Authentikationsverfahren

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

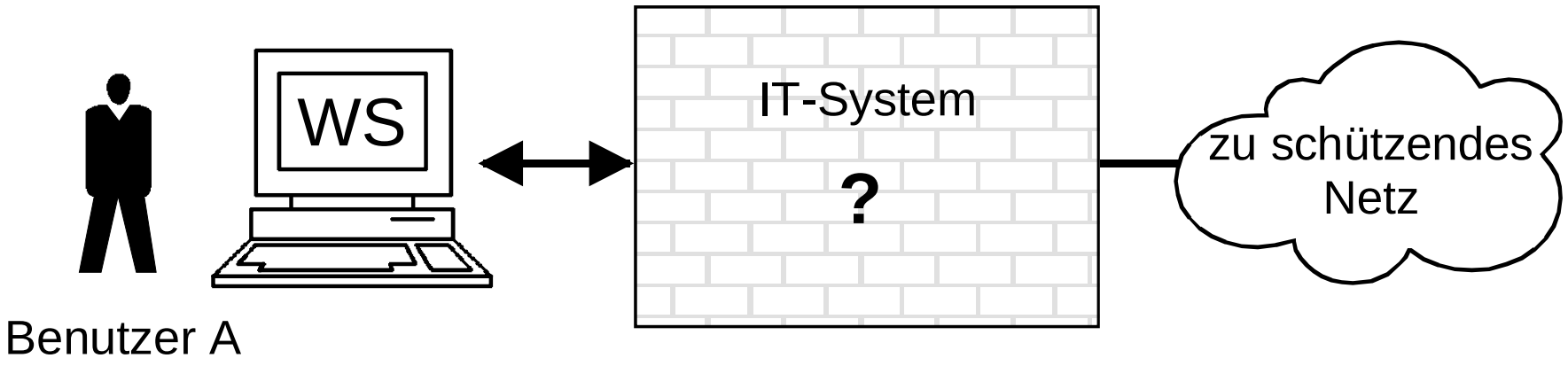
- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren S/Key
- Security Token (Digipass)
- SSL Client Authentikation
- Authentikationsverfahren mittels Mobilfunk
- Authentikation mit der Signaturkarte
- Zusammenfassung

Inhalt

- **Identifikation und Authentikation**
  - Generelle Authentikationsverfahren
  - Passwort-Verfahren - Passwortregeln
  - Einmal-Passwort-Verfahren S/Key
  - Security Token (Digipass)
  - SSL Client Authentikation
  - Authentikationsverfahren mittels Mobilfunk
  - Authentikation mit der Signaturkarte
  - Zusammenfassung

Indentifikation und Authentikation

Wer ist tatsächlich Benutzer A ?



- Wenn ein Nutzer Zugang haben möchte, muss er sich dem IT-System gegenüber
  - **identifizieren** und
  - **authentisieren**

Identifikation

- Die **Identifikation** ist die Überprüfung eines vorgelegten, kennzeichnenden Merkmals, z.B. des Benutzernamens.
- Eine Person wird eindeutig durch die Angabe von Vorname, Nachname, Geburtsort und Geburtstag identifiziert.
- In Deutschland wird die Eindeutigkeit der Identifikation von den Standesämtern garantiert.
- Eine Identifikation muss immer innerhalb eines Systems (Organisation) abgesprochen sein, damit sie eindeutig ist.
- Damit eine solche Absprache mit verschiedenen Benutzern zustande kommt, müssen klar definierte Regeln eingehalten werden.
- Ein Beispiel:
  - CCITT »Recommendation« X.509 bzw. ISO 9594-8
  - Ein Konzept eindeutiger, kennzeichnender Namen oder »distinguishing identifier«

Authentikation

- **Authentikation** bezeichnet einen Prozeß, in dem überprüft wird, ob »jemand« oder »etwas« echt oder berechtigt ist.
- Authentikation bedeutet die Verifizierung (Überprüfung) der Echtheit bzw. der Identität.
- Die Überprüfung des Personalausweises einer Person ist eine solche Authentikation.
- Was muss und kann z.B. identifiziert und authentisiert werden ?
  - Kommunikationspartner: z.B. Benutzer, Prozesse, Instanzen, das Security Management
  - Kommunikationsmedien: z.B. Workstation, Serversysteme, Firewall-Elemente (Packet Filter, Application Gateway, Proxy, Security Management), Security Token usw.
  - Nachrichten: z.B. Mails, Dateien, Java-Applets usw.

Inhalt

- Identifikation und Authentikation
- **Generelle Authentikationsverfahren**
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren S/Key
- Security Token (Digipass)
- SSL Client Authentikation
- Authentikationsverfahren mittels Mobilfunk
- Authentikation mit der Signaturkarte
- Zusammenfassung

Generelle Authentikationsverfahren
→ Übersicht

- **Passwort-Verfahren**
  - Einfachste Authentikationsverfahren
  - Wenn das Passwort im Klartext über das Internet übertragen wird, dann kann es mitgelesen und mißbräuchlich verwendet werden
  - Passwortregeln müssen eingehalten werden

- **Einmal-Passwort**
  - Jedes Passwort wird nur einmal verwendet
  - Zwei unterschiedliche Methoden:
    - Passworte werden im Vorfeld bestimmt und verteilt
    - Benutzer kann sie nach einem definierten Verfahren berechnen

- **Challenge-Response-Verfahren**
  - Benutzer muss sich spontan kryptographisch beweisen
  - Dazu braucht er einen Schlüssel und ein Verfahren
  - Z.B. Zufallszahl als Challange, Signatur dieser als Response

Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- **Passwort-Verfahren - Passwortregeln**
- Einmal-Passwort-Verfahren S/Key
- Security Token (Digipass)
- SSL Client Authentikation
- Authentikationsverfahren mittels Mobilfunk
- Authentikation mit der Signaturkarte
- Zusammenfassung

