**Institut für Telematik**
unter Betreuung der
**Fraunhofer-Gesellschaft**

# Tätigkeitsbericht 2002

Tätigkeitsbericht 2002

## Progress Report 2002

# Inhalt

# Vorwort

Das fünfte Jahr des Bestehens unseres Instituts ist nun überraschenderweise sein letztes. Nicht fehlende Erfolge der wissenschaftlichen Tätigkeit sind dafür der Grund. Immerhin konnte ein drittes Patent zur sicheren Verwahrung elektronischer Dokumente angemeldet und eine Reihe von neuesten Forschungsergebnissen auf internationalen Wissenschaftstagungen vorgestellt werden. Auch gaben unsere Symposien zum „Digitales Bezahlen“ und zur „Sichere Telemedizin“ Aufschluss über jüngste Entwicklungen. Wir konnten sogar bei der europaweiten Ausschreibung eines Registers für die neue Internet Top Level Domain „.eu“ als einziger deutscher Kandidat antreten. Auch das große Interesse der Medien belegt die hohe Relevanz unserer Aktivitäten. So gab es sowohl eine Reihe von Fernsehbeiträgen in ARD, ZDF und 3sat über unsere Arbeit als auch eine Vielzahl von Berichten in der Fach- und Publikums-Presse.

Die Schwierigkeiten ergaben sich aus der stetig schlechter werdenden Wirtschaftslage und der verringerten Neigung von Unternehmen, Forschungs- und Entwicklungsaufträge zu erteilen. So konnten 2002 „lediglich“ Aufträge im Wert von etwa 500.000 Euro eingeworben werden. Zusammen mit den vom Land Rheinland-Pfalz bereitgestellten Fördermitteln hat dies erneut nicht für einen ausgeglichenen Haushalt ausgereicht. Im Umfeld der ebenfalls schwierigen Finanzlage des Landes und fehlender Zusagen über weitere Förderung sah sich der Trägerverein des Instituts deshalb genötigt, am 8. Januar 2003 die Liquidation zu beschließen.

Es ist sehr bedauerlich, dass die von uns in fünf Jahren aufgebaute Fachkompetenz nicht erhalten werden kann und es von hier aus keine interessanten Beiträge mehr zur Entwicklung der Zukunftstechnologie Telematik geben wird. Angesichts der großen internationalen Anstrengungen auf diesem Gebiet hätten wir uns von allen Beteiligten aus Wirtschaft und Politik einen längeren Atem und eine größere Bereitschaft zur Förderung unserer Arbeit gewünscht. Dennoch müssen wir dem Land dankbar sein, Mittel für einen geordneten Abbau zur Verfügung gestellt zu haben.

Univ.-Prof. Dr. sc. nat. Christoph Meinel
Prof. Dr. rer. nat. Thomas Engel

Trier, im März 2003

# Foreword

The fifth year of the existence of the Institute for Telematics is to our all surprise its last one. The reason for that is not at all based on missing results or success in the scientific work of the Institute. A third patent on safe keeping digital documents could be applied and a series of research papers were presented at important international scientific conferences. Furthermore, the both symposia on “Digital Payment” and “Secure Telemedicine” have provided competent information about most recent developments. We applied as the only German candidate for the European-wide register for the new Internet top level domain “.eu”. Another proof for the high relevance of our activities in Internet research is the great interest of the media. Thus, various contributions in German TV (ARD, ZDF, 3sat) about our work were broadcasted and a variety of reports was published in the technical press and in newspapers.

The Institute’s difficulties resulted from the bad economic situation in Germany, which has become constantly worse over the last year. Companies and institutions reduced their orders for research and development. Nevertheless, orders at the amount of approximately 500.000 EURO could be achieved in 2002. However, together with the state subsidies provided by the German state Rhineland-Palatinate this amount was not sufficient for a balanced budget. The difficult financial situation of state finances and missing promises about further subsidies lead to the decision to liquidate the institute on 15th January 2003.

For us it is very regrettable, that the professional competence in the field of future technology of telematics is unsustainable, that was established with plenty commitments by all the co-workers and researchers of the institute within these five years. In view of the large international efforts in this area we would have wished ourselves a longer breath and more willingness to promote the Institute from all persons involved in companies and politics. Nevertheless we must be grateful to the state for providing at least funds for a regular dismantling.

# Das Institut im Profil

Institut im Profil

## Grundsätzliches

Das Institut für Telematik in Trier befasst sich mit den vielfältigen, neuen Potentialen, die sich aus der Verschmelzung von Telekommunikation und Informatik ergeben. Durch die Verknüpfung von Computern, Mobilfunk und Internet schaffen wir Möglichkeiten, über stationäre und mobile Geräte aller Art jederzeit effizient auf die in den weltweit verbreiteten Computer-Netzwerken vorhandenen Informationen zugreifen, mit diesen sicher umgehen und sie intelligent nutzen zu können. Wir betreiben Hightech-Forschung, die unserer Wirtschaft einen wichtigen Entwicklungs-Vorsprung geben soll und bilden in unserer Region die hochqualifizierten IT-Nachwuchskräfte aus, die Deutschland so dringend braucht. Abläufe in Wirtschaft, Verwaltung, Verkehr und Gesundheitswesen können durch die Ergebnisse unser praxisorientierten Arbeit wesentlich rationeller gestaltet werden. Dabei streben wir danach, die Anwendungen so einfach und nutzerfreundlich wie möglich zu machen. Dadurch wird auch der Alltag in der digitalen Welt einfacher und die Freizeit bequemer.

Mit der Fraunhofer-Gesellschaft verbunden und als eingetragener Verein verfasst, sind wir Deutschlands führendes gemeinnütziges und außeruniversitäres Forschungs- und Entwicklungs-Zentrum fürs Internet. Am 1. Januar 1998 gegründet, widmen wir uns in der Tradition des Fraunhofer-Ideals sowohl der anwendungsorientierten Grundlagenforschung als auch der Entwicklung maßgeschneiderter Problemlösungen für Handel, Industrie, Medizin und Verwaltung. Der Erschließung und Weiterentwicklung neuester wissenschaftlicher Ergebnisse für eine Anwendung in Wirtschaft und Gesellschaft gilt unser besonderes Augenmerk.

Dank unserer Konstruktion sind wir sehr unabhängig. Unser Leistungsanspruch ist hoch und die Mitarbeiter sind hervorragend qualifiziert. Zudem sind wir sehr flexibel und können permanent neue Forschungsthemen aufgreifen. Deshalb gelingt es dem Institut immer wieder, in kurzer Zeit wissenschaftliche Höchstleistungen zu erbringen.

Internet/Intranet, Sicherheit der Datenkommunikation in offenen Netzen, Telemedizin, Elektronisches Publizieren, Systementwurf und –analyse, das sind die derzeitigen Forschungs- und Entwicklungsfelder unseres Instituts. (🕮 Kompetenzbereiche, 🕮 Weitere wichtige Projekte). Wir agieren sozusagen auf der Bugwelle neuester technologischer Entwicklungen und wollen durch das ‚Ausreizen' technischer Potentiale Pilotlösungen für die tägliche Praxis schaffen.

Unsere Auftraggeber sind sowohl weltbekannte Großunternehmen wie Siemens oder die Dresdner Bank als auch kleine und mittelständische Firmen, Krankenhäuser, Finanzdienstleister und Verwaltungen in Rheinland-Pfalz, Baden-Württemberg und Luxemburg.

Nach fünf Jahren Arbeit weist unsere wissenschaftliche Bilanz zwei Patente (ein weiteres beantragt), vier Promotionen (3 weitere kurz vor Abschluß) und über 90 Fachbeiträge zu internationalen Konferenzen auf – eine Leistung, die auch international zu hoher Reputation führte.

## Institutsphilosophie

Der Telematik als junger und hoch innovativer Wissenschaftsdisziplin kommt bei der Weiterentwicklung von der Informations- zur Wissensgesellschaft eine Schlüsselrolle zu. Auf diesem jungen und sich rasant umfassend entwickelnden Gebiet ist das Institut für Telematik in Trier tätig. In seiner Forschungs- und Entwicklungstätigkeit vereinigt es die Suche nach neuen wissenschaftlichen Erkenntnissen und technologischen Lösungen mit dem Bemühen, die gewonnenen Erkenntnisse und Lösungen zügig für eine praktische Nutzung in Wirtschaft und Gesellschaft zu erschließen.

Die Leistungen des Instituts werden im Rahmen von konkreten, zum überwiegenden Teil aus der Wirtschaft finanzierten Forschungs- und Entwicklungsaufträgen erbracht. Selbst Teil der Wirtschaft, kann das Institut so die Ziele seiner Projektpartner aus Wirtschaft und Gesellschaft besonders kompetent umsetzen und eine effektive Schnittstelle zwischen Wissenschaft und Wirtschaft bilden.

Die hochtalentierten Mitarbeiter des Instituts, die häufig als junge Hochschulabsolventen zum Institut kommen, können hier wissenschaftlich aktiv bleiben, sich weiter graduieren und zugleich ihre Kenntnisse in praktischen und wirtschaftlich orientierten Projekten umsetzen und erweitern. Somit bereiten wir die akademische Elite unseres Fachs durch anwendungsbezogene Projekte schnell und gezielt auf die Tätigkeit als Führungskräfte der Wirtschaft vor.

## Telematik

Die Telematik hat sich erst Anfang der 90er Jahre zu etablieren begonnen. Der Begriff ist ein Kunstwort, gebildet aus Telekommunikation und Informatik. Sie bezieht ihre Aufgaben und Anwendungen aus der durch die mit der technischen Entwicklung explosionsartig wachsenden und immer breiter verfügbaren, weltweiten Vernetzung von Computern und Geräten, die völlig neue Lösungen bei der Suche, Bereitstellung und Verarbeitung von Informationen möglich machen. Als Schlüsseltechnologie beim Übergang in die Informations- und Wissensgesellschaft kommt der Telematik eine unschätzbar hohe und zentrale Bedeutung nicht nur in der Arbeitswelt, sondern auch in fast allen anderen Bereichen des persönlichen und gesellschaftlichen Lebens zu.

Im Spannungsfeld der sich rasant entwickelnden Informations- und Kommunikationstechnologien entwickelt die Telematik eine ganz eigenständige Perspektive und übernimmt eine Vorreiterrolle auf einem Gebiet, das adäquat nicht mehr von den ursprünglichen Wissenschaften und Techniken der Telekommunikation und Informatik separat bearbeitet werden kann. Gab es früher einerseits isolierte Rechner ohne Netzverbindungen und andererseits Netze, an die zwar verschiedene Telekommunikationseinrichtungen, jedoch noch kaum Computer angeschlossen waren, so entstehen seit einigen Jahren sich ständig verdichtende Netze, in denen sich Computer als primäre Kommunikationseinrichtungen durchsetzen; sowohl auf der Makroebene – national, international und global – als auch auf der Mikroebene - im Unternehmen, in der Behörde oder im Krankenhaus. Dies bedeutet in der Konsequenz, dass die Informatik in immer mehr Fällen das Wissen und die Methoden der Telekommunikation berücksichtigen muss, und genauso ist die Telekommunikation immer häufiger dazu gezwungen, Informatikkenntnisse umzusetzen. Wo zwei Wissenschaften derartige Abhängigkeiten entwikkeln, kann sich die neue und eigenständige Disziplin der Telematik gut entfalten.

Zusammenfassend lässt sich sagen, dass sich Telematik mit dem Einsatz informatorischer Komponenten, Verfahren und Systeme befasst, die eine starke Telekommunikationskomponente aufweisen. Neben den Grundprinzipien der digitalen Übertragungs- und Vermittlungstechnik werden in der Telematik moderne verteilte Anwendungen behandelt. Auf vernetzten Rechnern ablaufende Anwendungsprogramme ermöglichen eine rechnerübergreifende Funktionsintegration und beziehen zunehmend auch Kommunikationsmechanismen für multimediale Informationen mit ein.

Stichpunktartig seien nur einige der Forschungsthemen der Telematik aufgelistet:

- Netze, Dienste und Protokolle
- Mobilkommunikation
- Internet und WWW
- Architekturen für moderne verteilte Systeme
- Verteilte Anwendungen
- Sicherheit in Netzen
- Smartcards

Die Telematik als gleichermaßen stark technologie- und anwendungsgetriebene Wissenschaftsdisziplin eröffnet damit ein zukunftsträchtiges und umfassendes Leistungsspektrum, dessen hohe wirtschaftliche und gesellschaftliche Bedeutung in den unterschiedlichen Anwendungsbereichen in Wirtschaft, Medizin, Verwaltung und Wissenschaft sich bereits heute abzuzeichnen beginnt. Der Großteil des Potentials der jungen Disziplin der Telematik liegt jedoch in der Zukunft und wird dort zu in ihrem vollen Ausmaß noch nicht vorstellbaren Veränderungen unserer Lebens- und Arbeitsumwelt führen.

## Entstehung

Das Institut für Telematik hat unter Leitung von Univ.-Prof. Dr. sc. Christoph Meinel am 1. Januar 1998 seine Arbeit aufgenommen. Institutionelle Voraussetzungen waren schon früher geschaffen worden. Auf Grund der sehr erfolgreichen Entwicklung der 1996 gegründeten und von Prof. Meinel geleiteten Trierer Außenstelle des heutigen Fraunhofer-Instituts für Wirtschafts- und Technomathematik wurde am 1. November 1997 der Trägerverein „Institut für Telematik e.V." gegründet. Ziel dieses Vereins ist die „Förderung der anwendungsnahen Grundlagenforschung und der angewandten Forschung ... auf allen Gebieten, die für die Telematik bedeutsam sind" sowie die Unterhaltung eines eigenen Forschungsinstituts. Zum Vorsitzenden des Vereins wurde Univ.-Prof. Dr. sc. nat. Christoph Meinel,

Lehrstuhlinhaber im Fach Informatik an der Universität Trier, gewählt und mit dem Aufbau eines eigenständigen Instituts für Telematik beauftragt. Die Fraunhofer Management-Gesellschaft in München wurde mit der Geschäftsbesorgung betraut, ein Auftrag, der heute von der Fraunhofer-Gesellschaft selbst ausgeführt wird. Das Institut für Telematik verfügt so über gute Verbindungen zu den Instituten der Fraunhofer-Gesellschaft.

**Entwicklungsgeschichte auf einen Blick**

01.11.1997 Gründung des Trägervereins
01.01.1998 Gründung des Instituts
27.04.2000 Erste Promotion
04.09.2000 Erstes Patent erteilt
22.11.2000 Zweites Patent erteilt
10.04.2001 Zweite Promotion
10.05.2001 Mitgliedschaft in der Initiative D21
04.12.2001 Kuratorium beschließt Ausbau
10.01.2002 Dritte Promotion
18.01.2002 Erfinderpreis Rheinland-Pfalz
26.02.2002 Vierte Promotion
31.07.2002 Drittes Patent beantragt
25.10.2002 Antrag auf .eu-Domainverwaltung
08.01.2003 Verein beschließt Selbstauflösung

## Entwicklung des Instituts

Auf der Basis des Ende 2001 vom Kuratorium vorgeschlagenen und von der Mitgliederversammlung beschlossenen Ausbauplans hat das Institut neue Räumlichkeiten gemietet und nach notwendigen Bau- und Renovierungsmaßnahmen Anfang 2002 übernommen. Systemadministration und Sekretariat wurden personell gestärkt, Öffentlichkeitsarbeit und Marketing in professionelle Hände gegeben. All diese durch den Ausbauplan veranlassten Maßnahmen hatten ihren Preis.

Auf der Einnahmeseite erfüllten sich nicht alle Projekterwartungen, da sich vom zweiten Halbjahr 2001 an die Wirtschaftslage in Deutschland deutlich verschlechterte. Insbesondere unser jahrelang sehr erfolgreiches PKI-Projekt mit der Dresdner Bank wurde nach dem Zusammengehen mit der Allianz AG nicht fortgesetzt. Auch die bei der rheinland-pfälzischen Stiftung Innovation beantragte Förderung eines hochinnovativen Studienbuch-Projekts für den Virtuellen Campus wurde nicht gewährt. Folge: Es traten rote Zahlen auf. In der Summe betrug das Defizit zum Jahresende fast 400.000 Euro. Da das Institut als gemeinnützig tätiger Verein keine Rückstellungen bilden konnte und keine Bank-Sicherheiten vorhanden waren, mussten die laufenden Fehlbeträge über den auf 250.000 Euro begrenzten Kontokorrentkredit gedeckt werden - eine Situation, die das Institut 2002 immer wieder an den Rand der Zahlungsfähigkeit brachte. Bemühungen der Institutsleitung, Unterstützung großer Industrieunternehmen oder aus dem politischen Bereich zu erhalten, blieben leider erfolglos.

Auch eine vom Landes-Wissenschaftsministerium finanzierte Übernahme von Mitarbeitern des Instituts an die Universität Trier brachte infolge der bescheidenen Auftragslage keine wesentliche Entlastung. Kurz wurde eine vollständige Integration in die Universität diskutiert, aber aufgrund der finanziellen Risiken für undurchführbar angesehen. Es wurde dann von Seiten des Wissenschaftsministerium und der Universität eine vollständige Liquidation des Instituts ins Gespräch gebracht. Aufgrund der Tatsache, dass Rheinland-Pfalz dem Institut die weitere Unterstützung entzog, musste der Trägerverein dann seine Liquidation zum 15.01.2003 beschließen.

## Technische Ausstattung

Die am Institut für Telematik bearbeiteten Projekte sind auf ein hohes Niveau der technischen Ausstattung und Infrastruktur angewiesen. Intern sind die verschiedenen Institutsbereiche über einen ATM-Backbone mit z. Zt. 24 Glasfasern verbunden, die im Institutsrechenzentrum über einen ATM-Switch mit den zentralen Servern und einer leistungsfähigen, unterbrechungsfreien Stromversorgung zusammenlaufen.

Sämtliche Arbeitsplätze der Wissenschaftler, des technischen Personals, der Sachbearbeiter und der wissenschaftlichen Hilfskräfte sind mit hochleistungsfähigen PCs bzw. mit Workstations ausgestattet. Darüber hinaus wurde ein Wireless LAN installiert, welches die kabellose Einwahl ins Intranet gestattet.

Am Institut für Telematik sind Standleitungen in verschiedene Netze (z.B. Global-Access) vorhanden, die eine breite Palette von Auswahlmöglichkeiten bieten. Dabei ist für eine ausreichende Bandbreite sowie durch direkte Anbindung in den De-CIX nach Frankfurt für kurze Paketlaufzeiten und eine schnelle Verbindung mit den Netzen anderer Provider und in die USA gesorgt.

