Referat im Proseminar Electronic Commerce

Thema: Anwendungen von Kryptographie für E-Commerce

Betreuer: Michael Galler

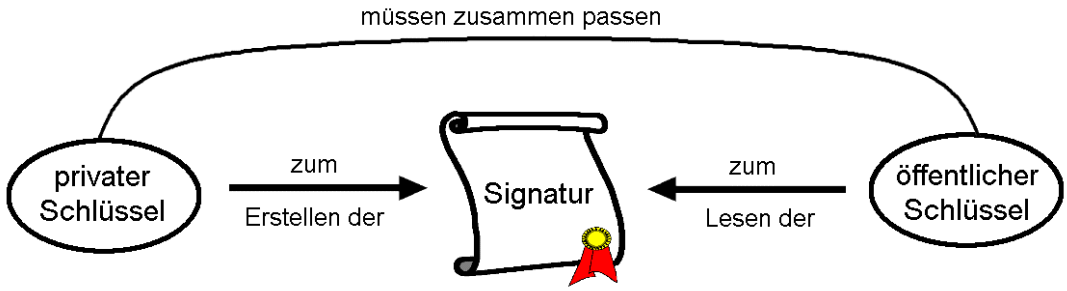
Stoffsammlung/Grobgliederung

Problem der Sicherheit des E-Commerce

- nötig für Sicherheitsgarantie: Verschlüsselungsverfahren
- bisher akzeptierte Beweismittel: persönlich unterschriebene Dokumente

Die digitale Signatur

- muss unabstreitbar sein
- Methode der asymmetrischen Kryptographie



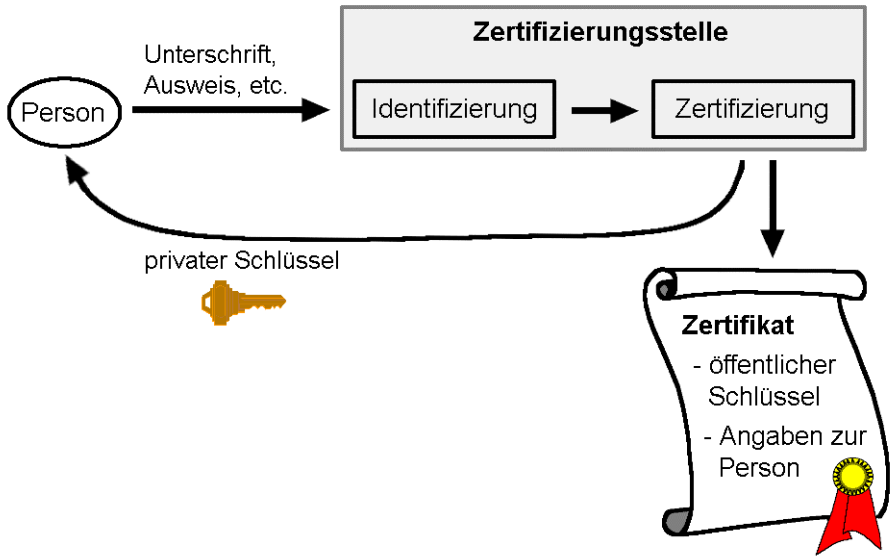
digitaler Schlüssel: Folge von Zahlen

Problem: keine sichere Verbindung zwischen öffentlichen Schlüssel und der tatsächlichen Identität des Erstellers der Signatur.

Bsp: Geschäftspartner kann nicht sicher sein, dass der Vertrag von Hr. Maier authentisch ist, weil auch ein dritter (Hr. Huber) die digitale Signatur (mit entsprechendem öffentlichen Schlüssel) auf den Namen Maier ausgestellt haben hätte können.

Authentizität durch Zertifizierungsstellen

Zertifizierungsstelle: Dienstleister für sicheren E-Commerce



wichtig: Zertifizierungsstelle muss vertrauenswürdig sein. → gesetzliche Vorgaben zur Identifizierung und zum Betrieb von Zertifizierungsstellen. → deutsches Signaturgesetz (später im Vortrag)

Stark ausgeprägte Zertifizierungsstellen:

Banken *(Vorteil: wirken vertrauenswürdig, haben meist schon Erfahrungen aus dem Online-Banking Bereich), Mobilfunkbetreiber!*

Risiken beim E-Commerce (laut Schoeder, Detlef; Müller, Günter):

- Kundenrisiko
  ist der Zahlungsempfänger zuverlässig?
  Z.B. fristgerechte Leistung, Lieferung der vereinbarten Menge in vereinbarter Qualität, Umgang mit Kundendaten, Verhalten bei Liefermängeln).
- Finanzrisiko
  kann der Leistungsempfänger bezahlen?
  auch durch Beurteilung und bestätigung Dritter (z.B. Banken)
- Gewährleistungsrisiko
  bei der Bank.

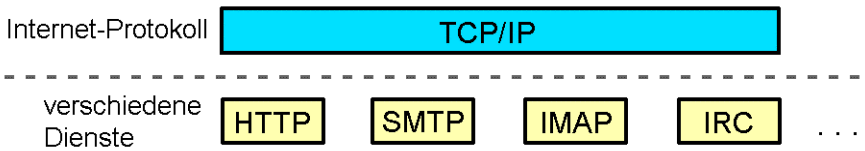
Zertifizierungs-Standards (*„zu viele Köche verderben den Brei“*)

Problem, wenn z.B. jede Bank ihre eigene Zertifizierungsstelle betreibt: Inkompatibilitäten und kein gegenseitiges Vertrauen zweier Geschäftspartner unterschiedlicher Banken.
„Da es für den Empfänger einer digital signierten Nachricht nahezu unmöglich ist, selbst festzustellen, welche Sorgfalt die Zertifizierungsstelle des Absenders bei der Abwicklung von Prozessen aufwendet, wird er den Angaben in fremden Zertifikaten nicht vertrauen.“
(Schwerpunktaufsatz von Lamberti und Költzsch)

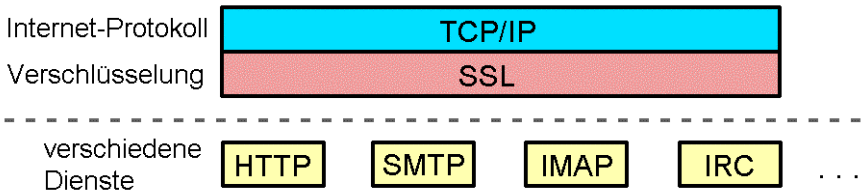
→ Banken beteiligen sich gemeinsam an einheitlichen Zertifizierungsstellen.
z.B. Trust Center (national) oder Identrus (international).

SSL – ein Verschlüsselungsprotokoll für das Internet

„Secure Sockets Layer protocol“ entwickelt von Netscape (momentan Version 3).
Bekannt (aus erstem Vortrag):



SSL läuft zwischen den Dienstprotokollen und TCP/IP:



Oft läuft die Herstellung einer sicheren Verbindung mit SSL (Authentifizierung) automatisch im Hintergrund ab. Z.B. beim Browsen (HTTP->HTTPS).
(*Bei Emailprogrammen auch! MIME -> S/MIME*)

Verschlüsselungsgrad lässt sich messen an:

- Länge der Schlüssel
- Verschlüsselungstiefe (wieviel Bits)

Prinzip des Aufbaus einer SSL-Verbindung (SSL Handshake) (Grob!)

Skizzieren an Tafel!

- Anfrage des Clients, dann Austausch von Versionsnummern und der verfügbaren Verschlüsselungstypen.
- Einigung auf Verschlüsselungstyp, z.B. DES, Tripple-DES, RC4, Blowfish
- Austausch der (öffentlichen) Schlüssel (z.B. mit „RSA key exchange“)
  Server schickt sein Zertifikat!
- Authentifizierung (*manchmal auch des Servers beim Client*)
- gemeinsame Generierung der „Session Keys“ (einer zum Verschlüsseln und einer zum Entschlüsseln) die dann für die laufende Verbindung verwendet werden.
  Dabei Verwendung der öffentlichen und privaten Schlüssel (*d.h. Client verschlüsselt mit öffentlichem Schlüssel vom Server, der Server kann diese Informationen dann mit seinem privatem Schlüssel entschlüsseln. Und umgekehrt*)

Dann steht die Verbindung. Daten werden verschlüsselt durch die „Session Keys“ ausgetauscht!

Das Signaturgesetz (SigG) in Deutschland (*Auch bekannt als „Mulimediagesetz“*)

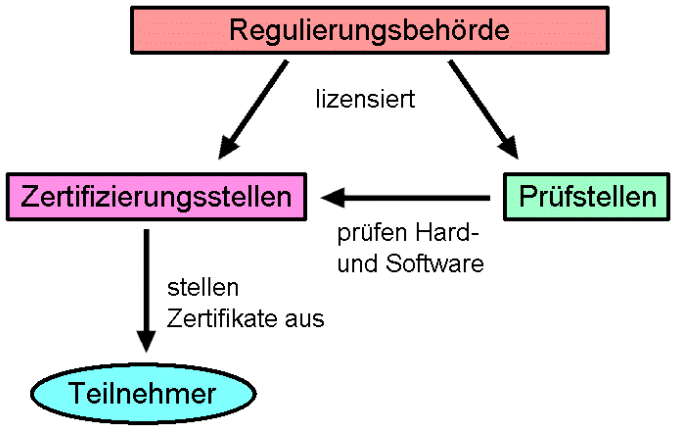
Inkrafttreten am 01.08.1997. (*evtl. Durchgeben*)

Damaliger Ansatz: Umsetzung der Anforderungen aus der Signaturrichtline der EU.
Seit Mai 2001: Rahmengesetz über elektronische Signatur. Gleiche Rechtswirkkraft der elektronischen Signatur wie bei herkömmlicher Unterschrift.
Dazu sind aber noch Änderungen im BGB nötig! Womit noch in diesem Jahr zu Rechnen ist.

SigG soll Rahmenbedingug für „sichere“ digitale Signatur schaffen.

Bestimmungen des SigG (u.a.):

- Struktur (der Behörden):



- wie die Zertifizierungsstelle Personen zuverlässig identifizieren soll
- Inhalt eines Zertifikats
- Zulässigkeit eines elektronischen Dokuments darf vor Gericht nicht alleine aus dem Grund verweigert werden, weil es ein elektronisches Dokument ist.
- Datenschutz
- Technische Komponenten
  (*müssen nach dem Stand der Technik „sicher" sein - schwammig!*)

Kann völlige Sicherheit gewährleistet werden?

Nein! Verschlüsselungsverfahren haben nur kryptografische Sicherheit. Verschlüsselung ist theoretisch also brechbar durch einfaches Durchprobieren!

Sinnvoller Ansatz: Aufwand (*also die Länge des Schlüssels*) muss so groß sein, dass er auch mit den voraussichtlich in den nächsten Jahren vorhandenen Computersystemen als sicher gilt.

Vor- und Nachteile des deutschen Signaturgesetzes:

Dt. Signaturgesetz ist schon leicht veraltet. Es gibt zwar bald einen neuen Gesetzesentwurf, aber z.B. die USA sind schon einen Schritt weiter gegangen. Dort ist die digitale Signatur der bisher üblichen Unterschrift rechtlich schon völlig gleichgestellt.

Vorteil:

- Leicht zu durchschauen, auch für Privatpersonen
- keine Spezialzertifikate, oder Sonderregelungen
- Einheiltlichkeit.
  Deutschland ist eines der wenigen Länder mit einheitlicher Gesetzgebung!

Nachteil:

- wenig flexibel
- Problem bei Pseudonymen
- Wenn ein Schlüssel der Regierungsbehörde geknackt wird, wackelt die ganze Sicherheitsstruktur
- Keine Zulassung eines Schlüssels für juristische Personen.
  Bsp: Werkstudent (muss immer wieder neuer Schlüssel erstellt werden)