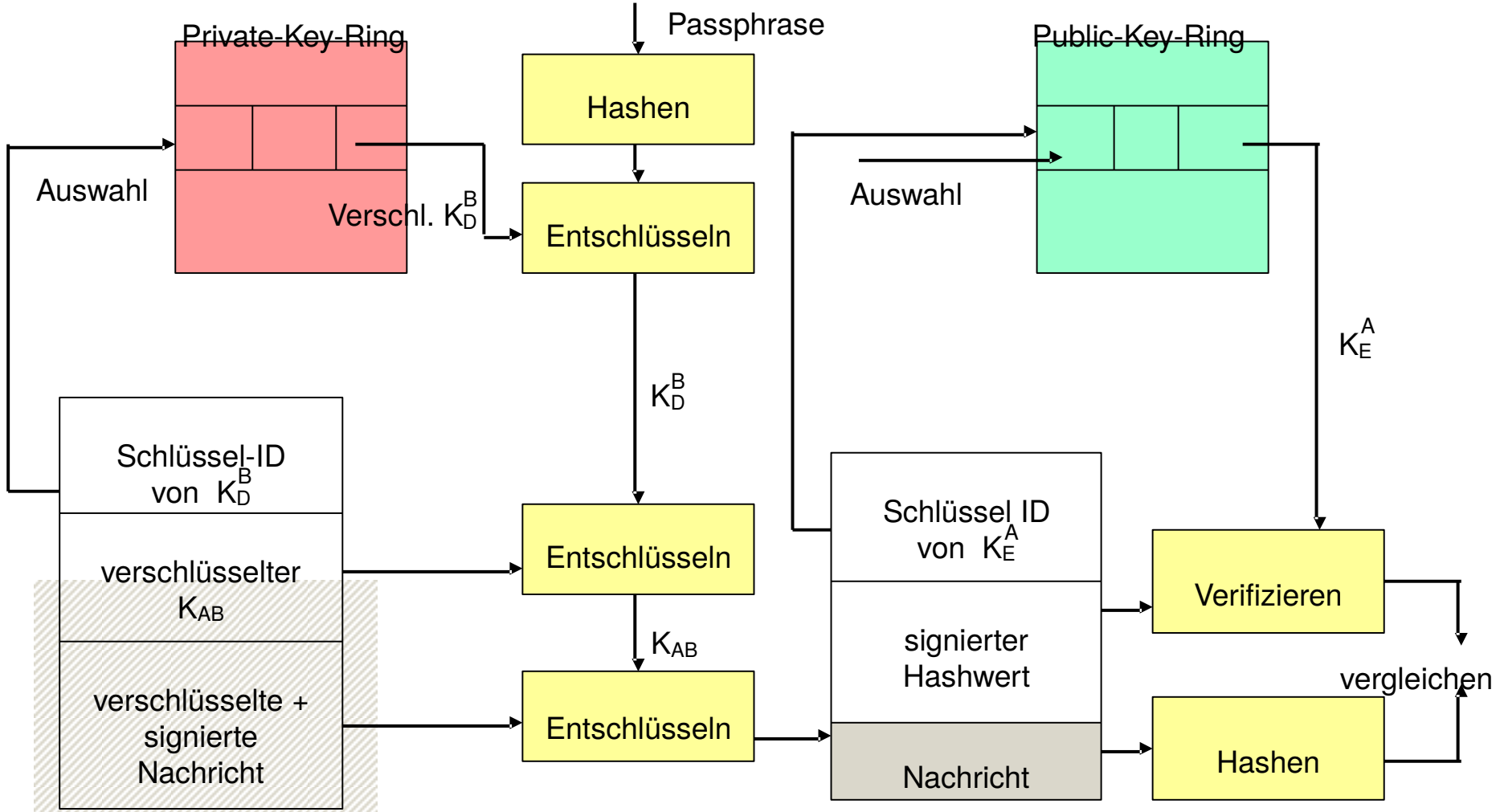
- mit Pseudozufallszahlengenerator PRNG generiert,
- Berechnung eines initialen Zufallswerts: Messen der Verzögerungszeiten bei Tastatureingaben

Verschlüsseln und Signieren einer Nachricht

LEHRSTUHL 14
SOFTWARE ENGINEERING



Entschlüsseln und Verifikation einer Nachricht



Web of Trust

Vertrauenslevel für die öffentlichen Schlüssel anderer:

- Owner-Trust: von Benutzer festgelegt Grad an Vertrauen, das der Benutzer in den Besitzer des öffentlichen Schlüssels hat.

  Mögliche Bewertungen:

  - Benutzer ist unbekannt (unknown user)
  - nicht vertrauenswürdig (usually not trusted to sign)
  - geringfügig vertrauenswürdig (usually trusted to sign)
  - immer vertrauenswürdig (always trusted to sign)
  - Ultimativ vertrauenswürdig (eigener Schlüssel)
- Signature-Trust: vom PGP-System festgelegt

Signature-Trust

Signature-Trust:

- Falls öffentlicher Schlüssel im Public-Key-Ring:

  Signature-Trust-Wert = Owner-Trust-Wert

- Andernfalls: Signature-Trust-Wert = „unknown user“

Im Public-Key-Ring:

- Menge von Zertifikaten/Signaturen pro Public-Key
- Key-Legimitation-Field (KLF):

  gewichtete Summe der Attribute der Signaturen für den öffentlichen Schlüssel (vom PGP-System berechnet)

Bemerkung: unter PGP sind auch X.509-Zertifikate verwendbar

Berechnung des KLF

Berechnung des KLF: Algorithmus:

- Mindestens eine Signatur ist „Ultimate Trusted“: KLF = 1
- Ansonsten: Berechnung der gewichteten Summe:
  - „Always Trusted“-Signaturen haben ein Gewicht von 1/X
  - „Usually Trusted“-Signaturen haben ein Gewicht von 1/Y
  - X, Y sind Benutzer-konfigurierbare Parameter

Beispiel: X=2, Y=4, volles Vertrauen erfordert:

- 2 „Always Trusted“-Signaturen oder
- 4 „Usually Trusted“-Signaturen oder
- 1 „Always Trusted“ und 2 „Usually Trusted“-Signaturen oder
- 1 „Ultimate Trust“-Signatur

Fazit Web of Trust

Fazit Web of Trust:

- Keine zentrale Vertrauenswurzel, benutzer-interpretierbare Vertrauenslevel (Benutzer-‘zertifizierte‘ Schlüssel)
- Verständnis der Nutzer für diese Vorgehensweise notwendig

Fazit E-Mail-Sicherheit:

- Standardschutzziele bei der Kommunikation werden erfüllt
- Flexibilität durch Wahl der Verfahren und Kombination
- individuelle Anwendung auf einzelne Mails
- Problem: Interoperabilität von Secure-Mail-Systemen
- Problem: Sichere Basis notwendig: Schlüsselspeicherung etc.
- Problem: Unternehmerische Sicherheitspolicy muss Umgang mit verschlüsselten Mails festlegen, Beispielregeln?

Sicherheitsengineering