

UniCard 2.0 / CAPRI

Open Source Software-Lösung für die Kartenproduktion
Christof Pohl, IT & Medien Centrum, TU Dortmund

Warum UniCard 2.0?

- Nicht realisierte Funktionen
 - Bezahlungsfunktion
 - Kopierfunktion
 - E-Ticket

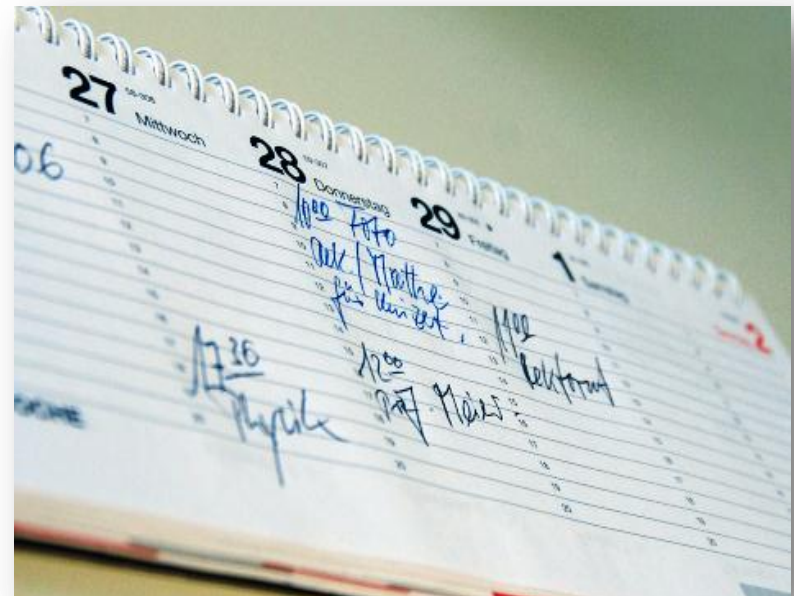


Projektvorbereitung und Entscheidungen

- Beteiligung wichtiger Partner an der Hochschule
 - Rechenzentrum, Verwaltung, Bibliothek, Studentenwerk, ...
- Entscheidung über Funktionen
 - Bezahlungsfunktion, Crypto-Funktion, kontaktlose Funktionen, ...
- Karten-Hardware & Design
 - Ziel: Beschaffung von „Rohlingen“

Projektvorbereitung und Entscheidungen (cont.)

- Abstimmung mit PKI
 - CPS, Zertifikatsprofile, Schnittstellen, ...
- Produktions-/Personalisierungssoftware
 - Bedruckung, Zertifikate, ...
- Endnutzer-Software
 - SmartCard-Middleware (Crypto-Funktionen), Terminals, ...
- ...



Aspekte der NRW-Empfehlung

- GeldKarte (Emittent: Sparkasse Dortmund)
 - Dual-Interface-Chip mit SECCOS 6 Betriebssystem
- SECCOS „Marktplatz“ & MIFARE Classic
- SECCOS Signaturanwendung
 - Schlüssel- und Zertifikatshoheit bei Hochschul-CA/DFN-PKI
- E-Ticket innerhalb der Projektlaufzeit nicht realisierbar



Projekt UniCard 2.0

- Herausforderungen
 - Hardware-Neuentwicklung SECCOS-Signaturanwendung
 - Software für Kartenpersonalisierung und –nutzung
 - Projektinitialisierung: 8/2010 bis 12/2010
 - Projektlaufzeit: von 12/2010 bis 10/2011
- Beteiligte
 - TU und FH Dortmund
 - Sparkasse Dortmund, DSV, S-Card, ...
 - EURO Kartensysteme GmbH, SRC GmbH
 - cv cryptovision GmbH

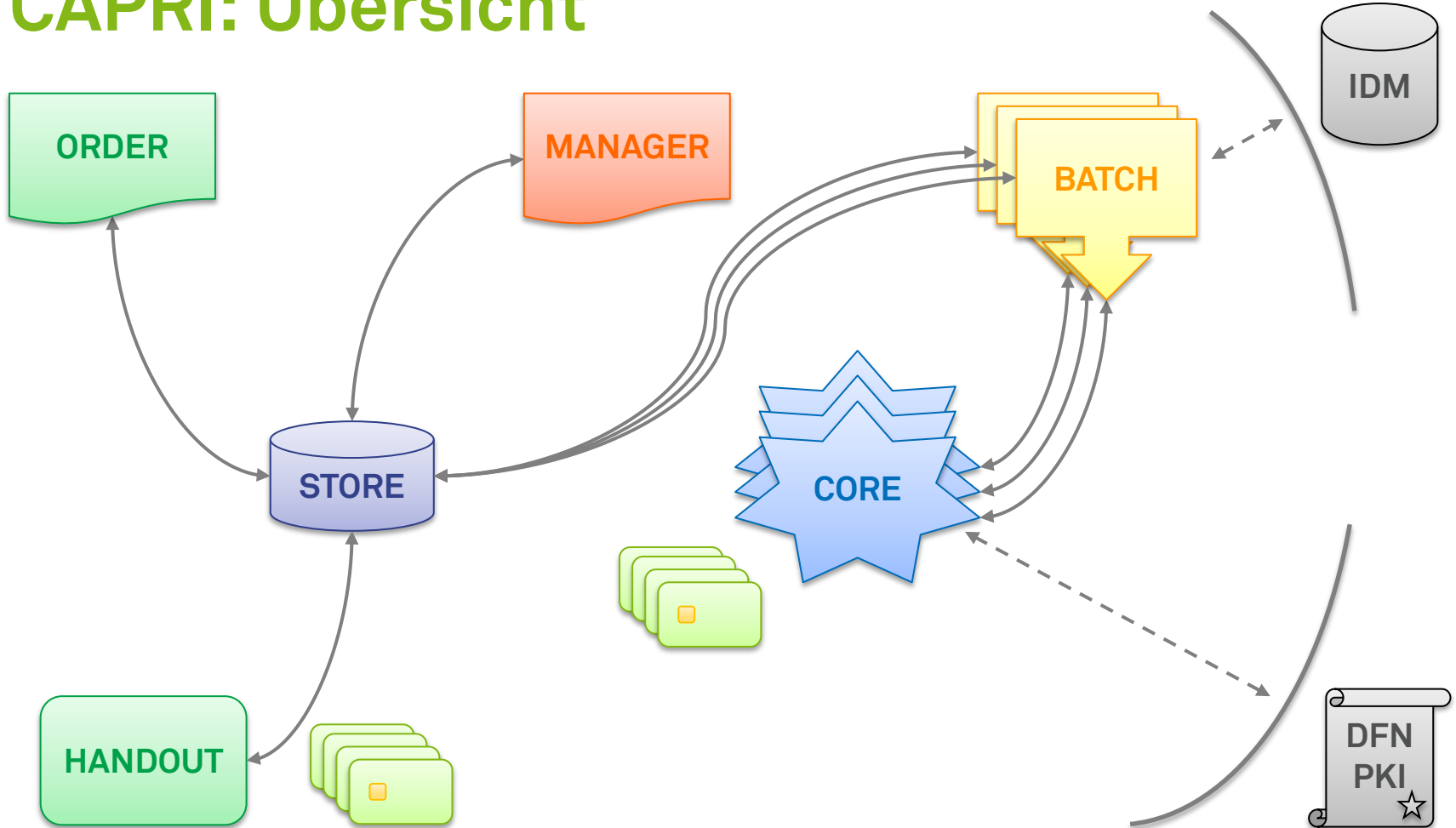
CAPRI: Card Production Infrastructure

- CAPRI Order: Kartenbestellung
- CAPRI Data Store: Datenhaltung
- CAPRI Manager: RA-Verwaltungstool
- CAPRI Batch: Steuerung des Personalisierungsprozesses
- CAPRI Production Core: Personalisierung einzelner Karten
- CAPRI Handout: Erstellung der Begleitdokumente, Abschluss der Bestellung

Warum CAPRI?

- Keine umfassende, flexible Personalisierungssoftware verfügbar
- Integration kommerzieller Lösungen in Hochschul-IT schwierig
- Existierende Lösungen an Hochschulen ...
 - ... sind zumeist stark individualisiert,
 - ... decken nur Teile des Gesamtprozesses ab,
 - ... sind (meistens) nicht frei verfügbar.

CAPRI: Übersicht



CAPRI Order

- Web-basiertes Karten-Bestellformular
- Portlet/JSR 268 (Liferay)
- Authentifizierung/Autorisierung des Antragstellers
- Basisdaten für Bestellung
 - Name, Vorname
 - Zentraler Uni-Account/IDM-ID
 - E-Mail-Adresse
 - Hochladen eines Fotos
- „Live“-Anzeige des Produktionsstatus



CAPRI Data Store

- Zentrale Datenhaltung für CAPRI
- Webservice-Schnittstelle für Bestellungen
- Alternative Bestell-Frontends möglich
 - Einfache Integration in übergeordnete Prozesse möglich (Immatrikulation, Einstellung, ...)
- Wird von allen CAPRI-Komponenten genutzt



CAPRI Manager

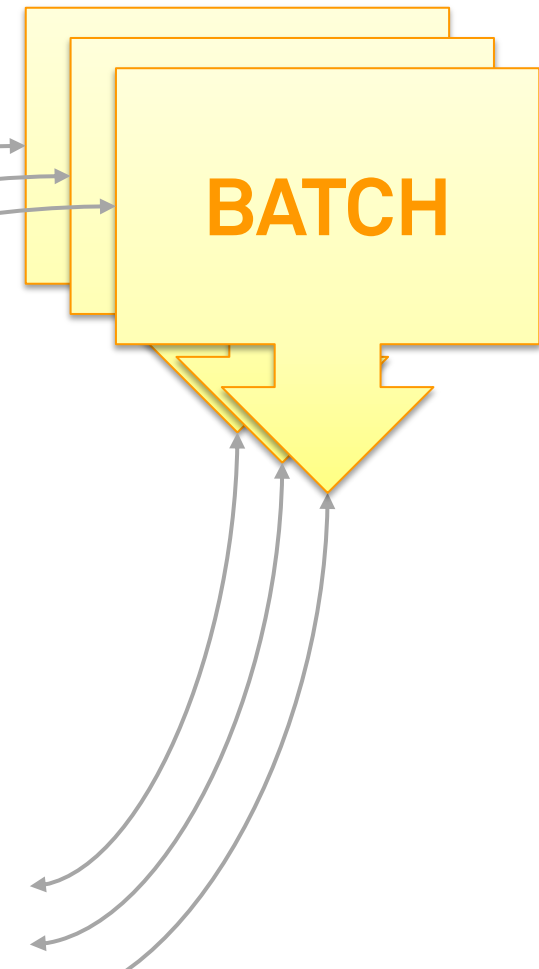
- Web-basiertes Verwaltungstool für RA-Admins
- Portlet/JSR 268 (Liferay)
- Liste aller eingegangenen Bestellungen
- Zahlreiche Filtermöglichkeiten/Suchfunktionen
 - Studierenden-/Mitarbeiterkarten, Name, Antragsdatum, ...
- Sichtung und Freigabe der Anträge
- Überblick über Bestellvorgänge
- Verteilung auf mehrere Produktionsstraßen
- Statusinfos zur Produktion



MANAGER

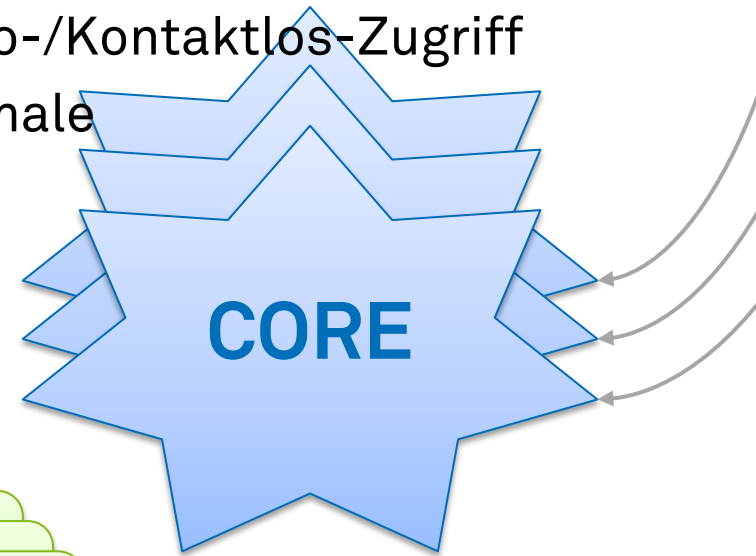
CAPRI Batch: Preproduction

- „Technische“ Steuerung der Produktion
- Datenabgleich mit IDM/Hintergrundsystemen
- Gesichtserkennung/automatisierte Foto-Bearbeitung
- Speicherung von Fotos für Folgekarten möglich
- Ggf. Sperrung „alter“ Zertifikate (z.B. bei Verlust oder Umtausch)
- Priorisierung einzelner Aufträge



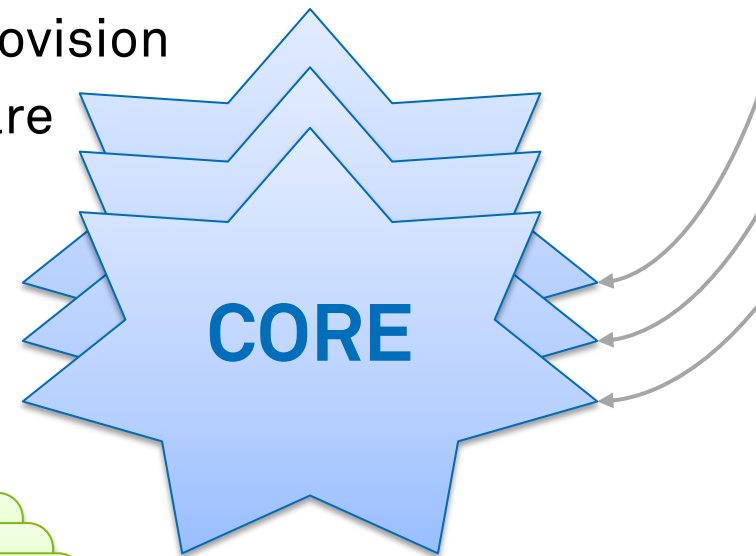
CAPRI Production Core

- Personalisierung der Karte
- Ansteuerung des Kartendruckers
 - Hardware-Handling (Drucker/Rohling) auf Treiber-Ebene
 - Positionierung des Rohlings für Crypto-/Kontaktlos-Zugriff
 - Aufdruck der Personalisierungsmerkmale
- Schlüssel-Generierung
 - Auf der Karte oder extern
- Zertifikatserstellung
 - Webservice-Schnittstelle des DFN
- Speichern der Zertifikate auf der Karte



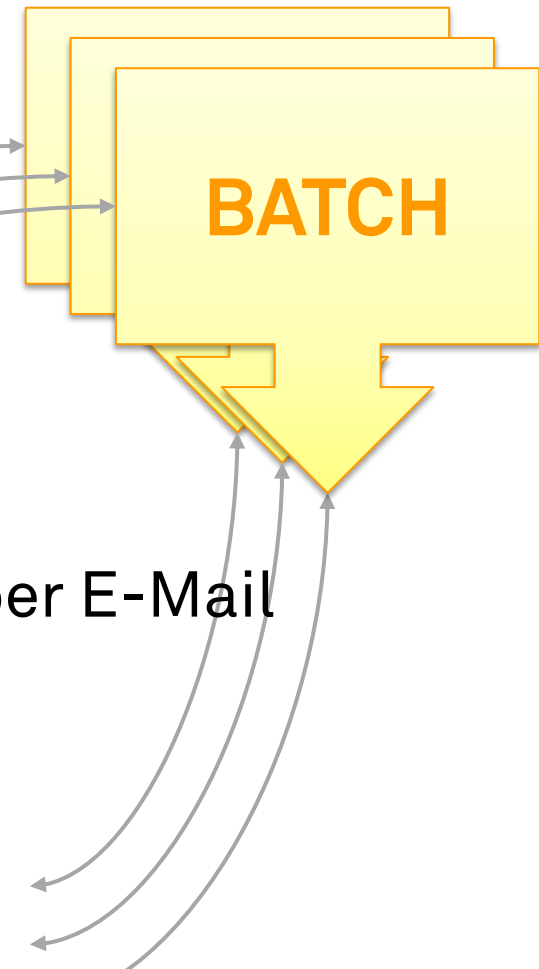
CAPRI Production Core (cont.)

- Benötigt: PKCS#11 für Zugriff auf die Karte
 - Standardisiertes Interface
- Realisierung: SmartCard-Middleware
 - UniCard 2.0: sc/interface von cv cryptovision
 - Low-Level-Zugriff auf Karten-Hardware
 - In Planung: Campus-Lizenz - transparente Crypto-Use-Cases
- TODO: Schreiben von MIFARE/Marktplatz-Attributen



CAPRI Batch: Postproduction

- Erstellung von Begleitdokumenten
 - Anschreiben
 - PIN/PUK-Brief
 - Infoblatt
 - Empfangsbestätigung
- Ablage der Dokumente im CAPRI Store (verschlüsselt)
- Nach Fertigstellung: Benachrichtigung per E-Mail
- Zusätzlich: Status in Studierenden/Personalverwaltung



CAPRI Handout

- Manuell: Produzierte Karten in Kartei nach Matrikel-/Personalnummer sortieren
- Bei Abholung: Sichtkontrolle Karte, amtlicher Lichtbildausweis, ggf. Studienbescheinigung
- Danach: CAPRI Handout
 - Entschlüsselung und Ausdruck der Begleitdokumente
 - Bestellabschluss im Store/weiteren Hintergrundsystemen



CAPRI - Softwarearchitektur

- Java Enterprise Anwendung
- Orientierung am SOA-Paradigma
 - „Lose Kopplung“ verschiedener CAPRI-Dienste
 - Abstraktion der CAPRI-Dienste durch WebServices
 - Gekapselter Zugriff auf Hintergrundsysteme (IDM, HIS-SVA, HIS-SOS, ...)
- Portlets/JSR 268 (JSF) für CAPRI Order & Manager
- Swing für CAPRI Production Core & Handout

CAPRI – Open Source bei CampusSource

- Geplant: Veröffentlichung von CAPRI unter der GPL
 - SmartCard-Middleware (PKCS#11 Interface) wird benötigt
 - Direkt unterstützt: cryptovision sc/interface
- Einstellung in die CampusSource Softwarebörse
- Verfügbarkeit: 24.12.2011 ;-)
- Mitarbeit weiterer Entwickler möglich und erwünscht!



Fazit UniCard 2.0/CAPRI

- Bezahlungsfunktion
- Kontaktlose Funktionalitäten
- Crypto-Funktionen
- **E-Ticket für ÖPNV**
- CAPRI verfügbar unter GPL
- Austausch aller Karten
in Dortmund (ca. 30.000)
zum WiSe 2011/12