JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL C. SCHWICKERT

Treber, Udo; Berg, Jan H.; Schwickert, Axel C.

Smart-Card-Anwendungen am Fachbereich Wirtschaftswissenschaften der Justus-Liebig-Universität Gießen

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 7 / 2004
ISSN 1613-6667

Arbeitspapiere WI Nr. 7 / 2004

Autoren: Treber, Udo; Berg, Jan H.; Schwickert, Axel C.

Titel: Smart-Card-Anwendungen am Fachbereich Wirtschaftswissenschaften der Justus-Liebig-Universität Gießen

Zitation: Treber, Udo; Berg, Jan H.; Schwickert, Axel C.: Smart-Card-Anwendungen am Fachbereich Wirtschaftswissenschaften der Justus-Liebig-Universität Gießen, in: Arbeitspapiere WI, Nr. 7/2004, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2004, 90 Seiten, ISSN 1613-6667.

Kurzfassung: An der Justus-Liebig-Universität (JLU-) Gießen wurde zum Wintersemester 02/03 eine multifunktionale Chipkarte als Studentenausweis eingeführt. Im Gegensatz zu herkömmlichen Systemen handelt es sich um eine Smart Card, die in der Lage ist, kryptographische Verfahren auszuführen und damit – eingebettet in die Public-Key-Infrastruktur (PKI) der JLU Gießen – eine sichere Personenidentifizierung im Internet zu ermöglichen. Dies eröffnet zahlreiche neue Anwendungsmöglichkeiten, vor allem da die Nutzung nicht mehr auf uni-interne Terminals beschränkt, sondern grundsätzlich von jedem Personal Computer (PC) mit Chipkartenleser und Internetanschluß möglich ist.

Ziel des Arbeitspapiers ist es, mögliche Anwendungsgebiete und Einsatzbereiche der Smart Card am Fachbereich Wirtschaftswissenschaften der JLU Gießen aufzuzeigen und zu analysieren. In Kapitel 2 werden zunächst die Grundlagen zu Chipkarten erläutert. Anschließend folgt eine Darstellung grundlegender Sicherheitsaspekte von Smart Cards und deren sicherheitsrelevanter Anwendung. Dabei wird vor allem auf die Rolle der Smart Card innerhalb einer Public-Key-Infrastruktur eingegangen. In Kapitel 3 wird die organisatorische und infrastrukturelle Situation am Fachbereich Wirtschaftswissenschaften dargelegt. Kapitel 4 befaßt sich mit der Anforderungsanalyse. Dort werden fachliche Anwendungsbereiche auf Basis der Situationsanalyse ermittelt und bewertet sowie die technischen Anforderungen erläutert. Das Kapitel 5 „Systementwicklung und Integration“ beschreibt die Realisierung einer beispielhaften Anwendung inklusive der zugehörigen Server- und Client-Konfigurationen.

Schlüsselwörter: Smart Card, Chipkarte, Public Key Infrastructure, Zertifikate, elektronische Signatur, Electronic University, Fachbereich, Universität

Inhaltsverzeichnis

Abbildungsverzeichnis

Seite

Abkürzungsverzeichnis

API.....Application Programming Interface
CA.....Certificate Authority
CPU .....Central Processing Unit
CRL .....Certificate Revocation Lists
DAT.....Digital Audio Tape
DES.....Data Encryption Standard
DSL.....Digital Subscriber Line
EEPROM.....Electrical Erasable Read Only Memory
E-Mail.....Electronic Mail
HRZ .....Hochschulrechenzentrum
HTML.....Hypertext Markup Language
GB.....Gigabyte
GHz.....Gigahertz
ID.....Identifier
IP.....Internet Protocol
ISDN.....Integrated Services Digital Network
ISO.....International Standardisation Organization
IT .....Informationstechnologie
IT-SeC .....IT-Service-Center
I/O.....Input/Output
JLU .....Justus-Liebig-Universität
KB.....Kilobyte
Kbit.....Kilobit
LAMP.....Linux/Apache/MySQL/PHP(PERL)
LDAP.....Lightweight Directory Access Protocol
MB.....Megabyte
MBA.....Master of Business Administration
MHz.....Megahertz
NPU .....Numeric Processing Unit
OPAC .....Online Public Access Catalogue
OSI.....Open Systems Interconnection
PA .....Prüfungsamt
PC .....Personal Computer
PC/SC .....Personal Computer/Smart Card
PEM.....Privacy Enhanced Mail
PIN.....Personal Identification Number

PKCS .....Public Key Cryptography Standard
PKI.....Public-Key-Infrastruktur
PS/2.....Personal System 2
RAM .....Random Access Memory
RMV .....Rhein-Main-Verkehrsverbund
ROM .....Read Only Memory
RSA .....Rivest Shamir Adleman
SCSI.....Small Computer System Interface
SHA .....Secure Hash Algorithm
SPIC.....Student Personal Information Center
SSL .....Secure Socket Layer
S/MIME.....Secure Multipurpose Mail Extensions
TAN.....Transaction Number
UniGI-CCA .....Chipcard Certification Authority der Universität Gießen
UniGI-SCA .....SSL-Server Certification Authority der Universität Gießen
USB .....Universal Serial Bus
VPN .....Virtual Private Network
WCMS.....Web Content Management System
WPS.....Web Portal System
W-LAN.....Wireless Local Area Network

1 Problemstellung, Ziel und Aufbau

Zug fahren, Arztbesuche, Geld abheben oder Filme ausleihen, in fast jeder Lebenssituation begegnet man den kleinen bunten Plastikkarten. Unlängst haben sie in nahezu jedermanns Leben Einzug gehalten. Nicht zuletzt aufgrund der rasanten technischen Entwicklung der Chipkarte, wird die Liste von Anwendungsgebieten immer länger. Fast jedes Unternehmen setzt bereits auf die Nutzung von Chipkarten, bspw. im Bereich der Arbeitszeiterfassung, dem Gebäudezugang oder dem Bezahlen in der Betriebskantine. Der Grund dafür ist einfach, sollen doch vor allem die Verwaltungskosten durch die vollständige elektronische Erfassung, Verarbeitung und Auswertung aller Daten gesenkt werden, während gleichzeitig der Komfort der Nutzer erhöht wird. Im Zuge der Entwicklung von „intelligenten" Chipkarten gewinnt aber auch immer mehr deren sicherheitsrelevante Anwendung an Bedeutung. Eingesetzt als Identifikations- und Sicherheitsmedium, sind sogenannte Smart Cards in der Lage, elektronische Dokumente zu verschlüsseln und zu signieren und dadurch Ziele wie die Geheimhaltung von Informationen, die Verbindlichkeit und deren Nichtabstreitbarkeit sicherzustellen. Die Probleme, die aus der Nichtgewährleistung dieser Ziele gerade in einem solch unsicheren und offenen Medium wie dem Internet entstehen, wurden bereits hinreichend diskutiert.[1] Grundsätzlich gilt nach wie vor: Wenn das Internet mit allen seinen Vorteilen sinnvoll für die Abwicklung kritischer Prozesse genutzt werden soll, muß ein gewisses Maß an Sicherheit garantiert werden können. Dies gilt für Kaufverträge ebenso wie für Finanztransaktionen.[2]

Auch die Universitäten haben die Vorteile von Chipkartenanwendungen erkannt. Mittlerweile haben viele deutsche Universitäten einen elektronischen Studentenausweis eingeführt oder planen eine baldige Ausgabe.[3] So setzt die Chipkarte ihren Siegeszug unter Namen wie Campuskarte, MUCK, TUNIKA oder einfach Unicard fort.[4] Ebenso vielfäl-

1 Zu den Gefahren im Netz vgl. Janowicz, Krzysztof: Sicherheit im Internet, Köln: O'Reilly Verlag 2002, S. 2 ff.

2 Vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, 2., aktualisierte und erweiterte Aufl., Heidelberg: dpunkt-Verlag 2002, S. 153 f.

3 Bei Recherchen im Internet lassen sich über 50 Chipkartenprojekte an deutschen Universitäten und Fachhochschulen ausmachen. Eine Auswahl in Form einer Übersicht findet sich unter URL: http://www.ruhr-uni-bochum.de/dezernat6/chipkarte/externes/chip_andere_hs.htm.

4 Die TU Berlin führte eine multifunktionale Chipkarte unter dem Namen Campuskarte ein. Weitere Informationen unter URL: http://wwwpc.prz.tu-berlin.de/tu-chipkarte.

Hinter MUCK verbirgt sich die „Multifunktionelle-Universitäts-Chipkarte" der Universität Würzburg. Weitere Informationen unter URL: http://www.zv.uni-wuerzburg.de/sb/infoseiten/info_index.htm.

Die Universität Trier führte eine Chipkarte unter dem Namen „Trierer Universitätskarte" (TUNIKA) ein. Weitere Informationen unter URL: http://www.uni-trier.de/tunika/tunika.htm.

Die Chipkarten der Universitäten Freiburg und Leipzig werden Unicard genannt. Weitere Informationen unter URL: http://www.verwaltung.uni-freiburg.de/chipkarte, bzw. http://www.uni-leipzig.de/vorles/card.

tig wie die Namensgebung sind dabei aber auch die Kartenarten und die Anwendungsgebiete. Allen gemein ist allerdings das Ziel, nahezu alle Prozesse, von der Rückmeldung, über die Bücherausleihe bis hin zum Bezahlen in der Mensa, sinnvoll zu elektronisieren. Dabei handelt es sich meist um sogenannte Multifunktionskarten, die mehrere Funktionalitäten vereinen und dadurch die oft bis dahin vorherrschenden kostenintensiven Insellösungen ablösen.

Als Pionier gilt dabei die Universität Trier, die bereits 1997 über 11.000 Chipkarten in den Umlauf brachte. Bei dem bis heute unter dem Namen „Trierer-Modell“ bekanntem Verfahren, wird als Studentenausweis eine kontoungebundene Geldkarte der örtlichen Bank ausgegeben. Diese Kooperation zeigt sich bei der äußeren Gestaltung der Karten ebenso wie bei der Nutzung des Chips. So dient eine Seite der Chipkarte der Universität als Studentenausweis, auf der Angaben zum Karteninhaber, wie der Name, Matrikelnummer, ein Lichtbild etc. zu finden sind, während die andere Seite der Bank zur Nutzung überlassen ist. Auch auf dem Speicherchip finden sich neben den Geldkartendaten der Bank noch Angaben zur Person in elektronischer Form. Dadurch werden neben der Bezahlfunktion weitere Anwendungen im Bereich der studentischen Selbstverwaltung möglich. Beispiele sind hier die Rückmeldung oder das Ändern von Personendaten. Dies kann allerdings nur über eigens für diesen Zweck von der Universität aufgestellte Spezial-Terminals erfolgen, da ein Einsatz im offenen Internet aufgrund des fehlenden Identitätsnachweises nicht möglich ist.[5] Als weiterer Nachteil ist sicherlich die Abhängigkeit von der örtlichen Bank zu sehen. Aus diesem Grund setzen viele Universitäten eigene Chipkarten und Bezahlverfahren ein. Die ausgegebenen Karten sind meist eine Kombination aus einem kontaktbehafteten und einem kontaktlosen Chip, wobei letzterer hauptsächlich für Zahlungsvorgänge im Bereich der Universität genutzt wird. Auf dem kontaktbehafteten Chip finden sich, wie beim „Trierer-Modell“, die persönlichen Daten des Karteninhabers. Aber auch bei dieser Lösung wird meist auf den Einsatz von Sicherheitsmechanismen verzichtet, so daß ein Einsatz im Internet nicht möglich und die Nutzung auf uni-interne Terminals beschränkt ist. Nicht zuletzt aus diesem Grund, werden diese Modelle oft als Minimallösungen bezeichnet, finden allerdings aufgrund der relativ niedrigen Kosten zahlreiche Nachahmer.[6]

Einen anderen Weg ging die Justus-Liebig-Universität (JLU-) Gießen, als sie zum Wintersemester 2002/2003 eine multifunktionale Chipkarte als Studentenausweis einführte. Wie bei den anderen Modellen werden damit bereits zahlreiche Anwendungen realisiert. So dient sie mittlerweile als elektronische Geldbörse, Bibliotheksausweis, Fahrkarte für

5 Weitere Informationen zur diesem Modell unter URL: http://www.uni-trier.de/tunika/allgemein.htm.

6 Als Beispiele solcher Lösungen sind die Chipkartenprojekte der Universität Würzburg, Ulm, Leipzig oder der TH Karlsruhe zu nennen.

den öffentlichen Nahverkehr und einiges mehr.[7] Aber im Gegensatz zu den bisher vorgestellten Verfahren, handelt es sich dabei um eine Smart Card mit kryptographischem Koprozessor, die in der Lage ist, kryptographische Verfahren auszuführen und damit, eingebettet in eine Public-Key-Infrastruktur (PKI), eine sichere Personenidentifizierung im Internet zu ermöglichen.[8] Dies eröffnet zahlreiche neue Anwendungsmöglichkeiten, vor allem da die Nutzung nicht mehr auf uni-interne Terminals beschränkt, sondern grundsätzlich von jedem Personal Computer (PC) mit Chipkartenleser und Internetanschluß möglich ist.

Auch am Fachbereich Wirtschaftwissenschaften der Justus-Liebig-Universität Gießen lassen sich zahlreiche Anwendungsbereiche ausmachen. Nicht zuletzt da die grundlegenden technischen Vorraussetzungen in Form einer bestehenden portalgestützten Web Site und der Smart Card gegeben sind, liegt die Forderung nahe, die Vorteile durch eine Umsetzung nutzbar zu machen. Dazu muß im Vorfeld ein Konzept erstellt werden, in dem mögliche Anwendungsgebiete diskutiert und Möglichkeiten einer Integration aufgezeigt werden. An dieser Stelle setzt die vorliegende Arbeit an.

Ziel dieser Arbeit ist es, mögliche Anwendungsgebiete und Einsatzbereiche der Smart Card am Fachbereich Wirtschaftswissenschaften aufzuzeigen und zu evaluieren. Dabei beschränkt sich die Diskussion auf den Einsatz des kontaktbehafteten Kryptochips, mit dem sich eine Reihe von authentifizierungs- und sicherheitskritischen Anwendungen realisieren lassen. Neben der Anwendung der Smart Card als Authentifizierungsmedium für Rechnersysteme innerhalb des Fachbereichs liegt ein besonderes Augenmerk auf den Einsatzmöglichkeiten im Internet. In diesem Bereich bildet das Web Portal System (WPS) des Fachbereichs eine geeignete Implementierungsplattform und damit das Zielsystem vieler Anwendungen. Im Anschluß an die Anwendungsanalyse soll eine beispielhafte Anwendung realisiert werden.

Zu diesem Zweck werden in Kapitel 2 zunächst die theoretischen Grundlagen erläutert, wobei kurz die Entwicklung der Chipkarten dargestellt und anschließend der Begriff der Smart Card definitorisch abgegrenzt werden soll. Anschließend folgt eine Darstellung grundlegender Sicherheitsaspekte von Smart Cards und deren sicherheitsrelevanter Anwendung. Dabei soll vor allem auf die Rolle der Smart Card innerhalb einer Public-Key-Infrastruktur eingegangen und deren wichtigste Anwendungsgebiete kurz erläutert werden. In Kapitel 3 folgt eine umfassende Situationsanalyse, in der zum einen auf die organisatorischen Gegebenheiten und zum anderen auf die infrastrukturellen Grundlagen am Fachbereich Wirtschaftswissenschaften eingegangen wird.

7 Zu den bereits realisierten Einsatzgebieten der Chipkarte an der Universität Gießen, vgl. Kapitel 3.3.1.2 Derzeitige Nutzung und Entwicklungen.

8 Weitere Informationen zum Chipkartenprojekt an der Justus-Liebig-Universität Gießen unter URL: http://www.uni-giessen.de/chipkarte.

Der eigentliche Kern der Arbeit folgt in Kapitel 4 mit der Anforderungsanalyse. Dort werden fachliche Anwendungsbereiche auf Basis der Situationsanalyse ermittelt und evaluiert. Die technischen Anforderungen dazu werden in Kapitel 4.4 beschrieben. Anschließend legt die Priorisierung der Anwendungsgebiete fest, welche im folgenden prototypisch realisiert werden sollen. Das Kapitel 5 „Systementwicklung und Integration" beschreibt die Realisierung der beispielhaften Anwendung und deren Integration in das Web Portal System des Fachbereichs. Ein Ausblick, in dem vor allem auf die erwarteten zukünftigen Entwicklungen und den weiteren Projektverlauf eingegangen wird, schließt die Arbeit ab.

2 Smart Cards und Public-Key-Infrastruktur

2.1 Chipkarten – Eine Einführung

Mittlerweile nicht mehr aus dem alltäglichen Leben wegzudenken, liegen die Wurzeln der Chipkarte bereits in den 50er Jahren, damals allerdings in Form einer einfachen Plastikkarte, welche lediglich die unzulängliche Haltbarkeit von Karten aus Papier oder Karton überwinden sollte. Eine erste solche Karte wurde 1950 von Diners Club in den USA herausgeben,[9] um dem damals noch exklusiven Kreis von Besitzern bargeldlose Zahlvorgänge in Hotels und Restaurants zu ermöglichen. Später folgten VISA und Mastercard und steigerten somit die weltweite Akzeptanz von Plastikkarten. Zur eindeutigen Identifikation diente lediglich die Hochprägung der Karte in Verbindung mit der Unterschrift des Besitzers auf dem Kartenbeleg, die mit der Referenzunterschrift auf der Karte verglichen wurde. Dieses System hatte neben der hohen Mißbrauchsgefahr vor allem den entscheidenden Nachteil, daß die Daten nicht ohne weiteres maschinell ausgewertet, verbucht und verarbeitet werden konnten. Aus diesem Umstand wurden die Karten wenig später mit einem Magnetstreifen versehen. Auf diesem waren die Kartendaten zusätzlich gespeichert und konnten einfacher maschinell ausgewertet werden. Diese Kombination aus Hochprägung, Referenzunterschriftenfeld und Magnetstreifen findet bis heute in Form der Kreditkarte weltweit die breiteste Verwendung.[10]

Die Entwicklung der eigentlichen Chipkarten begann im Jahre 1968, als das Patent für den Einbau integrierter Schaltflächen in einfache Plastikkarten von den beiden Deutschen Jürgen Dethloff und Helmut Gröttrupp angemeldet wurde. Bald folgten ähnliche Patente in Frankreich und Japan. Da es nun möglich war, die Karten mit einer Sicher-

9 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, 4. überarbeitete und aktualisierte Aufl., München; Wien: Hanser Verlag 2002, S. 2.

10 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 2 f.

heitslogik auszustatten, konnten erstmals auch sensitive Daten direkt auf der Karte hinterlegt werden. Die bisher erforderliche und kostenintensive Verbindung zu einem gesicherten Host, bspw. zum Abgleich der Personal Identification Number (PIN), war nun nicht mehr erforderlich. Ebenso konnten die Kartendaten nicht mehr kopiert oder manipuliert werden, wie das bei den Magnetstreifenkarten der Fall ist. Trotz anfänglicher Probleme waren damit die Vorraussetzung für eine Reihe neuer Anwendungen geschaffen.[11]

Ihren Durchbruch hatte die Chipkarte aber erst 1986. Nach einem erfolgreichen Pilotprojekt führte die französische Telefongesellschaft PTT die Chipkarte zum Telefonieren in ganz Frankreich ein. Bereits vier Jahre später waren fast 60 Millionen Chipkarten im Umlauf. Mit einer Verzögerung von etwa drei Jahren erfolgte in Deutschland ebenfalls die Einführung der Chipkarte im Telefonsektor. Auch auf dem Bankensektor nahmen die Franzosen eine Vorreiterrolle ein. Bereits 1984 wurden Bankkarten mit integriertem Chip von einigen französischen Banken ausgegeben. In Deutschland machte dieses Prinzip erst 1997 unter dem Namen „Geldkarte“ Schlagzeilen. Mittlerweile sind die Anwendungsfelder für Karten aller Art nicht mehr überschaubar. Spätestens seit der Entwicklung der kontaktlosen Chipkarte findet man Karten in sämtlichen Lebenssituationen. Beim Bezahlen in Kantinen, Schwimmbädern und Parkhäusern, als Zugangskontrolle zu Gebäuden, Ski-Liften und Flugzeugen findet die kontaktlose Karte Anwendung.[12] Die bundesweite Einführung der Krankenversichertenkarte im Jahr 1994 hat schlußendlich dazu geführt, daß fast jeder Deutsche zumindest eine Chipkarte besitzt. Damit seien nur einige Bereiche und Kartentechniken angesprochen.[13]

Eine solch rasante Verbreitung in den unterschiedlichsten Bereichen macht eine Abstimmung bzw. Standardisierung unabdingbar. Aufgrund der hohen wirtschaftlichen Bedeutung ging dieser Normungsprozeß auch relativ schnell vonstatten. Die Ergebnisse sind in den Standards ISO 7810-7813 sowie ISO 7816 zu finden.[14] In den Standards sind neben dem Aufbau und der Lage aller Elemente auf der Karte auch alle OSI-Schichten

11 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 3 f.

12 Dabei ist die Form solcher Medien nicht unbedingt auf die einer Karte begrenzt. Durch die kontaktlose Übertragungstechnik finden auch Formen wie Ringe, Stöpsel und Knöpfe Anwendung. Vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 192.

13 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 4 ff.

14 Eine Übersicht über die verschiedenen Arbeitsgruppen der weltweiten Chipkartennormung findet sich in Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 13.

von dem Physical Layer bis zum Application Layer genormt.[15] Abbildung 1 zeigt exemplarisch eine Chipkarte nach dem „ID-1"-Format.[16]

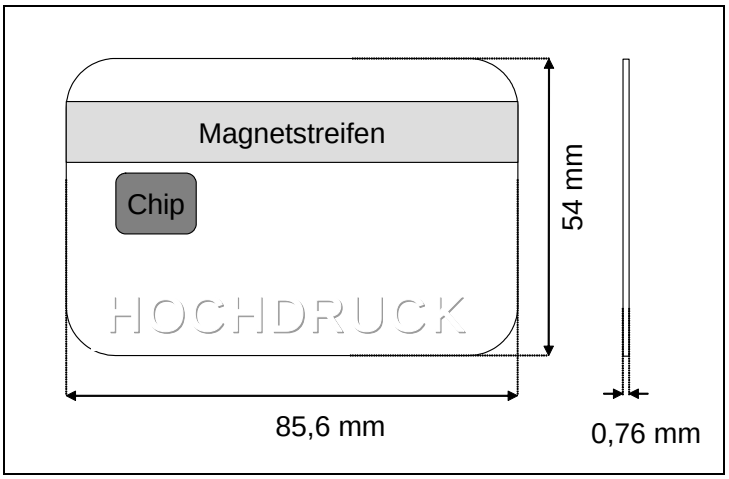

Abb. 1: Schematische Darstellung einer Chipkarte nach dem „ID-1"-Format[17]

Wie in diesem Abschnitt bereits zu erkennen ist, gibt es eine fast unüberschaubare Zahl von Kartenarten, Techniken und Merkmalen. Zudem sind sie meistens nicht in Reinform, sondern oft in Kombination zu finden. Man denke bspw. nur an die Kreditkarte oder die EC-Karte mit Geldkarten-Chip. Im folgenden Abschnitt sollen die einzelnen Kartenarten voneinander abgegrenzt und anschließend der Begriff der Smart Card definiert werden.

2.2 Definitorische Abgrenzung des Begriffs Smart Card

Eine definitorische Abgrenzung des Begriffs der Smart Card ist insofern von Bedeutung, da dieser weder im alltäglichen Sprachgebrauch noch in der Literatur eine einheitliche Verwendung findet. So werden bspw. des öfteren die Begriffe Chipkarte und Smart Card synonym verwendet.[18] Dies sorgt nicht selten für Verwirrung und Verständnisprobleme. Daher werden im Folgenden zuerst die einzelnen Kartenarten kurz darge-

15 Für eine kurze Beschreibung der einzelnen Ebenen und die zugehörigen Standards vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 193 f.

16 Neben dem kreditkartengroßen „ID-1"-Format existieren weitere Formate. Wie bspw. das „ID-000"-Format für den Einsatz in Mobiltelefonen. Vgl. dazu Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 30 ff.

17 In Anlehnung an Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 30.

18 Dies ist auch in diversen Online-Wörterbüchern der Fall. Vgl. dazu Networds, Online im Internet: URL: http://www.networds.de/cgi-bin/n2dbi_sel_anzeige.pl?sword=chipcard&, 19.02.2004 oder Net-Lexikon, Online im Internet: URL: http://net-lexikon.de/Chipkarte.html, 19.02.2004.

stellt und erläutert. Anschließend soll der Begriff Smart Card im Sinne dieser Arbeit definiert werden.

Als Oberbegriff für alle Karten, die in dem Zusammenhang mit Identifikation und Authentifizierung stehen, soll in Anlehnung an ISO 7810 der Begriff „Identifikationskarten“ dienen. Abbildung 2 gibt einen Überblick über die einzelnen Kartenarten.

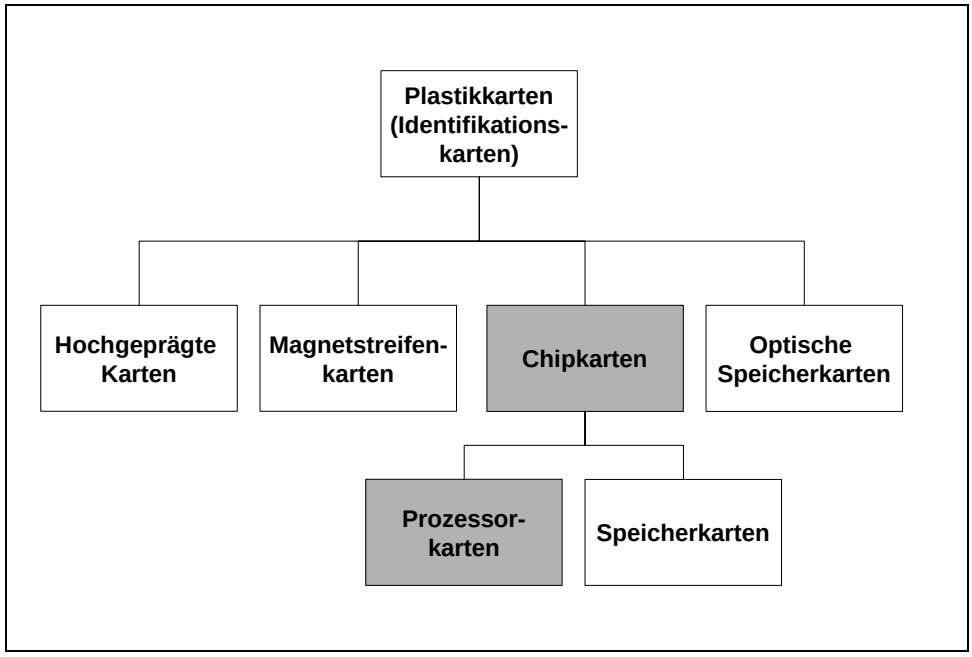

Abb. 2: Überblick über die verschiedenen Kartenarten

Hochgeprägte Karten sind die ältesten Vertreter der Identifikationskarten. Die Art und die Lage der Zeichen auf der Karte sind in der Norm ISO 7811 festgelegt. Dabei sind auch Bereiche für die einzelnen Daten auf der Karte definiert. So ist bspw. ein Bereich für die Kartenidentifikationsnummer und ein anderer für persönliche Daten des Karteninhabers reserviert. Dies erlaubt eine rudimentäre maschinelle Verarbeitung dieser Daten.[19]

Eine erste Weiterentwicklung in diesem Sektor waren die Magnetstreifenkarten. Der auf der Rückseite angebrachte Magnetstreifen enthält die digital kodierten Kartendaten. Zum Auslesen muß der Magnetstreifen lediglich an einem Lesekopf vorbeigezogen werden. Insgesamt sind alle Normen für diese Kartenart in ISO 7811 zu finden. Die Norm beschreibt die Eigenschaften des Magnetstreifens, die Kodiertechnik und die Lage der Magnetspuren. Eine Besonderheit ist dabei, daß die dritte Spur auch beschreibbar ist. Die maximal zu speichernde Datenmenge liegt etwa bei einem Kilobyte. Grundsätzlich werfen diese Karten einige Sicherheitsfragen auf. Da der Magnetstreifen über keine Schutzmechanismen verfügt, kann jede Karte ohne weiteres mit einem handelsüblichen

19 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 17 f.

Schreib-/Lesegerät ausgelesen, manipuliert und kopiert werden. Wie eingangs bereits erwähnt, ist dadurch eine Speicherung von sensitiven Daten auf der Karte selbst nicht möglich. Daher bedarf die Authentifizierung einer Online-Verbindung zu einem gesicherten Host, auf dem ein Abgleich bspw. per PIN erfolgen kann.[20]

Alle Karten, die mit einer integrierten Schaltung ausgestattet sind, werden unter dem Namen Chipkarten zusammengefaßt und deren wesentliche Eigenschaften in der ISO Normen Reihe 7816 festgelegt. Die integrierten Schaltungen besitzen Elemente zur Datenübertragung, Verarbeitung und Speicherung. Die Übertragung der Daten kann sowohl über Kontakte als auch kontaktlos erfolgen. Im Vergleich zu den Magnetstreifenkarten bieten Chipkarten ein Vielfaches an Speicherkapazität. Der größte Vorteil ist allerdings, daß die Daten gegen unbefugten Zugriff geschützt werden können. Der Zugriff erfolgt nur über eine wohldefinierte Schnittstelle, die vom Betriebsystem oder einer Sicherheitslogik gesteuert wird. Dadurch ist es möglich, daß die Karte Daten beherbergt, die nicht von außen gelesen, sondern nur intern verarbeitet werden können. Es ist also möglich, sensitive Daten, wie bspw. PIN oder private Schlüssel, direkt auf der Karte zu hinterlegen. Auf eine aufwendige und kostenintensive Verbindung zu einem Host-Rechner kann somit verzichtet werden. Aufgrund der Unterschiede in der Leistungsfähigkeit und Funktionalität unterscheidet man in diesem Zusammenhang Speicherkarten und Prozessorkarten.[21]

Wie der Name schon sagt, finden Speicherkarten ihre Hauptanwendung im Speichern von Informationen. Diese bestehen aus einem oder mehreren Speichern und können zusätzlich mit einer Sicherheitslogik ausgestattet sein, die im einfachsten Fall nur aus einem Schreib- und Löschschutz für den Speicher besteht. Über den Input/Output-Port (I/O-Port) werden Daten synchron von und zur Karte übertragen. Bekannte Beispiele sind die Krankenversichertenkarte und die Telefonkarte, wobei letztere mit einer Sicherheitslogik versehen ist.[22]

Prozessorkarten hingegen sind als vollständige Computer zu verstehen. Sie verfügen zusätzlich über einen Prozessor und einen Arbeitsspeicher. Oftmals findet sich auch ein Koprozessor für spezielle Aufgaben, z. B. kryptographische Verfahren, zusätzlich auf der Karte. Abbildung 3 zeigt die typische Architektur einer Prozessorkarte mit Koprozessor.

20 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 18 ff. und Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 190.

21 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 20. und Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 190.

22 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 21 f.

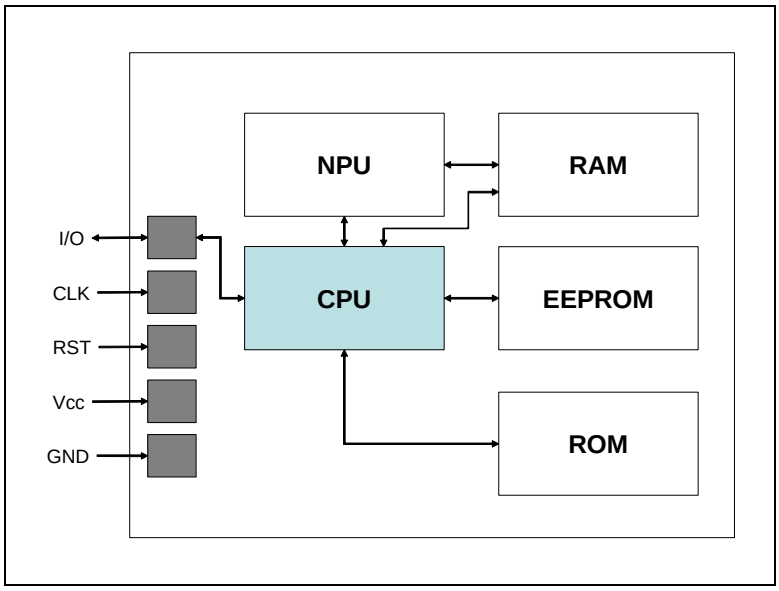

Abb. 3: Schematischer Aufbau einer Prozessorkarte mit Koprozessor[23]

Könnte rein äußerlich betrachtet der Vergleich von einer kleinen Chipkarte mit einem herkömmlichen Computer noch befremdlich erscheinen, ändert sich dies mit einem Blick unter die Oberfläche grundlegend. Nahezu jede Basiskomponente eines vollständigen Computers ist in angepaßter Form auch im Innenleben einer Prozessorkarte zu finden. Herz der Karte ist die Central Processing Unit (CPU), die zusammen mit der Numeric Processing Unit (NPU) alle Operationen steuert und ausführt.[24] Das Random Access Memory (RAM) ist der flüchtige Arbeitsspeicher des Prozessors. Im Unterschied zu einem herkömmlichen PC ist das Betriebsystem fest im Read Only Memory (ROM) eingebrannt. Anstatt einer Festplatte besteht der nicht-flüchtige Speicher der Karte aus einem Electrical Erasable Read Only Memory (EEPROM). Auf diesem können Daten und Programme unter Kontrolle des Betriebssystems gelesen, geschrieben oder ausgeführt werden. Unabhängig von der Art der Datenübertragung kann die Karte nur über die I/O-Schnittstelle mit der Außenwelt kommunizieren.[25]

Der Vollständigkeit halber soll an dieser Stelle noch kurz auf die optischen Speicherkarten eingegangen werden. Optische Karten bieten von allen Karten die größte Speicherkapazität. Diese liegt oftmals im Megabyte-Bereich und eignet sich somit sogar zur Archivierung von Multimediadaten wie bspw. Bildern. Ein wesentlicher Nachteil ist al-

23 In Anlehnung an Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 22.

24 Dabei wird die CPU meist vereinfachend als Prozessor und die NPU als Koprozessor bezeichnet.

25 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 22 f. und Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 190 f.

lerdings, daß diese Karten nach dem heutigen Stand der Technik nur einmal beschreibbar sind.[26]

In der Praxis finden sich die dargestellten Kartenarten meist nicht in Reinform, sondern als Kombination einzelner Typen und Techniken. Dies kann mehrere Gründe haben. Als ein Hauptgrund sei die Auf- und Abwärtskompatibilität von Techniken genannt. So findet sich bspw. auf Kreditkarten neben dem Magnetstreifen auch noch die Hochprägung. Ein anderer Grund ist die Abdeckung verschiedener Funktionalitäten mit nur einer Karte. Solche multifunktionalen Karten bestehen häufig aus der Kombination von kontaktloser Speicherkarte und kontaktbehafteter Prozessorkarte, wobei bspw. der kontaktlose Teil für Bezahlvorgänge und der kontaktbehaftete Teil zum verschlüsseln und signieren von Daten benutzt wird. Bei solchen Kombinationen trifft man häufig auf die Begriffe Dual-Access- oder Dual-Interface-Karten, sowie Twin-Karten. Unter einer Dual-Access/Interface-Karte wird in den meisten Fällen eine Karte mit einem Chip verstanden, auf den man kontaktlos und kontaktbehaftet zugreifen kann.[27] Die sogenannten Twin-Karten beschreiben eine echte Kombination von bspw. Speicherkarte und Prozessorkarte, auf welcher die Chips unabhängig voneinander sind und zwischen denen keinerlei Datenaustausch stattfindet.[28] Diese Begriffe werden allerdings nicht einheitlich verwendet. Ein weiterer interessanter Grund für eine Kombination ist der Verbund von Techniken. Die große Speicherkapazität einer optischen Speicherkarte wird bspw. mit der Intelligenz einer Mikroprozessorkarte kombiniert. Dadurch wird es möglich die Daten in dem optischen Speicher verschlüsselt zu hinterlegen und somit vor unerlaubtem Zugriff zu schützen.[29] Den Möglichkeiten sind durch die nahezu beliebige Kombination von Chiptypen und Übertragungstechniken fast keine Grenzen gesetzt. Eine ausführliche Beschreibung aller Kombinationen und den daraus entstehenden Möglichkeiten würde den Rahmen dieser Arbeit übersteigen.

Wie anfangs bereits erwähnt, finden sich in der Literatur viele verschiedene Definitionen der Smart Card. Einigkeit besteht anscheinend nur in der Ansicht, daß alle Smart Cards Chipkarten sind. Darunter weichen die einzelnen Definitionen allerdings weit voneinander ab. Im Rahmen dieser Arbeit sollen unter dem Begriff Smart Card, die Karten verstanden werden, die mit einem Mikroprozessor (CPU) ausgestattet und

26 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 26 f.

27 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 918.

28 Die schematischen Darstellungen solcher Architekturen finden sich bei: Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 24 f.

29 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 26 f.

grundsätzlich in der Lage sind, kryptographische Verfahren auszuführen.[30] Darunter fallen selbstverständlich nicht nur reine Prozessorkarten, sondern auch Kombinationen solcher mit anderen Kartentypen.

2.3 Grundlegende Sicherheitsaspekte der Smart Card

Smart Cards werden ebenso wie Plastikkarten hauptsächlich zur Identifikation eingesetzt. Jedoch bieten diese Karten entscheidende Vorteile gegenüber anderen Kartenarten und Medien. Diese sollen im Folgenden kurz erläutert werden.

Grundsätzlich gibt es drei Möglichkeiten zur Identifizierung einer Person: Der Besitz einer Sache, das Wissen um ein Geheimnis oder die Eigenschaften des Körpers.[31] Während herkömmliche Sicherheitsmechanismen meist nur eine Möglichkeit prüfen, sind mit dem Einsatz von Smart Cards Kombinationen möglich. In den meisten Fällen ist dies eine Kombination aus dem Besitz einer Sache (in diesem Fall die Smart Card) und dem Wissen um ein Geheimnis. Das Geheimnis stellt in den meisten Fällen eine PIN dar. Da das Wissen des Geheimnisses nur dem Karteninhaber zugänglich ist bzw. sein sollte, ist bei einer solchen Kombination sichergestellt, daß sich auch tatsächlich diese Person mit der Karte authentifiziert. So ist es bspw. nur dem Karteninhaber gestattet, auf die auf der Karte gespeicherten Daten zuzugreifen, bzw. eine Berechtigung hierfür zu erteilen. Ohne das Wissen um die PIN ist die Karte nahezu wertlos; ebenso wie das Wissen um die PIN ohne die Karte wertlos ist. Damit die PIN nicht durch sukzessives Ausprobieren möglicher Kombinationen ermittelt werden kann, ist jede Karte mit einem Fehlversuchszähler ausgestattet. Dieser Zähler sperrt die Karte, sobald eine vorher festgelegte Anzahl von Fehlversuchen registriert wird.[32]

Trotzdem ist die Verwendung von PIN nicht ganz unproblematisch. Zum einen bieten sich bei der Eingabe der PIN zahlreiche Möglichkeiten eines Angriffs, sei es durch einfaches „über die Schulter schauen“ oder durch die Manipulation des Terminals. Zum anderen müssen sich die Benutzer mittlerweile zahlreiche Nummern und Paßwörter merken, daß oft Trivialwerte, wie bspw. „1234“ verwendet werden oder die PIN sorglos auf der Karte notiert wird.[33] Aus diesem Grund wird verstärkt an Systemen zur Benut-

30 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 945. Auch Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 191. Wobei Merz in seiner Definition den privaten Schlüssel als wichtigstes Merkmal einer Smart Card sieht.

31 Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 501 f., auch Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 164.

32 Vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 197.

33 Zu der Sicherheit und Problemen von PIN-Verfahren vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 503 ff.

zeridentifikation gearbeitet, die auf den Eigenschaften des Körpers basieren. Bekannte Beispiele sind der Fingerabdruck oder eine Prüfung der Netzhaut. Diese biometrischen Verfahren haben den Vorteil, daß sie nicht wissensbasiert sind und somit nicht vergessen oder verraten werden können. Demnach sind diese nicht übertragbar und damit unstreitig an eine Person gekoppelt und bieten dadurch eine sicherere Benutzeridentifikation. Solche Verfahren kranken aber häufig an dem hohen technischen Aufwand, nicht ausgereifter Technologie und mangelnder Benutzerakzeptanz.[34] Diese Verfahren können aber alternativ oder zusätzlich zu der Sicherung durch PIN eingesetzt werden. Es wäre daher möglich, die Benutzeridentifikation anhand von drei unabhängigen Kriterien durchzuführen und wirklich nur dem Besitzer Zugriff auf die Karte zu gestatten.

Um an dieser Stelle den Vergleich mit einem herkömmlichen PC wieder aufzugreifen, kann man sagen: „Eine Smart Card ähnelt einer Workstation im Netzwerk, die durch ein gußeisernes Gehäuse und sicheres Kommunikationsprotokoll geschützt ist“[35]. Diese Eigenschaften unterscheiden die Smart Card sicherheitstechnisch von herkömmlichen Computersystemen und Speichermedien, denn niemand kann auf der Ebene der Hardware oder des Betriebssystems in die Karte eindringen. Schließlich ist die wohldefinierte und geschützte I/O-Schnittstelle die einzige Verbindung der Karte mit der „Außenwelt“. Versucht man diese Schnittstelle durch einen physischen Angriff, bspw. durch „öffnen“ der Karte oder Abfräsen der Oberfläche, zu umgehen, zerstört sich die Karte eher selbst. Physische Angriffe sind daher schon allein bauartbedingt nahezu aussichtslos.[36] Aber selbst dem berechtigten Besitzer erlaubt die Karte keineswegs einen uneingeschränkten Zugriff auf den Speicher, bzw. die Daten. Da der Zugriff auf die Smart Card nur durch ein Application Programming Interface (API) erfolgen kann, wird sichergestellt, daß nur die von der Smart Card bereitgestellten Funktionalitäten von außen abgerufen werden können. Der gesamte Befehlsumfang der API-Funktionen ist im Personal Computer/Smart-Card-Standard (PC/SC-Standard) festgelegt.[37]

Durch diese speziellen Schutzmaßnahmen eignet sich die Smart Card im besonderen Maße als Geheimnisträger. Es wundert daher nicht, daß die Smart Card im Rahmen von Public-Key-Infrastrukturen als Träger von privaten Schlüsseln Verwendung findet. Durch den kryptographischen Koprozessor ist die Karte in der Lage, ein Schlüsselpaar

34 Für eine ausführliche Beschreibung von im Chipkartenumfeld eingesetzten biometrischen Verfahren vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 509 ff.

35 Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 190.

36 Für eine vollständige Darstellung von Angriffen auf Smart Cards und den Sicherheitsmerkmalen vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 521 ff.

37 Vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 197.

zu erzeugen und zu verwenden, ohne daß der private Schlüssel jemals außerhalb der Karte sichtbar ist. Alle sicherheitsrelevanten Vorgänge, wie das Verschlüsseln und Signieren von Daten, können ausschließlich innerhalb der Karte ablaufen.

Im folgenden Abschnitt soll nun auf die sicherheitsrelevanten Anwendungen von Smart Cards eingegangen werden. Zu diesem Zweck werden zunächst kurz die kryptographischen Grundlagen sowie die Notwendigkeit von Zertifikaten erläutert. Anschließend wird auf die Anwendung der Smart Card im Rahmen einer Public-Key-Infrastruktur eingegangen.

2.4 Sicherheitsrelevante Anwendungen

2.4.1 Kryptographische Grundlagen

Schon seit Jahrhunderten stellen sich in der Nachrichtenübermittlung die gleichen Fragen: Wie kommen meine Informationen ungesehen, unverändert bei dem richtigen Empfänger an? Auf der anderen Seite steht die Frage: Wie kann ich sicher sein, daß die Informationen von dem angegebenen Absender stammen und diese Informationen verbindlich sind?

Daraus lassen sich die vier Ziele der Kryptographie ableiten: Die

- Vertraulichkeit,
- die Integrität,
- die Authentizität und
- die Verbindlichkeit oder Nichtabstreitbarkeit.

Diese Ziele sind voneinander unabhängig und stellen jeweils unterschiedliche Anforderungen an das System.[38] Gerade in Zeiten fortschreitender „Virtualität“ und vernetzter Unternehmen sind diese Forderungen wichtiger denn je. Wenn es möglich sein soll, rechtsverbindliche Verträge und Erklärungen über ein solch unsicheres und offenes Medium wie dem Internet abzuschließen, muß durch geeignete Methoden und Techniken eine gewisse Sicherheit und Verbindlichkeit geschaffen werden.

Zwar haben sich im Laufe der Jahre die Methoden verändert, jedoch ist das Prinzip nach wie vor das Gleiche. Die Nachricht wird von dem Sender derart verschlüsselt und damit unkenntlich gemacht, daß er sicher sein kann, daß nur der Empfänger in der Lage ist diese Informationen zu lesen. Kryptographische Verfahren schützen demnach Daten, Texte, etc. vor Offenlegung oder Manipulation, indem diese nach einem gewissen Mu-

38 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 178. Für eine eher technische Sicht sowie eine Übersicht der Bedrohungen vgl. Schäfer, Günter: Netzsicherheit – Algorithmische Grundlagen und Protokolle, Heidelberg: dpunkt-Verlag 2003, S. 8 f.

ster oder Prinzip unkenntlich gemacht werden. Die Kryptographie bedient sich zu diesem Zweck digitaler Schlüssel und mathematischer Funktionen bzw. Algorithmen. Diese digitalen Schlüssel sind im Kern nichts anderes als Zeichenfolgen, deren Qualität und Sicherheit in erster Linie von deren Länge und dem verwendeten Verfahren abhängt. Grundsätzlich unterscheidet man zwischen symmetrischen und asymmetrischen Verfahren.[39]

Bei den symmetrischen Verfahren kommt der gleiche Schlüssel zum ver- und entschlüsseln zum Einsatz. Der bekannteste Vertreter ist hier der Data-Encryption-Standard-Algorithmus (DES).[40] Da die eingesetzten Schlüssel gleich sind, unterliegen sie zwingend der Geheimhaltung. Aus diesem Grund werden diese Verfahren auch als Private-Key-Verfahren bezeichnet. Darin liegt auch zugleich das Hauptproblem dieser Verfahren. Besonders problematisch ist dieser Umstand, will man mit einem bisher unbekannten Kommunikationspartner Kontakt aufnehmen. Schließlich wäre es höchst fahrlässig und unsinnig, den geheimen Schlüssel einfach an die verschlüsselte Nachricht anzuhängen. Daher muß der Schlüsseltausch über ein sicheres Medium, bspw. durch eine eigenhändig übergebene Diskette, stattfinden. Dies ist aber gerade in einer Internetumgebung in den wenigsten Fällen möglich. Trotz dieser Problematik haben symmetrische Verfahren durchaus ihre Vorteile. Diese liegen vor allem in der hohen Verarbeitungsgeschwindigkeit, so daß auch große Datenmengen in relativ kurzer Zeit ver- und entschlüsselt werden können. Die zuvor geschilderte Problematik umgeht man durch die Kombination mit asymmetrischen Verfahren.[41]

Asymmetrische Verfahren umgehen das Problem des Schlüsseltauschs, indem zur Ver- und Entschlüsselung von Daten unterschiedliche Schlüssel eingesetzt werden. Diese Ungleichheit ist jedoch von einem Algorithmus künstlich hervorgerufen, und beide Schlüssel werden von einer ähnlichen mathematischen Funktion erzeugt. Daher ist es theoretisch möglich, von dem einen auf den anderen Schlüssel zu schließen. Da die Sicherheit des gesamten Systems genau auf diesem Punkt beruht, wird dieser Schluß durch den Einsatz von komplexen mathematischen Funktionen verhindert. Das be-

39 Vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 197. Für eine Übersicht der gängigsten Kryptoalgorithmen vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 181, und Schäfer, Günter: Netzsicherheit – Algorithmische Grundlagen und Protokolle, a. a. O., S. 30.

40 Für die Beschreibung der Funktionsweise des DES-Algorithmus vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 183 ff. Ausführlicher vgl. Schäfer, Günter: Netzsicherheit – Algorithmische Grundlagen und Protokolle, a. a. O., S. 39 ff.

41 Vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 156 f. und 161 f., vgl. auch Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, Braunschweig; Wiesbaden: Vieweg Verlag 2002, S. 6 f.

kannteste asymmetrische Verfahren ist das RSA-Verfahren.[42] Dieses nutzt zur Schlüsselerzeugung das mathematische Problem, große Zahlen zu faktorisieren.[43] Ein solches Schlüsselpaar besteht aus einem öffentlichen und einem privaten Schlüssel. Während der öffentliche Schlüssel den Kommunikationsteilnehmern zur Verfügung gestellt wird, bleibt der private Schlüssel geheim. Diese Verfahren werden demnach auch als Public-Key-Verfahren bezeichnet.

Wird nun eine Nachricht mit dem frei zugänglichen, öffentlichen Schlüssel des Empfängers verschlüsselt, ist diese nur mit dessen privatem Schlüssel zu entschlüsseln. Dadurch ist sichergestellt, daß nur dem Empfänger Zugang zu den übermittelten Informationen gewährt wird. Neben der sicheren Verschlüsselung von Daten kann durch den Einsatz von asymmetrischen Verfahren auch die Anwendung der digitalen Signatur realisiert werden. Diese sichert neben der Datenintegrität vor allem die Authentizität von Sender und Empfänger und ist damit das elektronische Äquivalent zur eigenhändigen Unterschrift.[44]

Um ein Dokument zu signieren, berechnet der Sender eine digitale Prüfsumme, den sogenannten Hash-Wert, des zu signierenden Dokuments.[45] Diese wird dann mit seinem privaten Schlüssel chiffriert. Der verschlüsselte Hash-Wert bildet die digitale Signatur und wird an das Dokument angehangen und mit diesem übertragen. Um nun die Identität des Senders sowie die Integrität des Dokuments sicherzustellen, wird die digitale Signatur zunächst mit Hilfe des öffentlichen Schlüssels des Absenders vom Empfänger entschlüsselt. Zusätzlich berechnet der Empfänger ebenfalls den Hash-Wert des übertragenden Dokuments und vergleicht die beiden Werte. Stimmen diese überein, kann sichergestellt werden, daß das Dokument auf dem Weg nicht verändert wurde. Ansonsten hätte sich auch die Prüfsumme verändert. Durch die erfolgreiche Entschlüsselung mit dem öffentlichen Schlüssel des Absenders ist zudem gewährleistet, daß einzig und allein dessen Besitzer Unterzeichner des Dokumentes sein kann.[46]

---

42 Dieses Verfahren ist nach seinen Erfindern Rivest, Shamir und Adleman benannt.

43 Für die Beschreibung der Funktionsweise des RSA-Verfahrens vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 158 ff., auch Schäfer, Günter: Netzsicherheit – Algorithmische Grundlagen und Protokolle, a. a. O., S. 71 ff., und Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 191 ff.

44 Die Rechtsgültigkeit digitaler Signaturen ist im Gesetz zur digitalen Signatur festgelegt, vgl. dazu Artikel 3, § 1, Absatz 2 des Informations- und Kommunikationsdienst-Gesetz.

45 Das „Hashing“ wird von sog. Digest-Algorithmen übernommen. Der Secure Hash Algorithm (SHA) ist eines der gängigsten Verfahren. Für eine genaue Spezifikation und Funktionsweise vgl. Burrows, James H.: Federal Information Processing Standards Publication 180-1 - Secure Hash Standard, Online im Internet: http://www.itl.nist.gov/fipspubs/fip180-1.htm, 17.04.1995.

46 Zur Funktionsweise digitaler Signaturen vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 164 ff.

An dieser Stelle drängt sich unweigerlich die Frage auf, wie sichergestellt werden kann, daß ein Schlüssel auch wirklich einer Person zuzuordnen ist. Alle bisher dargelegten Sicherheitsvorkehrungen, wie das Verschlüsseln und Signieren von Daten, sind ohne eine eindeutige Zuordnung von Personen oder Instanzen zu Schlüsseln geradezu wertlos. Was bringt die sicherste Verschlüsselung und die beste Signatur, wenn nicht sichergestellt werden kann, daß dieser Schlüssel auch wirklich dem gewünschten Kommunikationspartner gehört? So könnte ein Unbekannter sich als der gewünschte Partner ausgeben und dem Sender „seinen" öffentlichen Schlüssel zukommen lassen. Die Folgen wären fatal. Diese Problematik wird durch Zertifikate im Rahmen einer Public-Key-Infrastruktur gelöst.

2.4.2 Zertifikate und Public-Key-Infrastruktur

Zertifikate übernehmen in der digitalen Welt die Aufgabe von amtlichen Dokumenten. Bezogen auf das Problem der Zuordnung von Schlüsseln zu Personen oder Instanzen, bedeutet dies, daß eine Stelle die Echtheit eines öffentlichen Schlüssels bestätigt. Dazu wird der öffentliche Schlüssel zusammen mit weiteren persönlichen Daten einer Person von der ausstellenden Stelle geprüft und anschließend signiert.[47] Die ausstellende Stelle wird Zertifizierungsinstanz bzw. Certificate Authority (CA) genannt und der von dieser Stelle signierte, öffentliche Schlüssel mit dazugehöriger digitaler Signatur und den zusätzlichen Parametern wird als Zertifikat bezeichnet.[48]

Als Standard für Zertifikate hat sich der in Abbildung 4 dargestellte X.509-Standard durchgesetzt. Dieser Standard liegt im Moment in der dritten Version vor und legt genau fest, welche Informationen das Zertifikat in welcher Form enthalten muß und darf. Dieses Format ist auch in dem Public Key Cryptography Standard (PKCS)[49] enthalten und bildet somit auch die Grundlage für viele Anwendungen für digitale Signaturen. Die bekanntesten sind die Internetschutzmechanismen Secure Socket Layer (SSL), Privacy Enhanced Mail (PEM) und Secure Multipurpose Mail Extensions (S/MIME).

47 Da die Vertrauenswürdigkeit eines Zertifikates unter anderem davon abhängt, wie aufwendig eine solche Prüfung ausfällt, werden Zertifikate in unterschiedliche (Güte-)Klassen eingeteilt. Dies wirkt sich selbstverständlich auch auf die Kosten für ein Zertifikat aus. Vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 183 f.

48 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, a. a. O., S. 21 und Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 232.

49 Für eine kurze Übersicht der einzelnen Teile von PKCS, vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 171 f.

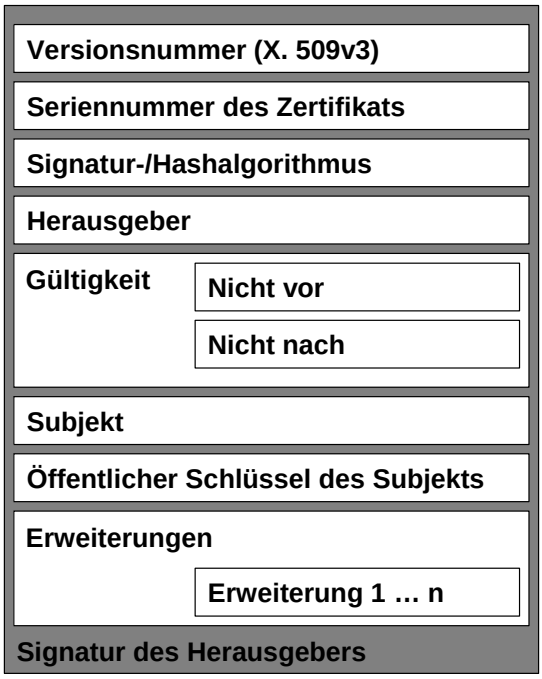

Abb. 4: Aufbau eines X.509-Zertifikats[50]

Die wichtigsten Informationen, die ein Zertifikat enthalten muß, sind der Name und der öffentliche Schlüssel des Besitzers sowie Angaben bezüglich der Zertifizierungsstelle (CA). Dabei sind die Namen des Subjekts und des Herausgebers gemäß den Vorgaben des X.500 Standards formuliert. Damit soll eine weltweit einheitliche Verzeichnisstruktur sichergestellt werden. Neben der Versionsnummer enthält jedes Zertifikat eine für jede CA eindeutige Seriennummer, so daß durch die Kombination aus Herausgeber und Seriennummer jedes Zertifikat eindeutig bestimmt werden kann. Damit es möglich ist, die Signatur zu verifizieren, ist der verwendete Signatur- und Hash-Algorithmus in dem Zertifikat vermerkt. Eine weitere zentrale Information ist der Gültigkeitszeitraum des Zertifikates. Zudem sieht der X.509v3 Standard zahlreiche Erweiterungen für optionale Felder vor. Dadurch ist es möglich, weitere Angaben zum Verwendungszweck zu machen oder mehrere öffentliche Schlüssel in einem Zertifikat unterzubringen und diese auch von unterschiedlichen Zertifizierungsstellen unterschreiben zu lassen.[51]

Grundsätzlich kann jeder Zertifikate ausstellen und anbieten. Dies hat allerdings zur Folge, daß keine Anhaltspunkte für die Vertrauenswürdigkeit der einzelnen Aussteller vorhanden sind. Aus diesem Grund werden Zertifikate in der Regel in hierarchischen

50 Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, a. a. O., S. 22.

51 Vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 170 f., Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, a. a. O., S. 21 ff.

Public-Key-Infrastrukturen organisiert.[52] Die Infrastruktur besteht aus einer Wurzelinstanz an der Spitze, den untergeordneten CA und darunter den einzelnen Benutzern. Das Prinzip ist einfach: Die Zertifikate der untergeordneten Instanzen werden jeweils mit dem privaten Schlüssel der übergeordneten Instanzen signiert und dadurch als vertrauenswürdig erklärt. Durch den jeweiligen Verweis in den Zertifikaten kann bei der Gültigkeitsprüfung die vollständige Kette durchlaufen werden. Der Wurzelinstanz kommt damit eine besondere Rolle zu. Da diese an der Spitze der Hierarchie steht, signiert sie ihr eigenes Zertifikat selbst und bildet somit den Vertrauensanker in dem hierarchischen Modell. Es ist daher nicht verwunderlich, daß diese Aufgaben meist von staatlichen Behörden oder großen Zertifizierern übernommen werden.[53] Die Zertifikate der Roots sind meistens in den Web-Browsern integriert, so daß diese dem Benutzer automatisch als vertrauenswürdig angeboten werden.[54]

Zu den Aufgaben der CA gehört neben dem Ausstellen und Signieren von Zertifikaten vor allem die Publikation von öffentlichen Schlüsseln und die Verwaltung von Sperrlisten für ungültige Zertifikate. Die Publikation erfolgt meist durch ein frei zugängliches Web-Verzeichnis, so daß der Prüfer einer signierten Nachricht den zugehörigen signierten öffentlichen Schlüssel via Internet anfordern kann. In diesem Zusammenhang wird häufig auch der Begriff des Trust Centers anstatt CA verwendet.[55]

Die sogenannten „schwarzen Listen“ werden von den CA geführt und enthalten ungültige Zertifikate. Denn trotz aller Sicherheitsvorkehrungen gibt es immer wieder Fälle, in denen der private Schlüssel abhanden kommt oder auf sonstigem Wege in falsche Hände gerät. In diesem Moment muß eine Möglichkeit geschaffen werden, den Verlust in möglichst kurzer Zeit allen Teilnehmern mitzuteilen. Zu diesem Zweck führt jede CA sogenannte Certificate Revocation Lists (CRL), in denen die Serienummer des Zertifikats zusammen mit einem Zeitstempel und weiteren Informationen eingetragen werden. Diese werden anschließend von der CA signiert und den Teilnehmern zur Verfügung gestellt. Allerdings garantiert die Existenz einer CRL keine maximale Sicherheit. Dafür ist hauptsächlich die teilweise recht lange Zeit verantwortlich, die von dem Bekannt-

52 Grundsätzlich sind auch andere Strukturen denkbar. Vgl. dazu Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 172 f.

53 So wird beispielsweise das Wurzelzertifikat für Signaturen gemäß dem Signaturgesetz der Bundesrepublik Deutschland von der Regulierungsbehörde für Telekommunikation und Post verwaltet. Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, a. a. O., S. 25.

54 Zu dieser Problematik vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, a. a. O., S. 24.

55 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, a. a. O., S. 23 ff. Zum Ablauf einer solchen Prüfung vgl. und Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 233 f. und Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 174.

werden eines Vorfalls, bis zum Abruf der aktualisierten CRL durch die Teilnehmer verstreicht. Da dem Angreifer dadurch unter Umständen genügend Zeit zur Verfügung gestellt wird, weiteren Schaden anzurichten, wird bereits an alternativen Verfahren gearbeitet.[56]

Ist in den vorangegangenen Kapiteln bereits die technische Eignung von Smart Cards als Schlüsselträger erläutert worden, soll nun kurz auf die organisatorischen Aspekte einer Smart Card innerhalb einer PKI eingegangen werden. Grundsätzlich wird die Smart Card nach Herstellung von der zuständigen CA personalisiert, d. h. die persönlichen Daten des Karteninhabers werden auf die Karte gespielt und das Schlüsselpaar generiert.[57] Anschließend wird der öffentliche Schlüssel von der CA signiert, im öffentlichen Verzeichnis des Trust Centers als gültiges Zertifikat geführt und somit den Teilnehmern zur Verfügung gestellt. Dieser ganze Prozeß kann dabei auch alternativ von einem beauftragten Trust Center durchgeführt werden. Die Ausgabe der personalisierten Smart Card erfolgt meist durch eine persönliche Übergabe. Dabei muß in der Regel ein Personalausweis vorgelegt und der Empfang persönlich quittiert werden. Je nach System erhält der Empfänger die Karte zusammen mit dem PIN-Brief in einem versiegelten Umschlag. Der Umschlag beinhaltet meist die Start-PIN, den Personal Unblocking Key (PUK) und einen Sperrcode.[58] Ausgestattet mit diesen Informationen, ist der Inhaber nun in der Lage, die Karte innerhalb einer PKI einzusetzen.

Eingebettet in eine solche Umgebung, ergeben sich für Smart Cards eine Reihe von interessanten Anwendungsmöglichkeiten. Im folgenden Abschnitt sollen die wichtigsten sicherheitsrelevanten Anwendungen von Smart Cards dargestellt werden.

2.4.3 Verschlüsseln, signieren und authentisieren mit Smart Cards

Die Anwendung von Smart Cards als Identifikations- und Sicherheitsmedien dient in erster Linie der sicheren Umsetzung der bekannten kryptogaphischen Ziele. Durch die technischen Eigenschaften der Smart Card und der organisatorischen Integration in eine PKI wird der Kreis geschlossen, der für eine lückenlose Implementierung von sicherheitskritischen Anwendungen vorausgesetzt wird.

56 Vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, a. a. O., S. 25 ff., Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 175 ff.

57 Zu den Möglichkeiten der Schlüsselgenerierung für Smart Cards, vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 838 ff.

58 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 836.

Eine erste interessante Anwendung ist der Austausch von sensitiven Informationen, bei dem zum einen die Geheimhaltung und zum anderen und Authentizität von Sender und Empfänger sichergestellt werden muß. Hier findet die digitale Signatur Anwendung, dessen genereller Ablauf bereits in Kapitel 2.4.1 dargelegt wurde. Im Folgenden soll daher vor allem auf die Rolle der Smart Card in diesem Prozeß eingegangen werden. Abbildung 5 zeigt die grundsätzlichen Abläufe beim Signieren und Verifizieren bei der Anwendung „digitale Signatur“ innerhalb einer PKI.

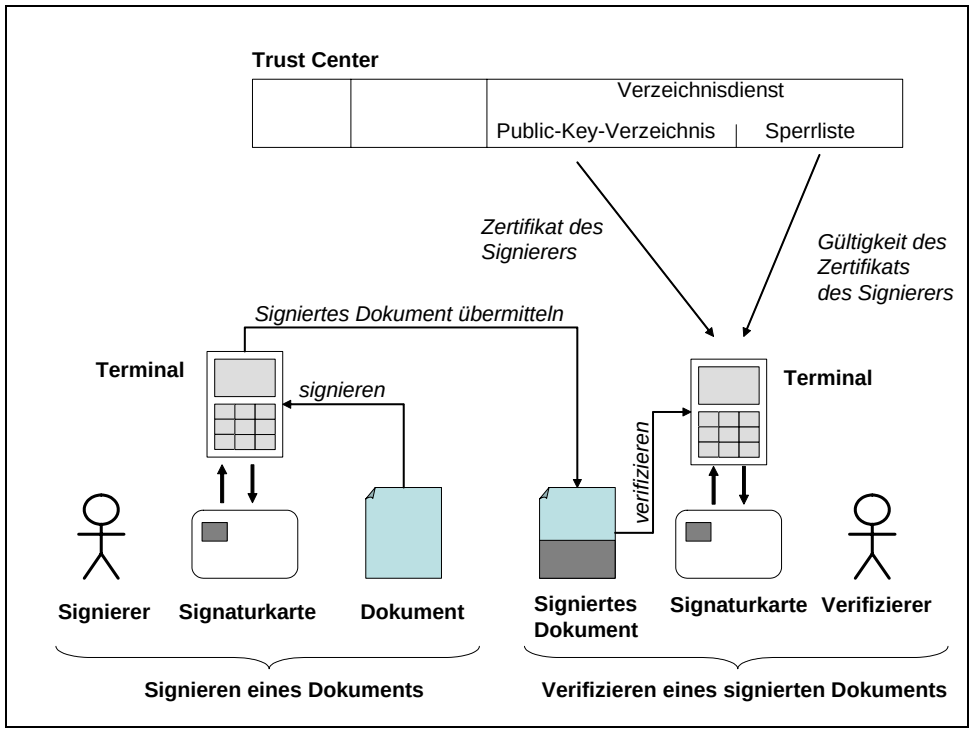

Abb. 5: Grundlegender Ablauf der Anwendung digitaler Signatur[59]

Beim Signieren eines Dokuments wird auf bekannte kryptographische Verfahren zurückgegriffen. Von dem Dokument wird ein Hash-Wert gebildet und mit dem privaten Schlüssel des Signierers verschlüsselt. Dabei unterscheidet man zwei Verfahren. Bei der „digital signature with appendix“ wird die digitale Signatur lediglich der Nachricht angefügt. Dadurch wird die zu übermittelnde Datenmenge um die angehangene Signatur erweitert und das Dokument ist auch lesbar, wenn die Signatur nicht geprüft wird. Die zweite Methode umgeht diese Problematik, indem sie die Signatur mit der Nachricht verbindet. Dadurch wird die Datenmenge nicht erhöht und das Dokument zudem verschlüsselt und ist damit erst nach Prüfung der Signatur lesbar. Diese Methode nennt man treffend „digital signature with message recovery“.[60] Unabhängig davon in welcher

59 In Anlehnung an Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 836.

60 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 229 ff.

Form das Dokument signiert wird, ist es zudem möglich, das Dokument zusätzlich noch durch eine Verschlüsselung vor unerlaubter Einsicht zu schützen. Dazu wird das Dokument anschließend mit dem öffentlichen Schlüssel des Verifizierers bzw. des Empfängers verschlüsselt.

In jedem Fall muß sich der Karteninhaber zuerst als solcher identifizieren. Dies geschieht in den meisten Fällen durch die Eingabe der PIN am Terminal. Im Erfolgsfall erstellt die Smart Card die digitale Signatur mit Hilfe des gespeicherten privaten Schlüssels. Welche Funktionen dabei die Smart Card übernimmt und welche vom Terminal (PC) durchgeführt werden, muß im Systemdesign erörtert und festgelegt werden. Das Design bezieht sich vor allem auf die Frage, ob die Smart Card lediglich einen extern generierten Hash-Wert verschlüsselt oder diesen auch selbst erstellt. Dazu müßte das gesamte Dokument an die Karte gesendet werden, was je nach Größe des Dokuments und Leistungsfähigkeit der Smart Card zu erheblichen Performance-Problemen führen kann. Grundsätzlich kann alles außer der Ver- und Entschlüsselung mit dem privaten Schlüssel auch außerhalb der Karte erledigt werden.[61]

Das digital signierte und/oder verschlüsselte Dokument kann nun auf beliebigem Wege versandt werden. Um die Authentizität der Nachricht und des Senders zu prüfen, muß zunächst die digitale Signatur entschlüsselt werden. Da das Dechiffrieren nur mit dem öffentlichen Schlüssels des Signierers möglich ist, kann dieser im Bedarfsfall beim Trust Center angefragt werden. Dabei ist es durch eine Prüfung der Sperrliste (CRL) zudem möglich, die Gültigkeit des Zertifikats zu kontrollieren. Danach erfolgt die Prüfung in bekannter Weise, indem von der Nachricht wiederum ein Hash-Wert ermittelt und dieser Wert mit der entschlüsselten Signatur vergleichen wird.[62] Die Smart Card des Empfängers kommt dabei nur im Falle einer zusätzlichen Verschlüsselung des Dokuments zum Einsatz. In diesem Fall muß das gesamte Dokument vor der Prüfung der Signatur erst mit dem privaten Schlüssels des Empfängers entschlüsselt werden. Da dies allerdings nur mit Hilfe seiner Smart Card möglich ist, muß sich auch der Empfänger zuerst eindeutig als Karteninhaber identifizieren.

Ein weiterer Anwendungsbereich ist die Authentisierung mit Smart Cards gegenüber einem Kommunikationspartner, bspw. einem (Web) Server. Dies ist für diejenigen Anwendungen interessant, in denen bestimmte Informationen nur einem eingeschränkten Personenkreis (den Karteninhabern) zur Verfügung gestellt werden oder diesem bestimmte Rechte gewährt werden sollen. Eine weitere Unterteilung der Rechte oder Zugriffsmöglichkeiten kann anhand der Kartennummer vorgenommen werden. Dabei

61 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 230 f.

62 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 836 f.

ist es demnach unbedingt erforderlich, die Karte auf ihre Echtheit hin zu überprüfen. Die Prüfung erfolgt in einer Smart-Card-Umgebung mittels eines abhörsicheren Kommunikationsprotokolls, welches immer auf dem sogenannten Challenge-Response-Mechanismus basiert. Im einfachsten Fall sendet der Server eine Datenstring (den Challenge) an die Karte. Dieser wird anschließend verschlüsselt an den Server zurückgesandt (Response). Der Server führt selbst eine solche Verschlüsselung durch und vergleicht beide Werte. Stimmen sie überein, so ist die Karte authentifiziert. Vorteil des Challenge-Response-Prinzips ist, daß sensitive Daten nicht unverschlüsselt an den Kommunikationsteilnehmer gesendet werden.[63] In der Anwendung von kontaktlosen Karten kommt diesem Aspekt eine besondere Beachtung zu.[64] Je nach verwendetem Algorithmus, den beteiligten Instanzen und dem Ablauf kann das Challenge-Response-Verfahren unterschiedlich ausgestaltet sein. Abbildung 6 gibt einen Überblick über die verschiedenen Ausprägungen von Authentisierungsverfahren im Umfeld von Smart Cards.

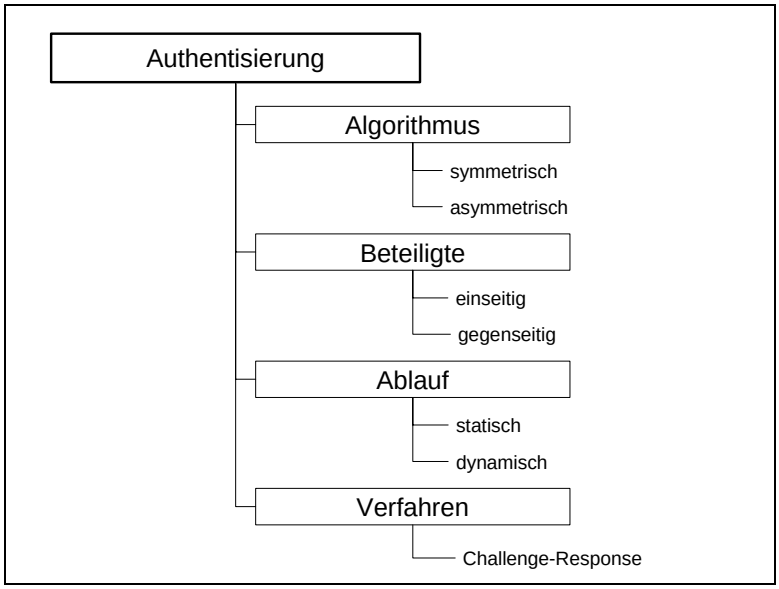

Abb. 6: Klassifizierungsbaum der Authentisierung[65]

Für die Authentisierung können sowohl symmetrische, als auch asymmetrische Verfahren zum Einsatz kommen. Dies bestimmt grundsätzlich die Art und Weise, wie der Challenge verschlüsselt und der Response entschlüsselt wird. Im Falle einer symmetri-

63 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 219 f., Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 197 f., Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, a. a. O., S. 19.

64 Vgl. Merz, Michael: E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, a. a. O., S. 193.

65 In Anlehnung an Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 220.

schen Authentisierung wird dazu jeweils der gleiche Schlüssel verwendet, während beim Einsatz von asymmetrischen Verfahren zum einen der private und zum anderen der öffentliche Schlüssel zum Einsatz kommt. An dieser Stelle sei nochmals an die Vor- und Nachteile von asymmetrischen Verfahren erinnert, die im Umfeld von Smart Cards eine Rolle spielen können. Hier muß ein Trade Off zwischen der erhöhten Sicherheit und der langsameren Ausführungsgeschwindigkeit stattfinden.[66] Dennoch bietet sich im Rahmen einer vorhandenen PKI der Einsatz von asymmetrischen Algorithmen an. Dabei werden diese häufig dazu eingesetzt, um einen symmetrischen Schlüssel auszutauschen, der im Anschluß zum Aufbau einer SSL-Verbindung gebraucht wird.[67] Damit ergänzen sich die Vor- und Nachteile der jeweiligen Algorithmen. Eine weitere Einteilung kann anhand der beteiligten Instanzen getroffen werden. War bis jetzt lediglich von der Authentisierung der Smart Card gegenüber einem Host die Rede, sind durchaus Anwendungen denkbar, in denen auch die Echtheit des Servers sichergestellt werden muß. Während bei der einseitigen Authentisierung nur jeweils die Authentizität eines Kommunikationspartners sichergestellt ist, ist bei der gegenseitigen Authentisierung am Ende die Echtheit beider bestätigt. Die Unterscheidung in statische und dynamische Verfahren zielt auf die Art des für den Challenge verwendeten Datenstrings ab. Bei einem statischen Ablauf wird immer der gleiche Datensatz für die Anfrage verwendet, z. B. die Kartennummer. Dies birgt jedoch die Gefahr, daß ein Angriff durch das Wiedereinspielen früherer Daten möglich wäre. Dynamische Verfahren hingegen verwenden für jede Anfrage andere Daten. Dazu werden meist Zufallszahlen generiert.[68] Welche Authentisierung letztendlich zum Einsatz kommt, hängt neben der Leistungsfähigkeit der Smart Cards vor allem vom gewünschten Sicherheitsniveau ab.

Im Folgenden soll nun kurz der Ablauf einer dynamischen, asymmetrischen Authentisierung erläutert werden, wie sie bspw. im Rahmen einer PKI eingesetzt werden kann. Zur Vereinfachung ist in Abbildung 7 lediglich die einseitige Authentisierung dargestellt.

Grundsätzlich folgt der Ablauf der symmetrischen Authentisierung, mit dem Unterschied, daß hier unterschiedliche Schlüssel zum Einsatz kommen. Der Server bzw. das Terminal sendet eine Zufallszahl an die Smart Card. Die Karte verschlüsselt diese mit dem privaten Schlüssel und sendet sie wieder zurück an den Server. Der Server entschlüsselt die chiffrierte Zufallszahl mit dem öffentlichen Schlüssel der Karte, bzw. des Benutzers, und vergleicht das Ergebnis mit der Ausgangszahl. Stimmen die Werte über-

66 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 220.

67 Zu der Beschreibung eines solchen SSL-Handshakes vgl. Schwenk, Jörg: Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, a. a. O., S. 92 ff.

68 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 219.

ein, ist die Karte authentifiziert.[69] Zur Prüfung der Gültigkeit und Authentizität des öffentlichen Schlüssels kann im Rahmen einer PKI das Zertifikat bei dem Trust Center angefragt und damit dessen Gültigkeit überprüft werden. Eine zweiseitige Authentisierung funktioniert im Grunde analog zu der einseitigen. Aber anstatt zwei Authentisierungen nacheinander durchzuführen, werden Verfahren verwendet, bei dem die beiden Schritte miteinander verflochten sind.[70]

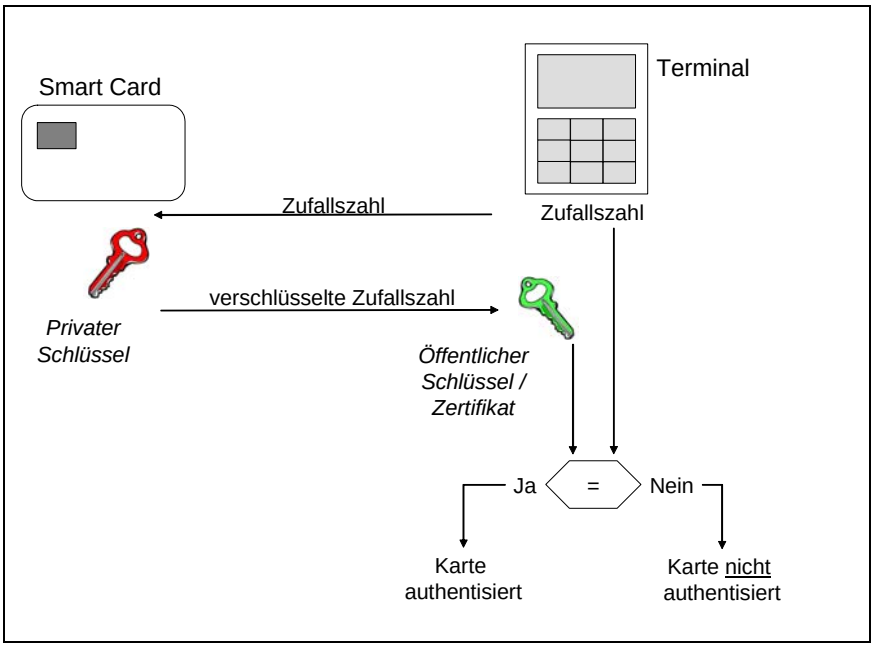

Abb. 7: Prinzip einer einseitigen, dynamischen und asymmetrischen Authentisierung einer Chipkarte durch das Terminal[71]

3 Situation am Fachbereich 02

3.1 Überblick über den Fachbereich

Der Betrachtungsgegenstand der Situationsanalyse ist der Fachbereich 02 (Wirtschaftswissenschaften) der Justus-Liebig-Universität Gießen. Wie in der folgenden Abbildung zu erkennen, folgt der Aufbau grundsätzlich einer für den Hochschulbetrieb charakteristischen dezentralen Organisationsform.

69 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 228.

70 Vgl. Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 223.

71 In Anlehnung an Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten – Aufbau – Funktionsweise – Einsatz von Smart Cards, a. a. O., S. 228.

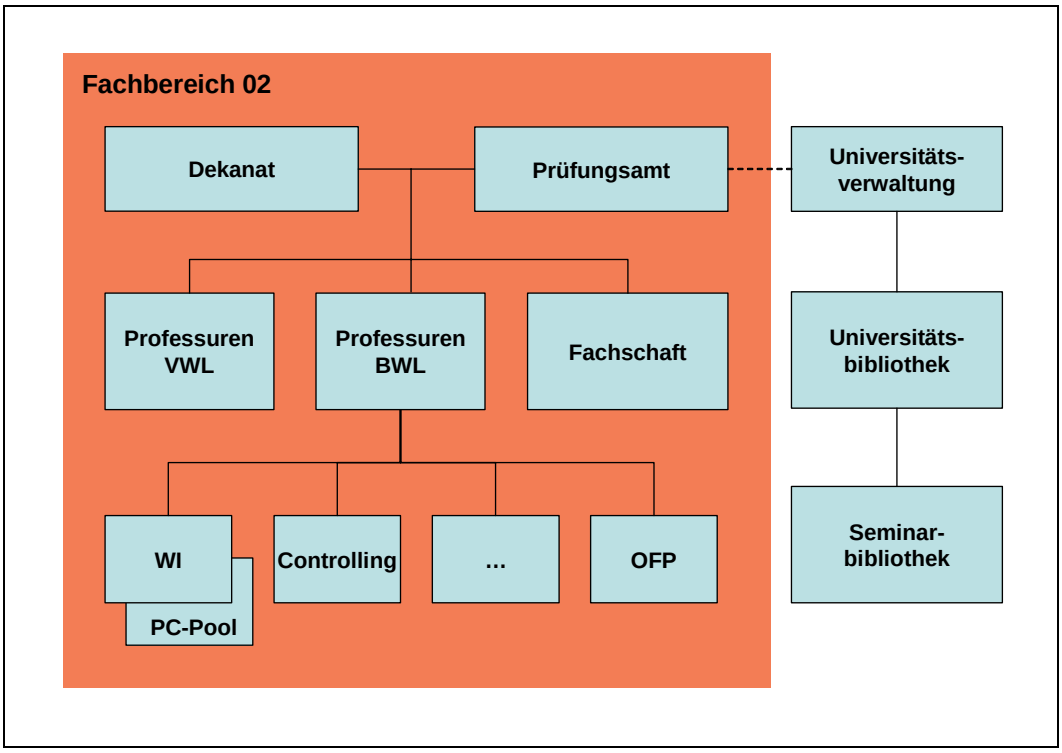

Abb. 8: Grundstruktur des Fachbereichs 02

Zentrale Steuerungseinheit bildet das Dekanat, welches neben der Koordinationsfunktion auch mit fachbereichsübergreifenden Aufgaben betraut ist. Das Dekanat stellt somit auch die organisatorische Verbindung zur Universitätsverwaltung her. Eine zweite stabsähnliche Stelle ist das Prüfungsamt, das zwar der zentralen Verwaltung der Universität untergliedert und damit weisungsgebunden ist, aber operativ aus dem Fachbereich gesteuert wird. Zentrale Aufgaben sind die Koordinierung der Prüfungen und die Verwaltung der Prüfungsergebnisse. Neben den zentralen Einrichtungen besteht der Fachbereich im Wesentlichen aus teilautonomen Organisationseinheiten. Die größte Gruppe bilden hier die Professuren. Derzeit (März 2004) finden sich am Fachbereich neun betriebswirtschaftliche und sieben volkswirtschaftliche Professuren. Des weiteren existieren am Fachbereich neben dem PC-Pool noch die studentischen Organisationen, z. B. die Fachschaft. Die Seminarbibliothek gehört organisatorisch nicht zum Fachbereich. Sie untersteht durch den Anschluß an die Universitätsbibliothek der zentralen Universitätsverwaltung, soll aber an dieser Stelle nicht zuletzt durch die räumliche und fachliche Nähe zum Fachbereich dennoch erwähnt werden.

Der gesamte Web-Auftritt des Fachbereichs wird durch das Web Portal System realisiert. Das WPS ist im Grunde ein dezentrales Web Content Management System (WCMS), welches den einzelnen Organisationseinheiten ermöglicht, Dokumente und Informationen einfach und ohne HTML-Kenntnisse online bereitzustellen. Als zentrale Anlaufstelle bietet das WPS ein Portal, das alle Web Sites navigatorisch integriert.

Im Folgenden sollen zunächst die wichtigsten Organisationseinheiten näher beschrieben werden. Dabei liegt ein besonderes Augenmerk auf den sicherheits- und authentifizierungskritischen Aufgaben und den derzeit vorherrschenden Lösungen. Ziel ist es, sicherheitsrelevante Problembereiche aufzudecken, die anschließend als Ansatzpunkte für Smart-Card-Anwendungen dienen können.

3.2 Organisatorisches Umfeld

3.2.1 Beteiligte Organisationseinheiten

3.2.1.1 Professuren und Dekanat

Grundsätzlich bestehen die Professuren aus einem Lehrstuhlinhaber (Professor), einem Sekretariat, den wissenschaftlichen Mitarbeitern sowie studentischen Hilfskräften. Der Aufgabenbereich der Professuren umfaßt im Wesentlichen Forschung und Lehre. Gerade der Bereich der Lehre macht die Professuren zu den größten Informationsanbietern im Umfeld des Fachbereichs. Zu den Informationen gehören neben den allgemeinen Angaben über Fachgebiet, Mitarbeiter, Adresse etc. vor allem Informationen zu den angebotenen Lehrveranstaltungen. Dazu zählen zum einen organisatorische Angaben, wie bspw. Zeit und Ort und zum anderen die bereitgestellten Lehrmaterialien. Da manche Lehrveranstaltungen, z. B. Seminare oder Übungen nur von einer begrenzten Teilnehmerzahl besucht werden können, sind für diese Veranstaltungen gesonderte Anmeldungen durch die Professuren durchzuführen. Mit in den Bereich der Lehre fällt auch die Durchführung von Prüfungen und die anschließende Veröffentlichung der Prüfungsergebnisse. Des weiteren führen die meisten Professuren Evaluationen ihrer Lehrveranstaltungen durch und stellen Diskussionsforen zur Verfügung. Im Bereich der Forschung treten die Professuren vor allem als Anbieter von Arbeitspapieren und Forschungsergebnissen auf.

Realisiert werden alle Funktionalitäten und Aufgaben fast ausschließlich durch den Einsatz des Web Portal Systems.[72] Daher fällt die Administration des Web Portal Systems mit in den Aufgabenbereich der Professuren, bzw. dessen Mitarbeiter. Das WPS stellt zum Schutz im Grunde zwei Sicherungsmechanismen zur Verfügung. Zum einen besteht die Möglichkeit, den Zugriff auf bestimmte Bereiche oder Informationen durch eine Benutzername/Paßwort-Kombination zu schützen und zum anderen den Zugriff nur durch den Internet-Protocol-(IP)-Bereich der Universität zu erlauben. Diese Optionen bestehen auch zur Zugriffskontrolle auf die Online-Evaluationen und die Diskussionsforen. Die Probleme und Unzulänglichkeiten dieser Sicherheitslösungen sollen in Kapitel 3.3.2.3 „Probleme und Unzulänglichkeiten bisheriger Sicherheitslösungen“ behandelt

72 Vgl. dazu Kapitel 3.3.2.1 Merkmale und Funktionsweise.

werden. Grundsätzlich lassen sich aber im Bereich der Professuren folgende sicherheits- und authentifizierungskritische Aufgaben festhalten:

- Durchführung von verbindlichen Anmeldungen (z. B. zu Seminaren)
- Veröffentlichung von Klausurergebnissen
- Veröffentlichung von sonstigen sensitiven Informationen (z. B. Skripte)
- Anbieten von fach- bzw. lehrveranstaltungsbezogenen Diskussionsforen
- Durchführung von Online-Evaluationen
- Veröffentlichung von Arbeitspapieren
- Administration des Web Portal Systems

Koordiniert werden die einzelnen Professuren durch das Dekanat. An dessen Spitze stehen der Dekan, der Prodekan und der Studiendekan. Darunter existieren zahlreiche Gremien und Ausschüsse für die unterschiedlichsten Aufgabenbereiche, die den Fachbereich als Ganzes betreffen. Ausgestattet mit dem WPS stehen dem Dekanat grundsätzlich die gleichen Funktionalitäten wie den Professuren zur Verfügung; das Dekanat hat aber im Gegensatz zu den Professuren weit weniger Kommunikationsbeziehungen zu den Studierenden. Die Rolle des Dekanats ist in diesem Zusammenhang die des Entscheidungsträgers.

3.2.1.2 Prüfungsamt

Das Prüfungsamt des Fachbereichs beschäftigt drei Mitarbeiter und sorgt im Wesentlichen für die Umsetzung der Prüfungsordnung. Wie eingangs bereits erwähnt, ist das Prüfungsamt zwar organisatorisch der Universitätsverwaltung untergliedert, wird aber operativ von Fachbereich gesteuert. Der Aufgabenbereich umfaßt zum einen die Beratung und zum anderen die Verwaltung. Letzterer bezieht sich dabei auf alle Prozesse von der Anmeldung zu Prüfungen[73] bis hin zur Verbuchung der Ergebnisse.

Dabei existiert derzeit (März 2004) noch keine Web-Lösung. Zwar ist das Prüfungsamt mit dem WPS ausgestattet, nimmt damit aber lediglich die Beratungsfunktion wahr. An- und Abmeldungen zu Prüfungen müssen von den Studierenden persönlich und vor Ort zu den angegebenen Terminen vorgenommen werden. Ebenso wie bei Umbuchungen, Anträgen oder sonstigen prüfungsrechtlichen Belangen erfolgt die gesamte Kommunikation dabei in Papierform. Dafür werden vom Prüfungsamt Formulare zur Verfügung gestellt, die von den Studierenden ausgefüllt werden. Da die Daten intern aber bereits

73 Unter Prüfungen sollen im folgenden alle Studienleistungen verstanden werden, die für den Abschluß des Studiums im Sinne der Diplomprüfungsordnung nötig sind. Dementsprechend auch Seminare, Diplomarbeiten, etc.

durch entsprechende Systeme[74] in elektronischer Form vorgehalten und verwaltet werden, müssen demnach die handschriftlich ausgefüllten Formulare in einem nächsten Schritt „per Hand“ in das System übertragen werden. Die Folgen solcher Medienbrüche sind neben dem erhöhten Arbeitsaufwand vor allem die hohe Fehlerwahrscheinlichkeit. Des weiteren kommt es während der Anmeldefristen durch den erhöhten Arbeitsaufwand immer wieder zu langen Wartezeiten am Prüfungsamt.

Ein weiterer Ansatzpunkt ist die Möglichkeit der Noteneinsicht für die Studierenden. Eine solche Übersicht über die geleisteten Prüfungen ist derzeit nur zu jeweils einem Termin am Ende des Semesters möglich und muß von den Studierenden gesondert beantragt werden. Es ist dementsprechend zur Zeit für die Studierenden nicht möglich, jederzeit eine Übersicht über die erbrachten Studienleistungen zu erhalten. Hauptproblemfelder beim Prüfungsamt ergeben sich somit in folgenden Bereichen:

- An- und Abmeldungen zu Prüfungen
- Noteneinsicht

3.2.1.3 Sonstige Organisationseinheiten

Die Fachschaft des Fachbereichs Wirtschaftswissenschaften vertritt als studentische Organisation vor allem die Interessen der Studierenden am Fachbereich. Dazu gehört neben der Mitarbeit in den Gremien und Ausschüssen des Fachbereichs die Beratung und Informationsversorgung der Studierenden. Auch die Fachschaft nimmt die meisten Aufgaben durch das WPS wahr. In diesem Zusammenhang ist unter anderem die Bereitstellung von alten Klausuren zu nennen. Diese sind zur Unterstützung der Prüfungsvorbereitung auf der Web Site der Fachschaft herunterzuladen. Um die Klausuren vor unerlaubten Zugriff zu schützen, sind diese lediglich aus dem IP-Bereich der Universität erhältlich. Das wirft dementsprechend einige Probleme auf.[75] Zudem stellt die Fachschaft, wie die Professuren auch, Diskussionsforen zur Verfügung. Im Fachschaftsforum wird Studierenden, Mitarbeitern und Externen die Möglichkeit gegeben, aktuelle Themen und Belange zu diskutieren. Dieser Kommunikationskanal hat sich in der Vergangenheit öfters als höchst problematisch herausgestellt. Das lag vor allem daran, daß durch unsachliche und zum Teil beleidigende Beiträge die Diskussion zerstört und nicht zuletzt dadurch das Image des Fachbereichs in Mitleidenschaft gezogen wurde. Mittlerweile werden die Beiträge durch Mitarbeiter der Fachschaft gesichtet und bei Bedarf gelöscht oder zensiert. Die Möglichkeit der eindeutigen Identifizierung der Teilnehmer durch die Smart Card könnte diesem Problem entgegenwirken.

74 Vgl. dazu Kapitel 3.3.4 Systeme des Prüfungsamts.

75 Vgl. dazu Kapitel 3.3.2.3 Probleme und Unzulänglichkeiten bisheriger Sicherheitslösungen.

Eine weitere Organisationseinheit, die im Smart-Card-Umfeld eine Rolle spielt, ist der PC-Pool des Fachbereichs. Organisatorisch der Abteilung IT-Service-Center (ITSeC) der Professur Wirtschaftsinformatik unterstellt, bietet er den Studierenden u. a. die Möglichkeit, Hausarbeiten am PC anzufertigen oder das Internet zur Recherche zu nutzen. Weiterhin wird der PC-Pool für Lehrveranstaltungen genutzt, die praktische PC-Übungen enthalten. Um den Studierenden Zugriff auf die bereitgestellten Rechner zu ermöglichen, können bei der betreuenden Professur Accounts beantragt werden. Grundsätzlich kann ein solcher Account zwar online via WPS beantragt werden, muß aber anschließend gegen Vorlage des Studentenausweises persönlich abgeholt und dessen Empfang quittiert werden. Dadurch ergeben sich für die Studierenden zusätzliche Wege und für die Mitarbeiter zusätzlicher Arbeitsaufwand.

Als weitere abgrenzbare Organisationseinheiten soll an dieser Stelle noch kurz auf die Studienschwerpunkte eingegangen werden. Die Studienschwerpunkte sind organisatorisch gesehen ein Zusammenschluß von mehreren Professuren, die zusammen Lehrveranstaltungen anbieten. Im Rahmen dieser Analyse, sind diese jedoch analog zu den Professuren zu behandeln.

3.2.2 Kommunikatoren

3.2.2.1 Studierende

Unter Studierenden sollen im Rahmen dieser Arbeit alle ordentlich Studierenden am Fachbereich Wirtschaftswissenschaften der JLU-Gießen verstanden werden, die mit der Uni-Chipkarte ausgestattet sind. Derzeit sind ca. 2000 Studierende in den Fächern BWL, VWL und Ökonomie eingeschrieben.[76] Daneben studieren am Fachbereich Wirtschaftswissenschaften noch zahlreiche Nebenfachstudenten, die lediglich ein begrenztes Veranstaltungsangebot wahrnehmen. Die Gruppe der Studierenden spielt in dem Umfeld der Smart-Card-Anwendungen eine zentrale Rolle. Denn zum einen sind sie die größte Gruppe von Smart-Card-Besitzern und gleichzeitig die größten Informationsnachfrager am Fachbereich. Diese Eigenschaften machen die Studierenden zu den Hauptkunden der abgebotenen Smart-Card-Anwendungen. Daher müssen bei der Konzeption gerade die Ziele der Studierenden berücksichtigt werden.

Grundsätzlich lassen sich die Ziele der Studierenden ohne repräsentative Umfrage nicht ohne weiteres analysieren. Trotzdem läßt sich nicht zuletzt aufgrund einschlägiger Forumsbeiträge ein grobes Meinungsbild formen. Das Kerninteresse der Studierenden liegt dabei vor allem in der Vermeidung von Wege- und Wartezeiten bei sämtlicher

76 Vgl. Pressestelle der Justus-Liebig-Universität Gießen: Die Universität in Zahlen, Online im Internet: http://www.uni-giessen.de/neu2/informationen/uni-zahlen.html, 05.03.2004.

Kommunikation. Online verfügbare Prüfungsanmeldungen, Noteneinsicht und Lehrmaterialien würden dementsprechend auf positive Resonanz stoßen. Dies betrifft vor allem die bisher noch nicht online verfügbaren Funktionalitäten, wie die gesamte Kommunikation mit dem Prüfungsamt. Erfahrungen von anderen Universitäten zeigen allerdings auch, daß von Seiten der Studierenden zum Teil starke Befürchtungen bezüglich des Datenschutzes bestehen.[77] Weiterhin darf nicht vergessen werden, daß die Akzeptanz solcher Anwendungen in erster Linie von dem gebotenen Nutzen für die Studierenden abhängt. Schließlich sind zur Nutzung der Angebote auch gewisse Investitionen nötig, z. B. für Chipkartenlesegeräte. Es ist davon auszugehen, daß die Studierenden solche Investitionen erst tätigen werden, wenn damit ein „echter" Zusatznutzen verbunden ist.

3.2.2.2 Mitarbeiter

Als Mitarbeiter sollen in diesem Zusammenhang vor allem die Angestellten der beteiligten Organisationseinheiten betrachtet werden. Dies sind bei den Professuren die Professoren, die Mitarbeiter des Sekretariats, die wissenschaftlichen Mitarbeiter sowie die studentischen Hilfskräfte. Grundsätzlich sind die Mitarbeiter nicht mit der Uni-Chipkarte ausgestattet. Eine Sonderposition nehmen an dieser Stelle die wissenschaftlichen Mitarbeiter ein, die gleichzeitig Studierende im Rahmen eines Promotionsstudiengangs sind. Sie sind, ebenso wie die studentischen Hilfskräfte auch, Träger des elektronischen Studentenausweises. Im Rahmen dieser Analyse soll dieser Umstand durchaus Beachtung finden, wenn auch durch das Fehlen von echten Mitarbeiterkarten ein ausschließlicher und flächendeckender Einsatz von Smart Cards nicht möglich ist.

Die Mitarbeiter der Professuren sorgen in erster Linie für die Erfüllung der anfallenden Aufgaben. In diesem Rahmen spielt vor allem die Pflege und Administration des WPS eine zentrale Rolle. So stellen die Mitarbeiter Informationen, Lehrmaterialien, Klausurergebnisse etc. ein und entscheiden darüber, ob und in welcher Form der Zugriff auf die Daten beschränkt wird. Dadurch liegt der Einsatz von Schutzmechanismen und Smart-Card-Anwendungen im Verantwortungsbereich der Mitarbeiter. Dabei muß das Angebot von Schutzmechanismen dem gewünschten Sicherheitsniveau genügen. Das Interesse an Smart-Card-Anwendungen dürfte in erster Linie davon abhängen, inwieweit die Unzulänglichkeiten bisheriger Lösungen dadurch überwunden werden. Dies gilt ebenso für die Mitarbeiter anderer Organisationseinheiten, die mit dem WPS ausgestattet sind.

77 Vgl. Papendick, Astrid: Studicard 2003, Online im Internet: http://www.uni-mainz.de/Organisationen/gruenlinx/unipress/chipkarte_UP330_dez02.html, 14.08.2003; auch Fachschaftsrat Informatik, TH Darmstadt (Hrsg.): Abgekartetes Spiel – Wie Chipkarten den Hochschulalltag verändern, Online im Internet: http://www.uni-mainz.de/Organisationen/gruenlinx/chips/Readerchipneu.pdf, 1996; auch Warner, Ansgar: Die Chipkarte kommt, in: sbz, Nr. 38/2001, S. 8-10.

Bei den Mitarbeitern des Prüfungsamts dürfte das Interesse weniger auf den verbesserten Sicherheitsfunktionalitäten des WPS liegen, da dieses System bis dato ausschließlich zur Beratung eingesetzt wird. Vielmehr sind die durch den Einsatz von Smart-Cards erst ermöglichten neuen Funktionalitäten von Interesse. Dies betrifft vor allem den bereits angesprochenen Problembereich der An- und Abmeldungen. Da es dabei infolge von Medienbrüchen immer wieder zu erhöhtem Arbeitsaufwand und Überlastungen der Mitarbeiter kommt, liegt in diesem Punkt mit Abstand das größte Verbesserungs-potential. Die Akzeptanz von Seiten des Prüfungsamts dürfte dementsprechend hoch sein.

3.2.2.3 Scientific Community

Zu dieser Personengruppe sollen alle wissenschaftlich aktiv forschenden Personen zusammengefaßt werden, die auf dieser Ebene mit dem Fachbereich in Beziehung stehen. Dies sind sowohl interne als auch fachbereichsexterne Forschende. An dieser Stelle soll vor allem auf die Externen eingegangen werden, da alle internen Forschenden gleichzeitig auch unter Studierende oder Mitarbeiter fallen.

Das Interesse liegt bei beiden Gruppen grundsätzlich in der Informationssammlung zu Forschungsaktivitäten, Arbeitspapieren und sonstiger Literaturrecherche, aber bei den Externen zudem auch in Informationen über eine mögliche Zusammenarbeit im Bereich der Forschung oder Lehre. Zu denken ist dabei an Lehrveranstaltungen und Seminare, die von Gastdozenten durchgeführt oder von Gästen besucht werden. An dieser Stelle ist insbesondere darauf zu achten, daß durch den Einsatz von Smart-Card-Anwendungen die Externen nicht ausgeklammert werden.

3.2.2.4 Gäste und Interessenten

Eine weitere Adressatengruppe, die im Umfeld des Fachbereichs Beachtung finden muß, besteht aus Gästen und sonstigen Interessenten. In dieser Gruppe sollen alle externen Stakeholder zusammengefaßt werden, die in beliebiger Beziehung zum Fachbereich stehen und nicht in die Scientific Community fallen. Dazu gehören unter anderen Unternehmen aus der privaten Wirtschaft, Abiturienten sowie Hochschulwechsler. Diese Gruppe ist selbstverständlich nicht mit der Uni-Chipkarte ausgestattet. Dennoch sind Gäste und Externe im weitesten Sinne als Kunden zu verstehen. So interessieren sich bspw. Abiturienten für das Lehrveranstaltungsangebot oder die lehrenden Professoren, Unternehmen für Lehrinhalte und mögliche Kooperationen, Hochschulwechsler für die Anerkennung ihrer Studienleistungen usw. Mögen die Ziele der Einzelnen noch so unterschiedlich sein, so muß bei dem Design von Smart-Card-Anwendungen vor allem eines berücksichtigt werden: Alle Bereiche und Informationen, die mit einer Smart Card

geschützt werden, sind für Externe nicht mehr verfügbar. Dementsprechend muß genau abgewogen werden, in welchen Bereichen Interessen von Externen bestehen.

3.2.3 Kommunikationsbeziehungen im organisatorischen Umfeld

Nachdem im vorhergehenden Kapitel die beteiligten Organisationseinheiten und Kommunikatoren beschrieben worden sind, soll nun speziell auf deren Kommunikationsbeziehungen eingegangen werden. Auf der Grundlage der zuvor aufgedeckten Ansatzpunkte für Smart-Card-Anwendungen zeigt Abbildung 9 übersichtsartig die wichtigsten Kommunikationsbeziehungen der Teilnehmer.

Wie in der Abbildung zu erkennen, nehmen die Studierenden eine zentrale Position im gesamten Kommunikationsgefüge des Fachbereichs ein. Die intensivste Beziehung besteht dabei zu den Professuren. Das liegt vor allem daran, daß der Austausch von Informationen nahezu über das gesamte Semester stattfindet. Dies betrifft vor allem den Bereich der allgemeinen Informationen und den der breitgestellten Lehrmaterialien. Weiterhin sind die Studierenden die Adressaten der veröffentlichten Prüfungsergebnisse, melden sich zu Veranstaltungen an den Professuren an, nehmen an Diskussionsforen teil und evaluieren am Ende des Semesters die besuchten Lehrveranstaltungen. Mit dem Prüfungsamt treten die Studierenden neben der allgemeinen Beratung vor allem bei den An- und Abmeldungen zu den Prüfungen und bei der Noteneinsicht in Kontakt. Um den PC-Pool des Fachbereichs nutzen zu können, muß von den Studierenden ein Account beantragt werden. Eine weitere Kommunikationsbeziehung besteht zu der Fachschaft, die die Studierenden mit Informationen versorgt und Diskussionsforen betreibt. Die Mitarbeiter übernehmen die Pflege und die Administration des WPS an den Professuren. Die Überlappung der Gruppe der Mitarbeiter und Studierenden kennzeichnet die in diesem Zusammenhang wichtige Schnittmenge bezüglich der Ausstattung mit der Uni-Chipkarte.[78]

Alle aufgezeigten Kommunikationsbeziehungen bieten daher Ansatzpunkte für Smart-Card-Anwendungen am Fachbereich Wirtschaftswissenschaften. Eine Ausnahme bilden hier die Beziehungen zu Gästen und Interessenten und der Scientific Community. Diese sind aber insofern von Interesse, daß die für Externe interessanten Bereiche nicht für den Einsatz von Smart Cards geeignet sind. Daher müssen sie in diesem Zusammenhang eine gesonderte Beachtung finden.

78 Vgl. dazu Kapitel 3.2.2.2 Mitarbeiter.

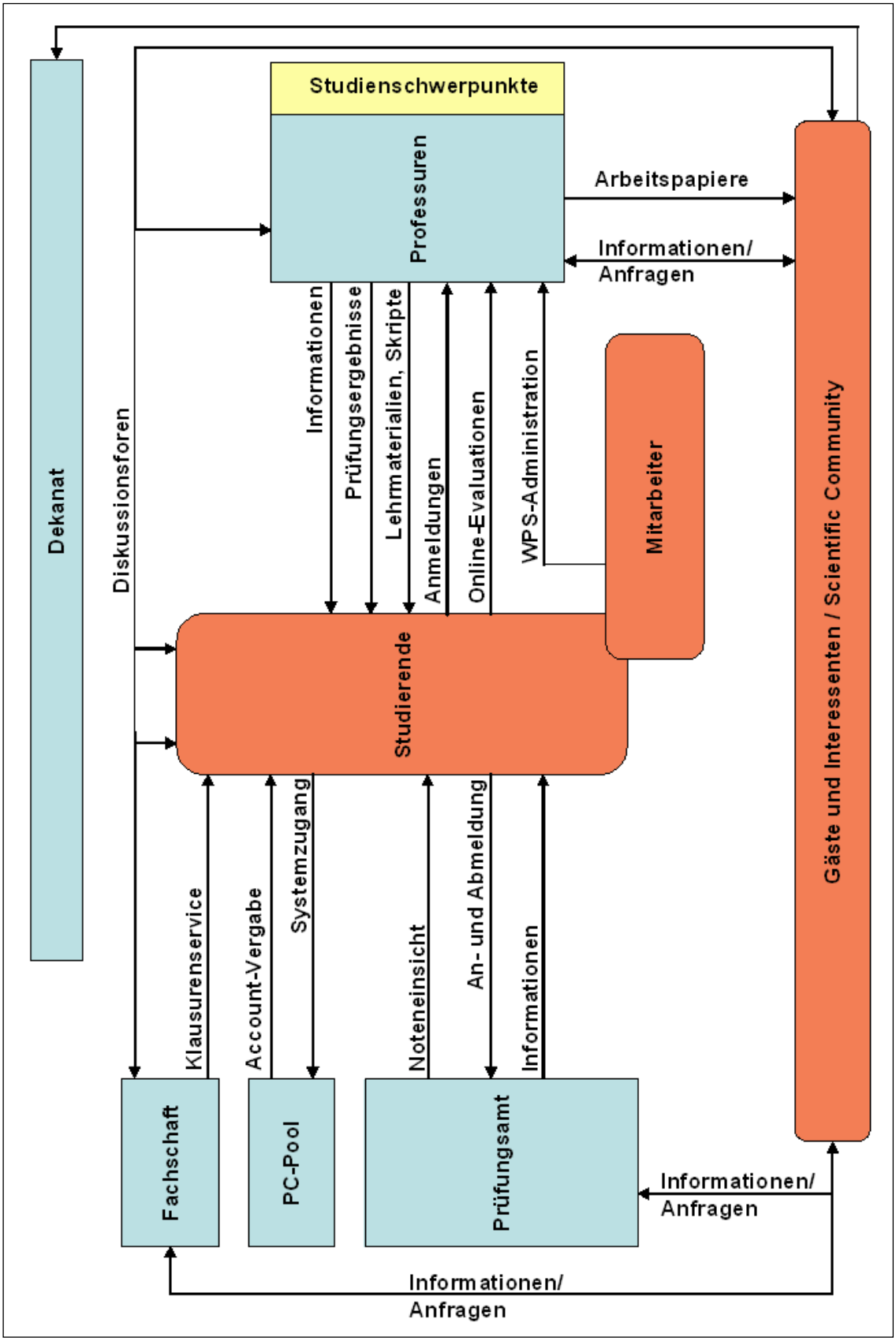

Abb. 9: Kommunikationsbeziehungen der Teilnehmer

3.3 Infrastrukturelle Grundlagen

3.3.1 Die Uni-Chipkarte der Universität Gießen

3.3.1.1 Aussehen und Inhalt

Seit dem Wintersemester 2002/2003 gibt die Justus-Liebig-Universität Gießen eine multifunktionale Chipkarte als Studentenausweis aus. Bei der bislang noch namenlosen Karte,[79] handelt es sich um eine Plastikkarte im ID-1 Format, die mit zwei unabhängigen Mikrochips ausgestattet ist. Diese auch als Twin-Karte bezeichnete Smart Card beinhaltet einen kontaktlosen Mifare-Chip und einen kontaktbehafteten Mikroprozessor mit Krypto-Koprozessor.[80]

Im Wesentlichen beherbergt die Karte drei Arten von Daten. Neben den in Abbildung 10 zu erkennenden optisch lesbaren Daten, beinhaltet der Mifare-Chip in erster Linie die Daten der elektronischen Geldbörse und der kontaktbehaftete Chip den kryptographischen Identitätsschlüssel (Private Key).

Abb. 10: Vorder- und Rückseite der Uni-Chipkarte der Justus-Liebig-Universität Gießen

Insgesamt beinhaltet die Uni-Chipkarte derzeit folgende Datensätze:

Optisch lesbare Ausweisdaten auf dem Kartenkörper

- Ausweistyp "Studienausweis"
- Ausweisnummer
- Vorname(n), Name, ggfs. Titel
- Lichtbild
- Logo des Rhein-Main-Verkehrsverbund (RMV) mit Zusatzangaben
- Gültigkeitsende
- Barcode der Ausweisnummer (Rückseite)

79 Vgl. Partosch, Günter: Informationen zur Chipkarte, Zum Namen der Chipkarte der Studierenden der JLU, Online im Internet: http://www.uni-giessen.de/chipkarte/name.html, 17.01.2003.

80 Vgl. Kapitel 2.2 Definitorische Abgrenzung des Begriffs Smart Card.

Daten im kontaktlosen Mifare-Chip

- Technische Prozessordaten (Betriebssystem, Prozessornummer)
- Elektronische Geldbörse
- Status "Studierender"
- Matrikel- und die Ausweisnummer
- Kartenfolgeziffer
- Beginn und Ende des Gültigkeitszeitraumes

Daten im kontaktbehafteten Mikrochip

- Technische Prozessordaten (Betriebssystem, Prozessornummer)
- Name und Ausweisnummer[81]
- Privater PKI-Schlüssel (nicht lesbar)
- Öffentlicher PKI-Schlüssel (Schlüsselzertifikat)
- Karten-PIN und -PUK in verschlüsselter Form[82]

Da sich das Interesse dieser Arbeit lediglich auf den kontaktbehafteten Mikrochip bezieht, soll dieser im Folgenden näher beschrieben werden. Grundsätzlich handelt es sich dabei um einen Mikroprozessor mit kryptographischem Koprozessor, der in der Lage ist, kryptographische Verfahren auszuführen. Des weiteren verfügt der kontaktbehaftete Chip über einen 32 Kilobyte (KB) großen Speicher, auf den unter Kontrolle des Betriebssystems (TCOS V2) zugegriffen werden kann. Hauptsächlich sind dort die kryptographischen Schlüssel hinterlegt. Das ist zum einen der öffentliche Schlüssel (Schlüsselzertifikat) und zum anderen der geheime Schlüssel. Letzterer ist „von außen“ nicht lesbar und wurde bei der Personalisierung innerhalb der Karte generiert und nur das Betriebsystem ist in der Lage, diesen Schlüssel für Vergleichsoperationen zu nutzen.[83] Das Schlüsselzertifikat befindet sich im Grunde nur zur Vereinfachung auf der Karte, schließlich ist dieser öffentliche Schlüssel im Verzeichnis der CA für alle Teilnehmer zugänglich.[84] Das Zertifikat hat dabei den gleichen Gültigkeitszeitraum wie der Studentenausweis und wird bei jeder ordnungsgemäßen Rückmeldung für das folgende Seme-

81 Die Ausweisnummer besteht dabei aus verschiedenen Elementen. Dadurch ist es möglich, bestimmte Informationen aus der Ausweisnummer zu entnehmen, z. B. die Matrikelnummer oder die Gruppenzugehörigkeit. Vgl. Partosch, Günter: Informationen zur Chipkarte, Chipkarten-Info -- Ausweisnummer, Online im Internet: http://www.uni-giessen.de/chipkarte/ausweisnummer.html, 23.09.2003.

82 Vgl. Fock, Falko: Informationen zur Chipkarte, Aussehen und Inhalt der JLU-Chipkarte, Online im Internet: http://www.uni-giessen.de/chipkarte/beschreibung.html, 29.10.2002.

83 Vgl. Partosch, Günter: Informationen zur Chipkarte, Information zu den Mikrochip-Prozessoren, Online im Internet: http://www.uni-giessen.de/chipkarte/mikroprozessoren.html, 17.01.2003.

84 Vgl. Kapitel 3.3.3 Die Zertifizierungsinstanz der Universität Gießen.

ster automatisch verlängert.[85] Um die Karte vor unerlaubtem Zugriff zu schützen, sind alle Anwendungen der Chipkarte mit einer PIN gesichert. Dabei verfügt die Karte über einen Fehlversuchszähler, der die Karte bei zehnmaliger Falscheingabe sperrt. Die Karte kann in diesem Fall nur durch die Eingabe des PUK wieder freigeschaltet werden.[86]

Während der Mifare-Chip über die eingebaute Antenne Strom und Daten überträgt, ist der kontaktbehaftete Chip nur in Verbindung mit einem an den PC angeschlossenen Chipkartenleser nutzbar. Derzeit werden von der Universität die Chipkartenleser „KAAN Standard Plus“ von der Firma Kobil[87] verwendet und empfohlen. Mit dem Chipkartenleser und der mitgelieferten Software ist die Uni-Chipkarte in der PKI-Umgebung der Universität einsetzbar und sicherheitskritische Anwendungen wie die Signatur, Verschlüsselung und Authentisierung können an jedem PC mit Internetanschluß genutzt werden.[88]

3.3.1.2 Derzeitige Nutzung und Entwicklungen

Derzeit befindet sich die Chipkarte mit ihrem gesamten Funktionsumfang noch in der Einführungsphase und viele der möglichen Einsatzgebiete werden erst nach und nach realisiert. Zu Anfang sei an dieser Stelle nochmals darauf hingewiesen, daß die Chipkarte derzeit nur als (elektronischer) Studienausweis für Studierende ausgegeben wird. Eine Einführung der Chipkarte als Mitarbeiterausweis für Angestellte der Universität ist zwar im Gespräch, allerdings noch nicht beschlossen.[89] Im Folgenden sollen die bereits realisierten und die geplanten Einsatzgebiete der Chipkarte dargestellt werden.

Die meisten bereits realisierten Anwendungsbereiche beziehen sich auf die Nutzung der Daten auf der sichtbaren Oberfläche. In diesem Zusammenhang ist als erstes die Eigenschaft der Chipkarte als fälschungssicherer Studienausweis zu nennen. Zudem ist durch die Integration eines Lichtbildes keine gleichzeitige Vorlage des Personalausweises zur Personenkontrolle mehr nötig. Dadurch wird nicht nur die Identitätskontrolle innerhalb der Universität, bspw. bei Anwesenheitskontrollen bei Klausuren, sondern auch die Nutzung des öffentlichen Nahverkehrs vereinfacht. Das aufgedruckte RMV-Logo inkl. Gültigkeitszeitraum dient dabei als Fahrkarte für den öffentlichen Nahverkehr. Weiterhin findet die Chipkarte als Leseausweis für die Universitätsbibliotheken Verwendung.

85 Vgl. Fock, Falko: Informationen zur Chipkarte, Info zur Chipkarten-Aktualisierung, Online im Internet: http://www.uni-giessen.de/chipkarte/aktualisierung.html, 21.09.2003.

86 Vgl. Partosch, Günter: Informationen zur Chipkarte, Chipkarten-Info zu PIN und PUK, Online im Internet: http://www.uni-giessen.de/chipkarte/pinPuk.html, 17.01.2003.

87 Weitere Informationen unter URL: http://www.kobil.de.

88 Vgl. Partosch, Günter: Informationen zur Chipkarte, Information über Chipkarten-Leser, Online im Internet: http://www.uni-giessen.de/chipkarte/chipkartenleser.html, 16.01.2003.

89 Vgl. Partosch, Günter: Informationen zur Chipkarte, Chipkarten-Info – Ausweisnummer, a. a. O.

Dabei wird der rückseitig angebrachte Barcode zur einfachen und schnellen Personenerfassung genutzt. Aber nicht nur bei der Bücherausleihe wird der Barcode genutzt, denn grundsätzlich ist eine Verwendung in sämtlichen Bereichen der Personenerfassung denkbar, z. B. im Studentensekretariat oder bei der Erfassung von Klausurteilnehmern.[90] Im Bereich der Bibliotheken können darüber hinaus Bücher über das Internet vorbestellt und verlängert werden. Dazu muß ein zur Uni-Chipkarte zugehöriges spezielles Bibliothekspaßwort beantragt werden. Nach Eingabe der Ausweisnummer (Chipkartenummer) und des Paßworts in der Internetanwendung der Bibliothek, stehen diese Funktionen zur Verfügung.[91]

Die derzeitige Nutzung des kontaktlosen Mifare-Chips bezieht sich in erster Linie auf Bezahlvorgänge im Bereich der Universität. Alle Bezahlvorgänge in Mensen und Cafeterias der Universität sind nahezu ausschließlich mit der Uni-Chipkarte zu tätigen. Des weiteren bestehen Bemühungen, die Kassen der Bibliothek und des Hochschulrechenzentrums (HRZ) an das System anzuschließen sowie im Bereich der Universität bargeldloses Fotokopieren zu ermöglichen.[92] Neben dem Ausdruck von Studienbescheinigungen an Selbstbedienungsterminals ist auch ein Einsatz der Chipkarte als Zugangsmedium zu den Räumen der Universität in Planung.[93] Wann diese Funktionalitäten verfügbar sein werden, ist allerdings noch nicht abzusehen.

Das größte Ungleichgewicht zwischen den realisierten und möglichen Anwendungsgebieten, besteht sicherlich bei der Nutzung des kontaktbehafteten Kryptochips. Sieht man einmal von der Möglichkeit des Signierens und Verschlüsselns von E-Mails ab, ist im Großen und Ganzen derzeit noch keine Anwendung produktiv und flächendeckend im Einsatz. Lediglich die E-Mail-Weiterleitung von der Universitäts-E-Mail zu einer externen E-Mail-Adresse kann derzeit online beantragt werden.[94] Des weiteren sollte die Rückmeldung zum Sommersemster 2004 bereits vollständig über das Internet möglich sein. Aufgrund von umfangreichen Umstellungen konnte dieser Termin allerdings nicht gehalten werden.[95] Geplant ist weiterhin der Zugriff auf uni-lizensierte oder uni-interne

90 Vgl. o.V.: Informationen zur Chipkarte, Einsatzgebiete für die Chipkarte, Online im Internet: http://www.uni-giessen.de/chipkarte/einsatzgebiete.html, 20.01.2004.

91 Vgl. JLU-Gießen, Bibliothekssystem: Ausleihe, Online im Internet: http://www.uni-giessen.de/ub/service/ausleihe.html, 11.03.2004.

92 Fock, Falko: Informationen zur Chipkarte, Info zur elektronischen Geldbörse der JLU-Chipkarte, Online im Internet: http://www.uni-giessen.de/chipkarte/geldboerse.html, 17.06.2003.

93 Vgl. o.V.: Informationen zur Chipkarte, Einsatzgebiete für die Chipkarte, a. a. O.

94 Soll eine externe E-Mail-Adresse zum Signieren und Verschlüsseln von E-Mails genutzt werden, so muß eine Umleitung von der Universitäts-Email-Adresse zu der externen beantragt werden, da nur die Universitäts-Email-Adresse im Zertifikat berücksichtigt ist. Vgl. dazu Partosch, Günter: Informationen zur Chipkarte, Chipkarte und E-Mail-Adresse, Online im Internet: http://www.uni-giessen.de/chipkarte/e-mail.html, 17.01.2003.

95 Vgl. Fock, Falko: Informationen zur Chipkarte, Aktuelles, Online im Internet: http://www.uni-giessen.de/chipkarte/aktuell.html, 11.03.2004; auch Fock, Falko: Informationen zur Chipkarte,

Informationen mittels Web-Server-Proxy-Dienst und/oder VPN.[96] Ferner ist der Zugang zum Internet (ohne HRZ-Account) und zu sonstigen Rechnersystemen an öffentlichen PC im Bereich der Universität im Gespräch. Des weiteren wurden bei der Planung bereits zahlreiche Anwendungen bedacht, die im Verantwortungsbereich der einzelnen Fachbereiche liegen, wie z. B. die Prüfungsverwaltung.[97]

3.3.2 Das Web Portal System (WPS)

3.3.2.1 Merkmale und Funktionsweise

Das WPS ist im Grunde ein speziell für den Einsatz in dezentralen Organisationsformen entwickeltes Web Content Management System.[98] Entwickelt und eingeführt wurde die erste Version bereits 1999 von den Mitarbeitern des Lehrstuhls für allgemeine BWL und Wirtschaftsinformatik unter der Leitung von Prof. Dr. Axel C. Schwickert an der Johannes-Gutenberg-Universität in Mainz.[99] Mittlerweile zur Version 2.5 herangereift, bildet es seit Anfang 2002 das infrastrukturelle Rückgrad der Web-Präsenz des Fachbereichs Wirtschaftswissenschaften der Justus-Liebig-Universität Gießen.[100]

Technisch gesehen basiert das WPS auf der als „LAMP“ bezeichneten Kombination mehrerer „serverseitigen“ Software-Komponenten. Im Einzelnen:

- Linux (Betriebssystem),
- Apache (Web Server),
- MySQL (Datenbank Server) und
- PHP (Middleware).

Diese bewährte Open-Source-Kombination hat neben der lizenzkostenfreien Nutzung und der hohen Stabilität vor allem den Vorteil der guten Skalierbarkeit. „Client-seitig“ dient lediglich ein Web Browser zur Nutzung und Administration der Web Sites.[101]

Chipkarten-Info zur Rückmeldung, Online im Internet: http://www.uni-giessen.de/chipkarte/rueckmeldung.html, 05.02.2004.

96 Vgl. dazu Kapitel 3.3.2.3 Probleme und Unzulänglichkeiten bisheriger Sicherheitslösungen.

97 Vgl. o.V.: Informationen zur Chipkarte, Einsatzgebiete für die Chipkarte, a. a. O.

98 Vgl. Schwickert, Axel C.; Ostheimer, Bernhard; Franke, Thomas S.: eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen, in: Arbeitspapiere WI, Nr. 9/2000, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes-Gutenberg-Universität Mainz: Mainz 2000, S. 3 ff.

99 Vgl. Schwickert, Axel C.; Ostheimer, Bernhard; Franke, Thomas S.: eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen, a. a. O., S. 5.

100 Vgl. Schwickert, Axel C.; Grund, Henning: Web Content Management – Grundlagen und Anwendungen mit dem Web Portal System V.2.5, in: Arbeitspapiere WI 3/2004, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2004, 62 Seiten., S. 41.

101 Vgl. Schwickert, Axel C.; Ostheimer, Bernhard; Franke, Thomas S.: eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen, a. a. O., S. 15.

Der organisatorische Aufbau folgt dabei der Grundstruktur des Fachbereichs. Jede Organisationseinheit verfügt über einen eigenen Internetbereich (Web Site), der von den jeweiligen Mitarbeitern gepflegt und mit Inhalt gefüllt wird. Als zentrale Anlaufstelle bietet das WPS ein Portal, welches die einzelnen Web Sites navigatorisch integriert sowie deren Inhalte aggregiert.[102] Das gesamte System folgt dabei dem Prinzip der Intranet-Erfassung und der Internet-Veröffentlichung. Den einzelnen Organisationseinheiten wird für die Pflege und Administration der Web Site jeweils eine eigene geschützte Intranetumgebung zur Verfügung gestellt. In dieser haben die Mitarbeiter nach erfolgreicher Authentifizierung Zugriff auf alle Funktionalitäten bzw. Module des WPS.[103] Dies sind z. B.:

- Organisatorische Einheit,
- File-Service,
- Diplomarbeiten, Projekte,
- Service,
- Lehrveranstaltungen,
- Online-Evaluationen,
- Sonderveranstaltungen,
- News und Aktuelles,
- Site Designer,
- Online Editionen und
- Papershop[104].

Die Bedienung aller Funktionalitäten des WPS ist über Web-Formulare realisiert. Nach der Eingabe der zu veröffentlichen Informationen werden diese „per Knopfdruck“ in HTML-Code umgewandelt und auf der Web Site veröffentlicht.[105] Dabei ist die für ein WCMS geforderte Trennung von Struktur und Inhalt konsequent umgesetzt. Alle Inhalte werden unabhängig ihrer Darstellung zentral in einer Datenbank vorgehalten.[106] Die Darstellungsweise der bei Abruf dynamisch erzeugten Seiten erfolgt nach Maßgabe der Einstellungen im Modul „Site-Designer“. Da die Erläuterung aller Module des WPS

102 Vgl. Schwickert, Axel C.; Grund, Henning: Web Content Management – Grundlagen und Anwendungen mit dem Web Portal System V.2.5, a. a. O., S. 44 f.

103 Vgl. Schwickert, Axel C.; Ostheimer, Bernhard; Franke, Thomas S.: eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen, a. a. O., S. 5 ff.

104 Vgl. Schwickert, Axel C.; Grund, Henning: Web Content Management – Grundlagen und Anwendungen mit dem Web Portal System V.2.5, a. a. O., S. 50 ff.

105 Vgl. Schwickert, Axel C.; Ostheimer, Bernhard; Franke, Thomas S.: eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen, a. a. O., S. 8.

106 Vgl. Schwickert, Axel C.; Grund, Henning: Web Content Management – Grundlagen und Anwendungen mit dem Web Portal System V.2.5, a. a. O., S. 58.

den Rahmen der Arbeit übersteigen würde,[107] soll im Folgenden lediglich auf die Programmteile eingegangen werden, mit denen die zuvor dargestellten sicherheits- und authentifizierungskritischen Aufgaben gelöst werden.

Eine zentrale Rolle spielt dabei der Zugriff auf den geschützten Intranetbereich der einzelnen Organisationseinheiten. Dabei erfolgt die Authentifizierung durch eine bereichsindividuelle Benutzername/Paßwort-Kombination. Beim Login besteht die Möglichkeit, die Zugangsdaten verschlüsselt an den WPS-Server zu übermitteln. Dazu wird auf das bekannte Challenge-Response-Verfahren zurückgegriffen. Im Erfolgsfall erteilt der Server eine temporäre Legitimation in Form einer sog. Session-ID. Weiterhin besteht die Möglichkeit den gesamten Datenverkehr in diesem Bereich, durch Anpassung der Systeme per SSL-Technologie zu sichern.[108]

Das Modul „File-Service“ erlaubt das Einstellen von Dateien beliebiger Formate in das WPS und dient daher bspw. im Bereich der Professuren zur Veröffentlichung von Lehrmaterialien und Prüfungsergebnissen. Zur Durchführung von Online-Evaluationen der Lehrveranstaltungen stellt das WPS ein eigenes Modul zur Verfügung. Dieses unterstützt zum einen die Generierung von Fragebögen und zum anderen deren Auswertung. Unter dem Modul „News und Aktuelles“ besteht neben der Veröffentlichung von aktuellen Informationen und dem Verschicken von E-Mail-Newslettern die Möglichkeit, Diskussionsforen anzubieten. Diese werden bspw. von den Professuren zur Unterstützung der Lehre oder von der Fachschaft zum Meinungsaustausch am Fachbereich genutzt. Bei allen bisher erwähnten Bereichen besteht die Möglichkeit, die einzelnen Inhalte mit einem Zugriffsschutz zu versehen. Dies kann durch eine zuvor festgelegte Benutzername/Paßwort-Kombination und/oder durch eine IP-Bereichsbeschränkung geschehen.

Unter dem Modul „Lehrveranstaltungen“ besteht die Möglichkeit, automatisch Anmeldeformulare für bestimmte Veranstaltungen zu generieren und zu veröffentlichen. Dabei existiert zur Zeit noch keine Sicherheitslösung zur Konsistenzprüfung der eingegebenen Daten oder zur eindeutigen Identifizierung der Teilnehmer. Dies gilt ebenso für die unter „Service“ verfügbare Account-Beantragung für den PC-Pool. Weiterhin steht den Organisationseinheiten ein Modul zur Verwaltung einfacher Papershops zur Verfügung. Darüber können sie Arbeitspapiere oder sonstige Dokumente gegen Entgeld anbieten. Die Zahlungsabwicklung wird dabei von Firstgate übernommen.

107 Eine Beschreibung der einzelnen Module der WPS Version 2.5 findet sich bei: Schwickert, Axel C.; Grund, Henning: Web Content Management – Grundlagen und Anwendungen mit dem Web Portal System V.2.5, a. a. O., S. 51ff.

108 Vgl. Schwickert, Axel C.; Ostheimer, Bernhard; Franke, Thomas S.: eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen, a. a. O., S. 15 f.

3.3.2.2 Student Personal Information Center (SPIC)

Durch die zunehmende Akzeptanz und den erweiterten Funktionsumfang ist die Nutzungsintensität des WPS in der letzten Zeit stark angestiegen. Dies wirkt sich selbstverständlich auf die Menge der zur Verfügung stehenden Informationen aus. Dieser Umstand ist auf der einen Seite positiv zu beurteilen, bewirkt aber auch die Gefahr eines „Information Overflows“ bei den Nachfragern. Davon sind vor allem die Studierenden betroffen. Um dieser Gefahr entgegenzuwirken, ist ein sog. Student Personal Information Center in Planung. Dieses Modul soll den Studierenden erlauben, die für sie relevanten Informationen und Funktionen auszuwählen und personalisiert zu kanalisieren. Zu diesem Zweck soll Studierenden im Rahmen des WPS ein eigener geschützter Web-Bereich zur Verfügung gestellt werden. Im Sinne eines personalisierten Studierenden-Portals kann das SPIC folgende Funktionalitäten umfassen:

- Zusammenstellung eines individuellen Vorlesungsplans,
- Verwaltung ausgeliehener Bücher mit Erinnerungsfunktion,
- Allgemeine Erinnerungsfunktionen,
- Verwaltung abonnierter E-Mail Newsletter,
- Verwaltung ausgewählter Download-Center,
- Verwaltung ausgewählter Foren,
- Erstellung einer individuellen Startseite,
- Verwaltung der Wahlfächer und Studienleistungen (Noten) und
- Anmeldungen zu Prüfungen[109].

Das SPIC ist mit seinem Funktionsumfang im Rahmen dieser Arbeit in zweierlei Hinsicht interessant. Zum einen erfordert die Personalisierung eine eindeutige Identifikation der einzelnen Benutzer[110] und zum anderen bietet das SPIC einen Rahmen für die durch den Einsatz der Smart Card ermöglichten neuen Funktionalitäten wie z. B. die Noteneinsicht und die Prüfungsanmeldungen. Das SPIC befindet sich derzeit im Entwicklungsstatus und die Einführung ist zu Beginn des Wintersemesters 04/05 geplant.

3.3.2.3 Probleme und Unzulänglichkeiten bisheriger Sicherheitslösungen

Die vom WPS angebotenen Sicherheitslösungen machen es möglich, bestimmte Bereiche und Informationen vor unerlaubtem Zugriff zu schützen. Dennoch bestehen bei vielen bisher angesprochenen Aufgaben Probleme oder Unzulänglichkeiten. Das betrifft zum einen die Intranet-Administration und zum anderen die Internet-Veröffentlichung.

109 Vgl. Schwickert, Axel C.; Grund, Henning: Web Content Management – Grundlagen und Anwendungen mit dem Web Portal System V.2.5, a. a. O., S. 59 f.

110 Vgl. Schwickert, Axel C.; Grund, Henning: Web Content Management – Grundlagen und Anwendungen mit dem Web Portal System V.2.5, a. a. O., S. 60.

Der Zugang zum administrativen Intranet-Bereich der einzelnen Organisationseinheiten ist, wie zuvor dargelegt, durch eine bereichsindividuelle Benutzerkennung/Paßwort-Kombination geschützt. Alle Mitarbeiter einer Organisationseinheit nutzen daher die gleichen Zugangsdaten, so daß keine eindeutige Identifizierung einzelner Mitarbeiter stattfindet. Dies hat zur Folge, daß dementsprechend alle Mitarbeiter über die gleichen Rechte verfügen und nicht verfolgt werden kann, wer welche Aktionen tätigt. Im Schadensfall, ist der Verantwortliche also nicht ohne weiteres auszumachen. Dabei ist die geschilderte Bedrohung von „Innerhalb“ noch als weniger gefährlich einzuschätzen. Anders stellt sich dieses Problem dar, sollten die Zugangsdaten auf irgendwelchem Wege an unbefugte Dritte gelangen. Die Möglichkeit, Schaden durch die Veröffentlichung von gezielten Fehlinformationen anzurichten wäre dabei sicherlich noch das geringste Übel.

Im Bereich der Internet-Veröffentlichung soll sowohl durch den Paßwort-Schutz als auch durch die Begrenzung des IP-Nummerkreises im Grunde sichergestellt werden, daß nur die gewünschten Personen Zugriff auf die geschützten Bereiche erhalten. In der Realität bedeutet dies, daß bspw. nur die Teilnehmer einer Lehrveranstaltung auch Zugriff auf die bereitgestellten Lehrmaterialien erhalten oder an den anschließenden Evaluationen teilnehmen können.

Bei der Erreichung dieser Ziele wirft die Begrenzung des IP-Bereichs sicherlich die größten Probleme auf. Dabei gewährt der Web Server nur denjenigen Benutzern den Zugriff, denen bei der Anmeldung im Internet eine IP-Adresse aus dem IP-Nummernbereich der Universität Gießen zugeteilt wurde. Dies geschieht entweder durch die Nutzung von Rechnern innerhalb der Universität oder durch die Einwahl am Hochschulrechenzentrum der Universität Gießen. Benutzer, die keinen Account beim HRZ besitzen, sind daher nicht in der Lage, die geschützten Funktionalitäten vom heimischen PC zu nutzen und müssen dafür auf die Rechner der Universität bspw. im PC-Pool zurückgreifen.[111] Dies betrifft vor allem Nutzer von DSL- (Digital Subscriber Line) oder sonstigen Breitband-Internetzugängen, da das HRZ keine Einwahlmöglichkeit für derartige Zugänge bietet.[112] Als einzige Lösung dieses Problems wird vom HRZ eine VPN-Lösung (Virtual Private Network) angeboten.[113] Zur Einwahl in das VPN ist aber trotzdem ein HRZ-Vollaccount nötig.[114] Neben der Installation zusätzlicher Software ist der größte Nachteil daran die aus der Nutzung zweier Provider resultierende doppelte Ko-

111 Zu der IT-Ausstattung am Fachbereich vgl. Kapitel 3.3.5.

112 Vgl. zu dieser Problematik Ackermann, Kurt: Warum kein DSL-Zugang zum Datennetz der JLUG ?, Online im Internet: http://www.uni-giessen.de/hrz/datennetze/unigi-net/dsl.htm, 21.05.2003.

113 Vgl. Ackermann, Kurt: UNIGI-NET, VPN: Für wen?, Online im Internet: http://www.uni-giessen.de/hrz/datennetze/unigi-net/vpn/usage.html, 19.05.2003.

114 Vgl. Ackermann, Kurt: UNIGI-NET, VPN: Voraussetzungen, Online im Internet: http://www.uni-giessen.de/hrz/datennetze/unigi-net/vpn/voraussetzungen.html, 13.06.2003.

stenbelastung.[115] Neben den bisher aufgeführten Problemen der IP-Begrenzung ist das Hauptproblem daran sicherlich, daß dadurch nicht den gewünschten Adressaten exklusiv der Zugriff gewährt, sondern lediglich allen Benutzern eine technische Hürde in den Weg gestellt wird.

Sinnvoller ist da schon die Zugriffsbeschränkung mittels einer Benutzername/Paßwort-Kombination. Den gewünschten Adressaten kann dabei der Zugang exklusiv durch die Vermittlung der Zugangsdaten ermöglicht werden. Dies setzt natürlich voraus, daß alle Adressaten auch tatsächlich erreicht und ihnen die Zugangsdaten auf sicherem Wege vermittelt werden können. Bisher geschieht dies im Wesentlichen im Rahmen der Lehrveranstaltungen. Dabei kann allerdings nicht sichergestellt werden, daß alle Adressaten tatsächlich anwesend sind und dementsprechend die Zugangsdaten erhalten. Ferner resultieren daraus weitere Probleme, die aus der allgemeinen Problematik wissensbasierter Geheimnisse entstehen. In diesem Zusammenhang sei vor allem auf die unberechtigte Weitergabe an Dritte und das Vergessen von Zugangsdaten hingewiesen. Letzteres ist vor allem auf die Flut an Paßwörtern zurückzuführen, mit der die Adressaten im Laufe der Zeit konfrontiert werden.

Abgesehen von diesen Problemen ist eine solche Zugangsbeschränkung in den meisten Bereichen durchaus sinnvoll und ausreichend. Das betrifft im Grunde alle Anwendungsgebiete, in denen lediglich die Geheimhaltung sichergestellt werden soll (z. B. Lehrmaterialien, Klausurergebnisse etc.). Eine echte Authentifizierung der einzelnen Teilnehmer ist hingegen mit beiden derzeit realisierten Sicherheitsmechanismen nicht möglich. Problematisch ist dieser Umstand bspw. bei den Online-Evaluationen, da hier gewährleistet werden muß, daß jeder Teilnehmer seine Bewertung tatsächlich nur einmal abgibt. Ein weiterer Problembereich entsteht durch die fehlende Authentifizierung bei den Diskussionsforen. Zwar kann der Zugriff bspw. durch ein Paßwort geschützt werden, allerdings ist eine eindeutige Zuordnung der einzelnen Beiträge zu den Teilnehmern nicht möglich. Gleiches gilt für den Bereich der verbindlichen Anmeldungen. Dabei ist die eindeutige Zuordnung wesentliche Voraussetzung für die Verbindlichkeit und Nicht-Abstreitbarkeit. Gerade wenn daraus prüfungsrechtliche Konsequenzen entstehen, müssen diese Forderungen unbedingt erfüllt sein.

3.3.3 Die Zertifizierungsinstanz der Universität Gießen

Für die Personalisierung und Zertifizierung der Chipkarten betreibt das HRZ der Justus-Liebig-Universität in Zusammenarbeit mit dem Deutschen Forschungsnetz (DFN) eine eigene Zertifizierungsinstanz. Der Name UniGI-CCA steht dabei für „Chipcard Certifi-

115 Zu den Kosten des HRZ-Account vgl. Wolf, Dieter: Internet-Entgelt an der Justus-Liebig-Universität Gießen, Online im Internet: http://www.uni-giessen.de/hrz/kommuni/entgelt.html, 17.01.2002.

cation Authority der Universität Gießen“. Diese wurde von der DFN Toplevel CA zertifiziert und stellt ihrerseits die Zertifikate für die einzelnen Chipkarten(-Benutzer) aus.[116] Abbildung 11 zeigt die Darstellung des UniGI-CCA im Internet Explorer

Abb. 11: Darstellung des UniGI-CCA-Zertifikat im Internet Explorer

Die ausgestellten Zertifikate sind in der Form des X.509v3-Standards und stehen im Lightweight Directory Access Protocol (LDAP)/X.500-Verzeichnisdient der Universität den Anwendungsprogrammen zur Verfügung.[117] Da die UniGI-CCA ausschließlich Zertifikate für die Uni-Chipkarte ausstellt, betreibt das HRZ daneben noch die UniGI-SCA (SSL-Server Certification Authority der Universität Gießen) zur Zertifizierung der an der Universität betriebenen SSL-Server. Das Wurzelzertifikat ist auch in diesem Fall das DFN-Toplevel-Zertifikat.[118] Auch der WPS-Server des Fachbereichs Wirtschaftswissenschaften wurde von der UniGI-SCA als SSL-Server zertifiziert. Die Sicherheits-Policies beider CA sind durch die Einbindung in die Zertifizierungshierarchie des DFN auf deren Richtlinien festgelegt.[119] Durch die Zertifizierung der Chipkarten auf der einen und des WPS-Servers auf der anderen Seite sind am Fachbereich Wirtschaftswissenschaften im Grunde die technischen Voraussetzungen für eine sichere Kommunikation geschaffen.

116 Vgl. Weiß, Dieter: Chipkarten-Zertifizierungsinstanz der Universität Gießen (UniGI-CCA), Online im Internet: http://www.uni-giessen.de/hrz/unigi-ca/cca.html, 19.10.2002.

117 Partosch, Günter: Informationen zur Chipkarte, Chipkarte und E-Mail-Adresse, a. a. O.

118 Obermann, Jürgen: SSL-Server-Zertifizierungsinstanz der Universität Gießen (UniGI-SCA), Online im Internet: http://www.uni-giessen.de/hrz/unigi-ca/sca.html, 17.12.2001.

119 Zu der Policy des DFN vgl. DFN Cert: DFN PCA World Wide Web Policy: Online im Internet: http://www.pca.dfn.de/certification/policies/ssl-tls/cp-1.4/wwwpolicy.html, 15.12.2003.

3.3.4 Systeme des Prüfungsamts

Das Prüfungsamt des Fachbereichs Wirtschaftswissenschaften arbeitet zur Verwaltung des gesamten Prüfungsprozesses mit dem studienbegleitenden Prüfungsverwaltungssystem FlexNow.[120] Entwickelt wurde dieses System unter der Leitung von Prof. Dr. Elmar J. Sinz am Lehrstuhl für Wirtschafsinformatik an der Universität Bamberg. Im Grunde handelt es sich dabei um eine Datenbankanwendung, die den gesamten Prüfungsprozeß von der Erstellung des Prüfungsangebots über die Erfassung der Daten durch die Prüfer bis hin zum Ausstellen von Zeugnissen und Bescheiden abbildet und unterstützt.

Das gesamte System basiert auf der Client/Server-Architektur. Als Server dienen ein Datenbank- und ein Web Server mit einer gemeinsamen Datenbasis. Der Zugang erfolgt je nach Nutzergruppe mit unterschiedlichen Front Ends. Während zur Pflege und Administration der Daten durch die Mitarbeiter des Prüfungsamts und der Professuren eine „FlexNow-spezifische“ Software eingesetzt werden muß, ist für den Zugang für die Gruppe der Studierenden lediglich ein Web Browser nötig.[121] Abbildung 12 zeigt die grundlegende Architektur von FlexNow aus Nutzersicht.

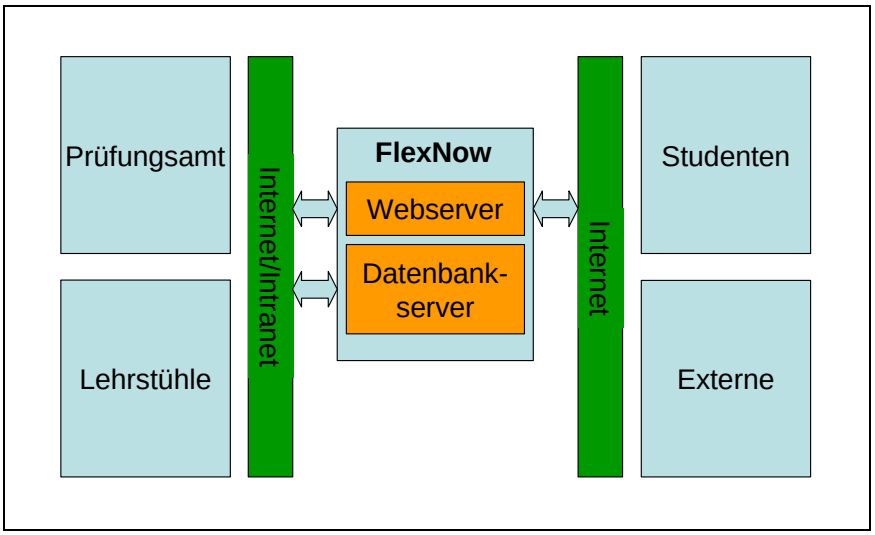

Abb. 12: Architektur von FlexNow aus Nutzersicht[122]

Am Fachbereich Wirtschaftswissenschaften wird das System bis dato (März 2004) allerdings nur für die interne Verwaltung der Daten eingesetzt. Zugriff auf das System haben derzeit nur das Prüfungsamt und die Professuren. Das Web Interface für die Stu-

120 Weitere Informationen zu FlexNow unter URL: http://flexnow.uni-bamberg.de.

121 Vgl. Sinz, Elmar, J.; Wismans, Benedikt: Das "Elektronische Prüfungsamt" – Bamberger Beitrag zur Wirtschaftsinformatik Nr. 47, Online im Internet: http://www.seda.sowi.uni-bamberg.de/forschung/publikationen/bamberger-beitraege/no47.pdf, 1998.

122 In Anlehnung an Sinz, Elmar, J.; Wismans, Benedikt: Das "Elektronische Prüfungsamt" – Bamberger Beitrag zur Wirtschaftsinformatik Nr. 47, a. a. O.

dierenden wird im Moment noch nicht eingesetzt. Dabei ist der Web Server von FlexNow in der Lage, auf Basis des gemeinsamen Datenbestands automatisch Web-Seiten zu generieren und dadurch zahlreiche Selbstverwaltungsfunktionalitäten für die Studierenden im Web bereitzustellen. Dies betrifft vor allem die An-/Abmeldung zu Prüfungen, die Noteneinsicht, die Stammdatenverwaltung etc. Um dabei die nötige Sicherheit zu gewährleisten, wird momentan nur das aus dem Home-Banking-Bereich bekannte PIN/TAN-Verfahren von FlexNow zu Verfügung gestellt.[123] In diesem Punkt liegt auch die Erklärung dafür, daß das Web Interface derzeit noch keine Verwendung am Fachbereich findet. Schließlich steht mit der Uni-Chipkarte ein wesentlich sichereres Identifikationsmedium zur Verfügung, so daß es nicht sinnvoll wäre, eine aufwendige PIN/TAN-Insellösung einzuführen. Dies gilt vor allem vor dem Hintergrund, daß bereits seit einiger Zeit an einer Chipkarten-Unterstützung für FlexNow gearbeitet wird. Nicht zuletzt da die vertraglichen Voraussetzungen von Seiten der Universität bereits geschaffen worden sind, kann mit der Verfügbarkeit einer solchen Unterstützung ca. Mitte April 2004 gerechnet werden.

3.3.5 IT-Ausstattung am Fachbereich Wirtschaftswissenschaften

Der Fachbereich Wirtschaftswissenschaften bietet mittlerweile nicht zuletzt durch die Einführung des WPS eine recht gut ausgestattete IT-Landschaft. Dies betrifft zum einen die Ausstattung der einzelnen Organisationseinheiten, deren Mitarbeiter ausnahmslos über einen vernetzten PC zur Erledigung der täglichen Aufgaben verfügen.[124] Chipkartenleser finden sich in diesem Bereich aber allenfalls sporadisch.

Zum anderen soll an dieser Stelle vor allem auf die „öffentlich“ verfügbaren Teile eingegangen werden, die für die Studierenden zur Nutzung bereitstehen. Eine zentrale Rolle spielt dabei der PC-Pool des Fachbereichs. Im Rahmen der Öffnungszeiten stehen den Studierenden hier 21 PC zur Verfügung. Alle PC befinden sich auf dem aktuellen Stand der Technik und sind – wie sämtliche Rechner des Fachbereichs – über das UNI-GI-NET mit dem Internet verbunden.[125] Auch die Rechner im PC-Pool sind derzeit noch nicht mit Chipkartenleser ausgestattet. Eine weitere Möglichkeit der PC-Nutzung für die Studierenden besteht im wirtschaftswissenschaftlichen Seminar. Jedoch sind die PC grundsätzlich nur für die Literaturrecherche (z. B. im Online Public Access Catalogue

123 Vgl. Sinz, Elmar, J.; Wismans, Benedikt: Das "Elektronische Prüfungsamt" – Bamberger Beitrag zur Wirtschaftsinformatik Nr. 47, a. a. O.

124 Ohne Berücksichtigung der studentischen Hilfskräfte, vgl. dazu Treber, Udo; Muschiol, Tim; Gillen, Arndt: Wireless LAN – Situations- und Anforderungsanalyse am Beispiel eines Universitätscampus, in: Arbeitspapiere WI 4/2004, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2004, 110 Seiten, S. 16 f.

125 Vgl. Treber, Udo; Muschiol, Tim; Gillen, Arndt: Wireless LAN – Situations- und Anforderungsanalyse am Beispiel eines Universitätscampus, a. a. O., S. 13.

(OPAC)- System) freigegeben. Daher ist die sämtliche weitere Nutzung untersagt.[126] Allerdings hält das Seminar auch 64 Notebook-Anschlüsse vor und bietet den Studierenden und Mitarbeitern neuerdings (seit Anfang März 2004) einen Netzzugang mittels eines Wireless Local Area Network (W-LAN). Weitere W-LAN Access Points befinden sich im Foyer des Seminargebäudes am Fachbereich, so daß ein Netzzugang auch in diesem Teil des Gebäudes und in den angrenzenden Außenbereichen möglich ist.[127] Diese Art des Zugangs steht selbstverständlich nur denjenigen Personen zur Verfügung, die über ein Notebook mit erforderlicher Hardware (W-LAN-Karte) und über einen HRZ-Account verfügen.[128] Dementsprechend würde auch die Anschaffung eines Chipkartenlesers bei den Studierenden bzw. Mitarbeitern liegen. Derzeit läuft das gesamte W-LAN-System noch im Probebetrieb, allerdings bestehen konkrete Bemühungen, die W-LAN-Verfügbarkeit am Fachbereich weiter auszubauen.[129]

3.4 Fazit der Situationsanalyse

Aus den bisherigen Ausführungen läßt sich ein ganz klarer Bedarf an sicheren Smart-Card-Anwendungen feststellen. Dieser resultiert in erster Linie aus den Unzulänglichkeiten bisheriger Lösungen. Erinnert sei an dieser Stelle vor allem an die Problematik im Bereich des Prüfungsamts, wodurch es immer wieder zu unnötigen Wege- und Wartezeiten auf der einen und zu Arbeitsüberlastungen auf der anderen Seite kommt. Im Bereich der Professuren und den sonstigen WPS-nutzenden Organisationseinheiten sind zwar viele Funktionen bereits online verfügbar und durch entsprechende Sicherheitsmechanismen ausreichend geschützt, dennoch sind auch hier gewisse Problemfelder auszumachen. Hauptsächlich beziehen sich diese auf die fehlende eindeutige Identifizierung der Adressaten oder liegen in der Verteilungs- und Verfügbarkeitsproblematik begründet.

Weiterhin läßt sich auch von Seiten der Kommunikatoren ein gewisser Bedarf feststellen. Dabei muß allerdings beachtet werden, daß die Ziele der Kommunikatoren in manchen Bereichen konfliktbehaftet sind. Es sei vor allem auf die Themen Datenschutz, Anonymität oder gar auf den „gläsernen Studenten“ hingewiesen. Auch wurde festgestellt, daß die Studierenden in dem Smart-Card-Umfeld die einzigen Kunden der Anwendungen sind. Das wird wahrscheinlich auch zunächst einmal so bleiben, da eine

126 Vgl. Treber, Udo; Muschiol, Tim; Gillen, Arndt: Wireless LAN – Situations- und Anforderungsanalyse am Beispiel eines Universitätscampus, a. a. O., S. 11.

127 Vgl. Netzgruppe HRZ: UNIGI-NET, WLAN (Hotspots), Online im Internet: http://www.uni-giessen.de/hrz/datennetze/unigi-net/WLAN/uni-hotspots.html, 04.03.2004.

128 Der HRZ-Account wird dabei zum Aufbau des VPN-Tunnels zum Netz der Universität gebraucht. Vgl. Kapitel 3.3.2.3 Probleme und Unzulänglichkeiten bisheriger Sicherheitslösungen.

129 Vgl. dazu insbesondere Treber, Udo; Muschiol, Tim; Gillen, Arndt: Wireless LAN – Situations- und Anforderungsanalyse am Beispiel eines Universitätscampus, a. a. O.

Einführung von Mitarbeiterkarten auch in nächster Zeit nicht zu erwarten ist. Ansonsten ließen sich eine Reihe von weiteren Problembereichen in den internen Arbeitsabläufen des Fachbereichs aufdecken, die einen Einsatz von Smart Cards rechtfertigen würden. In diesem Zusammenhang wurde lediglich die Administration des WPS berücksichtigt, da dabei in der Regel viele Personen mit „Doppelstatus“ (Studierender und Mitarbeiter) beteiligt sind.

Infrastrukturell sind im Großen und Ganzen die besten Voraussetzungen gegeben. Das liegt nicht zuletzt an der hohen Akzeptanz und Verbreitung des WPS, zumal dessen offene Systemarchitektur eine Integration von PKI-Instrumenten erleichtert. Durch die uni-eigenen CA, die sowohl die Chipkarten, als auch die Server des Fachbereichs zertifizieren steht eine lückenlose PKI zur Verfügung. Im Bereich des Prüfungsamts sind infrastrukturell im Grunde alle Weichen für einen Einsatz von Smart Cards gestellt. Dabei ist durch die Nutzung von FlexNow auch nahezu keinerlei Entwicklungsarbeit mehr nötig. Es bleibt daher nur abzuwarten, wann die geplante Smart-Card-Unterstützung auch tatsächlich verfügbar sein wird. Die IT-Ausstattung am Fachbereich, insbesondere der gut ausgestattete PC-Pool kann nach der Ausrüstung mit Chipkartenlesegeräten helfen, die Anwendungen für die Studierenden auch ohne besondere Investitionen nutzbar zu machen.

4 Anforderungsanalyse

4.1 Ziel und Vorgehen der Anforderungsanalyse

Zahlreiche Problemfelder finden sich am Fachbereich,[130] die einen Einsatz von Smart-Card-Anwendungen rechtfertigen. In diesem Kapitel soll zunächst die Rolle des SPIC als navigatorischer und technischer Rahmen der Smart-Card-Anwendungen beschrieben werden. Es folgt die Diskussion ausgewählter Anwendungsgebiete auf Basis der Situationsanalyse. Dabei soll herausgearbeitet werden, was die einzelnen Funktionalitäten leisten müssen und welche Teilnehmer in welcher Rolle beteiligt sind. Insbesondere sollen mögliche Zielkonflikte der Teilnehmer in der Diskussion Berücksichtigung finden. Sämtliche E-Mail-basierten Funktionalitäten werden dabei vernachlässigt, da diese grundsätzlich zwar im Bereich des Fachbereichs einsetzbar sind, aber nicht speziell von Organisationseinheiten angeboten, sondern individuell durch Drittsysteme (Outlook etc.) realisiert werden.

Anschließend werden im Sinne einer technischen Anforderungsanalyse die notwendigen Hard- und Softwareanforderungen ermittelt. Eine Priorisierung der einzelnen Anwendungsgebiete hat nachfolgend zum Ziel, besonders erfolgversprechende Funktio-

130 Vgl. Kapitel 3 Situation am Fachbereich 02.

nalitäten herauszufiltern, die im Anschluß prototypisch entwickelt werden. Da diese auf der einen Seite ein großes Nutzenpotential aufweisen und auf der anderen Seite auch relativ zeitnah produktiv genutzt werden sollen, erfolgt die Priorisierung anhand entsprechender Determinanten. Das Ergebnis soll anschließend als Entscheidungsgrundlage der zu entwickelnden Anwendungsgebiete dienen.

4.2 Das SPIC als Systemrahmen

Wie in Kapitel 3.3.2.2 bereits aufgeführt, spielt das SPIC im Zusammenhang mit der Integration von Smart-Card-Anwendungen eine besondere Rolle. An dieser Stelle soll allerdings das SPIC als Rahmen sämtlicher Smart-Card-Anwendungen betrachtet werden.[131]

Den Studierenden soll ein eigener geschützter Bereich zur Verfügung gestellt werden, der je nach Funktionsumfang auch sensitive und private Daten beinhalten kann. Aber allein die Personalisierung macht bereits eine eindeutige Identifizierung bzw. Authentisierung der einzelnen Benutzer unumgänglich. Zu diesem Zweck muß das System in der Lage sein, nur den betreffenden Studierenden Zugriff auf seinen Bereich zu gewähren. Da sich diese Funktion ausschließlich an Studierende richtet, steht auch einem Einsatz der Smart Card als einziges Zugangsmedium nichts im Wege. Diskussionswürdig ist allerdings, ob ein derart hohes Sicherheitsniveau auch wirklich erforderlich ist und in diesem Fall nicht „mit Kanonen auf Spatzen geschossen wird“. Grundlage einer solchen Bewertung ist sicherlich der letztendlich realisierte Funktionsumfang. Einzig der Zugriff auf die Noteneinsicht bzw. die Prüfungsanmeldungen würden eine derartige Sicherheitsmaßnahme rechtfertigen. Aber da diese Funktionalitäten im Rahmen dieser Arbeit unabhängig von ihrem späteren navigatorischen Rahmen diskutiert worden sind und dementsprechend über eigene Sicherheitskonzepte verfügen, sollen sie nicht als Teile des SPIC im engeren Sinne behandelt werden. Die verbleibenden SPIC-eigenen Funktionalitäten rechtfertigen nicht unbedingt ein derart hohes Sicherheitsniveau. Man denke bspw. an die Verwaltung abonnierter Newsletter, Downloadcenter etc. Von daher bietet es sich an, an dieser Stelle zwischen kritischen und unkritischen Funktionalitäten zu unterscheiden.

Unkritische Anwendungsgebiete sind die Teile des SPIC, die vor allem für eine bessere Übersicht der Benutzer sorgen und dadurch einem drohenden „Information Overflow“ entgegenwirken. Aber selbst in diesem Zusammenhang macht ein Einsatz der Smart Card durchaus Sinn. Da es ausschließlich den Studierenden ermöglicht werden soll, eine eigene Web-Umgebung zu verwenden, könnte das System die Smart Card zur einmali-

131 Dies bezieht sich selbstverständlich nur auf die geschützten Anwendungen über das Internet. Anwendungsgebiete wie bspw. der PC-Pool Account sind davon ausgenommen.

gen Einrichtung eines solchen Bereichs fordern. Einmal eingerichtet, könnte dem Benutzer die Möglichkeit gegeben werden, eine Benutzername/Paßwort-Kombination als alternative Zugangsmöglichkeit zu wählen. Der Vorteil liegt auf der Hand: Zum einen ist sichergestellt, daß nur Studierende in der Lage sind, diese Funktionalität zu nutzen und zum anderen sind sie nicht wegen jeder kleinen Änderung auf den Einsatz der Smart Card angewiesen.

Etwas anderes stellt sich dieses Szenario dar, betrachtet man das SPIC als eigenständiges Portal innerhalb des WPS welches durch eine einmalige Authentisierung Zugriff auf weitere kritische Anwendungen erlaubt. Dies betrifft z. B. den Zugriff auf geschützte Materialien innerhalb ausgewählter Download-Center oder die Teilnahme an ausgewählten Diskussionsforen. Dabei macht es durchaus Sinn, die Smart Card als einziges Zugangsmedium zum SPIC zu nutzen und eine einmalige Authentisierung im Sinne eines „Single Sign On“[132] durchzuführen. Dies ist allerdings nur bei den WPS-eigenen Funktionalitäten möglich, da der Zugriff auf externe Systeme bspw. des Prüfungsamts aus (sicherheits-) technischen Gründen eine erneute Authentisierung des Benutzers fordert. Daher sollen die einzelnen Funktionalitäten im Folgenden in drei Gruppen eingeteilt werden:

- (unkritische) SPIC-Funktionalitäten (z. B. Verwaltung von News)
- (kritische) WPS-Funktionalitäten (z. B. Downloads, Evaluationen)
- (kritische) externe Funktionalitäten (z. B. Prüfungsanmeldung)

Die unterschiedlichen Gruppen werfen demnach auch unterschiedliche Sicherheitsanforderungen auf. Um die Beziehung zwischen dem SPIC und den einzelnen (kritischen) Funktionalitäten zu verdeutlichen, ist das System der Zugriffsberechtigungen einzelner Anwendungen im Kontext des SPIC in Abbildung 13 dargestellt.

Wie in der Abbildung zu erkennen ist, bietet das SPIC die zwei zuvor diskutierten Zugangsmöglichkeiten an. Verschafft man sich mittels einer gewählten Benutzername/ Paßwort-Kombination Zugang zum SPIC, stehen dem Benutzer lediglich die unkritischen SPIC-Funktionalitäten zur Verfügung. Versucht der Benutzer dann innerhalb des SPIC weitere Smart-Card-geschützte Anwendungen zu nutzen wird er aufgefordert, sich mit der Smart Card zu authentisieren. Das gleiche gilt für die Nutzung von kritischen Funktionalitäten von extern ohne Nutzung des SPIC. Wird hingegen die Smart Card als Zugangsmedium zum SPIC genutzt, stehen dem Benutzer alle geschützten Funktionalitäten ohne weitere Anmelde- oder Authentisierungsvorgänge zur Verfügung. Eine Ausnahme ist hier, wie bereits erläutert, der Zugriff auf externe Systeme (wie FlexNow).

132 Unter dem Begriff „Single Sign On“ soll in diesem Zusammenhang eine einmalige Anmeldung (Authentisierung) an einem System verstanden werden, wodurch der Zugriff auf weitere geschützte Anwendungen möglich ist, ohne eine erneute Anmeldung vorzunehmen.

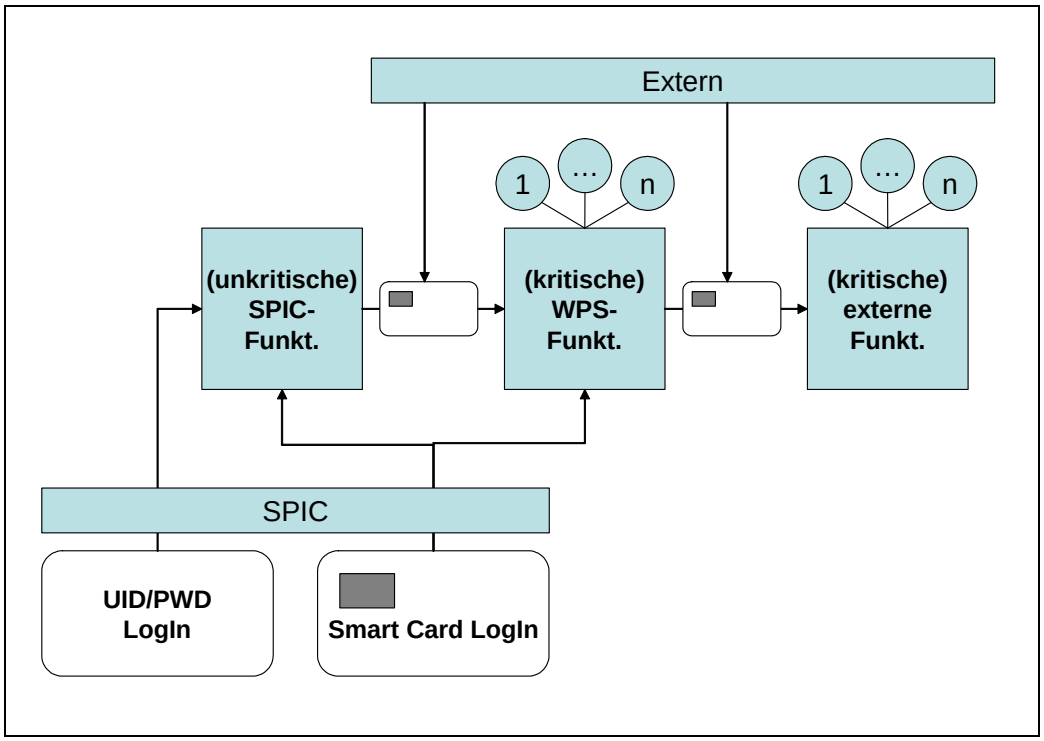

Abb. 13: Das System der Zugriffsberechtigungen einzelner Funktionalitäten im Kontext des SPIC

Im Folgenden sollen die einzelnen kritischen Anwendungsgebiete dargestellt und diskutiert werden. Dabei werden gemäß der zuvor vorgenommenen Gruppierung zunächst die WPS-Funktionalitäten und danach die externen Funktionalitäten erläutert. Anschließend soll im Zuge der Diskussion kritischer Anwendungsgebiete auf weitere Smart-Card-Anwendungen eingegangen werden, die nicht in direkten Zusammenhang mit dem SPIC bzw. dem WPS stehen.

4.3 Spezifikation der Anwendungen

4.3.1 Professuren: An- und Abmeldungen zu Lehrveranstaltungen

Im Folgenden soll auf die Problematik jeglicher prüfungsrelevanter Anmeldevorgänge eingegangen werden, die in den Aufgabenbereich der Professuren fallen. Dazu gehören in erster Linie die Teilnahme-Anmeldungen zu Seminaren, Übungen etc. Dabei muß den Studierenden die Möglichkeit gegeben werden, sich – ebenso wie bei den Anmeldungen beim Prüfungsamt – verbindlich für die betreffenden Veranstaltungen anzumelden. Dies bedeutet, daß hier grundsätzlich die gleichen Anforderungen gelten, wie bei den Anmeldungen beim Prüfungsamt. Die Verbindlichkeit ist in diesem Zusammenhang aber aus mehreren Gründen von zentraler Bedeutung. Für die angemeldeten Studierenden und für die Professuren entsteht dadurch eine Sicherheit in der Semester- und Kursplanung, nicht zuletzt da die Gefahr von „Spaß-Anmeldungen“ nahezu ausgeschlossen

wird. Durch die geschaffene Nicht-Abstreitbarkeit ist es möglich, „Pseudo-Teilnehmer“ eindeutig zu identifizieren und dementsprechend zu belangen. Auf der anderen Seite ist die Möglichkeit einer Anmeldung durch Dritte ebenso auszuschließen, wie die Eingabe von unsinnigen Anmeldedaten. Es entsteht eine für beide Seiten verläßliche Kursbelegung, die vor allem bei Veranstaltungen von Bedeutung ist, in denen die Nachfrage das Angebot an Plätzen übersteigt.

Die nachträgliche Kontrolle der Teilnehmer im Rahmen der Veranstaltungen ebenso die Ahndung von Mißbräuchen obliegt den Mitarbeitern der betreffenden Professur. Dabei unterscheidet sich die Vorgehensweise sowie der organisatorische Ablauf nicht von der bisherigen Lösung, mit dem Unterschied, daß kein Teilnehmer die Anmeldung mehr abstreiten kann.

Bei der Realisierung muß – wie bei anderen Smart-Card-Anwendungen auch – insbesondere darauf geachtet werden, daß alle Studierenden auch tatsächlich die Möglichkeit haben, die Anmeldung wahrzunehmen. Dabei ist zu berücksichtigen, daß die Termine und Fristen von den Professuren selbst festgelegt werden und dadurch im ganzen Semester sowie in der vorlesungsfreien Zeit stattfinden können.

4.3.2 Professuren: An- und Abmeldungen zu sonstigen Veranstaltungen

An dieser Stelle soll noch kurz auf die Anmeldungen zu nicht-prüfungsrelevanten Veranstaltungen eingegangen werden. Darunter fallen sämtliche Anmeldungen zu außercurricularen Veranstaltungen wie Exkursionen, Vorträge oder Workshops, die von den Professuren oder sonstigen Organisationseinheiten[133] angeboten werden. Grundsätzlich gelten dabei die gleichen Anforderungen wie für die zuvor diskutierten Anmeldungen zu Lehrveranstaltungen, aber aufgrund der unterschiedlichen Folgen macht eine Unterscheidung Sinn.

Auch hier ist das Ziel, eine für alle Teilnehmer verläßliche und verbindliche Teilnehmerliste zu erhalten; in diesem Fall stellt eine irregulär belegte Veranstaltung zwar ein Ärgernis dar, wirkt sich aber nicht direkt auf die Studien- oder Semesterplanung der Studierenden aus, die sich nicht mehr anmelden konnten. Aber auch hier sind je nach Art der Veranstaltung Szenarien denkbar, in denen die Auswirkungen ungleich intensiver sind. Man denke bspw. an Exkursionen, die nur mit einer ausreichend großen Teilnehmerzahl überhaupt durchzuführen sind. Daher ist bei diesen Veranstaltungen im Einzelfall zu entscheiden, welchen Grad an Verbindlichkeit eine Anmeldung aufweisen muß. Dies gilt vor allem vor dem Hintergrund, daß sich bestimmte Veranstaltungen auch an (universitäts-) externe Interessenten richten. Es muß daher ein Ausgleich zwi-

133 Wenn im Folgenden von allein von Professuren die Rede ist, bezieht sich dies grundsätzlich auch auf andere WPS-nutzende Organisationseinheiten.

schen Verbindlichkeit auf der einen und Flexibilität bzw. Verfügbarkeit auf der anderen Seite stattfinden. Es bietet sich daher an, bei dieser Art von Veranstaltungen auf jeden Fall eine alternative Anmeldemöglichkeit zu schaffen. Ansonsten sind die Anforderungen die gleichen wie bei den Anmeldungen zu den Lehrveranstaltungen.

4.3.3 Professuren: Vertrieb/Absatz/Verteilung von Materialien

Der/die Vertrieb/Absatz/Verteilung von Materialien bezieht sich in diesem Zusammenhang auf alle schützenswerten Informationen, die von den betreffenden Organisationseinheiten veröffentlicht, aber lediglich einem ausgewählten Adressatenkreis zugänglich gemacht werden sollen. Das betrifft in erster Linie die von den Organisationseinheiten im WPS-Modul „File Service“ eingestellten Dokumente. Vereinfachend, aber zutreffend kann man dabei auch von „Downloads“ sprechen. Im Bereich der Professuren sind dies z. B. bereitgestellte Lehrmaterialien und Prüfungsergebnislisten. Aber auch der von der Fachschaft angebotene Klausurenservice gehört dazu.

Ziel ist es, durch den Einsatz von Smart Cards die Probleme bisheriger Sicherheitslösungen in diesem Bereich zu überwinden.[134] Im Wesentlichen geht es dabei um Verteilung von Zugriffsrechten an einzelne Adressaten. So sollen bspw. nur die Teilnehmer einer Vorlesung auch Zugriff auf die Lehrmaterialien erhalten. Um dies zu gewährleisten, müßte eine individuelle Authentifizierung stattfinden und dafür alle Adressaten oder Teilnehmer bekannt sein. Eine solche Forderung ist sicherlich nicht immer zu erfüllen. Und nicht zuletzt, da sich dadurch auch die Sicherheitsmöglichkeiten grundlegend ändern, ist an dieser Stelle eine Einteilung in Informationen an einen bekannten und an einen anonymen Adressatenkreis sinnvoll.

In den meisten Fällen werden die Adressaten (weitgehend) anonym sein. Dabei sei insbesondere auf die Massenveranstaltungen der ersten Studienabschnitte hingewiesen; weder die einzelnen Namen noch die Matrikelnummern der Teilnehmer sind dabei bekannt. Grundsätzlich sind in diesem Zusammenhang die Teilnehmer jeder Veranstaltung anonym, es sei denn, eine Anmeldung bei der betreffenden Professur ist für den Besuch zwingend erforderlich. Die Sicherungsmöglichkeiten zur Verteilung der Zugriffsrechte sind daher vor allem durch die Anonymität der Adressaten beschränkt. Denkbar ist in diesem Fall eine Sicherung, die lediglich allen Smart-Card-Besitzern (Studierende) exklusiven Zugang zu den Informationen gewährt und eventuell den Abruf protokolliert. Eine solche Aufzeichnung der Daten ist aber datenschutzrechtlich nicht ganz unproblematisch und könnte eventuell auf Widerstand bei den Studierenden stoßen.

134 Vgl. Kapitel 3.3.2.3 Probleme und Unzulänglichkeiten bisheriger Sicherheitslösungen.

Sind die Adressaten hingegen bekannt, stehen weitaus mehr Sicherungsmöglichkeiten zur Verfügung. Dies ist bspw. im Rahmen von Seminaren und sonstigen anmeldepflichtigen Veranstaltungen der Fall.[135] Dabei sind die Teilnehmer im Vorfeld durch die Anmeldung bekannt. Ihnen kann von daher exklusiv der Zugang zu bestimmten Informationen gewährt werden. Dazu muß das System in der Lage sein, die Anmeldedaten zur späteren Verteilung der Zugriffsrechte zu nutzen, so daß bspw. nur die angemeldeten Seminarteilnehmer berechtigt sind, die zugehörigen Lehrmaterialien abzurufen. Ein besonderes Anwendungsfeld bildet in diesem Zusammenhang die Veröffentlichung von Klausurergebnislisten durch die Professuren. In diesem Fall findet die Anmeldung nicht bei den Professuren statt, sondern beim Prüfungsamt.[136] Dabei sind den Professuren die Prüfungsteilnehmer durch den Datenaustausch mit dem Prüfungsamt bekannt und die Verteilung der Ergebnisse könnte ausschließlich an die Teilnehmer erfolgen. Welche Art der Zugriffsverteilung letztendlich zum Einsatz kommt, sollte den zuständigen Organisationseinheiten überlassen werden. Auch wenn in den meisten Fällen wohl auf die unbestimmte (anonyme) Lösung zurückgegriffen werden muß, sollte das System trotzdem in der Lage sein, beide Lösungen anzubieten.

Ein weiteres Feld, welches an dieser Stelle Beachtung finden muß, ist das Angebot an Arbeitspapieren der Professuren. Dabei ist ein „Smart-Card-gesichertes“ Angebot an externe Kunden nicht möglich und die bisherige (First-Gate-) Lösung sinnvoll und praktikabel. Anders bei internen Kunden; dabei könnte den Studierenden der Zugang durch die Nutzung der Smart Card gewährt werden. Soll ein solches Angebot auch für die Studierenden kostenpflichtig sein, könnte eine alternative Abrechnungsmethode vereinbart werden. Eine eindeutige Identifizierung der Kunden ist in jedem Fall möglich. Daher ändern sich die organisatorischen Abläufe lediglich in diesem Punkt, da nun eine Stelle geschaffen werden muß, die die Abwicklung des internen Vertriebs übernimmt. Sieht man einmal von den erforderlichen Nutzungsmöglichkeiten für die Studierenden ab, sind durch die bisherigen Lösungen alle organisatorischen und technischen Anforderungen gegeben.

4.3.4 Professuren: Evaluationen von Lehrveranstaltungen

Hauptproblem der Online-Evaluationen ist es, sicherzustellen, daß auch nur diejenigen eine Veranstaltung bewerten, die auch tatsächlich an dieser teilgenommen haben. Dabei muß zudem gewährleistet werden, daß sich jeder Teilnehmer auch nur einmal an der

135 Vgl. Kapitel 4.3.3 Professuren: Vertrieb/Absatz/Verteilung von Materialien und Kapitel 4.3.4 Professuren: Evaluationen von Lehrveranstaltungen.

136 Vgl. Kapitel 4.3.6 Prüfungsamt: An- und Abmeldungen zu Prüfungen.

Evaluation beteiligt. Von diesen beiden Aspekten hängt im Grunde die Qualität und Aussagekraft einer Evaluation ab.

Von daher sind die Anforderungen eigentlich klar zu formulieren. Als erstes muß das System in der Lage sein, nur die tatsächlichen Teilnehmer einer Veranstaltung zur Bewertungsabgabe zuzulassen. Dabei begegnet man in Bezug auf die Bekanntheit des Adressatenkreises der gleichen Problematik, wie bei der Verteilung der Zugriffsrechte auf schützenswerte Materialien.[137] Aber in diesem Fall ist das Problem der Anonymität – ähnlich wie bei der Veröffentlichung der Klausurergebnisse – unter Zuhilfenahme der Klausuranmeldungen zu lösen und nur die Prüfungsteilnehmer zur Bewertungsabgabe zuzulassen. Nachteilig an dieser Lösung ist sicherlich, daß die Menge an Teilnehmern, die nicht an der Prüfung teilnehmen von der Evaluation ausgeschlossen würden. Die zweite Anforderung ist, sicherzustellen, daß jeder nur eine Bewertung abgibt. Es muß dementsprechend protokolliert werden, wer bereits an der Evaluation teilgenommen hat. Aber da die Bewertung im Grunde anonym erfolgen soll, ist an dieser Stelle zu gewährleisten, daß dabei keine Daten aufgezeichnet werden, die einen Rückschluß auf die abgegebene Bewertung zulassen.

Die Bedeutung dieses Aspekts ist sicherlich nicht zu unterschätzen. Es ist davon auszugehen, daß von Seiten der Studierenden in dieser Hinsicht arge Bedenken bestehen. Nicht zuletzt da es sich bei Bewertungen in einem Über- und Unterordnungsverhältnis immer um eine heikle Sache handelt; könnte es doch dazu führen, daß die Evaluation aus der Befürchtung negativer Konsequenzen entweder nicht wahrheitsgemäß durchgeführt oder sogar im Ganzen verweigert wird. In abgewandelter Form begegnet man hier der gleichen Problematik wie bei den Diskussionsforen.

4.3.5 Diskussionsforen

Der Einsatz der Smart Card im Bereich der Diskussionsforen ist sicherlich sehr umstritten. Dennoch sollen im Folgenden verschiedene Funktionalitäten in diesem Bereich diskutiert werden, nicht zuletzt da diese Kommunikationsmöglichkeit einige Probleme aufwirft, die durch den Einsatz der Smart Card behoben werden könnten.[138]

Grundsätzlich finden sich für die Smart Card zwei voneinander unabhängige Einsatzgebiete im Bereich der Diskussionsforen. Zum einen kann der Zugriff auf bestimmte Foren beschränkt und zum anderen kann die aktive Teilnahme nur in Verbindung mit einer eindeutigen Identifizierung erlaubt werden. Erstes ist sicherlich weniger problematisch, da es im Grunde keine wesentliche Neuerung zu den bisherigen Schutzmecha-

137 Vgl. Kapitel 4.3.3 Professuren: Vertrieb/Absatz/Verteilung von Materialien.

138 Vgl. zu den Problemen der Diskussionsforen insbesondere den Abschnitt über die Fachschaft in Kapitel 3.2.1.3 Sonstige Organisationseinheiten.

nismen der Foren[139] darstellt. Da hier lediglich die Vertraulichkeit der Beiträge sichergestellt werden soll, gelten dabei die gleichen Möglichkeiten und Voraussetzungen wie beim Zugriffsschutz bei dem/der Vertrieb/Absatz/Verteilung von Materialien.[140]

Die Hauptprobleme, die aus der Anonymität der Diskussionsteilnehmer entstehen, können im Grunde nur durch den zweiten Einsatzbereich der Smart Card gelöst werden. Dabei wird den Teilnehmern eine aktive Beteiligung nur in Verbindung mit einer eindeutigen Identifizierung erlaubt. In der Praxis bedeutet dies, daß jeder Beitrag auch tatsächlich einer realen und bekannten Person zugeordnet werden kann. Das macht zum einen offizielle Aussagen (bspw. von Seiten der Professoren) möglich und zum anderen wird durch die Aufhebung der Anonymität die Gefahr von unsachlichen oder beleidigenden Beiträgen nahezu ausgeschaltet. Sollte dies in Ausnahmefällen dennoch passieren, kann der „Schuldige“ eindeutig identifiziert, von der Teilnahme ausgeschlossen und/oder das Vergehen auf sonstigem Wege geahndet werden.

Die Foren auf diese Art und Weise zu schützen birgt aber auch erhebliche Nachteile und Gefahren. Es ist anzunehmen, daß unter diesen Umständen vor allem auf (auch konstruktive) Kritik weitgehend verzichtet wird und die Foren daher ihrer Funktion nicht mehr gerecht werden können. Im Grenzfall könnte es sogar zu einem vollständigen Boykott der Diskussionsforen kommen. Das gilt hauptsächlich für die „offenen“ Foren, wie sie bspw. von der Fachschaft angeboten werden, aber grundsätzlich auch für sämtliche fach- oder lehrveranstaltungsbezogene Diskussionen, in denen unter anderem auch die Möglichkeit zur Kritik besteht und bestehen sollte. Es zeigt sich an dieser Stelle ein Interessenskonflikt zwischen den Forenbetreibern und den Teilnehmern. Ein Kompromiß ist z. B. in Form einer vorherigen Registrierung mit der Smart Card denkbar, wobei die Teilnehmer ein Pseudonym wählen mit dem sie in den Foren agieren können. Bei dieser Lösung bliebe die Anonymität in der Diskussion zunächst gewahrt und die Betreiber könnten im Ausnahmefall Rückschlüsse auf die wahre Identität des Betreffenden ziehen. Dies setzt selbstverständlich ein hohes Maß an Vertrauen in die Forenbetreiber voraus und es ist fraglich, ob ihnen das auch von Seiten der Teilnehmer ohne weiteres entgegengebracht wird.

Auch darf nicht vergessen werden, daß dieser Kommunikationskanal zudem verstärkt von universitätsexternen Teilnehmern genutzt wird, um sich bspw. über das „Studentenleben“ in Gießen, das Klima am Fachbereich und vieles mehr in Form eines Meinungsaustausches zu informieren. Diese Anspruchsgruppe würde vollständig aus der (aktiven) Diskussion ausgeschlossen werden. Von daher ist auch an dieser Stelle genau abzuwägen, in welchen Bereichen welche Art des Schutzes auch tatsächlich angemes-

139 Vgl. Kapitel 3.3.2.1 Merkmale und Funktionsweise.

140 Vgl. Kapitel 4.3.3 Professuren: Vertrieb/Absatz/Verteilung von Materialien.

sen ist. Insbesondere muß geklärt werden, wie mit externen Teilnehmern verfahren wird.

Die organisatorischen und technischen Rahmenbedingungen zum Betrieb der Diskussionsforen sind bereits vorhanden. Durch einen Einsatz der Smart Card würden die zuständigen Mitarbeiter sogar entlastet werden.

4.3.6 Prüfungsamt: An- und Abmeldungen zu Prüfungen

Dieses erste „WPS-externe“ Anwendungsgebiet bezieht sich vordergründig auf den Problembereich der Massenanmeldungen beim Prüfungsamt. Wie bereits im Rahmen der Situationsanalyse geschildert, kommt es in diesem Bereich vor allem zu den Stoßzeiten immer wieder zu unnötigen Wege- und Wartezeiten für die Studierenden und zu einer erhöhten Arbeitsbelastung für die Mitarbeiter des Prüfungsamts. Die medienbruchbehaftete Verarbeitung der Anmeldungen führt nicht selten zu Fehlern und Unstimmigkeiten.[141] Aus diesem Grund lassen sich für das System grundsätzlich zwei Kernziele festhalten: Zum einen muß durch den Einsatz der Smart Card eine Entzerrung des Anmeldeprozesses bewirkt werden. Dies bedeutet, eine Anmeldung[142] muß zeit- und ortsunabhängig über den gesamten Zeitraum der Anmeldefrist möglich sein. Zum anderen muß durch eine medienbruchfreie Verarbeitung der Daten die Anzahl möglicher Fehlerquellen und die Arbeitsbelastung der Mitarbeiter reduziert werden. Gerade der letzte Punkt stellt an das System eine besondere Forderung. Eine echte Reduktion der Belastung tritt nur ein, wenn die getätigten Anmeldungen im Sinne der Prüfungsordnung einwandfrei sind und auf eine aufwendige „manuelle“ Nachbearbeitung verzichtet werden kann. Von daher muß das gesamte System mit einer gewissen Intelligenz ausgestattet sein, die die Anmeldungen auf Fehler überprüft bzw. fehlerhafte oder logisch unsinnige Eingaben verhindert. Dies betrifft vor allem grundlegende Fälle wie bspw. eine Kontrolle der prüfungsrechtlichen Vorraussetzungen zur Anmeldung.

Zur Pflege des Systems muß ein Mitarbeiter abgestellt werden, der den reibungslosen Ablauf sowie die Stabilität des Systems sicherstellt. Vor allem ist dabei der Eingriff bei fachlichen Ausnahmefällen und die schnelle Behebung technischer Fehler von Bedeutung. Daher muß der betreffende Mitarbeiter in der Lage sein, das System fachlich und technisch zu betreuen.

Sicherheitstechnisch sind die Anforderungen an das System als recht einzustufen. Dies liegt vor allem daran, daß die Anmeldungen zu Prüfungen verbindlich, mit allen prüfungsrechtlichen Konsequenzen erfolgen müssen. Demnach muß das System minde-

141 Vgl. Kapitel 3.2.1.2 Prüfungsamt.

142 Ist in diesem Zusammenhang von Anmeldungen die Rede, bezieht sich dies grundsätzlich auch auf die Möglichkeit eines Prüfungsrücktritts (Abmeldung) innerhalb der Fristen.

stens das gleiche Sicherheitsniveau aufweisen wie die bisherige papierbasierte Lösung mittels persönlicher Unterschrift. Das betrifft vor allem die Sicherstellung der Authentizität der Studierenden und die damit verbundene Nicht-Abstreitbarkeit einer getätigten Anmeldung. Des weiteren müssen bei einer elektronischen Lösung – wie bei allen weiteren auch – sämtliche daraus entstehenden Sicherheitsanforderungen Beachtung finden. Gerade hierbei muß sichergestellt sein, daß für die Studierenden ausreichende Möglichkeiten zur Nutzung der Web-Anmeldung bereitstehen. Nur dadurch ist das Ziel der Entzerrung des Anmeldeprozesses zu erreichen. Dies gilt vor allem vor dem Hintergrund, daß die Durchführung nur innerhalb vorgegebener Zeiträume möglich ist. Sollte sich herausstellen, daß eine solche Forderung nicht zu erfüllen ist, muß eine alternative Anmeldemöglichkeit geschaffen werden.

4.3.7 Prüfungsamt: Prüfungsergebnisse

An dieser Stelle soll auf den Problembereich der Noteneinsicht für die Studierenden eingegangen werden. Dabei beschränken sich die Ausführungen ausschließlich auf die vom Prüfungsamt veröffentlichten Ergebnisse, die derzeit in Form einer Leistungsübersicht von den Studierenden persönlich beantragt werden können.[143] Die meist im Vorfeld von den Professuren herausgegebenen Prüfungsergebnislisten wurden im Abschnitt „Vertrieb/Absatz/Verteilung von Materialien“ behandelt.

Durch eine Implementierung dieser Funktionalität soll den Studierenden die Möglichkeit gegeben werden, jederzeit eine aktuelle Übersicht über die erbrachten Studienleistungen zu erhalten. Dazu gehört neben der Noteneinsicht auch der Überblick über die verschiedenen Fachkonten und Fehlversuche. Dementsprechend müssen diese Daten vom Prüfungsamt gepflegt, aufbereitet und vorgehalten werden, so daß auch bei Ausnahmeregelungen, Fehlerfällen etc. fachkundige Mitarbeiter den Datenbestand anpassen können.

Grundsätzlich handelt es sich dabei um höchst sensitive Daten, die nur von den Studierenden selbst eingesehen bzw. abgerufen werden dürfen. Da eine Möglichkeit zur Manipulation der Daten unter allen Umständen verhindert werden muß, ist den Studierenden hier ein rein lesender Zugriff zu gewähren. Dadurch steht an dieser Stelle das Ziel der Geheimhaltung der Daten im Vordergrund. Soll es weiterhin auch möglich sein, die erhaltene Notenübersicht als prüfungsamtlichen Leistungsnachweis z. B. im Rahmen von Bewerbungen zu verwenden, muß den Studierenden zusätzlich eine Druck- oder Speicherfunktion angeboten werden. In diesem Fall sind die Anforderungen an die Integrität und die Authentizität der Daten ungleich höher. Dabei ist unbedingt sicherzustel-

143 Vgl. Kapitel 3.2.1.2 Prüfungsamt.

len, daß vor, während und nach dem Speicher-/Druckvorgang keine Möglichkeit zur Manipulation besteht.

Selbstverständlich müssen auch hier ausreichende Möglichkeiten zur Nutzung bereitstehen, wenngleich diese Funktionalität im Gegensatz zu den Anmeldungen beim Prüfungsamt nicht von zentraler Bedeutung für den Studienerfolg ist und zudem auch noch auf bisherigem (Papier-)Wege nutzbar ist. In diesem Zusammenhang ist die Möglichkeit einer Online-Noteneinsicht eher als „Nice to have“ für die Studierenden zu sehen, was gleichzeitig den Arbeitsaufwand für die Mitarbeiter des Prüfungsamts verringert.

4.3.8 Professuren: WPS-Administration

Wie bereits im Rahmen der Situationsanalyse dargelegt, fällt diese Aufgabe in den Bereich der Mitarbeiter, und da diese nicht alle mit der Uni-Chipkarte ausgestattet sind, kann in diesem Zusammenhang lediglich ein alternativer Smart-Card-Einsatz in Betracht gezogen werden. Von daher muß das System zweierlei Zugangsmöglichkeiten anbieten: Einen personalisierten Zugang mittels der Smart Card und den bisherigen bereichsindividuellen Zugang.

Allerdings wirft diese Unterscheidung einige Probleme auf, die nicht zuletzt in dem gesamten Rechtesystem des WPS begründet sind. Im Grunde müßte zunächst die gesamte Benutzerverwaltung des WPS personalisiert werden, d. h., jeder Mitarbeiter müßte einen eigenen individuellen Zugang (bspw. Benutzername/Paßwort-Kombination) erhalten. Anschließend könnte die Anmeldung am System alternativ mit der Smart Card realisiert werden. Diese Forderung ist in sofern von Bedeutung, als daß ansonsten den Smart-Card-Nutzern ausschließlich Nachteile entstehen (können). Warum sollte man seinen persönlichen Account nutzen, wenn auch ein „anonymer“ Zugang zur Verfügung steht? Außerdem wären nur dadurch die geschilderten Probleme zu lösen.[144]

Eine solche Umstellung wirft dementsprechend weitreichende Änderungen in organisatorischer sowie technischer Hinsicht auf. Nach einer Umstellung auf ein personalisiertes Zugangssystem müssen solche „Accounts“ auch verwaltet und gepflegt werden. Demnach ist die technische Ausstattung der Professuren entsprechend anzupassen.

4.3.9 ITSeC: PC-Pool Account

Bezogen sich die bisher diskutierten Anwendungsgebiete ausschließlich auf den Einsatz der Smart Card als Sicherheits- und Zugangsmedium für Internet- bzw. WPS-basierte Funktionalitäten, soll an dieser Stelle auf die Verwendung an Rechnersystemen inner-

144 Vgl. Kapitel 3.3.2.3 Probleme und Unzulänglichkeiten bisheriger Sicherheitslösungen.

halb des Fachbereichs eingegangen werden. Das betrifft den Problembereich der Accountvergabe zur Nutzung des PC-Pools.[145]

Dabei geht es in erster Linie um die Lösung des Account-Problems. Um dieses Problem zu umgehen, müssen die Systeme zur Benutzerverwaltung auf die Nutzung der Smart Card als Zugangsmedium umgestellt werden. Grundsätzlich wäre eine vorherige Anmeldung nicht mehr erforderlich, ist aber aus Verwaltungsgründen sinnvoll. Denkbar ist dabei eine Internet-basierte Möglichkeit zur Aktivierung der Smart Card als Zugangsmedium für die Rechner des PC-Pools. Des weiteren ist zu überlegen, ob Studierenden ohne PC-Pool-Account die Möglichkeit gegeben wird, die Rechner im Sinne eines „Thin-Clients“ bspw. zum Surfen im Internet nutzen zu können. Den Benutzern stünden in diesem Fall keine Verzeichnisse zum Ablegen von Dateien und nur eine begrenzte Menge an Anwendungssoftware zur Verfügung. Dies würde jedoch grundsätzlich allen Studierenden ermöglichen, Smart-Card-Anwendungen zu nutzen und insbesondere die Klausuranmeldungen im PC-Pool durchzuführen.

4.4 Server-/Client-seitige Anforderungen

4.4.1 Hardware

Server-seitig gelten im Grunde die gleichen Anforderungen wie an den Betrieb des WPS. Demnach scheint ein Server mit folgender Ausstattung angemessen:

- 2x Intel Xeon 2,4 GHz (Gigahertz) Prozessor
- 2 GB (Gigabyte) Arbeitsspeicher
- 2x 36 GB Small Computer System Interface (SCSI-) Festplatte
- Gigabit Netzwerk-Adapter
- Digital Audio Tape (DAT-)Streamer 40 GB[146]

Dies gilt ebenso für die Server-Ausstattung des Prüfungsamts. Dabei ist allerdings zu beachten, daß die benötigte Leistungsfähigkeit der Hardwarekomponenten, wie beim Betrieb des WPS in erster Linie von der Nutzungsintensität abhängt. Vor allem da die Beanspruchung der Leistungsreserven bei SSL-Anwendungen um ein vielfaches höher ist als bei „normalen“ ungesicherten Anwendungen, muß dieser Aspekt gesondert berücksichtigt werden. Davon betroffen sind insbesondere die Systeme des Prüfungsamts, bei denen es bspw. zu den Anmeldezeiten zu einer wesentlich höheren Nutzungsintensität kommt. Den daraus resultierenden Leistungs- und Speicherproblemen ist wenn möglich im Vorfeld entsprechend vorzubeugen. Zumindest sollten geeignete Schutz-

145 Vgl. dazu den Abschnitt über den PC-Pool in Kapitel 3.2.1.3 Sonstige Organisationseinheiten .

146 Vgl. Schwickert, Axel C.; Grund, Henning: Web Content Management – Grundlagen und Anwendungen mit dem Web Portal System V.2.5, a. a. O., S. 24 f.

mechanismen installiert werden, die im Falle eines Systemabsturzes drohenden Datenverlust verhindern.

Auf Seiten der Clients muß im Grunde lediglich ein handelsübliches PC-System mit Internetanbindung und Chipkartenleser vorhanden sein. Dazu ist der Chipkartenleser „KAAN Standard Plus“ der Firma Kobil oder ein kompatibles Modell an den PC anzuschließen.[147] Dies kann alternativ am Universal Serial Bus (USB) oder am seriellen (Com-) Port geschehen. In letzterem Fall muß allerdings zusätzlich ein PS/2 (Personal System 2)-Anschluß zur Stromaufnahme vorhanden sein. Weitere Hardwareanforderungen in Bezug auf die Leistungsfähigkeit, Speicherkapazität etc. ergeben sich in erster Linie aus den Anforderungen der benötigten Software. Für den performanten Betrieb läßt sich an dieser Stelle ein System mit mindestens folgender Ausstattung empfehlen:

- Intel Pentium III 500 MHz (Megahertz) Prozessor
- 128 MB (Megabyte) Arbeitsspeicher
- 10 GB Festplatte
- 56 Kbit (Kilobit)
- V.90 kompatibles Modem oder ein ISDN-Adapter

4.4.2 Software

Auf den zentralen Server-Rechnern muß ein Web Server mit zugehöriger SSL Engine installiert sein. Des weiteren ist für bestimmte Anwendungen eine leistungsfähige Datenbank vorzuhalten. Auf welcher Plattform (Windows, Linux etc.) die Komponenten laufen, ist im Grunde nebensächlich. Es bietet sich daher gerade im Falle einer Integration in das WPS an, die vorhandene LAMP-Architektur beizubehalten und zu nutzen.[148] Diese ist nur um die SSL Engine und die zugehörigen Konfigurationseinstellungen zu ergänzen, die – um es einfach auszudrücken – eine Kommunikation zwischen Web Server und dem Chipkartenleser der Clients ermöglichen. Bei einer Integration in das WPS, bzw. in das SPIC müssen die entsprechenden Module selbstverständlich auf dem Server installiert sein. Auf Seiten des Prüfungsamts gelten die gleichen Anforderungen, nur daß hier das „Chipkarten-fähige“ FlexNow korrekt konfiguriert bereit stehen muß.

Die Clients müssen lediglich über ein laufendes System verfügen, auf welchem ein aktueller Web Browser sowie die mitgelieferte Chipkartensoftware installiert ist. Der Web Browser muß als Interface-Software X.509 Zertifikate unterstützen.[149] Beide Programme und auch die Gerätetreiber für den Chipkartenleser sind für mehrere Plattformen erhält-

147 Vgl. dazu Kapitel 3.3.1.1 Aussehen und Inhalt.

148 Vgl. Kapitel 3.3.2.1 Merkmale und Funktionsweise.

149 Dies ist derzeit bei nahezu allen aktuellen Web Browsern der Fall, z.B.: Microsoft Internet Explorer, Netscape 4.7x und 7.x, Mozilla.

lich.[150] Gerade da es sich in diesem Zusammenhang um sicherheitskritische Anwendungen handelt und dieser Aspekt von Seiten der Benutzer oft vernachlässigt wird, soll an dieser Stelle nochmals auf die Notwendigkeit eines aktuellen Anti-Viren-Programms (Viren-Scanner) hingewiesen werden. Zwar kann eigentlich durch die Nutzung der Smart Card nahezu kein Schaden angerichtet werden, aber nicht zuletzt aus Gründen der Systemsicherheit und -stabilität sollte ein Viren-Scanner auf jedem System installiert werden. Dabei kann auf verbreitete Freeware- bzw. Shareware-Programme zurückgegriffen werden.

4.5 Priorisierung der Funktionalitäten

Alle im letzten Kapitel diskutierten Anwendungsgebiete sind im Grunde erfolgversprechende Einsatzfelder für erste Smart-Card-Anwendungen am Fachbereich. Dennoch müssen im Rahmen derart weitreichender Änderungen bestimmte Anwendungsfelder priorisiert werden, um dadurch eine Auswahl der im Anschluß prototypisch zu realisierenden Funktionalitäten zu treffen. Zwar sind im Grunde alle Voraussetzungen zur Implementierung aller Funktionalitäten nicht zuletzt in Form von vorhandenem Know-How an der Professur Wirtschaftsinformatik geschaffen, dennoch mangelt es an nötigen freien Entwicklungskapazitäten. Und vor allem da sicherlich einige Probleme und Gefahren nicht im Vorfeld eindeutig zu identifizieren und dadurch nicht zu berücksichtigen sind, macht ein solches prototypisches Vorgehen Sinn. Die daraus gewonnenen Erfahrungen können im Anschluß helfen, weitere Funktionalitäten zu konzipieren und zu entwickeln.

Die ersten Einsatzgebiete sollen insbesondere eine Testplattform bilden und daher möglichst keine großen Umstellungen in Organisation und Technik nach sich ziehen. Des weiteren sollten diese für alle Teilnehmer einen echten Zusatznutzen darstellen, da ansonsten die Gefahr besteht, daß die Anwendungen durch die mangelnde Akzeptanz nicht zum Einsatz kommen bzw. genutzt werden. Gerade vor dem Hintergrund herrschender Skepsis von Seiten der Kunden, spielt dieser Aspekt eine gewichtige Rolle. Aus diesen beiden Kernanforderungen an die zu entwickelnden Funktionalitäten, lassen sich zwei Hauptdeterminanten zur Entscheidungsfindung ableiten: Der Implementierungsaufwand und der Zusatznutzen.

Der Implementierungsaufwand beschreibt dabei die organisatorische und technische Realisierbarkeit auf Basis der zuvor geschilderten Voraussetzungen. Weiterhin finden dabei auch Abhängigkeiten von anderen Systemen (bspw. des Prüfungsamts) Berück-

150 Offiziell unterstützt werden zur Zeit folgende Betriebsysteme: Windows 98(SE), Windows NT, Windows 2000 und XP, LINUX, Solaris, FreeBSD und OpenBSD, vgl. Partosch, Günter: Informationen zur Chipkarte, Information über Chipkarten-Leser, a. a. O.

sichtigung. Die zweite Determinante, der Zusatznutzen, versucht wiederzugeben, inwieweit durch eine Implementierung der betreffenden Funktionalität die Ziele der Kunden und Anbieter im Vergleich zu der vorherrschenden Lösung besser erfüllt werden. Sie bildet somit auch einen Gradmesser für die erwartete Akzeptanz der Anwendung. Dabei ist zu beachten, daß im Falle konfliktbehafteter Ziele der Teilnehmer der Nutzen jeweils gegeneinander abgewogen wurde. Grundsätzlich gilt, daß es sich bei der Bewertung beider Determinanten lediglich um subjektive Einschätzungen handelt, die im Wesentlichen nicht im Vorfeld überprüft werden konnten. Die in der folgenden Abbildung dargestellte Einschätzung soll auf Basis der Anforderungen dementsprechend nur als erste Entscheidungshilfe dienen.

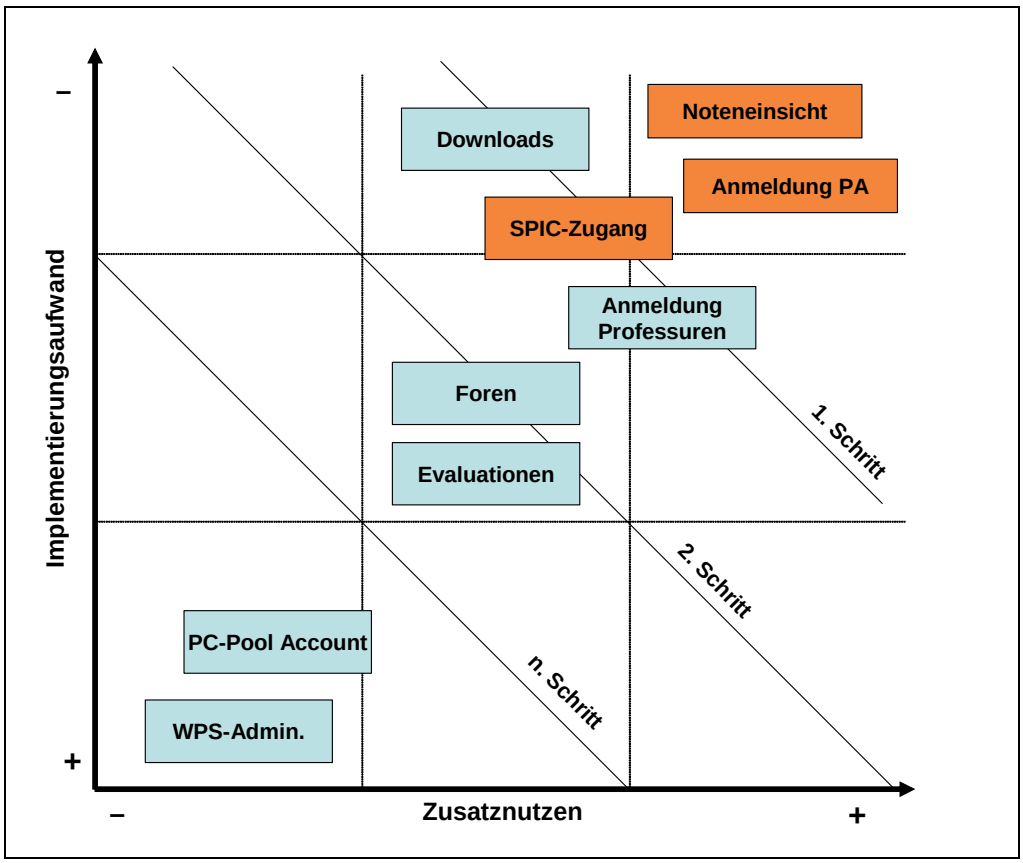

Abb. 14: Prioritätsmatrix der fachlichen Anwendungsgebiete

Die zuvor diskutierten Anwendungsgebiete wurden in der Matrix anhand der Ausprägung der beiden Determinanten eingeordnet. Dabei wurden die neuen bzw. die durch den Einsatz der Smart Card erst ermöglichten Funktionalitäten farblich hervorgehoben. Auf den ersten Blick zu erkennen ist, daß die Noteneinsicht und die Anmeldung beim Prüfungsamt (PA) den höchsten Zusatznutzen und gleichzeitig den geringsten Implementierungsaufwand auslösen. Das ist auch nicht weiter verwunderlich, hält man sich vor Augen, daß diese Funktionalität von Seiten der Kunden, als auch von den Mitarbeitern als vorteilhaft eingeschätzt wird und der (Zusatz-) Nutzen für beide sehr hoch ist.

Der geringe Implementierungsaufwand liegt vor allem daran, daß dabei auf die Leistung eines externen Systems (FlexNow) zurückgegriffen wird und daher diese Funktion nur noch navigatorisch eingebettet werden muß.[151] Nicht zuletzt soll dies auch im Rahmen der Implementierung des SPIC geschehen. Von daher nimmt der SPIC-Zugang in diesem Zusammenhang eine Sonderrolle ein. Um Mißverständnissen vorzubeugen, sei an dieser Stelle darauf hingewiesen, daß sich der als recht niedrig eingeschätzte Aufwand lediglich auf die Realisierung des Zugangs bezieht und nicht auf die Entwicklung des SPIC selbst. Der Zugang ist – um dies vorwegzunehmen – durch eine einfache Authentisierung der Benutzer am Server zu lösen. Das gilt ebenso für die Sicherung schützenswerter Materialien (Downloads), wobei die Einschätzung beider Determinanten auf der rudimentären Sicherung durch die Smart Card basiert.[152] Daraus resultiert auch der mittlere Zusatznutzen nicht zuletzt da die Probleme auf beiden Seiten (Kunden und Anbieter) nicht vollständig behoben werden. Etwas aufwendiger ist die Implementierung der Anmeldungen an den Professuren, weil dies höhere Anforderungen an die Datenintegrität und Authentizität sowie ein Datenbanksystem fordert. Dies gilt auch für die übrigen Anwendungsgebiete, auf die an dieser Stelle nicht weiter eingegangen werden soll. Anzumerken ist lediglich, daß sich die Einschätzung eines mittleren Zusatznutzens bei den Evaluationen und den (Diskussions-) Foren aus den Zielkonflikten der verschiedenen Teilnehmer ergibt.[153]

Aus der übersichtsartigen Darstellung läßt sich dementsprechend eine Art „Roadmap“ zur Implementierung der verschiedenen Smart-Card-Anwendungen erstellen. Es bietet sich an, in einem ersten Schritt die Anmeldungen beim Prüfungsamt und die Noteneinsicht zu realisieren. Im Zuge dessen ist zudem der Zugang zum SPIC als navigatorischer Rahmen und als erste Smart-Card-Anwendung innerhalb des WPS zu implementieren. Es bleibt daher festzuhalten, daß zunächst die farblich hervorgehobenen neuen Anwendungsgebiete verwirklicht werden.

4.6 Fazit der Anforderungsanalyse

Nach der Diskussion im letzten Kapitel hat sich herausgestellt, daß es Sinn macht, zunächst die drei priorisierten Anwendungsgebiete (SPIC-Zugang, Anmeldungen zu Prüfungen, Prüfungsergebnisse) zu realisieren. Zwar würden rein technisch gesehen viele

151 Vgl. Kapitel 3.3.4 Systeme des Prüfungsamts.

152 Gemeint ist dabei die unspezifische Sicherung, welche für den Zugriff lediglich eine gültige Smart Card fordert. Insbesondere der Aufwand wäre, bei einer spezifischen und personalisierten Lösung als ungleich höher einzuschätzen. Vgl. dazu Kapitel 4.3.3 Professuren: Vertrieb/Absatz/Verteilung von Materialien.

153 Vgl. Kapitel 4.3.4 Professuren: Evaluationen von Lehrveranstaltungen und Kapitel 4.3.5 Diskussionsforen.

andere Funktionalitäten im Prinzip den gleichen Aufwand[154] nach sich ziehen, stehen aber teilweise zahlreichen Akzeptanzproblemen gegenüber. Vor allem im Hinblick auf die Akzeptanz der Studierenden bietet sich ein schrittweises Vorgehen in diesem Zusammenhang an.[155] Nach der Verfügbarkeit von erfolgreichen und nutzbringenden Smart-Card-Anwendungen ist davon auszugehen, daß der Großteil der Adressaten mit zunehmendem Kontakt die Notwendigkeit und Sinnhaftigkeit solcher Sicherheitsmechanismen verstehen und akzeptieren werden.

Die technischen Anforderungen für die Systementwicklung sind vor allem durch die vorhandene PKI und Nutzung der WPS-Architektur nahezu vollständig gegeben. Dies gilt insbesondere auch im Hinblick auf die Realisierung weiterer Anwendungsgebiete, die in diesem ersten Schritt nicht zuletzt aufgrund begrenzter Entwicklungskapazitäten noch keine Berücksichtigung finden konnten. Zwar ist bis zur endgültigen Fertigstellung des SPIC noch einige Entwicklungsarbeit zu leisten, dennoch können die grundlegenden Zugriffsmechanismen bereits vorbereitet werden. Kein Einfluß besteht in dieser Hinsicht auf die Systeme des Prüfungsamts. Hingewiesen sei an dieser Stelle vor allem auf die Abhängigkeit von der externen Entwicklung von FlexNow. Selbst im Falle einer Terminverschiebung steht aber der vorläufigen Implementierung des SPIC ohne die betreffenden Funktionalitäten nichts im Wege. Dies gilt selbstverständlich nur unter der Voraussetzung, daß dafür genug Entwicklungspersonal verfügbar sowie der entstehende finanzielle Aufwand tragbar ist.

Im Folgenden soll daher die Implementierung des SPIC-Zugangs und die Möglichkeit eines „Single Sign On“ beschrieben werden. Dazu wird zunächst ein Überblick über das System und dessen grundlegender Architektur und Abläufe gegeben werden. Es folgt die Erläuterung der notwendigen technischen Anpassungen an der Server- und Client-Konfiguration. Abschließend soll kurz auf die Integration weiterer Funktionalitäten eingegangen werden.

154 Dies bezeiht sich, im Gegensatz zu Kapitel 4.5 lediglich auf die Einrichtung der Sicherheitsfunktionalitäten und nicht auf andere organisatorische und technische Änderungen im System (WPS).

155 Vgl. dazu insbesondere Abb. 14 Prioritätsmatrix der fachlichen Anwendungsgebiete.

5 Systementwicklung und Integration

5.1 Systembeschreibung

Gemäß den Anforderungen an das System der Anmeldung, soll es nur den betreffenden Studierenden möglich sein, auf das personalisierte SPIC und auf weitere Funktionalitäten zugreifen zu können. Das macht eine eindeutige Identifizierung der Benutzer unabdingbar. Des weiteren muß verhindert werden, daß die übertragenen Daten vom Benutzer oder von Dritten unberechtigterweise abgehört bzw. manipuliert werden können. Dabei ist auch insbesondere darauf zu achten, daß die Karte während des gesamten Vorgangs im Kartenleser steckt und diese auch nicht ausgetauscht werden kann.

Gelöst wird dies durch eine einseitige asymmetrische Authentisierung der Uni-Chipkarte am WPS-Server. Dazu wird auf das bekannte Challenge/Response-Verfahren zurückgegriffen, welches im Ergebnis eine sichere SSL-Verbindung zwischen Server und Client aufbaut.[156] Aus Benutzersicht stellt sich der ganze Vorgang wie folgt dar.

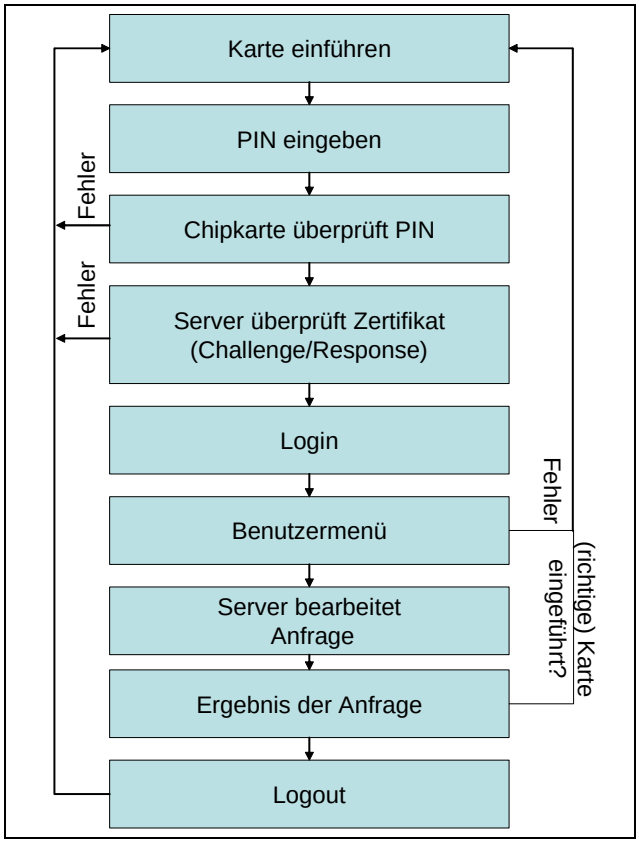

Abb. 15: Anwendungssicht des Benutzers

Zur Benutzeridentifikation wird der Studierende aufgefordert, seine Uni-Chipkarte in den Kartenleser einzuführen. Es folgt der Zufallszahlentausch im Rahmen der Chal-

156 Vgl. Kapitel 2.4.3 Verschlüsseln, signieren und authentisieren mit Smart Cards.

lenge/Response-Authentisierung am Server. Dabei muß sich der Benutzer mittels PIN-Eingabe gegenüber der Karte identifizieren. Abbildung 16 zeigt die Login-Maske zur Anmeldung am SPIC.

Abb. 16: Darstellung der Authentifizierungsmaske des SPIC

Bei der erstmaligen Anmeldung wird der Benutzer nachdem er auf „Authentifizieren“ geklickt hat, aufgefordert, seine Karte einzulegen und seine PIN einzugeben. Anschließend wird das Zertifikat (der öffentliche Schlüssel) des Benutzers auf Gültigkeit überprüft. Im Erfolgsfall ist der Benutzer authentisiert und eine sichere SSL-Verbindung aufgebaut. Nun gewährt der Server im Sinne eines „Single Sign On“ Zugriff auf die betreffenden Funktionalitäten. Die Authentisierung wird dementsprechend an weitere Anwendungen „durchgereicht“. Die folgende Abbildung zeigt anhand von Screenshots den Anmeldevorgang am SPIC und die Möglichkeit des Zugriffs auf eine geschützte Datei innerhalb eines Download-Centers ohne erneute Authentifizierung.

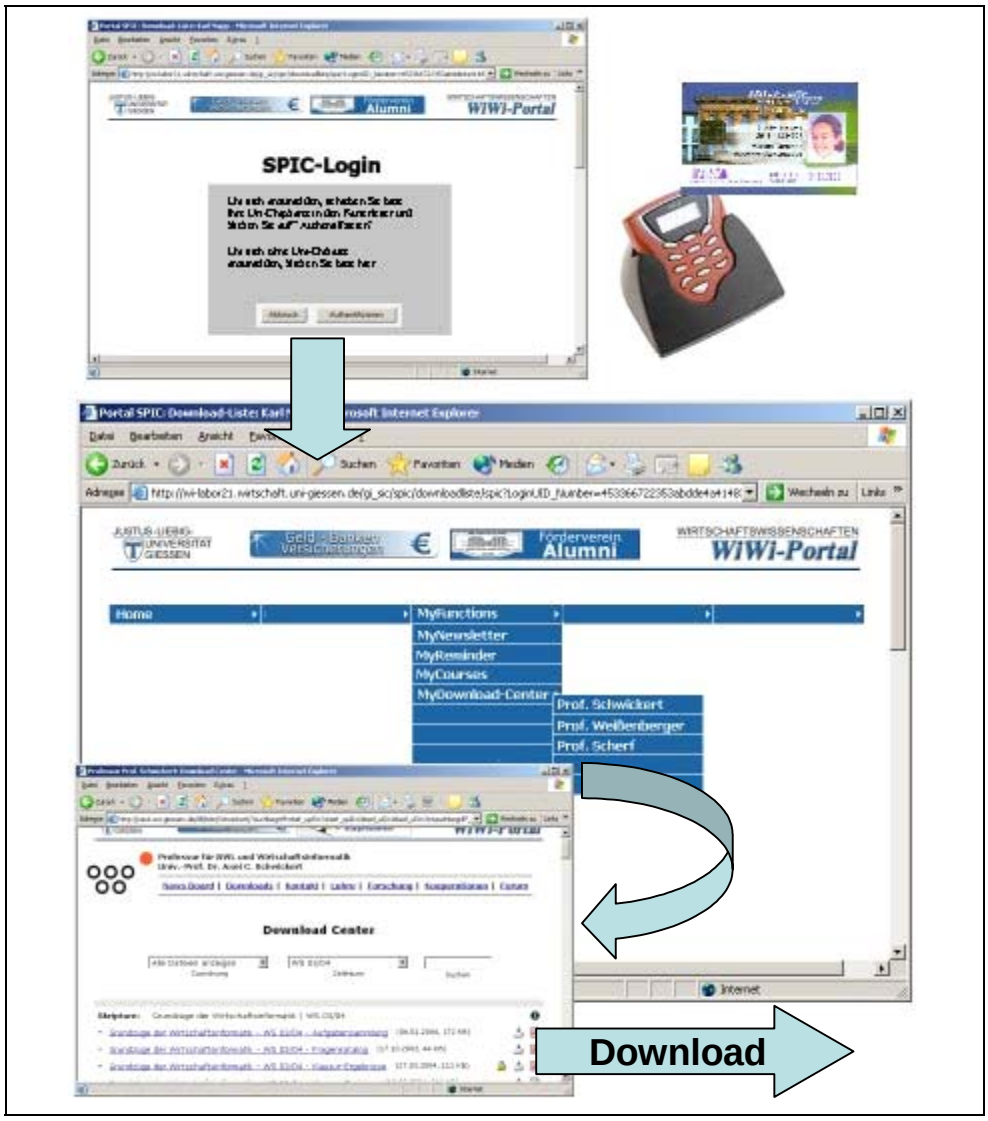

Abb. 17: Prinzip des SPIC „Single Sign On“

Dabei wird jedem Benutzer nach der erfolgreichen Authentisierung ein System-interner Schlüssel (ID) zugeordnet. Es bietet sich an, einen solchen aus den ausgelesenen Zertifikatsinformationen zu generieren. Unter dieser ID werden im Folgenden alle Datenbankeinträge abgelegt und dadurch eine spätere Zuordnung aller Einträge gewährleistet. Bei jeder Transaktion muß aber geprüft werden, ob sich die richtige Uni-Chipkarte durchgängig im Kartenleser befindet. Wird sie entfernt oder gegen eine andere Karte ausgetauscht, ist die Verbindung direkt zu unterbrechen und ein erneuter Anmeldevorgang zu fordern. Zum Ende muß ein Logout am System stattfinden, um dadurch die Benutzersitzung eindeutig zu beenden. Damit kein unnötiges Sicherheitsrisiko durch eine nicht beendete Verbindung eingegangen wird, muß jede Session mit einem „Time Out“ geschützt werden. Nach Ablauf einer voreingestellten Zeit ohne getätigte Aktion, wird der Benutzer automatisch abgemeldet.

5.2 Server-Konfiguration

Auf dem zentralen (Apache-)Web-Server müssen der öffentliche und private SSL-Schlüssel des Web Servers in Verzeichnissen vorgehalten werden, deren Pfad in der Konfigurationsdatei httpd.conf für den öffentlichen Schlüssel unter der Konfigurationsanweisung SSLCertificateFile und für den privaten Schlüssel unter der Konfigurationsanweisung SSLCertificateKeyFile im PEM-Format[157] angegeben werden.[158] Abbildung 18 zeigt die Konfigurationsanweisungen innerhalb des SSL-Konfigurationsbereiches des Apache-Servers. Alle im Folgenden gemachten Angaben werden im Konfigurationskontext des für SSL angelegten VirtualHost gemacht.

```
/* ------------ httpd.conf – Datei ---------------

<IfDefine SSL>
<VirtualHost wiwi.uni-giessen.de:443>
…
SSLCertificateFile /etc/httpd/ssl.crt/public-key.pem

SSLCertificateKeyFile /etc/httpd/ssl.crt/priv-key.pem
…
</VirtualHost>
</IfDefine SSL>
```

Abb. 18: Konfiguration des Apache-Servers bzgl. des öffentlichen und privaten Schlüssels

Da das Zertifikat des Web Servers durch das HRZ zertifiziert ist und dieses wiederum durch das DFN Toplevel-Zertifikat, müssen dem Web Server alle Zertifikate bis zum Toplevel-Zertifikat (Wurzelzertifikat, Root Certificate) bekannt gemacht werden.[159] Mit der Konfigurationsanweisung SSLCACertificatePath (SSLClientAuthentifikationPath) ist es möglich, dem Web Server alle Zertifikate bekanntzumachen. Dazu müssen alle Zertifikate in das anzugebende Verzeichnis im Dateisystem des Servers gelegt werden. Mittels des durch OpenSSL mitgelieferten Programms c_rehash werden die Dateien über einen Hash-Wert[160] gekennzeichnet, der als symbolischer Verweis angelegt wird und auf die Datei des Zertifikats verweist. Fehlt der Verweis eines Zertifikats, wird es nicht beachtet, der Apache-Server kann dieses Zertifikat dann nicht finden.[161, 162] Durch

157 Das PEM-Format entspricht den Spezifikationen für Privacy Enhanced Mail. Vgl. hierzu Kapitel 2.4.2 Zertifikate und Public-Key-Infrastruktur.

158 Vgl. Eilebrecht, Lars; Rath, Nikolaus; Rohde, Thomas: Apache Webserver – Installation, Konfiguration, Administration, 4., erweiterte und überarbeite Aufl., Bonn: mitp-Verlag 2002, S. 567 f.

159 Vgl. Kapitel 3.3.3 Die Zertifizierungsinstanz der Universität Gießen.

160 Vgl. hierzu Kapitel 2.4.1 Kryptographische Grundlagen ff.

161 Vgl. Eilebrecht, Lars; Rath, Nikolaus; Rohde, Thomas: Apache Webserver – Installation, Konfiguration, Administration, a. a. O., S. 569 f.

die Konfigurationsanweisung SSLVerifyDepth wird festgelegt, wie viele Zertifikate bis zum Wurzelzertifikate notwendig sind. Wird ein Client-Zertifikat direkt von einer CA ausgestellt ist der Wert Eins.[163] In der Universität Gießen muß der Wert also Zwei lauten, da das Client-Zertifikat des Web-Servers vom HRZ zertifiziert wurde.

Abbildung 19 zeigt die entsprechenden Anweisungen in der Serverkonfigurationsdatei innerhalb der SSL-VirtualHost-Konfiguration. Durch diese Anweisungen kann der Web Server dem Client auf unkomplizierte Weise alle Zertifikate bis hin zum Wurzelzertifikat senden. Der Client-Nutzer muß sich die verschiedenen Zertifikate dann nicht mehr manuell von den verschiedenen Web-Seiten des HRZ und des DFN herunterladen und installieren.

```
/* ------------ httpd.conf – Datei ---------------

<IfDefine SSL>
<VirtualHost wiwi.uni-giessen.de:443>
…
SSLCACertificatePath /etc/httpd/ssl.crt/

SSLVerifyDepth 2
…
</VirtualHost>
</IfDefine SSL>
```

Abb. 19: Konfiguration bzgl. aller Zertifikate bis hin zum Wurzelzertifikat

Ein Zugriff auf die Seiten des Web Servers, die eine Authentisierung durch den Chip-Karten-Inhaber erfordern, geschieht durch die Abfrage kartenspezifischer Daten. Abbildung 20 illustriert die Konfigurationsanweisungen. SSLRequire dient hier der Zugriffskontrolle. In einem ersten Schritt wird mit der Umgebungsvariablen SSL_CLIENT_VERIFY geprüft, ob der Chip-Karten-Inhaber die zur Karte passende PIN eingegeben hat. Im dann folgenden Schritt, wird durch die Umgebungsvariable SSL_CLIENT_I_DN_CN der Name des Zertifikats überprüft, welches genau dem Wert „UNIGI-CCA“ entsprechen muß, was bei allen herausgegebenen Smart Cards der Fall ist.

162 Hierbei ist besonders wichtig, daß die Zertifikate in dem angegebenen Verzeichnis mit den Leserechten für „other“ – also für die Welt – ausgestattet sind. Andernfalls kann der Server dem Client nicht die dort abgelegten Zertifikate schicken.

163 Vgl. Eilebrecht, Lars; Rath, Nikolaus; Rohde, Thomas: Apache Webserver – Installation, Konfiguration, Administration, a. a. O., S. 572.

Hierbei steht

- I für Issuer (Austeller),
- DN für Distinguished Name (aussagekräftiger Name) und
- CN für Certificate Name (Name des Client-Zertifikats).[164]

```
/* ------------ httpd.conf – Datei ----------------

<IfDefine SSL>
<VirtualHost wiwi.uni-giessen.de:443>
…
SSLRequireSSL
SSLVerifyClient optional

SSLRequire ( %{SSL_CLIENT_VERIFY} eq "SUCCESS" \
           and %{SSL_CLIENT_I_DN_CN} eq "UNIGI-CCA")

…
</VirtualHost>
</IfDefine SSL>
```

Abb. 20: Zugriffskontrolle seitens des Apache-Servers

Um auch Personen ohne Smart Card den Zugang zu den Web-Seiten durch Abfrage eines individuellen Paßwortes zu ermöglichen, wird der SSLRequire-Anweisung die Anweisung SSLVerifyClient mit dem Wert „optional“ vorangestellt. Dem Benutzer ohne Smart Card kann dann ein anderer Login zur Verfügung gestellt werden.

5.3 Client-Konfiguration

Die Kommunikation mit dem Smart-Card-Leser bzw. mit der Smart Card erfolgt über globale Umgebungsvariablen, wie sie in der PC/SC-Spezifiaktion festgelegt sind. Nach einer erfolgreichen Authentisierung können weitere Kartendaten ausgelesen werden und für weitere Anwendungen zur Verfügung stehen. Durch geeignete Sicherheitskonzepte muß nun sichergestellt werden, daß eindeutige Kartendaten im Nachhinein nicht mehr abgeändert werden können. Dies könnte bspw. durch verdeckte Paßwörter oder durch den Einsatz von Cookies geschehen.

Die Clients müssen grundsätzlich den technischen Anforderungen genügen und lediglich für den Einsatz der Smart Card vorbereitet werden. Dies bedeutet, daß der Smart-Card-Leser sowie die zugehörige Software installiert werden muß. Durch die Installation der Gerätetreiber und der mitgelieferten Software wird sichergestellt, daß die vom Server geforderten Authentifizierungsanfragen auch verarbeitet und dementsprechend

164 Vgl. Eilebrecht, Lars; Rath, Nikolaus; Rohde, Thomas: Apache Webserver – Installation, Konfiguration, Administration, a. a. O., S. 572 f. und 579 f.

an die Smart Card weitergeleitet werden. Die folgende Abbildung 21 zeigt die Installationsroutine der Smart-Card-Treiber.

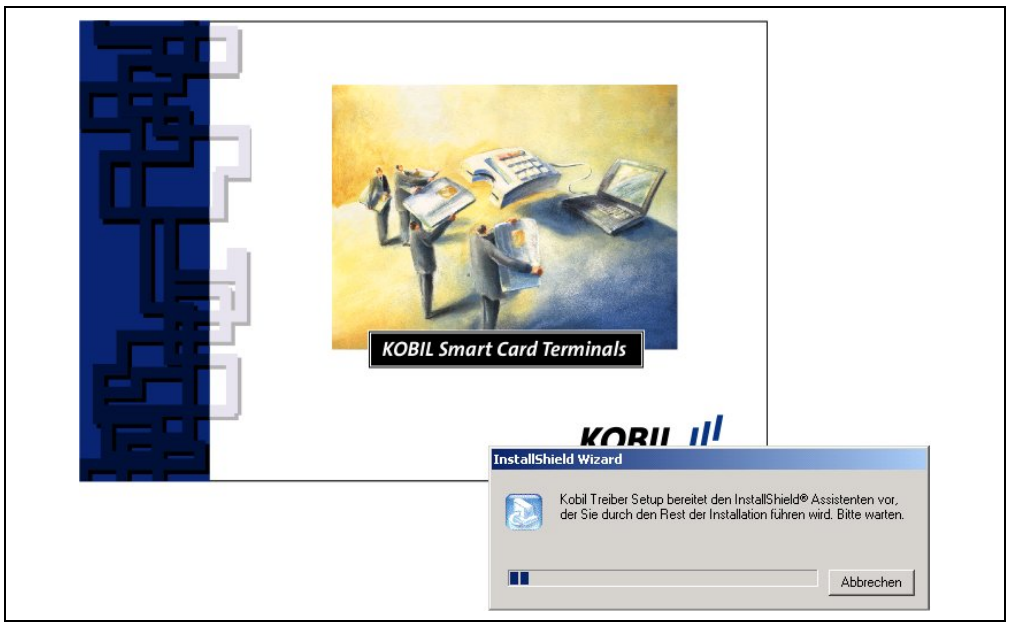

Abb. 21: Installationsroutine der Smart-Card-Treiber

Anschließend kann der Smart-Card-Leser angeschlossen und die Anwendungs-Software installiert werden. Mit dem mitgelieferten „CardManagement Tool“ kann die Funktion des Kartenlesers und der Smart-Card überprüft werden. Im Erfolgsfall zeigt das Diagnose-Programm den Inhalt der Smart Card bzw. die Zertifikate wie in Abbildung 22 dargestellt an.

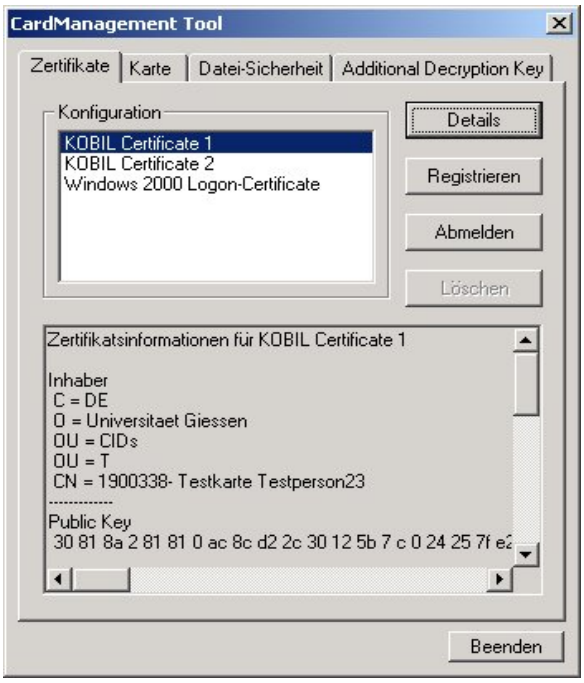

Abb. 22: Anzeige des Zertifikats mit dem Kobil „CardManagement Tool“

Um nun die Smart-Card im Rahmen der PKI der Universität Gießen einsetzen zu können, muß anschließend – sofern noch nicht geschehen – das Karten-Zertifikat durch den Klick auf „Registrieren“ in den Zertifikatsspeicher von Windows gespeichert werden. Wie in Abbildung 23 dargestellt, wird der Benutzer nochmals gefragt, ob das auf der Chipkarte gespeicherte Zertifikat registriert werden soll. Das Karten-Zertifikat wird durch den Klick auf „Ja“ automatisch in der Gruppe der „Eigenen Zertifikate“ gespeichert.

Abb. 23: Registrierung des Karten-Zertifikats

Nach der bis an diese Stelle durchgeführten Client-Installation meldet sich der SSL-Server der Wirtschaftswissenschaften (Wiwi-Server) wie in Abbildung 24 dargestellt beim Anwählen der Web Site mit einer Sicherheitsinformation.

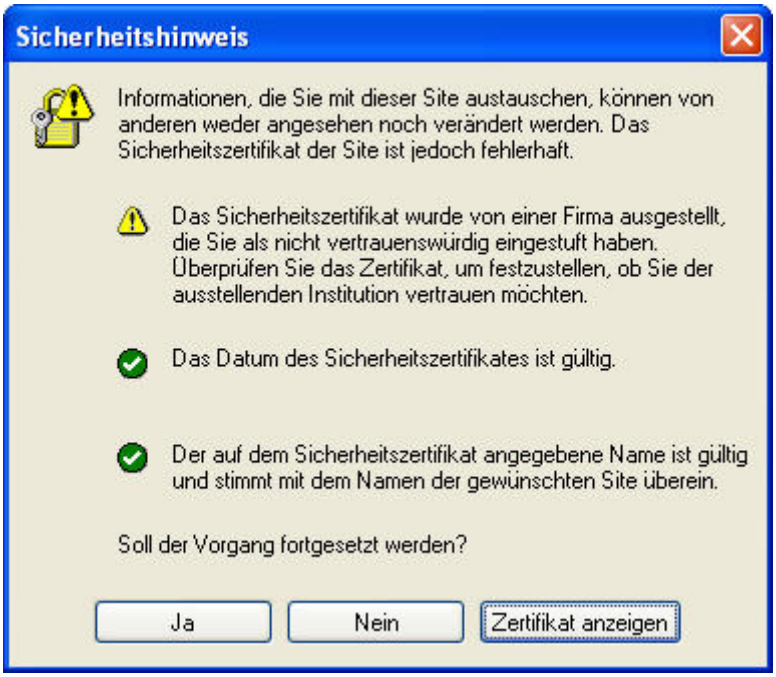

Abb. 24: Sicherheitshinweis des Internet Explorers

In dem sich öffnenden Fenster ist ein gelbes Warndreieck ersichtlich, welches darüber informiert, daß das Wurzelzertifikat im System (Zertifikatsspeicher von Windows) des

Benutzers bei der Gruppe der „Vertrauenswürdigen Stammzertifizierungsstellen“ noch installiert werden muß. Durch den Klick in „Zertifikat anzeigen“ zeigt sich das Zertifikat des Wiwi-Servers (Abbildung 25).

Abb. 25: Zertifikatsinformation des Wiwi-Servers

Es ist dort nachzulesen, daß das Zertifikat für den Server wiwi.uni-giessen.de von der Zwischenzertifizierungsstelle UNIGI-SCA ausgestellt wurde und vom 04.08.2003 bis 03.08.2005 gültig ist. Allerdings kann das Client-System das Zertifikat nicht bis zu einer Zertifizierungsstelle verifizieren. Das wird durch das rote X in der linken oberen Ecke angezeigt. Beim Klick auf den Reiter „Zertifizierungspfad“ sieht man dann, welche Informationen der Wiwi-Server übermittelt. Abbildung 26 zeigt den Zertifizierungspfad, der vom Wiwi-Server aufgrund der in Kapitel 5.2 „Server-Konfiguration“ gemachten Konfiguration (siehe Abbildung 19) bis zum Toplevel-Zertifikat des DFN übermittelt wird.

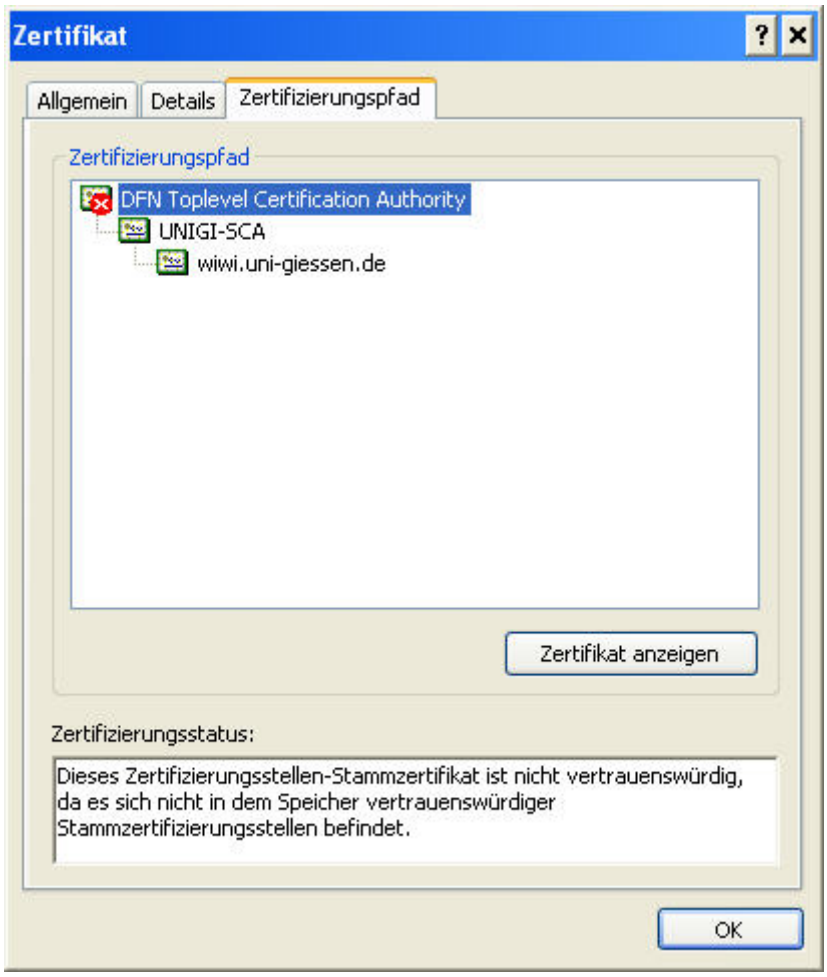

Abb. 26: Zertifizierungspfad des Wiwi-Zertifikats

Der Status des Zertifizierungspfads klärt darüber auf, daß das Stammzertifizierungsstellen-Zertifikat deshalb nicht vertrauenswürdig ist, weil sich dieses Zertifikat nicht in der Liste der Stammzertifizierungsstellen des Client-Systems befindet. Sofern der User sich an einem fremden System befindet und er selbst keine Installationen diesbezüglich vornehmen kann, aber dem User die Zertifizierungsstelle bekannt ist und vertrauenswürdig erscheint, kann durch zweifaches Klicken auf „OK“ und durch Klicken von „Ja“ an der Stelle der Sicherheitsinformation (vgl. Abbildung 24) die Vertrauenswürdigkeit zwischen Client-System und Wiwi-Server hergestellt werden. Diese bleibt so lange im Client-System gespeichert, bis der User den Browser komplett schließt.

Die zuletzt beschriebenen Schritte haben den Vorteil, daß auf einfache Art und Weise eine Vertrauensstellung zwischen Client und Server hergestellt werden kann. Lediglich der anfänglichen Sicherheitsinformation (vgl. Abbildung 24) muß vertraut werden. Danach besteht eine SSL-geschützte Verbindung zwischen Client-System (Browser) und Wiwi-Server.

Wird der Wiwi-Server häufig/regelmäßig von einem Client-System kontaktiert, bietet es sich an, das notwendige Toplevel-Zertifikat auf diesem Client-System zu installieren.

Ausgehend von Abbildung 26 ist es notwendig, daß der User auf „Zertifikat anzeigen“ klickt. Der Wiwi-Server zeigt dann folgendes in Abbildung 27 dargestellte Fenster.

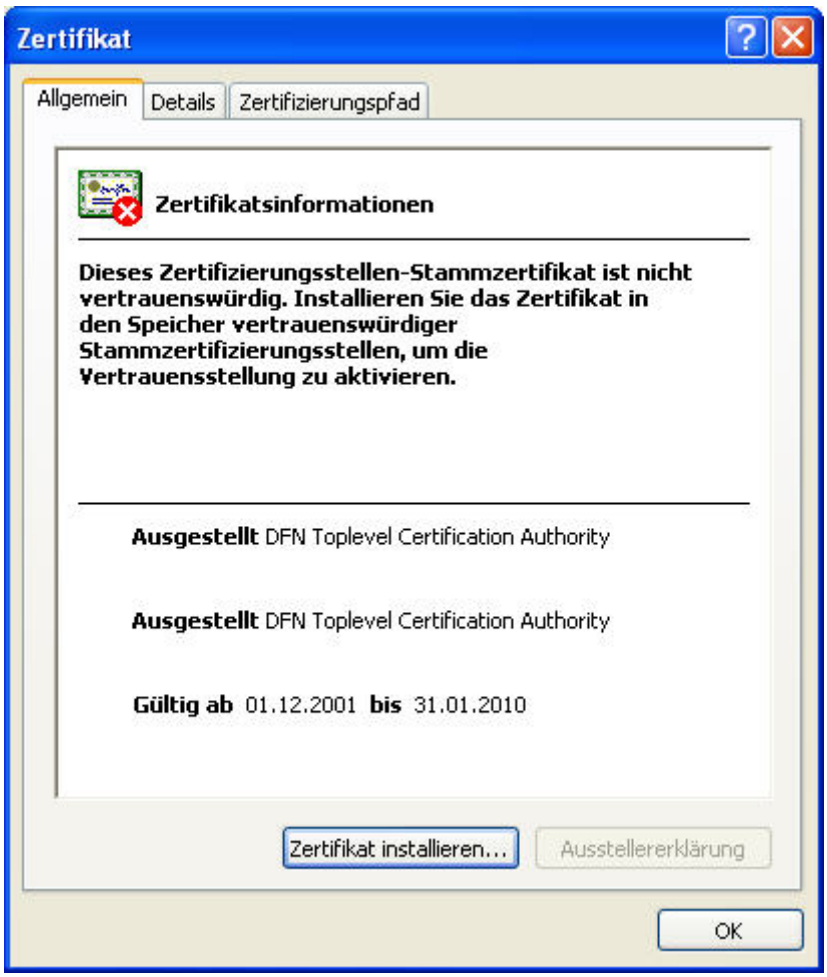

Abb. 27: Stammzertifikat der Toplevel-Zertifizierungsstelle DFN

An dieser Stelle kann dann das Zertifikat mittels des Button „Zertifikat installieren…“ im Zertifikatsspeicher von Windows installiert werden. Es folgt ein „Zertifikatsimport-Assistent“ bei dem man durch klicken in „Weiter“ und „Fertig stellen“ das in Abbildung 28 dargestellte Zertifikat wiederum durch Klicken in „Ja“ in den Speicher der Stammmzertifikate installiert. Zuvor kann sich der User an dieser Stelle genau über den Fingerabdruck des Stammzertifikats informieren und diesen mit den auf den Web-Seiten des DFN veröffentlichten Daten vergleichen. Dadurch ist sichergestellt, daß der User jederzeit eine Kontrolle über die von Ihm installierten Zertifikate behält.

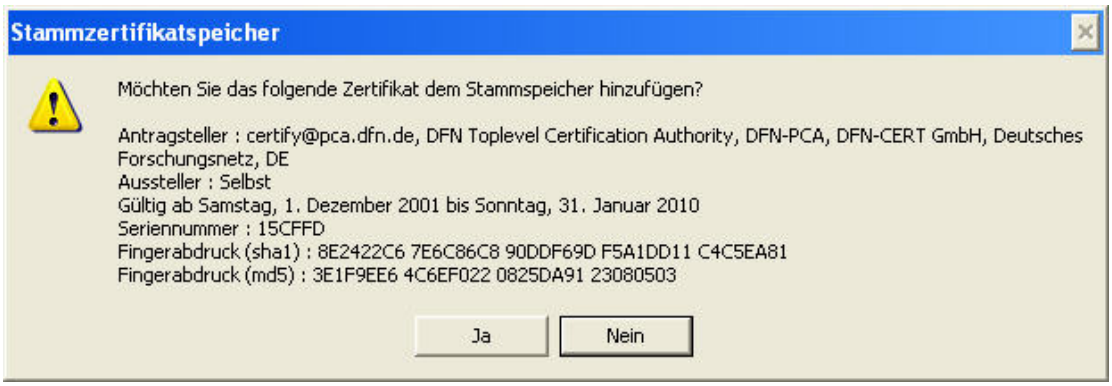

Abb. 28: Bestätigung des Client-Systems beim Installieren des Stammzertifikats

Die Bestätigung des Users durch den Klick in „Ja“ beantwortet das Client-System mit der in Abbildung 29 gemachten Erfolgsbestätigung.

Abb. 29: Erfolgsbestätigung des Zertifikats-Assistenten

Nach dieser Stammzertifikats-Installation wird der User nicht mehr mit dem Sicherheitsfenster des Internet Explorers konfrontiert, denn die vom Wiwi-Server geschickten Daten können mit den im Stammzertifizierungsspeicher abgespeicherten Daten verifiziert werden.

Beim Anwählen der SPIC-Login-Page wird der User aufgefordert, den zur Karte passenden PIN-Code einzugeben. Abbildung 30 zeigt die Aufforderung zur Pin-Eingabe.

Abb. 30: PIN-Eingabe

Nach erfolgreicher PIN-Eingabe wird ein erneutes Fenster zur Clientauthentifizierung angezeigt. Abbildung 31 zeigt die Clientauthentisierung, die Aufschluß darüber gibt, welche Clientzertifikate auf dem Rechner bzw. in dem Profil des Users des Windows-Systems installiert sind.

Abb. 31: Clientauthentifizierung

Das eigene Zertifikat wird nach bisher durchgeführter Installation wie folgt im Internet Explorer angezeigt. Der Klick in „Zertifikat anzeigen…“ zeigt das in Abbildung 32 dargestellte Zertifikat.

Abb. 32: Darstellung des Karten-Zertifikats im Internet Explorer

Durch die Auswahl des passenden Kartenzertifikats und den Klick in „Ja“ in Abbildung 31 gelangt der User in das personalisierte SPIC. Das Client-System ist zudem für die Nutzung aktueller und zukünftiger Smart-Card-Anwendungen konfiguriert und Authentisierungsanfragen werden dementsprechend an die Smart Card Software durchgereicht.

5.4 Integration weiterer Anwendungen

Gemäß der Priorisierung sollen weiterhin die Möglichkeit der Online-Prüfungsanmeldung sowie die Noteneinsicht realisiert werden. Da dafür auf die Leistung eines externen Systems (FlexNow) zurückgegriffen wird, sind diese Funktio-nalitäten als kritische externe Anwendungen einzuordnen. Demnach ist dabei keine Behandlung im Sinne eines „Single Sign On“ möglich.[165] Das bedeutet, daß die beiden Funktionalitäten zwar innerhalb des SPIC navigatorisch eingebettet werden, aber eine eigene Authentisierung fordern. Die folgende Abbildung zeigt den Ablauf des Zugriffs auf des System des Prüfungsamts und die Internet-Komponente von FlexNow, wie sie voraussichtlich auch am Fachbereich zum Einsatz kommen wird.

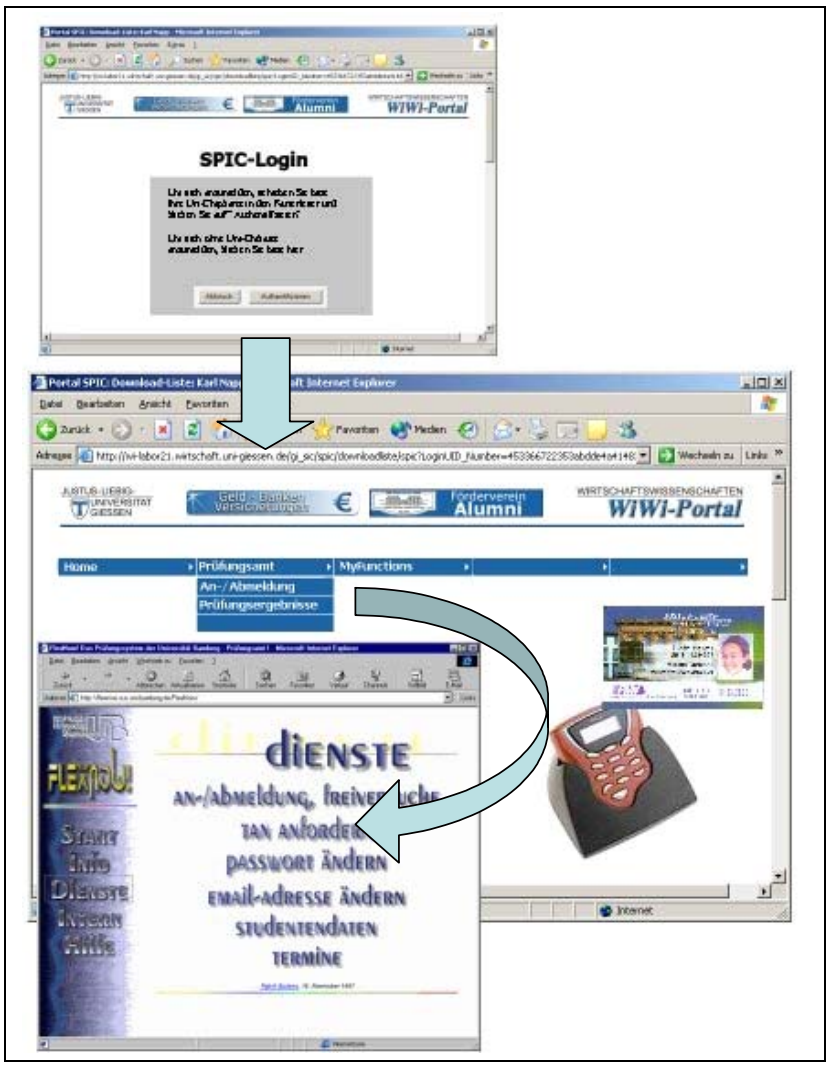

Abb. 33: Prinzip des Zugriffs auf die Internet-Komponente von FlexNow[166]

165 Vgl. Kapitel 4.2.

166 Dabei ist zu beachten, daß der Screenshot von FlexNow die Internet-Komponente in ihrer bisherigen Form (mit PIN/TAN-Verfahren) zeigt. Die betreffenden Funktionalitäten würden in der Smart-Card-Version nicht mehr benötigt.

Dabei ist die Anmeldung am FlexNow-System ungeachtet vorheriger Authentisierung im Rahmen des SPIC erneut mit der Smart Card durchzuführen. Eine Übernahme der Authentisierung ist in diesem Fall aufgrund technischer und organisatorischer Gegebenheiten nicht möglich.

Anders bei weiteren kritischen WPS-Funktionalitäten; diese könnten ohne weiteres in das SPIC implementiert werden. Die Vorgehensweise ist dabei die gleiche wie beim Zugriff auf das SPIC. Das gilt selbstverständlich nur für alle weiteren Funktionalitäten, die lediglich eine Authentisierung fordern. Sollen bestimmte Anwendungsfelder zusätzlich eine „echte“ digitale Signatur bedingen, muß noch nach einer geeigneten Lösung gesucht werden. Dies gilt bspw. für den Bereich der Diskussionsforen oder bei den Anmeldungen an den Professuren.

6 Fazit und Ausblick

Der nach wie vor anhaltende Boom von Chipkarten, insbesondere von Smart Cards, ist relativ gut zu erklären. Die zuvor aufgezeigten sicherheitsrelevanten Anwendungen wie das Verschlüsseln, Signieren und Authentisieren ist schon seit Jahren durch ausgereifte Techniken und Methoden möglich. Aber erst in Kombination mit der Smart Card als sicheres Identifikationsmedium können die mit der Geheimhaltung privater Schlüssel einhergehenden Probleme asymmetrischer Verfahren gelöst und damit deren Anwendung sicherer gestaltet werden. Dies hat dementsprechend weitreichende Auswirkungen auf die (wirtschaftliche) Nutzung des Internets, da durch den Einsatz von Smart Cards bisherige Probleme im Internet-Umfeld gelöst werden können. Gerade in Hinblick auf die Elektronisierung kritischer Anwendungen und Prozesse spielt die Smart Card eine wichtige Rolle. Sie hilft, die Möglichkeiten der weltweiten Vernetzung nahezu vollständig zu nutzen und als Ergebnis eine nachhaltige Reduzierung der Transaktionskosten zu erreichen.

Dies gilt auch für die Universitäten, deren Ziel der Elektronisierung nicht zuletzt aufgrund aktueller Entwicklungen die Kostensenkung ist. Dabei greifen die meisten Universitäten allerdings auf Minimal-Lösungen, in Form von Chipkarten nach dem Trierer-Modell zurück. Die Anwendungsfelder solcher Lösungen sind vor allem dadurch begrenzt, daß ein Einsatz der Karte im öffentlichen Internet nicht möglich ist.

Anders an der Universität Gießen: Hier sind die Einsatzgebiete durch die Entscheidung zugunsten einer „echten“ Smart Card und einer eigenen PKI nahezu unbegrenzt. Eine solch umfassende Lösung hat aber auch ihren Preis und gerade vor dem Hintergrund der bereits getätigten Investitionen ist eine Ausnutzung der Möglichkeiten nahezu zwingend. Am Fachbereich Wirtschaftswissenschaften besteht zudem in Verbindung mit

dem WPS, der guten IT-Ausstattung und vorhandenem technischen Know-How eine hervorragende Ausgangssituation zur Implementierung von geschützten Smart-Card-Anwendungen. Von Seiten der Kommunikatoren lassen sich zahlreiche fachliche Anwendungsgebiete am Fachbereich feststellen. Im Rahmen dieser Arbeit wurden einige diskutiert und dabei die Notwendigkeit, Vorteile und Nachteile dieser Funktionalitäten aufgezeigt. Die Realisierung findet dabei ihre Begrenzung vor allem in den verfügbaren Entwicklungskapazitäten und nicht aufgrund fehlender Anwendungsgebiete. Würden die bestehenden Kapazitäten in Form von qualifizierten Mitarbeitern etc. entsprechend ausgeweitet, könnten viele sinnvolle und notwendige Funktionalitäten zeitnah implementiert werden. Dies beschränkt sich nicht nur auf die bereits diskutierten Anwendungen, sondern auch auf die Planung und Entwicklung weiterer Funktionalitäten, die im Rahmen dieser Arbeit noch keine Beachtung finden konnten. Zu denken sei bspw. an eine Web-gestützte Studienplanung für die Studierenden, in der ihnen die Möglichkeit gegeben wird, das Studium im Sinne eines Projektmanagements zu planen. Ein weiteres wichtiges Feld ist das Angebot von kostenpflichtigen Lehrveranstaltungen wie bspw. ein Master of Business Administration (MBA)-Studiengang. Gerade vor dem Hintergrund aktueller Entwicklungen im Hochschulbereich wird das Angebot solcher entgeltlichen Angebote in Zukunft zunehmend wichtiger.

Ein in dieser Arbeit oft angesprochener Aspekt ist die Akzeptanz von Smart-Card-Anwendungen. Selbstverständlich ist die Forderungen nach Datenschutz mehr als gerechtfertigt, nur darf diese nicht – teilweise aufgrund von unvollständigen oder gar falschen Informationen – absurde Formen annehmen. Dieser Aspekt ist für den Hochschulbetrieb sowie für das Internet im Allgemeinen nahezu symptomatisch. Der notwendige Einstellungswandel muß sich in beiden Fällen langsam von „Anonym & Gratis“ zu „Persönlich & Kostenpflichtig“ vollziehen. Daher gilt gerade bei der Integration von Smart-Card-Anwendungen, die ein hochsensibles Thema wie den Datenschutz berühren, der Grundsatz: Evolution statt Revolution.

Literaturverzeichnis

1. **Ackermann, Kurt:** UNIGI-NET, VPN: Für wen?, Online im Internet: http://www.uni-giessen.de/hrz/datennetze/unigi-net/vpn/usage.html, 19.05.2003.
2. **Ackermann, Kurt:** Warum kein DSL-Zugang zum Datennetz der JLUG ?, Online im Internet: http://www.uni-giessen.de/hrz/datennetze/unigi-net/dsl.htm, 21.05.2003.
3. **Ackermann, Kurt:** UNIGI-NET, VPN: Voraussetzungen, Online im Internet: http://www.uni-giessen.de/hrz/datennetze/unigi-net/vpn/voraussetzungen.html, 13.06.2003.
4. **Burrows, James H.:** Federal Information Processing Standards Publication 180-1 - Secure Hash Standard, Online im Internet: http://www.itl.nist.gov/fipspubs/fip180-1.htm, 17.04.1995.
5. **DFN Cert:** DFN PCA World Wide Web Policy: Online im Internet: http://www.pca.dfn.de/certification/policies/ssl-tls/cp-1.4/wwwpolicy.html, 15.12.2003.
6. **Eilebrecht, Lars; Rath, Nikolaus; Rohde, Thomas:** Apache Webserver – Installation, Konfiguration, Administration, 4., erweiterte und überarbeite Aufl., Bonn: mitp-Verlag 2002.
7. **Fachschaftsrat Informatik, TH Darmstadt (Hrsg.):** Abgekartetes Spiel – Wie Chipkarten den Hochschulalltag verändern, Online im Internet: http://www.uni-mainz.de/Organisationen/gruenlinx/chips/Readerchipneu.pdf, 1996.
8. **Fock, Falko:** Informationen zur Chipkarte, Aussehen und Inhalt der JLU-Chipkarte, Online im Internet: http://www.uni-giessen.de/chipkarte/beschreibung.html, 29.10.2002.
9. **Fock, Falko:** Informationen zur Chipkarte, Info zur elektronischen Geldbörse der JLU-Chipkarte, Online im Internet: http://www.uni-giessen.de/chipkarte/geldboerse.html, 17.06.2003.
10. **Fock, Falko:** Informationen zur Chipkarte, Info zur Chipkarten-Aktualisierung, Online im Internet: http://www.uni-giessen.de/chipkarte/aktualisierung.html, 21.09.2003.
11. **Fock, Falko:** Informationen zur Chipkarte, Chipkarten-Info zur Rückmeldung, Online im Internet: http://www.uni-giessen.de/chipkarte/rueckmeldung.html, 05.02.2004.
12. **Fock, Falko:** Informationen zur Chipkarte, Aktuelles, Online im Internet: http://www.uni-giessen.de/chipkarte/aktuell.html, 11.03.2004.
13. **Janowicz, Krzysztof:** Sicherheit im Internet, Köln: O'Reilly Verlag 2002.
14. **JLU-Gießen, Bibliothekssystem:** Ausleihe, Online im Internet: http://www.uni-giessen.de/ub/service/ausleihe.html, 11.03.2004.
15. **Merz, Michael:** E-Commerce und E-Business – Marktmodelle, Anwendungen und Technologien, 2., aktualisierte und erweiterte Aufl., Heidelberg: dpunkt-Verlag 2002.

16. **Netzgruppe HRZ:** UNIGI-NET, WLAN (Hotspots), Online im Internet: http://www.uni-giessen.de/hrz/datennetze/unigi-net/WLAN/uni-hotspots.html, 04.03.2004.

17. **Obermann, Jürgen:** SSL-Server-Zertifizierungsinstanz der Universität Gießen (UniGI-SCA), Online im Internet: http://www.uni-giessen.de/hrz/unigi-ca/sca.html, 17.12.2001.

18. **o.V.:** Informationen zur Chipkarte, Einsatzgebiete für die Chipkarte, Online im Internet: http://www.uni-giessen.de/chipkarte/einsatzgebiete.html, 20.01.2004.

19. **Papendick, Astrid:** Studicard 2003, Online im Internet: http://www.uni-mainz.de/Organisationen/gruenlinx/unipress/chipkarte_UP330_dez02.html, 14.08.2003.

20. **Partosch, Günter:** Informationen zur Chipkarte, Information über Chipkarten-Leser, Online im Internet: http://www.uni-giessen.de/chipkarte/chipkartenleser.html, 16.01.2003.

21. **Partosch, Günter:** Informationen zur Chipkarte, Chipkarten-Info zu PIN und PUK, Online im Internet: http://www.uni-giessen.de/chipkarte/pinPuk.html, 17.01.2003.

22. **Partosch, Günter:** Informationen zur Chipkarte, Chipkarte und E-Mail-Adresse, Online im Internet: http://www.uni-giessen.de/chipkarte/e-mail.html, 17.01.2003.

23. **Partosch, Günter:** Informationen zur Chipkarte, Zum Namen der Chipkarte der Studierenden der JLU, Online im Internet: http://www.uni-giessen.de/chipkarte/name.html, 17.01.2003.

24. **Partosch, Günter:** Informationen zur Chipkarte, Information zu den Mikrochip-Prozessoren, Online im Internet: http://www.uni-giessen.de/chipkarte/mikroprozessoren.html, 17.01.2003.

25. **Partosch, Günter:** Informationen zur Chipkarte, Chipkarten-Info -- Ausweisnummer, Online im Internet: http://www.uni-giessen.de/chipkarte/ausweisnummer.html, 23.09.2003.

26. **Pressestelle der Justus-Liebig-Universität Gießen:** Die Universität in Zahlen, Online im Internet: http://www.uni-giessen.de/neu2/informationen/uni-zahlen.html, 05.03.2004.

27. **Rankl, Wolfgang; Effing, Wolfgang:** Handbuch der Chipkarten – Aufbau Funktionsweise – Einsatz von Smart Cards, 4., überarbeitete und aktualisierte Aufl., München; Wien: Hanser Verlag 2002.

28. **Schäfer, Günter:** Netzsicherheit – Algorithmische Grundlagen und Protokolle, Heidelberg: dpunkt-Verlag 2003.

29. **Schwenk, Jörg:** Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, Braunschweig; Wiesbaden: Vieweg Verlag 2002.

30. **Schwickert, Axel C.; Ostheimer, Bernhard; Franke, Thomas S.:** eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen, in: Arbeitspapiere WI, Nr. 9/2000, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes-Gutenberg-Universität Mainz: Mainz 2000.

31. **Schwickert, Axel C.; Grund, Henning:** Web Content Management – Grundlagen und Anwendungen mit dem Web Portal System V.2.5, in: Arbeitspapiere WI

3/2004, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2004, 62 Seiten.

32. **Signatur-Gesetz:** Gesetz zur digitalen Signatur, Artikel 3 § 1 Absatz 2 des Informations- und Kommunikationsdienst-Gesetz.

33. **Sinz, Elmar, J.; Wismans, Benedikt:** Das "Elektronische Prüfungsamt" – Bamberger Beitrag zur Wirtschaftsinformatik Nr. 47, Online im Internet: http://www.seda.sowi.uni-bamberg.de/forschung/publikationen/bamberger-beitraege/no47.pdf, 1998.

34. **Treber, Udo; Muschiol, Tim; Gillen, Arndt:** Wireless LAN – Situations- und Anforderungsanalyse am Beispiel eines Universitätscampus, in: Arbeitspapiere WI 4/2004, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2004, 110 Seiten.

35. **Warner, Ansgar:** Die Chipkarte kommt, in: sbz, Nr. 38/2001, S. 8-10.

36. **Weiß, Dieter:** Chipkarten-Zertifizierungsinstanz der Universität Gießen (UniGI-CCA), Online im Internet: http://www.uni-giessen.de/hrz/unigi-ca/cca.html, 19.10.2002.

37. **Wolf, Dieter:** Internet-Entgelt an der Justus-Liebig-Universität Gießen, Online im Internet: http://www.uni-giessen.de/hrz/kommuni/entgelt.html, 17.01.2002.

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: Online-Bestellung unter http://wi.uni-giessen.de → Forschung

Herausgeber: Univ.-Prof. Dr. Axel C. Schwickert
Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungsarbeiten, Diplom-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr- und Vortragsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Univ. Prof. Dr. Axel C. Schwickert, Justus-Liebig-Universität Gießen.

Hinweise: Wir nehmen Ihre Anregungen und Kritik zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit dem Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe und deren Bezug erhalten Sie auf der Web Site der Professur unter der Adresse http://wi.uni-giessen.de