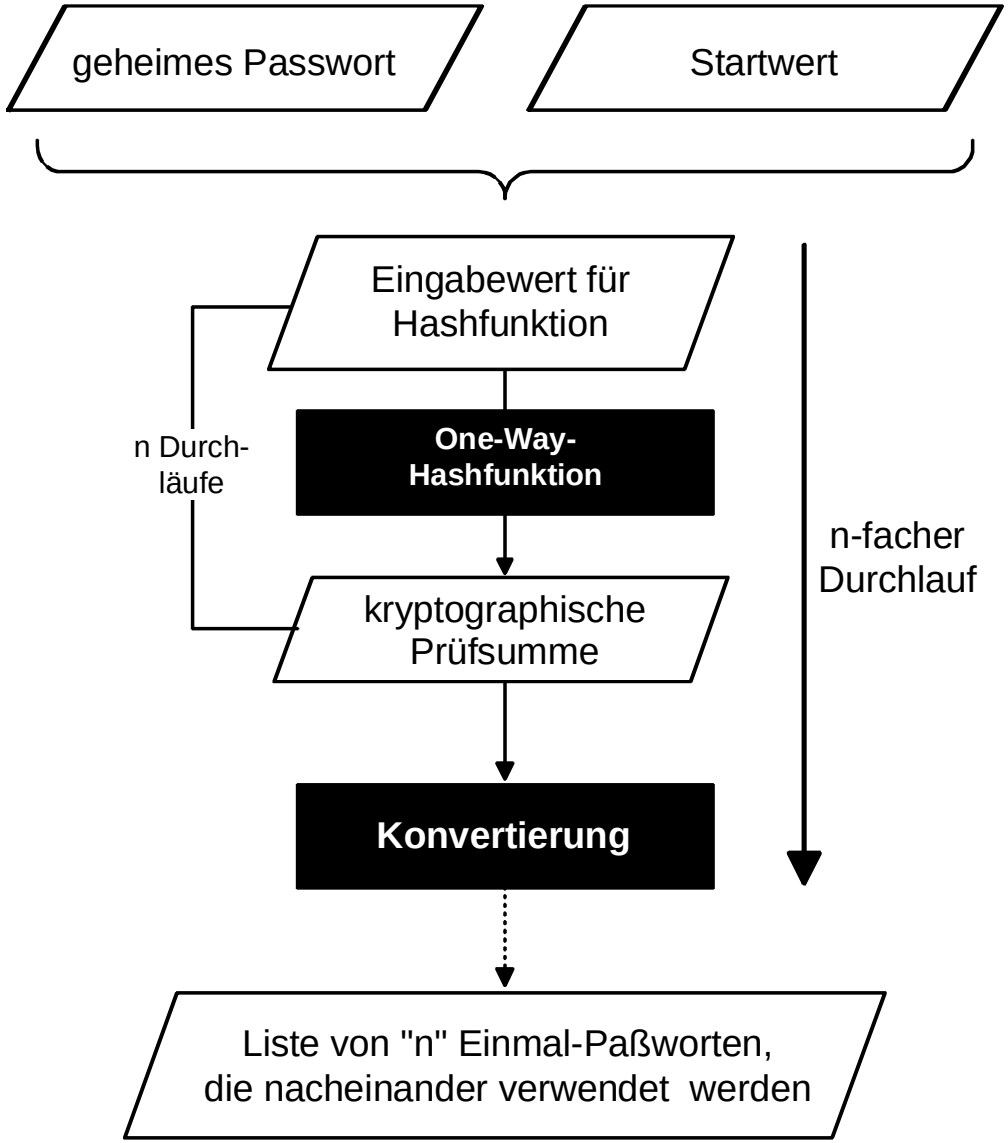
Passwort-Verfahren
→ Die wichtigsten Passwortregeln (GDD)

- Nirgends notieren! Niemandem mitteilen!
- Das Passwort darf nur dem Nutzer bekannt sein.
- Mindestlänge: 6 Stellen
- Vor- und Familiennamen nie (allein) verwenden, sondern:
- stets alphanumerisch gestalten (Buchstaben und Zahlen/Zeichen).
- Keine Trivialpassworte (z. B. 4711, 12345 oder andere nebeneinander liegende Tasten) verwenden.
- In angemessenen Zeitabständen ändern; nicht zu oft!
- Automatisch verhindern, dass (aus Bequemlichkeit) als neues wieder das alte Passwort gewählt wird.
- Für besonders wichtige Funktionen/sensible Daten: Zusatzpasswort (»4- Augen-Prinzip«). Oder zwei Personen kennen je das halbe Passwort.
- Passwort des Systemverwalters - nur ihm bekannt - für Vertretungsfall versiegelt aufbewahren.

Inhalt

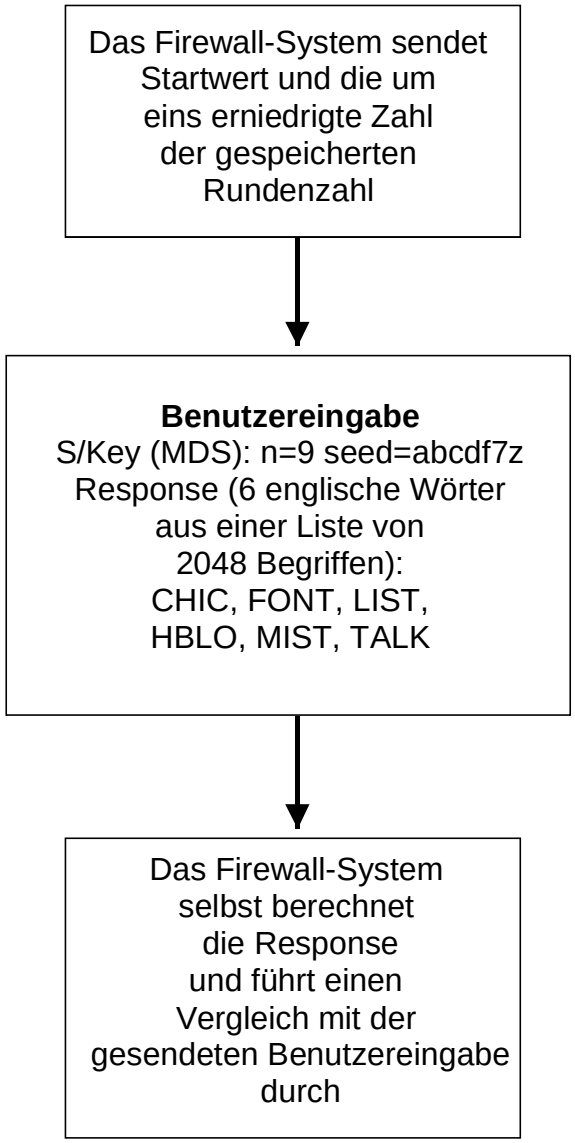
- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- **Einmal-Passwort-Verfahren S/Key**
- Security Token (Digipass)
- SSL Client Authentikation
- Authentikationsverfahren mittels Mobilfunk
- Authentikation mit der Signaturkarte
- Zusammenfassung

Einmal-Passwort-Verfahren S/Key (1/3)
→ S/Key-Berechnung



- Das Einmal-Passwort besteht aus sechs englischen Wörtern

Einmal-Passwort-Verfahren S/Key (2/3)
→ S/Key-Ablauf



Einmal-Passwort-Verfahren S/Key (3/3)
→ Bewertung

- **Vorteile des S/Key-Verfahrens**
  - Die Software auf dem Client ist einfach zu handhaben
  - Sie ist für viele Rechnersysteme verfügbar

- **Nachteile des S/Key-Verfahrens**
  - Die Speicherung der geheimen Informationen beim Client ist problematisch (Passwort)
  - Sechs englische Begriffe müssen eingegeben werden

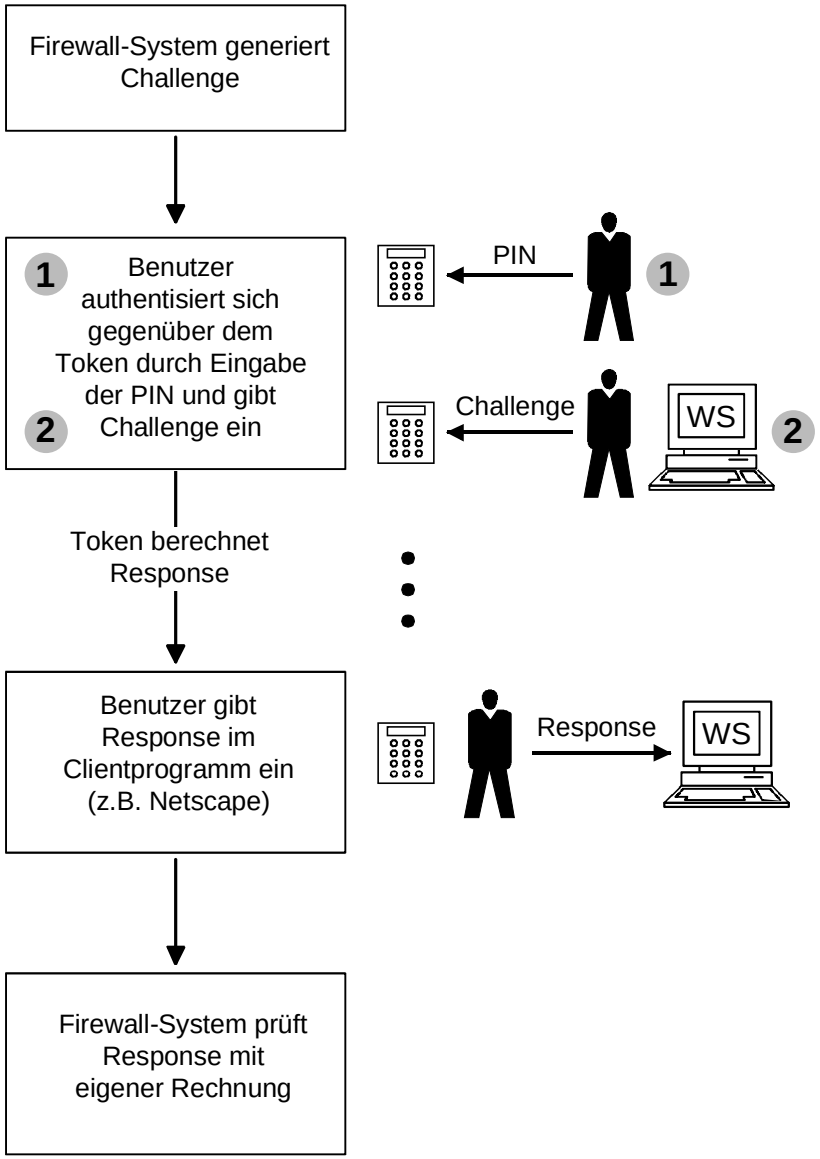
Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren S/Key
- **Security Token (Digipass)**
- SSL Client Authentikation
- Authentikationsverfahren mittels Mobilfunk
- Authentikation mit der Signaturkarte
- Zusammenfassung

Security Token (1/3)
→ Verfahren

- Benutzer hat ein persönliches Security Token
- Firewall-System hat ein Sicherheitsmodul, welches Callenges für die Benutzer/Security Token berechnet
- Die Firewall sendet eine Challenge an den Benutzer
- Der Benutzer berechnet mit Hilfe des Security Tokens die Response
- Das Sicherheitsmodule muss überprüfen, ob die Response zur Challenge passt.

