Institut für Betriebssysteme und Rechnerverbund

Sicherheitsaspekte in e-Learning-Umgebungen unter Berücksichtigung digitaler Signaturkarten

Rainer David

Betreuer: Stefan Schmidt, Astrid Weilert

TECHNISCHE UNIVERSITÄT CAROLO-WILHELMINA ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund

Institut für Betriebssysteme und Rechnerverbund

Agenda

- **e-Learning Umgebungen**
  - Einführung
  - Modelle
  - Sicherheitsaspekte in e-Learning Umgebungen
- **Smartcards / Signaturkarten**
  - Einführung
  - Vorteile zu herkömmlichen Sicherheitsmechanismen
  - Programmierung (Standards, Middleware)
- **Ausblick**
  - Integration in die e-Learning Umgebung

TECHNISCHE UNIVERSITÄT CAROLO-WILHELMINA ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund

http://europa.eu.int/comm/education/elearning/indexde.html

Institut für Betriebssysteme und Rechnerverbund

e-Learning / Einführung

- **e-Learning ist eine zusätzliche technisch basierte Methode um sich Wissen anzueignen und ergänzt klassische Lernmodelle**
  - Anteil e-Learning am Bildungsbudget deutscher Firmen 2001: 2,4% (330 Mio Euro) / 2005: 15% (2 Mrd Euro)
- **Trägt dem Vorwissen des Lernenden besser Rechnung (asynchrones, selbstbestimmendes Lernen)**
- **Verbesserter Lerneffekt durch multimediale Inhalte und interaktive Komponente**
  - Enorme Kosten bei der Erstellung der Lerninhalte
  - Einsatz genormter Tuturials in unterschiedlichen Gebieten

13.05.2003
Sicherheitsaspekte in e-Learning-Umgebungen unter Berücksichtigung digitaler Signaturkarten.
TECHNISCHE UNIVERSITÄT CAROLO-WILHELMINA ZU BRAUNSCHWEIG

Institut für Betriebssysteme und Rechnerverbund

e-Learning / Modelle

- **Lokal begrenzte e-Learning Komponenten**
  - z.B. erstellt mit Macromedia Director
  - Sorgloser Einsatz multimedialer Inhalte
  - Verteilung und Installation notwenig
  - keine Lernkontrolle
- **Vernetzte e-Learning Umgebung**
  - WEB-Learning (z.B. Blackboard, Hyperwave)
  - Bandbreitenoptimierte Inhalte und Komponenten
  - Kommunikation und Diskussion (Nachrichten, Chat, Anmerkungen)
  - Zentraler Zugang über Internet (Bandbreite, Kosten)
  - Zentrale Lernkontrolle => Kursauswertung
  - Zentrale Administration (Gruppenverwaltung)
  - Zentrale Aktualisierung von Lerninhalten

Institut für Betriebssysteme und Rechnerverbund

e-Learning / Sicherheitsaspekte

- **Anmeldung (Benutzername, Passwort)**
  - Gefährdungspotential durch Belauschen oder „über die Schulter schauen“; Unsichere Wahl der Zugangsdaten

➔ ***Wandel von „innerbetrieblicher“ Fortbildung zu einer Dienstleistung***

- **Sicherstellung der Authentität des Benutzers**
- **Verschlüsselte und unveränderbare Informations-übertragung**
  - Prüfungsergebnisse
- **Rechtsverbindliche Vorgänge**
  - Annahme der Nutzungsbedingungen; Versicherungen
- **Finanztransaktionen**
  - Überweisungen des Semsterbeitrages; Skripte; Bücher (Handy: paybox; Zertifikat: T-Pay)

13.05.2003 Sicherheitsaspekte in e-Learning-Umgebungen unter Berücksichtigung digitaler Signaturkarten.
TECHNISCHE UNIVERSITÄT CAROLO-WILHELMINA ZU BRAUNSCHWEIG Institut für Betriebssysteme und Rechnerverbund

Institut für Betriebssysteme und Rechnerverbund

Beispiele für Sicherheitsmechanismen

T-Pay
Die Zukunft des Bezahlens im Internet.

- Installation eines Browserzertifikates (X.509) (Private/Public-Key Mechanismus)
- Abrechnung über Telefonrechnung

RSA SecurID Select

- Zeitbasierte Generierung von Zugangstoken
- Wechsel der Token alle 60 Sekunden

➔ **Notwendigkeit der Integration unterschiedlicher Sicherheitsmechanismen**

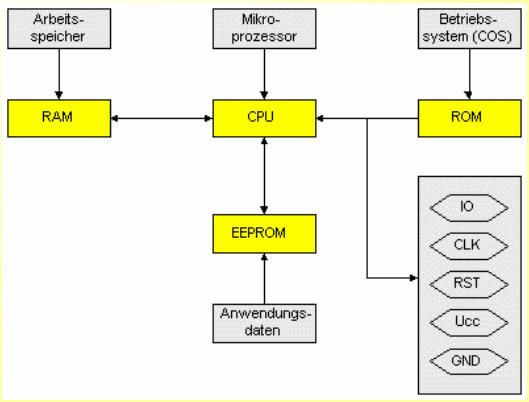
Institut für Betriebssysteme und Rechnerverbund

Smartcards / Signaturkarten

- **Geschichte**
  - 1950: Vollplastikkarte DinersClub; 1968: J. Dethloff und H. Grötrupp melden Plastikkarte mit integriertem Schaltkreis als Patent an; 1984 wurde mit der Telefonkarte der französischen PTT 2 der Durchbruch erzielt
- **Typen von Smartcards:**
  - Speicherchipkarten, Erweiterte Speicherchipkarten, Prozessorchipkarten
- **Heutige Einsatzgebiete:**
  - Telefonkarten, Krankenversichertenkarte, Geldkarte, Sim-Karten in Handys und Signaturkarten

Institut für Betriebssysteme und Rechnerverbund

Schemadarstellung einer Prozessorchipkarte



Institut für Betriebssysteme und Rechnerverbund

TCOS 2.0 Betriebssystem

➔**Erstes nach deutschem Signaturgesetz zugelassenes Betriebssystem für die digitale Signatur**

- **Smart Card Ics**
  - SLE66CX320P,E4 hoch evaluiert,Hersteller:Infineon AG
- **Asymmetrische kryptographische Verfahren**
  - RSA mit 512 Bit –1024 Bit
- **Symmetrische kryptographische Verfahren**
  - DES, DES 3, IDEA

Institut für Betriebssysteme und Rechnerverbund

Vorteile von Smartcards

- **Chip mechanisch belastbar in Plastikkarte integriert**
- **Chipfunktionen durch Pin oder Biometrische Authentifizierung geschützt**
- **Geheime Daten (privaten Schlüssel) verlassen niemals den Chip**
- **Integrierte Funktionen**
  - Hashfunktion, Signieren von Daten, Überprüfung von Signaturen, Verschlüsseln von Daten; Schlüsselerzeugung
- **Gleichstellung mit handschriftlicher Unterschrift**

➔ Bietet homogene Infrastruktur für Vielzahl von Sicherheitsaspekten

Institut für Betriebssysteme und Rechnerverbund

Nachteile von Smartcards

- **Chipkartenleser und Middleware-Installation notwendig**
- **Kosten für eigene Kartengenerierung und Schlüsselverwaltung oder Trustcenter (45 €)**
- **Unterstützung unterschiedlicher Zielbetriebssysteme und Kartenleser**
- **Unterschiedliche Karten-Betriebssysteme mit unterschiedlichem Funktionsumfang**
- **Erhöhte Kosten für Softwareentwicklung und Zertifizierungsverfahren**

➔ Erschwerte Marktdurchdringung (vgl. Geldkarte)

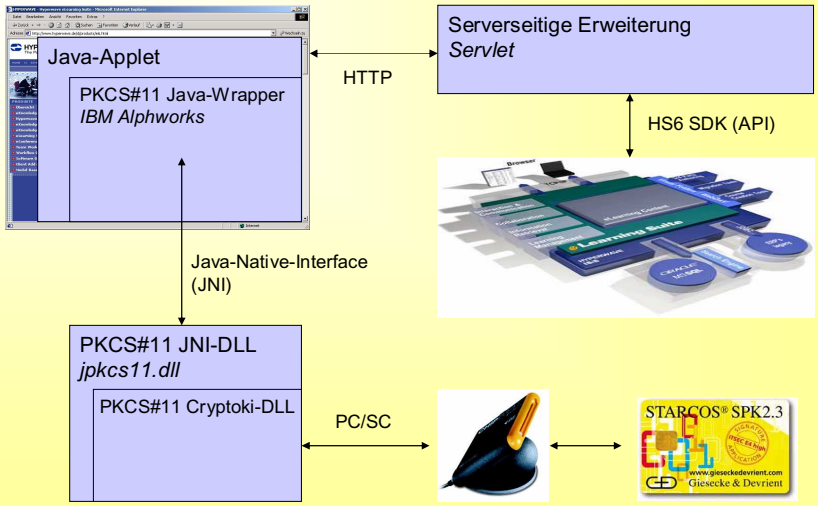
Institut für Betriebssysteme und Rechnerverbund

Programmierung von Smartcards

- **Standard-Schnittstellen für Chipkarten-Terminals**
  - CT-API (Telekom und TÜV)
  - PC/SC (Microsoft, Bull, HP, IBM, Schlumberger, Siemens, Gemplus, Toshiba – Standard auf Windows-Plattformen)
- **Middleware für Funktionszugriff**
  - OCF
    - Framework in Java
    - Unterstützung diverser Standards z.B. PC/SC
    - Treiber Klassen für spezifische Kartenfunktionalitäten)
  - PKCS#11 (Cryptographic Token Interface "Cryptoki")
    - PKCS ist eine Gruppe von Industrie Standards, die von den RSA Laboratories in Zusammenarbeit mit Industrie, Forschung und Behörden herausgegeben werden.
    - Definiert eine Programmierschnittstelle für beliebige kryptographische Token

Institut für Betriebssysteme und Rechnerverbund

Beispielimplementierung PKCS#11



Institut für Betriebssysteme und Rechnerverbund

Mögliche Problemstellungen

- **Ungenügende Unterstützung der Smardcards für entsprechende kryptografische Aufgaben**
- **Entscheidung Middleware (OCF, PKCS#11)**
- **Entscheidung Java-VM (Sun-Plugin, Microsoft VM, ...)**
- **JAVA-Sicherheitsmechanismus (VM)**
  - JNI Zugriff
  - Zertifizierung der Applet-Klassen
- **Hyperwave Integration**
  - Simulation einer Anmeldung mit Benutzername und Passwd
  - Eingeschränkten Zugriff auf Plattform-Funktionalität

Institut für Betriebssysteme und Rechnerverbund

Vielen Dank für Ihre Aufmerksamkeit

TECHNISCHE UNIVERSITÄT CAROLO-WILHELMINA ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund