

IT Sicherheit

- AUTHENTIFIZIERUNG -

“Transilvania” Universität Brasov




Authentifizierung

- Wissen und Besitz
- Challenge Response Verfahren
- Kerberos
- Chipkarte und Biometrie
- Public-Key Infrastructure und Signaturgesetz

Authentifizierung

Situation:

Benutzer von IT-Systemen werden nur bei erstmaligen Systemzugang authentifiziert und haben dann Zugriff auf alle Daten, Prozesse, Serverdienste des IT-Systems.

- ❑ Zugriffe auf digitale Informationen erfolgen durch Benutzer über Rechner, aber auch durch Benutzerprozesse auf Anwendungsserver, die im Auftrag von Benutzern agieren
- ❑ Einfaches Login mit Passwort und Pauschal-Zugang zu allen Diensten, die das System  ist in offenen verteilten Systemen nicht mehr ausreichend
- ❑ Es ist nicht sicher, ob Benutzer bzw. Benutzerprozesse mit dem System bzw. Anwendungsserver kommunizieren



Authentifizierung Ziel

- Autorisierte Zugriffe auf authentische Dienste in offenen vernetzten IT-Systemen
- Verhindern von Spoofing-Attacken und Man-in-the-Middle- Attacken !



Authentifizierung

Authentifizierung und Autorisierung

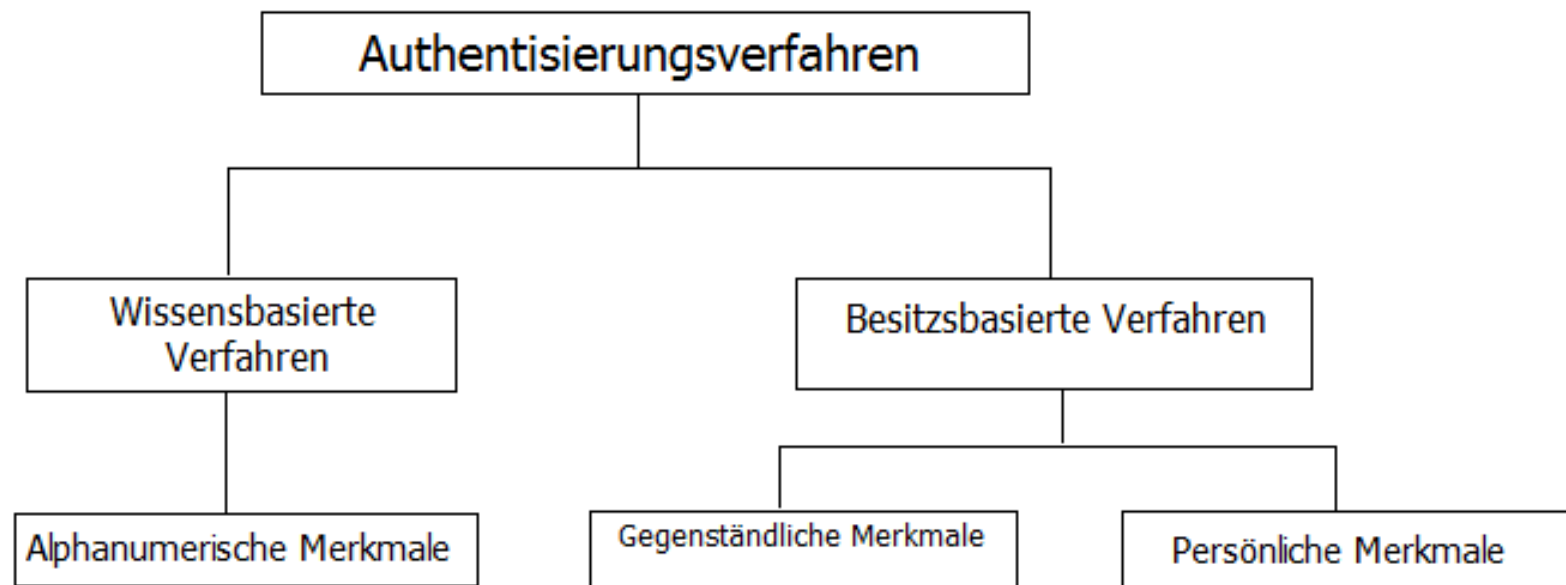
Identifizierung: Erkennen der Identität einer Person, eines Rechners (Identifikation) bzw. Prozesses z.B. Benutzerkennung, User-ID, Internet-Adresse