Security Token (2/3)
→ Ablauf



Security Token (3/3)
→ Bewertung

- **Vorteile eines Security Tokens**
  - Das Verfahren stellt keine besondere Anforderung an die Hardware und Software des Benutzers
  - Der Austausch von Challenge und Response wird über Anzeige und Tasten des Rechnersystems und des Security Token durchgeführt
  - Dieses Verfahren ist besonders sicher, da das Security Token eine sichere Hardware ist

- **Nachteile eines Security Tokens**
  - Für den Benutzer ist das Security-Token-Verfahren aufwendig, da es in mehreren Schritten durchgeführt wird
    - Aktivieren des Security Tokens
    - Eingabe der Challenge und
    - Eingabe der Response

Inhalt

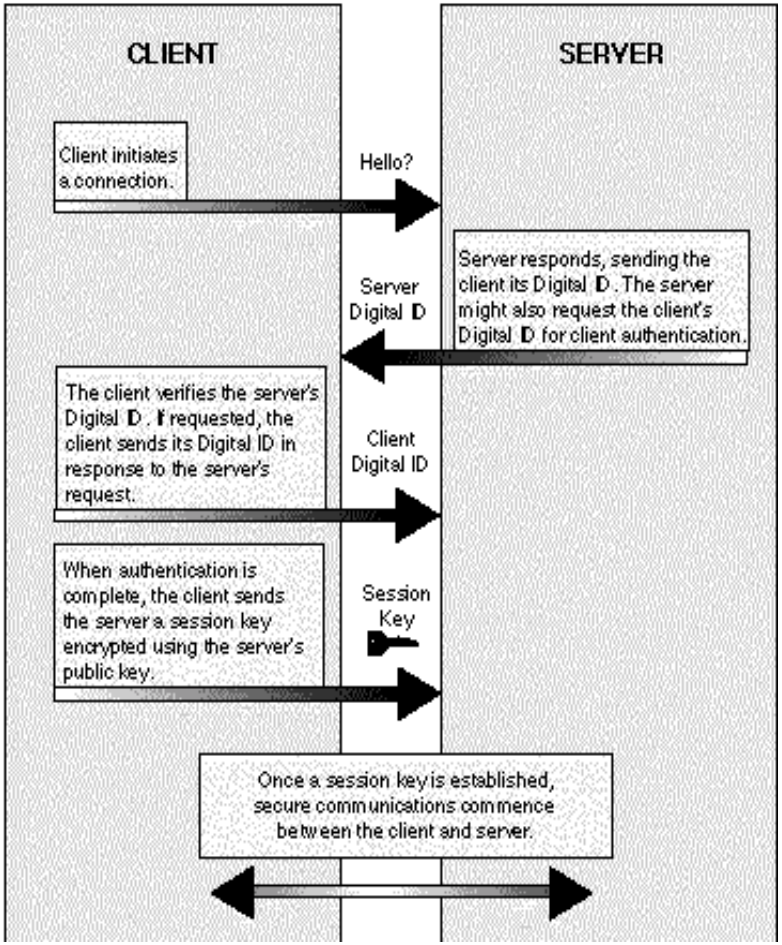
- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren S/Key
- Security Token (Digipass)
- **SSL Client Authentikation**
- Authentikationsverfahren mittels Mobilfunk
- Authentikation mit der Signaturkarte
- Zusammenfassung

SSL-Authentikation
→ Server Authentikation

- Serverzertifikate
  - SSL-Zertifikate:
    - SSL= Secure Socket Layer, Protokoll von Netscape
    - Authentikation i.R. zwischen Server und Client
      auch zwischen Client und Server möglich
    - Verschlüsselung des Datenstroms zwischen Server und Client
    - Datenintegrität für Online-Transaktionen
    - Unterschiedliche Verschlüsselungsstärken (40, 56, 128 bit)
    - Hybrides Verschlüsselungsverfahren:
      Schlüssel: asymmetrisch, eigentlichen Daten: symmetrisch

Zertifikate: SSL-Server Zertifikat
→ Server Authentikation

- Verschlüsselt den Datenstrom zwischen Server und Client

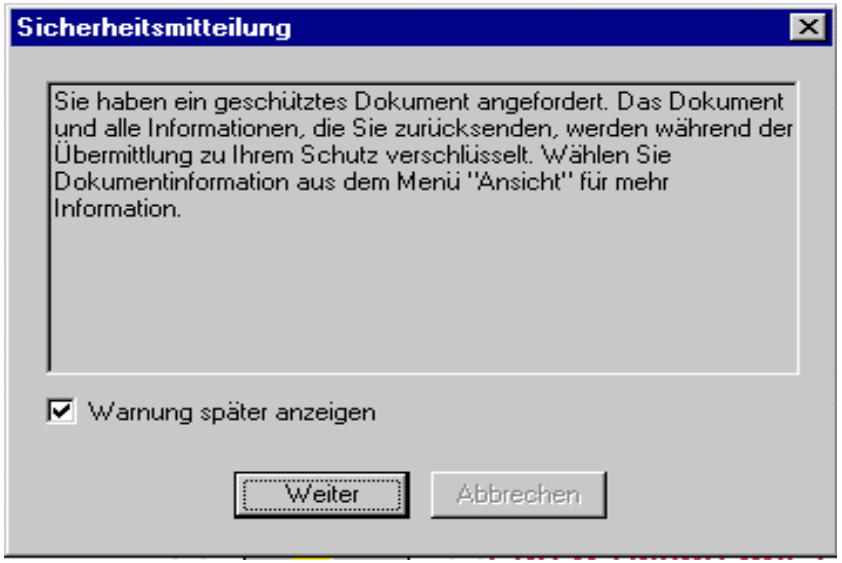


Ablauf:

1. Client wählt Internetseite an
2. Server übermittelt dem Client sein öffentliches Zertifikat
3. Client prüft das Zertifikat auf Gültigkeit
4. Client generiert Zufallszahl (=Sessionkey), verschlüsselt diese für den Server
5. Server entschlüsselt die Zufallszahl und verschlüsselt die Daten nun mit dem Sessionkey für den Client.
6. Verschlüsselter Datenaustausch zwischen Server und Client

Hinweise im Browser auf eine SSL-Verbindung

- 1. Benutzerhinweis



- 2. „Ungeöffnetes Schloß“ in der Statuszeile / Titelleiste des Browser

Beispiel:
SSL-Verschlüsselung nur Server - Authentikation

- Web-Mail Zugang von T-Online:
  - https://webmail.t-online.de
    56 bit Verschlüsselung
- Online-Banking der Commerzbank, Frankfurt
  - https://comline01.commerzbank.com/.....

