

JUSTUS-LIEBIG-



UNIVERSITÄT
GIESSEN

Einsatz neuer PKI-basierter Chipkarten

an der JLU Gießen

Falko Fock

Hochschulrechenzentrum

11. DFN-Workshop “Sicherheit in vernetzten Systemen”

Hamburg, 3./4. Februar 2004

Übersicht

- Die junge Geschichte der digitalen Signatur
- Das rechtliche Umfeld
- Sicherheit bei der elektronischen Signatur
- Mehr als nur eine Signatur
- Server-Authentisierung
- JLU-Ausgangspunkt
- Bild der JLU-Chipkarte
- Kosten bei der JLU
- Chipkarten-Ausgabe und -Aktualisierung
- Chipkarten-Herstellung (Personalisierung), PIN-Brief
- Chipkarten-Einsatz
- Argumente für PKI-basierte Chipkarten
- Zeitlicher Projektverlauf
- Besonderheiten an der Universität Gießen
- Karten-Erstausrüstung an der JLU
- Rezertifizierung und Rückmeldung
- Weitere Informationen, Links



JLU-Chipkarte, Vorderseite



JLU-Chipkarte, Rückseite

Die junge Geschichte der digitalen Signatur

- 1978: asymmetrisches Kryptographie-Verfahren RSA
RSA = Rivest – Shamir – Adleman
Bringt die moderne Kryptographie für einen breiten Einsatz
- 1997: In Deutschland tritt weltweit das erste Gesetz zur Digitalen Signatur in Kraft (Signaturgesetz – SigG)
- 2000: Die EU führt eine vergleichbare Richtlinie ein
- 2001: Die BRD passt das Signatur-Gesetz den EU-Richtlinien an

- Heute werden die Signaturen im SigG unterschieden nach
 - Signatur eines akkreditierten ZDA (z.Zt. ca. 30)
 - Signatur eines angezeigten ZDA (z.Zt. 1)
 - fortschrittliche Signaturen nach X.509V3
 - sonstige Signaturen(ZDA = Zertifizierungsdiensteanbieter)

Das rechtliche Umfeld

- **In der ZPO** gilt seit langer Zeit die (handschriftlich unterzeichnete) **Urkunde als stärkstes Beweismittel.**
- Viele **Formvorschriften** werden dahingehend erweitert, dass auch elektronische Unterschriften (digitale Signaturen) zugelassen werden.
- Wegen der technischen Problematik der digitalen Signaturen, werden nur solche der handschriftlichen Unterschrift gleichgestellt, die von **akkreditierten ZDAs** ausgegeben werden.
- **Bei den meisten Rechtsgeschäften ist jedoch keine bestimmte Form vorgeschrieben**, die Partner können sich frei vereinbaren (Handschlag, Fax, E-Mail usw.)
- Wer bei einer gerichtlichen Auseinandersetzung ggf. eine Beweisführung erbringen muss, verwendet die Schriftform – oder zukünftig – die digitale Signatur.

Sicherheit bei der elektronischen Signatur

- Digitale Urkunden sind um ein Vielfaches sicherer als Urkunden in Papierform.
- Digital signierte Urkunden haben eine sehr hohe Fälschungssicherheit. Jede Manipulation der Daten führt zu einem Fehler.
- Mit der digitalen Signatur kann zuverlässig festgestellt werden, dass
 - das Dokument von einer bestimmten Person signiert wurde (Urheberschaft, Non-Repudiation)
 - nach dem Signieren keine Änderungen vorgenommen wurden (Integrität).
- **Vorteile von digitalen Signaturen:**
 - sicher
 - die Dokumente sind elektronisch bearbeitbar
- **Nachteile der digitalen Signaturen:**
 - aufwendige Herstellung, PKI
 - oft Zusatzgeräte für den Einsatz nötig (Chipkarten-Lesegeräte)
- **Technische Realisierung** einer sicheren "Signaturerstellungseinheit"
 - Einbringen eines Mikroprozessor-Chips in eine "Chipkarte" (Smartcard)
 - Vereinbarung einer PIN (Personal Identifikation Number)
(Zweikomponenten-Sicherheit: Besitz und Wissen)

Mehr als nur eine Signatur

- Beim SigG wird nur die digitale Signatur im eigentlichen Sinne betrachtet
(Signieren von Dokumenten)
- Es gibt wesentlich **mehr praktische Anwendungen**, bei denen die Signatur **zur Authentisierung** als zum Verschlüsseln/Signieren benutzt wird:
 - Anmeldung bei einem Server
 - Abruf von privaten Daten aus einer Datenbank
- Wer digitale Signaturen einsetzt, zum Beispiel zum Verschlüsseln, muss sich über viele Konsequenzen Gedanken machen und Lösungen bereitstellen (Schlüssel verloren, Mitarbeiter im Krankenhaus usw.)
- Bei umfassendem Einsatz “elektronischer Signaturen” sind i. allg. 3 Schlüssel bzw. Signaturen erforderlich (Authentisierung, Signatur, Verschlüsselung) mit 2-3 PINs.
- Bisher wurden in Deutschland nur ca. 25.000 Chipkarten von den akkreditierten ZDAs ausgegeben, fortgeschrittene Signaturen werden jedoch schon zu vielen hunderttausend und mehr eingesetzt.

Server-Authentisierung

- Benutzer verwendet PC mit angeschlossenem Chipkarten-Leser
- Benutzer ruft Serverdienst auf
- Server besorgt sich das Benutzer-Zertifikat (von der Chipkarte oder einem Verzeichnisdienst)
- Server generiert eine Challenge (Zufallsdaten werden mit dem Zertifikat verschlüsselt)
- Server sendet die Challenge zum PC und fordert die Entschlüsselung an
- Hat der Benutzer mit der richtigen PIN den Leser freigeschaltet und passt das Zertifikat zum geheimen Schlüssel des Benutzers, kann der PC die richtig entschlüsselten Daten zurücksenden
- Der Benutzer hat sich authentisiert, wenn der Server die korrekten Daten zurückerhält (Challenge-Response-Verfahren).
- **Server-Konfiguration zur Authentisierung (Apache .htaccess-Inhalt):**

SSLRequireSSL

SSLVerifyClient require %{SSL_CLIENT_VERIFY} eq "SUCCESS"

Ausgangspunkte (1)

- Signaturgesetz (elektronische Signaturen gesetzlich anerkannt)
- **sichere Authentisierung im Internet** mittels X.509-Zertifikaten
- PGP-Einsatzproblem im kommerz. und administrativen Umfeld
- **Keine Alternativen zur aufwendigen PKI**
- **Chipkarte als optischer Ausweis** (mit ÖPNV-Semesterticket), Bibliotheksausweis (Barcode), mit kontaktlosem Einsatz als elektronische Geldbörse für inner-universitäre Kleinbeträge und beim Gebäudezugang, PKI für Authentisierung und Sicherheit im Internet
- Vereinbarung einer hessenweiten einheitlichen Ausweisnummer für Studierende, Hochschulmitarbeiter und andere Personengruppen

Ausgangspunkte (2)

- **Verfügbarkeit von Programmen** für das PKI-Umfeld (Outlook, Netscape, Mozilla, Apache-Webserver, IIS, Acrobat)
- **Problem**, eine bezahlbare Lösung zu finden
 - eigener CA-Betrieb reduziert CA-Kosten
 - Kosten i. allg. an Zertifikatsanzahl gekoppelt (25-100 €/Jahr)
- **Problem** mit der Sichtanzeige von Semesterticket (ja/nein) und Gültigkeitsdauer (so genannte TRW-Folie, nur bei Hochschulen erforderlich)
- Minimierung der Akzeptanzprobleme =
eine multifunktionale Chipkarte
- **Lösung:**
 - Eine Chipkarte mit kontaktbehafteten Kryptochip (32 KB) und kontaktlosem Mifare-Chip (1K, 16 Sektoren)
 - Einfache Anwendung = vorerst nur ein Schlüsselpaar
 - TRW-Folie muss eingesetzt werden (bei der JLU 15 mm breit)

Kosten bei der JLU

- **Hard- und Software** 180.000 €
 - Aus HBFEG- und Landesmitteln finanziert
 - ohne Kosten für die Chipkarten und den Mifare-Einsatz bei Kassenterminals, Gebäude-Zugangseinrichtungen u. dgl. m.
- **Chipkarten** 300.000 € (15 €/Stück, 20.000 Studierende, Erstausst.)
 - Studierender leistet Pfand (15 €)
 - daher Hochschul-Chipkartenkosten < 75.000 € pro Jahr
- **Personal**, eine Projektstelle für 1 Jahr (durch die Universität bereitgestellt)

Im Projekt sind 600 Chipkartenleser für öffentliche PCs und 6 "Druckstationen" enthalten, jedoch keine der universellen SB-Stationen wie bei früheren Chipkarten-Projekten.

Chipkarten-Ausgabe und -Aktualisierung

Studierende

- erhalten bei der Immatrikulation einen vorläufigen Papierausweis
- können ihre Chipkarte 4-10 Tage später abholen (persönlich), Abholbereitschaft wird im Web angezeigt
- **aktualisieren ihre Chipkarte halbjährlich** im Rahmen der Rückmeldung in zwei Schritten (ggf. zeitlich unabhängig):
 - (a) den **Kryptochip** mit einem Chipkartenleser-PC (an öffentlichen PCs der Hochschule oder **über das Internet**, mit PIN-Eingabe)
= Zertifikatswechsel und Rückmeldung
 - (b) den **Mifare-Chip** und die optische Angaben an einer Druckstation **auf dem Campus** (bei diesem Vorgang erfolgt auch der Bescheinigungsdruck)

Chipkarten-Herstellung

(Personalisierung)

- Die Chipkarte enthält nur die Person identifizierende Daten, das sind **Name und Matrikel-/Personalnummer, sowie das Gültigkeitsende**. Die genannte Personennummer steht nur im "lokalen" Mifare-Chip.
- Beim **1. Kartendurchlauf** werden die Studierendendaten auf den Kartenrohling gebracht und der Zertifikatsantrag erzeugt. (2 min)
- Der **2. Durchlauf** (am nächsten Tag) schreibt das Zertifikat in den Kryptochip und druckt den "PIN-Brief". (1 min)
- **PIN-Brief** ist ein DIN-A4-Blatt mit
 - Chipkarten- und Chipkarten-Infoblatt-Empfangsbestätigung
 - Start-PIN (Personal Identification Number)
 - PUK (Personal Unblock Key)
 - Sperrcode
- PIN, PUK, Sperrcode und Chipkarte werden in einem verschlossenen Briefumschlag zur Abholung bereitgehalten (Zeitbedarf 1 min).



Eltron-Drucker zur Kartenpersonalisierung

27x53x26 cm (HxBxT)

Zertifikatsinhalt

Parameter	Inhalte
Version	X.509v3
Seriennummer	Eindeutige laufende Nummer der CCA
Algorithmusidentifikation	SHA1 with RSA
Ausstellende Stelle	C=DE, O=Universitaet Giessen, OU= Hochschul- rechenzentrum, CN= UNIGI-CCA
Gültigkeitsdauer	Start- und Ablaufdatum, innerhalb derer das Zertifikat gültig ist (1 Semester + 1 Monat)
Teilnehmer	C=DE, O=Universitaet Giessen, OU=CIDs, OU=n, CN=cryptoProcessorSN- personal name
Public-Key des Benutzers	Public-Key-Informationen des Teilnehmers
Signatur der ausstellenden Stelle	Signatur der UNIGI-CCA
Erweiterungen	<ul style="list-style-type: none"> •subject alternative name (= E-Mail-Adresse) •key usage •cert type •CRL distribution points certificate policies

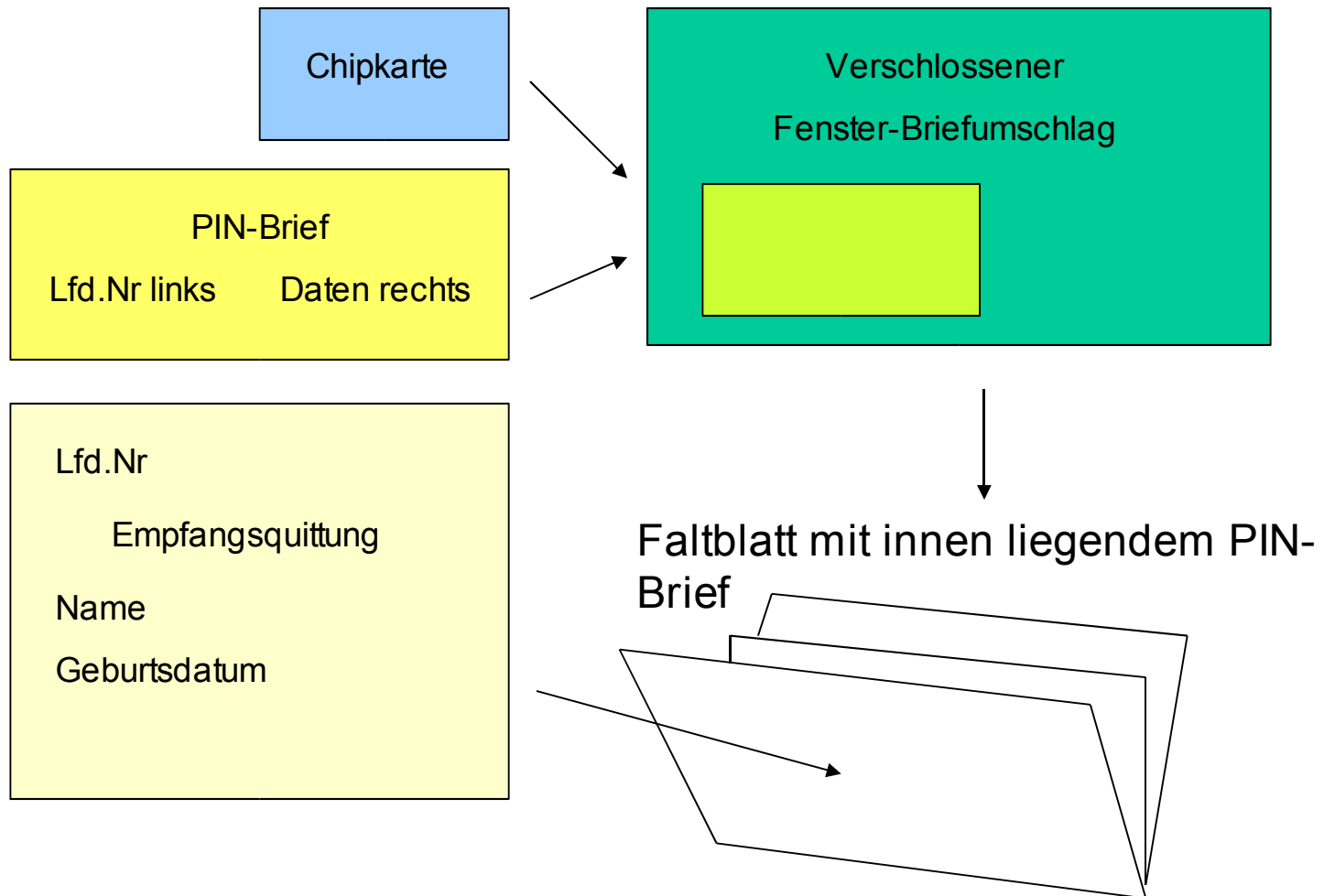
PIN-Brief

Gedruckt als ein DIN-A4-Blatt; wird geteilt in

- *2/3 = Karten-Empfangsbestätigung*
- mit Angabe der ausstellenden Behörde und der Ausweisnummer
- *1/3 = PIN-Brief = Hinweis und PIN-Daten*
- PIN-Brief enthält:
 - 6-stellige Start-PIN (10 Versuche, dann blockiert)
 - 8-stellige PUK (personal unblock key)
 - 12-stelligen Sperrcode
 - Ausgabedatum (zur Unterscheidung zweier PIN-Briefe)