Authentisierung: Prüfung der behaupteten Identität der Person, des (Authentifikation) Rechners bzw. Prozesses (Authentifizierung) z.B. Passwort-Abfrage

Autorisierung: Person, Rechner bzw. Prozess erhält nach erfolgreicher Authentifizierung den Zugriff auf die entsprechenden Dienste bzw. Systemkomponenten

Authentifikationsmerkmale charakteristische Merkmale, anhand derer eine zweifelsfreie Authentifizierung zur Autorisierung erfolgen kann (z.B. PIN/TAN, digitale Signatur, Fingerabdruck, Stimme, Gesicht)

Klassifikation



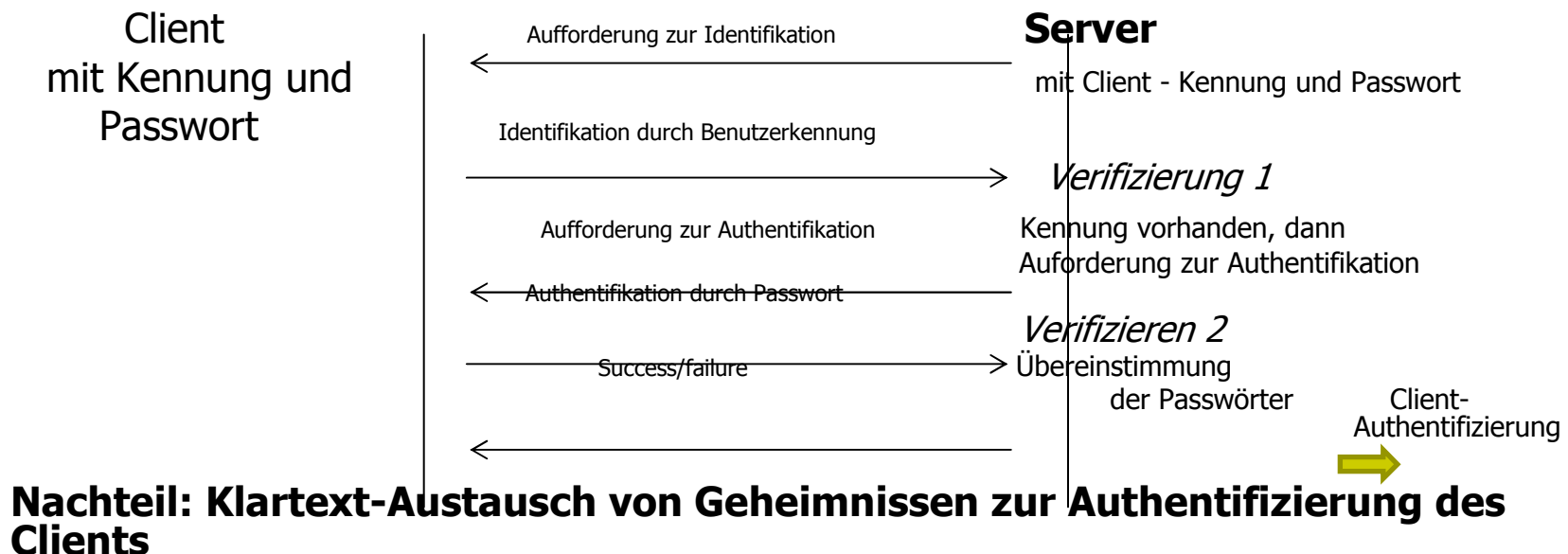
Verschiedene Authentifikationsprotokolle

zwischen anfragenden Client und Dienste anbietenden Server

Authentifizierung

(A) Alphanumerische Merkmale

Klassisch: Zugangskontrolle durch Passwort-Verfahren





Authentifizierung

(A) Alphanumerische Merkmale

Besser: Benutzerkennung und Passwörter verschlüsselt übertragen !

Problem Passwort Cracking: Verschlüsselte Passwortdatei auf Server für lesende Zugriffe öffentlich zugänglich; Angreifer rät ein Passwort, verschlüsselt es und vergleicht es mit der Passwortdatei

Anforderungen an Passwörter: mindestens 8 Zeichen, darunter Buchstaben, Ziffern und Sonderzeichen; kurze Verfallzeiten; keine Wiederholung u.a.

Systemgenerierte Passwörter: Zufallszeichenfolge hoher Qualität notwendig !

Beispiel: **Personal Identification Number (PIN) der Eurocheque-Karte**

Tripel-DES zur Verschlüsselung des Klartextes bestehend aus
Kontonummer, Bankleitzahl und Kartensequenznummer; kurze DES-
geringer Zufall !

Schlüssel,

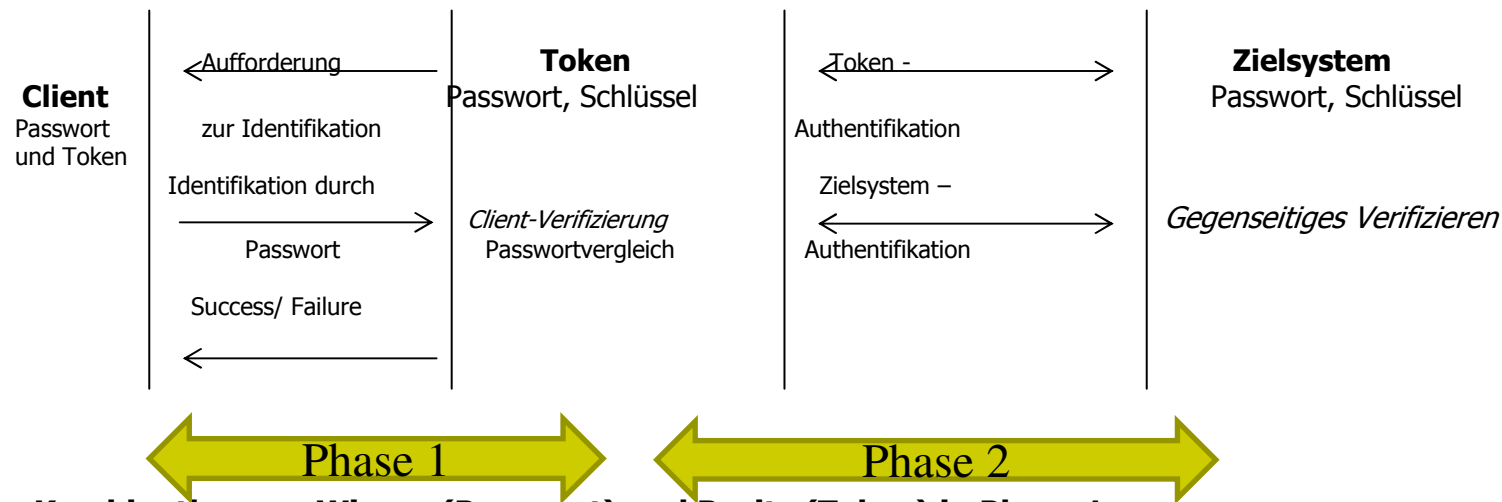
Authentifizierung allein durch Passwörter bzw. PIN ist nur in geschützten Netzen ausreichend (mindestens aber: Einmal-Passwörter aus vereinbarter Liste)

Authentifizierung

(B) Alphanumerische und gegenständliche Merkmale

Benutzer ist im Besitz eines persönlichen Tokens (u.a. Smart Card)

Authentifizierung in 2 Phasen: (A) Client – Token und (B) Token - Zielsystem



Kombination von Wissen (Passwort) und Besitz (Token) in Phase 1

Authentifizierung in Phase 2 erfolgt durch Challenge-Response Protokolle

Authentifizierung

(B) Alphanumerische und gegenständliche Merkmale

Authentifizierung durch die Kombination von Wissen (Passwort) und Besitz (Token) erhöht die Sicherheit erheblich

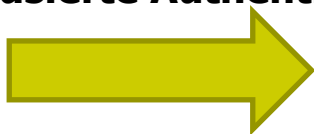
Phase 2 – Authentifizierung erfolgt mit symmetrischen bzw. asymmetrischen Verschlüsselungsverfahren (u.a. 3DES, IDEA, RSA, ElGamal)

Token in Form von Chipkarten speichern Passwörter, symmetrische und/oder asymmetrische Schlüssel und berechnen Hashwerte sowie digitale Signaturen

Benutzerdatenbank im Zielsystem ist besonders zu schützen

Gegenseitige Authentifizierung von Token und Zielsystem verhindert Maskerade-Angriffe

Chipkartenbasierte Authentifizierung lässt sich durch biometrische Verfahren erweitern



Smart Card - basierte Lösungen liefern optimale Authentifizierung und Zugangskontrolle

Authentifizierung

(C) Gegenständliche und persönliche Merkmale

Authentifizierung durch die Kombination von Token und körperlichen Merkmalen von Benutzern, wie Fingerabdruck und Iriserkennung, gewährleistet individuelle Benutzerverifikation

Jeder Benutzer ist ein Individuum und seine körperlichen Merkmale sind einmalig !

**Benutzer identifiziert sich mittels eines körperlichen Merkmals, wie Fingerabdruck, gegenüber dem persönlichen Token und dieses gegenüber dem Zielsystem
Persönliche Merkmale sind nur sehr schwer fälschbar**

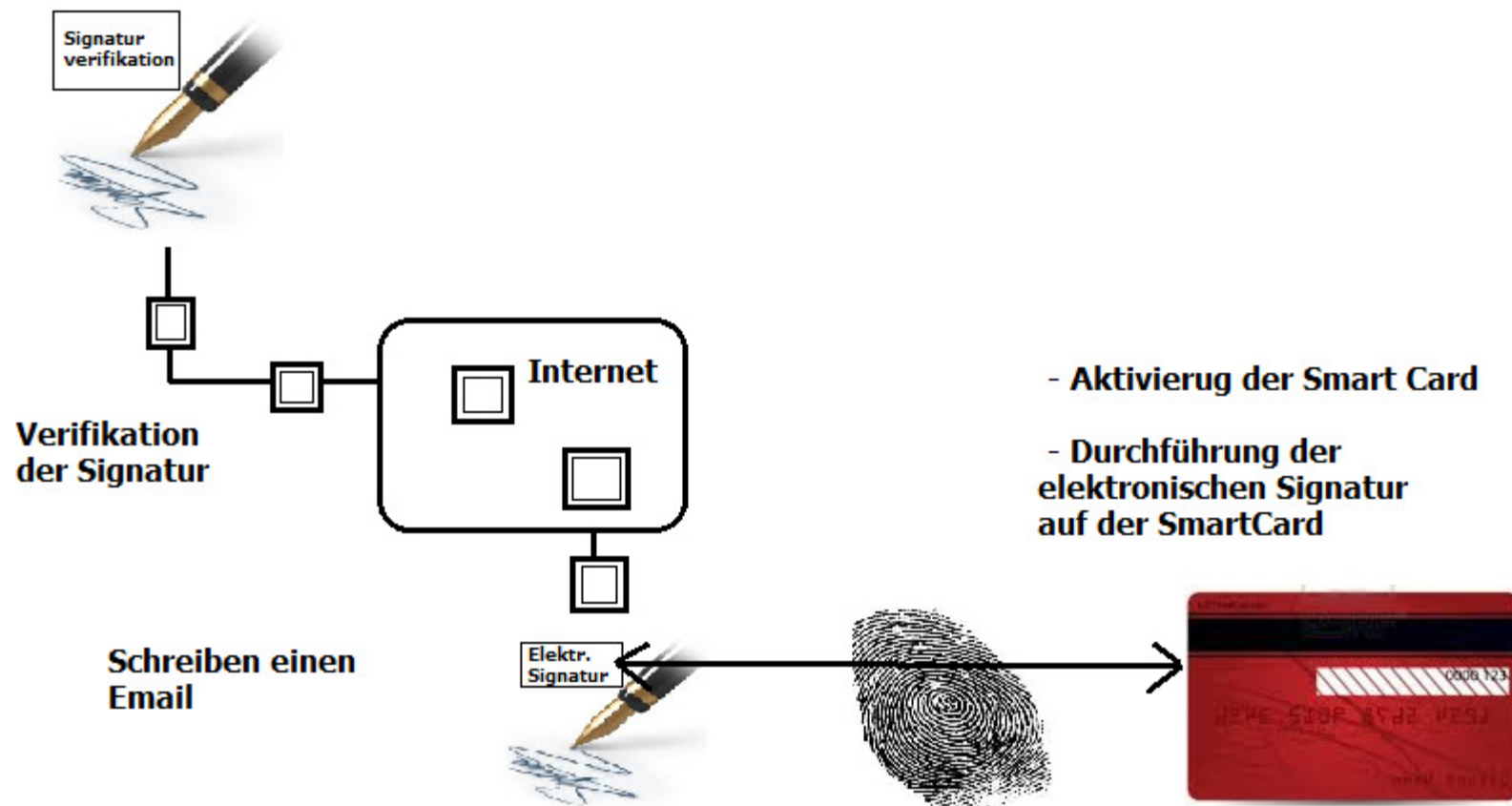
Single Sign On, d.h. gleichzeitiger Zugang zu allen Anwendungen und Systemen, für die der Benutzer autorisiert ist, wird praktisch möglich



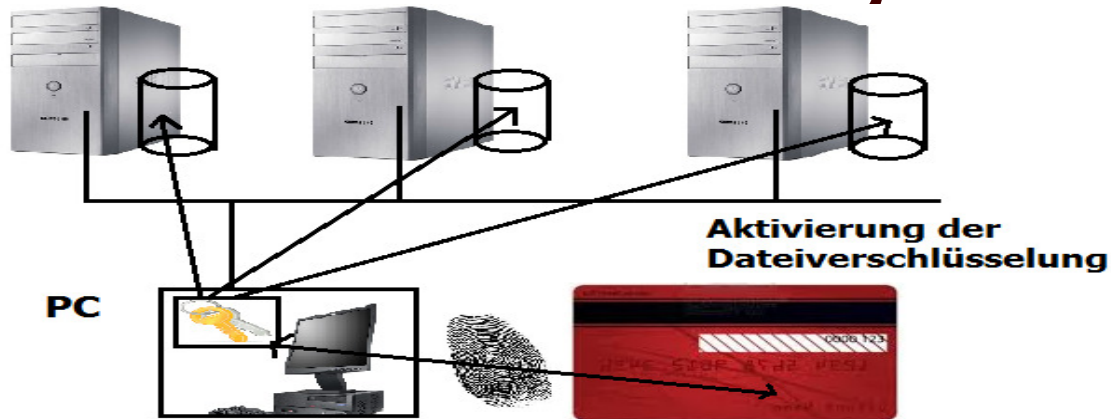
Smart Card - basierte Lösungen mit biometrischen Merkmalen liefern Authentifizierung und Zugangskontrolle mit hoher Sicherheit

Authentifizierung

Signatur und eMail-Sicherheit



Authentifizierung



Signatur und Datei-Sicherheit



Authentifizierung

Authentifikationsprotokoll mit Challenge- Response Verfahren

- Authentifizierung des Clients durch Server nach erfolgreichem Protokollverlauf
- Client und Server verfügen über zuvor ausgetauschte Geheimnisse
- Geheime Informationen werden nicht direkt übertragen

Prinzip Client erhält auf Anfrage eine einmalige Zufallszahl (Challenge) vom Server, die er mit seinem Geheimnis verknüpft und an den Server zurücksendet
Server verifiziert den Client anhand seines Geheimnisses und kann eine Authentifizierung vornehmen

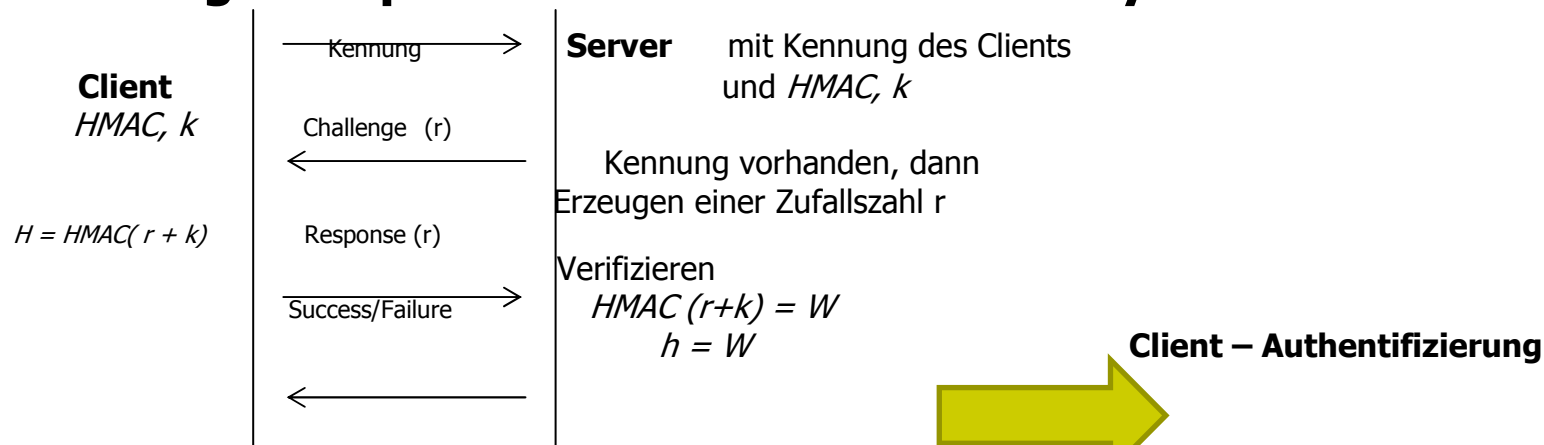
Verfahrensklassen

Hashwertbasierte Authentifizierung (symmetrische Verschlüsselung)

Authentifizierung mit digitaler Signatur (asymmetrische Verschlüsselung)

Authentifizierung

Challenge-Response Verfahren mit einer keyed Hashfunktion



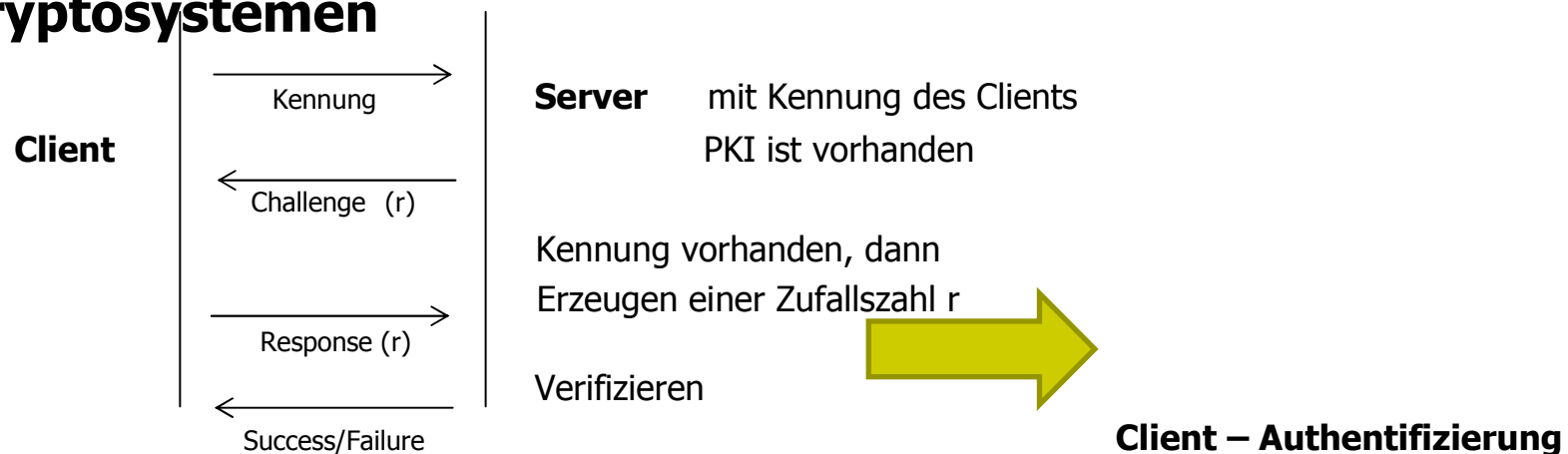
Jede weitere Protokollnachricht wird mit dem Hashwert der Nachricht authentifiziert.

Vorteil: kein Austausch von Geheimnissen zur Authentifizierung des Clients

Nachteil: der geheime Schlüssel muss zuvor mit jedem Kommunikationspartner sicher ausgetauscht werden;
entspricht nur einer (einfachen) elektronischen Signatur

Authentifizierung

Challenge-Response Verfahren mit asymmetrischen Kryptosystemen



Vorteil: Wird die Signatur auf einer Smart Card signaturgesetz-konform erstellt, so liegt eine verbindliche Authentifizierung des Clients vor !

Chipkartenbasierte Authentifizierung:

1. Signierer authentifiziert sich gegenüber der Smart Card (PIN)
2. Smart Card authentifiziert sich gegenüber dem PC (CRV)
3. PC authentifiziert sich gegenüber der Smart Card (CRV)



Authentifizierung

Authentifikationsprotokoll mit Zero-Knowledge Verfahren

Spezialfall eines Challenge-Response Verfahrens

Server besitzt keine gespeicherten Geheimnisse über Client und kann diesen dennoch authentifizieren

Informationen werden zwischen Client und Server so ausgetauscht, dass ein Dritter keinerlei Kenntnis des Geheimnisses zur Authentifizierung erlangt

bekanntes Verfahren stammt von Fiat und Shamir: Fiat-Shamir Verfahren

Voraussetzung vertrauenswürdige Zertifizierungsinstanz (Trust Center)

Prinzip

Setup: Trust Center und Chipkarte mit einer öffentlichen eindeutigen Kennung verfügen über ein Geheimnis bestehend aus k Zahlenwerten und zugehörigen k öffentlichen Werten

Authentifizierung: Client (Chipkarte) und Server tauschen Hilfswerte nach dem Challenge-Response Verfahren so aus, dass der Server eine Authentifizierung vornehmen kann, ohne die geheimen k Zahlenwerte kennen zu müssen.



Authentifizierung

Authentifikationsprotokoll PPP

Das PPP-Protokoll stellt zwei verschiedene Möglichkeiten der Authentifizierung von Clients zur Verfügung:

- Password Authentication Protocol (PAP)**
- Challenge-Handshake Authentication Protocol (CHAP)**

Nach dem Verbindungsaufbau definiert das CHAP-Protokoll drei Pakete, die im Informationsfeld von PPP-Frames übertragen werden (bei PAP nur zwei). Bei PAP wird das Passwort im Klartext übertragen und bei CHAP „verschlüsselt“ im Hashwert. Die Hashfunktion H wird auf eine Kombination der Zufallsfolge C (Challenge) und des Passworts PW des Benutzers angewandt.

Die Authentifizierung ist ein Teil des LCP-Protokolls und erfolgt nach der Verbindungsaufbauphase. Die Authentifizierung ist beim Aufbau einer PPP-Verbindung optional.



Authentifizierung

Authentifikationsprotokoll Kerberos

Ziel: Client Authentifizierung und geheimer symmetrischer Schlüssel für Kommunikation zwischen Client und Service Server



Authentifizierung

Authentifikationsprotokoll WLAN 802.1x/EAP

1. Mobile Client (MC) meldet sich beim Access Point (AP) an
2. AP blockiert alle IP requests des Clients und verlangt dessen Identifikation (username,password)
3. Die User credentials leitet der AP (durch den uncontrolled port) weiter zum Authentifikations-Server (AS), der den Authentifikations-Dialog zwischen MC und AS beginnt
4. AS (mit RADIUS) und MC führen einen EAP authentication dialog (mehrere Anfragen und zugehörige Antworten) über den AP hinweg durch (EAP messages zwischen MC und AP sind in LAN frames und zwischen AP und AS in RADIUS packets eingekapselt)
5. Nach erfolgreicher Authentifizierung des MC öffnet der AP seinen controlled port, um die eindeutige Verbindung mit dem MC herzustellen(nur der MC wurde authentifiziert – one way authentication)
6. Verschlüsselter Datentransfer zwischen MC und AP nach dem WEP Protokoll kann beginnen