    128 bit Verschlüsselung

Zertifikatsinformationen

Gültigkeitszeitraum

Organizational Unit

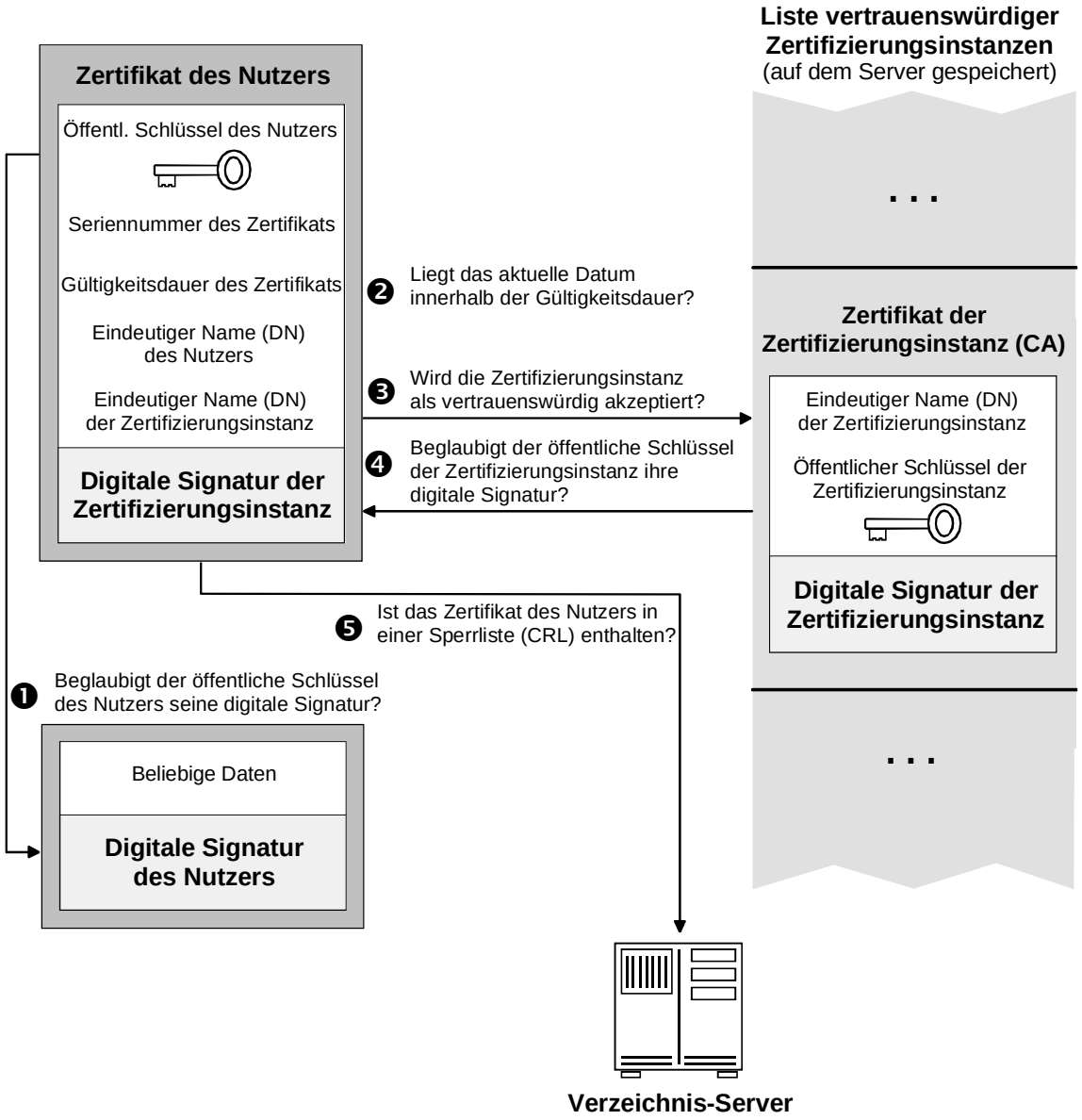
Common Name:
muss mit der URL übereinstimmen ,
Firmennamen enthalten

VeriSign als Herausgeber des Zertifikates

SSL Client Authentication

- Mit Hilfe von SSL (Secure Socket Layer) kann auch eine Client Authentication realisiert werden
- Der Client schickt dem Server seinen öffentlichen Schlüssel in Form eines Zertifikats und zusätzlich Daten, die mit dem geheimen Schlüssel des Clients digital signiert wurden.
- Das Zertifikat wurde zuvor von einer vertrauenswürdigen unabhängigen Institution, einer Zertifizierungsstelle, ausgestellt und enthält neben dem öffentlichen Schlüssel des Client, Informationen, die diesen eindeutig identifizieren.
- Um die Echtheit und Integrität des öffentlichen Schlüssels zu garantieren, ist das Zertifikat mit dem privaten Schlüssel der Zertifizierungsstelle signiert (z.B. VeriSign, GobalSign).

Überprüfung eines Client-Zertifikats



Ablauf der Client-Authentikation (1/2)

- Der Server überprüft die digital signierten Daten mit dem öffentlichen Schlüssel des Client, der dem Client-Zertifikat entnommen werden kann.
- Verläuft die Überprüfung erfolgreich, ist die Zusammengehörigkeit des öffentlichen und des geheimen Schlüssels des Clients verifiziert. Außerdem steht damit fest, dass die signierten Daten nach der Signatur nicht verändert wurden.
- Die Zusammengehörigkeit vom öffentlichen Schlüssel und dem DN (Distinguished Name) des Client-Zertifikats ist damit hingegen nicht bewiesen.
- Der Server überprüft den Gültigkeitszeitraum des gesendeten Client-Zertifikats.

Ablauf der Client-Authentikation (2/2)

- Der Server überprüft anhand des DN (Distinguished Name) und der ihm vorliegenden Liste, ob es sich bei der ausstellenden CA (Certification Authority) um eine bekannte CA handelt.
- Das Zertifikat des Client wird dann mittels des öffentlichen Schlüssels der ausstellenden CA überprüft.
  Der öffentliche Schlüssel der CA wird der Liste der bekannten CAs entnommen.
- Dieser optionale Schritt erlaubt es, eine CRL (Certificate Revocation List) einzubinden.
  Hier kann überprüft werden, ob das Zertifikat des Client in der Zwischenzeit gesperrt wurde, obwohl der Gültigkeitszeitraum noch nicht abgelaufen ist.

SSL Authentikation
→ Bewertung

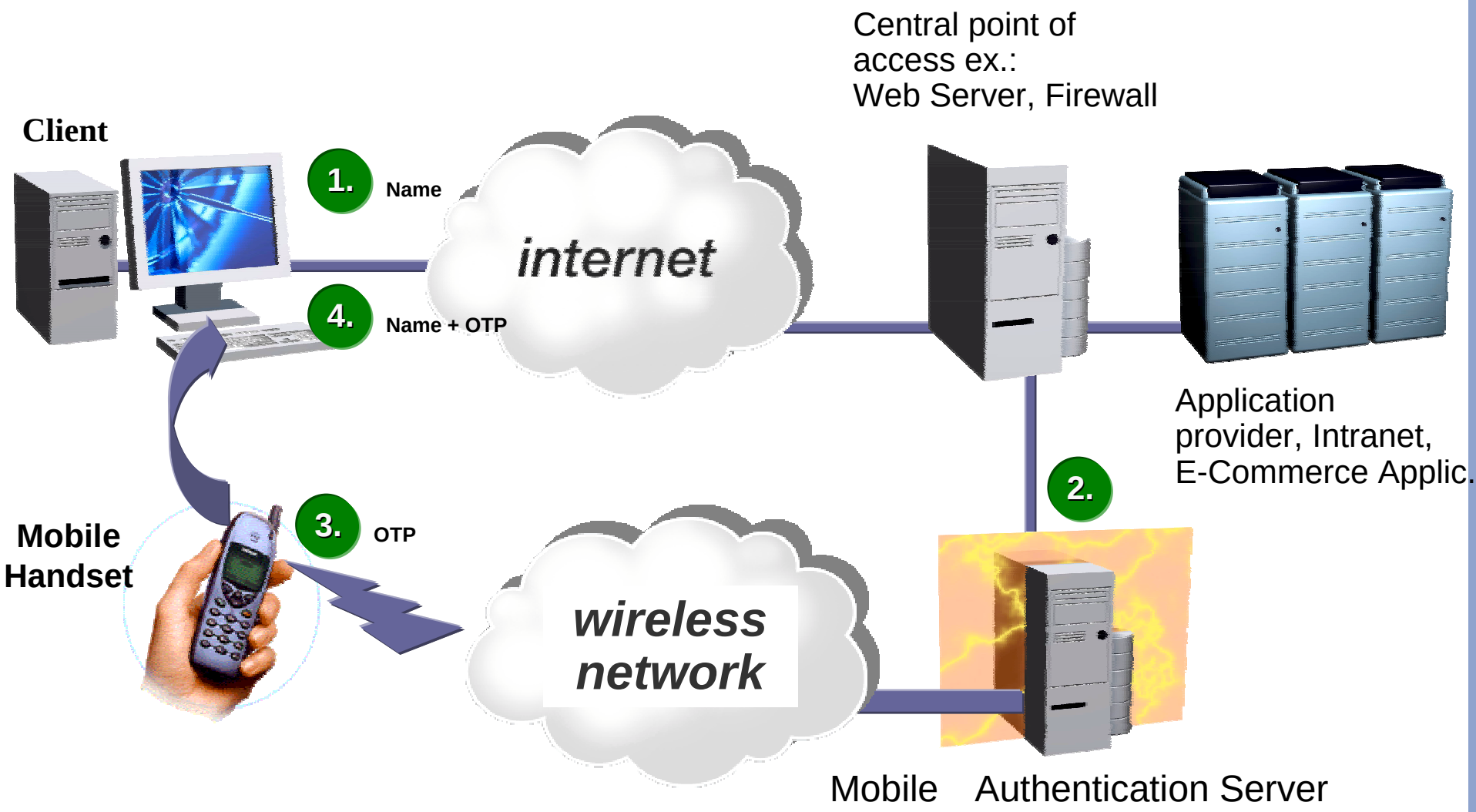
- Die Qualität der SSL-Client-Authentikation hängt ab von :
  - Der Vertrauenswürdigkeit der Zertifizierungsinstanz
  - Dem Level, auf dem die Zertifizierungsinstanz die Authentizität des Teilnehmers überprüft
  - Der Bereitstellung einer CRL (Certificate Revocation List) durch die Zertifizierungsinstanz

- Verschiedene Zertifizierungs-Anbieter bieten unterschiedliche Klassen von Zertifikaten an.
  - Ein Zertifikat der Klasse 1 bekommt der Teilnehmer schon nach der Zusendung des Namens und der E-Mail-Adresse, ohne dass seine Identität näher geprüft wird.
  - Für ein Zertifikat der Klasse 2 wird z.B. die Zusendung einer Kopie des Ausweises oder des Führerscheins verlangt.
  - Bei höheren Klassen muss der Teilnehmer sich persönlich (z.B. mit Hilfe des Ausweises) bei einer Registration Authority (RA) authentisieren.
    Hierbei stellt sich die Frage, wie vertrauenswürdig eine solche Registration Authority (RA) ist.

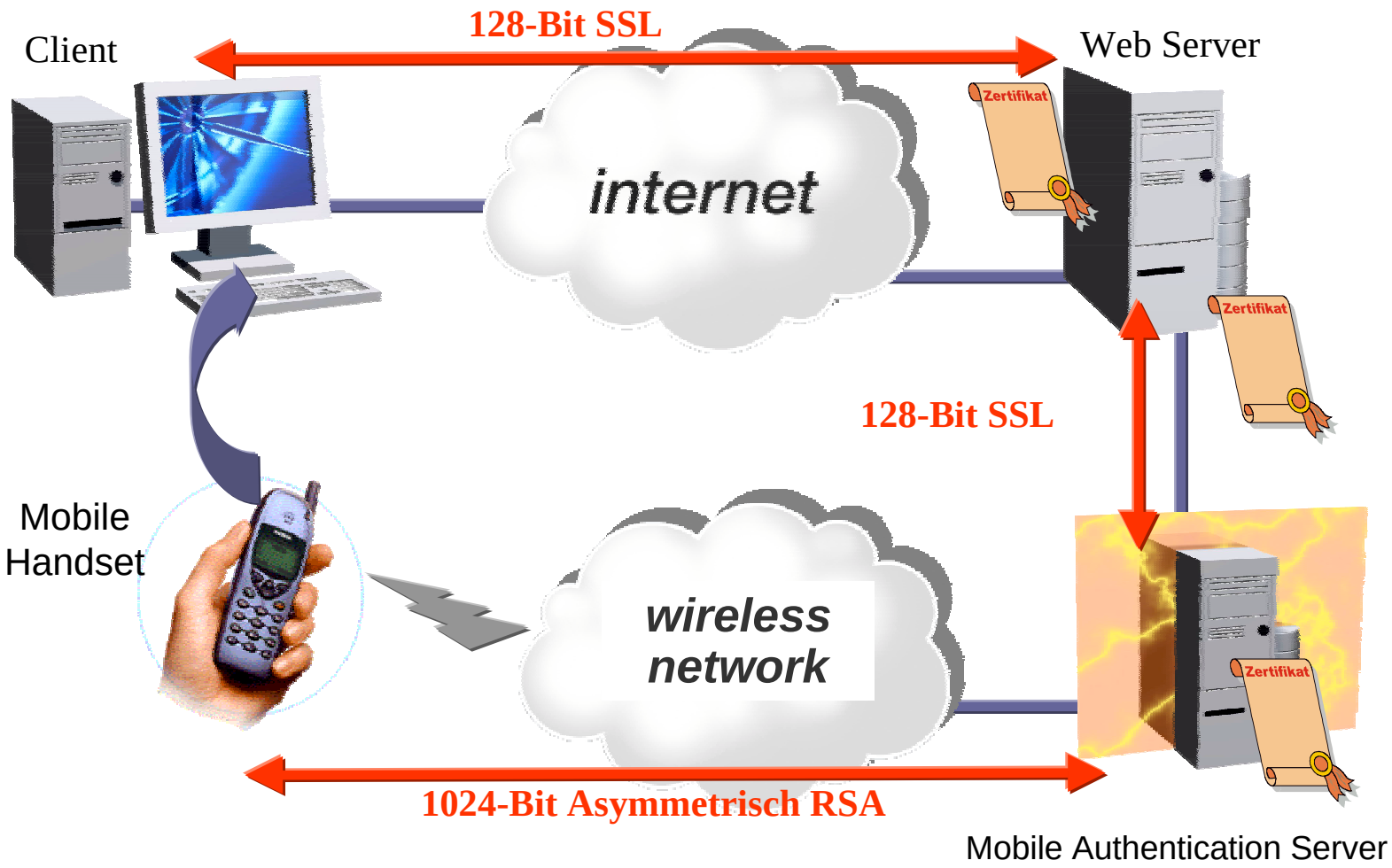
Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren S/Key
- Security Token (Digipass)
- SSL Client Authentikation
- **Authentikationsverfahren mittels Mobilfunk**
- Authentikation mit der Signaturkarte
- Zusammenfassung