PIN-Brief-Ausgabe

sicher – praktisch - preiswert



Chipkarten-Einsatz

(1) Kryptochip

- **Authentisierung im Internet**

- für die Mailweiterleitung einer fiktiven Hochschul-Mailbox an reale, externe Benutzer-Mailbox
- beim Zugang zum Hochschul-Intranet (z.B. über VPN-Server)
- bei der verbindlichen Anmeldung zu jeder Art von Diensten
 - z.B. beim Zugang zum Hochschul-Prüfungsorganisationssystem
 - z.B. beim Zugang zu RZ- oder Fachbereichsserver

Alle Zugänge sind mit der selben Chipkarte und PIN gesichert, defacto nur ein Passwort (PIN). Mit der Chipkarte sind die alten Passwort-Probleme behoben: gebraucht wird

Besitz (1 Karte) und Wissen (1 PIN).

- **Versenden verbindlicher, elektronisch signierter, ggf. auch verschlüsselter E-Mail oder PDF-Dokumente**
- **Dateisicherung durch Verschlüsselung mit der Karte**
- **Einsparen von (Fahr- und Warte-)Zeit und Geld durch Zugang vom heimischen PC zu allen Hochschuldiensten**



Kobil-Chipkartenleser

KAAN Standard Plus

HBCI-Klasse 2

Chipkarten-Einsatz

(2) Mifare-Chip und optische Angaben

- Studenausweis mit Lichtbild
- Bibliotheksausweis (Barcode)
- Maschinenlesbarer Ausweis in Klausuren (Barcode)
- ÖPNV-Fahrkarte (Semesterticket)
- Bargeldloses Bezahlen im Studentenwerk und Hochschulbereich (Kleinbeträge)
- Kontaktloser, elektronischer Schlüssel für Raum- und Gebäudezugang
- Gleitzeitkarte für Mitarbeiter

Chipkarten-Einsatz

(3) Sperrmöglichkeiten

- Durch Studierende und (HRZ- bzw. Studentensekretariats-)Mitarbeiter **über Webseite** (Sperrcode und Angaben für Rückfrage erforderlich)
- Sonst Fax, Postbrief oder persönlich
- Sperre kann **temporär** (max. 14 Tage, noch keine neue Karte) **oder dauerhaft** erfolgen (mit kostenpflichtiger neuer Karte, 45 €)
- **Weitergabe** der Einzel-Sperr-Info sofort per Mail, Status aller Chipkarten geht zusätzlich über Nacht **an alle interessierten/berechtigten Hochschulinstitutionen**
- **Automatischer Gültigkeitsablauf am Semesterende!**
- **Kein Schlüsselersatz erforderlich, kein Schlüsselrisiko!**

Argumente für PKI-basierte Chipkarten

(1) technische

- **Keine Alternative zur PKI !!**
- **Eine Chipkarte** für alle Anwendungen = **Akzeptanz**
- **“Relativ preiswert”** (15 €/Karte für alle Anwendungen, alternativ 5-10 €/Karte für eine SOS/POS-campus-orientierte Chipkarten-Lösung)
- **Für Studierende und Mitarbeiter** kann die **gleiche Chipkarte**, Software- und Hardware-Ausstattung benutzt werden.
- **Viele IT-Dienste sind auf die PKI/X.509-basierten Zertifikate bereits vorbereitet:** Windows2000, XP, Mailprogramme (Outlook, Netscape, Mozilla), die Mehrzahl der VPN- und Webserver (Apache, IIS), PDF-Datenformat (Acrobat)
- Aus unseren Erfahrungen sind **Chipkartenpfand und Chipkartenleser** für zu Hause **kein Gegenargument** (ggf. Weiterverkauf des Lesers wie mit Fachbüchern, Verwendung für das Homebanking), **sofern Anwendungen angeboten werden.**

Argumente für PKI-basierte Chipkarten

(2) organisatorisch/politische

- Es gibt **ernsthafte PKI-Planungen** öffentlicher Institutionen (z.B. BundOnline2005, Städte, Hochschulen) und Realisationen in Großbetrieben (z.B. BMW mit 45.000 Mitarbeitern, LH mit 60.000, Siemens mit mehr als 100.000) sowie in vielen Mittelbetrieben.
- **Hochschulen sollten** die Studierenden mit dem komplexen Umfeld einer PKI **vertraut machen**.
- Hochschulen erhalten für ihre Netzinfrastruktur und den Serverbetrieb einen **hohen Sicherheitsgewinn**, wenn sie PKI-basierte Chipkarten verwenden.
- Hochschul-Chipkarte und Chipkarten-Einsatz sind für die Mehrzahl der Studierenden **etwas Positives**, auch dann, wenn sie persönlich (noch) keinen technischen Vorteil mit der Chipkarte erhalten oder nutzen.
- Studierende erhalten bei intensiver Kartennutzung einen hohen **Service-Gewinn** (Einsparung von Zeit und Geld, Sicherheitsgewinn).

Anwendungen

(sicher mit 1 Karte + 1 PIN)

- **SOS** – Rückmeldung, Anschriftenänderung, Datenabfrage
- **POS-Zugang**
- **Mailweiterleitung** JLU-Adresse nach extern
- **PC-Pool-Login** (Windows, Linux)
- **VPN-Zugang** (ohne Benutzerkennung)
- **Verbindliche Anmeldungen** / Bestellungen
- **Signierte PDF-Dokumente**
- **Dateiverschlüsselung**

Zeitlicher Projektablauf

- März 2000 1. Treffen FH Gießen-Friedberg und JLU
- Juni 2000 Informationsangebote, Projektgruppe
- Dez 2000 Präsidiumsbeschluss und HBFEG-Antrag
- Sept 2001 HBFEG-Bewilligung, Ausschreibung
- Dez 2001 Auftrag an InterCard
- April 2002 Konzeptanpassung mit Offline-CA
- Juli-Aug 2002 Geräteanlieferung und Tests
- Sept-Dez 2002 Kartenherstellung und –Ausgabe (Erstausstattung)
- Dez 2002 erste PKI-Anwendungen (Mail-Weiterleitung)
- Febr-Juni 2003 elektr. Geldbörse in allen Mensen+Cafeterien
- April 2004 Rückmeldung/Anschriftänderung (HIS-SOS) und Bescheinigungsdruck mit Chipkarte

Planung

- II/2004 VPN-Zugang mit Chipkarte
- I-III/2004 POS (FlexNow), Pool-PC-Zugang mit Karte (MS+Linux)
- Jan 2005? elektronische Wahlen denkbar
- ??? Mitarbeiter-Chipkarte, Gebäude- und Raumzugang, Umbau der Gleitzeiterfassung von Barcode auf Mifare (HRZ-Gebäude I/2004)

Besonderheiten an der Universität Gießen

- Es gibt eine **Hessische Immatrikulationsverordnung** (HImmaVO), Hochschulen können wahlweise Chipkarten als Studiausweise einsetzen, legt u. a. Datenumfang von Papiausweis und Chipkarte fest.
- Eine **Uni-Satzung** zur Chipkarte beschreibt weitere Einzelheiten, beispielsweise Pfandzahlung, Kartenrückgabe, Eigentum und **Verbindlichkeit**.
- Um eine “Chipkarten-Lösung zu halben Kosten” einführen zu können, wurden **keine vollwertigen SB-Stationen** früherer Projekte angeschafft, sondern einfache Validierungs-/Druckstationen zur Mifare- und TRW-Datenaktualisierung sowie Chipkartenleser für alle öffentlichen Pool-PCs.
- Aus gleichem Grund fehlen Geldbörsen-Aufwerter (aufwerten an normalen Kassen zu deren Öffnungszeiten); **Zahlung der Semestergebühren nur mit Banküberweisung** (personalisierter Überweisungsträger wird gedruckt).
- Optionales **Internet-Entgelt** für HRZ-Voll-Account und **Semesterbeitrag** werden mit eigenen Programmen **über Nacht verarbeitet/gutgeschrieben und der Eingang im Web angezeigt**.
- Bei der Einschreibung wird eine **fachspezifische JLU-E-Mail-Adresse** erzeugt, die später mit der Chipkarte freigeschaltet werden kann.
- Die JLU-Chipkarte verwendet **“fortgeschrittene Signaturen”** (im Gegensatz zu qualifizierten), weltweit nutzbar und kompatibel mit fast allen Anwendungen, Signaturen haben aber ausserhalb der Uni keine “Signaturgesetz-Garantie”.

Karten-Erstausgabe an der JLU

- E-Mail und Flugblatt zur **Anforderung der Papier-Lichtbilder**
- Alternativ: Abgabe eines **Digitalbildes per E-Mail** (erheblicher Mehraufwand)
- **Einscannen** der Papierbilder durch Hilfskräfte
- **Web-Statusanzeige** für Studierende, welche Erfordernisse erfüllt sind (Pfand, Bild, E-Mail-Angabe, Druckauftrag)
- **4 Monate lang** herstellen der Kartenerstausstattung
- **Abholbereitschaft** im Web über Statusanzeige

Karten-Ausgabe

- Ausgabe *nur persönlich* im Studentensekretariat
- **Vorlage von Personalausweis/Reisepass**
- Vergleich: Person – Passbild – Chipkartenfoto
- **Mitarbeiter nimmt Pass-Ausstellungsbehörde und Passnummer auf**
- **Studierender quittiert Empfang** der Karte und Infoseite – und erhält eine transparente Schutzhülle (2 Fächer: JLU-Chipkarte und EC-Karte)
- **Karteninhaber geht zur Validierungsstation** und erhält nach der Karteneinführung automatisch
 - RMV(ÖPNV)- und Gültigkeitsaufdruck auf die Chipkarte
 - Bescheinigungen + personalisierten Überweisungsvordr.

Rezertifizierung und Rückmeldung

- **halbjährlich** (Rezertifizierung alternativ ggf. jährlich)
- Vor Beginn der Rückmeldung werden **neue Zertifikate für alle Studierenden** erstellt
- Laufzeit bis Ende neues Semester + 1 Monat
- Automatische **Freigabe zum Download nach Beitragszahlung**
- **Rückmeldung an einem PC mit Chipkartenleser und PIN**
(im Studentensekretariat ohne PC/Chipkarte weiterhin möglich)
- PC-Rückmeldung an beliebigem Ort, umfasst
 - Laden des neuen Zertifikats
 - optional Aktivierung der JLU-Mailadresse (Mailweiterleitung)
 - Anschriftsänderung (jetzt 1, später 2 Adressen), nach Bedarf
 - Rückmeldung (ggf. Hinweise bei Verweigerung)

Probleme an der JLU

- Personalausstattung unzureichend
- Alle Arbeits- und Organisationsprozesse anpassen
- Chipkarte muss sofort bereitstehen
- Verzögerungen bei fast allen Software-Anpassungen, teils organisatorisch teils technisch bedingt
- Lieferanten/Unternehmen haben keine ausgereiften Produkte für Massenanzwendung
- Kartendefekte durch mechanische Belastung
- Es gibt noch keine Mitarbeiterkarte
- **aber ... keine Alternative**

Weitere Information

- Zum **Chipkarten-Betrieb**:
 - <http://www.uni-giessen.de/chipkarte/>
- Zur **Planung** (2000/2001, z.T. überholt):
 - <http://.../chipkarte/vorplanung/>
- **Projekt-Partner**:
 - <http://.../chipkarte/projekt-partner/>
- **Projektleiter**:
 - Falko.Fock@hrz.uni-giessen.de
 - siehe auch www.uni-giessen.de >
Überblick/Personal > X.500/LDAP-Verzeichnis

Danke für Ihr Interesse!

***Die JLU-Chipkarte hofft auf
Nachahmer!***

Wenn Sie noch Fragen haben ...