

Vorlesung Netzbasierte Informationssysteme

Sichere Internetprotokolle

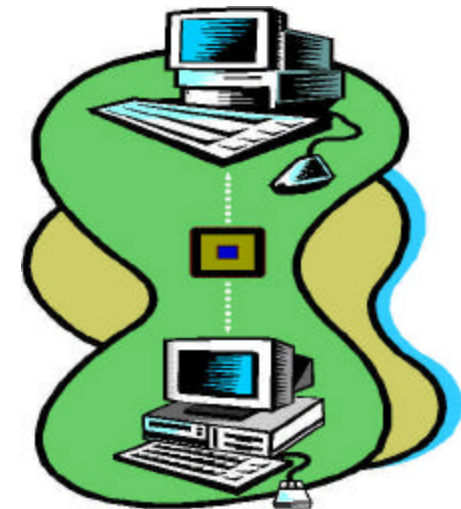
Prof. Dr. Adrian Paschke

Arbeitsgruppe Corporate Semantic Web (AG-CSW)
Institut für Informatik, Freie Universität Berlin
paschke@inf.fu-berlin.de
<http://www.inf.fu-berlin.de/groups/ag-csw/>

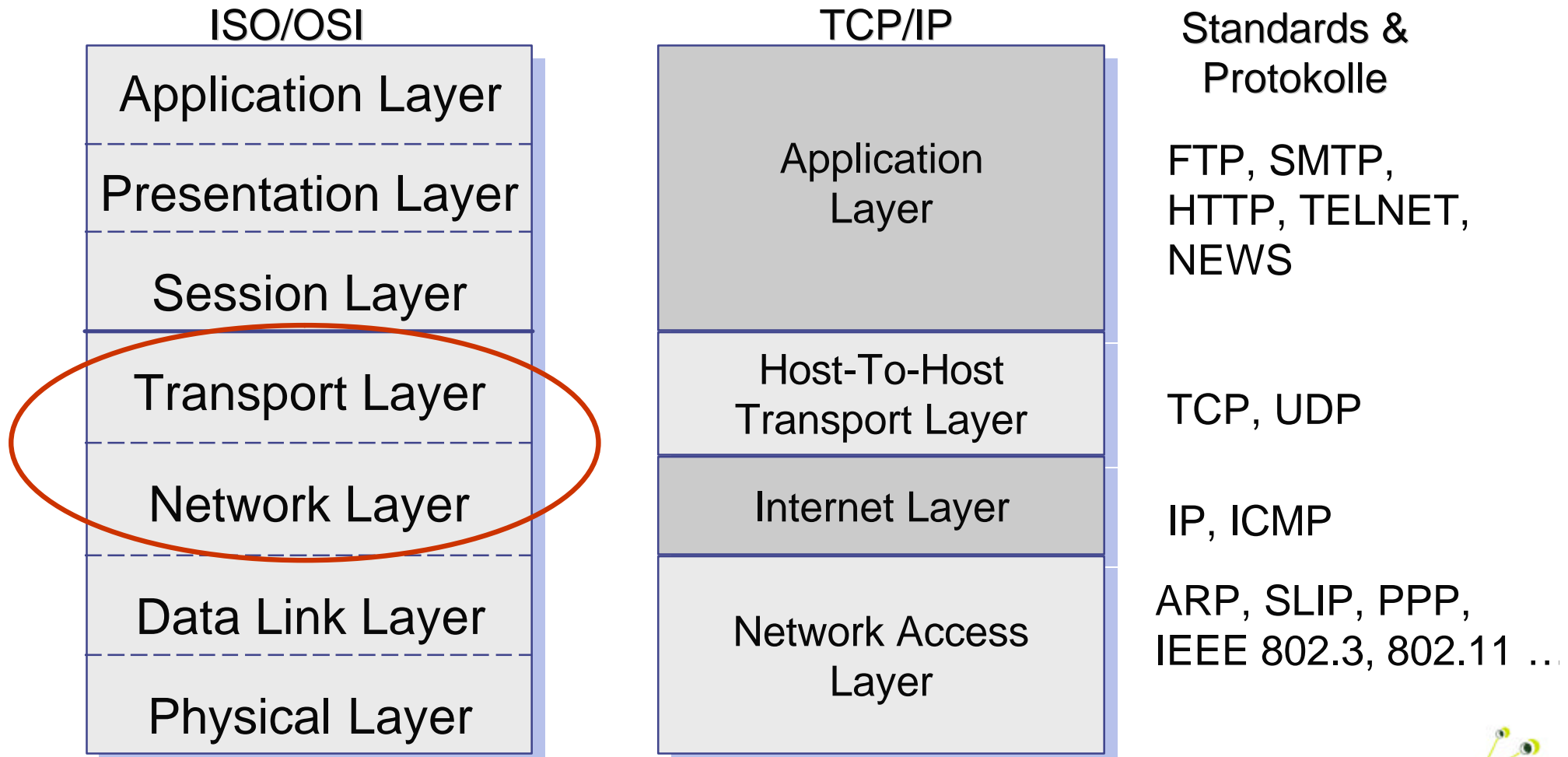


Sichere Internetprotokolle

- Transaktionssicherheit im Internet
- Kryptographische Verfahren
- Public Key Infrastructures
- Sichere Internetprotokolle



Die Protokolfamilie TCP/IP*



*Hansen/Neumann, Kap.6.6

Transaktionssicherheit für Internetbasierte Geschäftssysteme

Geeignete Rahmenbedingungen, welche Geschäftsparteien am Internet

- eine verlässliche gegenseitige Identifizierung
- die Integrität einer übertragenen Nachricht
- die Uneinsehbarkeit des Inhaltes
- die Nicht-Abstreitbarkeit des Absendevorganges oder Empfanges einer Nachricht

garantieren sollen.

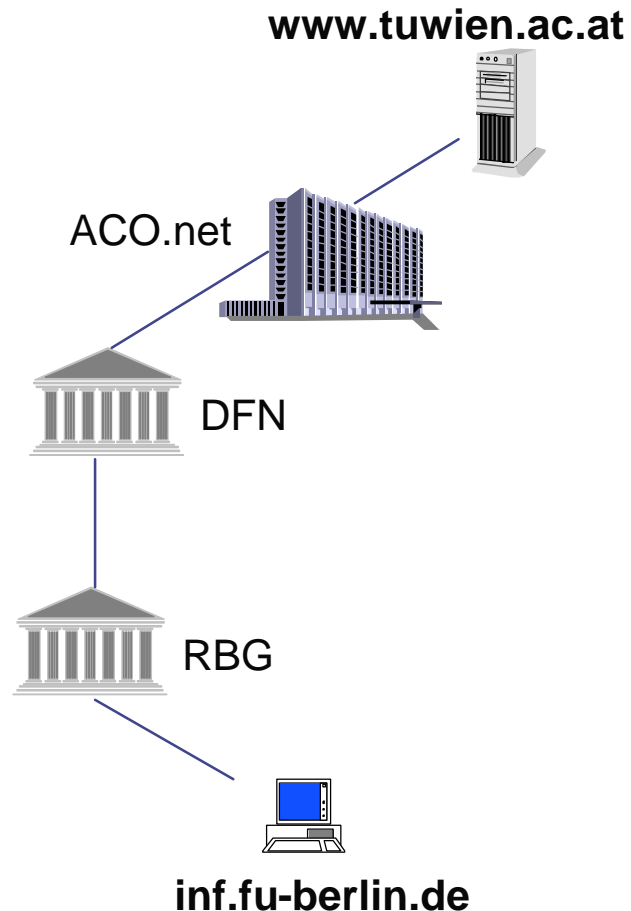
Allgemeine Sicherheitsanforderungen

- Vertraulichkeit / Geheimhaltung
 - Kein Zugang zu Informationen für nicht-authorisierte Teilnehmer
- Integrität
 - Schutz der Daten vor unberechtigter Veränderung
- Unabstreitbarkeit
 - Nachweis der Urheberschaft
- Authentifikation
 - Zuverlässige Feststellung der Identität
- Zugriffskontrolle
 - Regelt den Zugriff auf Objekte oder Informationen
- Verfügbarkeit
 - Vorhandensein von Ressourcen und Daten für rechtmäßige Benutzer

Angriffe

- **Passive Angriffe**
 - Eavesdropping (Lauschangriff):
 - unbemerktes Abhören und Aufzeichnen übertragener Nachrichten durch nicht autorisierte Personen
 - Traffic analysis (Verkehrsflussanalyse):
 - Rückschlüsse auf Teilnehmer ziehen durch Beobachtung der gesendeten Nachrichten
- **Aktive Angriffe**
 - Spoofing / Masquerading:
 - Gefälschte Identität
 - Tampering:
 - Verfälschung von Nachrichten
 - Replay:
 - Nachrichten werden gespeichert und später erneut abgeschickt
 - Denial of Service:
 - Dienstleistung wird verhindert

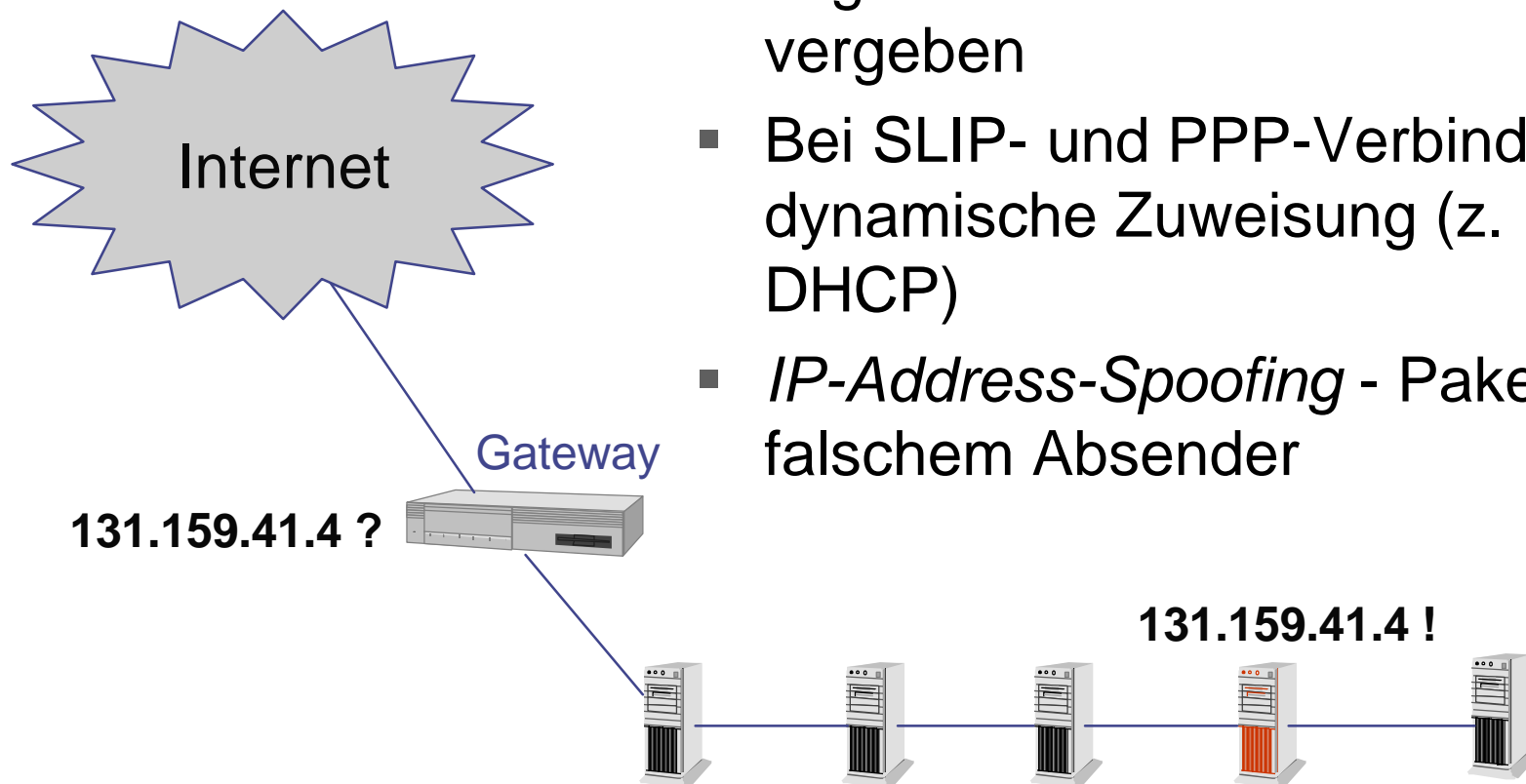
Sicherheitsproblematik Routingvorgang



- Routing-Vorgang ist unsicher
 - Netzwerke außerhalb der unternehmensinternen LANs unterliegen weder der eigenen Kontrolle noch der einer zentralen Autorität
 - Keine Zustellungsgarantie
 - Übertragungsgeschwindigkeit nicht beeinflussbar
 - Dynamische Routenwahl: Route ist nicht vorhersehbar
- Inhalt der Pakete ist einsehbar und modifizierbar
 - Übertragung der Protokollelemente der Anwendungsebene im Klartext

Identifizierung mit IP-Adresse

- IP-Adresse wird innerhalb des zugewiesenen Adressbereiches frei vergeben
- Bei SLIP- und PPP-Verbindungen dynamische Zuweisung (z. B. DHCP)
- *IP-Address-Spoofing* - Pakete mit falschem Absender



Sicherheit bei IPv4

Jede am Internet übertragene Nachricht kann problemlos abgehört oder abgefangen werden. Die Identifikation von Rechnern anhand der IP-Adresse ist in vielen Bereichen ungenügend.

- Abschottung des unternehmensinternen Netzwerkes von der Außenwelt (Firewall)
- Kryptographisch abgesicherte Übertragung (z. B. IPSec, SSL, TLS)
- Authentifizierung mit Zertifikaten, Einsatz globaler Public-Key-Infrastrukturen

Absicherung von Internetprotokollen

Application Layer	Kerberos, SSH, S/MIME, SET, etc.
Transport Layer	Transport Layer Security (TLS)/SSL
Network Layer	IP Security (IPSec)
Data Link Layer	Hardware Verschlüsselung

=> Kryptographische Verfahren zur Absicherung von Internetprotokollen

Kryptographische Verfahren

- Umwandlung eines Klartextes (p , *plain text*) in einen chiffrierten Text (c , *ciphertext*) mit Hilfe einer reversiblen kryptographischen Funktion f :

$$f(p) = c$$

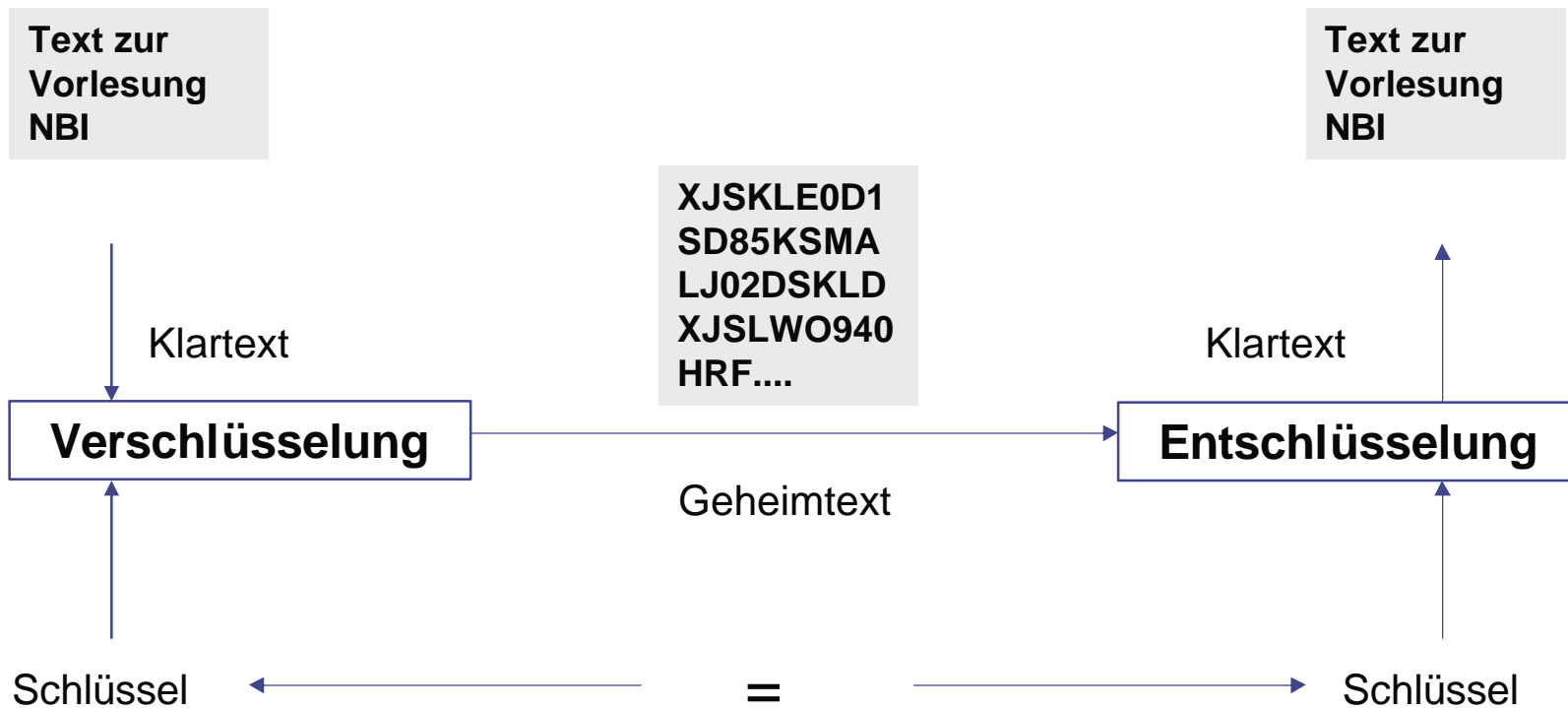
$$\bar{f}(c) = p$$

- Kryptoanalyse beschäftigt sich mit der Dechiffrierung von Daten
- Steganographische Verfahren ermöglichen das Verstecken von geheimer Information in Dateien mit „unverdächtigem“ Inhalt

Eigenschaften kryptographischer Algorithmen

- Mathematische Grundlagen kryptographischer Algorithmen
 - Primzahlfaktorisation (bei RSA), etc.
 - Hashfunktionen
- Verarbeitungsverfahren
 - alphabetisch
 - polyalphabetisch (verbirgt Häufigkeitsverteilungen von Buchstaben)
 - bitbasiert
- je nach Verarbeitungsweise unterscheidet man
 - Stromchiffrierung (fortlaufende Chiffrierung)
 - Blockchiffrierung (Chiffrierung von Stücken des Klartext mit fester Länge)

Ver- und Entschlüsselung mit symmetrischer Kryptographie



Klassische symmetrische Verfahren

■ Cäsar-Verfahren

- $c = (p + s) \bmod 26$, bei $s = 3$
- **A** ® **D**
- **B** ® **E**
- **C** ® **F**
-

■ Vigenère-Verfahren

- abhängig von der Position im Text (zusätzliches Verschlüsselungswort), z. B. **HALLO**
- **HALLOHALLOHALLOHALLO**
- **DIESISTEINENACHRICHT**
- Abbildung: Caesar-Verschiebung um den Wert des zugeordneten Buchstabens :
 - **D** ® **D + H = K**
 - **I** ® **I + A = I**
 - **E** ® **E + L = P**
 - . . .

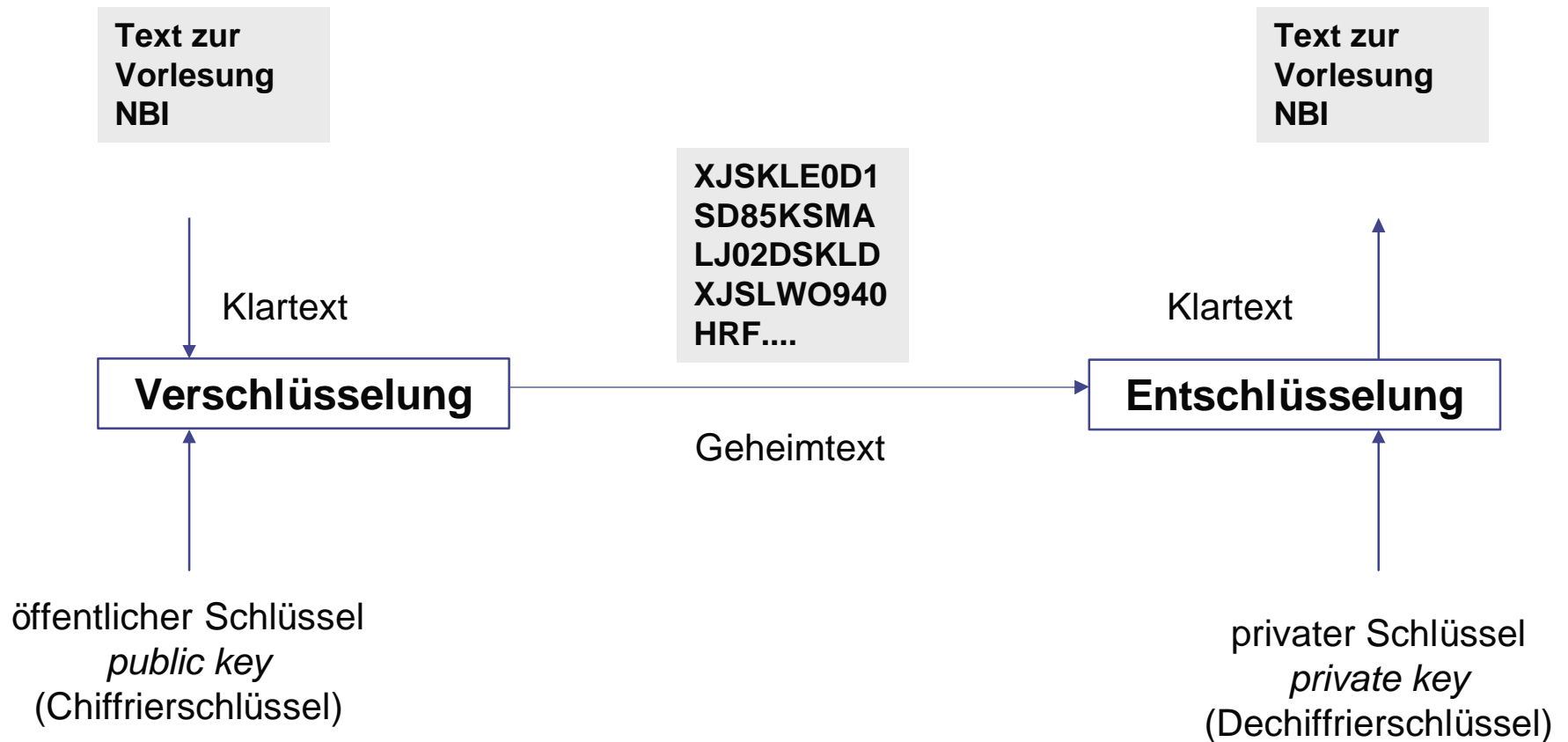
Symmetrische Verfahren

- IDEA - *international data encryption standard*
 - Entwickelt von Lai & Massey, 1992, ETH Zürich, patentrechtlich geschützt (Ascom Systec AG, Schweiz)
 - Blockchiffrierung (64bit-Blöcke) durch einen 128bit-Schlüssel
 - Verschlüsselung in acht Runden, jede Runde verwendet sechs Teilschlüssel
- DES, 3DES
 - basiert auf dem zu Anfang der 70er Jahre von IBM entwickelten Verschlüsselungsverfahren *Lucifer*. Nach Änderungen durch die National Security Agency (NSA), wurde DES 1976 zum offiziellen Standard für amerikanische Regierungsbehörden ernannt.
- AES
 - Blockchiffre, dessen Blocklänge und Schlüssellänge unabhängig voneinander die Werte 128, 192 oder 256 Bit erhalten kann. Nachfolgestandard zu DES der US-amerikanischen Regierungsbehörden (2000).
- RC4, etc.

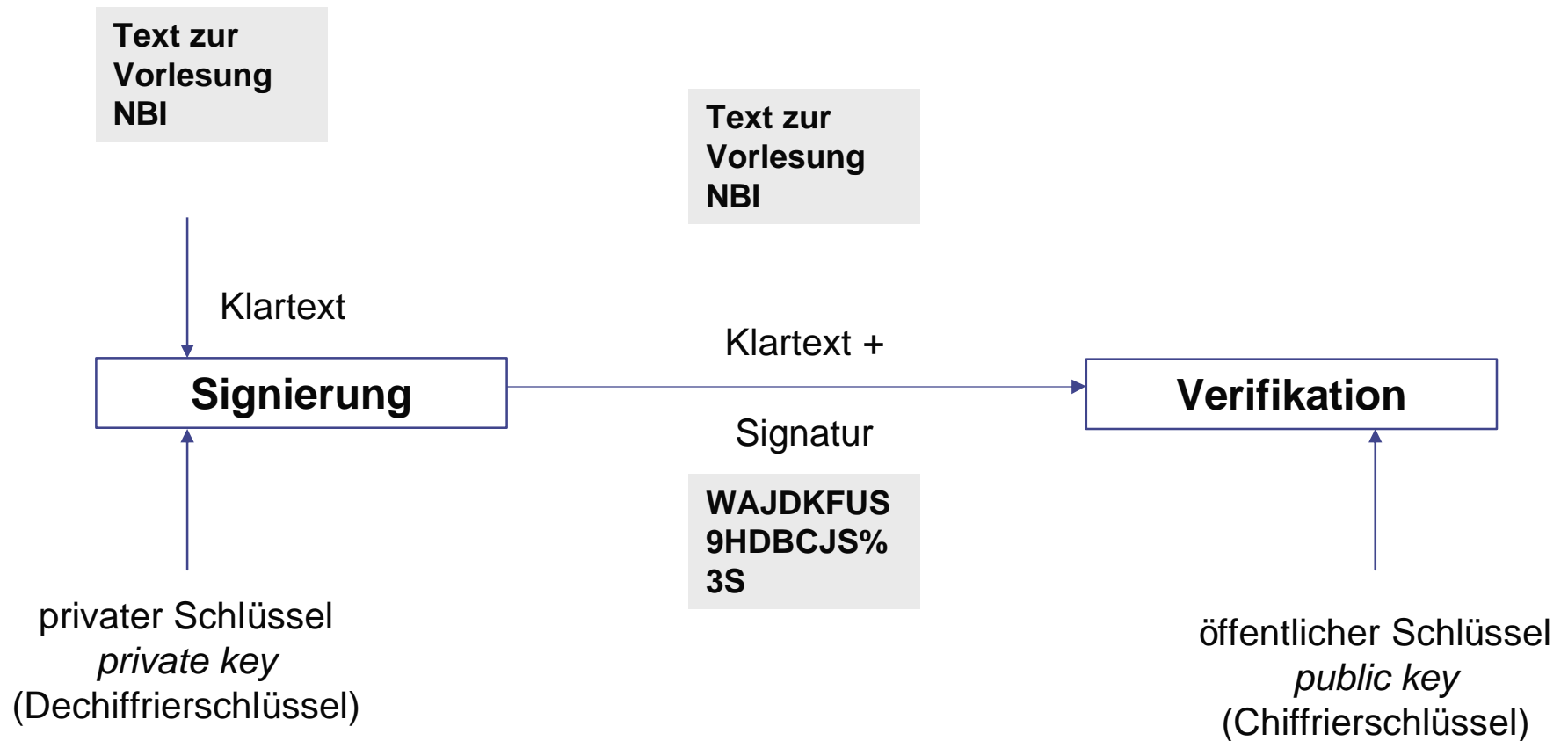
Asymmetrische Kryptographie

- Einführung durch Diffie und Hellman 1976
 - Beispiele: RSA, Diffie-Hellman, ElGamal, Elliptische Kurven
- Generierung von **Schlüsselpaaren**:
 - privater Schlüssel (*private key*):
nur dem Inhaber bekannt
Funktion: Entschlüsselung, Signierung
 - öffentlicher Schlüssel (*public key*):
wird auf allgemein zugänglichen Servern bereit gestellt
Funktion: Verschlüsselung, Verifikation
- Anwendung für
 - Verschlüsselung **und**
 - digitale Signaturen

Ver- und Entschlüsselung mit asymmetrischer Kryptographie



Digitale Signaturen



Unterscheidung symmetrischer und asymmetrischer Verfahren

- symmetrisch:
 - **ein** Schlüssel für *Chiffrierung* und *Dechiffrierung*
 - *international data encryption algorithm* (IDEA)
 - *digital encryption standard* (DES, Triple-DES)
 - *advanced encryption standard* (AES, = Rijndael-Algorithmus)
 - DES Nachfolger seit Ende der 90'er Jahre
- asymmetrisch
 - unterschiedliche Schlüssel für *Chiffrierung* und *Dechiffrierung* (Schlüsselpaar)
 - Rivest Shamir Adleman (RSA)
 - *digital signature algorithm* (DSA)
 - ...

RSA am Beispiel

- Entwickelt von Rivest, Shamir, Adleman (1978)
- Ansatzpunkt ist die Schwierigkeit, große Zahlen effizient in ihre Primfaktoren zu zerlegen
- Zutaten: p, q zwei große Primzahlen
- öffentlicher Schlüssel e (zum Chiffrieren)
 - $n = p * q$
 - e eine teilerfremde Zahl zu $(p-1)*(q-1)$
- privater Schlüssel d
 - d mit $d * e = 1 \pmod{((p-1)*(q-1))}$
- Chiffrieren: $c = m^e \pmod n$
- Dechiffrieren: $m = c^d \pmod n$

$$p = 47 \quad q = 59 \quad n = 2773 \quad e = 17$$

$$e * d = 1 \pmod{46 * 58} = 1 \pmod{2668}$$

d.h. $d = 157$

HALLO ... => 0801121215....

(Block-)Chiffrieren:

$$0801^{17} \pmod{2773} = 2480$$

$$1212^{17} \pmod{2773} = 2345$$

Dechiffrieren:

$$2480^{157} \pmod{2773} = 801$$

$$2345^{157} \pmod{2773} = 1212$$

„Sicherheit“ von RSA

- 2005 wurde von Wissenschaftlern der Universität Bonn die im Rahmen der RSA Factorization Challenge von RSA Laboratories vorgegebene 200-stellige Dezimalzahl RSA-200 in ihre zwei großen Primfaktoren zerlegt. Die Faktorisierung begann Ende 2003 und dauerte bis Mai 2005. Unter anderem kam ein Rechnerverbund von 80 handelsüblichen Rechnern an der Universität Bonn zum Einsatz.
- Für die Faktorisierung von RSA-1024 (309 Dezimalstellen) oder RSA-2048 (617 Dezimalstellen) sind 100.000 \$ bzw. 200.000 \$ ausgeschrieben.
- Es ist (noch) nicht bewiesen, dass es sich bei der Primfaktorzerlegung um ein prinzipiell schwieriges (z.B., NP-vollständiges) Problem handelt.

Einsatz von RSA

RSA Data Security Inc. (Patent lief 2000 aus)
(<http://www.rsa.com>)



- IPSec
- SSL/TLS
- SET von Visa, Mastercard
- S/MIME (Secure E-Mail)
- (Open)PGP
- Kerberos
- ...



Elektronische Unterschrift

- Berechnung des elektronischen Fingerabdruck (engl. message digest) eines Dokumentes
- Verschlüsselung des Fingerabdruckes mit dem privaten RSA Schlüssel
- Kontrolle
 - Entschlüsselung des Fingerabdruck mit dem öffentlichen Schlüssel des Urhebers
 - Berechnung des Fingerabdrucks und Vergleich beider Werte

Message Digest

- Message Digest (elektronischer Fingerabdruck) wird als Prüfsumme benutzt, um die Echtheit der Daten zu garantieren
 - Hashfunktionen als Einwegfunktionen ohne effiziente Umkehr
 - Erzeugen aus einer beliebig großen Menge von Eingabedaten einen Hashwert (Message Digest) mit fester Länge
- Verbreitete Verfahren
 - MD4 (engl. Message-Digest 4)
 - 1990 von Ronald L. Rivest veröffentlicht. Gilt heute als unsicher.
 - MD5 und SHA-1 (Secure Hash Algorithm 1)
 - erzeugen einen Hashwert mit einer Länge von 128 Bit (hexadezimal notiert), Blockgröße 512 Bit
 - "Franz jagt im komplett verwahrlosten Taxi quer durch Bayern"
 - => a3cca2b2aa1e3b5b3b5aad99a8529074
 - MAC (Message Authentication Code)

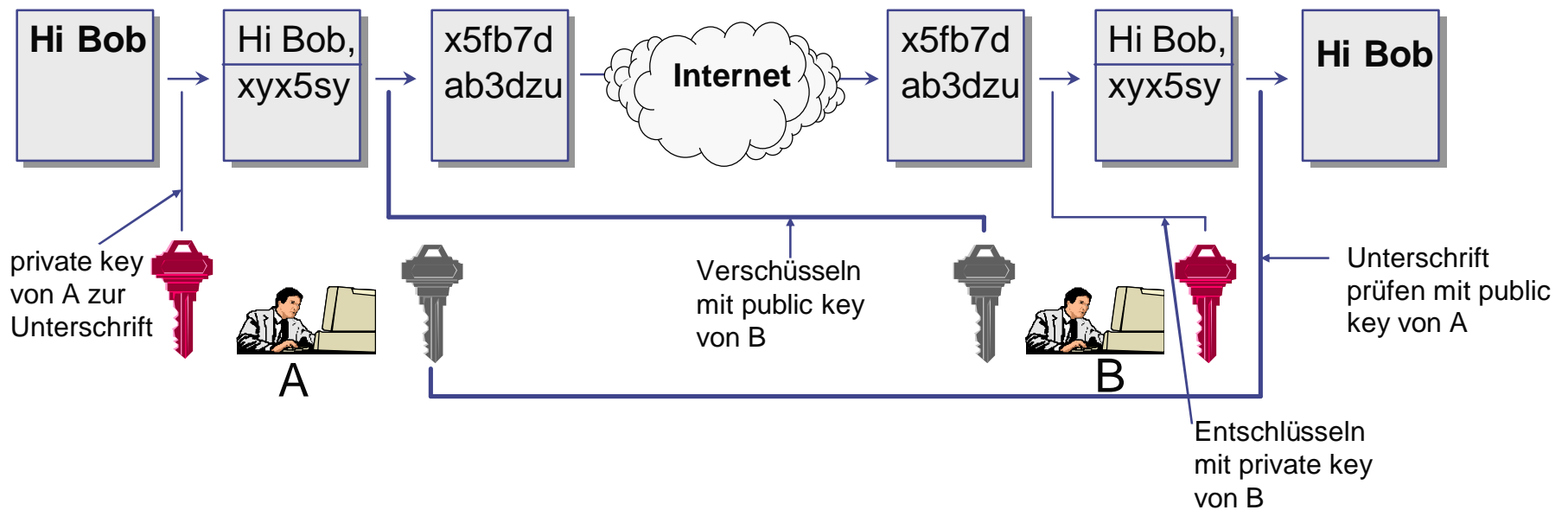
Vor- und Nachteile von Asynchronen Verfahren

- +++ kein geheimer Schlüsselaustausch
- ++ spontane Kommunikation
- + geringe Gesamtanzahl Schlüssel
- + einfaches Hinzutreten / Entfernen von Teilnehmern
- + neue Anwendungsfelder (Signaturen,...)
- Schlüsselmanagement notwendig
- hoher Rechenaufwand notwendig

Kombination von Techniken

- Integrität wird gewährleistet durch Prüfsumme oder *Message Digest*
 - Hash über den Inhalt der Nachricht (128 oder 160 Bit Hash)
- Kombination von symmetrischen und asymmetrischen Verfahren (Verschlüsselung des Session Key)
- Identität kann durch *digitale Unterschrift* sichergestellt werden:
 - Diese wird mit dem Private Key erzeugt und kann mit dem Public Key verifiziert werden
 - Digital unterschriebene *Zeitmarken* können bei Bedarf erstellt werden (z. B. bei beschränkt gültigen Angeboten)

Einsatz von PK-Kryptographie



- Wie kommt der Absender in einem öffentlichen Netz auf zuverlässige Weise an den öffentlichen Schlüssel des Empfängers?

Möglichkeiten der Verteilung

- **Persönlicher Kontakt**
schlecht skalierbar auf große Benutzergruppen
- **Sicherer Kanal (Standleitung, ...)**
nicht immer verfügbar
- **Vertrauenswürdiger Dritter**
am praktikabelsten

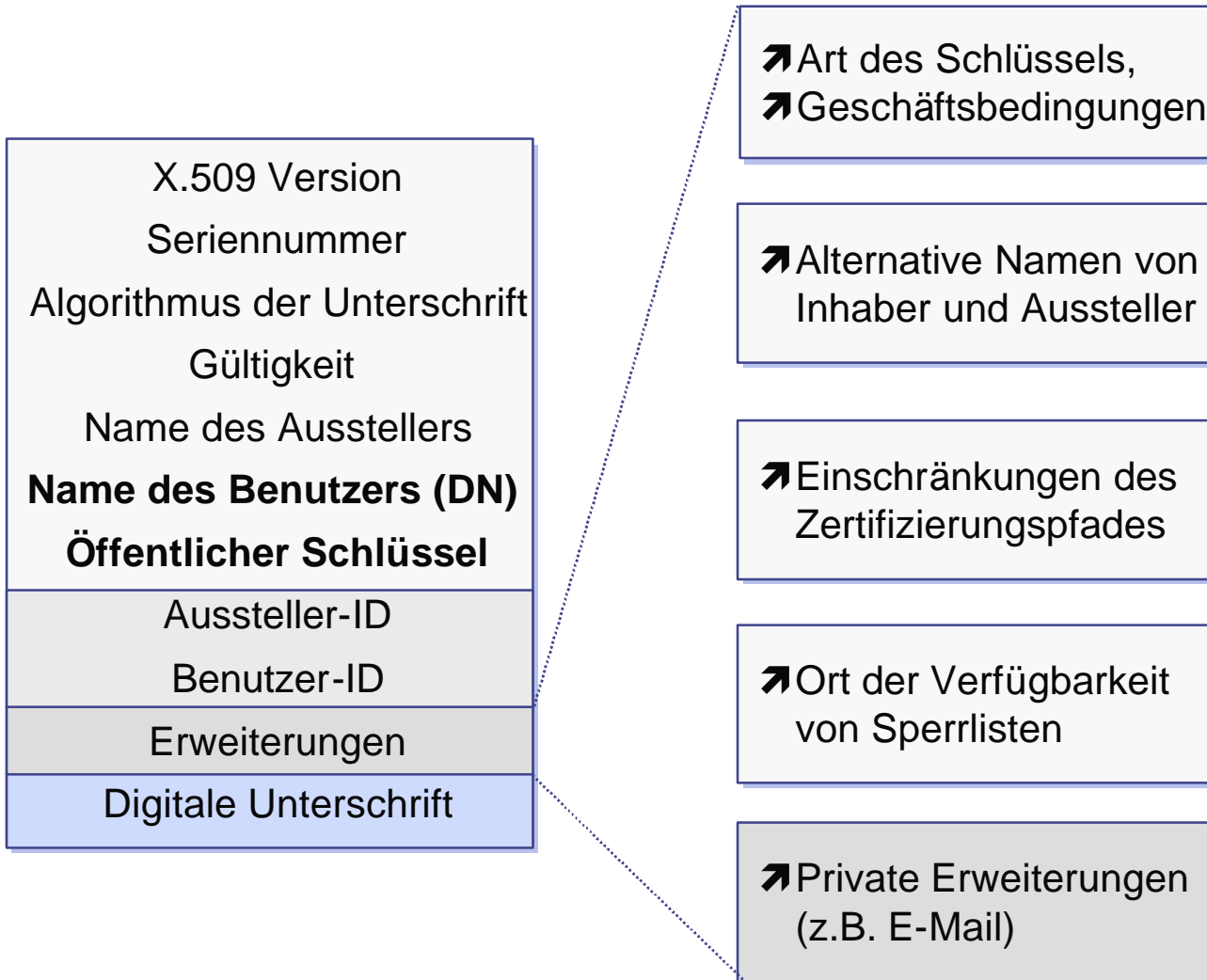


Zertifikate

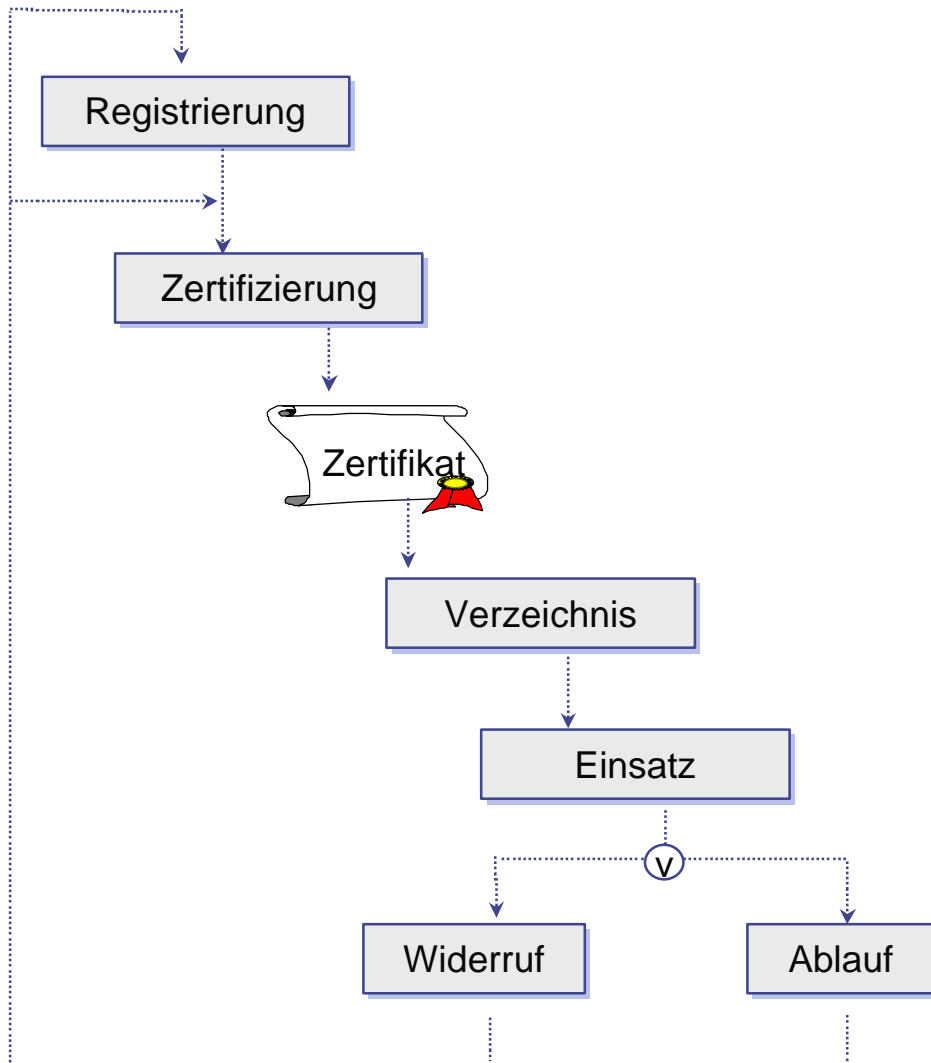
- ◆ Bindung zwischen Benutzer und einem Schlüssel
- ◆ Von einem(!) vertrauenswürdigen Dritten unterschriebener öffentlicher Schlüssel
- ◆ State-Of-The-Practice: Identitäts-Zertifikate für Server und Anwender nach dem Standard X.509 Version 3 (z.B. für S/MIME, SSL)
- ◆ Wesentliche Bestandteile:
 - ◆ Seriennummer
 - ◆ Persönliche Daten
 - ◆ Öffentliche Schlüssel einer Person oder Organisation
 - ◆ Unterschrift der Zertifizierungsstelle
- ◆ Beschränkte Gültigkeitsdauer
 - ◆ Ungültigkeit nach Ablauf der Frist
 - ◆ Möglichkeit des vorzeitigen Widerrufs (*Certificate Revocation*)



Zertifikate nach ITU-T X.509v3



Lebenszyklus eines Zertifikates



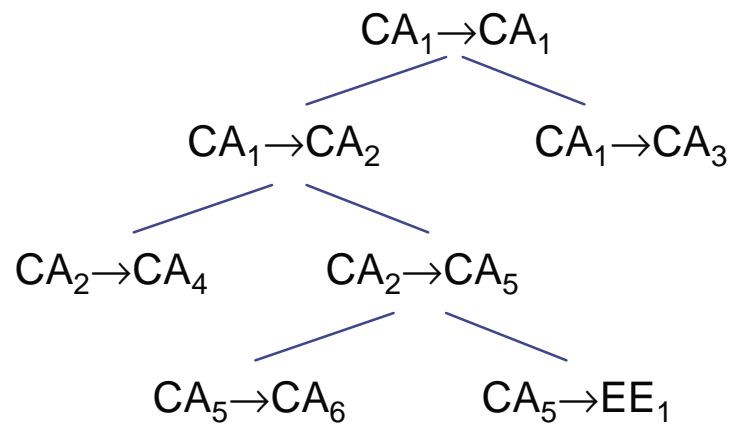
- Schlüsselpaar wird selbst oder von der Registrierungsstelle erzeugt
- Registrierung beinhaltet Erbringung der vorgeschriebenen Identitätsnachweise
- Verzeichnisdienst ermöglicht anderen Benutzern Zugriff auf das Zertifikat
- Bei Widerruf: Publikation des ungültigen Zertifikates über Sperrliste (Certificate Revocation Lists, CRL), RFC 2559

Vertrauensmanagement

- Gegenseitige Zertifizierung von Benutzern
 - z.B. PGP Key Key-Signing-Parties
 - Schwierigkeiten bei verstreuten Benutzergruppen
 - Keine festen Vertrauenspfade (Wem muss ich vertrauen ?)
 - Widerruf von Schlüsseln / Zertifikaten problematisch
 - Keine festen Regeln für die Verteilung der Schlüssel
- Zertifizierungsinstanzen
 - Hierarchisches Vertrauensmodell bei X.509-Zertifikaten
 - Deutsche Telekom, RGB CA, VeriSign, Thawte, ...
 - Zertifizierungsrichtlinien mit Vorgaben zur Überprüfung der Identität
 - Registrierung von Zertifikaten und CRLs in LDAP-Directories

PKI Netzwerke

- Hierarchische CA's

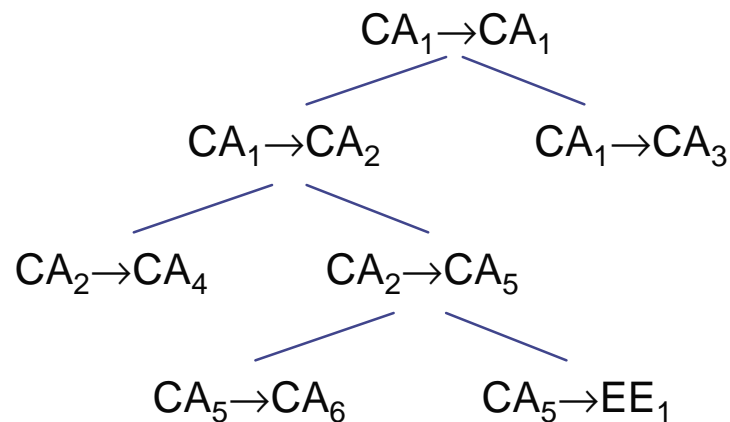


Zur Verifikation von EE_1
folgt man der Kette

$CA_5 \rightarrow EE_1$
 $CA_2 \rightarrow CA_5$
 $CA_1 \rightarrow CA_2$
 $CA_1 \rightarrow CA_1$ ←vertraut

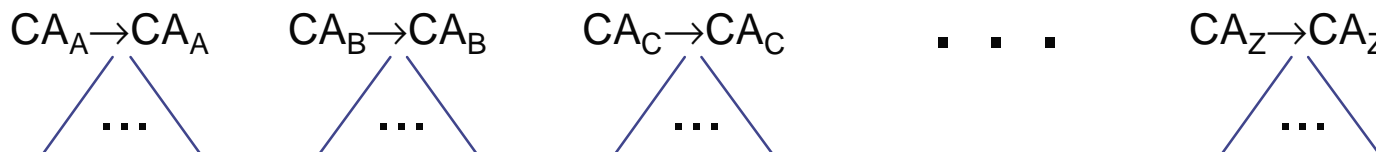
PKI Netzwerke

- Hierarchische CA's



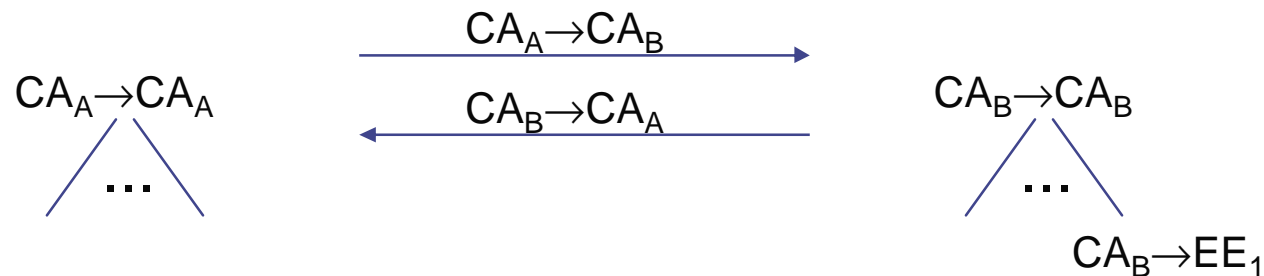
Wenn der private Schlüssel von CA₁ bekannt wird, bricht die Hierarchie zusammen

- Mehrere Wurzelzertifikate (IE, Firefox ...)

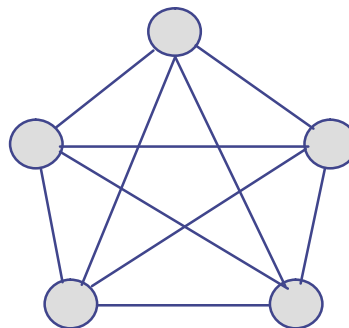


PKI Netzwerke

- Kreuzzertifikation
 - Zwei CA's zertifizieren sich gegenseitig

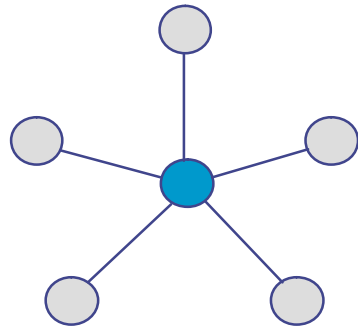


- $N(N-1)$ Kreuzzertifikate sind nötig



Brücken-CAs

- CA als zentraler Hub für mehrere CAs, die sich gegenseitig vertrauen (US Federal Bridge CA, European Bridge CA)



- Prüfung von Zertifikaten

$CA_5 \rightarrow EE_2$

$CA_1 \rightarrow CA_1 \leftarrow \text{vertraut}$

$CA_{\text{Brücke}} \rightarrow CA_5$

$CA_1 \rightarrow CA_{\text{Brücke}}$

PKI Probleme

- Unterschiedliche Voraussetzungen zur Erlangung von Zertifikaten
- Serverzertifikate werden oft nicht von Benutzern überprüft
- Aussagekräftigkeit von Zertifikaten („Josef Maier“, „www.postbank.de“)
- Vertrauen in unterschiedlichste CAs?
- Unachtsamkeiten in Bezug auf private Schlüssel
- Sicherheit von privaten Rechnern
- etc.

Gesetzliche Rahmenbedingungen

- In Deutschland ist das Signaturgesetz seit Mai 2001 in Kraft.
- Durch einen Zusatz im BGB § 126 a ist die qualifizierte Signatur der eigenhändigen Unterschrift weitgehend gleichgestellt.
- Bis auf Ausnahmen wie z.B. Bürgschaften, Kündigung von Arbeitsverträgen und Zeugnisse können Dokumente und Verträge elektronisch signiert werden und sind auch vor Gericht als Beweismittel anerkannt.
- Beweislastumkehr: Bei einem qualifiziert elektronisch signierten Dokument muss bewiesen werden, dass die Signatur ungültig ist, wenn jemand das anzweifelt.

Das Signaturgesetz

- Das Signaturgesetz unterscheidet zwischen einer *einfachen*, einer *fortgeschrittenen* und einer *qualifizierten elektronischen Signatur*.
- Der Beweiswert einer einfach signierten E-Mail ist vor Gericht gering, wenn nicht weitere Indizien für die Authentizität vorgetragen werden.
- Fortgeschrittene Zertifikate ermöglichen die Identifizierung des Signaturschlüssel-Inhabers und dass Änderungen der Daten, auf die sie sich beziehen, nachträglich erkannt werden können.
- Die qualifizierte elektronische Signatur wird der handschriftlichen Signatur gleichgestellt.

Qualifizierte elektronische Signaturen

- Die *qualifiziert zertifizierte elektronische Signatur* muss „auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer *sicheren* Signaturerstellungseinheit erzeugt worden sein.
 - Oberste Aufsichtsbehörde ist die Regulierungsbehörde für Post- und Telekommunikation (RegTep).
 - Bei den qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung i.S.v. § 15 Abs. 1 S. 4 SigG wird die Sicherheit durch gesetzlich anerkannte fachkundige Dritte gewährleistet.
- Zur Erstellung einer qualifizierten elektronischen Signatur muss eine „sichere Signaturerstellungseinheit“ eingesetzt werden.

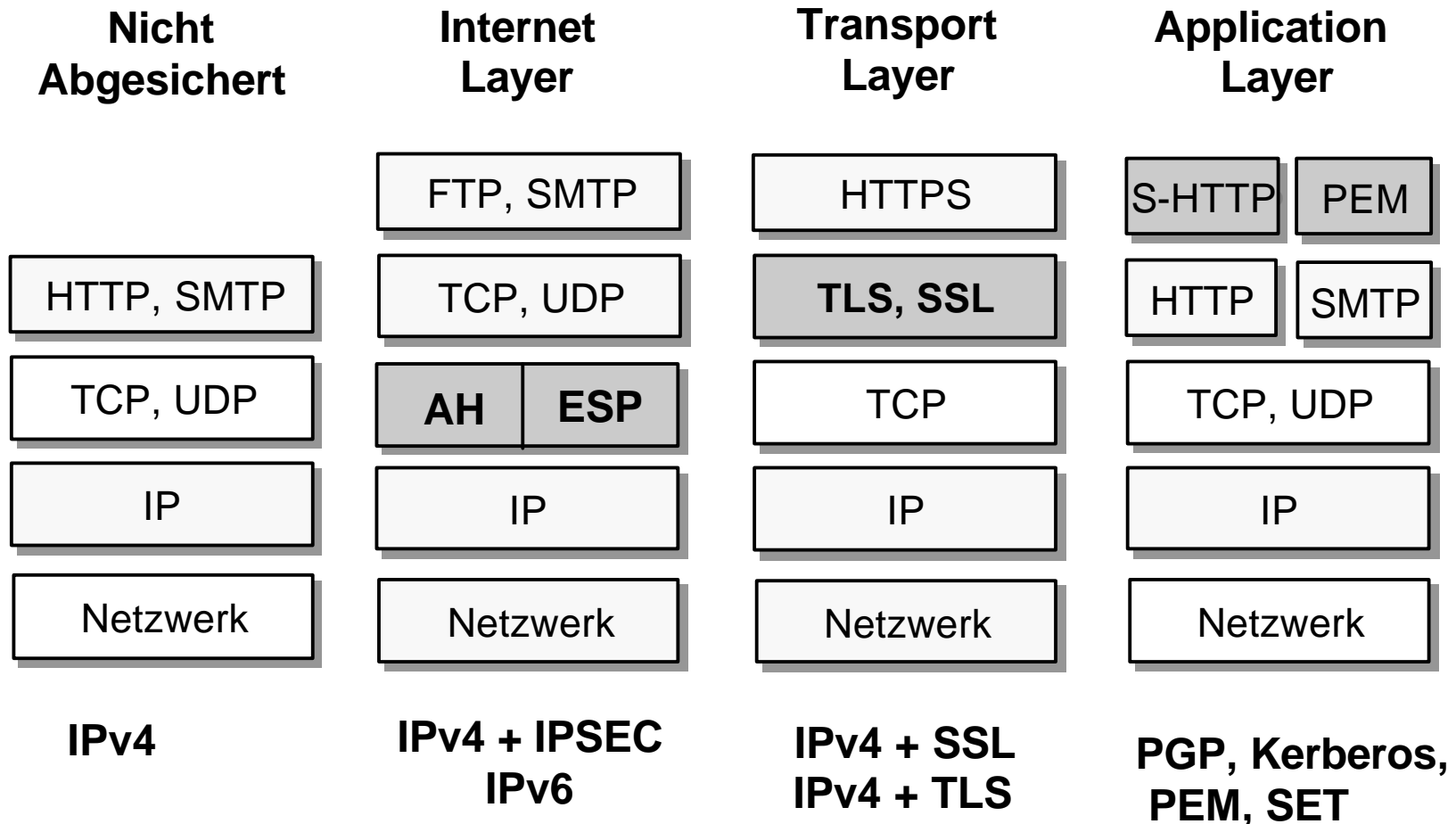
Ausführungspraxis Chipkarten

- Derzeit erfüllen lediglich bestimmte Chipkartenleseeinheiten diese hohen Sicherheitsanforderungen.
- Chipkarten enthalten einen Private Key, der während des Signiervorgangs durch Eingabe einer – ebenfalls auf der Chipkarte hinterlegten - PIN (Nutzer-Identifizierung) zur Erstellung einer Signatur verfügbar wird.
- Die Beweisführung bei qualifizierten Signaturen, dass der Karteninhaber NICHT signiert hat, obliegt damit dem Karteninhaber.
- Das Problem können durch Manipulationen am Kommunikationskanal zwischen Karte und Codierungssoftware entstehen.

Signaturkarten-Anbieter und Kartenlesegeräte

- Liste der durch die Regulierungsbehörde für Telekommunikation und Post akkreditierten Signaturkarten-Anbieter und Zertifizierungsdiensteanbieter
 - <http://www.bundesnetzagentur.de/>
- Information des Bundesamt für Sicherheit in der Informationstechnik BSI unter
 - <http://www.bsi.bund.de/esig/>
- Beispielanwendung: CO₂-Emissionshandel

Absicherung der Internet-Protokolle



Was leistet IPSec

- Gewährleistung der Authentizität der Gesprächspartner
- Integrität der übertragenen Daten
- Vertraulichkeit der übertragenen Daten
- Schutz gegen Replay-Angriffe (Aufnehmen und Wiederspielen von Daten)
- Schlüssel Management

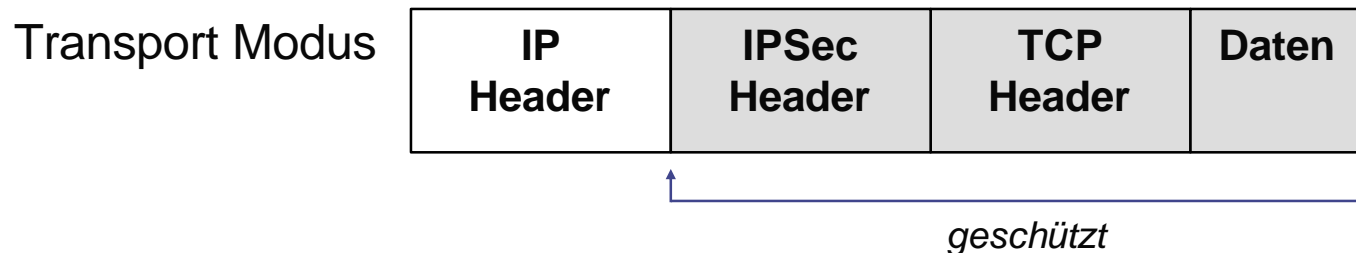
- IPSec kann in zwei unterschiedlichen Modi betrieben werden
 - Transport modus (Meist zwischen zwei Systemen (PCs))
 - Tunnelmodus (Als Tunnel zwischen zwei, oder mehreren Standorten)

IPSec Sicherheitsprotokolle

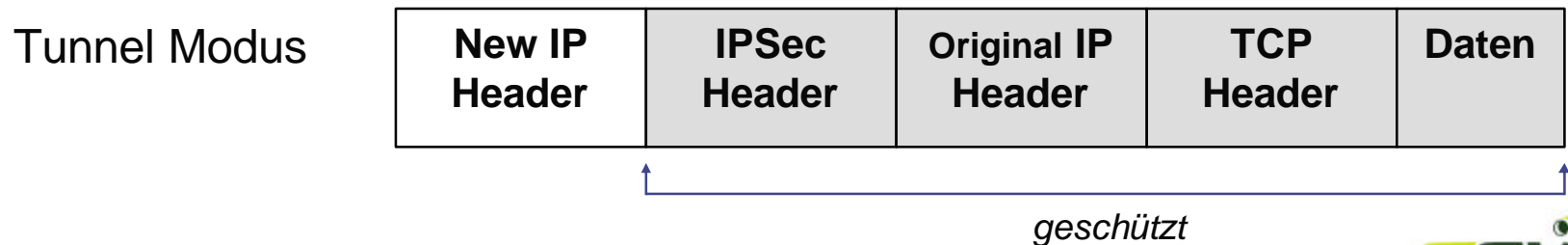
- Authentication Header (AH):
 - Prüft **Echtheit eines Paketes** sowie die **Integrität** der Daten während ihrer Übertragung
 - Mit Hilfe einer **Sequenznummer** kann sich der Empfänger vor Angriffen schützen, die aus einer mehrmaligen Wiederholung desselben Paketes hervorgehen können.
- Encapsulating Security Payload (ESP) bietet:
 - wird verwendet, um vertrauliche **Daten zu verschlüsseln** und ihre Integrität zu garantieren.
- Beide Protokolle können alleine oder zusammen verwendet werden
- Parallele Entwicklung ähnlicher Merkmale in IPv6
- Einsatz zur Realisierung von Virtual Private Networks (VPN) auf OSI-Schicht 3

IETF IPsec Erweiterung von IPv4

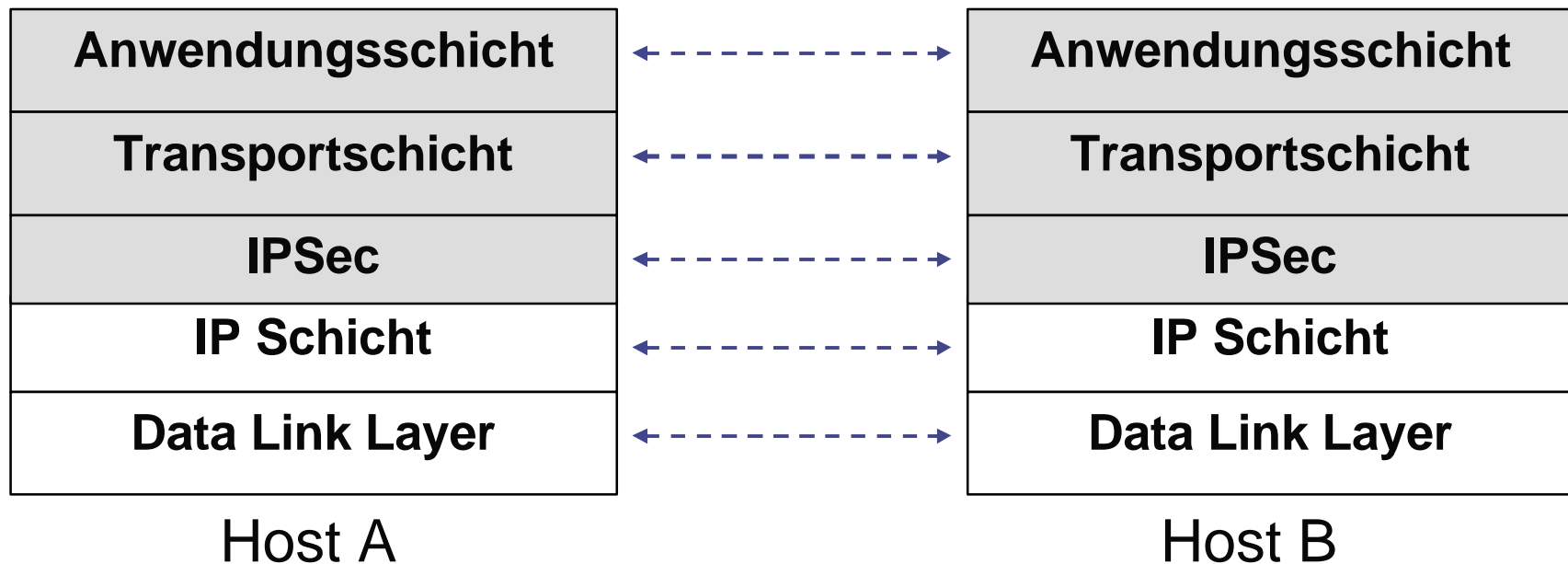
- Transport Modus: Schützt die oberen Schichten
 - Nur die Daten werden verschlüsselt, nicht der originale IP-Kopf



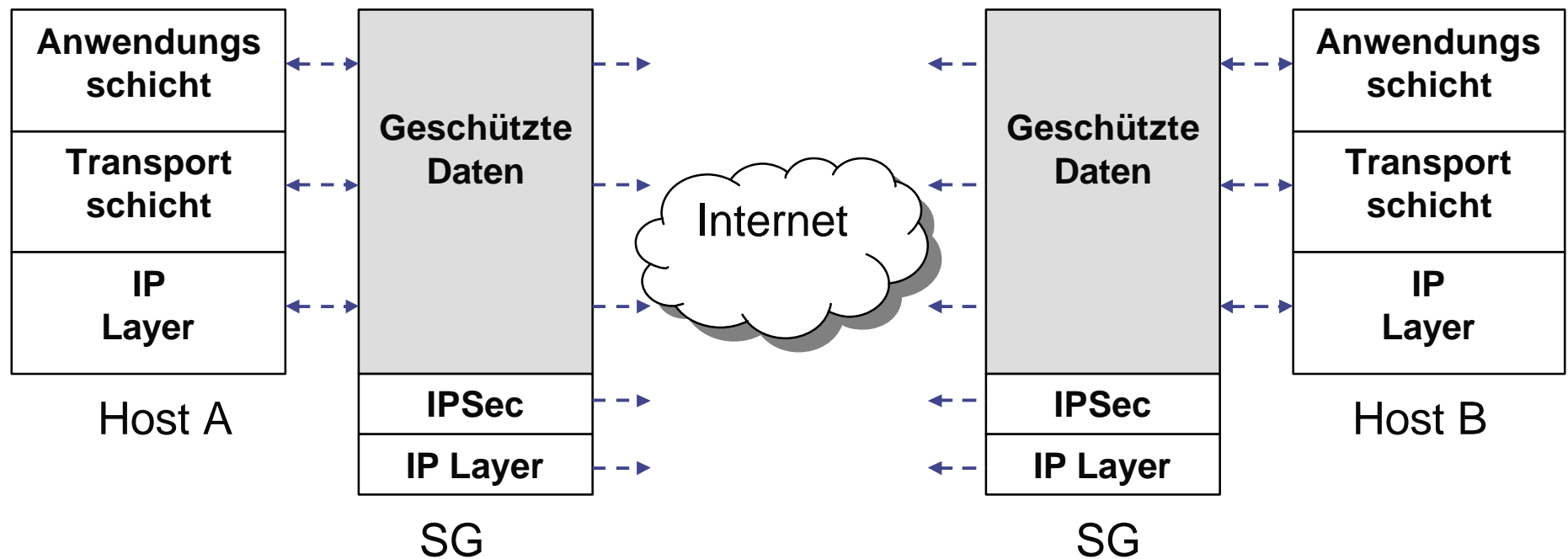
- Tunnel Modus: Schützt die gesamte IP Übertragung



Transport Modus



Tunnel Modus



SG = Security Gateway: Es wird ein neuer IP-Header erzeugt, der nur die IP-Adressen des SG beinhaltet und nicht der eigentlichen Kommunikationspartner

Schlüsselverwaltung bei IPSec

- IPSec Internet Key Exchange (IKE), RFC 2409
 - Der Schlüsselaustausch dient zum Austausch von Sessionkeys.
 - Verhandelt symmetrische Verschlüsselungsalgorithmen und asymmetrische Signaturalgorithmen.
- IPSec sieht die Schlüsselverwaltung in zwei verschiedenen Arten vor:
 - Manuell: der symmetrische Schlüssel wird statisch auf jedem Client hinterlegt (Pre Shared Key (PSK))
 - Automatisch: der symmetrische Schlüssel wird automatisch erzeugt, bzw. in Intervallen erneuert (RSA)

SSL / TLS

- ◆ *Secure Sockets Layer* ursprünglich von Netscape
- ◆ Handshake auf Basis von RSA
- ◆ Offener Standard
 - ◆ Spezifikation frei verfügbar
 - ◆ Programmbibliotheken erhältlich
- ◆ Applikationsunabhängig
 - ◆ WWW(!), News, FTP verfügbar
- ◆ IETF Transport Layer Security (TLS, RFC 2246) als leichte Weiterentwicklung von SSL v3.1

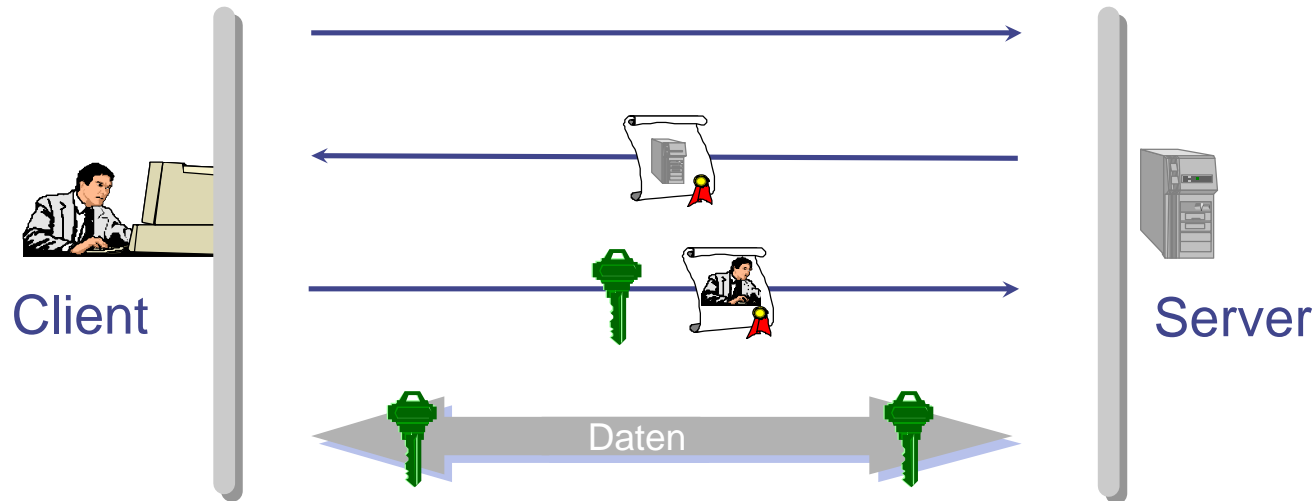
Anwendungs-
Protokoll

SSL/TLS

TCP/IP

Netzwerk-
Zugang

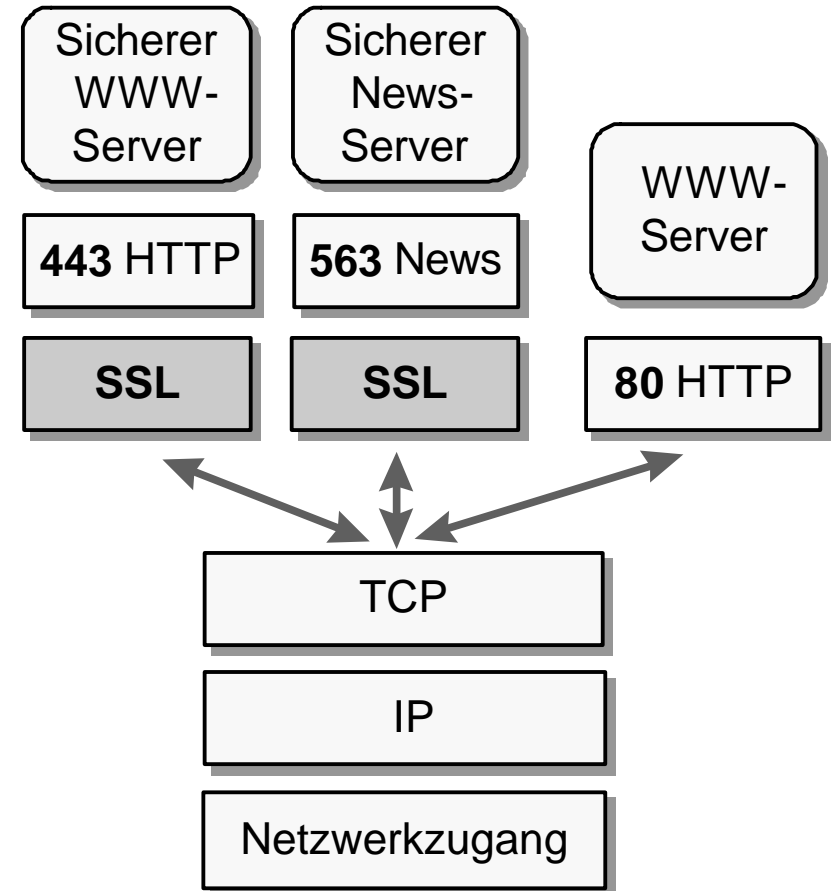
Überblick: SSL - Handshake



- ◆ Authentifizierung durch X.509-Zertifikate
 - ◆ Obligatorisch im Falle des Servers
 - ◆ Optional für den Klienten
- ◆ Aushandeln der Parameter für symmetrische Verschlüsselung

SSL - Funktionsumfang

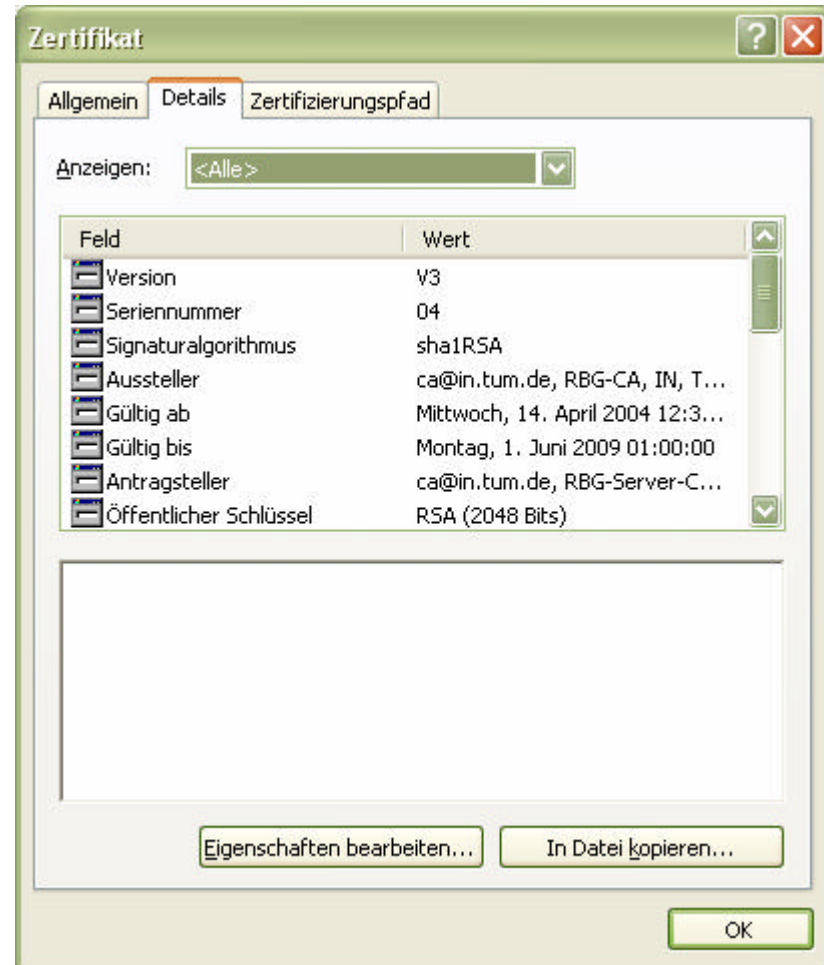
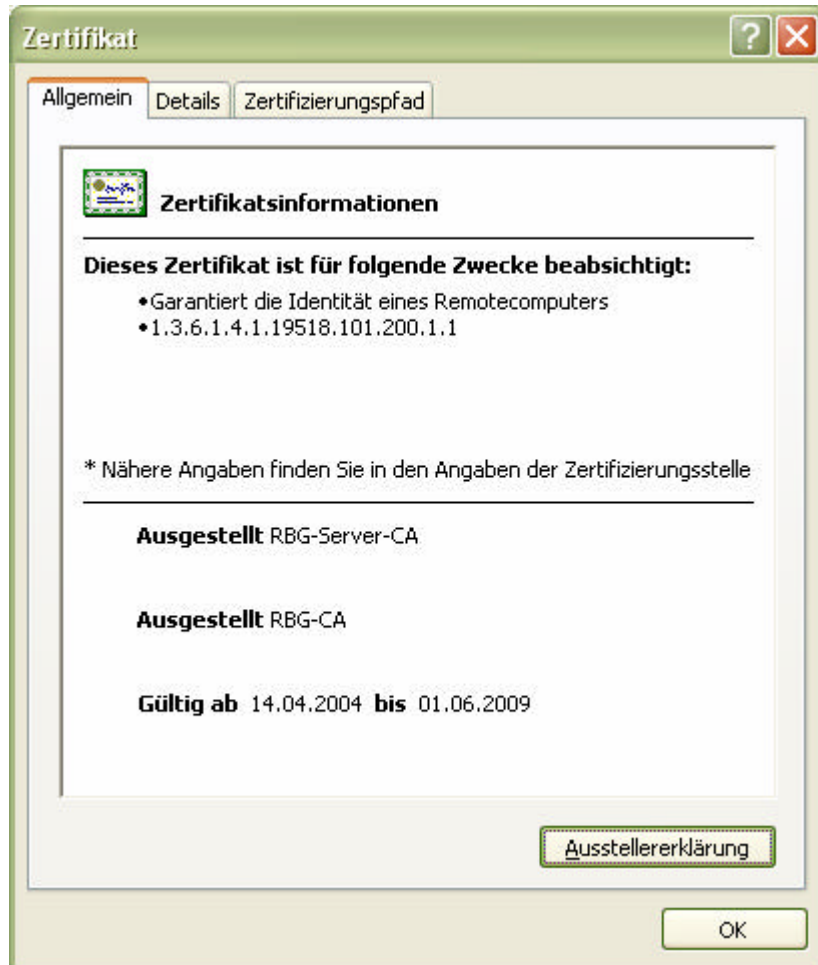
- Sicherheits-Handshake
 - Abgleich Versionsinformation
 - Authentifizierung des Servers vorgeschrieben
 - Authentifizierung des Client möglich
 - Austausch eines Session Keys
- Verschlüsselung des Datenstromes
 - Nach erfolgtem Handshake und Einigung auf gemeinsames Verfahren
 - Integritätsüberprüfung der Daten mit *Message Digest*
- Neuinitialisierung auf Wunsch eines der beiden Teilnehmer



State-of-the-Practice

- Entsteht 1993 mit Entwicklung von SSL
- Primäres Ziel: Server-Authentifizierung für Electronic-Commerce-Anwendungen
- Flaches Vertrauensmodell, mehrere Zertifikate sind Bestandteil des WWW-Browser (z.B.: Netscape, Internet Explorer)
- Server müssen von einer dieser Stellen zertifiziert werden
- Zertifizierungsstellen-Software auch für den unternehmensinternen Bereich erhältlich
- Benutzer-Zertifikate werden langsam verbreitet
- Fast alle Browser und Server setzen bevorzugt TLS mit RSA- und AES-Verschlüsselung ein

Zertifikate im Internet Explorer

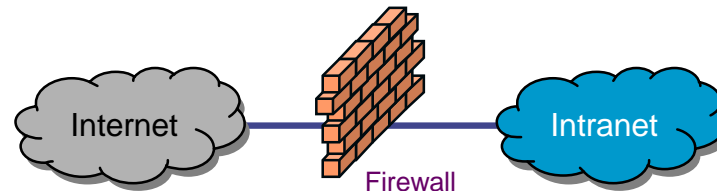


Allgemeine Sicherheitsanforderungen

- ✓ Vertraulichkeit / Geheimhaltung
 - ✓ Kein Zugang zu Informationen für nicht-authorisierte Teilnehmer
- ✓ Integrität
 - ✓ Schutz der Daten vor unberechtigter Veränderung
- ✓ Unabstreitbarkeit
 - ✓ Nachweis der Urheberschaft
- ✓ Authentifikation
 - ✓ Zuverlässige Feststellung der Identität
- Zugriffskontrolle
 - Regelt den Zugriff auf Objekte oder Informationen
- Verfügbarkeit
 - Vorhandensein von Ressourcen und Daten für rechtmäßige Benutzer

Firewalls

- Firewalls als eine spezielle Art der Zugriffskontrolle
- Zentrale Kontrollinstanz beim Zugriff auf private Netze
 - Das private Netz kann nur über die Firewall betreten oder verlassen werden.
 - Schafft einen klar definierten Zugriffspunkt für Zugriffe von außen
 - Verhindert, dass Angreifer alle Rechner erreichen können



Ziele von Firewalls

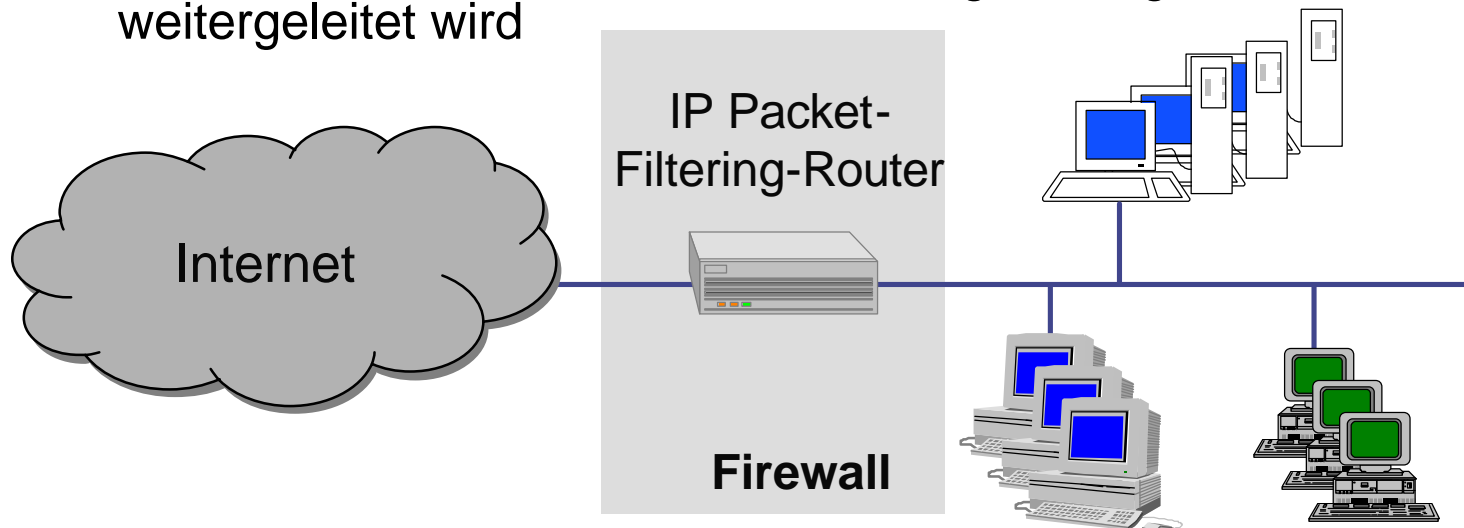
- Zugangskontrolle auf Netzwerkebene
- Zugangskontrolle auf Benutzerebene
- Rechteverwaltung
- Kontrolle auf der Anwendungsebene
- Beweissicherung und Protokollauswertung
- Alarmierung
- Verbergen der internen Netzstruktur

Wichtige Firewalltypen

- Packet Filtering Firewalls
 - Circuit Level Gateways
 - Application Level Gateways
- } Proxies
- Die wenigsten professionellen Firewalls gehören nur einer einzigen Kategorie an
 - Meistens werden verschiedene Typen kombiniert

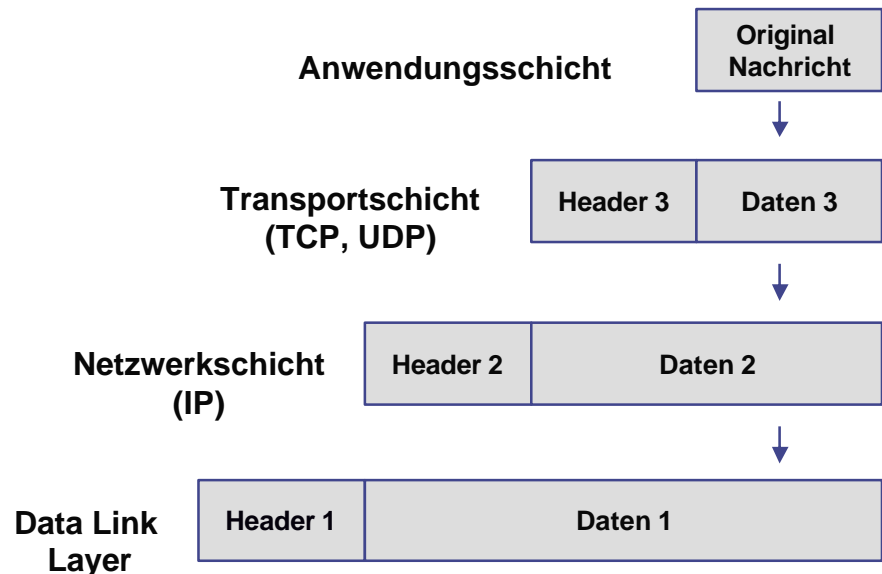
Packet-Filtering-Firewalls

- Arbeiten auf der Schicht 3 und 4 des OSI-Modells bzw. des TCP/IP Modells
 - Abhängig vom TCP- und IP-Header der Pakete und von den Regeln kann die Firewall das Paket ablehnen, es weiterleiten oder eine Nachricht zum Ursprung zurücksenden
- Sind oft Teil eines Routers
 - Router erhält Pakete von einem Netzwerk und leitet sie an ein anderes Netzwerk weiter
 - Jedes Paket wird mit einer Anzahl Regeln verglichen, bevor es weitergeleitet wird



Selektionskriterien von Paket-Filtern

- IP-Adressen im IP Header
- Portnummern im TCP/UDP Header
- Protokollnummern (Datagrammtyp) je nach benutztem Service (TCP/UDP/...) unterschiedlich
- SYN-/ACK-Flag zur Richtungsfeststellung (TCP)



nach diesen Kriterien wird das Paket dann jeweils gefiltert

Politik von Paket-Filtern

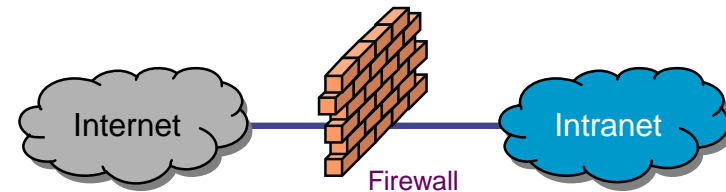
- Zwei Arten von Regeln

- **Gebotsregeln (Allow)**

Alles, was nicht explizit erlaubt ist, ist verboten

- **Verbotsregeln (Deny)**

Alles was nicht explizit verboten ist, ist erlaubt



- Die erste Strategie ist der zweiten vorzuziehen

Beispiel

Nr	Typ	Quell-adr.	Ziel-adr.	Quell-port	Ziel-port	Aktion
1	TCP	*	123.4.5.6	>1023	23 (SSH)	Allow
2	TCP	*	123.4.5.7	>1023	80 (WWW)	Allow
3	TCP	129.6.48.254	123.4.5.8	>1023	22 (telnet)	Allow
6	*	*	*	*	*	Deny

Stärken von Paket-Filtern

- Paketfilterung ist eine kostengünstige Technologie
- Paketfilter ist heute auf fast allen Router-Produkten standardmäßig implementiert
- Kaum zusätzlicher Administrations- und Konfigurationsaufwand notwendig
- Paketfilterregeln können dem Benutzer kommuniziert werden
- Sie sind leicht erweiterbar, wenn neue Dienste oder Protokolle transportiert werden müssen (hinzufügen neuer Regeln reicht im Normalfall)

Schwächen von Paket Filtern

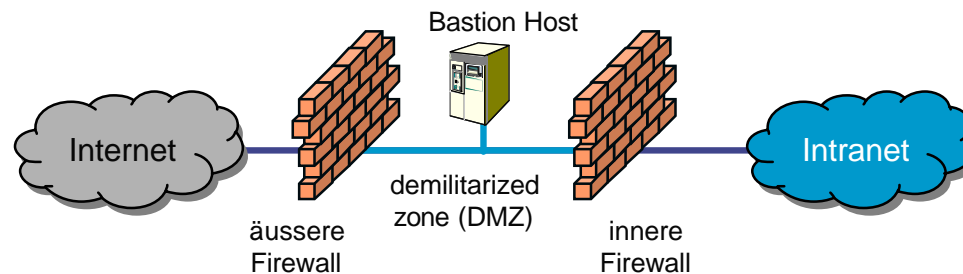
- Bei großen Netzen können Filterregeln sehr umfangreich und schwer nachvollziehbar werden
- Protokollmeldungen enthalten oft keine Informationen über Inhalt der übertragenen und verworfenen Pakete
- Einige Protokolle sind für Paket Filter ungeeignet, da variable Portnummern verwendet werden
- Unzureichende Integrität der Portnummern und IP-Adressen, da diese gefälscht werden können (IP-Spoofing)
- Keine Benutzerauthentifizierung
- Keine Kontrolle der Inhalte der Datagramme

Circuit-Level-Gateways

- Arbeiten auf der Transport-Schicht des OSI-Modells bzw. auf der TCP-Schicht (4) des TCP/IP-Modells
- Ermöglicht Kontrolle ganzer Verbindungen
- Überwachen das TCP-Handshaking zwischen Paketen von vertrauenswürdigen Servern oder Clients und nicht vertrauenswürdigen Hosts und umgekehrt, um herauszufinden, ob eine Session legitim ist oder nicht
- Um Pakete auf diesem Weg zu filtern, benutzen Circuit Level Gateways die Daten im Header des TCP-Protokolls
- Wurde das Handshaking als legitim erkannt baut das C.-L.-Gateway die Verbindung auf und die Pakete werden nur noch hin und her transportiert ohne weiteres Filtern

Circuit-Level-Gateways (2)

- Wurde die Verbindung geschlossen wird sie aus der Tabelle gelöscht
- Filterung von „Verbindungen“, nicht auf Anwendungsebene
- Ein C.-L.-Gateway agiert als Proxy gegenüber dem Client als Server und gegenüber dem Server als Client
- Meist auf sog. Bastion Host installiert
- Beispielarchitektur:



Application Level Gateways

- Arbeiten auf der Anwendungsschicht, d.h. Filtern spezieller Anwendungen
- Für jeden Dienst wird ein spezifisches Proxyprogramm auf dem Application-Level-Gateway eingesetzt (telnet, SMTP, FTP, HTTP)
- Nutzdatenanalyse ist möglich
 - Daten können analysiert und z.B. nach bestimmten Schlüsselwörtern durchsucht werden (z.B. E-Mail, HTML-Seiten)
 - Intrusion Detection – Feststellen auffälliger Zugriffsmuster
- Möglichkeit der Einschränkung von bestimmten Dienstmerkmalen
- Cache Funktionalität für Webseiten

Zusammenfassung: Application-Level-Gateways

- Bieten ein hohes Maß an Sicherheit
- Sehr umfangreiche Protokollierung ist möglich
- Authentisierung des Benutzers kann vorgenommen werden (im Gegensatz zu Packet Filtering)
- Dienste können benutzerabhängig erlaubt werden
- Allerdings: Höherer Rechenaufwand nötig

Ungelöste Probleme

- Eingeschränkter Zugriff auf erwünschte Dienste
- Kein Schutz gegen Tunneling (z.B. IPSec)
- Kein Schutz gegen 'Angriffe von Innen'
- Keine Kontrolle über 'Hintertüren' (z.B. Modems)
- Evtl. Durchsatzprobleme
- Kein Schutz gegen Viren und Mail Bomben

Literatur

- Pflichtliteratur:
 - Hansen, H. R.; Neumann, G.: Wirtschaftsinformatik 2, Informationstechnik, 9. Auflage, *Kapitel 6.8*, Lucius&Lucius, 2005.
- Vertiefende Literatur:
 - Bauer, F. L. (2000). Entzifferte Geheimnisse. Berlin et al.: Springer
 - Schneier, B. (1996). Angewandte Kryptographie. Bonn et al.: Addison-Wesley
 - Chapman, B., Zwicky, E. (1995) Building Internet Firewalls, O'Reilly.
 - Eckert, C. (2001) IT-Sicherheit, Oldenburg Verlag.