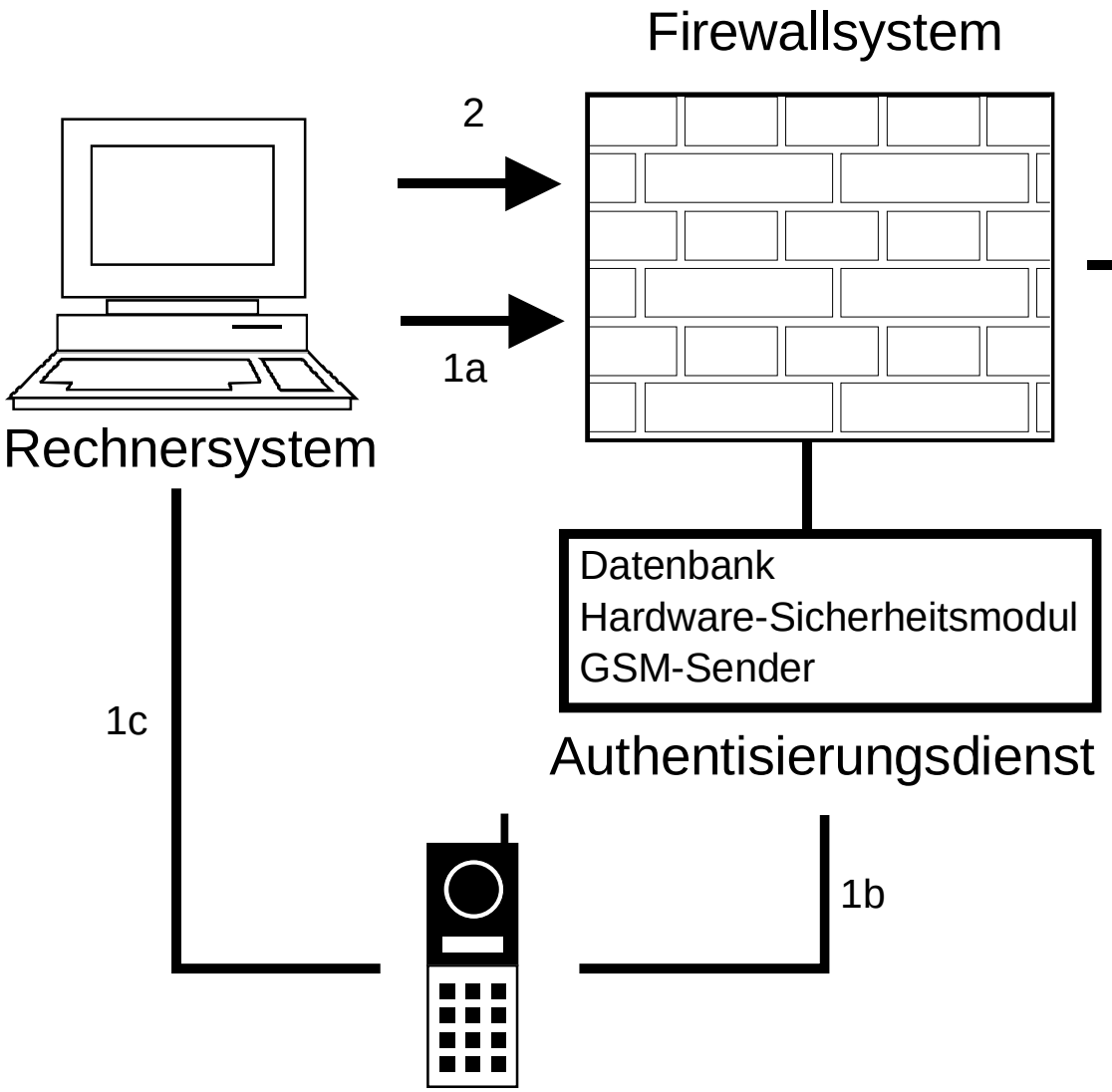
Authentikationsverfahren mittels Mobilfunk
→ Überblick (1/2)



Authentikationsverfahren mittels Mobilfunk
→ Überblick (2/2)



Authentikationsverfahren mittels Mobilfunk



1 a, b, c	Passwort-Anforderung u. -Übermittlung
2	Authentisierung
3	Erlaubter Zugriff auf Webserver

Authentikationsverfahren mittels Mobilfunk
→ Bewertung

Einmal Passwort

- Keine Speicherung des Passwortes notwendig
- Individuelle Generierung on Demand
- Kryptographisch starke Passwörter

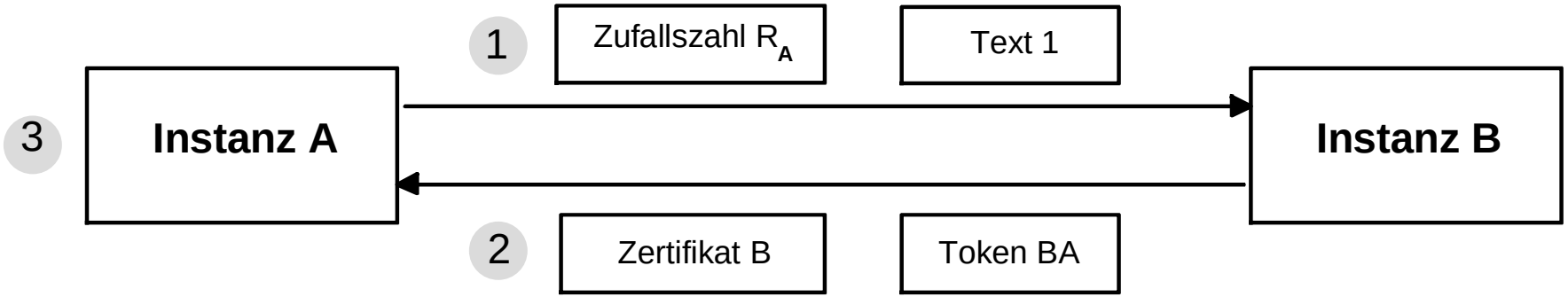
- **Administration**
  - Kein Vergessen von Passwörtern mehr
    - Benutzerkomfort
    - Kostenersparnisse
  - Administration beinhaltet nur das Registrieren von Benutzern

- **Nutzung von vorhandener Infrastruktur**
  - Mobiltelefon
  - keine Software und deren Installation/Wartung auf der Client Seite notwendig
  - kann für mehrere Anwendungen verwendet werden

Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren S/Key
- Security Token (Digipass)
- SSL Client Authentikation
- Authentikationsverfahren mittels Mobilfunk
- **Authentikation mit der Signaturkarte**
- Zusammenfassung

Signaturkarte (SmartCard)



- **Aufbau des TokenBA:**
  TokenBA = R_B // A // R_A // Text3 // sS_B (R_B // A // R_A // Text2)
- sSX (Y) =
  Signatur der Daten Y unter Verwendung des geheimen Schlüssels SX
- ePX (Y) =
  Verschlüsselung der Daten Y unter Verwendung des öffentlichen Schlüssels PX
- A // B = Ergebnis der Konkatenation von A und B
- RX = Zufallszahl von X

Inhalt

- Identifikation und Authentikation
- Generelle Authentikationsverfahren
- Passwort-Verfahren - Passwortregeln
- Einmal-Passwort-Verfahren S/Key
- Security Token (Digipass)
- SSL Client Authentikation
- Authentikationsverfahren mittels Mobilfunk
- Authentikation mit der Signaturkarte
- **Zusammenfassung**

Authentikationsverfahren
→ Zusammenfassung

- Authentikationsverfahren sind die Grundlage für die Identifikation und Authentikation von Nutzern.
- Zunehmend wird es wichtiger, Authentikationsverfahren zu verwenden, die in der globalen handelnden Gesellschaft über staatliche Grenzen und Verantwortungsbereiche hinaus verwendet werden können.

Authentikationsverfahren

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen