Sicherheitsproblematik und Kryptographie

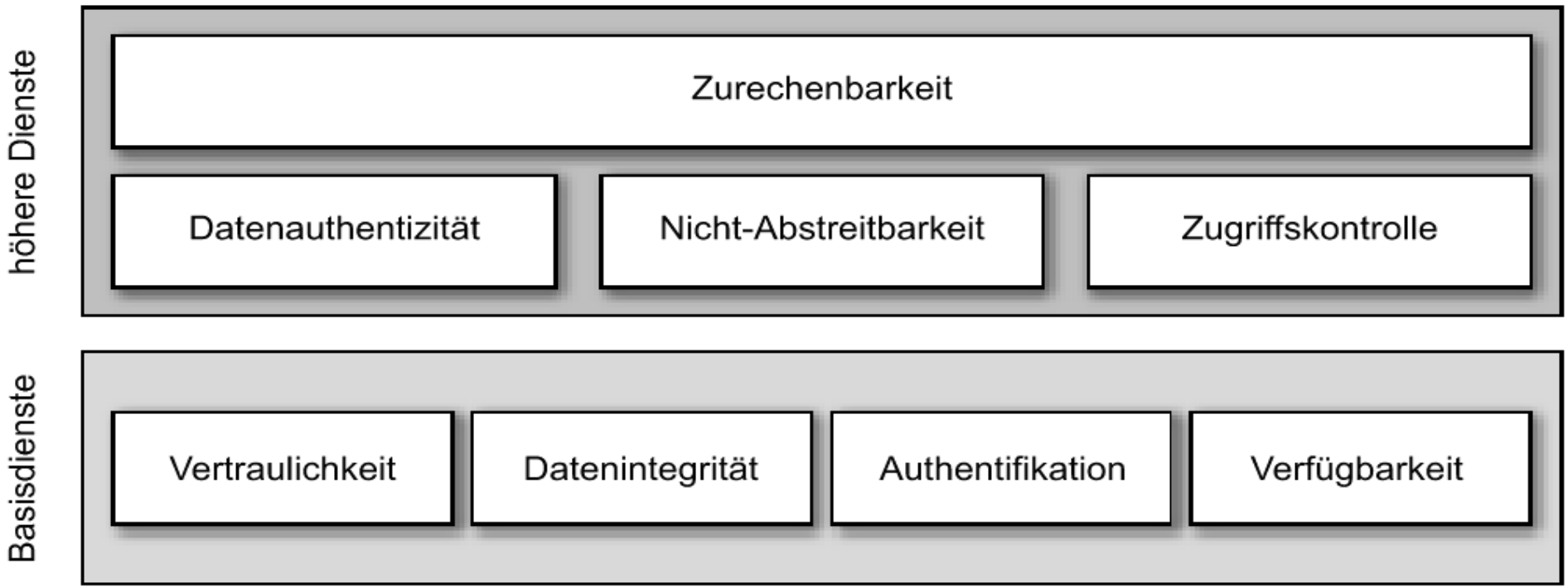
- Sicherheitsproblematik
- Transaktionssicherheit im WWW
- Kryptographische Verfahren
- Sichere Protokolle: IPv6, SSL, PCT ...
- Zertifikate zur Identifikation
- Elektronische Signaturen



Sicherheitstechnische Aspekte

- Datensicherheit (engl.: data security)
  - beinhaltet die Verhinderung von Datenverlust, Datendiebstahl und Datenverfälschung
  - Durch vorbeugende Maßnahmen soll die jederzeitige Vollständigkeit und Korrektheit der Daten gewährleistet werden

Schema für informations-technische Sicherheitsdienste



Sicherheitsdienste

- Vertraulichkeit (engl.: confidentiality)
  - verhindern, dass geheime Information für unberechtigten Dritten zugänglich wird
- Datenintegrität (Unveränderthеit, kurz: Integrität, engl.: data integrity)
  - garantieren, dass Daten in unveränderter Form (im „Originalzustand“) vorliegen
- Authentifikation (engl.: authentication)
  - nachweisliche Identifikation eines Benutzers oder eines Kommunikationspartners

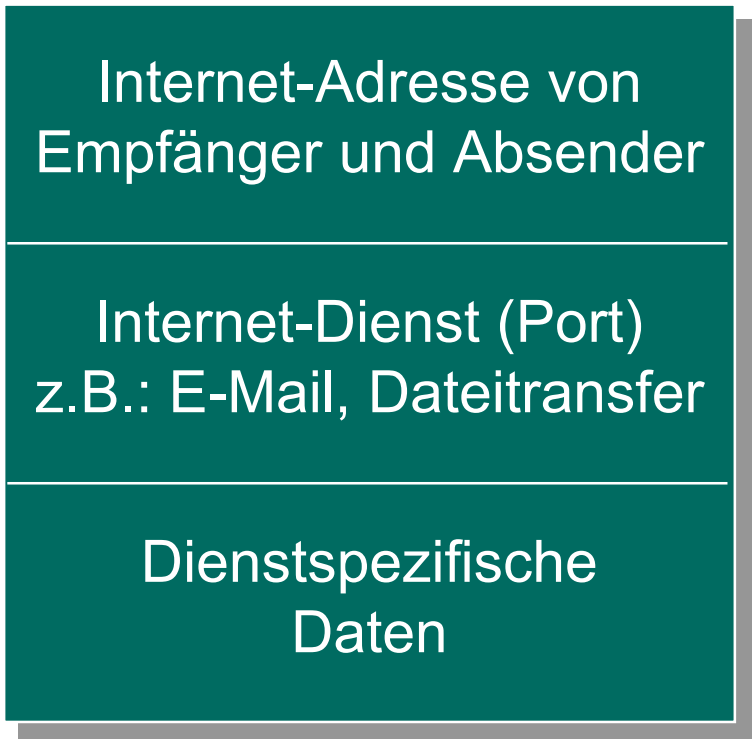
Sicherheitsdienste

- Verfügbarkeit (engl.: availability)
  - Garantie, dass Dienste, die berechtigten Benutzer eines IS angeboten werden, diesem auch stets zur Verfügung stehen
- Datenauthentizität
  - nachweisliche Identifikation (Integrität und Herkunft) von Information
- Nicht-Abstreitbarkeit (engl.: non-repudiation)
  - gewährleisten, dass Absender das Versenden einer Meldung ebenso wenig abstreiten kann wie Empfänger den Erhalt einer Meldung

Sicherheitsdienste

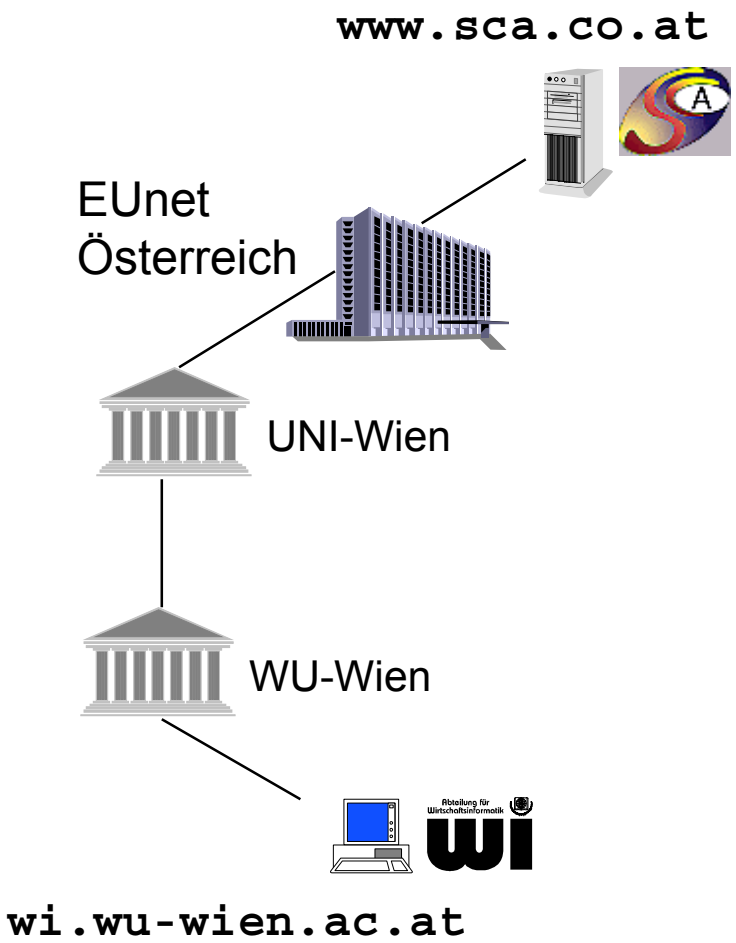
- Zugriffskontrolle (engl.: access control)
  - basiert auf korrekter Authentifikation von Benutzern (und Programmen)
  - befasst sich mit Autorisierung von Zugriffen, um jedem Benutzer ausschließlich die Aktionen zu gewähren, welche ihm auf Grund seiner Legitimation erlaubt sind
- Zurechenbarkeit (engl.: accountability)
  - baut auf Zugriffskontrolle und Nicht-Abstreitbarkeit auf
  - protokolliert, welche Benutzer welche Systemressourcen in Anspruch genommen haben

Sicherheitsproblematik - IP



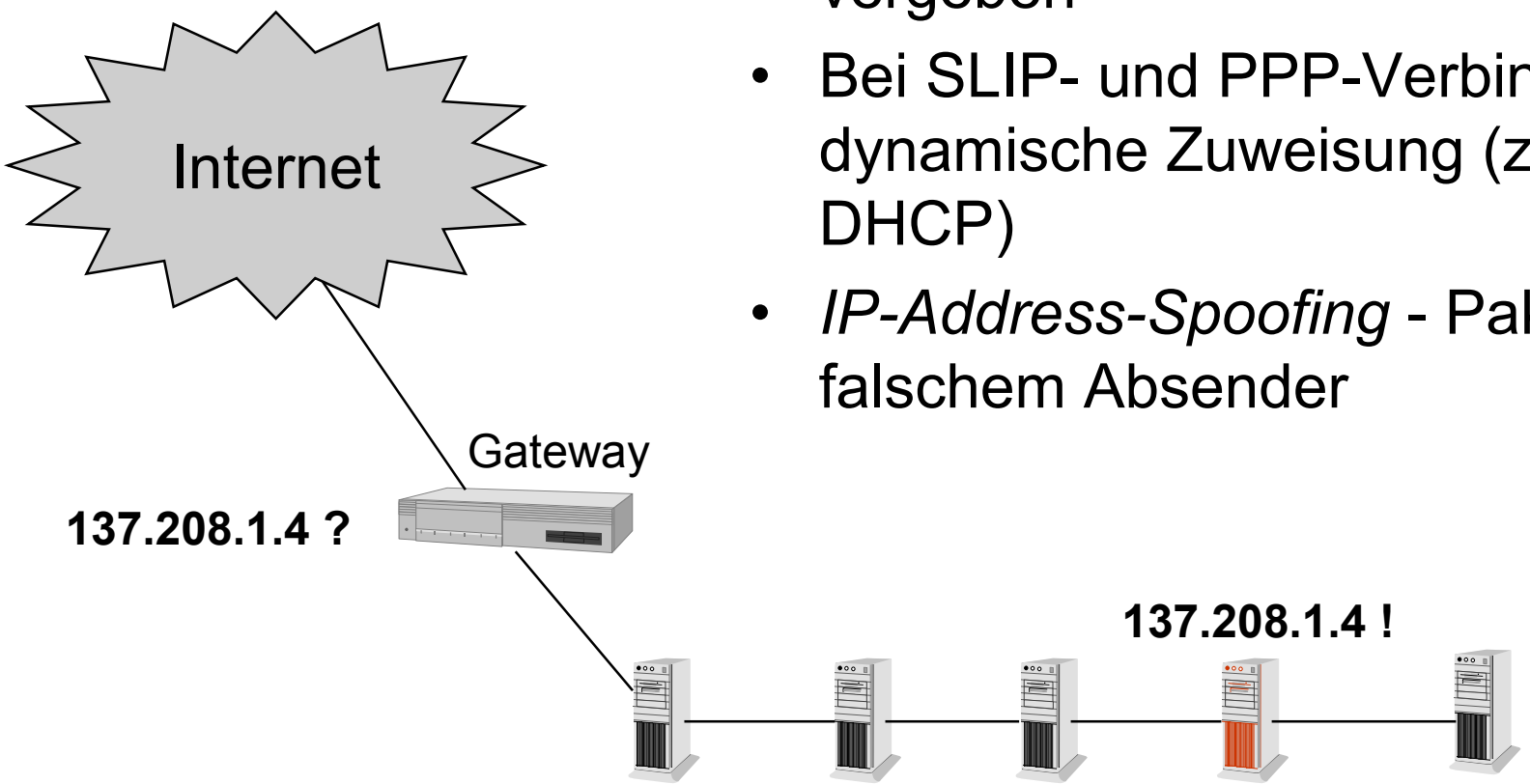
- Übertragung der Protokollelemente der Anwendungsebene im Klartext (Kennwörter)
- Internet-Address-Spoofing zur Umgehung von Firewalls
- Inhalt der Pakete ist modifizierbar

Sicherheitsproblematik Routingvorgang



- 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
- Routingvorgang ist unsicher

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

Transaktionssicherheit

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.

Konsequenzen

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

- Authentifizierung mit Zertifikaten, Einsatz globaler Public-Key-Infrastrukturen
- Kryptographisch abgesicherte Übertragung (SSL, S-HTTP, PEM)
- Abschottung des unternehmensinternen Netzwerkes von der Außenwelt (Firewall)

Kryptographische Verfahren

Symmetrische Verfahren

DES (Data Encryption Standard)	Fixe Schlüssellänge 56 Bit,
Triple-DES	Fixe Schlüssellänge 168 Bit
RC2, RC4 (Algorithmus unveröffentlicht)	Keine fixe Schlüssellänge
IDEA	Fixe Schlüssellänge 128 Bit

Hash-Verfahren

MD2, MD5	128 Bit Hash
SHA	160 Bit Hash

Asymmetrische Verfahren (Public Key Verfahren)

Diffie-Hellman	Erstes Verfahren, nur digitale Unterschrift
RSA	1978 entwickelt; bekanntestes Verfahren. Variable Schlüssellängen (Üblich sind 512 - 2048)
DSS	Digital Signature Standard, maximal 1024 Bit.

Beispiel für asymmetrische Schlüssel

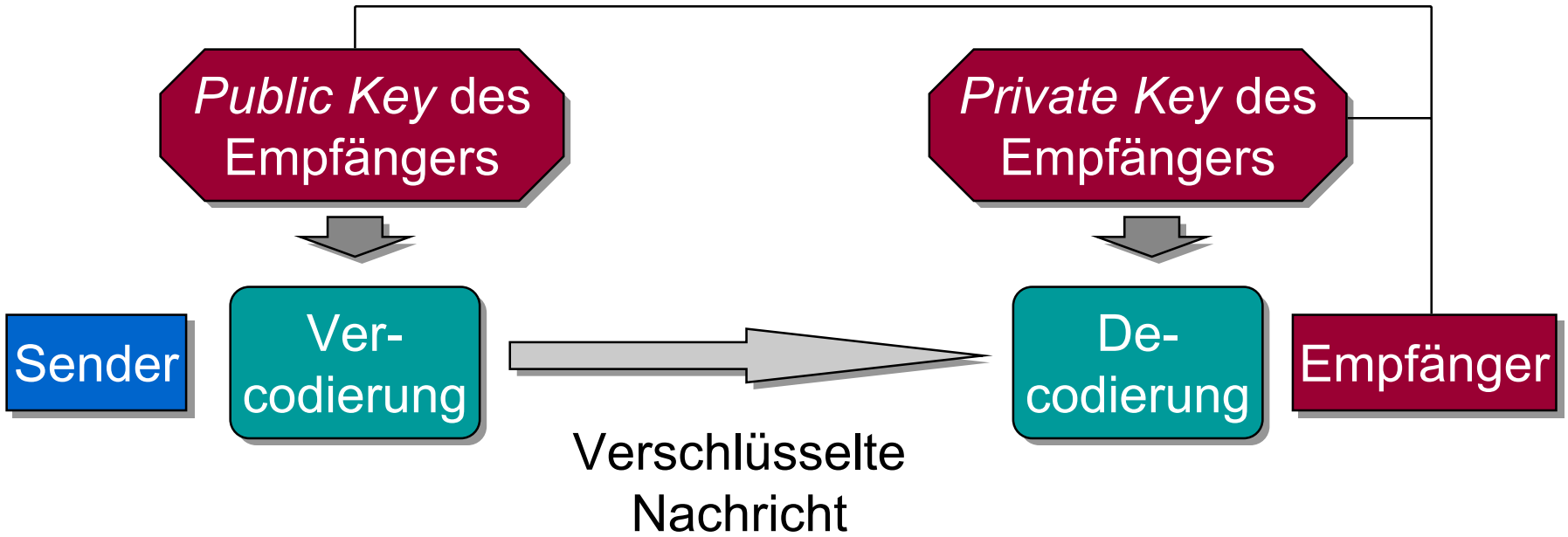
- RSA-Verfahren

1. Buchstaben werden Zahlen zugeordnet: 01 für A, 02 für B,… und 26 für Z

z.B.	W	I	R	T	S	C	H	A	F	T
	23	09	18	20	19	03	08	01	06	20

2. Verschlüsselt Produkt zweier hinreichend großer Primzahlen (p und q)
   z.B. n = 2773 (2773 = 47 × 59) und Primzahl e, die sich aus p, q und d (hier d=157) berechnet: $1 = d \times e \bmod (p-1) \times (q-1)$, hier daher e = 17
3. Da zwei Buchstaben höchstens die Zahl 2626 (Z = 26) erzeugen können und 2626 kleiner als 2773 ist, werden je zwei Buchstaben als Block zusammengefasst, z.B. 2309, 1820, …, 1100
4. Blöcke werden mit $Block_{neu} = Block_{alt}^{\ e} \bmod n$ verschlüsselt
   z.B. 2309 wird verschlüsselt zu 1717 = $230917 \bmod 2773$
5. Entschlüsselt wird durch $Block_{neu}^{\ d} \bmod n = Block_{alt}$
   z.B. $1717^{157} \bmod 2773 = 2309$

Public Key Kryptographie

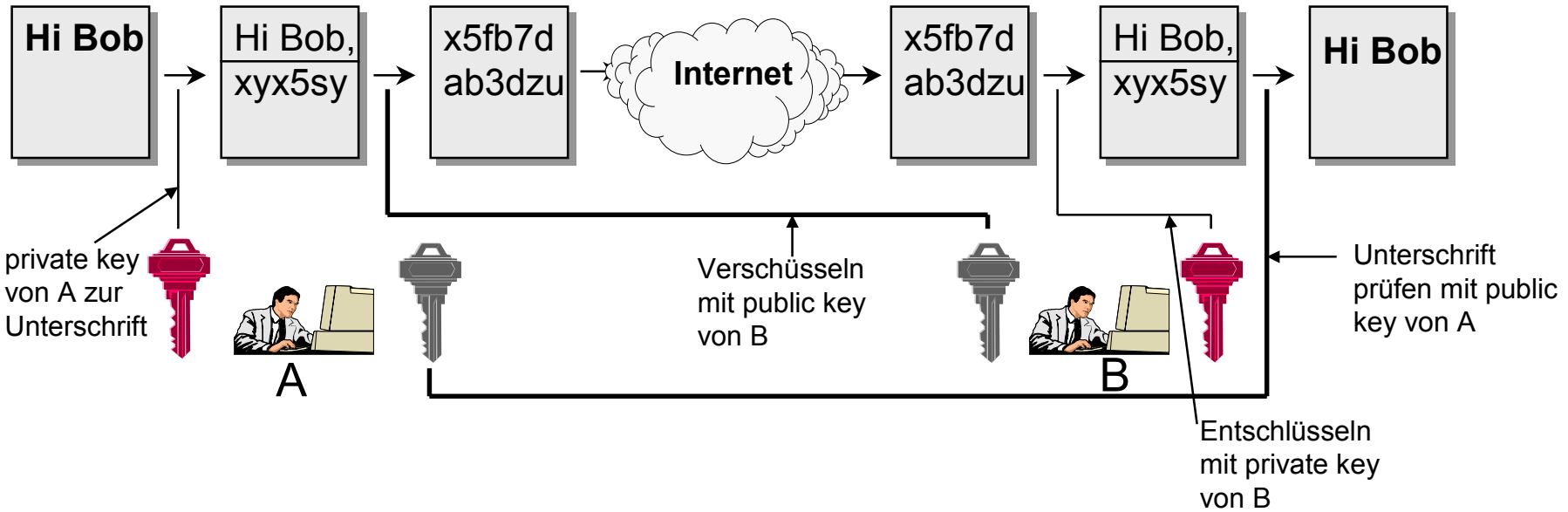


- Eine mit einem Public Key verschlüsselte Nachricht kann nur mit *zugehörigem* Private Key entschlüsselt werden.

Public-Key-Kryptographie

- Integrität wird gewährleistet durch *Message Digest* - Hash über den Inhalt der Nachricht.
- Identität kann durch *digitale Unterschrift* sichergestellt werden. Diese wird mit dem Private Key erzeugt und kann mit dem Public Key verifiziert werden.
- Möglichkeit: Digital unterschriebene *Zeitmarken* können bei Bedarf erstellt werden (z. B. bei beschränkt gültigen Angeboten).
- Beispiel Algorithmen von Public-Key-Systemen:
  - Diffie-Hellman; Logarithmus
  - RSA (Rivest - Shamir - Adleman); Faktorisieren vom Produkt zweier Primzahlen

Einsatz von PK-Kryptographie



- Wie kommt der Absender in einem öffentlichen Netz auf zuverlässige Weise an den öffentlichen Schlüssel des Empfängers ?
- Aus Performance-Gründen meist nur digitale Unterschrift eines Message Digest.

Einsatz von PK-Kryptographie

Copyright für RSA-Algorithmus hat die RSA Data Security Inc. (http://www.rsa.com).



Einige Lizenznehmer und Produkte sind :

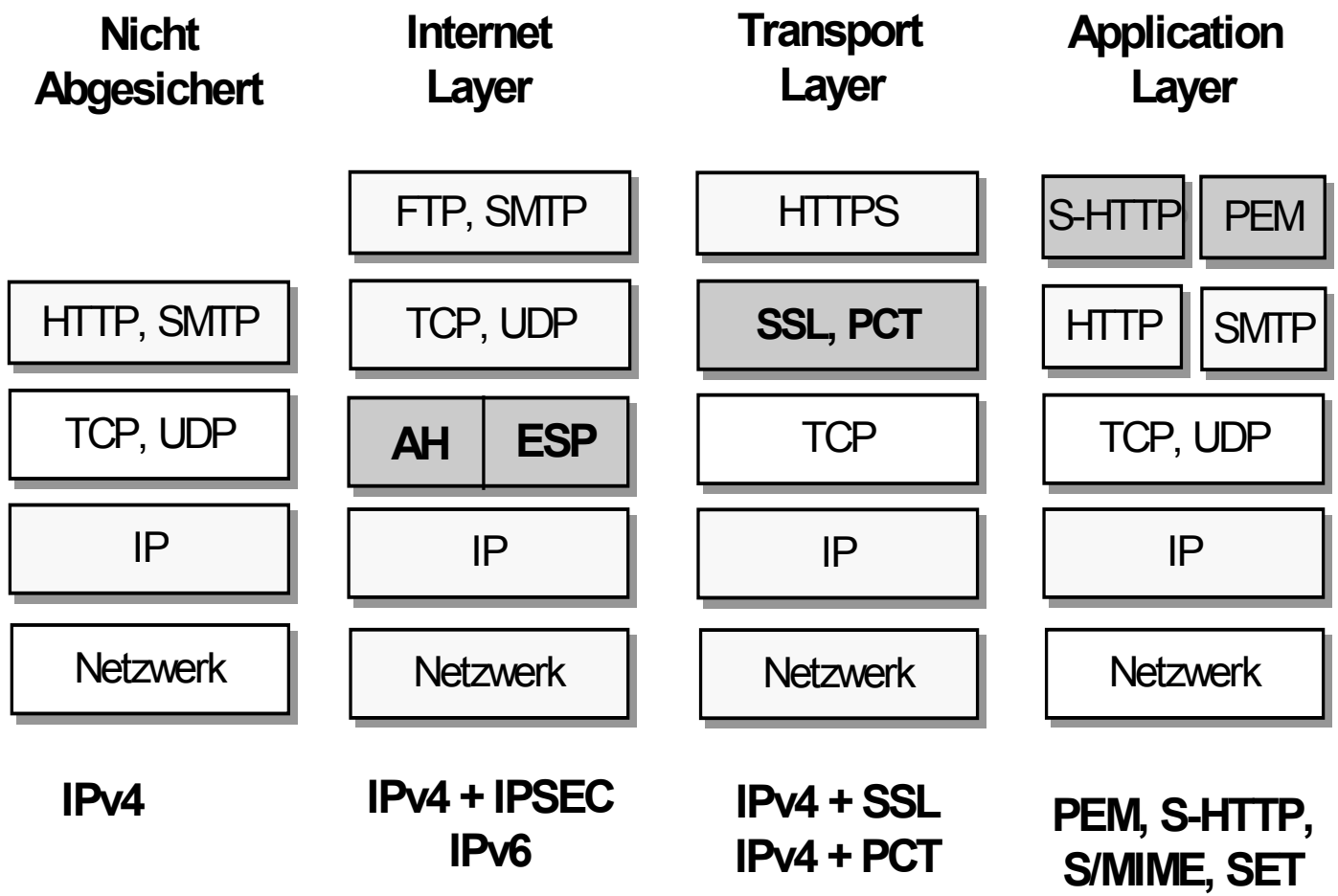
- SSL von Netscape
- PCT von Microsoft
- S-HTTP von EIT
- Ecash von Digicash
- SET von Visa,Mastercard
- S/MIME (Secure E-Mail) von Microsoft, Lotus

„Knacken“ des RSA-Verfahrens

- Zahlen p, q und d sind geheim und lassen sich nur mit sehr hohem Aufwand aus n und e berechnen

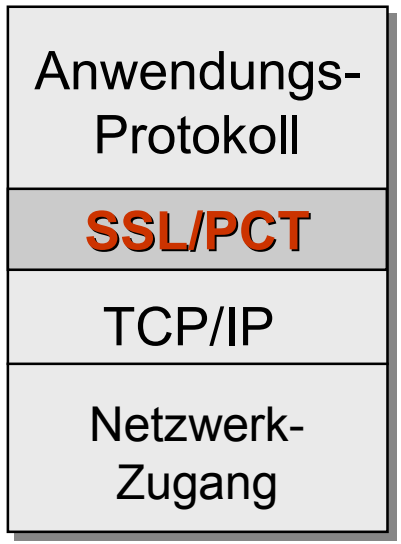
Stellen der Zahl	**Rechen-operationen**	**Rechenzeit** (Annahme eine Operation = 10^{-6} Sekunden)
50	$1{,}4 \times 10^{10}$	3,9 Stunden
70	$9{,}0 \times 10^{12}$	104 Tage
100	$2{,}3 \times 10^{15}$	74 Jahre
200	$1{,}2 \times 10^{23}$	$3{,}8 \times 10^{9}$ Jahre

Absicherung der Internet-Protokolle



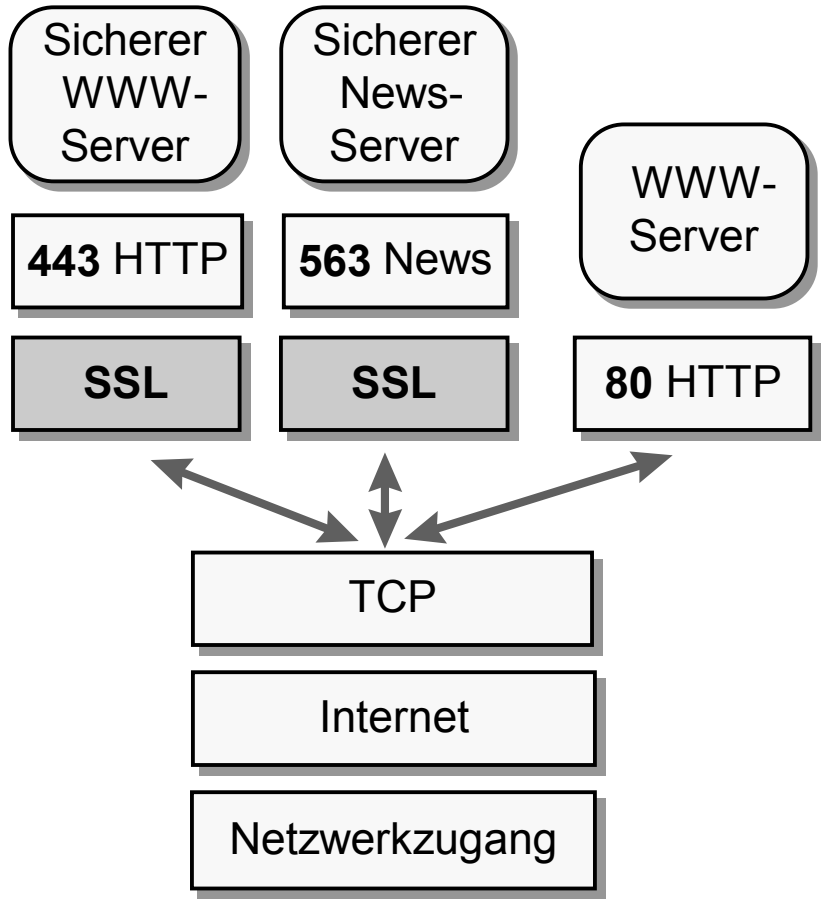
Transport Layer Security: SSL und PCT

- *Secure Sockets Layer* von Netscape
- Offener Standard
  - Spezifikation frei verfügbar
  - Programmbibliotheken erhältlich
  - Weiterentwicklung durch Netscape
- Applikationsunabhängig
  - WWW, News, FTP verfügbar
  - Zahlreiche SSL-basierte Erweiterungen sind im Entstehen
- *Private Communications Technology* von Microsoft
  - Schneller Verbindungsaufbau
  - Derzeit zu SSL kompatibel, nahezu ident mit SSLv3
- Standardisierungsbemühungen durch die IETF
  - TLS-Working Group

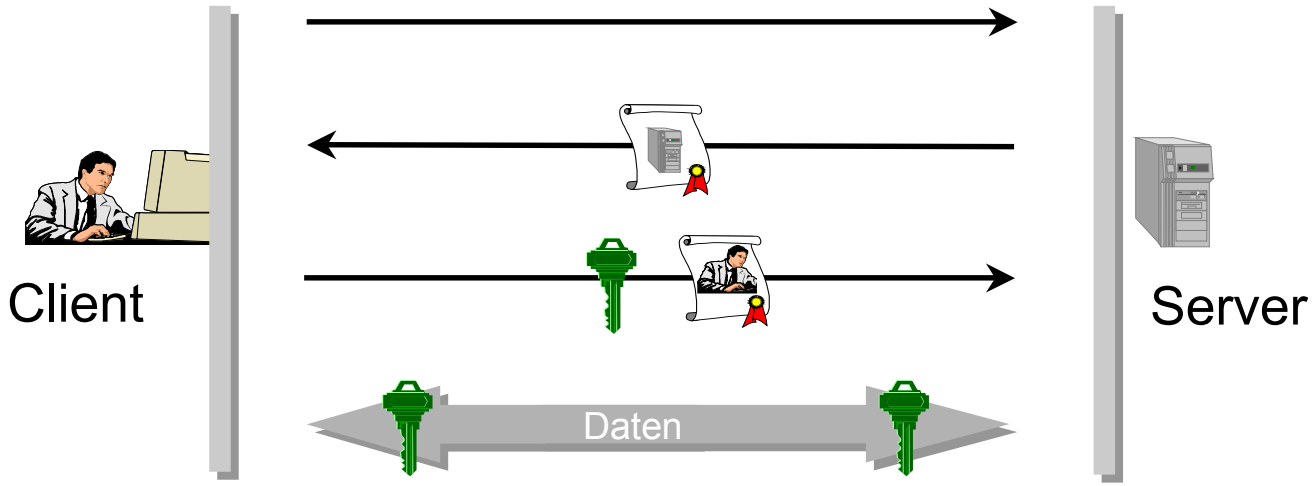


SSL - Funktionsumfang

- 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



Überblick: SSL - Handshake



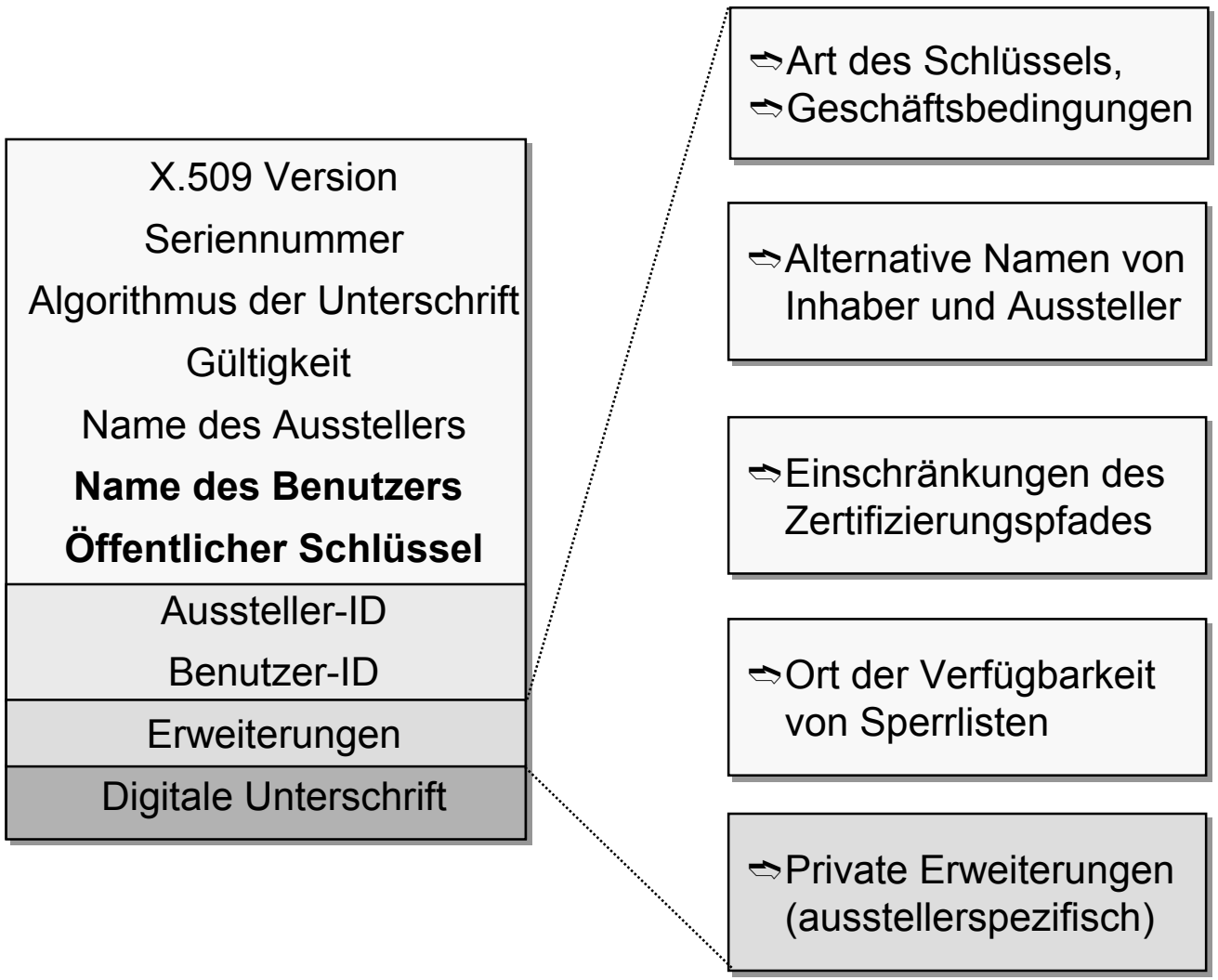
- Authentifizierung durch X.509-Zertifikate
  - Obligatorisch im Falle des Servers
  - Optional für den Klienten
- Aushandeln der Parameter für symmetrische Verschlüsselung

Zertifikate

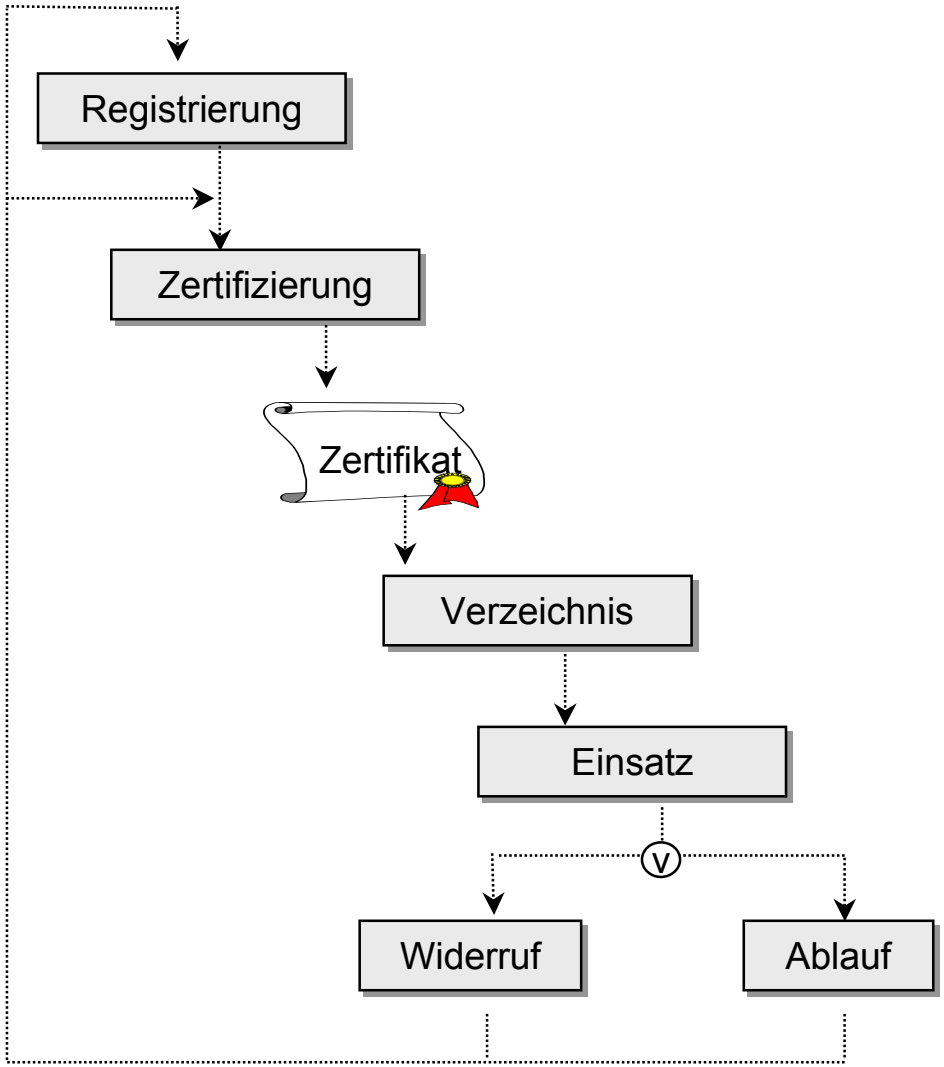


- Von der Zertifizierungsstelle unterschriebener öffentlicher Schlüssel
- Wesentliche Bestandteile:
  - Seriennummer
  - Persönliche Daten (Name, Firmenzugehörigkeit)
  - Öffentliche Schlüssel einer Person oder Organisation
  - Unterschrift der Zertifizierungsstelle
- Von Dritten leicht überprüfbar
- Beschränkte Gültigkeitsdauer
  - Ungültigkeit nach Ablauf der Frist
  - Möglichkeit des vorzeitigen Widerrufs (*Certificate Revocation*)
- State-Of-The-Practice: Identitäts-Zertifikate für Server und Anwender nach dem Standard X.509 Version 3

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.

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 Communicator, Internet Explorer)
- Beispiel Zertifizierungsstelle: RSA-Tocher Verisign (www.verisign.com)
- Server müssen von einer dieser Stellen zertifiziert werden
- Zertifizierungsstellen-Software auch für den unternehmensinternen Bereich erhältlich (Netscape, Xcert)
- Benutzer-Zertifikate werden zunehmend langsam verbreitet

Installation eines „sicheren“ WWW-Servers

- Installation der Software
- Starten des “unsicheren” Servers zur Durchführung der Konfiguration (beliebiger Port)
- Schlüsselerzeugung (Kommandozeile)
- Mail an Zertifizierungsstelle
  - Nachweis der persönlichen Angaben
  - Schlüsseldatei mit dem generierten *öffentlichen* Schlüssel
- Einbinden des erteilten Zertifikates (nach Erhalt der digitalen Unterschrift der CA)
- Starten des sicheren Servers

Funktionalität von WWW-Browsern



- Kennzeichen einer abgesicherten Verbindung
  - URL: https
  - Optische Präsentation, Hinweis bei Verbindungsauf- und -abbau
- Sichere Verbindung bedeutet
  - Verbindungspartner besitzt gültiges Zertifikat
  - Server wurde eindeutig identifiziert
  - Weitere Datenübertragung erfolgt verschlüsselt
- Anzeige des Verschlüsselungsstatus eines Dokuments
- Verwaltung von Zertifizierungsstellen
- Verwaltung von persönlichen Zertifikaten
- Vertrauens-Management nicht standardisiert!
  - Wie werden neue CA-Zertifikate hinzugefügt ?
  - Wie werden Zertifikate von unbekannten CAs behandelt ?

Verschlüsselungsstatus eines Dokuments

Verschlüsselungsverfahren:

This is a secure document that uses a medium-grade encryption key suited for U.S. export (RC4-40, 128 bit with 40 secret).

Zertifizierungsstelle:

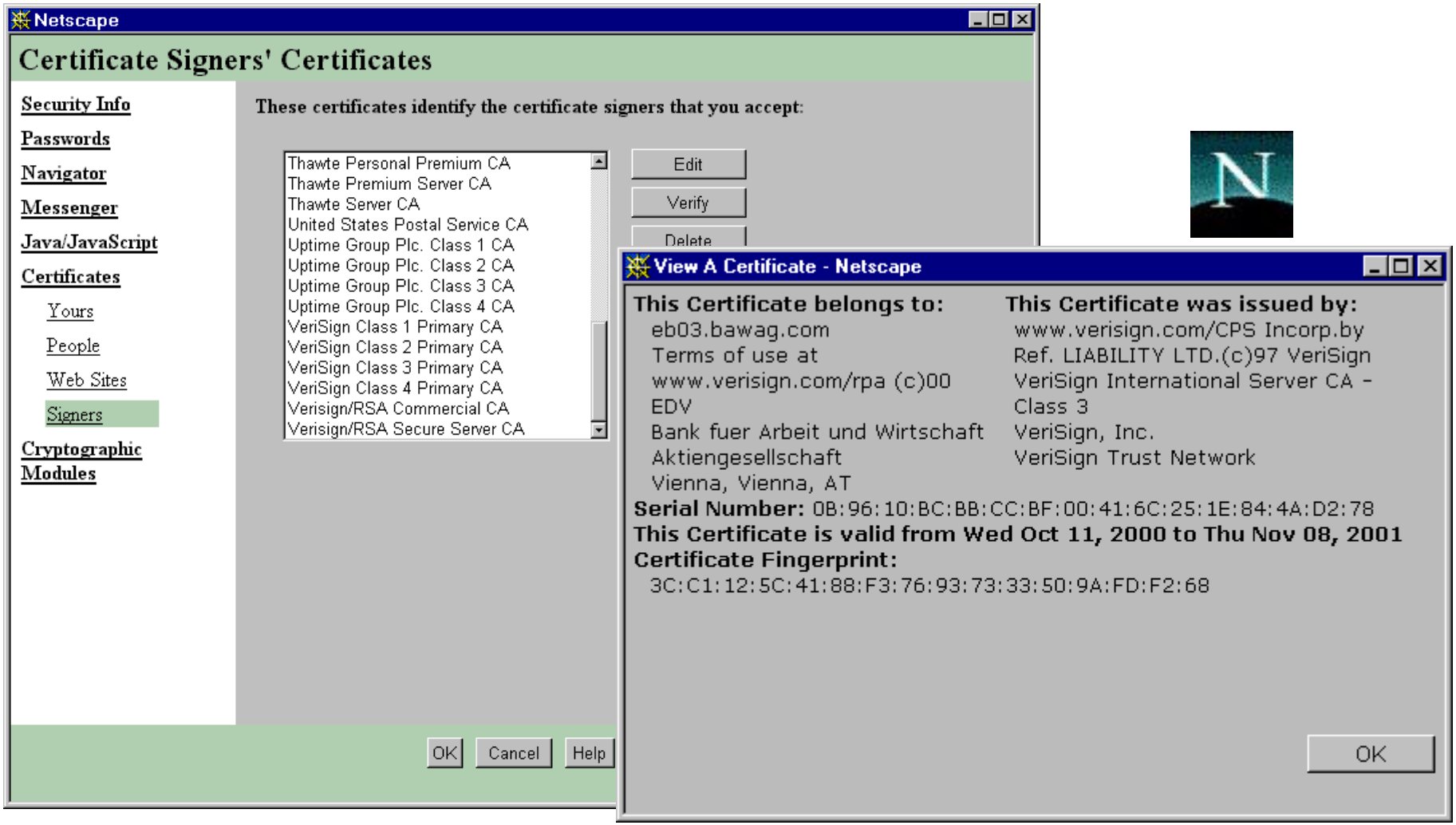
This Certificate belongs to:
online.bankaustria.com
Dataservice Informatik
Bank Austria AG
Vienna, Vienna/Austria, at

This Certificate was issued by:
Secure Server Certification Authority,
RSA Data Security, Inc. US

Zertifikat:

Serial Number: 7D:9F:20:47:45:12:9A:16:A7:2E:62:28:D5:1E:80:01
This Certificate is valid from Wed Oct 11, 2000 to Thu Nov 08, 2001
Certificate Fingerprint:
80:F3:1A:CA:91:3B:44:2E:7F:94:62:82:BF:AD:B0:1D

Verwaltung von Zertifizierungsstellen



Österreichisches Signaturgesetz

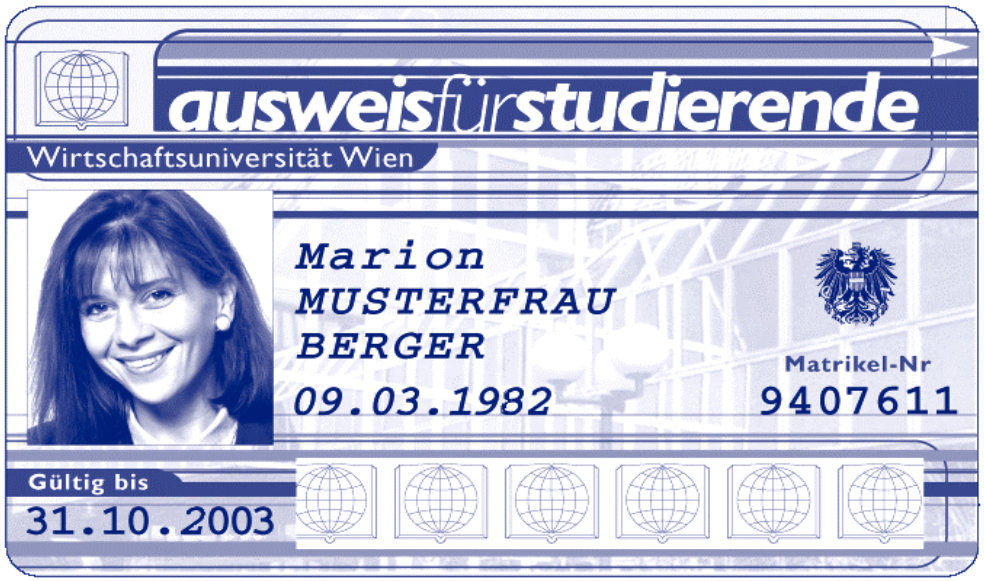
- Seit 1.1.2000 ist das österreichische Signaturgesetz (SigG, BGBl 190/99) in Kraft.
- Qualifiziertes Zertifikat
  - eine elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und deren Identität bestätigt wird.
- Gleichstellung der elektronischen Signatur (unter best. Voraussetzungen) mit handschriftlicher Unterschrift
  - im Rechts- und Geschäftsverkehr verwendbar und als Beweismittel zulässig (-> Beweislastumkehr)
- Zertifizierungsdiensteanbieter (ZDA) in Österreich
  - Generali Office-Service und Consulting AG
  - Datakom Austria GmbH
  - Arge Daten - Österreichische Gesellschaft für Datenschutz (Verein)

WU-Chipkarten-Projekt

- Signaturkarte: Chipkarte, die elektronische Unterschrift ermöglicht
- Chipkarte wird Zertifikat sowie den Private Key des Benutzers enthalten
- Zertifikat (X.509): Benutzerdaten + Public-Key des Benutzer, vom Trustcenter mit Privat-Key unterschrieben
  - Vorname, Nachname, Seriennummer des Chips
  - Nicht: Matrikelnummer

Ausweis für Studierende

- ~ 23.000 Multifunktionskarten (Ausweis + Signaturkarte - keine Quickfunktionalität)
- Kostenlos für die Studierenden
- In der Universitäts-Studienevidenzverordnung 1997 (UniStEVO 1997) geregelt
- Signifikate Erweiterung der Services



Neue Dienste für Studierende an der WU

- Rückmeldung zum Studium
  (Zahlscheininskription bleibt bestehen)
- Studienwechsel
- Diplom- u. Vorprüfungsanmeldung
- Übernahme von Bescheiden
- Drucken v. Erfolgsnachweisen
- 24-h-Zutritt zu PC-Räumen
- Bibliothek
- ÖH-Wahlen?

„Sichere“ elektronische Signatur

Zur Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift bedarf es einer sicheren elektronischen Signatur, die auf einem qualifizierten Zertifikat oder auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren im Sinne des §18 erstellt wird.

- Secure Viewer zur Gleichstellung mit handschriftlicher Unterschrift
- Chipkarten-Leser, Papierladen (Unterdruckpapier -> unter Verschluss, Normalpapier)



Literatur zum Thema

- Fischer/Rensing/Rödig: „Open Internet Security. Von den Grundlagen zu den Anwendungen“, Springer Verlag, 2000
- HANSEN/Neumann: Wirtschaftsinformatik 1, 8. Auflage, Fischer, 2001.
- Schneier: „Secrets & Lies. IT-Sicherheit in einer vernetzten Welt“, dpunkt.verlag/Wiley, 2001
- Information zum österreichischen Signaturgesetz
  - http://www.tkc.at/
- EU Richtlinien zu elektronischen Signaturen
  - http://europa.eu.int