Institut für Betriebssysteme und Rechnerverbund

Sicherheitsaspekte in e-Learning-Umgebungen unter Berücksichtigung digitaler Signaturkarten

Rainer David

Betreuer: Stefan Schmidt, Astrid Weilert

IBR

TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG
Institut für Betriebssysteme und Rechnerverbund
http://www.fu-bs.de http://www.ibr.cs.tu-bs.de

Agenda

- **Grundlagen**
  - Einführung, Anknüpfung an das erste Seminar
  - Entscheidung für eine Middleware
- **Entwicklungsschwerpunkte**
  - Ausführung des Applets ohne vorrangehender Installation
  - Entwicklung eines Dienstes zur Benutzer und Zertifikatsverwaltung
  - Verwaltung der Kartensession
- **Livepräsentation mit Vergleich zu konventionellem System**
  - Login
  - Nachrichtensystem

Einführung

- Sicherheitsaspekte spielen bislang in E-Learning Plattformen nur eine untergeordnete Rolle
- Die Natur dieser Plattformen entwickelt sich zunehmend zu umfassende Portallösungen mit erweiterten Möglichkeiten des Missbrauchs

- Smartcard stellen Möglichkeiten zur Verfügung um diesen neuen Sicherheitsaspekten gerecht zu werden
- Die Integration soll in die webbasierte Hyperwave eLearning-Suite erfolgen => Java => Applet
- Zugriff auf die Smartcard muss aus Java erfolgen => Wahl einer geeigneten Middleware zur Verwendung der kryptografischen Operationen

➔ **Die entstandene Lösung wurde SecureEls genannt**

Wahl der Middleware

Middleware in der Entscheidung:

- **OCF:** Javabasiertes Framework; Kartenspezifische Treiber durch Java-Klassen und Implementation standardisierter Interfaces
- **PKCS#11:** Definition der Struktur einer Systembibliothek für den Kartenzugriff

Entscheidungskriterien:

- Marktdurchdringung, Zukunftssicherheit, praktische Anwendung
- Zugriff auf Kryptofunktionen und Kartenzertifikate
- Beispielapplikation

Ergebnis der Auswahl:

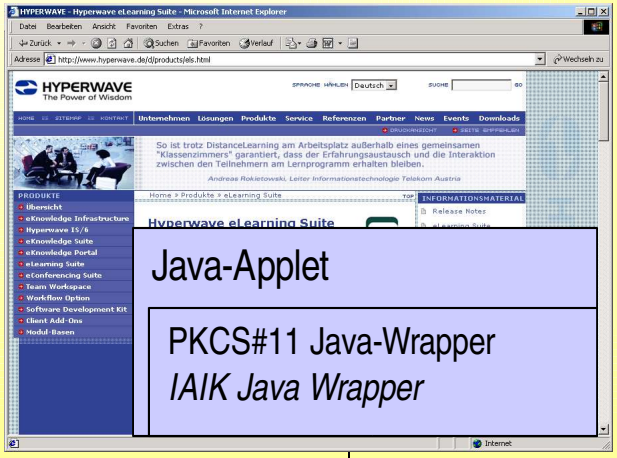
- **OCF:** Java-Architektur => homogenes System unter; spezifizierte Paramter
- **PKCS#11:** aufwendiger Javazugriff; gute Marktdurchdringung; einfacher, abstrakter Zugriff auf Kartenfunktionen

=> Serverumfeld

=> Client

➔ **Entscheidung zugunsten PKCS#11 => IAIK PKCS11 Java Wrapper**

Appletzugriff auf PKCS#11



JNI-Zugriff nur aus signierten Applets möglich

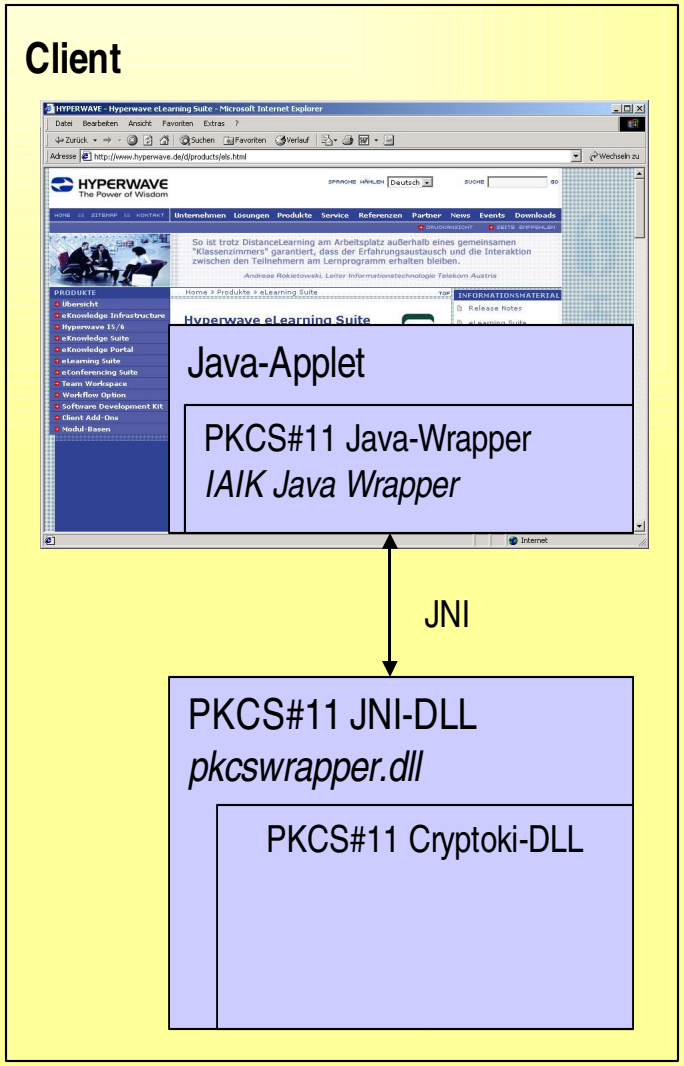
Java-Native-Interface (JNI)

PKCS#11 JNI-DLL
pkcswrapper.dll

PKCS#11 Cryptoki-DLL

PC/SC

Wrapperinstallation



Standard IAIK-Bibliothek

- Manuelle Installation der PKCS#11 JNI-DLL
- Start des Applets
- Verwendung der Smartcard

➔ **Wiederspricht dem Appletcharakter**

Erweiterte IAIK-Bibliothek

- Start des Applets
- Automatische Detektion der PKCS#11 JNI-DLL
- ggf. automatische Installation der PKCS#11 JNI-DLL
- Verwendung der Smartcard

➔ **IAIK zur Integration übermittelt**

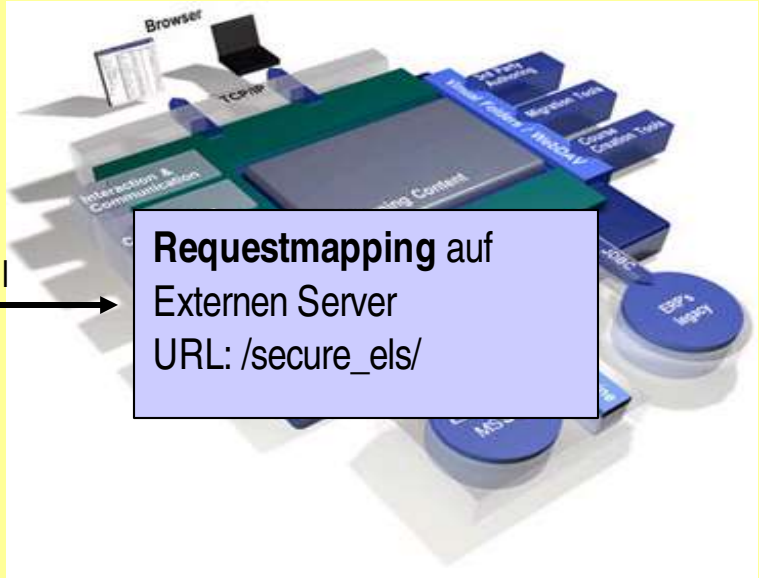
SecureEls Serverdienst

Grundfunktionalitäten

- Verwaltung von Nutzerdaten
- Zertifikatsverwaltung
- Steuerung des Nutzerlogins

Nutzerzugriff über Internetbrowser

HTTP-Protokoll



Tomcat-Server

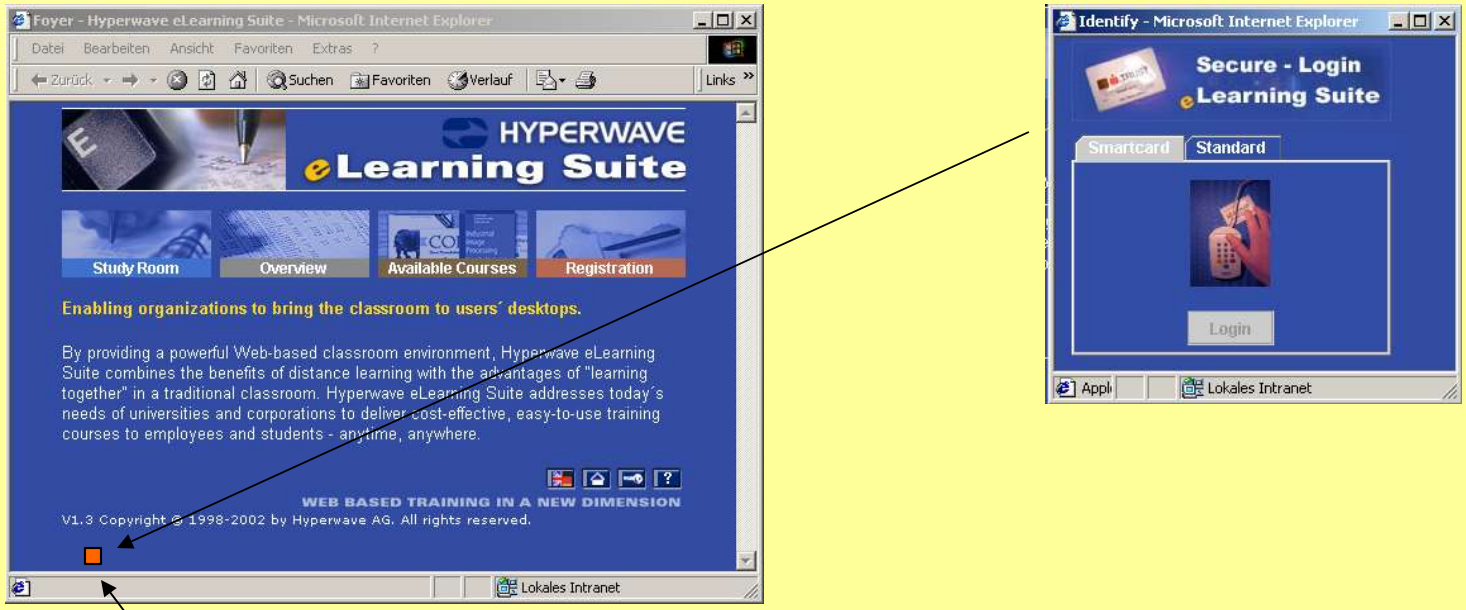
SecureEls-Servlet

AJP12-Protokoll

Verwaltung der Kartensession

- Nur einmalige PIN-Eingabe
- Zentrale Konfigurationsmöglichkeiten

➔ Fensterübergreifende Verwaltung der Kartensession



Kartensession in neuem Fenster

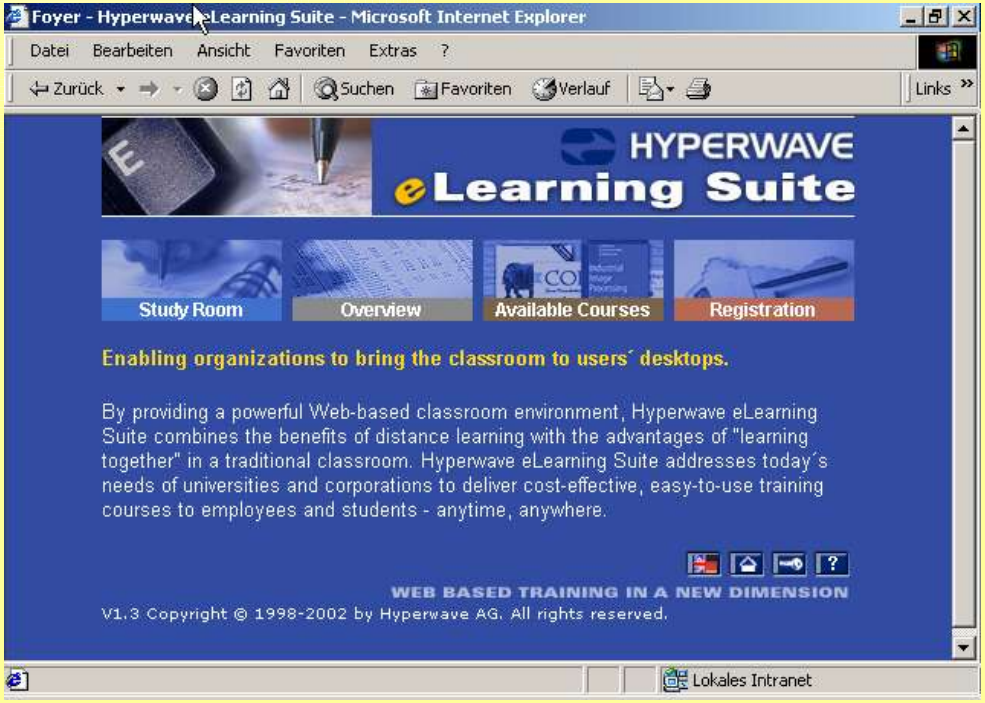
- Automatische Erzeugung der Fensterinstanz
- Statischer Bereich in neuem Fenster
- Erweiterte Konfigurationsmöglichkeiten

Gemeinsamer Classloader
(Statische Instanz ermöglicht
Den fensterübergreifen Zugriff)

ProviderApplet

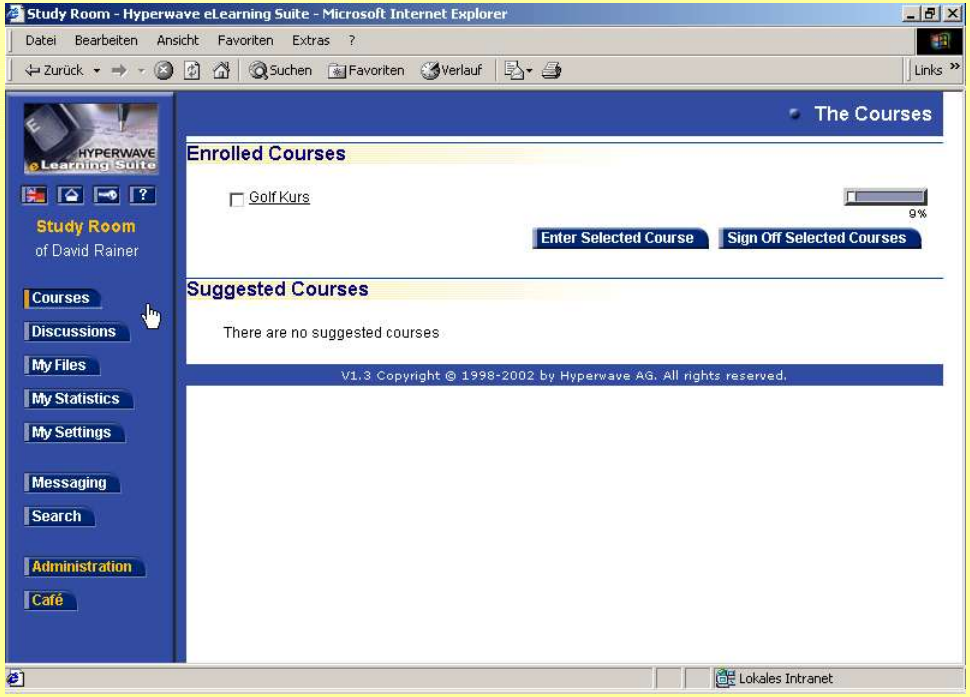
Hyperwave Login

- Login durch Benutzername und Passwort
- Überprüfung der Logindaten
- Anmeldung am System



Hyperwave Nachrichtensystem

- Nachrichteneingabe in HTML-Formular
- Layerverwendung um Updatebereiche zu definieren
- Überprüfung der Vollständigkeit der Eingaben



Vielen Dank für Ihre Aufmerksamkeit