



Vorlesung

VPN: Drahtgebunden und drahtlos

Fachbereich Informatik (FB 20)

Lehrstuhl Prof. Buchmann

WS-05 / V2 - 20.205.1

In Zusammenarbeit mit dem CAST-Forum

Dr. Wolfgang Böhmer

Skript: <http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/>

Email: wboehmer@cdc.informatik.tu-darmstadt.de





Verfahren zur Authentifizierung

1. Digitale Signatur / elektronische Signatur
 1. Mechanismen einer digitalen Signatur
2. PKI und Trust Center
 1. x.500 und x.509v.3
 2. Zertifizierung und Validierung
 3. PKI-Unterscheidungsmerkmale
 4. Einsatz von Digitalen Zertifikaten
3.
 1. Einfache Authentifizierung
 2. Starke Authentifizierung
 1. Ein-Wege/ Zwei-Wege/Drei-Wege-Authentifizierung
 3. Zwei Faktoren-Authentifizierung in der Praxis
 1. Zeitsynchrone mittels Token-Cards
 2. Speicherkarten und Smarts-Cards





Asymmetrische Verschlüsselung (*public –Key-Verfahren*)

Einen Schlüssel (a) zum Verschlüsseln

Einen Schlüssel (b) zum Entschlüsseln

Verschlüsselung:

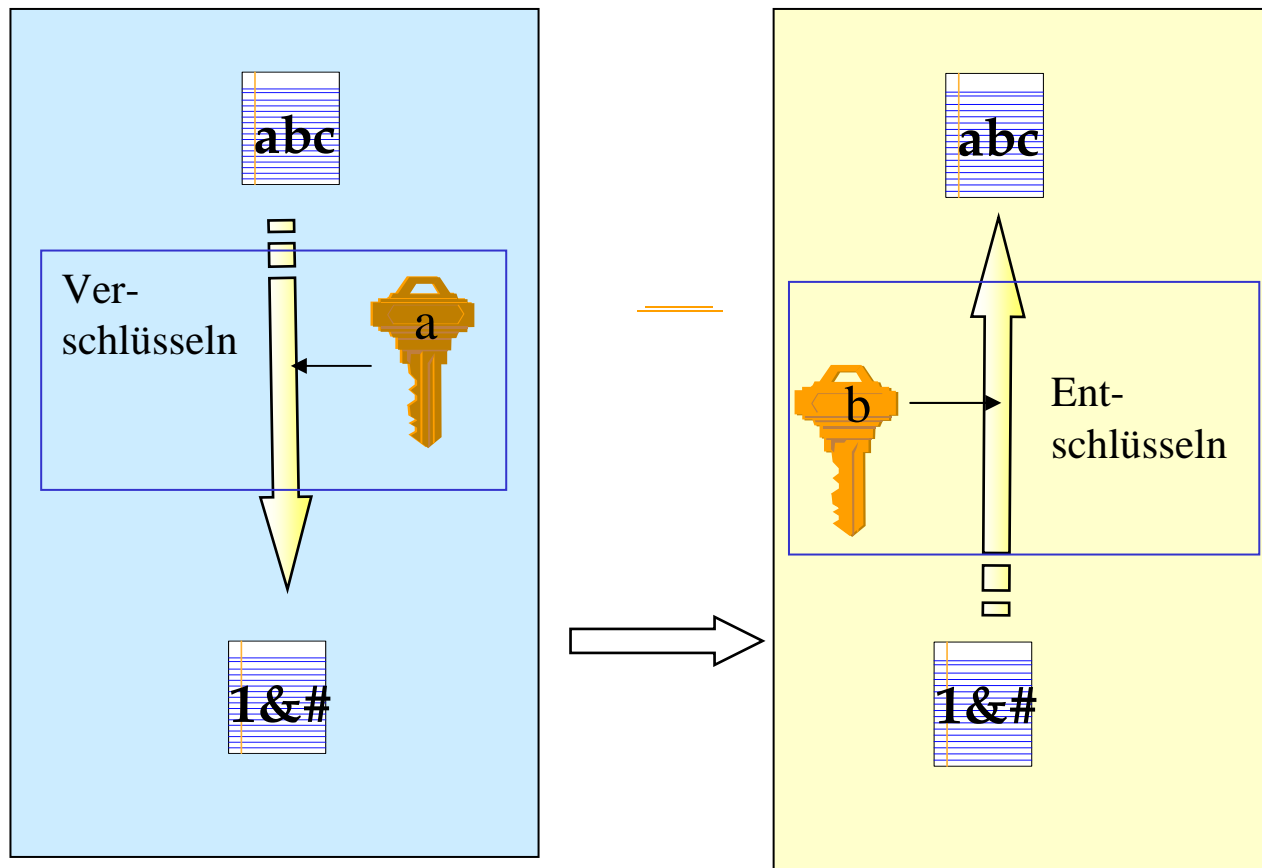
Geheimtext := Algorithmus_a
(Klartext)

Entschlüsselung:

Klartext := Algorithmus_b
(Geheimtext)

Es ist unmöglich von (a) auf (b) zu schließen

Nachteil: immense Rechenkapazität erforderlich



RSA-Algorithmus /

Funktionsprinzip der Primzahlenzerlegung



- RSA ist eine Blockchiffre, bei dem der Ausgangstext und der Chiffretext ganze Zahlen zwischen 0 und $n-1$ bei beliebigen n sind.
- RSA kann zur Verschlüsselung und für digitale Signaturen verwendet werden
- RSA ist der derzeit bekannteste und flexibelste asymmetrische Kryptoalgorithmus.
- Beide Schlüssel werden von zwei großen Primzahlen p und q erzeugt und müssen geheim sein.
 - Eine Zahl $n > 1$ ist eine Primzahl, wenn ihre einzigen Teiler ± 1 und $\pm n$ sind.
- Es wird das Produkt $n = p \cdot q$ der beiden Primzahlen und einen ausgewählten öffentlichen Schlüssel e an den Sender geschickt.
- Dieser kann nun aus der Nachricht (M) ein Kryptogramm C erzeugen, gemäß der Formel: $C = M^e \bmod n$
- Das Kryptogramm C übermittelt der Sender dem Empfänger, der es dechiffrieren kann, da er die Verschlüsselungsfunktion e und die beiden Primzahlen p und q kennt.
- Die Entschlüsselungsfunktion lautet: $M = C^d \bmod n$





Öffentliche Schlüssel bei RSA

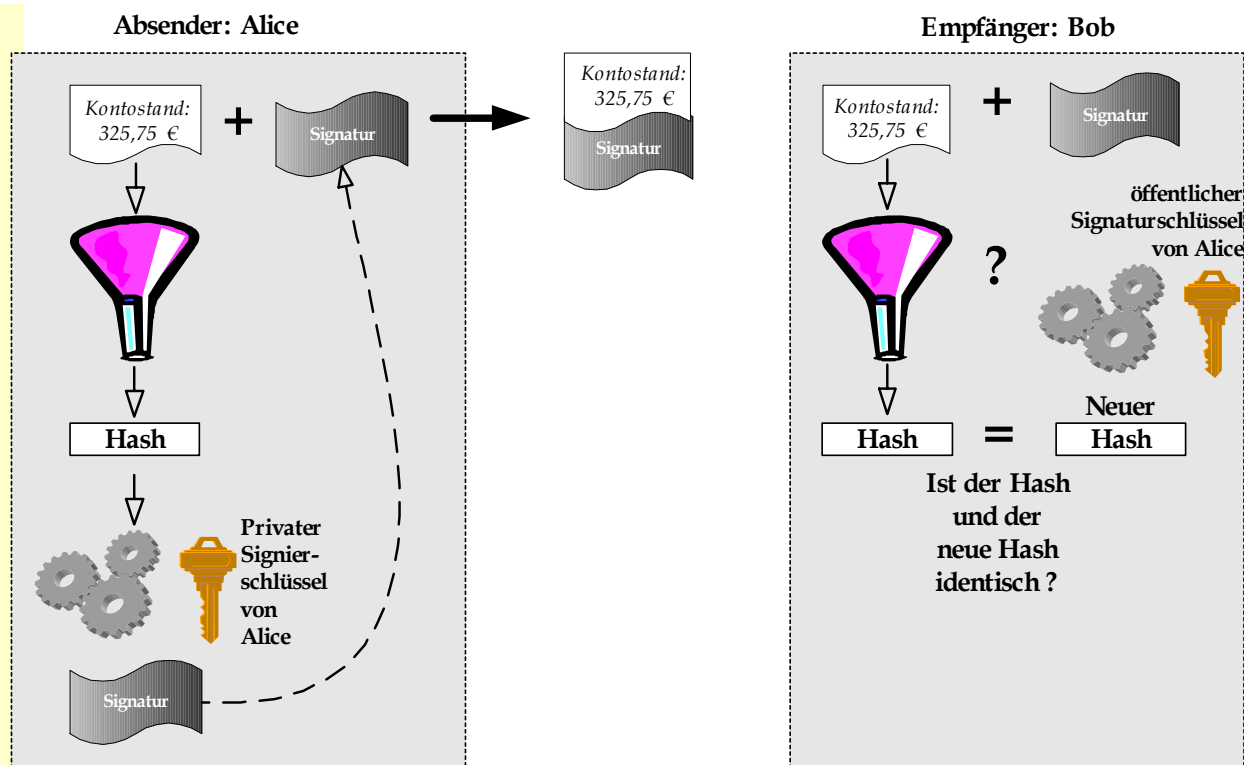
- Sowohl Absender als auch Empfänger müssen n kennen.
- Der Absender kennt den Schlüssel e
- Der Empfänger kennt nur den Schlüssel d
- Dabei ist der öffentliche Schlüssel:
 - n : Produkt zweier Primzahlen p und q (und sind streng geheim)
 - e ist relativ prim zu $(p-1)*(q-1)$, wenn beide Zahlen keinen gemeinsamen Teiler außer 1 haben.
- Der private geheime Schlüssel ist:
 - $d: e^{-1} \bmod ((p-1)*(q-1))$
- Die Sicherheit des Verfahren beruht darauf, dass es sehr einfach ist n aus den beiden Primzahlen zu berechnen, jedoch sehr schwierig ist n so zu faktorisieren, dass die richtige Primzahl herauskommt.





Elektronische Signatur

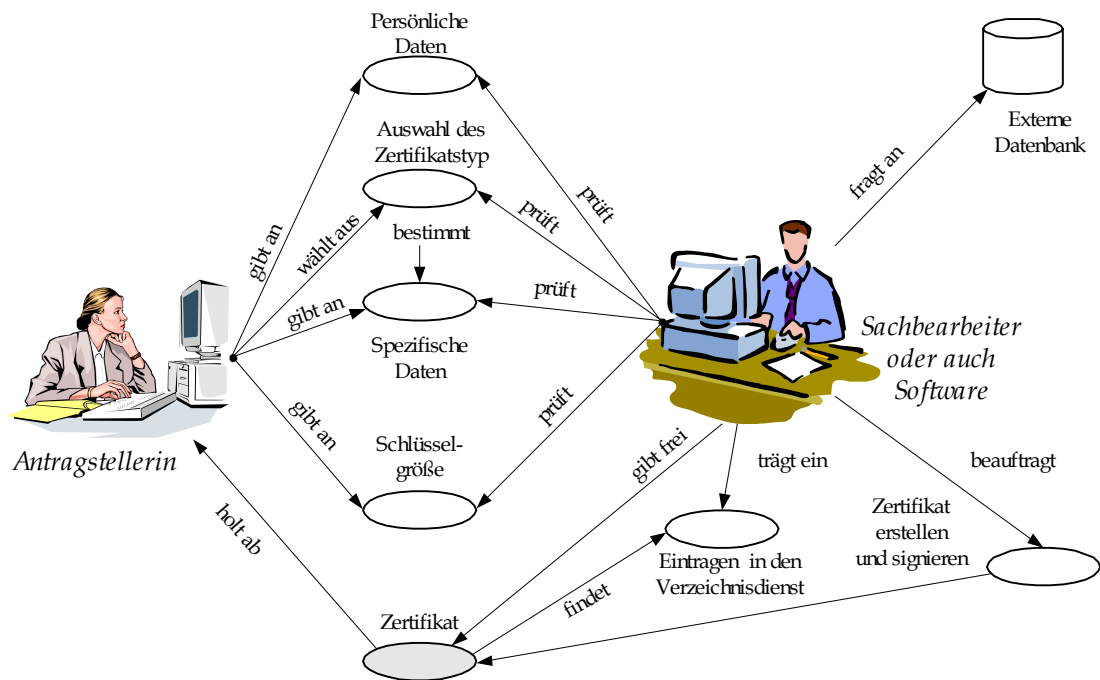
1. Nachricht wird mit einem Hashwert fixiert
2. Hashwert wird vom Sender mit seinem *private Key* signiert
3. Nachricht wird zum Empfänger geschickt
4. Empfänger bildet die gleiche Hashfunktion über die Nachricht
5. Mittels öffentlichen Schlüssel wird Zuordnung geprüft
6. Vergleich der Hashfunktionen liefert Resultat





Beantragung eines Zertifikates

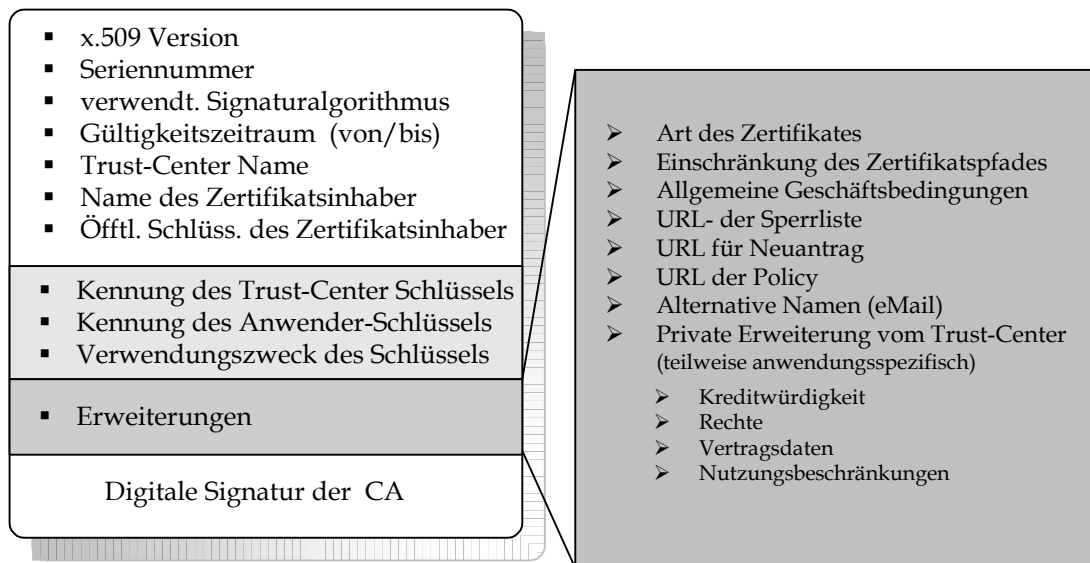
Prozessdarstellung zur
Beantragung eines
Zertifikates





Zertifikat gemäß X.509v.3

- Zertifikatsstandard gemäß ITU-T. (ISO-Standard 9594)
- Die Graustufen zeigen die jeweiligen Ergänzungen



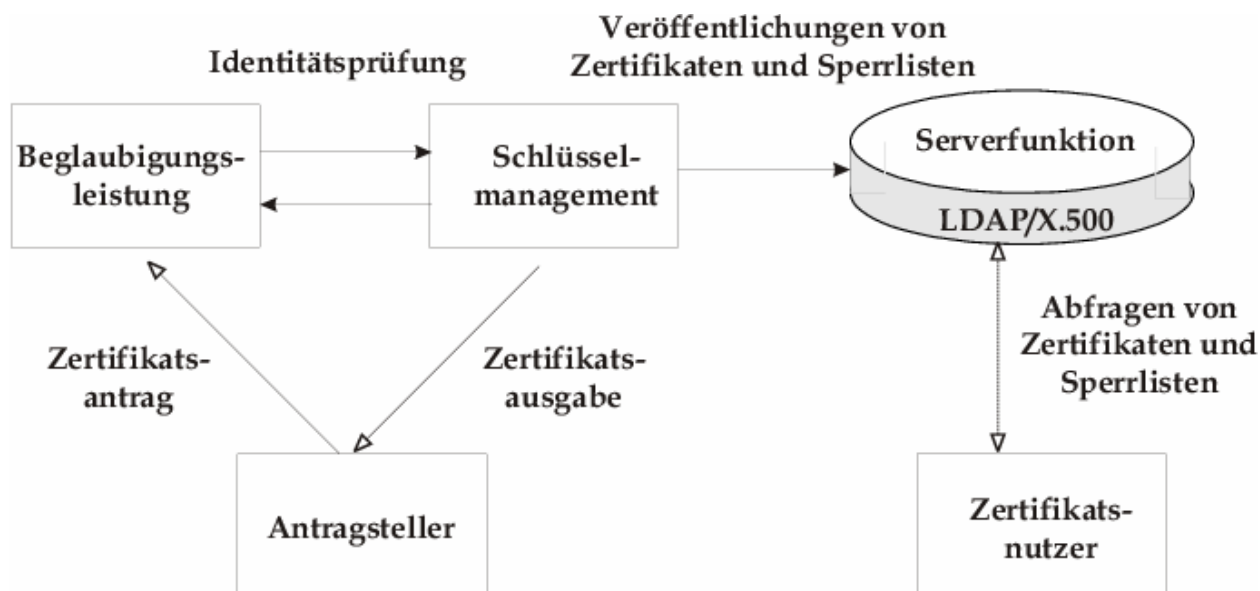
- x.509.v1
- x.509.v2
- x.509.v3





Aufgaben einer Zertifizierungsinstanz

- Beglaubigungsfunktionen (*Registration Authority, RA*)
- Serverfunktionen (*LDAP, X.500, X.509v.3*)
- Schlüsselmanagement (*Certification Authority, CA*)





Verfahren zur Authentifizierung (x.509)

- Prinzipiell lassen sich alle Identifikations- und Authentifizierungsverfahren auf die Überprüfung von drei Faktoren zurückführen
 - Etwas, das man weiß (*Passwörter*)
 - Etwas, das man darstellt (*Aussehen, Biometrie*)
 - Etwas, das man besitzt (*Zugriffstoken*)
- Reale Sicherungssysteme koppeln häufig mehrere Varianten (z.B. EC-Karten)
 - Gute Sicherungssysteme zeichnen den Überprüfungsvorgang auf
- Zwei große Gebiete umfasst die Absicherung von Informationen und Informationssysteme im Sinne einer Authentifizierung
 - Zugangssicherung bzw. Zugriffssicherung bei technischen Systemen
 - Feststellung der Identität einer Person (Fingerabdrücke, Stimme, Iris, Pin, TAN)
 - Integrität und Urheberschaft bei elektronischen Dokumenten
 - Authentizität (*Echtheit*) von elektronischen Dokumenten
 - Ist das Dokument X unverändert?
 - Stammt das Dokument X tatsächlich von der Person Y?





Einfache Authentifizierungsverfahren (*one-way, two party*)

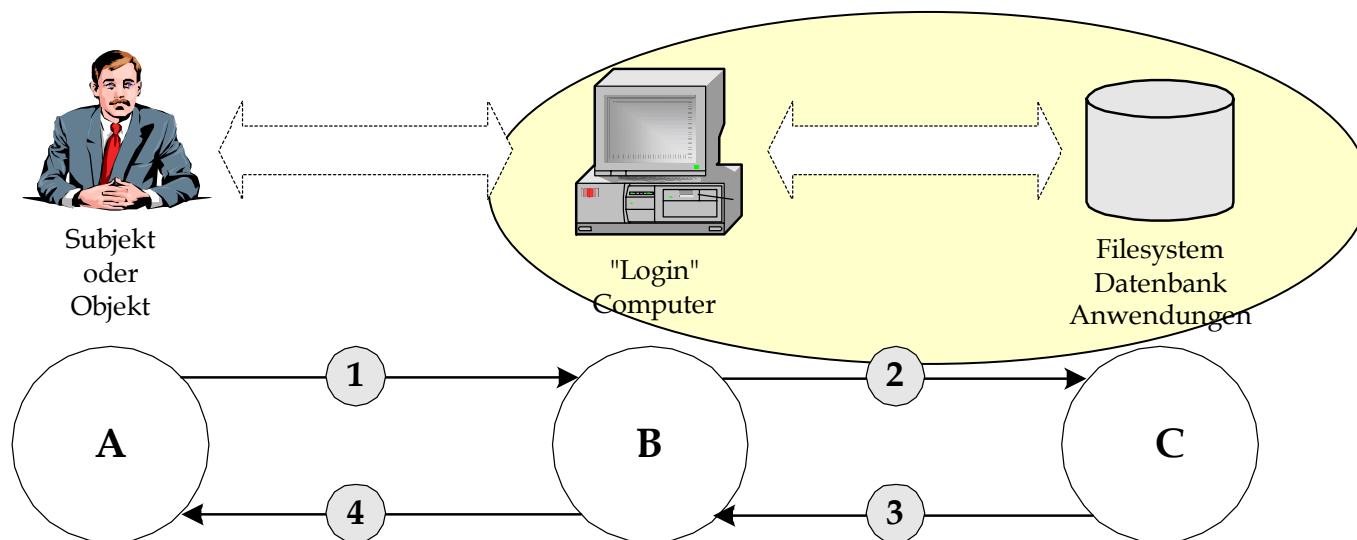
- Einfache ungeschützte Verfahren
 - Verwendung von statischen Passwörtern
- Geschützte Verfahren
 - Umwandlung von ungeschützten in geschützte möglich
 - Einsatz von Hashfunktion auf Nutzerkennung und Passwort
- Alternativ Einmal-Passwörter
 - Interessante Variante wurde von Lamport 1981 vorgeschlagen, das nicht auf PKI-verfahren beruht.
 - S/Key Implementierung (RFC-1760)
 - OTP-Verfahren nach IETF (RFC-2289)





Einfaches ungeschütztes Authentifizierungsverfahren

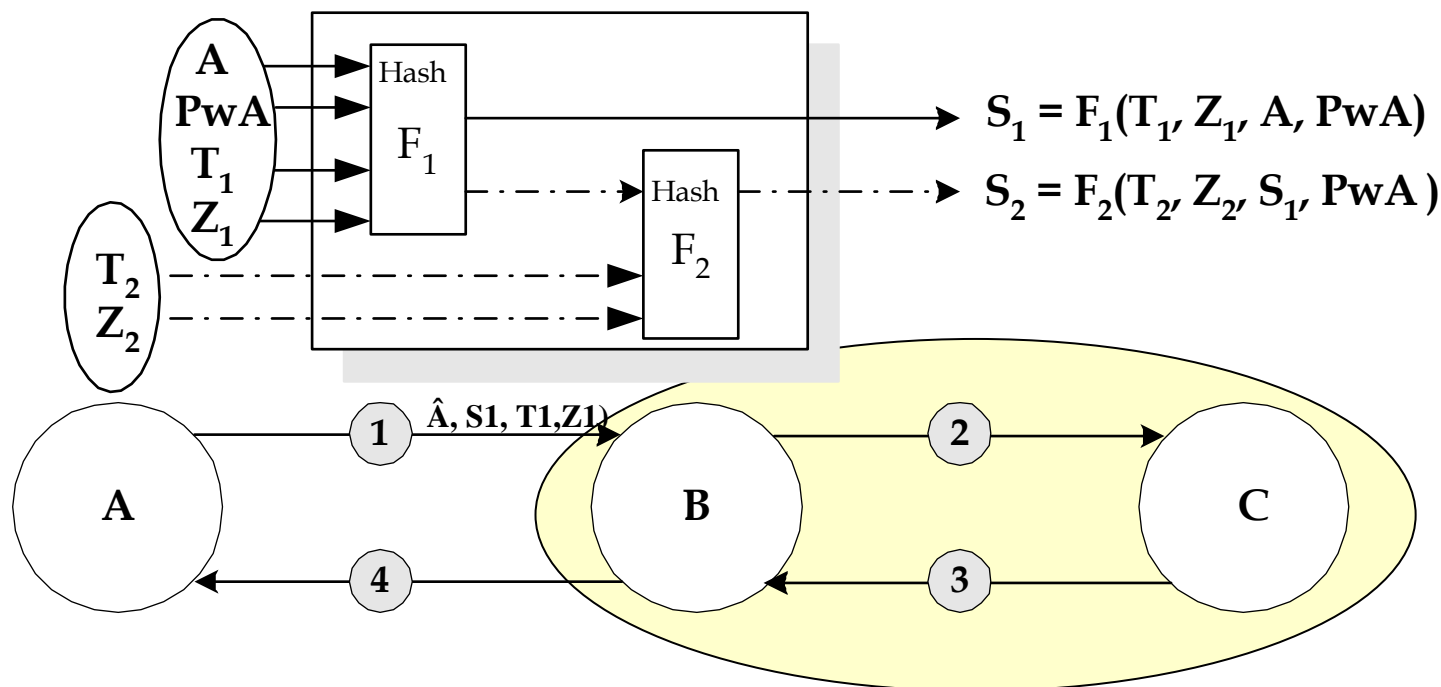
- Geringes Sicherungsniveau (statische Passwörter, dictionary attack -> L0phtcrack)
- Wirksamkeit des Verfahrens hängt von Geheimhaltung der PwD und der Wahl der PwD ab.
- Beachtenswert die PwD-Regeln im Grundschutzhandbuch des BSI





Einfache geschützte Verfahren

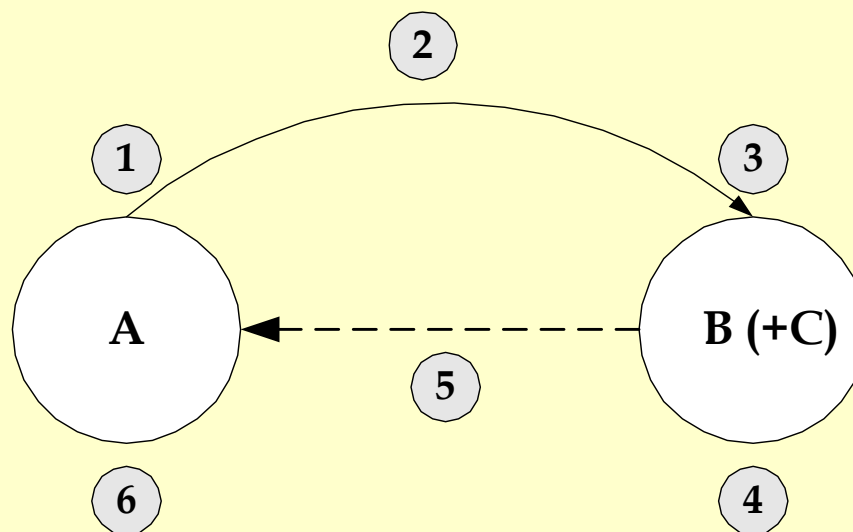
- Verwendung von Zeitmarken und Zufallszahlen (*optional*)





Starke Authentifizierungsverfahren (*two-way, two-party*)

- Beruhen auf asymmetrische Verschlüsselungsverfahren (Public-Key-Cryptosysteme PKCS#1-PKCS#15)





Zwei Faktoren-Authentifizierung in der Praxis

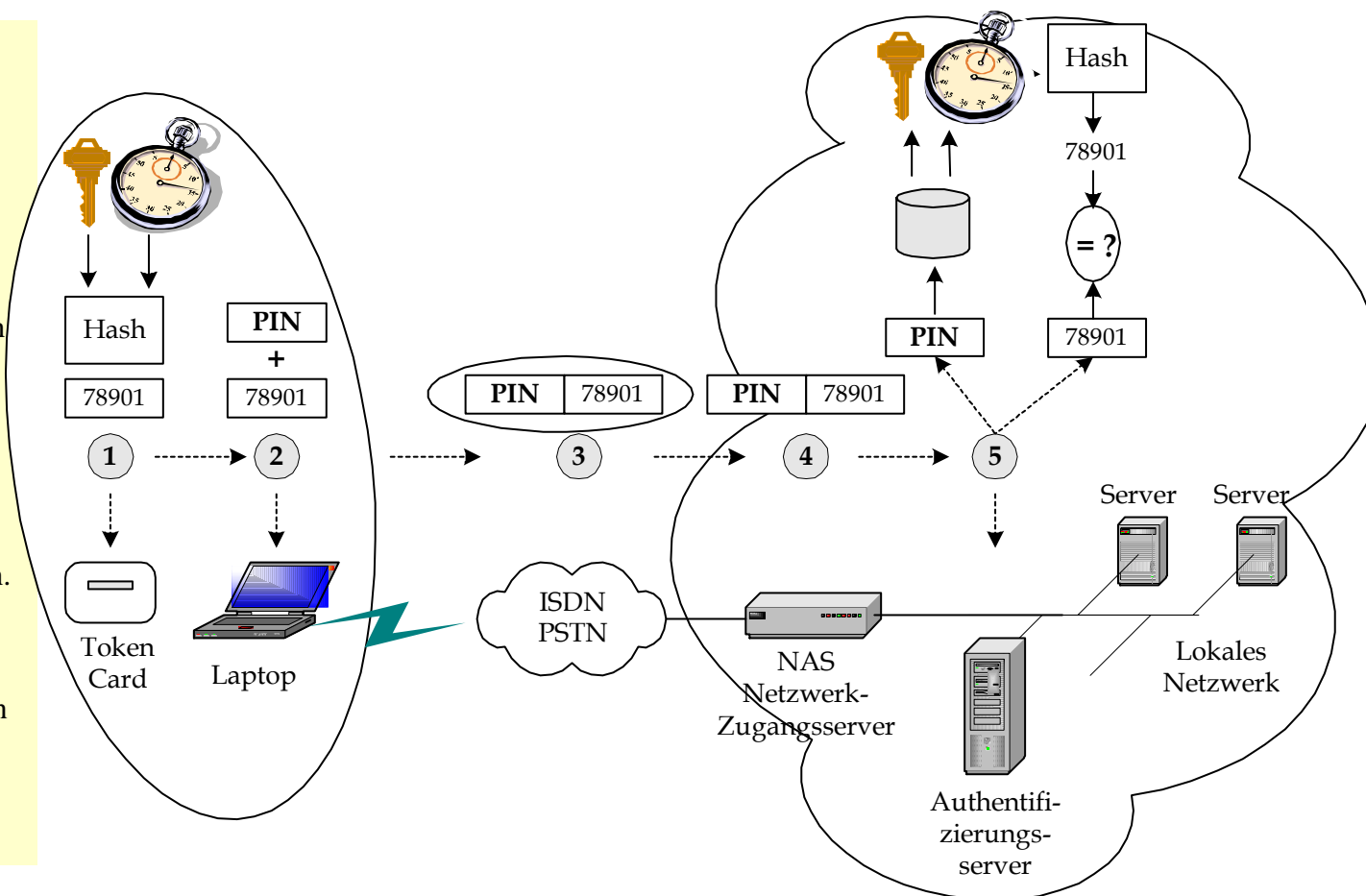
- Anwendung von Besitz und Wissen
 - Zeitsynchrone Authentifizierung mittels Token-Cards
 - Abstrakter Begriff Token beschreibt eine Authentifizierungsinformation (SecureID-Cards)
 - Token häufig eine Ziffer die die Funktion eines Einmal-Passworts hat
 - Zeitstempel spielt ein Rolle
 - Speicherkarten und Smart-Cards
 - Siegeszug der Plastikkarten beginnt 1968 durch franz. Journalist R. Moreno
 - Grundidee: Integration einer Prozessorschaltung auf eine Plastikkarte
 - Ab ca. 1970 wird die Prozessorkarte mit PIN-Schutz und Zählerfunktion erweitert





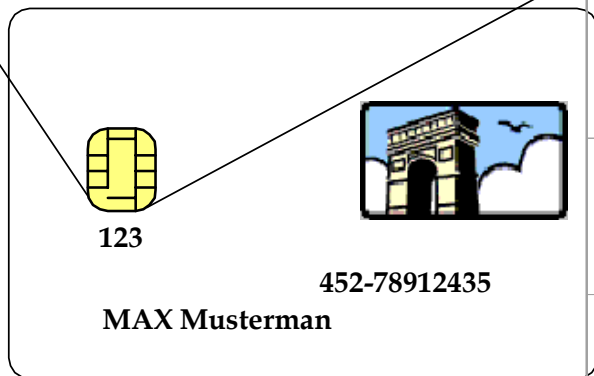
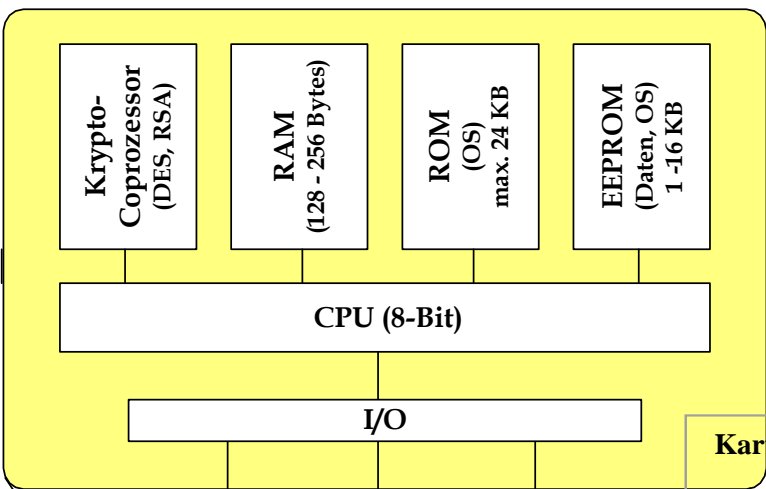
Zeitsynchrone Zwei-Faktoren-Authentifizierung

1. Vorab erfolgte Personalisierung
2. Nutzer liest aus der Token-Card das Einmal-Passwort (78901)
3. DFÜ-Software wählt via Fernsprechnet den Zugangsserver zum Unternehmen. PIN und Token werden transparent über das Netz geschickt
4. Verbindung zum Authentifizierungs-Server erfolgt
5. Im A-Server erfolgt eine Trennung von PIN und Token. Der zur PIN zugehörige Schlüssel wird gesucht. Zeitmarke und Schlüssel werden zur Bildung des neuen HASH verwendet. Vergleich gibt Aufschluß über Erfolg/Mißerfolg





Speicherkarten und Smart-Cards



Kartentechnologie	Speicherkarte	Sicherheit des Speichers	Kosten
Magnetstreifenkarte	< 350 bytes (R/W)	Keine	Karte sehr kostengünstig, Leser moderat, Leser/Schreiber teuer
Chipkarte	Bis 20 Kbytes (WROM oder R/W)	Zugriff über Logik eingeschränkt Aktive Aufgaben (Verschlüsselung) möglich	Karte moderat bis teuer Leser = Schreiber Sehr kostengünstig
Laserkarte	1 MB (WORM)	Keine	Karte kostengünstig Leser/Schreiber sehr teuer





Übungen

1. Welche Rolle spielt die genaue Zeit bei einem TrustCenter?
2. Besitzt eine geleistete elektronische qualifizierte Signatur nach Ablauf des Schlüsselgültigkeitszeitraum (i.d.R. 6 Jahre) noch Gültigkeit?
3. Nutzen beim Einsatz von reiner asymmetrischer Verschlüsselung und elektronischer Signatur beide Verfahren den gleichen prinzipiellen Prozessablauf bezogen auf die Schlüssel?
4. Welche nicht zeitsynchrone zwei-Faktoren Authentifizierung können Sie sich zukünftig bei einer Kontobewegung vorstellen, wenn die Möglichkeit der SmartCard ausgeschlossen wird.
5. Wie tauschen VPN-Gateways untereinander Zertifikate aus?





Literatur

- <http://www.tu-darmstadt.de/ss/comments/20.183.1>
- **Huston G.: Internet Performance Survival Guide, QoS Strategies for Multiservice Networks, ISBN 0-471-37808-9**
- **Comer, 1995: Internetworking with TCP/IP Vol. I., ISBN 0-13-216987-8**
- **ITU-T Recommendation Series X: Data Networks and Open System Communications, Directory X.509 (03/2000)**
- **ITU-T Recommendation Series X: Data Networks and Open System Communications, Directory X.500 (02/2001)**

