TECHNISCHE UNIVERSITÄT ILMENAU

# Integration elektronischer Zahlung und Zugangskontrolle in ein elektronisches Lernsystem

**R. Grimm, B. Schulz-Brünken, K. Herrmann**

**Nr. 12** **Mai 2004**

Diskussionsbeiträge

INSTITUT FÜR MEDIEN- UND KOMMUNIKATIONSWISSENSCHAFT

# Integration elektronischer Zahlung und Zugangskontrolle in ein elektronisches Lernsystem

R. Grimm, B. Schulz-Brünken, K. Herrmann

Nr. 12 Mai 2004

Herausgeber: Der Rektor der Technischen Universität Ilmenau
Redaktion: Institut für Medien- und Kommunikationswissenschaft,
Prof. Dr. Rüdiger Grimm
ISSN 1617-9048
Kontakt: Rüdiger Grimm, Tel.: +49 3677 69 4735
E-Mail: ruediger.grimm@tu-ilmenau.de

# Integration elektronischer Zahlung und Zugangskontrolle in ein elektronisches Lernsystem

## Teilprojekt von DaMiT (Data Mining Tutor)

## im Rahmen des BMBF - Programms „Neue Medien in der Bildung“ (2001-2003)

Rüdiger Grimm

Barbara Schulz-Brünken

Konrad Herrmann

## Inhalt

| | | |
|---|---|---|
| **1** | **Aufgabenstellung, Voraussetzungen und Arbeitspakete** | **03** |
| 1.1 | Aufgabenstellung | 03 |
| 1.2 | Voraussetzungen, unter denen das Vorhaben durchgeführt wurde | 04 |
| 1.3 | Planung und Ablauf des Vorhabens | 04 |
| 1.3.1 | Arbeitspakete des Teilprojektes | 04 |
| 1.3.2 | Zeitlicher Ablauf des Teilprojektes | 06 |
| 1.4 | Wissenschaftlicher und technischer Stand, an den angeknüpft wurde | 07 |
| 1.4.1 | Eigene Vorarbeiten | 07 |
| 1.4.2 | Bekannte Konstruktionen, Verfahren und Schutzrechte, die für die Durchführung des Vorhabens benutzt wurden | 08 |
| 1.4.3 | Verwendete Fachliteratur sowie benutzte Informations- und Dokumentationsdienste | 08 |
| 1.5 | Zusammenarbeit mit anderen Stellen | 09 |
| **2** | **Ergebnisse und Nutzen** | **10** |
| 2.1 | Ergebnisse | 10 |
| 2.1.1 | Arbeitspaket 7.1: Überblick über elektronische Zahlungsverfahren | 10 |
| 2.1.2 | Arbeitspaket 7.2: Integration von Zahlungsmöglichkeiten in das DaMiT System | 11 |
| 2.1.3 | Arbeitspaket 7.3: Zugangskontrolle | 12 |

| | | |
|---|---|---|
| 2.1.4 | Arbeitspakete 7.4 und 7.5: Implementierung eines *Zahlungssystems* und eines *Zugriffskontrollverfahrens* in das DaMiT System | 15 |
| 2.2 | Voraussichtlicher Nutzen, insbesondere Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplanes | 16 |
| 2.3 | Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen, der während des Vorhabens bekannt geworden ist | 17 |
| 2.4 | Erfolgte oder geplante Veröffentlichungen | 18 |
| **3** | **Zusammenfassende Betrachtung und Ausblick** | **19** |
| 3.1 | Beitrag des Ergebnisses zu den förderpolitischen Zielen des Förderprogramms, -schwerpunkts, -konzepts | 19 |
| 3.2 | Wissenschaftlich-technisches Ergebnis des Vorhabens, die erreichten Nebenergebnisse und die gesammelten wesentlichen Erfahrungen | 20 |
| 3.3 | Fortschreibung des Verwertungsplanes | 20 |
| 3.3.1 | Erfindungen und Schutzrechte | 20 |
| 3.3.2 | Wirtschaftliche Erfolgsausichten nach dem Ende des Projekts | 20 |
| 3.3.3 | Wissenschaftliche und/oder technische Erfolgsaussichten nach Projektende | 21 |
| 3.3.4 | Wissenschaftliche und wirtschaftliche Anschlussfähigkeit | 22 |
| 3.4 | Arbeiten, die zu keiner Lösung geführt haben | 22 |
| 3.5 | Präsentationsmöglichkeiten für mögliche Nutzer | 23 |

## Zusammenfassung

Die Zielsetzung des Teilprojektes war es, für den Data-Mining-Tutor elektronische Zahlungsmöglichkeiten und die elektronische Zugangskontrolle auf der Basis bereits vorhandener Systeme zu erarbeiten und in das System zu integrieren. Zahlungs- und Zugriffskontrollsysteme wurden beispielhaft implementiert. Eine wichtige Rolle spielt in diesem Zusammenhang das System Paybest der Ilmenauer Firma 4FO AG. Das Ergebnis der Arbeiten im Teilprojekt ist ein dem Wert angemessenes Dienstangebot von E-Learning-Systemen (am Beispiel von DaMiT). Das Lernen im DaMiT-System ist durch die implementierten Zahlungsmöglichkeiten kommerziell auswertbar. Es gilt der Grundsatz: „Wer bezahlt, bekommt mehr." Ein besonderer Vorteil gegenüber anderen Schutz- und Zahlungsvorrichtungen (Alleinstellungsmerkmal von DaMiT) besteht darin, dass durch das Kundenrollenmodell die spezifischen Bedürfnisse der unterschiedlichen Nutzer befriedigt werden können. Der Schutz der Nutzer (Datenschutz, Vertraulichkeitsschutz) wird durch die implementierten Zugangskontrollverfahren und durch das Rollenmodell (anonyme oder persönliche Zugänge) gewährleistet. Studierende werden durch die Möglichkeit des kostenfreien Zugangs besonders gefördert. Das Teilprojekt hat durch seine Arbeit die technische Basis entwickelt, um das DaMiT System kommerziell nutzen zu können.


# 1 Aufgabenstellung, Voraussetzungen und Arbeitspakete

## *1.1 Aufgabenstellung*

Im Verbundprojekt DaMiT wurde ein generisches Tutorsystem für das Gebiet des Data Mining entwickelt, evaluiert und bundesweit in der Fernlehre und in der Präsenzlehre angewendet sowie der beruflichen Weiterbildung angeboten. Neuartig ist u.a. die Verzahnung freier Lehrinhalte mit kommerziellen Dienstleistungen im Internet. Dadurch werden einerseits Ressourcen der Wirtschaft für die praxisnahe Lehre an Universitäten und Hochschulen erschlossen und andererseits den akademischen Einrichtungen Möglichkeiten einer Verwertung tutorieller Leistungen eröffnet.

Die Technische Universität Ilmenau bearbeitete in ihrem Fachgebiet „Multimediale Anwendungen" das Thema „Zahlungssysteme und Zugriffskontrolle".

Auf der Basis einer Analyse vorhandener elektronischer Zahlungssysteme wurde die Integration elektronischer Zahlungsmöglichkeiten in das Tutor-System erarbeitet. Weiterhin wurden Verfahren zur Kontrolle der Zugangsberechtigung zu Dienstleistungen des Tutor-Systems entwickelt. Zahlungs- und Zugriffskontrollsysteme wurden beispielhaft implementiert.

Außerdem wurde der Lehrinhalt „Privacy im Internet" in das Tutor-System eingebracht und sein Einsatz in konkreten Lehrveranstaltungen des Fachgebietes an der TU Ilmenau erprobt.

- Forschungsperspektive: Ausbau der Integration von Zahlungs- und Zugriffskontrollverfahren für weitere Dienstleistungen.
- Lehrperspektive: Einbringen von Lehrinhalten in das Tutor-System und Einsatz des Tutor-Systems im Universitätslehrbetrieb.

- Kommerzielle Perspektive: Entwicklung und Einsatz von Fortbildungslehrinhalten mit Hilfe des Tutor-Systems für den außeruniversitären Lehrbetrieb.

Die Themen „Privacy - Persönliche Profilbildung“ und „Elektronische Zahlungssysteme“ sind Gegenstand des Lehrangebots des Fachbereichs „Multimediale Anwendungen“ an der TU Ilmenau. Im Rahmen von DaMiT wurden Tutorien entwickelt, zunächst eines, später auch weitere, die in folgenden Lehrveranstaltungen eingesetzt werden:

1. Vorlesung über „Trust (Vertrauen) im Internet“ als Hintergrundmaterial für Studenten

2. Praxiswerkstatt „Elektronische Zahlungssysteme“ für die interaktive Wissenssammlung der Studenten.

3. Lehrmaterial für universitätsübergreifende Ringvorlesungen im Land Thüringen.

## *1.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde*

Das Teilprojekt wurde vom Lehrstuhl „Multimediale Anwendungen“ im Institut für Medien- und Kommunikationswissenschaft der TU Ilmenau (Stiftungslehrstuhl der Deutschen Bank) unter der Leitung von Prof. Dr. Rüdiger Grimm ausgeführt.

Zur Antragstellung war der Lehrstuhl mit einem Professor, zwei wissenschaftlichen Mitarbeitern (je eine halbe Stelle) und einer Sekretärin (halbe Stelle) ausgestattet.

Wesentliche Vorarbeiten gab es zu elektronischen Zahlungssystemen, Zugangskontrolle und Datenschutz im Internet. Eine Kooperation mit der Ilmenauer Firma 4FriendsOnly Internet Technologies AG (4FO AG), die sich auf Spieleplattformen und ihren kommerziellen Download spezialisiert hat, befand sich im Aufbau. Ebenfalls im Aufbau befand sich die Kooperation mit der Ilmenauer Arbeitsgruppe für elektronische Medientechnik des Erlanger Fraunhofer Instituts für Integrierte Schaltungen (IIS) (seit 01.01.04 Institut für Digitale Medientechnologie, IDMT) und mit dem Fraunhofer Institut für Sichere Telekooperation (SIT) in Darmstadt.

Im Lehrstuhl war ein Labor für elektronische Zahlungssysteme etabliert, die Lehrveranstaltung Praxiswerkstatt „Elektronische Zahlungssysteme“ hatte bereits einmal stattgefunden. Der Antrag stellende Lehrstuhlinhaber Prof. Grimm hatte außerdem Erfahrung in Drittmittelprojekten zu den Themen Zugangskontrolle (EU-Projekte) und Datenschutz (BMBF DASIT - Datenschutz im Internet, mit der DZ Bank, M. Salmony, und der Universität Kassel, Prof. A. Roßnagel).

## *1.3 Planung und Ablauf des Vorhabens*

### 1.3.1 Arbeitspakete des Teilprojektes

*AP 5.6: Privacy - Persönliche Profilbildung* (Arbeitsthema „Abbildung der Lehrinhalte“, AT 5)

Das Thema „Privacy - Persönliche Profilbildung“ stellt eine Anwendung von Data Mining dar. Weltweit und nicht immer legal sammeln Web- und Mailserver, Dienste- und Content-Anbieter personenbezogene Daten. Diese Daten werden erst durch eine inhaltliche Verknüpfung untereinander aussagekräftig.

Gegen den unkontrollierten Einsatz solcher Profilbildung gibt es Gegenmaßnahmen, darunter gesetzliche Regelungen, gezielte Überprüfungen von Anbietern, bilaterale Vereinbarungen und Nutzerkontrollfunktionen.

In diesem Arbeitspaket wurde ein bestehendes Lehrangebot über diese Fragestellung in das Tutor-System von DaMiT als eigenständiger Tutor eingebracht. Der Einsatz des Tutors wurde in konkreten Lehrveranstaltungen des Fachgebietes an der TU Ilmenau erprobt.

*AP 7.1: Überblick über Elektronische Zahlungsverfahren* (Arbeitsthema „Zahlungssysteme und Zugriffskontrolle, AT 7)

Es gibt bereits eine große Zahl elektronischer Zahlungsverfahren auf dem Markt, zum Beispiel eCash, CyberCash, Paybox und Millicent. In diesem Arbeitspaket wurden die vorhandenen Zahlungssysteme nach verschiedenen Gesichtspunkten untersucht und entsprechend strukturiert dargestellt. Untersuchungsaspekte waren vor allem technische Grundlagen, Datenflussprotokolle, Eignung für verschiedene Anwendungen, rechtliche Bedingungen, Währungsbindung, Internationalität, Datenschutz, Nutzerfreundlichkeit und Kosten.

*AP 7.2: Integration von Zahlungsmöglichkeiten in das DaMiT-System*

Dieses Arbeitspaket behandelte die Frage, welche Bestandteile der Dienstleistung des DaMiT-Systems kostenpflichtig sind (oder sein können) und auf welche Weise ihre Inanspruchnahme schließlich abgerechnet wird. Das Tutor-System stellt spezifische Anforderungen an ein Zahlungssystem, weil die Dienstleistung eines Lernsystems eine digitale Ware besonderer Art ist. Sie kann zum Beispiel insgesamt, in Teilen ihres Datenbestandes, in Teilen von Lernabschnitten, zeitabhängig oder pro Benutzung abgerechnet werden.

Es besteht eine offensichtliche Verbindung zum Arbeitspaket AP3 (Zugangskontrolle), da sich Zahlung nur durchsetzen lässt, wenn man den Zugang zu kostenpflichtigen Diensten kontrollieren kann.

Ziel des Arbeitspaketes war eine Beschreibung der Zahlungsanwendung und ihrer Schnittstelle zum Zahlungssystem. Diese Schnittstelle sollte einen Standard bilden, im Idealfall kann sie sich an einen bestehenden Standard anlehnen (vgl. die heute noch nicht abgeschlossene W3C-Aktivität für eine Micropayment Markup-Language) und ist bindend für die Implementierung.

*AP 7.3: Zugangskontrolle*

In diesem Paket wurden Methoden erarbeitet, geschützte Teilbereiche des Tutor-Systems einzurichten und diese von frei zugänglichen Bestandteilen zu unterscheiden. Für einen entsprechenden Zugangsschutz zu den geschützten Bereichen wurde eine Lösung entwickelt und in das DaMiT-System integriert. Ziel des Arbeitspaketes war eine Anforderungsanalyse und eine Lösungsspezifikation.

Es besteht eine offensichtliche Verbindung zum Arbeitspaket AP 7.2 (Integration von Zahlung in DaMiT), da Zahlung die Freigabe und Nichtzahlung die Sperrung kostenpflichtiger Dienste bewirken soll. Weiterhin ist auch die Rolle des Nutzers (Rollenmodell) entscheidend für den Zugang.

*AP 7.4: Implementierung eines Zahlungssystems im DaMiT-Tutor-System*

In diesem Arbeitspaket wurde die in Arbeitspaket AP 7.2 (Integration von Zahlung in DaMiT) erarbeitete Lösung beispielhaft implementiert, in das DaMiT-System integriert und in der Laborumgebung erprobt.

*AP 7.5: Implementierung eines Zugriffskontrollverfahrens im DaMiT-Tutor-System*

In diesem Arbeitspaket wurde die in Arbeitspaket AP 7.3 (Zugangskontrolle) erarbeitete Lösung beispielhaft implementiert, in das DaMiT-System integriert und in der Laborumgebung erprobt.

### 1.3.2 Zeitlicher Ablauf des Teilprojektes

| AP | 1. HJ | 2. HJ | 3. HJ | 4. HJ | 5. HJ | Summe |
|---|---|---|---|---|---|---|
| 5.6 | | 1 | 1 | 1 | 1 | 4 |
| 7.1 | 4 | | | | | 4 |
| 7.2 | 1 | 3 | | 1 | | 5 |
| 7.3 | 1 | 2 | 1 | | 1 | 5 |
| 7.4 | | | 2 | 2 | 2 | 6 |
| 7.5 | | | 2 | 2 | 2 | 6 |
| Sum-me | 6 PM | 6 PM | 6 Pm | 6 PM | 6 PM | 30 PM |

30 PM entspricht einer vollen Person über 30 Monate

Der zeitliche Ablauf des Teilprojektes (5 Halbjahre, HJ) wurde wie folgt geplant:

|-- 1.HJ: 3.01-8.01 --| |-- 2.HJ: 9.01-2.02--| |-- 3.HJ: 3.02-8.02 --| |-- 4.HJ: 9.02-2.03--|

|--5.HJ: 3.03-8.03--|

AP 7.1-7.5 aus AT 7 – „Zahlungssysteme“, AP 5.6 aus AT 5 – „Lehrinhalte“, Angaben in Personenmonaten (PM): 12 PM = 1 PJ

Durch die verspätete Einstellung der Projektmitarbeiter zum 1.06.2001 bzw. 1.09.2001 ergab sich ein verzögerter Projektstart, der sich auch auf die ursprüngliche Verteilung der Arbeitspakete auswirkte.

## *1.4 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde*

### 1.4.1 Eigene Vorarbeiten

*Zahlungssysteme:*

Grimm, R., Zangeneh, K. (1996): Cybermoney in the Internet: An Overview over new Payment Systems in the Internet. In: P. Horster (Ed.): Communications and Multimedia Security II, 1996, IFIP, Chapman & Hall, London, pp. 183-195.

Grimm, R. (1997): Schwerpunkt Elektronisches Geld. Datenschutz und Datensicherheit (DuD) 7/1997, Juli 1997, Vieweg Verlag, Wiesbaden.

Fasel, A., Grimm, R. (2001): Praxiswerkstatt für Elektronische Zahlungssysteme. Studentenarbeiten zur Evaluation von elektronischen Zahlungssystemen nach einheitlichen Kriterien. Nicht veröffentlichte Vorversion, Ilmenau, April 2001.

*Sicherheit und Zugangskontrolle:*

Grimm, R. (1994a): Sicherheit für offene Kommunikation – Verbindliche Telekooperation. B.I. Wissenschaftsverlag, Mannheim, 1994, 274 Seiten.

Grimm, R. (1994b): Towards Trustworthy Communication Systems – Experiences with the Security Toolkit SecuDE. In: M.Medina, N.Borenstein (Eds.): Upper Layer Protocols, Architec-tures and Applications. IFIP Transactions C-25. Elsevier Science Publishers B.V. (North-Holland), 1994, pp. 107-120.

Grimm, R. (2000): Schwerpunkt Sicherheit und E-Commerce. Datenschutz und Datensicherheit (DuD) 10/2000, Oktober 2000, Vieweg Verlag, Wiesbaden.

*Datenschutz:*

Grimm, R., Löhndorf N. und Rossnagel, A (2000): e-Commerce meets e-Privacy. In: H. Bäumler (Hrsg.): E-Privacy – Datenschutz im Internet, Tagungsband der Kieler Sommerakademie 2000, Vieweg Verlag , Braunschweig, Wiesbaden, August 2000, S. 133-140.

Grimm, R., Rossnagel, A. (2000a): Datenschutz für das Internet in den USA. In: Datenschutz und Datensicherheit (DuD) 8/2000, August 2000, Vieweg Verlag, Wiesbaden, S.446-453.

Grimm R., Rossnagel, A. (2000b): Can P3P help to protect privacy worldwide? Proceedings of the ACM International Workshop on Multimedia and Security, November 4, 2000. Los Angeles, California, pp 157-161.

### 1.4.2 Bekannte Konstruktionen, Verfahren und Schutzrechte, die für die Durchführung des Vorhabens benutzt wurden

*Benutzte Software Komponenten für die Public Key Infrastructure (PKI):*

- Bouncy Castle Crypto APIs: http://www.bouncycastle.org/

- Technische Universität Graz, Institute for Applied Information Processing and Communications (IAIK): Java-Cryptography and Java-Security Archive

http://jce.iaik.tugraz.at/download/evaluation/index.php

*Benutzte Software Komponenten für das e-payment:*

- Lizenz-Vertrag mit der 4FriendsOnly.com Internet Technologies AG: 4FO Paybest Shop

*Untersuchte, aber nicht in das Tutor System implementierte Software Komponenten für die PKI:*

- Technische Universität Darmstadt: FlexiTrust PKI Software

- Fraunhofer SIT Darmstadt: MMS CA Software

*Untersuchte, aber nicht in das Tutor System implementierte Software Komponenten für das e-payment:*

- Firstgate Click&Buy

- Paybox

- Paysafecard

### 1.4.3 Verwendete Fachliteratur sowie benutzte Informations- und Dokumentationsdienste

*Fachliteratur:*

Datenschutz und Datensicherheit. (monatliche Fachzeitschrift) Vieweg, Wiesbaden, 2001-2003.

Fraunhofer SIT Darmstadt: „Sinn und Zweck“ einer Public Key Infrastruktur: http://pki.fraunhofer.de/einfuehrung.html

Grimm, R.: Vertrauen im Internet (Vorlesungsskript), 2000.

Middendorf, S., Singer, R. (1999): Programmierhandbuch und Referenz für die Java-2-Plattform. dpunkt-Verlag, Heidelberg, 1999.

Signaturgesetz: http://www.bsi.bund.de/esig/basics/legalbas/sigg2001.pdf

Schmeh, K. (1998): Safer Net. dpunkt-Verlag, Heidelberg, 1998.

Schneier, B. (2001): Secrets and Lies. IT-Sicherheit in einer vernetzten Welt. dpunkt-Verlag/Wiley, 2001.

Tung, B. (1999): Kerberos: A Network Authentication System. Addison Wesley Publishing Company, 1999.

*Programmierhilfen:*

- Microsoft Internet Explorer Site: Internet Explorer Features. 08/2001, http://www.microsoft.com/windows/ie/evaluation/features/default.asp

- Netscape Dokumentation Web-Site: DevEdge Online Documentation - Introduction to the Capabilities Classes. 06/1997 http://developer.netscape.com/docs/manuals/signedobj/capabilities/index.html

- Netscape Dokumentation Web-Site: DevEdge Online Documentation - Signing Software with Netscape Signing Tool. 1999 http://developer.netscape.com/docs/manuals/signedobj/ capabilities/index.html

- Sun Developer Help: Signing Jar files for Netscape Communicator with signtool. 08/2002, http://java.sun.com/developer/onlineTraining/Security/Fundamentals/magercises/Signtool/

*Standards:*

- RFC 1421-1424 - PEM-Standard (Schalenmodell): http://www.ietf.org/rfc/rfc1421.txt

- RFC 1510 - The Kerberos Network Authentication Service (V5): http://www.ietf.org/rfc/rfc1510.txt

- RFC 2246 - The TLS Protocol: http://www.ietf.org/rfc/rfc2246.txt

- RFC 2251-2256 - Lightweight Directory Access Protocol: http://www.ietf.org/rfc/rfc2251.txt

- RFC 2440 - OpenPGP Message Format: http://www.ietf.org/rfc/rfc2440.txt

- RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile: http://www.ietf.org/rfc/rfc2459.txt

*Informations- und Dokumentationsdienste:*

- Busch, C.: Competence Center for Applied Security Technology (CAST-Forum) Newsletter: http://www.cast-forum.de/

- Konzepte und Elemente Virtueller Hochschule (kevih) – Mailverteiler (Universität Tübingen)

### *1.5 Zusammenarbeit mit anderen Stellen*

*4FriendsOnly.com Internet Technologies AG Ilmenau:* Der Tutor wurde als Shopbetreiber registriert und das Zahlungssystem Paybest in das Tutor-System integriert. Somit wird die Möglichkeit zur Bezahlung für virtuelle Waren geschaffen.

*Fraunhofer IIS AEMT Ilmenau (seit 01.01.04 IDMT) und Fraunhofer SIT Darmstadt:* Die PKI („Public-Key Infrastructure“) des Tutor-Systems wurde bei der Entwicklung an die PKI von Fraunhofer angelehnt und ermöglicht. Dadurch entstand eine gemeinsame Basis zur gegenseiti-

gen Kompatibilität der ausgestellten Zertifikate und somit die Grundlage einer größeren systemübergreifenden PKI.

*Konsortialpartner DaMiT:* Universität Bonn (Prof. Dr. Stefan Wrobel), Technische Universität Chemnitz (Prof. Dr. Werner Dilger), Technische Universität Cottbus (Prof. Dr. Bernhard Thalheim), Technische Universität Darmstadt (Prof. Dr. Wolfgang Bibel), Universität Freiburg (Prof. Dr. Gerhard Strube), Universität Kaiserslautern (Prof. Dr. Rolf Wiehagen), Universität Lübeck (Prof. Dr. Thomas Zeugmann), Universität des Saarlandes (Prof. Dr. Jörg Siekmann) und Hochschule Wismar (Prof. Dr. Jürgen Cleve).

# 2 Ergebnisse und Nutzen

## *2.1 Ergebnisse*

### 2.1.1 Arbeitspaket 7.1: Überblick über elektronische Zahlungsverfahren

Im Arbeitspaket AP 7.1 wurde aufgrund von Vorarbeiten und aktuellen Recherchen ein Überblick über Elektronische Zahlungsverfahren erarbeitet. Neben internen Projektberichten (z.B. Folien zum Treffen mit Prof. Klaus Jantke in Ilmenau, 15.8.2001, und zum ersten Projekttreffen in Darmstadt, 17.9.2001) gingen die Ergebnisse in eine Reihe von Arbeiten der TU Ilmenau und ihrer Kooperationspartner ein:

- *Stetig aktualisiertes Handbuch der studentischen Praxiswerkstatt:*

Grimm, R., Fasel, A.: Handbuch/Praxisbericht - Elektronische Zahlungssysteme. Studentische Arbeiten im Rahmen der „Praxiswerkstatt für Zahlungssysteme“. Version 3.0 vom Sommersemester 2002, Version 3.1 vom Wintersemester 2002/03, Version 3.2 vom Sommersemester 2003 usw., TU Ilmenau, Fachgebiet Multimediale Anwendungen. Ilmenau, September 2003.

Es ist von entscheidender Bedeutung, dass diese Arbeit stetig weitergeführt wird, da die Untersuchungs- und Vergleichskriterien nicht statisch vorzugeben sind, sondern sich mit der wirtschaftlichen Entwicklung des Themas verändern. Neben den bereits bewährten Kriterien führen die Tester im Labor aufgrund ihrer aktuellen Erfahrung neue Kriterien ein, erkennen bisherige Kriterien als irrelevant und ordnen Kriterien auf neue Weise. Die Erfahrung von DaMiT ist hier entscheidend eingegangen (siehe auch die Beiträge von A. Fasel und A. Zobel auf der LIT’02).

- *Begleitende Projekt- und Diplomarbeiten, gute Ergebnisse erzielten dabei:*

Boos, Wolfgang, Nathrath, Tina, Schmidt, Andreas (2001): Die Bedeutung des elektronischen Zahlungssystems Geldkarte unter besonderer Berücksichtigung zukünftiger Applikationen. In Kooperation mit E-Commerce Testlabor. Betreuer Grimm, Dezember 2001.

Zobel, Angelika (2002): Kriterien zur Bewertung elektronischer Zahlungssysteme. In Kooperation mit E-Commerce-Testlabor. Betreuer Fasel, Grimm. September 2002.

Lorenz, Oliver (2004): Konzeption und Realisierung eines anbieterunabhängigen Web-Services zur Autorisierung von Online-Zahlungsaktionen. Betreuer: Fengler, Nützel (Informatik), Grimm. März 2004.

- *Auf den Leipziger Informatiktagen (LIT 2002) trug Andreas Fasel Ergebnisse der strukturierten Untersuchung elektronischer Zahlungssysteme vor:*

Fasel, A., Zobel, A (2002): Analyse elektronischer Zahlungssysteme. In: K. Jantke, W. Wittig, J. Herrmann (Hrsg.): Von e-Learning bis e-Payment. Das Internet als sicherer Marktplatz. Tagungsband LIT'02. Berlin, Akademische Verlagsgesellschaft Aka, 2002.

- Das *Zahlungssystem Paybest der Ilmenauer Firma 4FriendsOnly AG (4FO AG):*

In kontinuierlicher Kooperation mit der 4FO AG wurde wurde Paybest im Laufe des Projektablaufes weiterentwickelt. Dabei gingen auch Erkenntnisse dieses Arbeitspaketes sowie des Arbeitspaketes zur Integration von Zahlungsmöglichkeiten in das DaMiT-System ein. Das Zahlungssystem wird auf den folgenden Internetseiten fortlaufend aktuell beschrieben:

http://www.paybest.de/ und http://www.4fo.de/

- Veröffentlichung in der *europäischen Online-Zeitschrift epso-N:*

Die Entwicklung von Paybest und seine Integration in einen E-Learning-Service wurden von der Fachöffentlichkeit interessiert wahrgenommen. In der Online-Zeitschrift epso-N wurde die Integration von Paybest in das Download von Spielen und in das Nutzen des Data Mining Tutor beschrieben:

Centeno, Clara (: IPTS, Sevilla): Paybest, an emerging micropayment solution for digital goods and services. In: epso-N: Electronic Payment Systems Observatory – Newsletter, No 12, Feb 2002.

http://epso.jrc.es/newsletter

### 2.1.2 Arbeitspaket 7.2: Integration von Zahlungsmöglichkeiten in das DaMiT System

Im Arbeitspaket AP 7.2 wurde auf der Basis des erarbeiteten Überblicks über elektronische Zahlungsverfahren (AP 7.1) die Integration von Zahlungsmöglichkeiten in das DaMiT-System entwickelt. Neben internen Projektberichten (z.B. Folien zum zweiten Projekttreffen in Ilmenau, 24./25.1.2002) gingen die Ergebnisse in eine Reihe von Arbeiten der TU Ilmenau und ihrer Kooperationspartner ein:

- *Leipziger Informatiktage (LIT 2002):*

In einem *wissenschaftlichen Beitrag zu den Leipziger Informatiktagen (LIT 2002)* trug B. Schulz-Brünken theoretische Überlegungen sowie praktische Ergebnisse eines kunden- und bezahlorientierten Rollenmodells für E-Learning (insbesondere für den Data Mining Tutor) vor:

Schulz-Brünken, B., Herrmann, K., Grimm, R. (2002): Kundenrollen als Vermarktungskonzept im E-Learning. In: K. Jantke, W. Wittig, J. Herrmann (Hrsg.): Von e-Learning bis e-Payment. Das Internet als sicherer Marktplatz. Tagungsband LIT'02 (Leipzig, Sep 2002). Berlin, Akademische Verlagsgesellschaft Aka, 2002, S. 20-26.

- *Implementierung der Integration von Zahlungssystemen in den Data Mining Tutor*:

Das entscheidende und wichtigste Ergebnis dieser Integrationsarbeit ist die *Implementierung der Integration von Zahlungssystemen in den Data Mining Tutor*. Je nach der Kundenrolle hat dabei der Nutzer von DaMiT die Möglichkeit, anonym mit Paybest über Telefonwertmarken, persönlich mit der Kreditkarte, oder wahlweise mit einem anderen von Paybest unterstützten Zahlungssystem zu bezahlen. Dazu gehören Firstgate Click&Buy, Paysafecard, Paybox (seit November 2003 Moxmo) und Paypal. Die Integration weiterer Zahlungssysteme (wie etwa Moneybookers) ist in Arbeit. Durch die Kooperation mit der Firma 4FO AG und ihrem Zahlungsservice Paybest, das wir von DaMiT aus unterstützt haben, ist eine Nachhaltigkeit dieser Integrationsarbeit über die Projektlaufzeit von DaMiT hinaus garantiert.

### 2.1.3 Arbeitspaket 7.3: Zugangskontrolle

Im Arbeitspaket AP 7.3 wurden Anforderungsanalysen, Umsetzungsmöglichkeiten und exemplarische Implementierungen von Verfahren der Zugangskontrolle durchgeführt und erarbeitet. Die hierbei erzielten Ergebnisse gingen dabei sowohl in interne Projektberichte als auch in Arbeiten der TU Ilmenau und ihrer Kooperationspartner ein. Sie lassen sich wie folgt strukturieren und festhalten:

- *Analyse und Erprobung von Möglichkeiten der Zugangskontrolle:*

Hier wurde ein Überblick über den aktuellen Stand der Zugangskontrollmöglichkeiten mittels Authentifizierung und die exemplarische Implementierung der gängigen Verfahren durch Mitarbeiter und Studenten des Fachgebiets erarbeitet:

Internes Dokument: „Zugangskontrolle".

Der Zugang zum System wird durch die Benutzerrolle definiert, die neben den Bezahlungsmodellen auch die Zugangsregeln zum System festlegt:

Dokumente: "Benutzermodellierung im DaMiT-Projekt: Aktueller Stand" [IL-001], "Vorstellung eines Billing Modells für DaMiT-S" [pm2pptTUI].

- *Untersuchungen zu Public Key Infrastructures (PKIs):*

Es erfolgte die Untersuchung und Bewertung möglicher PKI-Verfahren und -Bestandteile im Bezug auf den Einsatz im DaMiT-System, wobei die folgenden wichtigsten PKI-Bestandteile einbezogen wurden: Certification Authority (CA), Registration Authorities (RAs), Certificate Revocation Lists (CRLs), der Verzeichnisdienst, die eingesetzte Policy und die verwandten Zertifizierungspfade.

Dokumente: "Sicherheitsanforderungen in DaMiT" [IL-002-01], "Strategie für die PKI in DaMiT" [IL-004]

Es wurde einer Auswahl möglicher Angriffe untersucht und ein Überblick über Sicherungsmöglichkeiten von digitalen Waren und Dienstleistungen gegeben.

Dokument: "Strategie für die PKI in DaMiT" [IL-004]

In einem *wissenschaftlichen Beitrag zu den Leipziger Informatiktagen (LIT 2003)* trug K. Herrmann das PKI-Konzept für DaMiT vor:

Herrmann, K.: Public Key Infrastructure (PKI) im Data Mining Tutor (DaMiT). LIT – Leipziger Informatiktage, HTWK Leipzig, 25.09.03.

- *Analyse und Erprobung von Signaturanwendungen:*

Um Signaturanwendungen ins System zu integrieren, erfolgte zuerst eine Analyse der möglichen signaturrelevanten Parameter für die PKI-Zertifikate. Das sind die Verschlüsselungsalgorithmen, die Schlüssellänge, der Fingerabdruckalgorithmus, die Arten der Signaturen, die nun spezifiziert werden konnten und ihre Einbettung in die Kommunikationsprotokolle.

Der Einsatz von Signaturanwendungen mittels PKI-Zertifikaten erfolgt neben der Sicherstellung von Integrität und Authentizität von E-Mails in zwei weiteren Anwendungsfällen. Zum einen können Aufgabenlösungen durch den Studenten im Lernsystem signiert werden, um die ständige Verfügbarkeit einer Originalitäts- und Authentizitätsprüfung zu gewährleisten und gleichzeitig den Zeitpunkt der Einreichung transparent zu machen. Zum anderen ist der Zugang zum Tutor-System mittels Benutzerzertifikat durch elektronische Signaturen realisiert worden.

Dokument: "Sicherheitsanforderungen in DaMiT" [IL-002-01]

Des Weiteren besteht auch die Möglichkeit der elektronischen Signatur von Java-Applets, diese ist jedoch im Tutor-System bislang noch nicht zum Einsatz gekommen.

Dokument: "Sicherheit bei Java-Anwendungen" [IL-003-01]

An einem Szenario für die Benutzung von signierter Kommunikation beim Abschluss eines Nutzungsvertrages mit dem DaMiT-System wird derzeit gearbeitet. Es wurde bisher noch nicht veröffentlicht.

- *Untersuchung und exemplarische Implementierung von Verschlüsselungsanwendungen:*

Auch hier erfolgte eine Analyse von möglichen Verschlüsselungsparametern für PKI-Zertifikate. Das sind die Verschlüsselungsalgorithmen, die Schlüssellänge und ihre Einbettung in die Kommunikationsprotokolle.

Verschlüsselung wird auf zwei Ebenen angewendet: Erstens werden E-Mails zum Schutz vor unautorisiertem Lesen und Manipulieren der Nachrichten verschlüsselt (S/MIME). Zweitens wird der Übertragungskanal zwischen Benutzern und dem Lernsystem im Web verschlüsselt und dadurch in seiner Vertraulichkeit geschützt (SSL – Secure Socket-Layer).

Dokument: "Sicherheitsanforderungen in DaMiT" [IL-002-01]

- *Entwurf, Entwicklung und Implementierung einer Public Key Infrastructure (PKI):*

Der Entwurf und die Entwicklung der PKI entstanden in enger Kooperation mit dem Fraunhofer SIT Darmstadt. Durch die Zusammenarbeit konnte eine Umsetzung der PKI realisiert werden, die ein Zusammenspiel mit anderen PKIs ermöglicht. Diese entstand, nachdem ein Überblick über mögliche Strategien des Zusammenspiels mit anderen PKIs erarbeitet wurde.

Internes Dokument: "Verbinden von unabhängigen PKIs"

Es folgte die Erweiterung und Anpassung der PKI-Zertifikate auf das vorhandene Kundenrollenmodell und die vorhandene Benutzerdatenbankstruktur. Daraus resultierte ein erster Entwurf einer eigenen PKI für DaMiT, sowie Spezifikationen zu den Teilen der PKI. Hierzu gehörte die Spezifizierung von Zertifikatsparametern, der Certification Authority (CA), der Rolle der Registration Authorities (RAs) sowie einer Policy, welche Szenarios für die Vergabe von Zertifikaten an RAs sowie an Studierende beschreibt.

Dokumente: "Sicherheitsanforderungen in DaMiT" [IL-002-01], "Strategie für die PKI in DaMiT" [IL-004] und "Festlegungen zur Registration Policy" [SB-037]

- *Spezifizierung der Zertifikatsparameter:*
  - verwendeter Verschlüsselungsalgorithmus ist RSA
  - verwendete Schlüssellänge beträgt 1024 Bit
  - der Fingerabdruckalgorithmus ist SHA1
  - der Gültigkeitszeitraum wird auf 6 Monate festgesetzt
  - die Zertifikatserzeugung erfolgt am Server
  - die benutzten Zertifikatstypen sind X.509v3-Zertifikate mit folgenden Attributen: Vorname, Name; E-Mail; Universität, Ort, Land; Matrikelnummer (bzw. User-ID bei RAs); Rolle; Aussteller (DaMiT-CA)

Der Identitätsbezug der Zertifikate ist über *personifizierte Zertifikate* hergestellt. Das benutzte Prüfungsmodell der Zertifikate ist das *Schalenmodell*, d.h. der Zeitpunkt der Signatur muss innerhalb des Gültigkeitszeitraums aller Zertifiate der Zertifikatskette liegen. Die Art der benutzten Signaturen ist die *fortgeschrittene elektronische Signatur*. Die benutzte Software ist *Java 1.4 mit IAIK Archiv*. Das benötigte *Plugin ist Java 1.4.1*. Das Zusammenspiel mit anderen PKIs ist festgelegt worden. Die Funktionalitäten des PSEs („Personal Security Environment“, das sind etwa Smartcards oder Passwort-geschützte Dateien auf dem PC, jeweils im ausschließlichen persönlichen Zugriff ihres Besitzers) wurden spezifiziert.

Nun konnten die Möglichkeiten der Verlängerung von abgelaufenen Zertifikaten und Benutzerkonten analysiert werden und hieraus eine Spezifikation zur Verlängerung abgelaufener PKI-Zertifikate und Benutzerkonten erstellt werden.

Dokument: "Memo zur Verlängerung von Login bzw. Zertifikat" [IL-005]

Es erfolgten nun exemplarische Implementierungen für den Signiervorgang der benutzerspezifischen Aufgabenlösungen, für eine Zugangskontrolle (Login) mittels PKI-Zertifikaten, sowie, mittels verschiedener Verfahren für eine Certification Authority (CA). Daraufhin wurden die im DaMiT-System einzusetzenden Funktionalitäten und die entsprechend zu nutzenden Verfahren festgelegt und beschrieben.

Dokument: "Strategie für die PKI in DaMiT" [IL-004]

Ins aktuelle Tutor-System wurde weiterhin die Hilfe- und FAQ-Unterstützung zur PKI integriert („FAQ“ = „Frequently Asked Questions“: das sind im Web übliche Online-Listen von am meisten geäußerten Fragen und deren Antworten). Eine Dokumentation und Illustrationen der PKI-Funktionalitäten dienen den Anwendern und den Produzenten des Inhalts als Hilfe.

Dokumente: "Public Key Infrastructure (PKI) in DaMiT - Aktueller Stand" [PM8-PKI], "Herzlich Willkommen zur PKI von DaMiT", "FAQs"

### 2.1.4 Arbeitspakete 7.4 und 7.5: Implementierung eines *Zahlungssystems* und eines *Zugriffskontrollverfahrens* in das DaMiT System

In den Arbeitspaketen AP 7.4 und AP 7.5 ist schließlich die Implementierung eines geeigneten Zahlungssystems sowie eines geeigneten Zugriffskontrollverfahrens in das DaMiT System vorgesehen. Die hierbei erzielten Ergebnisse lassen sich dabei wie folgt durch den aktuellen Systemstand dokumentieren:

- *Benutzerrollen:*

In der Metadaten-Spezifikation sind die *Benutzerrollen* definiert, die schließlich im System umgesetzt wurden. Es bestehen die Möglichkeiten, sich als Gast (anonym) oder als der Standard Lernende (Student) im System zu bewegen. Die Inhalte werden den Studenten kostenfrei zur Verfügung gestellt, während der Gast für bestimmte Inhalte bezahlen muss. Die Kostenpflichtigkeit der Inhalte ist somit rollenabhängig.

Dokument: "Metadaten im DaMiT-System" [KL-001], http://damit.dfki.de/

- *Paybest mit 4FriendsOnly.com Internet Technologies AG (4FO AG):*

Im Data Mining Tutor wird als integriertes Zahlungssystem Paybest von 4FriendsOnly.com Internet Technologies AG (kurz 4FO) genutzt. Zu diesem Zweck hat das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI GmbH) einen Lizenzvertrag mit 4FO über den Einsatz von Paybest abgeschlossen. Das DaMiT-System wurde als Shop bei 4FO registriert und aktiviert. Der Einsatz von Paybest als (Meta-)Micropayment-System im Tutor ist etabliert. Die Preisinformationen zu den kostenpflichtigen Inhalten werden in der Datenbank des Tutor-Systems gehalten.

- *Integration von PKI mit Verschlüsselung, Signatur und rollenbasiertem Zugang:*

Die *PKI ist im aktuellen System* integriert. Das Rollenmodell ist auf die PKI-Zertifikate erweitert worden und jedem registrierten Benutzer wird nach der Freischaltung durch eine RA ein PKI-

Zertifikat ausgestellt. Der Zugang zum Tutor-System ist nun mittels Authentifizierung per PKI-Zertifikat möglich. Außerdem kann das Zertifikat zum Erstellen von Signaturen für E-Mails und Java-Applets genutzt werden, oder zur Verschlüsselung von E-Mails bzw. des Übertragungskanal bei der Kommunikation mit dem Tutor-System eingesetzt werden.

Dokument: "Strategie für die PKI in DaMiT" [IL-004], http://damit.dfki.de/

Eine weitere Untersuchung zu PKI-Zertifikaten beschäftigte sich mit der Analyse und Darstellung der möglichen Verlängerung von abgelaufenen Zertifikaten und Benutzerkonten. Hieraus entstand eine Spezifikation zur Verlängerung abgelaufener PKI-Zertifikate und Benutzerkonten.

Dokument: "Memo zur Verlängerung von Login bzw. Zertifikat" [IL-005].

Ins System wurde nun neben der Möglichkeit von Signatur und Verschlüsselung bei der E-Mail-Kommunikation auch eine alternative Zugangsform "Login per Zertifikat" integriert, die eine Authentifizierung beim Login durch PKI-Zertifikate ermöglicht. Weiterhin wurde die Implementierung und Integration von Signatur- und Verschlüsselung beim Einreichen von benutzerspezifischen Aufgabenlösungen in das DaMiT-System durchgeführt. Eine generelle Verschlüsselung bei der Kommunikation mit dem Tutor-System, z. B. beim Download, schützt die Anwender vor dem Mitlesen und vor Manipulationen durch Fremde. Die Funktionalitäten für die Signatur von Java-Applets sind bereits vorgesehen und können bei Bedarf eingesetzt werden.

http://damit.dfki.de/

- *Aufbau von CA- und RA-Betrieb*

Es erfolgten die Implementierung und der Aufbau der Certification Authority (CA), sowie die Spezifizierung der Rolle der Registration Authorities (RAs).

Dokument: "Festlegungen zur Registration Policy" [SB-037], http://damit.dfki.de/ (Stand: 11.02.04)

- *Einsatz im Seminar:*

Das DaMiT-System wurde den Studierenden in der universitären Lehre bekannt gemacht und in einem Seminar von den Studierenden untersucht.

Seminarreferat: http://www.stud.tu-ilmenau.de/~sase-mw/warenkorbanalyse.zip

## 2.2 Voraussichtlicher Nutzen, insbesondere Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplanes

Der voraussichtliche Nutzen der Ergebnisse unseres Teilprojektes in DaMiT soll anhand der folgenden Aspekte verdeutlicht werden.

1. *Werteangemessenes Dienstangebot von E-Learning-Systemen:*
   Nur der Nutzer, der auch die Berechtigung erworben hat, bekommt Zugang zu den Lerninhalten des DaMiT-Systems. Das System sieht verschiedene Benutzerrollen vor (Rollenmo-

dell im DaMiT: Gast und Standard Lerner). Die Kosten für die Lerninhalte sind rollenabhängig.

2. *Kommerzielle Auswertbarkeit:*
   Das Rollenmodell des Systems wurde auf der Basis des Prinzips entworfen: „Wer für die Lerninhalte bezahlt, bekommt mehr Inhalt und mehr Service zur Verfügung gestellt." Ein Testbesuch des Systems zum Kennen lernen der Angebote ist kostenlos. Im Rollenmodell wurde ebenfalls definiert, dass Studenten freien Zugang zu den Inhalten haben.
3. *Schutz der Nutzer:*
   Der Schutz der Nutzer wird durch das Rollenmodell des Systems berücksichtigt. Die folgenden Teilaspekte spielen beim Schutz der Nutzer eine wichtige Rolle: Datenschutz, Vertraulichkeit und Gruppenschutz. Der Gruppenschutz bedeutet in diesem Zusammenhang, dass der Vertraulichkeitsschutz der Lerngruppen voreinander gewahrt werden muss, um z. B. Betrugsversuche zu verhindern. Der Benutzer, der das System als Gast nutzt, tut dies anonym und kostenlos. Erst wenn er die Lerninhalte ausführlich und mit der Unterstützung des Systems bearbeiten möchte, muss er Daten von sich preisgeben (pseudonym, Benutzername usw.), die vertraulich und sicher behandelt werden (z. B. verschlüsselte Übertragung mit SSL). Eine Ausnahme bilden Studierende, die sich u. a. anhand ihrer Matrikelnummer identifizieren müssen. Sie erhalten keinen anonymen aber dafür einen kostenfreien Zugang zum Data Mining Tutor.
4. *Spezielle Förderung von Studierenden:*
   Das DaMiT-System möchte Studierende fördern, indem es ihnen einen bequemen und kostenfreien Zugang zu den Lerninhalten ermöglicht. Die besondere Nutzergruppe „Studierende" wurde bei der Definition des Rollenmodells und bei dessen Umsetzung in der PKI und dem SSL-Login in das DaMiT-System berücksichtigt.

### 2.3 Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen, der während des Vorhabens bekannt geworden ist

Es sind keine Projekte bekannt, die im gleichen Maße wie DaMiT auf diese drei Schwerpunkte eingehen:

1. Zahlungsfunktionalität (e-Payment) für digitale Waren und Dienstleistungen,
2. Benutzerrollenmodell für verschiedene Anwendertypen (anonym, pseudonym, Student, Manager),
3. sowie die Nutzung einer PKI zur Gewährleistung von Zugangskontrolle, Vertraulichkeit und Integrität eingehen.

Die folgenden Projekte behandelten Teilaspekte:

- *Projekt AN.ON* (http://anon-online.de): garantierte Online-Anonymität für Internetbenutzer (Technische Universität Dresden, Freie Universität Berlin, ULD)
- Projekt WebGEO (http://www.webgeo.de/): anonymisiert Benutzerdaten
- *Überblick über Lern-Management-Systeme (LMS):*

- untersucht wurden CLIX, WebCT, eLS, ILIAS und Blackboard;
- in allen untersuchten Projekten wird eine PKI bisher nicht eingesetzt;
- e-Payment ist in den untersuchten Projekten nur vereinzelt vertreten und nicht in dem Maße differenziert, wie im DaMiT-System;
- e-Payment wird in Lehr- und Lernsystemen eingesetzt, allerdings geht es dabei meist um den pauschalen Erwerb von gesamten Kursen oder Kursblöcken - bei DaMiT wird die Zahlungsfunktion speziell auf einzelne Programme (Applets) bzw. (pay-per-feature) angewendet.

Dokument: "Lernplattformen" [SB-040]

- In den Markt neu eingeführte *Zahlungssysteme* werden kontinuierlich beobachtet und soweit relevant berücksichtigt (z.B. Paybest, PayPal). Teilweise sind beobachtete und versuchsweise implementierte Zahlungssysteme in dieser Form *nicht mehr am Markt verfügbar* (Paybox, CyberCash, eCash).
- *Benutzerrollenmodelle* werden in verschiedenen Systemen bereits eingesetzt.
- *PKIs mit Zertifikaten* sind in Lehr- und Lernsystemen bisher nicht vorhanden, wohl aber in anderen sicherheitsrelevanten Anwendungen des E-Commerce und E-Government (vgl. www.bsi.de und ISIS-MTT).
- *Neue Zugangskontrollverfahren und PKI-Lösungen* werden beobachtet und untersucht (z.B. FlexiTrust PKI, Bridge-CA).

## 2.4 Erfolgte oder geplante Veröffentlichungen

Die Ergebnisse unseres Teilprojektes zu DaMiT wurden während der Laufzeit des Projektes veröffentlicht.

*Zahlungssysteme:*

Grimm, R., Fasel, A. (2002/2003): Handbuch/Praxisbericht - Elektronische Zahlungssysteme. Studentische Arbeiten im Rahmen der „Praxiswerkstatt für Zahlungssysteme“. Version 3.0 vom Sommersemester 2002, Version 3.1 vom Wintersemester 2002/03, Version 3.2 vom Sommersemester 2003 usw., TU Ilmenau, Fachgebiet Multimediale Anwendungen. Ilmenau, September 2003.

Fasel, A. , Zobel, A (2002): Analyse elektronischer Zahlungssysteme. In: K. Jantke, W. Wittig, J. Herrmann (Hrsg.): Von e-Learning bis e-Payment. Das Internet als sicherer Marktplatz. Tagungsband LIT’02. Berlin, Akademische Verlagsgesellschaft Aka, 2002.

*Sicherheit und Zugangskontrolle:*

Grimm, R. (2002): Schwerpunkt Virtuelle Waren. Datenschutz und Datensicherheit (DuD) 5/2002, Mai 2002, Vieweg Verlag, Wiesbaden.

Schulz-Brünken, B., Herrmann, K., Grimm, R. (2002): Kundenrollen als Vermarktungskonzept in E-Learning. In: K. Jantke, W. Wittig, J. Herrmann (Hrsg.): Von e-Learning bis e-Payment. Das Internet als sicherer Marktplatz. Tagungsband LIT'02 (Leipzig, Sep 2002). Berlin, Akademische Verlagsgesellschaft Aka, 2002, S. 20-26.

Grimm, R., Nützel, J. (2002): Digital Rights Management, Security and Business Models. Proceedings of the ACM Multimedia 2002 Workshops – Multimedia and Security. Dec 6, 2002, Juan le Pins, France. (http://www1.acm.org/sigs/sigmm/MM2002/)

Grimm, R. (2003): Digital Rights Management: technisch-organisatorische Lösungsansätze. In: Arnold Picot (Hrsg.): Digital Rights Management. Springer: Berlin, Heidelberg, New York, 2003, S. 93-106.

Herrmann, K.: Public Key Infrastructure (PKI) im Data Mining Tutor (DaMiT). LIT – Leipziger Informatiktage, HTWK Leipzig, 25.09.03. (http://www.wi.hs-wismar.de/~cleve/wslit/)

*Datenschutz:*

Grimm, R. (2002): Datenschutz im elektronischen Geschäftsverkehr. Beitrag zum 6. IIR-Kongress C@sh World 2002 – Elektronische Bezahlsysteme, 20.2.2002, Frankfurt/M., 8 S.

Rossnagel, A., Banzhaf, J., Grimm, R. (2003): Datenschutz im Electronic Commerce. Schriftenreihe Kommunikation und Recht. Verlag Recht und Wirtschaft, Heidelberg, 2003, 325 S.

# 3 Zusammenfassende Betrachtung und Ausblick

## *3.1 Beitrag des Ergebnisses zu den förderpolitischen Zielen des Förderprogramms, -schwerpunkts, -konzepts*

Das förderpolitische Ziel des Programms besteht in der Unterstützung der Entwicklung und des Einsatzes der neuen Medien in der Bildung. Das Ergebnis dieses Teilprojektes lässt sich in den folgenden vier Punkten auf die förderpolitischen Ziele des Programms beziehen:

1. Ein werteangemessenes Dienstangebot von E-Learning-Systemen
2. Die kommerzielle Auswertbarkeit des Angebots:
   - elektronische Zahlungsmöglichkeiten,
   - Wer bezahlt, bekommt mehr
3. Schutz der Nutzer:
   - Datenschutz,
   - Vertraulichkeitsschutz der Gruppen voreinander,
   - Rollenkonzept (anonymer oder persönlicher Zugang)
4. Spezielle Förderung von Studierenden:
   - bequemer und kostenfreier Zugang
5. Passwort- oder Signaturgeschützter Zugang über Secure Socket Layer (SSL)

## *3.2 Wissenschaftlich-technisches Ergebnis des Vorhabens, die erreichten Nebenergebnisse und die gesammelten wesentlichen Erfahrungen*

Die wissenschaftlich-technischen Ergebnisse unseres Teilprojektes sollen an dieser Stelle noch einmal in Bezug auf die Arbeitspakete dargestellt werden.

Im Arbeitspaket AP 7.1 wurde eine strukturierte Analyse einer Reihe von elektronischen Zahlungsverfahren erarbeitet, die durch eine Nutzwertanalyse der Zahlungssysteme ergänzt wurde (Handbuch Zahlungssysteme). Außerdem wurde das bereits vor Projektbeginn existierende elektronische Zahlungssystem Paybest der Ilmenauer Firma 4FO AG weiterentwickelt und in das DaMiT-System integriert (AP 7.4 und 7.5).

Das Arbeitspaket AP 7.2 beschäftigte sich mit der Integration von Zahlungsmöglichkeiten in das DaMiT-System. Im Rahmen dieses Arbeitspaketes wurde eine sinnvolle, pädagogisch-didaktische Integration von Zahlungsmöglichkeiten in Lernmodule entwickelt, die auf dem Grundsatz: „Wer zahlt, bekommt Zugang zu mehr Inhalten“ basiert. Lerninhalte und der Zugang zu diesen Inhalten stellen also einen Wert an sich dar, der kommerziell vermarktet werden kann. Eine Ausnahme bilden im DaMiT-System Studierende. Ihnen wird, um ihre Studienarbeit zu fördern, der Zugang zu den Lerninhalten des Systems kostenfrei ermöglicht.

Das Arbeitspaket 7.3 setzte sich mit dem Thema der Zugangskontrolle auseinander. Die Basis für alle weiteren Arbeiten bildete das ökonomische, lernbezogene Rollenmodell (verschiedene Benutzerrollen: Gast, Standard-Lerner, Studierende). Dieses Rollenmodell musste bei der Umsetzung der Zugriffssteuerung auf die Inhalte und bei den Zahlungsanforderungen berücksichtigt werden. Um die Zugangskontrolle für die Benutzer einfach und bequem zu gestalten, wurden eine Public Key Infrastructure (PKI) und das elektronische Verschlüsselungsprotokoll SSL eingesetzt.

## *3.3 Fortschreibung des Verwertungsplanes*

### 3.3.1 Erfindungen und Schutzrechte

Erfindungen wurden im Rahmen unseres Teilprojektes von DaMiT nicht gemacht, daher wurden auch keine Schutzrechte angemeldet. Allerdings sind Erkenntnisse von DaMiT sowohl in die weitere Entwicklung von Paybest, als auch in die Entwicklung von Modellen virtueller Waren im Rahmen des Engagements des Fachgebietes Multimediale Anwendungen in der Fraunhofer Arbeitsgruppe für Elektronische Medientechnik (AEMT) in Ilmenau (seit 01.01.04 IDMT) eingegangen. Auch die Entwicklung der Praxiswerkstatt Elektronische Zahlungssysteme mit der Entstehung der Elektronischen Litfaßsäule für elektronische Zahlungssysteme (LITEZ) sind durch die Arbeiten in DaMiT beeinflusst worden.

### 3.3.2 Wirtschaftliche Erfolgsaussichten nach dem Ende des Projekts

In erster Linie legte unser Teilprojekt die technische Basis dafür, dass der Data Mining Tutor, der vom gesamten Konsortium gemeinsam entwickelt wurde, überhaupt die Möglichkeit hat, ein kommerzieller Dienst zu werden, indem wir den Zugangsschutz und die elektronischen Zah-

lungsmöglichkeiten für die Nutzer eingeführt haben. Ein besonderer Vorteil gegenüber anderen Schutz- und Zahlungsvorrichtungen *(Alleinstellungsmerkmal von DaMiT)* besteht darin, dass wir in einem Kundenrollenmodell die spezifischen Nutzungsbedürfnisse befriedigen können. Premiumnutzer können wertvolle Dienste in persönlicher Bindung an den Dienst bezahlen und auswerten, Studenten haben bequemen und freien Zugang, anonyme Nutzer können kostenlos testen oder mit einfachen anonymen Zahlverfahren wertvolle Informationen kaufen.

Unsere Schutzmechanismen haben allein keine kommerzielle Perspektive. Sie wirken nur im Rahmen des integrierten DaMiT-Rollenmodells. Ob und in welchem Maße DaMiT als Ganzes kommerziell erfolgreich eingesetzt werden kann, ist in diesem Bericht unseres Teilprojekts nicht darstellbar, sondern muss vom zusammenfassenden Bericht des Konsortialführers (Universität Saarbrücken) erörtert werden.

Die Arbeiten dieses Teilprojektes in DaMiT wirken an drei Stellen nachhaltig auf wirtschaftlich aussichtsreiche Entwicklungen:

1. auf die Weiterentwicklung des elektronischen Zahlungssystems und die Integration anderer Zahlungssysteme durch Paybest in der Ilmenauer Firma 4FO AG; *Einsatz sofort*
2. im Accounting- und Billing-Service im Rahmen der sich entwickelnden Web-Services von Digital Rights Management Systemen der Ilmenauer Fraunhofer Arbeitsgruppe für Elektronische Medientechnik (AEMT) (seit 01.01.04 IDMT); *Einsatz ab 2004*
3. In der weiterzuführenden Praxiswerkstatt „Elektronische Zahlungssysteme“. Diese ist zunächst ein studentisches Lehrangebot. Die Praxiswerkstatt wird jedoch durch eine elektronische Litfaßsäule begleitet, deren Aufgabe es ist, Anbietern von Zahlungssystemen eine Veröffentlichungsplattform zu bieten. Dieser Dienst hat eine kommerzielle Perspektive, die ab etwa Mitte 2004 auf erste Einnahmen zielt. Hier haben vor allem die Übersichtsarbeiten für elektronische Zahlungssysteme in DaMiT Einfluss genommen; *Einsatz ab sofort, fortlaufend.*

### 3.3.3 Wissenschaftliche und/oder technische Erfolgsaussichten nach Projektende

Die Arbeit in DaMiT hat die Kooperation mit anderen Arbeiten im Fachgebiet Multimediale Anwendungen, mit der Ilmenauer Firma 4FO AG und mit der Fraunhofer Arbeitsgruppe für Elektronische Medientechnik (AEMT) (seit 01.01.04 IDMT) nachhaltig beeinflusst. Diese Kooperationen auf der Basis der gewonnen Ergebnisse werden in die weitere wissenschaftlich-technische Zusammenarbeit eingehen:

- andere Arbeiten am Lehrstuhl von Prof. Grimm (Fachgebiet Multimediale Anwendungen) und dem Institut für Medien- und Kommunikationswissenschaft (IfMK) zu den Themen *Vertrauen, Zahlungssysteme, elektronische Veröffentlichung, Datenschutz*.
- Arbeiten mit der Ilmenauer Firma 4FO AG zum Thema Paybest, *elektronische Spiele, Accounting Service für virtuelle Waren.*
- Arbeiten mit der Ilmenauer Fraunhofer Arbeitsgruppe für Elektronische Medientechnik (AEMT) (seit 01.01.04 IDMT) zum Thema „Sicherheit für virtuelle Waren“, darunter *Ge-*

*schäftsmodelle für virtuelle Waren* und ihr *technischer Schutz*, hierzu gehören sowohl *Zugangsschutz zu Waren*, als auch Datenschutz der *Privatsphäre von Kunden*.

### 3.3.4 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Innerhalb des Projektes von DaMiT haben wir uns intensiv mit den Inhalten eines sinnvollen Nachfolgeprojektes auseinandergesetzt. Aus der Sicht unseres Teilprojektes stellen dabei zwei Themen eine besondere wissenschaftliche Herausforderung dar:

1. Die Entwicklung und technische Umsetzung von Geschäftsmodellen für den Vertrieb und die Pflege virtueller Dienstleistungen, in erster Linie für Lernsysteme und Spiele, die in theoretischer Hinsicht viele Gemeinsamkeiten aufweisen.
2. Die technische Unterstützung von Gruppenlernen, wobei das theoretische Konzept von Gruppen seinerseits einen offenen Forschungsgegenstand darstellt. Hier sind einerseits hierarchisch horizontale und vertikale Gruppen zu unterscheiden, andererseits zeitlich synchron und asynchron kooperierende Gruppen. Die gemeinsame Bearbeitung von Aufgaben ist ebenso zu behandeln wie die dauerhafte Archivierung von Ergebnissen für die spätere Nachbearbeitung.

Unabhängig davon, ob ein Nachfolgeprojekt in diesem Konsortium zu Stande kommt (in der gegenwärtigen wirtschaftlichen und bildungspolitischen Lage der Bundesrepublik Deutschland ist das eher unwahrscheinlich), werden diese Themen in anderen Zusammenhängen, wenn auch leider nicht in dieser thematischen Dichte und in dem Kontext des kompetenten und vielseitigen DaMiT-Konsortiums, weiter verfolgt werden. Es handelt sich nämlich um außerordentlich wichtige Forschungsfragen, wichtig sowohl für die wissenschaftlich erkenntnisorientierte, als auch für die wirtschaftliche Entwicklung unserer Gesellschaft.

## *3.4 Arbeiten, die zu keiner Lösung geführt haben*

Die ursprünglich angestrebte Teilaufgabe, Lehrinhalte zum Thema „Privacy“ (Datenschutz) als *Content* in den Data Mining Tutor einzubringen und in der Lehre einzusetzen (AP 5.6), kam zur Laufzeit des Projektes nicht zu Stande. Dieses wird Gegenstand nachfolgender studentischer Projekte.

Der Standardisierungsaspekt der Teilaufgabe, Zahlungssysteme in den DaMiT zu integrieren (AP 7.2) konnte noch nicht durchgesetzt werden. Das war im Laufe der Projektzeit auch nicht zu erwarten. Die Arbeiten hieran gehen aber weiter, etwa in Form einer Diplomarbeit (Oliver Lorenz, Informatik der TU Ilmenau, März 2004), in der Zahlungssysteme als Web-Services mit offenen, der Standardisierung zugänglichen Schnittstellen (WSDL mit dynamischen Parametern) implementiert werden.

### *3.5 Präsentationsmöglichkeiten für mögliche Nutzer*

Das System ist im Internet verfügbar (http://damit.dfki.de/).

Das System wurde auf Messen (Cebit, Learntec) und Anwenderkonferenzen (Datamining Cup) vorgestellt.

01 Rüdiger Grimm, „Vertrauen im Internet – Wie sicher soll E-Commerce sein?“, April 2001, 22 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, ruediger.grimm@tu-ilmenau.de

02 Martin Löffelholz, „Von Weber zum Web – Journalismusforschung im 21. Jahrhundert: theoretische Konzepte und empirische Befunde im systematischen Überblick“, Juli 2001, 25 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, martin.loeffelholz@tu-ilmenau.de

03 Alfred Kirpal, „Beiträge zur Mediengeschichte – Basteln, Konstruieren und Erfinden in der Radioentwicklung“, Oktober 2001, 28 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, alfred.kirpal@tu-ilmenau.de

04 Gerhard Vowe, „Medienpolitik: Regulierung der medialen öffentlichen Kommunikation“, November 2001, 68 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, gerhard.vowe@tu-ilmenau.de

05 Christiane Hänseroth, Angelika Zobel, Rüdiger Grimm, „Sicheres Homebanking in Deutschland – Ein Vergleich mit 1998 aus organisatorisch-technischer Sicht“, November 2001, 54 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, ruediger.grimm@tu-ilmenau.de

06 Paul Klimsa, Anja Richter, „Psychologische und didaktische Grundlagen des Einsatzes von Bildungsmedien“, Dezember 2001, 53 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, paul.klimsa@tu-ilmenau.de

07 Martin Löffelholz, „Von ‚neuen Medien’ zu ‚dynamischen Systemen’, Eine Bestandsaufnahme zentraler Metaphern zur Beschreibung der Emergenz öffentlicher Kommunikation“, Juli 2002, 29 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, martin.loeffelholz@tu-ilmenau.de

08 Gerhard Vowe, „Politische Kommunikation. Ein historischer und systematischer Überblick der Forschung“, September 2002, 43 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, gerhard.vowe@tu-ilmenau.de

09 Rüdiger Grimm (Ed.), „E-Learning: Beherrschbarkeit und Sicherheit“, November 2003, 90 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, ruediger.grimm@tu-ilmenau.de

10 Gerhard Vowe, „Der Informationsbegriff in der Politikwissenschaft“, Januar 2004, 25 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, gerhard.vowe@tu-ilmenau.de

11 Martin Löffelholz, David H. Weaver, Thorsten Quandt, Thomas Hanitzsch, Klaus-Dieter Altmeppen, „American and German online journalists at the beginning of the 21st century: A bi-national survey“, Januar 2004, 15 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, martin.loeffelholz@tu-ilmenau.de

12 Rüdiger Grimm, Barbara Schulz-Brünken, Konrad Herrmann, „Integration elektronischer Zahlung und Zugangskontrolle in ein elektronisches Lernsystem“, Mai 2004, 23 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, ruediger.grimm@tu-ilmenau.de

TU Ilmenau – Institut für Medien- und Kommunikationswissenschaft
Am Eichicht 1, 98693 Ilmenau

TU Ilmenau – Institut für Medien- und Kommunikationswissenschaft
Am Eichicht 1, 98693 Ilmenau