Die Qualität der Infrastruktur wird durch ein umfassendes Firewall-Konzept, die Bereitstellung verschiedener Server (etwa WWW, E-Mail, FTP, News), Internet-Zugang über Einwahlbatterien, Netzwerk-Monitoring und Netzadministration weiter gesteigert.

Die Ausstattung steht nicht nur dem Institut selbst zur Verfügung. Auch Projektpartnern und strate-

gischen Partnern wird die Nutzung der Netzinfrastruktur und der Ressourcen angeboten. Als zusätzlicher Service wird die Protokollierung der Akzeptanz bzw. Frequentierung der Internet-Präsenz und das Führen entsprechender Statistiken angeboten.

**Strategische Partner**

Die strategischen Partner des Instituts für Telematik kommen aus verschiedenen Bereichen der Wirtschaft und Gesellschaft. Unter anderem sind High-Tech-Unternehmen, wissenschaftliche Einrichtungen und politische Institutionen vertreten, so dass auf unterschiedliche Kompetenzen zurückgegriffen werden kann.

Wichtig ist uns aber vor allem, dass die am Institut vorhandene Expertise den Partnern in vollem Umfang zur Verfügung gestellt wird und so enge und für beide Seiten fruchtbare Beziehungen und Verflechtungen entstehen.

Zu folgenden Unternehmen und Institutionen bestehen Kooperationsbeziehungen:

- Ministerium für Wissenschaft, Weiterbildung, Forschung und Kultur, Mainz
- Universität Trier, insbesondere zur Abteilung Informatik und zum Zentrum für Wissenschaftliches Elektronisches Publizieren (WEP)
- IT-Services s.à.r.L., Luxemburg
- ITM Services AG, Essen
- Dresdner Bank AG, Frankfurt
- Allianz AG, München
- DREGIS – Dresdner Global IT-Services GmbH, Frankfurt
- Polytechnische Universität, Beijing
- Handwerkskammer Trier
- ABBL - Association des banques et banquiers, Luxemburg
- Dagstuhl, Internationales Begegnungs- und Forschungszentrum für Informatik
- Fraunhofer-Gesellschaft, München
- IAL, Luxemburg
- Deutsche Gesellschaft für Gesundheitstelematik e.V., Frankfurt
- Institut Supérieur de Technologie, Luxemburg
- Krankenhaus der Barmherzigen Brüder, Trier
- Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau, Mainz
- Polytechnische Hochschule Turin
- Stadt Trier
- University of Colorado at Boulder, USA
- Teletrust Deutschland e.V., Erfurt

Zu den strategischen Partnern sind auch die persönlichen Mitglieder des Kuratoriums und des Vereins zu zählen, denen ein eigener Abschnitt eingeräumt wird (🕮 Handelnde Personen).

**Projektpartner und Kunden**

Projektpartner des Instituts für Telematik sind nicht nur High-Tech-Unternehmen im Bereich der Forschung, sondern auch kleinere und mittlere Unternehmen, die wissenschaftliche Ergebnisse aus Computertechnik und Optimierung in der Praxis einsetzen. Auch manche unserer strategischen Partner sind Projektpartner. Das Institut für Telematik legt Wert darauf, sich auf unterschiedliche Partner einstellen und verschiedene Erwartungen erfüllen zu können.

Folgende Institutionen und Unternehmen gehören zu unseren Projektpartnern:

- Association des banques et banquiers, Luxemburg
- AGIS Allianz Gesellschaft für Informatik Service mbH, München
- Allianz AG, München
- Aufsichts- und Dienstleistungsdirektion Rheinland-Pfalz, Trier
- Caritas Trägergesellschaft Trier
- CERF-net Germany, Frankfurt
- Dateninformationszentrum Rheinland-Pfalz, Mainz
- Deutsche Forschungsgemeinschaft (DFG)
- DREGIS – Dresdner Global IT-Services GmbH, Frankfurt
- Dresdner Bank AG, Frankfurt
- DZI BANK Luxemburg S.A.
- Euro Info Center, Trier
- Global Access GmbH, Frankfurt
- GWI Research, Trier
- Handwerkskammer Trier
- IAL, Luxemburg
- Institut für Mittelstandsforschung INMIT, Trier
- ITM Services AG, Essen
- IT-Services s.à.r.L., Luxemburg
- Krankenhaus der Barmherzigen Brüder, Trier
- Ministerium für Inneres und Sport, Rheinland-Pfalz, Mainz
- Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau, Mainz
- Mutterhaus der Borromäerinnen, Trier
- Nikolaus Koch Stiftung, Trier
- Nord-LB, Luxembourg
- Quorum Medical AG, Schweiz
- Stiftung Burgen, Schlösser, Altertum, Koblenz
- Sozialministerium Baden-Württemberg
- Stadt Trier
- Stiftung Innovation des Landes Rheinland-Pfalz
- Trierischer Volksfreund
- Universität Trier
- ZFE Siemens AG, München

# Handelnde Personen

elnde Personen

Univ.-Prof. Dr. sc. nat.
Christoph Meinel

Prof. Dr. rer. nat.
Thomas Engel

Die Leitung des Instituts für Telematik hat **Univ.-Prof. Dr. sc. nat. Christoph Meinel** inne.

Christoph Meinel studierte von 1974 bis 1979 Mathematik und Informatik an der Humboldt-Universität zu Berlin. Nach einem Promotionsstudium an der Humboldt-Universität wurde ihm 1981 der Titel des Dr. rer. nat. verliehen. Von 1981 bis 1990 war er als wissenschaftlicher Assistent an der Sektion Mathematik der Humboldt-Universität zu Berlin und am Institut für Mathematik der Akademie der Wissenschaften in Berlin tätig. 1988 habilitierte er sich dort mit einer Arbeit aus dem Bereich der Komplexitätstheorie. Nach einem Forschungsaufenthalt an der Universität des Saarlands und einer Lehrstuhlvertretung an der Universität Paderborn wurde er 1992 zum ordentlichen Professor (C4) für „Theoretische Konzepte und neue Anwendungen der Informatik“ an die Universität Trier berufen. Christoph Meinel ist Autor, Mitautor und Herausgeber von 7 Büchern und mehr als 200 wissenschaftlichen Veröffentlichungen in renommierten wissenschaftlichen Zeitschriften und bei internationalen Kongressen. Sein Hauptinteresse gilt den Forschungsgebieten Telematik, VLSI-Design, Komplexitätstheorie. Prof. Meinel ist Direktor des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP) an der Universität Trier und Mitglied verschiedener Aufsichtsräte und internationaler Konferenzprogramm-Kommittees. So gehört er z.B. dem Aufsichtsrat des Internationalen Begegnungs- und Forschungszentrums für Informatik auf Schloss Dagstuhl an und ist Sprecher der Fachgruppe Komplexität der deutschen Gesellschaft für Informatik (GI). Prof. Meinel ist auch als Veranstalter verschiedener wissenschaftlicher Symposien und internationaler Tagungen in Erscheinung getreten. Unter seiner Leitung wurde z.B. 1999 die weltweit bedeutende STACS-Konferenz in Trier ausgerichtet. Er ist Veranstalter der Trierer Symposien des Instituts für Telematik und Herausgeber des elektronischen Kolloquiums ECCC. Prof. Meinel war Mitglied des Technologiebeirats des Landes Rheinland-Pfalz und ist Gründungsvorstand der Initiative der Software- und Serviceanbieter (ISS) Rheinland-Pfalz. Er vertritt das Institut für Telematik im TeleTrust Deutschland e.V. und in der Deutschen Gesellschaft für Gesundheitstelematik e.V.

Stellvertretender Direktor des Instituts für Telematik ist **Prof. Dr. rer. nat. Thomas Engel**.

Von 1987 bis 1992 studierte Thomas Engel Physik und Informatik an der Universität des Saarlandes in Saarbrücken mit dem Abschluß Diplom-Physiker. Seine Dissertation am Institut für Experimentalphysik an der Universität des Saarlandes beschäftigte sich mit Elektronenstreuvorgängen in Theorie, Simulation und Experiment. Daneben studierte er von 1992 bis 1996 Wirtschaftswissenschaften an der Fernuniversität Hagen.

Nach seiner Promotion zum Dr. rer. nat. Ende 1995 gehörte er im Januar 1996 zu den ersten Mitarbeitern des zeitgleich neu gegründeten Trierer Bereichs des Instituts für Techno- und Wirtschaftsmathematik (ITWM-Trier), des Rechtsvorgängers des Instituts für Telematik, als wissenschaftlicher Mitarbeiter, später Projektleiter und Gruppenleiter. Von April 1997 bis zur Neugründung des Instituts für Telematik war er stellvertretender Bereichsleiter des ITWM-Trier, seit Anfang 1998 ist er stellvertretender Direktor des Instituts für Telematik.

Im Wintersemester 1997/98 übernahm er eine Lehrstuhlvertretung im Fachbereich Elektrotechnik an der Hochschule für Technik und Wirtschaft (HTW) des Saarlandes sowie bis heute diverse Lehraufträge an Hochschulen der Großregion. Dr. Thomas Engel ist Sprecher der Regionalgruppe Trier-Luxembourg der Gesellschaft für Informatik (GI). Im Februar 2002 wurde Dr. Thomas Engel zum Professor am Institut Supérieur de Technologie (IST) der Luxembourg University of Applied Sciences berufen.

## Führungskreis

**Dipl.–Inform.**
**Frank Losemann**

| | |
|---|---|
| 1990-1997 | Studium der Informatik an der Uni Koblenz |
| Abschluss: | Dipl.-Inform. |
| Seit 1997 | Wissenschaftlicher Mitarbeiter am Institut für Telematik |
| Projekte: | Verantwortlich tätig im Bereich Sicherheitstechnologien für Internet und Intranet im Bankenbereich |

**Dipl.–Inform.**
**Uwe Roth**

| | |
|---|---|
| 1988 | Studium der Informatik an der Uni Kaiserslautern |
| Abschluss: | Dipl.-Inform. |
| 1995 | Systemberater, Schwerpunkt: Administration von großen Lotus-Notes Domänen |
| seit 1998 | Wissenschaftlicher Mitarbeiter am Institut für Telematik |
| Projekte: | Verantwortlich tätig im Bereich: Systementwicklung „Middleware“ |

**Dr. rer. nat.**
**Andreas Heuer**

| | |
|---|---|
| Bis 1995 | Studium der Physik an der Uni Münster |
| Abschluss: | Dipl.-Physiker |
| 1995-1997 | wissenschaftlicher Mitarbeiter an der Uni Münster |
| Seit 1997 | wissenschaftlicher Mitarbeiter am Institut für Telematik |
| Projekte: | Verantwortlich tätig im Bereich Web-Content-Management und elektronisches Publizieren |
| 2002 | Promotion zum Dr. rer. nat. |

## Mitarbeiter

Bis zum 31. März 2002 beschäftigte das Institut 32 Mitarbeiter und 26 wissenschaftliche Hilfskräfte. Dann wurden 13 Mitarbeiter von der Universität Trier übernommen.
Die Mitarbeiter kommen meist als junge Hochschulabsolventen zum Institut. Einige haben aber auch bereits Erfahrungen in der Industrie gesammelt und bringen ihre spezifischen praktischen Kenntnisse in die Projekte ein. Vertreten sind diplomierte bzw. promovierte Forscher aus den Fachgebieten Informatik, Mathematik, Physik, Ingenieur- und Wirtschaftswissenschaften, Informationswissenschaft sowie Jura.

Den noch nicht promovierten wissenschaftlichen Mitarbeitern wird im Rahmen der Projektarbeit des Instituts die Möglichkeit zur Promotion eingeräumt. Dies gilt übrigens auch für Fachhochschulabsolventen. Neben den fest angestellten Mitarbeitern gibt es auch Promotionsstipendiaten und Post-doc-Stipendiaten.

Die innovative und flache interne Organisationsstruktur im Institut gibt fachlich potenten Mitarbeitern Gelegenheit, Forschungs- und Entwicklungsprojekte für Wirtschaft und Gesellschaft schon sehr frühzeitig mit einem hohen Maß an Eigenverantwortung durchzuführen.

**Wissenschaftliche Mitarbeiter und Stipendiaten**

Absolu, Florence, M.A.
Dr. Akatova, Elena
Dipl.-Math. oec. Becker, Torsten
Dr. rer. nat. Birkel, Ulf
Chen, Tongbo, MSc
Cheng, Feng, MSc
Dewald, Stefan
Dr. rer. nat. Dusemund, Bernd
Dipl.-Ing. Ferring, Paul
Gevantmakher, Michail
Dr. iur. Gollan, Lutz
Dr. rer. nat. Heuer, Andreas
Hu, Ji, MSc
Jiang, Chunyan, MSc
Dipl.-Inform. Losemann, Frank
Ma, Mingchao, MSc
Dipl.-Inform. (FH) Müller, Ralf
Neuses, Dirk
Dipl.-Inform. Roth, Uwe
Dipl.-Geogr. Rudolf, Frank
Dr. rer. nat. Sack, Harald
Dipl.-Inform. Schmitt, Michael
Dipl.-Inform. Vorwerk, Lutz
Wanjun, Huang, MSc
Wei, Zhou, MSc

*Abb. 1: Mitarbeiter des Instituts für Telematik*

**Systemadministration**

Lentes, Bernd
Vieten, Michael

**Sekretariat/Verwaltung**

Dipl. Ing. (FH) Huberty, Barbara
Staatlich geprüfte Betriebswirtin Kern, Beate

**Wissenschaftliche Hilfskräfte**

Becker, Uwe
Berg, Karl
Boelter, Benjamin
Filkov, Hristo
Fisch, Karin
Fischer, Daniel
Himbert, Isabelle
Janetzki, Viktoria
Lange, Christoph
Meinel, Tobias
Minev, Mihail
Mitev, Martin
Muellenheim, Gerhard
Noll, Michael
Peters, Stefan
Scherer, Thomas
Schlegel, Rüdiger
Schmelzer, Christian
Schneider, Sebastian
Scholtes, Ingo
Schön, Michael
Trocha, Thomas
Wagner, Thomas
Willems, Christian
Woll, Romy
Zimmermann, Holger

**Praktikanten**

Andrei, Sabina
Demircan, Zyia
Hansen, Marc
Kirsch, Andrea
Schmit, Isabell
Ziegelmayer, Michael

## Mitglieder des Vereins

Rechtsträger des Instituts für Telematik ist der gemeinnützige, eingetragene Verein „Institut für Telematik e.V.". Die Mitglieder des Vereins zeichnen sich durch hohe fachliche und soziale Kompetenz aus und nehmen wichtige Positionen in Politik, Gesellschaft, Wirtschaft und Wissenschaft ein.

### Mitglieder

- Bitburger Brauerei Th. Simon
  *vertreten durch den Geschäftsführer Alfred Müller*
- Prof. Dr. rer. nat. Thomas Engel
  *Prof. am Institut Supérieur de Technologie (IST) der Luxembourg University of Applied Sciences*
- *Handwerkskammer Trier*
  *vertreten durch den Hauptgeschäftsführer Ass. Hans-Hermann Kocks*
- Industrie und Handelskammer Trier
  *vertreten durch den Hauptgeschäftsführer Arne Rössel*
- Ministerialdirigent Josef Mentges
  *Ministerium für Wissenschaft, Weiterbildung, Forschung und Kultur Rheinland-Pfalz, Mainz*
- Prof. Dr. sc. nat. Christoph Meinel
  *Professor für Informatik der Universität Trier*
- RWE Energie AG
  *vertreten durch den Leiter Netzregion Südwest Dipl.-Ing. Klaus Voußem*
- Sparkasse Trier
  *vertreten durch den Vorstandsvorsitzenden Dieter Mühlenhoff*
- Stadt Trier
  *vertreten durch den Oberbürgermeister Helmut Schröer*
- Universität Trier
  *vertreten durch den Universitätspräsident Univ.-Prof. Dr. Peter Schwenkmezger*

### Vorstand des Vereins

- Univ.-Prof. Dr. sc. nat. Christoph Meinel
  *Universität Trier, FB IV – Informatik (Vorstandsvorsitzender)*
- Prof. Dr. rer. nat. Thomas Engel
  *Luxembourg University of Applied Sciences (Stellvertretender Vorstandsvorsitzender)*

### Kuratorium

Zur Beratung und Festlegung der strategischen Ausrichtung der Forschungsschwerpunkte sowie als Kontrollorgan wurde dem Institut für Telematik ein sehr hochrangig besetztes Kuratorium zur Seite gestellt. Es berät über die vom Vorstand des Instituts erarbeiteten jährlichen Wirtschafts- und Stellenpläne, mittel- und langfristige Finanzplanungen, Unterlagen über die Errichtung bzw. Auflösung von Einrichtungen des Vereins sowie allgemeine Grundsätze über die Annahme und Verwendung von Mitteln, die dem Verein zur Förderung seiner Aufgaben zugewandt werden.

Das Kuratorium schlägt der Mitgliederversammlung die Erteilung oder Verweigerung der Entlastung des Vorstandes und die Genehmigung oder Ablehnung des vom Vorstand vorgelegten Jahresabschlusses vor. Im Innenverhältnis kommt der Beratung im Bereich der strategischen Ausrichtung der bearbeiteten Projekte und der wissenschaftlichen Ausrichtung des Instituts eine besondere Bedeutung zu.

Dem Kuratorium des Instituts für Telematik gehören hochrangige und kompetente Vertreter aus Gesellschaft, Wissenschaft und Wirtschaft an.

### Kuratoriumsvorsitzender

- Ministerialdirigent Josef Mentges
  *Ministerium für Wissenschaft, Weiterbildung, Forschung und Kultur, Rheinland-Pfalz, Mainz*

### Stellvertretender Kuratoriumsvorsitzender

- Dr. Gunther Frank
  *Geschäftsführer DREGIS - Dresdner Global IT-Services GmbH, Frankfurt/Main*

### Weitere Mitglieder des Kuratoriums

- Univ.-Prof. Dr. Dieter Maaß
  *Univ.-Präsident i.R., Vorstandsvorsitzender a.D. des DFN-Vereins, Kaiserslautern*
- Alfred Müller
  *Geschäftsführer der Bitburger Brauerei Th. Simon GmbH, Bitburg*
- Dr. Thomas Rochel
  *Vorsitzender der Geschäftsführung, Saarbrücker Zeitung, Saarbrücken*
- Paul Schuh
  *Conseiller de direction 1ère classe des Ministère des Communications, Luxembourg*
- Univ.-Prof. Dr. Peter Schwenkmezger
  *Präsident der Universität Trier*
- Dr. Hermann Josef Spital
  *Altbischof von Trier*
- Lucien Thiel
  *Direktor der ABBL - Association des banques et banquiers, Luxembourg*
- Dr. Friedrich Wöbking
  *Vorstandsmitglied der Allianz Versicherungs-AG und der Allianz Lebensversicherungs-AG, München*

# Personell verbundene Einrichtungen

Einrichtungen

Mit zwei Einrichtungen an der Universität Trier besteht eine besonders enge personelle Verbundenheit. Bei diesen Einrichtungen handelt es sich um den *„Lehrstuhl für Theoretische Konzepte und neue Anwendungen der Informatik"* und um das *„Zentrum für Wissenschaftliches Elektronisches Publizieren - WEP"* an der Uni Trier.

## Lehrstuhl für Theoretische Konzepte und neue Anwendungen der Informatik

Die Forschungsarbeiten am Lehrstuhl für Theoretische Konzepte und neue Anwendungen der Informatik liegen hier schwerpunktmäßig in den drei folgenden Bereichen:

1. Komplexität von Berechnungen
2. BDD-basierte Datenstrukturen für logische Funktionen
3. Elektronisches Publizieren

### 1. Komplexität von Berechnungen

In diesem Kernbereich der theoretischen Informatik geht es um die Charakterisierung des Ressourcenbedarfs für konkrete Berechnungen. Schwerpunkt der Forschung ist die Frage nach besseren oberen und unteren Schranken.

### 2. BDD-basierte Datenstrukturen für logische Funktionen

Zum computergestützten Entwurf von hochintegrierten Schaltkreisen und Kommunikationsprotokollen sind effektive Datenstrukturen erforderlich. Eine in diesem Zusammenhang sehr effektive Datenstruktur sind die BDDs (binary decision diagrams). Mit ihrer Hilfe können Chips und Kommunikationsprotokolle entworfen und - das ist besonders interessant - formal verifiziert und auf ihre Richtigkeit überprüft werden. Die Fachgruppe beschäftigt sich hauptsächlich mit der Kompaktifizierung und Optimierung solcher BDD-basierten Datenstrukturen für logische (0-1-wertige) Funktionen und mit der Verifikation sequenzieller Systeme.

### 3. Elektronisches Publizieren

Das zentrale Anliegen besteht in der praktischen Nutzbarmachung der neuen Kommunikationsmedien für Forschung und Lehre.
Konkrete Projekte sind:

- ECCC-Electronic Colloquium on Computational Complexity
- Weiterentwicklung und Betrieb eines WWW-basierten „Konferenz-Servers"
- Entwicklung der Suchmaschine „MOPS" für das WWW
- Entwicklung eines Forschungsportals für die OBDD-Forschung
- Entwicklung eines innovativen Kurs- Management Systems

## Zentrum für Wissenschaftliches Elektronisches Publizieren - WEP

Als Koordinationszentrum und fachübergreifende Einrichtung auf dem Gebiet des Wissenschaftlichen Elektronischen Publizierens an der Universität Trier hat sich das WEP in kurzer Zeit profiliert und etabliert. Im Vordergrund stehen dabei Optimierung bestehender, Erprobung und Evaluation neuer wissenschaftlicher Kommunikationsmöglichkeiten in Rechnernetzen (Internet/Intranet). Darüber hinaus stellt die Beratung und Zusammenarbeit mit Wirtschaft und Gesellschaft, d.h. der stete Dialog mit außeruniversitären Einrichtungen und Kooperationspartner, ein unverzichtbares Engagement des Kommunikationszentrums dar.

### Die Aufgaben des WEP:

- Initiierung, Verwaltung und Betrieb von online-Journalen
- Zugang zu fachspezifischen online-Recherche-Systemen
- Verwaltung von Bibliografiedaten-Beständen
- Unterstützung bei der Konzeption von Internet-Präsenzen
- Hypertext- und Multimedia-Anwendungen

### Leitung des WEP

Direktor: Univ.-Prof. Dr. sc. nat. Christoph Meinel

Geschäftsführer: Dr. rer. nat. Harald Sack

Weitere Informationen finden Sie unter URL:
www.informatik.uni-trier/~meinel/
www.informatik.uni-trier/TI/

# Kompetenzbereiche

Die Telematik ist ein sehr junges und sich rasant entwickelndes Forschungs- und Entwicklungsgebiet. Im Berichtsjahr 2002 war das Institut für Telematik in den nachfolgend beschriebenen Bereichen besonders aktiv. Darüber hinaus sollen zukünftig auch neue Bereiche erschlossen werden. Vertiefte Kompetenzen in ausgewählten Gebieten sind notwendig, um neue Aufgaben in angrenzenden Feldern bewältigen zu können.

1. Internet/Intranet
2. Elektronisches Publizieren
3. Telemedizin
4. Sicherheit in offenen Datennetzen
5. Systementwurf und -analyse

Eine Auswahl der bearbeiteten Projekte wird in einem gesonderten Abschnitt dargestellt (📖 Weitere wichtige Projekte).

## 1. Kompetenzbereich: Internet/Intranet

Die Einführung und schnelle weltweite Verbreitung von offenen Kommunikationsstandards hat seit Anfang der 90er Jahre zu einer unvorstellbar rasanten, weltweiten Verbreitung von Internet und WWW geführt. Scheinbar problemlos können die am Internet angeschlossenen Computer und Geräte miteinander kommunizieren, auf global verteilte Datenbestände zugreifen und diese bearbeiten und so komplexe Arbeits- und Geschäftsprozesse vollständig elektronisch abwickeln. Ziel der Hard- und Softwareentwickler ist es dabei, die hochkomplexen Vorgänge der Kommunikation hinter anwenderfreundlichen Programmen und intuitiv zu bedienenden Oberflächen zu verstekken und damit auch Nicht-Experten eine unmittelbare und sachgerechte Bedienung zu ermöglichen.

Kein Wunder also, dass die Projektpartner des Instituts diese Leistungspotenziale auch für das eigene Unternehmen oder die eigenen Behörde ausschöpfen wollen. Auf dem Boden sogenannter Intranets, also von unternehmensweiten Netzen, die auf der Internet-Technologie basieren, gewinnt ein Innovations- und Rationalisierungsprozess von enormem Ausmaß an Fahrt. Gefragt sind Ideen, Konzepte und Werkzeuge zum effizienten elektronischem Informationsmanagement bzw. zum elektronischen Dokumenten- und Workflow-Management.

Das Institut für Telematik stellt sich dieser Herausforderung und arbeitet an Lösungen, die die neuesten Erkenntnisse aus der aktuellen Forschung in anwendungsfähige Konzepte und Werkzeuge umsetzen durch:

- Konzeption von leistungsfähigen Internet- und Intranet-Präsenzen
- Bereitstellung von Werkzeugen zum Informations- und Dokumentenmanagement im Intranet
- Intranet-basiertes Workflow-Management
- Information-Broker
- Data-Warehousing
- Navigationssysteme für Datenbanken und Informationssysteme
- Sicherheitskonzepte im WWW
- Portfolio-Management-Systeme
- JAVA-Programmierung
- Netz-Infrastruktur-Entwicklung

## 2. Kompetenzbereich: Elektronisches Publizieren

Die Entwicklung der Internettechnologie hat revolutionäre Auswirkungen auch auf das Publikationswesen. Hier formen sich neue Funktionalitäten um den Begriff des Elektronischen Publizierens, also die Problematik der Bereitstellung, der Vernetzung bzw. der Archivierung multimedialer elektronischer Dokumente. Die sich etablierenden technischen Möglichkeiten rund um das Internet eröffnen ungeahnte Veränderungspotentiale und enorme Entwicklungsmöglichkeiten. Offene Standards, wie HTML, die über das Internet eine effektive Organisation von Verweisungsstrukturen und eine Einbeziehung multimedialer Daten (z.B. Ton- und Filmmaterial) leicht möglich machen, stellen insbesondere Verlage und Zeitungshäuser vor neue, ja existenzielle Herausforderungen. Eine im Institut für Telematik durchgeführte Umfrage zum Website-Management und -Authoring im Internet macht konzeptionelle Defizite deutlich. Die spezifischen Möglichkeiten des Internet durch seine mehrdimensionale Link-Strukturierung werden aufgrund fehlender Werkzeuge, wie leistungsfähiger Online-Redaktionssysteme, multilingualer Multiautorensysteme oder Hyperlink-Managementsysteme, bei weitem noch nicht ausgeschöpft.

Die Aktivitäten des Instituts im Bereich des elektronischen Publizierens sind vielfältig:

- Online-Redaktionssysteme für Internet und Intranet
- Multilinguale Multiautorensysteme

- Veranstaltungskalender
- Verteiltes Informationsmanagement
- Elektronische Tageszeitung
- Medienneutrale Informationshaltung
- Verbindung von Online- und Print-Produktionsketten
- Teleteaching

## 3. Kompetenzbereich: Telemedizin

Die Gesamtheit der Informationsübertragungen mit oder ohne Interaktionsmöglichkeiten, von Texten, Bildern, Audio- und/oder Videosystemen über Datennetze in der Gesundheitsfürsorge wird als Telemedizin bezeichnet. Die Vernetzung medizinischer Einrichtungen schafft dabei neue Möglichkeiten des gezielten Zugriffs auf Patientenakten und andere medizinische Daten durch berechtigte Nutzer. Fachkollegen an unterschiedlichen Orten können über elektronische Netze miteinander kommunizieren, Daten austauschen und mächtige, verteilte Datenbanken nutzen, um schnell an notwendige Informationen zu gelangen. Das Institut für Telematik ist in diesem Bereich in unterschiedlichen Projekten sehr aktiv:

- Mobile Datenerfassung in der Medizin
- DICOM-Bildmanagement und DICOM Zip
- DICOM-Präsentationssystem
- Adaptive Bildkompression
- System zur elektronischen Arztbriefschreibung
- Interaktive multimediale Patientenakte
- Intranet-basierte PACS-Systeme
- Patienten CD-System
- Patientenreminder
- Umfrage Telemedizin Rheinland-Pfalz

## 4. Kompetenzbereich: Sicherheit in offenen Datennetzen

Die Übertragung vertraulicher Daten über Online-Dienste schafft für die Anwender vielfältige Risiken. Da die Übertragungswege offen und Veränderungen oder Fälschungen nur schwer erkennbar sind, gilt es sicherzustellen, dass beim Datentransfer Unberechtigte fremdes Datenmaterial nicht einsehen oder gar manipulieren können.

Die jüngsten technischen Entwicklungen eröffnen zudem neue Möglichkeiten der wirtschaftlichen Betätigung und des Informationsaustausches. Warenbestellungen, Zahlungsanweisungen an Banken, Anträge bei Behörden, Übermittlung von sensiblen Daten im medizinischen Bereich und viele andere rechtlich relevante Vorgänge erfolgen bereits zu einem großen Teil auf elektronischem Wege. Hinzu kommen zukünftig verstärkt multimediale Anwendungen, die sich auf der Basis digitaler Daten etabliert haben und schnell weiter expandieren werden. Daraus resultiert der dringende Bedarf nach verfeinerten und anwendungsbezogenen Sicherheitskonzepten und -lösungen.

Das Institut für Telematik ist in folgenden Projektbereichen mit der Thematik befasst:

- Trust-Center - Zertifizierungstellen nach Signaturgesetz
- Sicherheitspolicies
- Sicherheitsaudits
- Lock-Keeper
- Firewalling (High-Security)
- Tiger Team
- Virtual Private Networks VPN
- Elektronische Modellierung von Datenzugriffshierarchien
- Zertifikat-Management
- Digitale Signaturen
- Electronic Commerce
- Mobile Commerce

## 5. Kompetenzbereich: Systementwurf und -analyse

Die in den letzten Jahren erreichten immensen Leistungssteigerungen im Bereich der Computerentwicklung sind nur durch ein eng verzahntes Zusammenspiel von Mensch und Computer beim Entwurf, der Analyse und Optimierung der immer komplexer werdenden Systeme möglich geworden. So ist der Entwurf von hoch- und höchstintegrierten mikroelektronischen Schaltkreisen mit Millionen von Transistoren ohne eine sehr weitgehende Einbeziehung von CAD-Werkzeugen (CAD - computer aided design) völlig undenkbar. Das gleiche gilt für den Entwurf und die Optimierung von zustandsendlichen Steuerungssystemen, also von sequenziellen Systemen mit eingebautem „Gedächtnis". Auch die im Zusammenhang mit der zunehmenden Vernetzung von verschiedenen Rechnersystemen (z.B. im Internet oder in ATM-Netzen) zu lösenden Fragen der Organisation und der Qualitätssicherung der Kommunikation werden immer komplexer und sind ohne Rechnerunterstützung und geeignete CAD-Werkzeuge nicht mehr zu bewältigen. Das Institut konzipiert in den folgenden Bereichen Lösungen und entwickelt in enger Zusammenarbeit mit den Universitäten in Trier, Kalifornien und Colorado Pilotsysteme, die neueste Erkenntnisse aus Wissenschaft und Forschung in praxisgerechte Werkzeuge umsetzen:

- EDA - Electronic Design Automation
- Logikentwurf und -minimierung
- Formale Schaltungsverifikation
- OBDD-Technolgie
- Protokollverifikation

# Tiger Team

Tiger Team

## IT-Sicherheitsanalysen durch ein Tiger-Team

*Die Zahl der öffentlich bekannten Sicherheitslücken in IT-Systemen steigt täglich und damit auch die Gefahr für ein Unternehmen, selbst Opfer eines Hacker-Angriffs zu werden. Das Institut für Telematik hat deshalb im Jahr 2002 ein eigenes „Tiger-Team" aufgestellt, das im Kundenauftrag nach Schwachstellen sucht. Als Zielgruppen wurden dabei neben Banken, die per se sehr hohe Sicherheitsanforderungen haben, auch kleine und mittlere Unternehmen aus der Region angesprochen, die oftmals nicht über das nötige Sicherheits-Know-how im eigenen Hause verfügen.*

## IT Security Analyses by a Tiger Team

*The number of publicly known vulnerabilities increases daily and, thus, the risk to become victim of a hacker attack rises as well. In 2002, the Institute for Telematics has reacted to this new situation and set up a „tiger team" that seeks for security holes in the infrastructure of a customer. Its new services were offered primarily to two customer groups: financial institutions which have very high security requirements per se, and regional small and medium-sized companies that often do not have the necessary in-house security knowledge.*

Moderne IT-Systeme sind komplexe Gebilde, die über eine Vielzahl von Funktionen und Konfigurationsmöglichkeiten verfügen. Diese Komplexität führt mittlerweile zu schwerwiegenden Sicherheitsproblemen - hervorgerufen sowohl durch Fehler in der Software als auch durch fehlerhafte Bedienung, Administration und Organisation. Das macht es Hackern leicht. Laut einer Studie des Computer Security Institute (CSI) und des FBI von April 2002 sind in den vorangegangenen 12 Monaten ca. 90 Prozent aller US-amerikanischen Firmen und Regierungsstellen Opfer eines Angriffs geworden. Im Falle eines erfolgreichen Einbruchs drohen einem Unternehmen nicht nur finanzielle Schäden durch den Ausfall der IT-Systeme und den Verlust wichtiger Firmendaten. Auch das Vertrauen der Kunden kann gefährdet sein - ein Grund, warum viele Einbrüche gar nicht erst in den Statistiken auftauchen.

Gefahren können von verschiedenen Seiten drohen: Professionelle Hacker führen gezielte Angriffe gegen einzelne Unternehmen durch, um sich oder anderen einen wirtschaftlichen Vorteil zu verschaffen. So genannte Script-Kiddies dagegen attackieren meist aus einem Spieltrieb heraus mit Hilfe frei verfügbarer Hacker-Tools wahllos Rechner im Internet. Aber es drohen auch Gefahren aus dem eigenen Netz: Eigene bzw. frühere Mitarbeiter können aus persönlichen oder finanziellen Interessen versuchen, Schäden anzurichten und nicht-autorisierte Daten auszuspähen. Eine weitere Risikogruppe stellen schließlich Viren, Würmer und trojanische Pferde dar, deren Ursprung oft nur schwer zu ermitteln ist.

Die häufigsten Probleme im Zusammenhang mit dem sicheren Betrieb von IT-Systemen sind in Abbildung 1 dargestellt. Insbesondere Fehler in zentralen Netzwerkdiensten, wie etwa WWW-Servern, haben in der Vergangenheit für Aufsehen gesorgt. Aber auch Applikationen auf Seiten der Endanwender, wie etwa E-Mail-Programme oder Webbrowser, können Sicherheitsprobleme aufweisen, wenn sie aktive Inhalte uneingeschränkt oder gar ohne Wissen des Benutzers ausführen. Aus diesem Grund sollte eine Sicherheitsinfrastruktur stets eine mehrstufige Filterung von Informationen sowohl auf der Ebene einzelner IP-Datenpakete als auch auf Anwendungsebene (z.B. Virenschutz) vorsehen.

Für eine umfassende Sicherheitsanalyse sind ebenfalls administrative und organisatorische Fragestellungen zu berücksichtigen. So ist sicherzustellen, dass ein Angreifer die Firewalls des Unternehmens nicht durch eine so genannte Backdoor umgehen oder unterlaufen kann. Weitere Punkte betreffen die Vergabe sicherer Passwörter, die Protokollierung aller relevanten Systemvorgänge und ihre Auswertung, sowie die Erstellung von Sicherheitskopien, um im Schadensfall das System wieder zügig in Betrieb nehmen zu können.

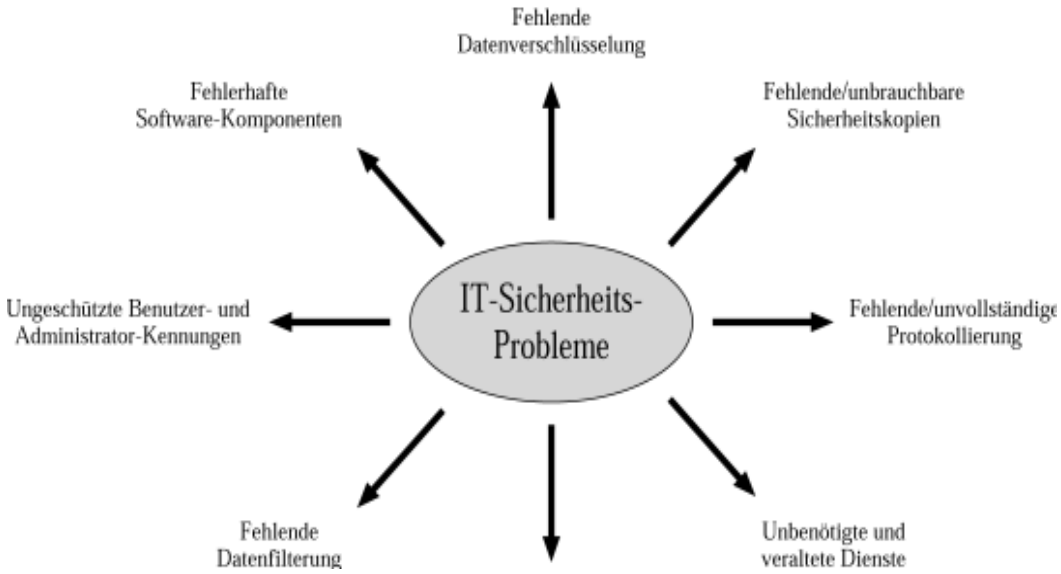



Abb. 1: IT-Sicherheitsprobleme

Als unabhängiges Forschungs- und Entwicklungsinstitut hat das Institut für Telematik ein „Tiger-Team" ins Leben gerufen, das kompetent und ohne Scheuklappen im Kundenauftrag IT-Systeme einer umfassenden Sicherheitsanalyse unterzieht.

Die Bandbreite der vom Institut angebotenen Dienstleistungen umfasst:

- Manuelle und automatisierte Penetrationstests
- Analyse des Netzwerk-Verkehrs
- Überprüfung und Bewertung von Firewall-Konfigurationen
- Analyse des Quellcodes von sicherheitskritischen Programmen
- Evaluation von IT-Sicherheitsleitlinien und Notfall-Plänen
- Integration und Konfiguration von Intrusion-Detection-Systemen

Für die Penetrationstests setzt das Institut dieselben Techniken und Tools ein, die auch Hacker für ihre Einbruchsversuche benutzen. Neben der Überprüfung von Schwachstellen in Standard-Applikationen hat sich das Tiger-Team auf die Überprüfung kundenspezifischer Applikationen spezialisiert, bei denen Standardtests keine verlässlichen Aussagen erlauben.

Insbesondere Web-Dienste, angefangen von einfachen Such-Funktionen bis hin zu komplexen Online-Shops, können bei fehlerhafter Implementation und Konfiguration zu ernsten Sicherheitsrisiken führen. So kann ein vermeintlich harmloses WWW-Formular, in das ein Internet-Nutzer Daten einträgt, zu Problemen führen, wenn die Plausibilität der Daten nicht serverseitig überprüft wird. Typische Fehler sind unterlassene Längenprüfungen, die intern zu einem Pufferüberlauf führen können. Als Folge ist ein Hacker in der Lage, sich unberechtigten Zugang zum System zu verschaffen oder den betroffenen Dienst zum Absturz zu bringen, so dass Anfragen weiterer Benutzer nicht mehr beantwortet werden können (engl.: Denial-of-Service).

Kompetenz auf dem Gebiet der IT-Sicherheit hat das Tiger-Team unter anderem im Rahmen eines groß angelegten Projekts mit einer namhaften deutschen Bank bewiesen. Aufgabe war es, deren - in Technologie und Umfang einzigartige - Application Service Providing-Lösung zu analysieren. Zum Kreis der weiteren Kunden zählt die Jedox GmbH (http://www.jedox.de), der das Institut nach erfolgreicher Testdurchführung eine Sicherheitsplakette (Abbildung 2) ausstellen konnte.


Abb. 2: Sicherheitsplakette des Instituts für Telematik

# Risiko Management

Risiko Management

## Fonds-Managementsystem macht Risiken besser kalkulierbar

*Die Bewertung und Beherrschung von Wertpapier-Risiken ist zur Zeit eine Schlüsselanforderung an zeitgemäßes Fonds-Management. Finanz-Dienstleiter stellen deshalb höchste Ansprüche an die unterstützenden Informations-Technologie und –Infrastruktur. Das Institut für Telematik entwickelte deshalb den „Fonds Manager", der als zukunftssicheres System intuitive Benutzung genauso gewährleistet wie Flexibilität in den Datenanbindungen.*

## Improved Risk Assessment by the Funds Management System

*Nowadays, the rating and controlling of risks of bonds is a key demand of modern funds management. Accordingly, providers of financial services are faced with high requirements when it comes to information technology and infrastructure. For that reason, the Institute for Telematics develops the „funds manager", which –as a future-proved system– allows for intuitive use and flexible data connection.*

Die Notwendigkeit eines risikobewussten Fonds-Managements hat vor allem die jüngere Vergangenheit gezeigt, als deutlich wurde, dass die weltweit zunehmende Zahl an Finanz-Transaktionen für Anleger nicht nur große Chancen bietet, sondern auch erhebliche Risiken mit sich bringt (Abbildung. 1): Zins-, Aktien- und Wechselkursschwankungen, aber auch Länder- und Kreditrisiken mit ihrer Ausfall-Problematik bringen die Gefahr hoher Verluste mit sich.

Bei der Entwicklung des „Fonds Managers" war das primäre Ziel, mögliche Wertpapierrisiken eines Fonds zu steuern und die wichtigsten Kenngrößen zu überwachen. In einer Simulationseinheit musste gleichzeitig eine Möglichkeit geschaffen werden, Risikogrößen durch „virtuelle" Transaktionen zu bestimmen um die optimale Zusammensetzung eines Fonds zu ermitteln. Dies soll es erleichtern, Wertpapiere nach ihren unterschiedlichen Wertsteigerungspotentialen und Risiken zu klassifizieren und sinnvolle Entscheidungsgrundlagen zu erarbeiten.

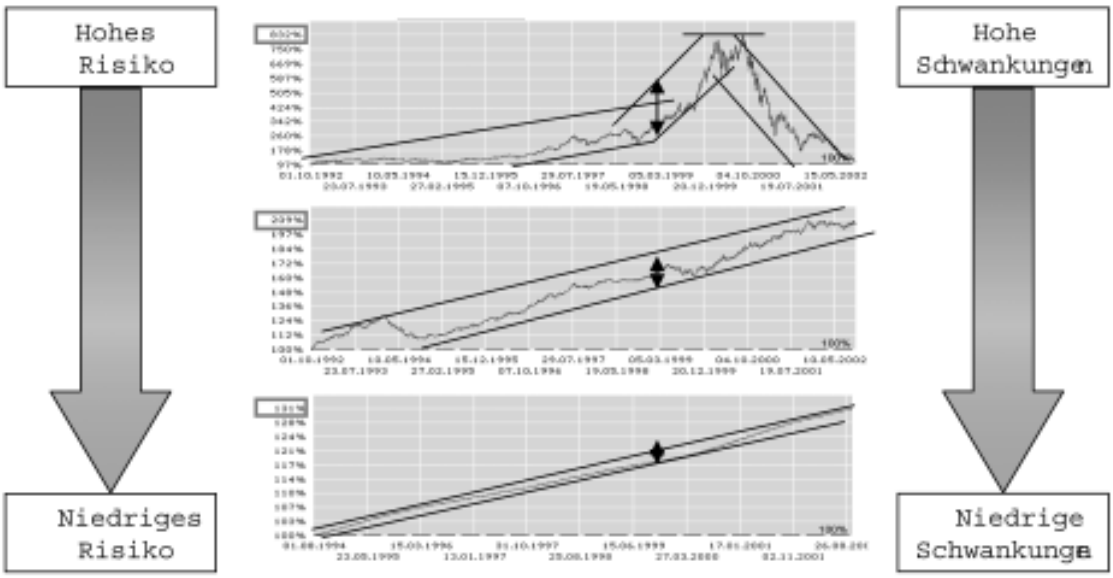



Abb. 1: Chancen stehen Risiken gegenüber

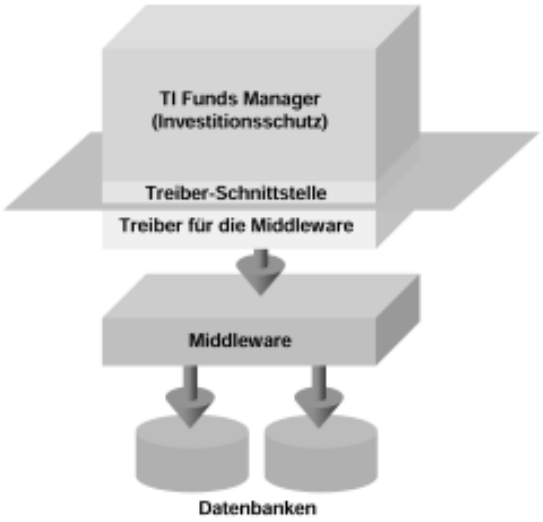



Abb. 2: Anbindung des „Fonds Managers“ an die Datenquellen über eine Middleware

Eine wichtige Anforderung an das Institut für Telematik war es, eine flexible Datenanbindung zu schaffen (Abbildung 2). In größeren Unternehmen findet sich eine große Anzahl von Datenquellen, deren Zusammensetzung (Hersteller, Art der vorgehaltenen Informationen) ständig im Fluss ist. Um die Anwendungsentwicklung frei von den Entwicklungen im Unternehmen gestalten zu können, hat sich der Einsatz von Middleware-Architekturen etabliert, die zwischen Informationsanbietern (in der Regel Datenbanken) und Informationskonsumenten vermittelnd tätig sind. Um auch in Zukunft die Möglichkeit zu besitzen, mit jeder Art von neuer Middleware zusammen zu arbeiten, wurde eine Abstraktionsebene (Interface) in die „Fonds Manager“-Anwendung eingeführt, für die eine konkrete Datenanbindung in der Art von Treiber-Programmen realisiert wurde. Nicht zuletzt dadurch besteht hoher Investitionsschutz für die Risiko-Management-Tool-Anwendung.

Fonds-

Management

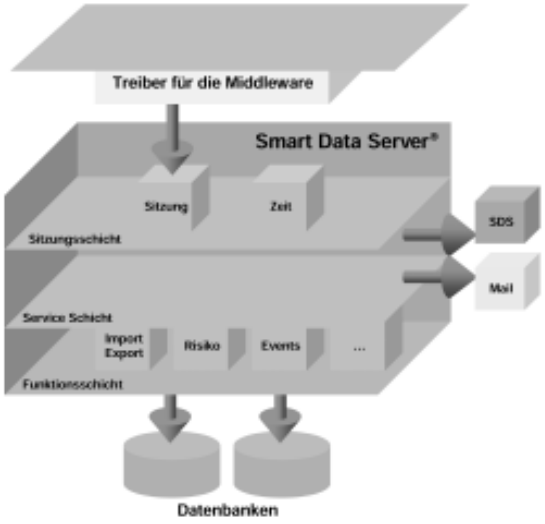



Abb. 3: Anbindung des „Fonds Managers“ an die institutseigene Middleware „Smart Data Server“ (SDS)

Neben der Anpassung an eine existierende Unternehmensinfrastruktur besteht die Möglichkeit der Anbindung an die institutseigene Middleware „Smart Data Server“ (SDS). Dabei handelt es sich um eine komponentenbasierte Plattform zur Entwicklung von frei definierbaren Funktionsmodulen, mit denen spezialisierte Lösungen für unternehmensweite Anwendungen geschaffen werden können. Der strikte Zugriff der Funktionsmodule auf die Unternehmensinfrastruktur über die Service-Schicht des Servers erleichtert deren Integration und Adaption (Abbildung 3).

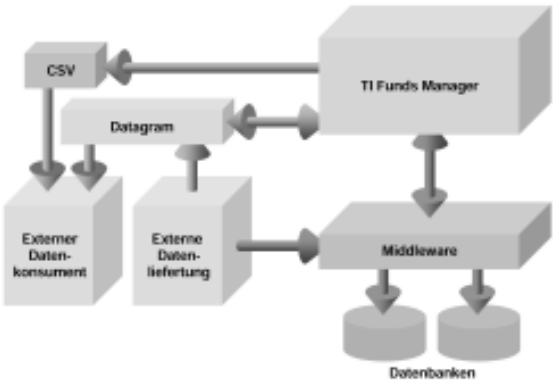



Abb. 4: Zusammenspiel externer Anwendungen mit dem „Fonds Manager“

Die Integration eines komplexen Systems in die existierende Unternehmensstruktur hat nicht nur Einfluss auf die Datenhaltung, sondern bedeutet auch Änderungen der Arbeitsabläufe. Weniger ein Ersetzen der bestehenden Anwendungen stand im Vordergrund, sondern vielmehr die Ergänzung des bestehenden Anwendungsportfolios um die neuen Features des „Fonds Managers“.

Damit ein optimaler Ablauf zwischen den Anwendungen möglich wurde, musste der „Fonds Manager“ um zwei Aspekte erweitert werden. Zunächst war ein Export-Mechanismus zu schaffen, der es Anwendungen ohne Zugriff auf die Datenbasis (über die Middleware) ermöglicht, an den Ergebnissen zu partizipieren, die der „Fonds Manager“ produziert. Hier wurde das allgemein verständliche CSV-Datei-Format, das äußerst einfach und flexibel aufgebaut ist, verwendet. Anwendern des Tabellen-Kalkulationsprogramms Excel dürfte es schon begegnet sein. Ferner wurde ein einfacher Mechanismus zum Auslösen des Exportvorgangs entwickelt. Hat eine Anwendung neue Daten über die Middleware in die Datenbasis eingespielt, so kann sie den „Fonds Manager“ über das Versenden sogenannter „Datagramme“ dazu bringen, Berechnungen den Export-Mechanismus weiterer Anwendungen zugänglich zu machen (Abbildung 4).

Datagramme sind verbindungslose Datenpakete (vergleichbar mit Postkarten) im Gegensatz zu einer verbindungsorientierten Datenkommunikation (vergleichbar mit Telefonaten). Das Beispiel Postkarte-Telefonat zeigt auch gleich einen weiteren Unterschied beider Kommunikationsformen: Datagramme sind eine Einweg-Kommonikation. Einmal versendet, hat der Auslöser des Datagramms keine Kontrolle mehr über die Zustellung des Datenpaketes. In unserem Falle ist dies auch nicht sinnvoll. Der Datenlieferant ist in keiner Weise daran interessiert, ob und wie der „Fonds Manager“ auf den Empfang der Nachricht reagiert. Hier ist das oberste Ziel, die auslösende Anwendung so wenig wie möglich in ihrer normalen Tätigkeit zu behindern. Ein Warten auf Reaktionen oder sogar deren Auswertung würde einen zu starken Einfluss auf die Anwendung haben, was nicht gewollt ist. Ein weiterer wichtiger Vorteil von Datagrammen ist die Betriebssystem-Unabhängigkeit, so dass die Datagrammauslösende Anwendung weder auf dem gleichen Rechner wie der „Fonds Manager“, noch auf einem Rechner mit gleichem Betriebssystem installiert sein muss.

Der „Fonds Manager“ wurde um Funktionalitäten ergänzt, die bisher nicht dem Risikomanagement zuzurechnen sind und daher in diesem System nicht vorgesehen waren. Dadurch können nun auf Basis des dispositiven Bestandes[1] Simulationen, Analysen und Modellierungen durchgeführt werden, bei denen auch Modellportfolios kreiert werden.
Konkret handelt es sich um folgende Erweiterungen:

- Simulation und Analyse unter Berücksichtigung des Exposures[2]
- Hedge-Ratios[3]
- Modellierung von Hedge-Strategien
- Portfolio-Reporting von Kennzahlen
  Indikativer Fondspreis[4]

[1] Das heißt, dass ausgeführte Kauf- bzw. Verkaufsorders in der Depotanzeige zur sofortigen Erhöhung bzw. Reduzierung des Bestandes führen, obwohl die Depotbuchung noch nicht stattgefunden hat.
[2] Das potentielle Risiko gegenüber dem Markt bzw. der Benchmark.
[3] Anzahl Kontrakte, die für die Absicherung einer Position notwendig sind
[4] Marktwert des dispositiven Bestandes geteilt durch die Anzahl der umlaufenden Anteile

# DICOM Management Suite

anagement-Suite

## DICOM Management Suite erleichtert Verwaltung medizinischer Bilder

*In Radiologie, Dermatologie, Pathologie, Pädiatrie und Chirurgie wird oft mit unterschiedlichen Quellen erstelltes Bildmaterial begutachtet bzw. bearbeitet, über offene Datennetze mit Fachkollegen ausgetauscht oder in Datenbanken gespeichert. Auch für die fachspezifische Aus- und Weiterbildung, das sogenannte TeleTeaching, oder für VideoKonferenzschaltungen (TeleConferencing) ist das Management von medizinischen Bildern wichtig. Hierfür hat das Institut für Telematik eine komfortable Software entwickelt und auf der Medica 2002 vorgestellt – die DICOM Management Suite.*

## DICOM Management Suite Eases Administration of Medical Images

*In radiology, dermatology, pathology, paediatry and surgery normally image material from different sources is used, transferred over open networks, exchanged with other physicians or stored in databases. Additionaly, for specific education, called TeleTeaching, or VideoConferencing (TeleConferencing) the management of medical images is important. Therefore, the Institute for Telematics has developed a comfortable software and presented this software on the Medica 2002 – the DICOM Management Suite.*

Die Digitalisierung medizinischer Bilder in Arztpraxen und Krankenhäusern schreitet immer mehr voran. Arzt und Patient haben beide ihren Nutzen davon. Telemedizinische Anwendungen, wie z. B. die Verwaltung und Archivierung von Patientendaten in elektronischen Patientenakten oder die Anbindung von Bildarchivsystemen einer Einrichtung an bestehende Radiologieinformationssysteme, werden heute bereits verwirklicht.

Eine entsprechende Software, die Ärzten das Management digitaler medizinischer Bilder im DICOM Format drastisch erleichtert, hat das Trierer Institut für Telematik entwickelt. Mit der „DICOM Management Suite" können in Krankenhäusern und Arztpraxen Röntgen-, Tomographie- oder Ultraschall-Aufnahmen auf beliebigen Datenträgern verwaltet werden.

Die DICOM Management Suite ist eine Sammlung verschiedener Applikationen zur Verwaltung und Archivierung von DICOM-Bildern. Sie kann individuell, je nach Anforderungsprofil, zusammen gestellt werden:

- DICOM View - DICOM-Viewer
- DICOM Disk - Archivierungssystem
- DICOM Mail - sicherer Versand von medizinischen Bilddaten
- DICOM Zip - patentierte und verlustfreie Kompression von DICOM-Bildern
- DICOM Beam - Präsentations- und Schulungssystem
- DICOM Repair - Tool zur Entfernung herstellerspezifischer Attribute
- DICOM Print - Druckausgabe auf DICOM-Druckern
- DICOM Edit - Editieren von DICOM-Dateien
- DICOM Base - Objekt orientierte Datenbank
- DICOM Scan - Digitalisierung medizinischer Bilddaten


Abb 1: Screenshot

**DICOM View**

DICOM View ist ein leistungsfähiger Betrachter für digitale medizinische Bilder. Es stellt alle nötigen Werkzeuge zur Verfügung, um ein DICOM-Bild oder eine Bildersequenz darzustellen.

**DICOM Disk (Patienten-CD System)**

Dieses System ermöglicht Medizinern die schnelle und benutzerfreundliche sowie kompakte Archivierung von Bilddaten. Bilder aus Röntgen-, CRT, MRT- und Ultraschall-Untersuchungen werden einfach und preiswert archiviert. Die bei einer Untersuchung auf einen CD-Rohling gespeicherten Bilder können an jedem herkömmlichen PC angeschaut werden. DICOM Disk bietet dem Arzt eine schnelle und komfortable, z. B. nach Patientennamen geordnete Übersicht über die vorhandenen Bilder bzw. Bildserien. Außerdem stellt es dem Arzt die wichtigsten Bildparameter zu Verfügung.
Die DICOM Disk hilft dabei, Kranken unnötige Strahlenbelastung durch Mehrfach-Röntgen zu vermeiden. Bei Untersuchungen kann der Arzt medizinische Aufnahmen als digitale Daten auf eine CD-ROM schreiben. Der Patient bekommt diese ausgehändigt und kann sie zu jedem anderen Arzt mitnehmen. Eine leistungsfähige Betrachtungs-Software, die mit auf die Patienten-CD gespeichert wird, sorgt dafür, dass die Bilder an jedem herkömmlichem PC angeschaut werden können.

**DICOM Mail**

Mit DICOM Mail können originale und komprimierte medizinische Bilder sicher per E-Mail versendet werden. Die Eigenschaften von DICOM Mail sind z. B. die visuelle Auswahl zu versendender DICOM-Bilder, die Kommentierung der zu versendenden Bilder, der Versand von mehreren DICOM-Bildern als E-Mail-Anhang und die Verwendung von digitalen Signaturen und Verschlüsselung.

**DICOM Zip**

Bei DICOM Zip handelt es sich um ein patentiertes Verfahren der adaptiven Bildkompression zur verlustfreien Kompression medizinischer Bilder im DICOM 3-Standard. Die Kompressionsraten betragen 1:2 bis 1:14. Komprimiert werden können sowohl Einzelbilder als auch Bildserien. Ärzte haben mit DICOM Zip die Chance, komprimierte

medizinische Bilder schnell über Netzwerke zu übertragen, zum Beispiel zur Zweitbefundung.

**DICOM Beam**

DICOM Beam ist ein Präsentationssystem für die Besprechung von Untersuchungsergebnissen radiologischer Schwarzweiß-Einzelbildaufnahmen im DICOM-Format. Einsatzfelder sind die Vorbereitung und Durchführung von Präsentationen für Konsultations- oder Schulungszwecke. Vor der Präsentation werden die ausgewählten Bilder über das Netzwerk auf denjenigen Rechner übertragen, auf der die Session ablaufen soll.

**DICOM Repair**

Alle Produkte von Herstellern DICOM basierter Lösungen sollten konform zum DICOM-Standard sein. Leider treten Abweichungen auf, da der Standard selbst es erlaubt, private Attribute zu spezifizieren. Einige Attribute werden so in neueren Fassungen des DICOM-Standards zu veralteten Attributen. Private und ruhende Attribute müssen aber durch DICOM-Applikationen verarbeitet werden können. Aus diesem Grunde wurde DICOM Repair entwickelt. DICOM-Dateien werden durch Entfernen privater und ruhender Attribute durch jeden DICOM-Viewer les- und darstellbar. Dies gilt gleichermaßen für Multiframe-Bilder.

**DICOM Print**

DICOM Print ist ein Client-Druck-Server zur Übermittlung hochqualitativer Druckausgaben, z. B. für Filme oder Folien, an spezielle DICOM-Drukker.

**DICOM Edit**

DICOM Edit ist ein Werkzeug zum Editieren von DICOM-Dateien. Es dient zur Anonymisierung von DICOM-Dokumenten oder zur Erstellung von Test-Dateien.

**DICOM Base**

DICOM Base ist eine auf Client-Server-Architektur basierende objektorientierte Datenbank zur Archivierung und Management von DICOM Daten. Sie verfügt über offene Schnittstellen zu Client-Browsern und wurde entwickelt zur Anbindung von DICOM-Datenbanken an medizinische Informationssysteme. Die Ablage der Daten in DICOM Base erfolgt verschlüsselt.

**DICOM Scan**

DICOM Scan macht die Digitalisierung von medizinischen Aufnahmen mittels handelsüblichem Scanner via TWAIN-Schnittstelle möglich. Die effiziente und kostensparende Archivierung auf digitalen Medien wird auch dazu führen, dass vorhandene Archive analoger Datenträger auf digitale Medien übertragen werden. Die digitalisierten Bilder werden im DICOM 3-Format abgespeichert. Über eine Eingabemaske können das jeweilige Bild beschreibende Daten wie Name des Patienten, Patientennummer, Modalität etc. eingegeben werden.

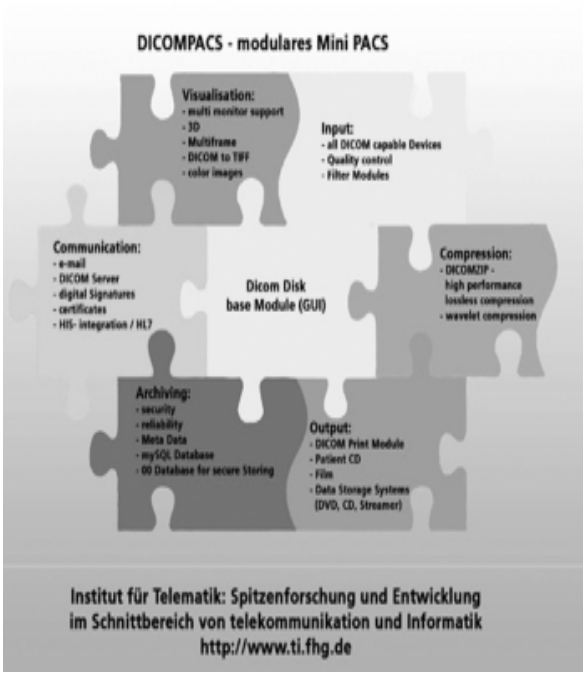



Abb. 2: DICOMPACS Module

# Weitere wichtige Projekte

In der Folge stellen wir eine Auswahl weiterer interessanter Projekte vor, an denen 2002 am Institut für Telematik gearbeitet wurde. Einige der Projekte sind bereits abgeschlossen, andere dauern noch an.

Bei der getroffenen Auswahl kommt es uns darauf an, einen breiten Einblick in die fachliche Arbeit des Instituts für Telematik zu geben, Kompetenzen an konkreten Beispielen aufzuzeigen und Ideen und Anreize weiterzugeben. Ein Blick auf unsere Website gibt zusätzliche Information über die hier nicht aufgeführten Projekte



## 1. Tele-TASK – neue Technologie für Online-Vortragsveranstaltungen

*Mit dem in Trier neu entwickelten E-Learning-System tele-TASK („Teleteaching Anywhere Solution Kit") steht eine drastisch vereinfachte Technologie für Online-Vorlesungen zur Verfügung. Jeder PC-Nutzer mit geeignetem Internetanschluss kann damit Online-Schulungen komfortabel abrufen. Auf einer Konferenz der weltweit größten Informatikergesellschaft „American Computing Machinery" (ACM) hat deren Fachgruppe „Computer Services an Universitäten und Colleges" im Jahr 2002 tele-TASK den Einstein Award für das „außergewöhnlichste und herausragendste" Projekt verliehen.*

## 1. Tele-TASK - Teleteaching Anywhere Solution Kit

*The newly developed e-learning system tele-TASK provides a new, drastically simplified technology for producing and attending online lectures has. Not only contents of teaching, which are presented to the students in the lecture-room by either a whiteboard or a video beamer are delivered but also video and audio of the lecturer. tele-TASK got the Einstein Award for the "most interesting, most provoking and best idea paper" on the international ACM SIGUCCS Conference 2002 in the USA.*

Mit tele-TASK wird nicht nur, wie üblich, ein Videobild des Dozenten übertragen, sondern simultan sein Bild, seine Stimme plus der Bildschirminhalt seines Präsentationsrechners. Durch den Einsatz einer elektronischen Tafel können dabei sogar die handschriftlichen Kommentare des Dozenten mit übertragen werden. Ein plattformunabhängiger Abruf der Veranstaltungen wird durch die weit verbreitete und kostenlose Betrachtungssoftware RealPlayer ermöglicht.

Navigation innerhalb der aufgezeichneten Kurse ist mittels elektronischem Inhaltsverzeichnis möglich. Zusätzlich werden Veranstaltungen für einen späteren Abruf (on demand) aufgezeichnet und archiviert. tele-TASK unterstützt alle gängigen Plattformen, verschiedene Netzbandbreiten und beliebige Präsentationsprogramme. Spezielle Installationen, Konfigurationen oder auch Vorkenntnisse seitens der Endanwender sind nicht erforderlich.

Das System wurde erstmals im Sommersemester 2002 für die Übertragung der Vorlesung „Informationssicherheit im Internet“ von Professor Christoph Meinel an der Universität Trier eingesetzt. Über 30.000 Zugriffe zeigen, wie unproblematisch und einfach die tele-TASK Technologie zu nutzen ist.

Um den Umgang mit der Teleteaching-Technik noch mehr zu erleichtern, wurde in Trier ein spezielles digitales Aufnahmegerät entwickelt – der tCube (vgl. Abbildung 1).

Player können somit genutzt werden. Nach einer erfolgreichen Aufnahme wird vom tCube innerhalb von Minuten automatisch eine CD oder DVD erstellt.

Ziel der tCube-Entwicklung war es, eine einfach nutzbare und universell einsetzbare Teleteaching-Lösung bereitzustellen. Der tCube passt von seinen Ausmaßen in einen gewöhnlichen Handkoffer und ist dadurch überall und sofort einsetzbar.

Weitere Informationen und ein grosses Angebot aufgezeichneter Vorlesungen zum Thema Internetsicherheit kann abgerufen werden unter:
http://www.tele-task.de

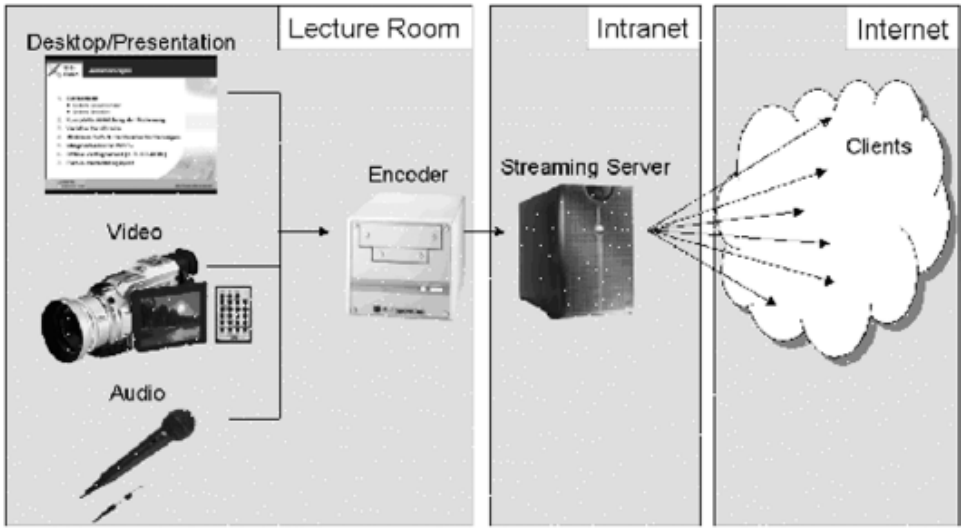



Abb. 1: Kombination und Weiterverarbeitung von verschiedenen Eingängen mit Hilfe von tCube

Der tCube besitzt keinen Monitor und braucht zu Aufnahmezwecken lediglich eingeschaltet zu werden. Als Schnittstellen besitzt tCube zwei Netzwerkbuchsen sowie mehrere Videoeingänge. Eine Netzwerkbuchse wird mit dem lokalen Netzwerk verbunden und einmal konfiguriert. Die zweite Netzwerkbuchse dient als Schnittstelle in das Inter-/Intranet. Ein Dozent kann seinen eigenen Laptop für die Präsentation benutzen. Ohne Konfiguration hat er dann automatisch Zugang zum Internet (falls erwünscht). Weiterhin greift der tCube den kompletten Desktop des Dozentenrechners ab. Das Gerät kann ähnlich wie ein Videorekorder über eine Webschnittstelle konfiguriert werden.

Der tCube beherrscht als Ausgabeformate Realmedia und MPEG 4. Durch die Unterstützung von MPEG 4 kann auch der kostenlose Apple Quicktime Server genutzt werden. Weiterhin steigt die Anzahl der Wiedergabeprogramme. Microsoft Mediaplayer oder auch der Apple Quicktime

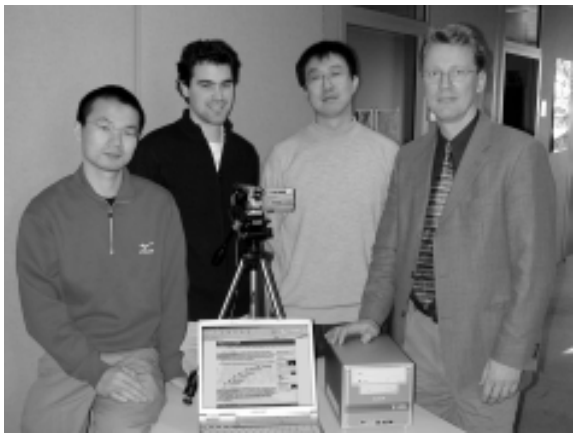


Abb. 2: Handlichkeit zeichnet den tCube (rechts unten) aus. Das Foto zeigt die tele-TASK-Entwicklergruppe rund um Prof. Meinel.

## 2. Automatisches Fahrtenbuch mit GPS-Unterstützung für Pocket PCs

*Nach dem großen Erfolg des GPS-Fahrtenbuches für PalmOS-Handhelds wurde am Institut für Telematik nun auch eine Version für Pocket PCs („Windows Handhelds") entwickelt, deren Verbreitung in den letzten Jahren stark zugenommen hat.*

## 2. Automated Driver's Logbook Keeping with a Handheld and GPS Support

*After the large success of the GPS supported driver's logbook for PalmOS handheld a version for Pocket PC, whose spreading increased in the last years, was now developed at the Institute for Telematics.*

Die Führung eines konventionellen Fahrtenbuchs ist eine lästige, umständliche und zeitraubende Angelegenheit. Eine Vielzahl von Angaben müssen von Hand in das Fahrtenbuch eingetragen werden - selbst bei den elektronischen Fahrtenbüchern sind zahlreiche Angaben vom Benutzer selbst einzugeben. Nicht so beim GPS-Fahrtenbuch des Instituts für Telematik - eine enorme Erleichterung für jeden, der die Kosten für Autofahrten abrechnen kann.

Das am Institut entwickelte Fahrtenbuch ermittelt die Daten einer Autofahrt automatisch. Im Gegensatz dazu müssen Nutzer anderer Fahrtenbuch-Programme immer selbst den Kilometerstand des Tachometers ablesen und dann zusammen mit anderen wichtigen Informationen (siehe Abb. 1) manuell eingeben. Diese Vorgehensweise ist jedoch vielen Autofahrern so unbequem, dass sie dem Finanzamt kein Fahrtenbuch vorlegen, sondern die für sie ungünstigere Pauschalversteuerungs-Lösung wählen. Bei der vollautomatischen Fahrtenbuchführung entfallen hingegen solche manuellen Eingaben.


| Eintragungen | elektronisches Fahrtenbuch ohne GPS | elektronisches Fahrtenbuch mit GPS |
|---|---|---|
| Datum und Uhrzeit | automatisch | automatisch |
| KM-Stand (Fahrtbeginn) | automatische Übernahme des aktuellen Kilometerstands | automatische Übernahme des aktuellen Kilometerstands |
| KM-Stand (Fahrtende) | muss eingegeben werden | automatische Berechnung |
| Start- und Zielort | müssen eingegeben werden | automatische Ermittlung |
| Name des Fahrers | automatisch Übernahme des letzten Eintrags | automatische Übernahme des letzten Eintrags |
| Besuchte Firma | muss angegeben werden | automatische Ermittlung |

Abb. 1: Vergleich herkömmlicher elektronischer Fahrtenbücher mit dem am Institut entwickelten GPS-Fahrtenbuch für Pocket PCs

Beim GPS-Fahrtenbuch werden mittels GPS die Position des Start- und Zielorts und die gefahrenen Kilometer automatisch ermittelt. Zudem wird bei Dienstfahrten mit Hilfe der Zielkoordinaten die besuchte Firma bestimmt. Es ist ein lernendes Fahrtenbuch: einmal eingegebene Zielorte und besuchte Firmen werden mit den Positionsdaten in einer Datenbank abgelegt.

Die Fahrtenbuch-Daten werden über die Docking-Station des Pocket PCs zu einem herkömmlichen PC übertragen und können dort zur Vorlage beim Finanzamt ausgedruckt werden (siehe Abb. 2).

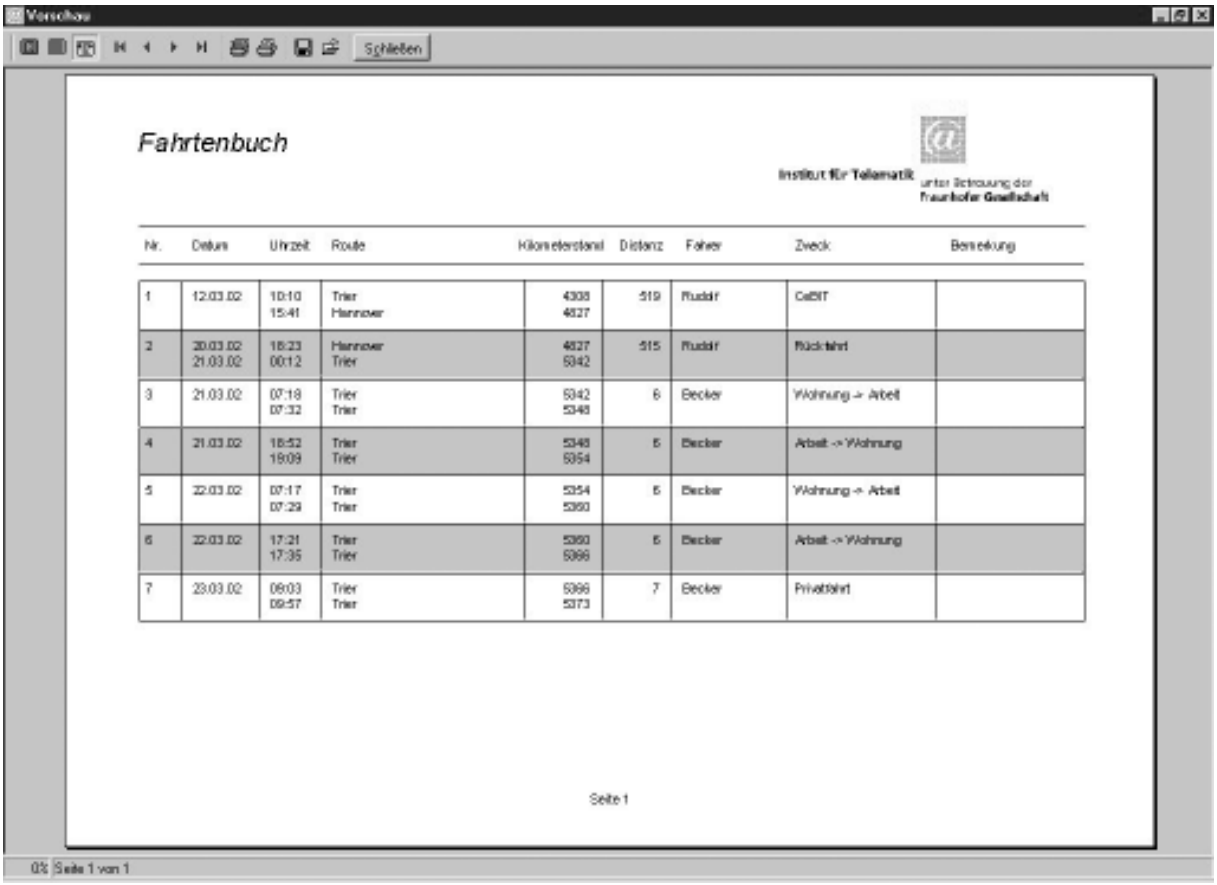



Abb. 2: Ansicht des Fahrtenbuchs am PC

Eine Benutzung des GPS-Fahrtenbuchs durch verschiedene Fahrer ist möglich. Es wird zwischen privaten und dienstlichen Fahrten sowie Fahrten zwischen Wohnung und Arbeitsstätte unterschieden. Ein Betrieb ohne GPS-Empfänger ist ebenfalls möglich.


Abb. 3: Das Fahrtenbuchprogramm auf einem Pocket PC

## 3. jDAPHNE: vom Prototypen zum Produkt

*Im Jahr 2002 wurde der Schwerpunkt bei der Entwicklung von jDAPHNE auf die Durchführung vielfältiger Tests gelegt. Mit Hilfe der Testergebnisse wurde der Programm-Code konsolidiert so dass der ehemalige Prototype eines Redaktionssystems nun als ausgewachsenes Produkt bezeichnet werden kann.*

## jDAPHNE: From a Prototype to a Product

*In the year 2002 the main focus in the development of jDAPHNE was set on various tests of single and complex functionalities. Due to this extensive code revision, jDAPHNE evolved from a productive prototype to a product.*

Bei jDAPHNE handelt es sich um ein modernes Online-Redaktionssystem, das in einfacher Art und Weise Unternehmen die Pflege ihrer Websites ermöglicht. Statt einer externen Internet-Agentur, internen Webmastern oder Online-Redaktionen, denen oftmals die inhaltliche Kompetenz fehlt, kann mit jDAPHNE der Sachbearbeiter selbst die von ihm aufbereiteten Inhalte ins Netz stellen. Verzögerungen in der Aktualität und gegebenenfalls inhaltliche Fehler durch die Einschaltung der technischen Fachkräfte können so vermieden werden.

Gemäß dem Mehr-Augen-Prinzip kann nach der Erstellung und vor der Publikation eine Kontrolle stattfinden, um die Qualität des Internetauftritts zu sichern.

Das System kann auf jeder üblichen Benutzeroberfläche genutzt werden. Einzige Vorgabe ist das Vorhandensein eines Browsers auf dem Arbeitsplatzrechner. jDAPHNE ermöglicht die Einrichtung verschiedener Zugriffsrechte. Je nach Position eines Mitarbeiters ist es ihm möglich, auf die Inhalte lesend, schreibend oder publizierend zu-

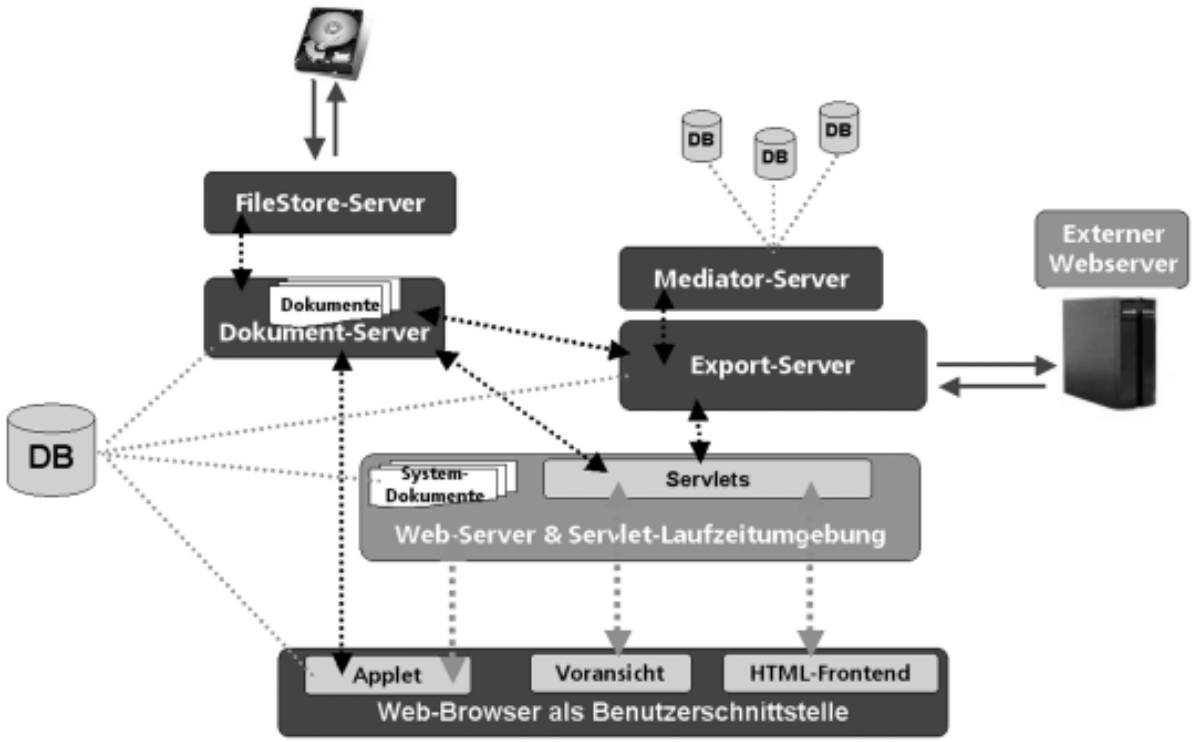



Abb.1: jDAPHNE System Architektur

zugreifen. Das von dem Programm gesteuerte Management der Querverweise (Hyperlinks) zwischen den einzelnen Dokumenten ist so ausgelegt, dass vom Programm Vorschläge für solche Links gemacht und so genannte tote Links deaktiviert werden.

Das Online Redaktions-System ist in aktueller Java-Technologie entwickelt. Einzelne Komponenten können, da die Kommunikation über RMI erfolgt, auf verschiedene Rechner verteilt werden. jDaphne unterstützt sowohl dynamisches als auch statisches Publizieren. Im ersteren Fall ist die Verfügbarkeit eines Servlet-Engines auf dem Web-Server notwendig. Für die statische Variante werden die Dokumente verzeichnisorientiert in das Dateisystem des Web-Servers geschrieben.

Zum Abschluss der Konsolidierungsphase hat das Institut eine CD mit einem komfortablen Installationsprogramm für Windows-Umgebungen vorgelegt. Installiert werden kann eine Basisversion bestehend aus jDAPHNE, einer open source-Datenbank, einem open source-Webserver und einer open source-Laufzeitumgebung für serverseitige Anwendungen. Auf der Basis dieser Installationsversion, die auch als Demonstrator genutzt werden kann, ist die individuelle Anpassung des Systems an die Infrastruktur und die Anforderungen der Kunden schnell und komfortabel möglich.


Abb. 2: Das interaktive Benutzerfrontend von jDAPHNE. Links die virtuelle Verzeichnisstruktur, rechts die in dem Verzeichnis enthaltenen Dokumente mit einer Auswahl von Metainformationen

Über die Konsolidierungsarbeit hinaus wurde die Systemfunktionalität stark erweitert. Besondere Bedeutung hat dabei die innovative mehrsprachliche Präsentation der Website. Hier beschreitet jDAPHNE in sofern einen außergewöhnlichen Weg, als dass das System gleichzeitig sowohl Content-Negotiation zwischen Web-Server und -Browser unterstützt als auch die Publikation der einzelnen Sprachversionen auf dedizierte virtuelle Server. Insbesondere die Verknüpfung dieser beiden Varianten durch entsprechend vom


Abb. 3: Der virtuelle Schreibtisch. Eine Übersicht aller gerade beim Benutzer lokal bearbeiteten Dokumente

System gesetzte Hyperlinks stellt für die Nutzer im Internet einen echten Mehrwert auf der Website dar.

Weiterhin wurde das System hinsichtlich seiner Benutzerfreundlichkeit weiter optimiert. Durch das geeignete Zusammenfassen von Einzelfunktionalitäten sind neue „Powerfunktio-nen“ entstanden, die beispielsweise mit einem Tastenklick die „ganze Web-Präsenz“ umbauen können.

Zu den neu hinzugekommenen Features gehören beispielsweise I-Frame-zentrierter Export und die zumindest im Intranet sinnvolle Nutzung von Office-Dokumenten als Einstiegsseiten für die von jDAPHNE verwalteten Verzeichnisse - Ressorts genannt. Bei anderen Systemen dieser Kategorie sind solche Exportvarianten nicht selbstverständlich.

## 4. Automatische Erinnerungs-SMS für Patienten

*Bei der Entwicklung eines Geräts, das Patienten automatisch an anstehende Vorsorge- und Impftermine erinnert, haben sich – wie im Jahresbericht 2001 aufgezeigt – nicht nur telemedizinisch bedeutsame Sachverhalte ergeben. Interessant sind auch die innovativen Methoden, mit denen eine komplexe innere Struktur nach außen hin als einfache Schnittstelle präsentiert wird. In diesem Projekt, das unterschiedliche Schnittstellen verbindet, konnten gleich mehrere Herausforderungen gemeistert worden.*

## 4. Selfacting Reminder-SMS for Patients

*Patientreminder is a program, which helps patients and medical doctors for having control about their dates for preventive medical checkups. The medical aspects are described in the progress report 2001. Moreover the technical aspects are meaningful. A complex internal structure is covered by a simple user interface. In this project several difficult tasks could be solved. The solution required the implementation of innovative methods of software engineering.*

So funktioniert das innovative Gerät: In einer Arztpraxis werden unter Verwendung der Krankenkassenkarte Patientendaten erfasst und gespeichert. In regelmäßigen Abständen wird die so angelegte Datenbank durchsucht. Stellt das Gerät einen baldigen Untersuchungstermin für einen Patienten fest, so wird dieses Datum markiert und mit Terminen anderer Patienten gesammelt und zur gemeinsamen Versendung vorbereitet.

Selbständig wählt sich das Gerät in das Telefonnetz ein und versendet die Informationen an eine Partnerfirma. Die entpackt die Informationen und versendet an mobile Telefongeräte der Patienten SMS-Nachrichten mit der Aufforderung, sich an seinen Arzt zu wenden, um einen Termin zu vereinbaren.

Im Herbst 2001 wurde die Idee für diesen Reminder geboren. Viele miniaturisierte Computer kamen damals neu auf den Markt. Handhelds und Palms waren und sind bis heute in Mode. Hier versprach ein kleines, preiswertes System geeignet zu sein, um als Träger obiger Produktidee in Arztpraxen Einzug zu halten. Enge preisliche Vorgaben machten es nötig, nach wirklich innovativen neuen Hard- und Softwarebausteinen zu suchen.

Als zur damaligen Zeit einziges Gerät erfüllte der Handheld-Computer „Agenda" diese Bedingungen. Mit seinem Touchscreen und seiner vorbereiteten E-mail-Funktionalität schien er technisch geeignet. Durch die Verwendung von open source-Software erfüllte er die finanziellen Rahmenbedingungen. Als erstes sollte die Ansteuerung eines Kartenlesers verwirklicht werden. Aber trotz Teilerfolgen konnte keine funktionsfähige Kommunikation aufgebaut werden.

Die Entwicklung und das Testen des Programms wurde dann mit der Hoffnung auf einen PC verlagert, in einer späteren Version des Kleingerätes das Programm darauf zu installieren. Vorteilhaft war, dass auf dem „Agenda" eine grafische Bibliothek (FLTK) verwendet wurde, die von ihrer Größe und Ausführungsgeschwindigkeit prädestiniert war auf Handhelds zum Einsatz zu kommen. Später zeigte es sich, dass die Bibliothek auch unter dem Windows-Betriebssystem eingesetzt werden kann.

Das Programm kann sich bei einem beliebigen Provider einwählen und die gepackten Informationen an die Partnerfirma versenden. Da aber die Provider nur E-Mails weitersenden von Nutzern, die bei ihnen auch einen E-Mail-Account besitzen, musste die Lösung auf die Verwendung eines „sendmail" Programms verzichten, das die Mails automatisch an die richtige Stelle weiterleitet. Das machte die Erstellung eines eigenen E-Mail-SMPT-Clients erforderlich. Hier wäre es für die Zukunft denkbar, den notwendigen Verbindungsaufbau mit einer verschlüsselten Variante vorzunehmen.

## 5. Die SDS-Middleware im Kontext von Web-Services und SOAP

*Das Institut für Telematik hat eine eigene Middleware-Plattform entwickelt, den Smart Data-Server (SDS). Er ist mit einem eigenen optimierten Kommunikationsprotokoll auf Basis einer XML-basierten Dokumenten-Austauschsprache versehen. Dieses Protokoll hat viele Ähnlichkeiten mit SOAP, dem Simple Object Access Protocoll. Nach dessen Standardisierung durch das World Wide Web Consortium war es somit einfach, eine zusätzliche Protokoll-Schnittstelle in den SDS zu integrieren. Somit ist der Smart Data Server nun auch ein Web-Service-Server.*

## 5. SDS-Middleware in the Context of Web-Services and SOAP

*The Institute for Telematics has developed a middleware platform, called Smart Data Server (SDS). It is provided with an optimised communication protocol based on the document interchange language „XML". This protocol is similar to SOAP, the „Simple Object Access Protocol". After the standardization of SOAP by the W3C it was easy to add this new protocol interface into the SDS. So the Smart Data Server has become a web service server.*

Folgende Definition von Web-Services hat das World Wide Web Consortium (W3C) in dessen Dokumentationen festgelegt:
Ein Web-Service ist eine Software, die durch eine URL identifiziert ist (RFC2396) und deren öffentliche Schnittstellen und Bindungen durch XML definiert werden. Seine Definitionen können durch andere Software-Systeme ermittelt werden. Diese Systeme können mit dem Web-Service in der vorgeschriebenen Art interagieren, wobei über Internet-Protokolle versandte XML-basierte Nachrichten verwendet werden.

Was bedeutet dies nun genau? Es soll ein einfacher, auf schon existierenden Standards aufbauender Mechanismus definiert werden, mit dem Dienste im Internet genutzt werden können. Der Zugriff auf diesen Dienst soll nachrichtenbasiert geschehen, also in der Form von Anfrage- und Antwort-Dokumenten. In diesem Punkt legt sich die Definition auf das allgemein akzeptierte Dokumentenaustausch-Format XML fest.

Bei dem Transport der Nachrichten ist die Definition etwas freier: Hier ist nur die Rede von Internet-Protokollen. Allen voran steht offensichtlich das HTTP-Protokoll, das die meisten Menschen wohl nicht kennen, was aber immer dann in Aktion tritt, wenn in einem Web-Browser eine Web-Site von einem Web-Server aufgerufen wird. Die Eingabe einer Internet-Adresse in dem Format „http://www.…" teilt dem Browser mit, dass er den WWW-Rechner mit dem HTTP-Protokoll ansprechen muss.

HTTP ist ein sehr populäres Protokoll, das oft auch den einzigen Zugang zu Rechnern darstellt, da alle anderen Protokolle und Dienste durch Firewalls blockiert sind. Ein anderes sehr populäres Internet-Protokoll ist SMTP, das für den Transport von E-Mails im Internet verantwortlich ist. Auch mit diesem Protokoll sind die Anforderungen erfüllt, die für die Erreichbarkeit eines Web-Services nötig sind. Die Anfrage- und Antwort-Dokumente können hier über den E-Mail-Mechanismus transportiert werden.

Eine Technologie, die zur Zeit mit Web-Services in Verbindung gebracht wird, ist SOAP, ursprünglich als „Simple Object Access Protocoll" definiert. Es erfüllt die Anforderungen der Web-Service-Definition im Hinblick auf Nachrichtenaustausch. Der Kern von SOAP ist das XML-Format zur Erstellung des Anfrage- und Antwort-Nachrichtendokumentes. SOAP selber definiert in keiner Weise die Implementierung des angesprochenen Dienstes auf der Web-Service-Seite. Das ist ein unbestrittener Vorteil, da damit weder Betriebssystem noch verwendete Programmiersprache festgelegt sind.

Web-Services stellen also im Internet leicht erreichbare, von Betriebssystemen und Programmiersprachen unabhängige Dienste zur Verfügung. Im Allgemeinen sind bei der Nutzung solcher Dienste auch weitere Server einbezogen, welche die Beantwortung einer Anfrage ermöglichen. Wichtigster Partner sind Datenbanken, die entsprechende Daten vorhalten, welche vom Dienst aufbereitet dem Client übermittelt werden. Ein Web-Service-Server hat somit auch vermittelnde Funktionen, weshalb ein solcher Server auch in die Kategorie von Middleware-Server fällt.

Das Institut für Telematik hat nun seine eigene Middleware-Plattform, den Smart Data-Server (SDS), weiterentwickelt (Abbildung 1). Da er mit einem eigenen, optimierten Kommunikationsprotokoll auf Basis einer XML-basierten Dokumenten-Austauschsprache versehen ist, das viele Ähnlichkeiten mit SOAP hat, war es einfach, eine zusätzliche Protokoll-Schnittstelle in den SDS zu integrieren. Dadurch ist der SDS jetzt auch ein Web-Service-Server.

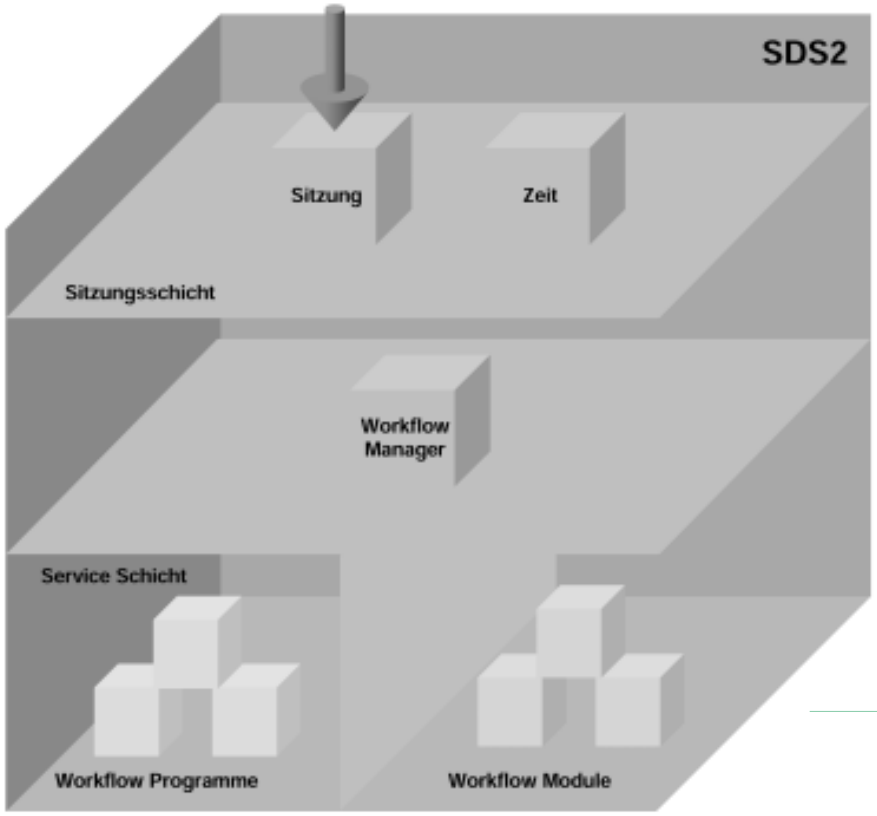



Abb. 1: Der SDS 2

Doch die Entwicklung des SDS hat auch an anderer Stelle nicht halt gemacht. Die internen Datenflüsse werden neuerdings in sogenannten Workflow-Programmen repräsentiert, die auf spezialisierten Workflow-Modulen aufbauen. Dabei handelt es sich um Meta-Programme, die nicht zur Übersetzungszeit des Servers vorliegen müssen, sondern erst zur Laufzeit des Servers die inneren Abläufe definieren. Damit ist höchste Flexibilität und zukünftige Erweiterbarkeit der Serverstruktur garantiert. Zusätzlich wird der interne Datenfluss parallelisiert, womit eine optimale Ressourcenauslastung des Servers möglich ist.

## 6. Lernplattform vermittelt spezifisches Wissen zur IT-Sicherheit

*Viele Risiken von IT-Systemen könnten vermieden werden, wenn sowohl die Benutzer als auch die im Management Verantwortlichen für Sicherheit sensibilisiert und entsprechend geschult werden. Mit der Lernplattform IT-Sicherheit entwickelt das Institut für Telematik ein Tutorensystem, das auf die jeweilige Benutzergruppe zugeschnittenes Wissen vermittelt. Anders als sonst werden die Übungen nicht in einer eingeschränkten Simulationsumgebung, sondern auf einem realen System durchgeführt. Lernende können ihre Kenntnisse dadurch leicht in die Praxis übertragen.*

## 6. A Tutoring System for IT Security

*Many risks of IT systems can be avoided if both the users and the IT managers are made sensitive to and trained for IT security. The Institute for Telematics develops a tutoring system, called Lernplattform IT-Sicherheit, that teaches knowledge about IT security for different user groups. In contrast to many other tutoring systems, exercises are not made in a restricted simulation environment but on a real system. This allows the learner to apply his skills easily in practice.*

Die Lernplattform IT-Sicherheit basiert auf dem Open-Source-Betriebssystem Linux, für das eine Vielzahl von freien Sicherheitstools existiert und welches sich daher als ideale Umgebung anbietet. Die Lernplattform soll jedoch nicht nur auf Linux zugeschnittene Inhalte anbieten, sondern auch allgemeine Sicherheitsaspekte abdecken. Die Bandbreite der behandelten Themen wird unter anderem Kryptographie, Authentisierung, Intrusion Detection, Firewalls, Netzwerk-Sniffing, Viren und Security-Scans umfassen.

Je nach Benutzertyp können die Anforderungen an IT-Sicherheit unterschiedlich ausfallen. Ein typischer Endbenutzer benötigt z.B. Informationen über den sicheren Versand von E-Mails; im Gegensatz zu einem Systemadministrator muss er sich aber in der Regel nicht mit Fragen der Einbruchserken-nung (Intrusion Detection) auseinandersetzen.

Auch die technische Tiefe kann je nach Benutzergruppe variieren. Die Lernplattform trägt diesem Umstand Rechnung, indem die angebotenen Informationen und Übungen je nach Zugehörigkeit zu einer Benutzergruppe unterschiedlich zusammengestellt werden.

Ein Benutzer, der die Lernplattform zum Studium einsetzt, agiert innerhalb einer kompletten Linux-Umgebung (siehe Abbildung 1). Die Interaktion mit dem Tutorensystem erfolgt über ein Web-Browser-Interface, das dem Benutzer die Lerninhalte auf vertraute und strukturierte Weise präsentiert (Abbildung2). Die Übungen er-

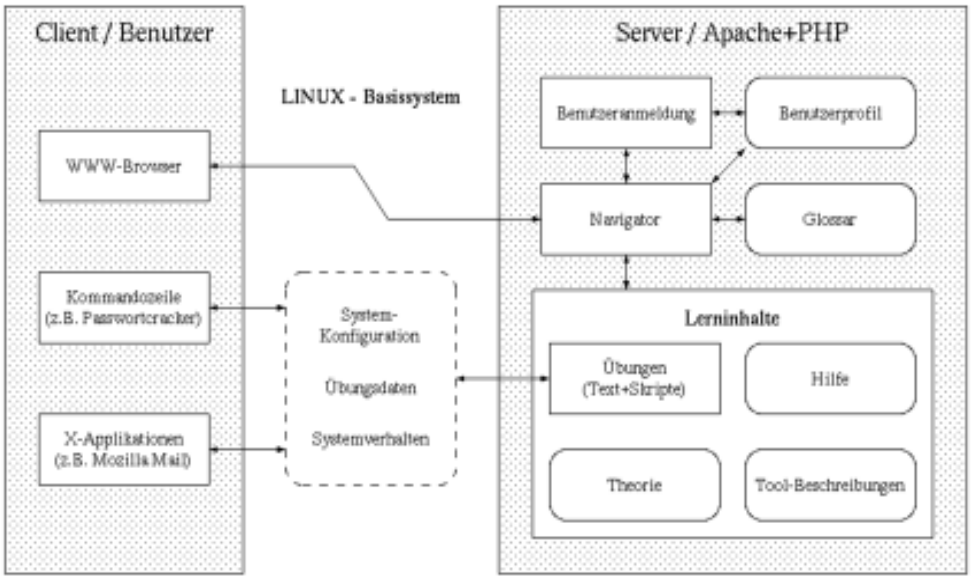



Abb. 1: Lernplattform IT-Sicherheit

folgen unmittelbar auf dem Linux-System durch den Aufruf kommandozeilenbasierter Tools oder X-Applikationen.

Die präsentierten Inhalte teilen sich grob in drei Kategorien auf:

- Theoretisches Grundwissen über das behandelte Themengebiet
- Technische Anleitungen zu Software-Tools und zur Konfiguration von Betriebssystem und Anwendungen
- Praktische Übungen auf der Basis der zuvor vermittelten Inhalte

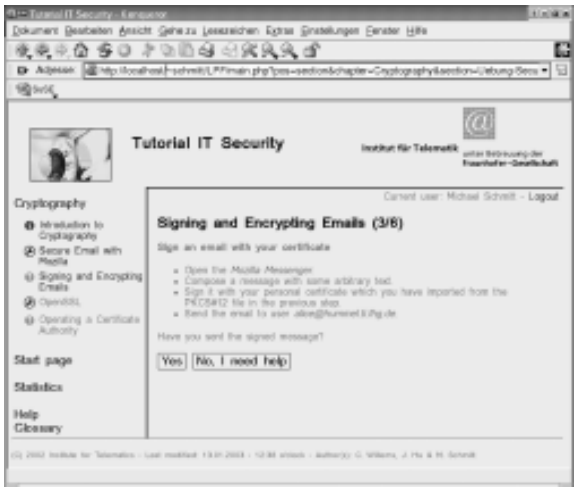



Abb. 2: Übungen zum Verschlüsseln und Signieren von E-Mails

Das Linux-System wird vor jeder Übung so konfiguriert, dass diese ordnungsgemäß und mit dem gewünschten Ergebnis durchgeführt werden kann. So werden beispielsweise wichtige Systemdateien verändert, damit der Benutzer bestimmte Dienste vorfindet. Um die Verwendung von Zertifikaten zu lehren, richtet das Tutorensystem einen virtuellen Partner ein, mit dem der Benutzer verschlüsselte und signierte E-Mails austauschen kann.

Ein wichtiger Aspekt beim Eigenstudium ist eine gezielte Hilfestellung und Lernkontrolle durch das Tutorensystem. Bei Problemen mit Übungen wird der Benutzer durch Rückfragen und Tipps unterstützt (Abbildung 3). Am Ende einer Aufgabe werden die Ergebnisse und Antworten durch die Lernplattform auf ihre Richtigkeit überprüft. Verweise auf das globale Glossar helfen weiter, wenn einmal eine Abkürzung oder ein Fachbegriff im Text unklar ist.

Auch der Fall, dass der Benutzer durch Fehlbedienung sein System in einen undefinierten Zustand versetzt, ist berücksichtigt. So ist geplant, das Tutorensystem komplett von der CD zu starten. Nach einem Neustart können die Übungen an der zuletzt besuchten Stelle fortgesetzt werden. Zu diesem Zweck werden alle benutzerspezifischen Informationen auf Diskette gesichert und bei erneuter Anmeldung am Lernsystem abgerufen. Alternativ dazu werden Techniken evaluiert, um das Tutorensystem online über das Internet anbieten zu können. Die Übungen sollen dann serverseitig auf einer virtuellen Maschine ablaufen.

Der aktuelle Bearbeitungsstand des Tutorials kann jederzeit über eine Statistikseite abgerufen werden. Neben einer Übersicht über die besuchten Kapitel bzw. erfolgreich abgeschlossenen Übungen sind die Verweildauern für jeden Abschnitt protokolliert. Diese Informationen sollen u.a. auch für die Weiterentwicklung der Lernplattform berücksichtigt werden, um den Umfang und die Struktur des Lernmaterials zu optimieren.

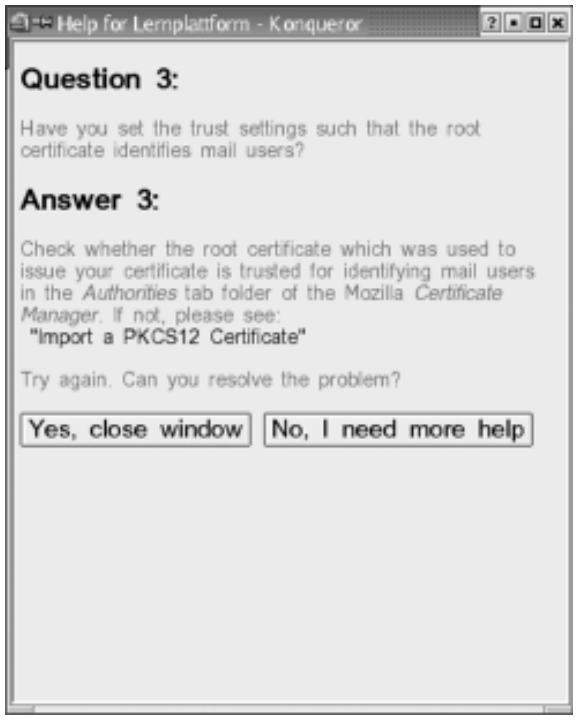



Abb. 3: Hilfestellung

## 7. Neues Verfahren verwandelt Röntgenbilder in dreidimensionale Objekte

*Digitaler Bildaustausch hilft in Krankenhäusern und Arztpraxen, Mehrfachaufnahmen zu vermeiden und dadurch Kosten einzusparen. Allerdings ist Standardisierung notwendig, damit sich die Geräte „verstehen". Deshalb setzt sich bei technischer Ausrüstung im medizinischen Bereich, wie bei Computer- und Magnetresonanz-Tomographen, immer mehr der DICOM-Standard (Digital Imaging and Communication in Medicine) durch. DICOM erlaubt den Transfer von Bilddaten gemeinsam mit dazugehörender Patienten- und Bildinformation. Der am Institut für Telematik entwickelte DICOM 3D-Generator zur Deformation von zweidimensionalen radiologischen Aufnahmen in der Kieferorthopädie verwendet diesen Standard als Bilddateiformat.*

## 7. A New Method that Transforms X-ray Images into 3D-Images

*Exchange of digital images helps to reduce the amount of radiological images and costs in hospital and doctor's praxis. A standard is necessary in order to let equipment communicate. Medical equipment like computer and magnet resonance tomography will conform to DICOM (Digital Imaging and Communication in Medicine) more and more. DICOM allows the transfer of image data together with patient related and image related data. The Institute for Telematics developed a DICOM 3D Generator. The Software uses the DICOM Standard as image format for the transformation of digital two-dimensional radiological images of the human jaw.*

In der Zahnmedizin gibt es ein nicht zu unterschätzendes Problem bei der Diagnose von Verletzungen oder Erkrankungen im Bereich der Zahnwurzeln: Die Diagnose wird durch die hufeisenförmige Struktur des Kiefers erschwert. Der Arzt muss sozusagen „im Kopf" die zweidimensionalen Bildserien räumlich zusammensetzen. Eine dreidimensionale Rekonstruktion durch einen Computer erleichtert diesen Vorgang.

Es war somit ein Verfahren für den kieferorthopädischen Bereich zu entwickeln. Für die Untersuchung, bei der das Verfahren angewandt werden soll, wird vom Computer-Tomographen eine Serie zweidimensionaler Schichtbildaufnahmen zur Verfügung gestellt. Systembedingt werden die Schichtbildaufnahmen so angefertigt, dass die hufeisenförmige Struktur des Kiefers in der Transversal-Ansicht zu sehen ist (Abbildung 1). Diese hufeisenförmige Struktur ist in eine gerade zu transformieren. Aus der so entstehenden Serie neuer Bilder wird ein 3D-Objekt generiert.

Im medizinischen Bereich gibt es bei den Verfahren zur Deformation von Objekten zwei Arten: solche, die entweder auf der Verformung von weichem oder von hartem Gewebe basieren.

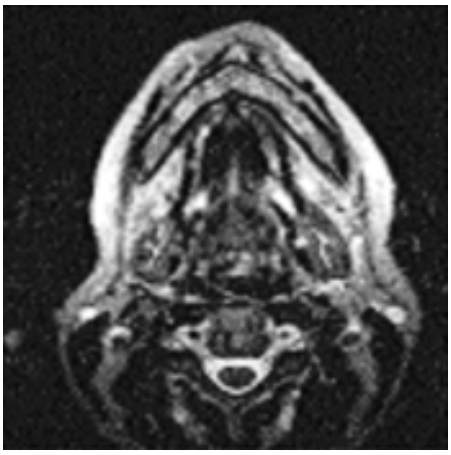


Abb. 1: Transversal-Ansicht des Kiefers

- Ein Beispiel für die Verformung weichen Gewebes ist die Simulation eines chirurgischen Eingriffs, bei dem Organe angefasst oder verschoben werden sollen.
- Verfahren, die hartes Gewebe verformen, werden zur Zeit eingesetzt, um reale Verformungen zu beschreiben.

Wir haben uns in dem genannten Anwendungsbeispiel auf die Simulation der Verformung von Hartgewebe für diagnostische Zwecke konzentriert. Man unterscheidet zwischen zweidimensionaler Verformung von Bilddaten und dreidimensionaler Verformung eines Objektes. Das von uns verwendete Verfahren ist geeignet für die Verformung von 2D-Bildern einer Bildserie, da es einfach realisierbar und kontrollierbar ist.

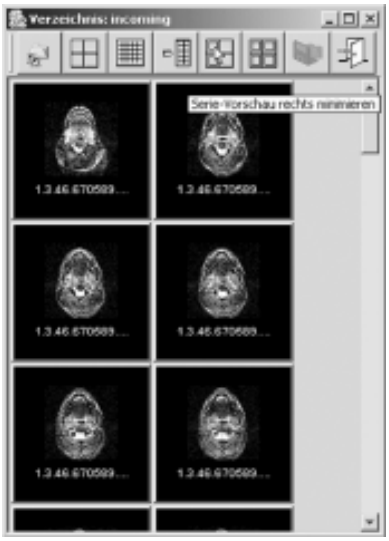



Abb. 2: Auswahl der Bilder und Bestimmen des Referenzbildes.

Die Anwendung erzeugt aus einer Serie von deformierten Bildern ein 3D-Objekt. Die Deformation einer Serie von zweidimensionalen DICOM-Bildern erfordert die Auswahl der zu deformierenden Bilder sowie des Referenzbildes vom Benutzer (Abbildung 2). Das Referenzbild ist in der ausgewählten Serie enthalten.

Ein Speichern der Auswahl bewirkt das Öffnen und Visualisieren des Referenzbildes. Der Benutzer kann nun die Schablone in die zu deformierende Region setzen und an diese anpassen (Abbildung 3). Ist der Vorgang abgeschlossen wird zunächst das Referenzbild und anschließend die ausgewählte Bildserie deformiert und visualisiert (Abbildung 4).
Es ist nun aus den deformierten Bildern ein 3D-Objekt generiert worden. Aus den Bildern wurde der durch die Deformation verzerrte und für die Diagnose nicht relevante Teil entfernt. Das 3D-Objekt kann nun als Serie zweidimensionaler DICOM-Bilder gespeichert werden. Für die Orientierung bei der Spezifikation einer Schnittebene wird ein transparenter Würfel mit der Schnittebene visualisiert. Sie kann durch Parameter angepasst werden. Mit Hilfe der Schnittebene ist es möglich, durch das Innere des Objektes zu „wandern". Das Objekt kann zusätzlich frei rotiert werden.

Aufgrund der Informationen, die in den DICOM-Bildern zusätzlich zu den Bilddaten abgelegt werden können, kann das 3D-Objekt, unter Berücksichtigung der Reihenfolge und des Abstandes der Schichtbilder zueinander, rekonstruiert werden. Mit Hilfe des konstruierten 3D-Objektes können nun Verletzungen besser, ohne Behinderung durch die Gestalt des Kieferknochens, diagnostiziert werden.

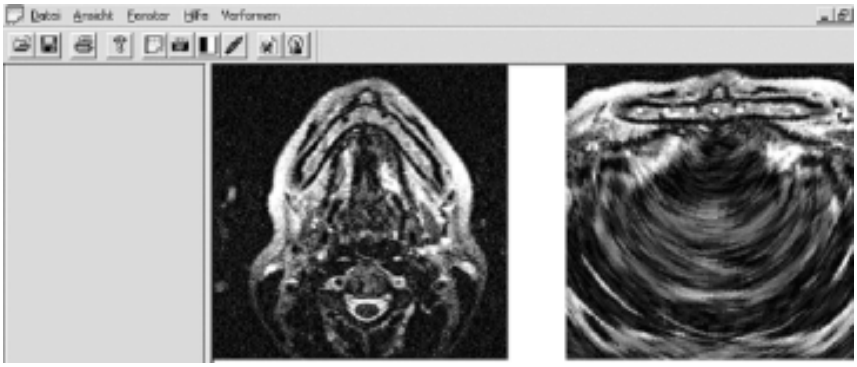


Abb. 3: Setzen der Schablone und Deformieren der Bilder.

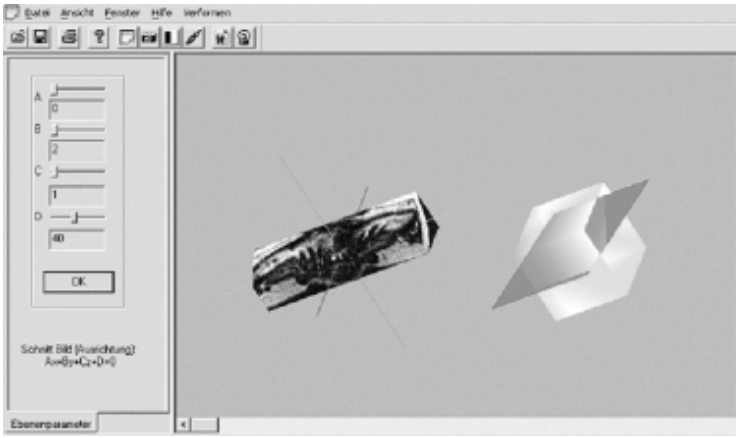



Abb. 4: Generieren des 3D-Objektes.

## 8. Das Trierer Trust Center und der elektronische Arztausweis

*Trust Center fungieren bei digitaler Kommunikation als vertrauenswürdige Dritte, gewissermaßen als „elektronische Notare". Sie sichern den Datenaustausch über E-Mails, in Intra- und Extranets, beim elektronischen Handel und in Archivierungssystemen. Geht es um rechtsverbindliche elektronische Kommunikation, arbeiten Trust Center entsprechend den Vorgaben des Signaturgesetzes. Dadurch wird das geforderte Sicherheitsniveau etabliert, das Nichtabstreitbarkeit und rechtliche Bindung der digitalen Signatur sicherstellt. Das Trust Center des Instituts für Telematik ist jetzt zum Beispiel in die Entwicklung des elektronischen Arztausweises eingeschaltet worden.*

## 8. The Trier Trust Center and the Health Professional Card

*Trust Centers act as trusted third party to enable secure communication of digital documents. They witness the identities of the communication parties. Their services help to secure data exchange for example by e-mail, communication in Intra- and Extranets, in electronic commerce and data storage in archival systems. If legal aspects are concerned, trust centers have to fulfill standards according to the digital signature law, ensuring the security level that provides non-repudiation and legal binding to the signatures created. Our Trust Center has also been involved in the deployment plans of the Health Professional Card.*

Trust Center sind in der Regel bemüht, ihre Dienstleistungen in Übereinstimmung mit Signatur-Gesetz und -Verordnung anzubieten. Das hebt den Wert und die Vertrauenswürdigkeit der ausgestellten Zertifikate auf das höchste Niveau. In Unternehmen wird dies aber nicht immer benötigt. Aus Kostengründen verzichten die Betreiber der größten und verbreitetsten Public-Key-Infrastrukturen derzeit meist auf die Erfüllung der hohen Anforderungen des Signaturgesetzes.

Die grundlegenden Anwendungsfälle für Dienstleistungen eines Trust Centers finden sich im Bereich sichere elektronische Kommunikation oder Datenspeicherung bis hin zu rechtlich verbindlicher Kommunikation mittels digitaler Signatur. Konkret bedeutet dies die Sicherung von E-Mail-Verkehr, Intra- und Extranets, E-Commerce-Anwendungen und Archivierungssystemen.

Das Trierer Trust Center des Instituts für Telematik bietet folgende Dienstleistungen an:

1. Zertifizierungsleistungen für Firmenkunden
2. Auftragsforschung und Entwicklung von Software und Komponenten für den Betrieb einer eigenen Zertifizierungsstelle
3. Beratung für den Aufbau und Betrieb von unternehmensinternen Zertifizierungsstellen
4. Schulungen/Informationsveranstaltungen für den Einsatz der Public-Key-Technologien
5. Online-Visualisierungen zur digitalen Signatur und Sicherheits-Protokollen
6. Zeitstempeldienste

Schwerpunkte der Tätigkeit des Trierer Trust Centers im Jahr 2002 waren die Auslagerung von Registrierungsstellen, alternative Registrierungs-Workflows, Attributs-Zertifizierung, Wartung der Public-Key Infrastrukturen von Kunden sowie die Konzeptentwicklung und -abstimmung mit Interessenten und Kunden.

In Kooperation mit Vertretern von Ärztekammern, Kassenärztlichen Vereinigungen und dem Fraunhofer Institut für Biomedizinische Technik hat das Institut im Jahr 2002 auf der Basis der vorhandenen Spezifikationen zur Health Professional Card (HPC) Prototypen für Kartenprofile und Registrierungsprozesse entwickelt. Darüber hinaus entstanden ein Projektplan und Angebote, die neben einer Pilotphase auch die flächendeckende Einführung des elektronischen Ausweises für Ärzte berücksichtigen.

Neben der Ärztekarte gibt es noch Karten für Apotheker sowie Karten für das Personal in Arztpraxen, Apotheken und Krankenhäusern. Letztere bieten den eingeschränkten Zugriff auf Patienten- oder Rezeptdaten, etwa zu Abrechnungszwecken. Auch weitere Berufsgruppen wie Heilpraktiker sind an der Heath Professional Card interessiert.

Natürlich unter angemessener Berücksichtigung des Datenschutzes, ermöglicht der Mechanismus des elektronischen Rezepts auch die Entdeckung von Unverträglichkeiten zwischen von unterschiedlichen Ärzten verschriebenen Medikamenten. Bisher ist der Arzt allein auf die vollständige Angabe aller eingenommenen Medikamente durch den Verbraucher angewiesen.

Weiterführende Informationen und Erklärungen zu den Trust Center-Technologien, Animationen und Visualisierungen zur Digitalen Signatur, SSL PKI und Zertifikaten finden sich im Internet unter der Adresse http://www.telematik-institut.de/titc.

## 9. Lock-Keeper – jetzt doppelter Datendurchsatz bei halber Laufzeit

*Absolute Sicherheit vor Online-Attacken durch Hacker erhält man nur, indem man das interne Rechnernetz eines Unternehmens und das Internet physikalisch voneinander abtrennt. Aber wie kann gleichzeitig Datenaustausch gewährleistet werden? Das Institut für Telematik fand in der Lock-Keeper Architektur (Patentnummer 198 38 253.7-31) die Antwort auf diese Frage. Im Jahr 2002 wurde die mit dem Erfinderpreis des Landes Rheinland-Pfalz ausgezeichnete Hochsicherheits-Schleuse weiterentwickelt: Im Vergleich zum Standard Lock-Keeper kann die Dual Gate-Version den Datendurchsatz verdoppeln und gleichzeitig die Latenzzeit für den Durchlauf der Schleuse halbieren.*

## 9. Lock-Keeper - Now Doubled Throughput in Half the Time

*The only way to achieve absolute safety from hackers' online attacks is to physically separate a companys' intranet from its Internet access. But how can there still be a flow of data between these two? The Institute for Telematics found the answer, developing its patented Lock-Keeper architecture (patent number 198 38 253.7-31). This high security sluice system, after receiving an innovation award from the state of Rhineland-Palatinate, was further improved in the year 2002: Compared to the original, standard Lock-Keeper, the Dual-Gate version simultaneously doubles the throughput and cuts the latency of the data flow in half.*

Die Sicherheitsgefahren aus dem Internet werden immer umfangreicher und sind noch lange nicht gebannt. Regelmäßig erregen Meldungen über „Hackerangriffe", neuartige Viren oder ausgeklügelte Internet-Würmer die Öffentlichkeit. Standardmäßig setzen Unternehmen in diesen Bereichen spezielle Software ein, die sogenannten „Firewalls", um sensible Daten vor Ausforschung und Missbrauch zu schützen. Diese trennen jedoch das interne Rechnernetz eines Unternehmens nicht von der Außenwelt, sondern analysieren und filtern lediglich die übermittelten Datenpakete. Es ist deshalb nicht auszuschließen, dass durch Fehler in der komplexen Firewall-Software oder im darunterliegenden Betriebssystem, mangelnde Kenntnisse des Bedienungspersonals oder fehlerhafte Konfiguration die Firewalls in ihrer Schutzfunktion gefährdet oder sogar außer Kraft gesetzt werden.

Bei vielen Unternehmen wie Banken und Versicherungen ist die Anforderung an die Sicherheit so hoch, dass Standardmittel der IT-Sicherheit dem nicht mehr gerecht werden. In solchen Fällen stellt der Lock-Keeper als eine Hochsicherheitslösung zum Datenaustausch zwischen zwei Netzwerken eine echte Ergänzung oder gar Alternative zu klassischen Firewall-Lösungen dar.

Das Lock-Keeper-Prinzip wurde am Institut für Telematik mit dem Ziel entwickelt, Daten zwischen einem internen, hochsicheren Netzwerk und einem externen, weniger sicheren Netz wie z.B. dem Internet austauschen zu können, ohne dabei eine - wenn auch nur kurzfristig bestehende - direkte Verbindung aufbauen zu müssen. In Anlehnung an den eher schlichten Ablauf, die Daten zwischen den beiden Netzwerken per Diskette zu transferieren, entstand die Idee, eine Lösung zu entwickeln, die diesen „Austausch per Diskette" automatisiert durchführen kann.

### Einfacher Schleusen-Mechanismus als Grundlage

Wie bei einer Schiffsschleuse werden beim Lock-Keeper die Daten so durchgeleitet, dass zu keinem Zeitpunkt eine direkte Verbindung zwischen dem inneren und dem äußeren Netzwerk besteht. Die internen Komponenten des Lock-Keepers sind an einer patentierten Schaltplatine angeschlossen, und zwar so, dass maximal zwei der drei Lock-Keeper-PC's gleichzeitig miteinander kommunizieren können. Dies gewähren sogenannte Schaltrelais (elektronische Schalter) auf der Platine, welche die Verbindung auf Hardware-Ebene in definierten Intervallen umschalten.

Zu keinem Zeitpunkt des Datentransfers besteht eine direkte physikalische Verbindung vom Internet zum Intranet, da beim Lock-Keeper der Datentransfer nicht nur auf Applikations- oder Protokollebene getrennt wird, wie es bei Firewalls üblich ist, sondern tatsächlich die Stromkreise der Leitungen unterbrochen werden. Der Informationsaustausch innerhalb der Schleuse findet je nach Zustand der „Schleusentore" nur jeweils mit einem Kommunikationspartner statt. Während des Aufenthalts in der Schleuse werden die Daten je nach Bedarf z.B. nach Viren, Trojanern oder sonstigen „bösartigen" Inhalten überprüft und dann abhängig vom Prüfungsergebnis entweder durchgelassen oder verworfen.

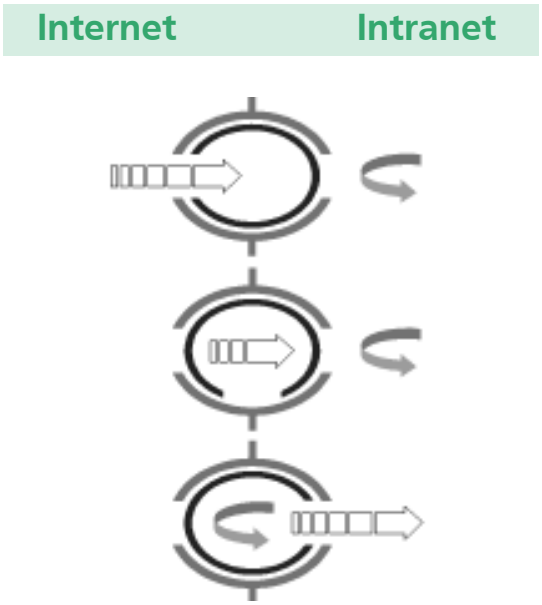



Abb. 1: Das Schleusenprinzip des Lock-Keepers

Die Schleusentechnologie des Lock-Keeper ist somit gegen Online-Attacken immun, da das zugehörige Sicherheitskonzept nicht etwa berechtigte von nicht erlaubten Anfragen trennt (wie bei einer Firewall), sondern grundsätzlich – unabhängig von einer optionalen Analyse – jeglichen Datenverkehr zwischen den inneren und dem äußeren Netzwerk abbricht, zwischenspeichert und hierdurch alle direkten Angriffsmöglichkeiten unterbindet.

Infolgedessen ist es sogar Insidern unmöglich, die Sicherheitsbarriere der hardwareseitigen Trennung von Netzwerken aufzuheben oder zu umgehen. Sowohl bei Software-Fehlern als auch bei versehentlichen oder absichtlichen Misskonfigurationen des Systems gestattet der konzeptuelle und technische Aufbau keine direkte Verbindung der Netze durch die Schleuse.

Für die Integration in die bestehende Infrastruktur wirkt das Lock-Keeper-Schleusensystem wie ein Proxy-Server zwischen den jeweiligen Netzwerken. Es werden Dienste wie Mailtransfer, Dateiaustausch, Datenbanksynchronisation und neuerdings auch Webzugriff unterstützt.

**Erweiterte Funktionalität**

In Zusammenarbeit mit dem luxemburgischen Unternehmen IT-Services s.à.r.l. wurde das ursprüngliche Lock-Keeper-Konzept zum sogenannten *Dual Gate Lock-Keeper* erweitert. Nunmehr werden vier Lock-Keeper-PC's verwendet. Somit können auch Unternehmen mit besonders hohen Performance-Ansprüchen die Vorteile der Schleusentechnologie nutzen. Im Vergleich zum Standard Lock-Keeper kann die *Dual Gate-Version* den Datendurchsatz verdoppeln und gleichzeitig die Latenzzeit für den Durchlauf der Schleuse halbieren. Durch diesen Ausbau werden mit dem Lock-Keeper neue Einsatzgebiete und Kundenkreise erschlossen.

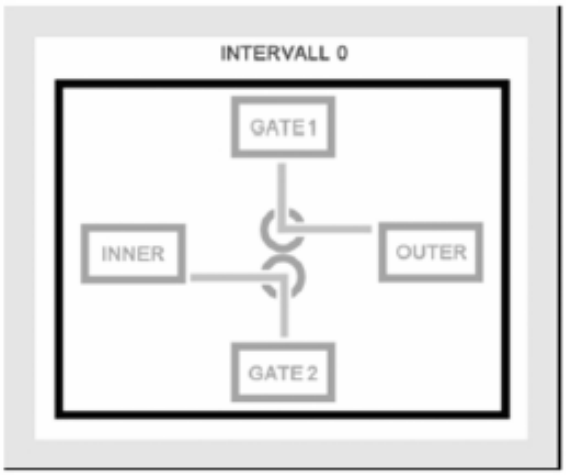



Abb.2: Erweiterung zum Dual Gate Lock-Keeper

Ein weiteres Novum ist die Entwicklung des sogenannten *Web Proxy Moduls*, welches den Zugriff auf das World Wide Web über den physikalischen Schutz des Lock-Keepers ermöglicht. Das *Web-Proxy Modul* erlaubt durch intelligentes Caching-Verhalten fast normales Browsen im Internet. Es ergänzt die etablierten Module *File Transfer* und *Mail Transfer* und erweitert das Spektrum der durch den Lock-Keeper angebotenen Funktionalitäten.

Darüber hinaus wurden die Hilfsmittel für das technische Bedienungspersonal verbessert: Mit der Entwicklung eines integrierten LCD-Displays zur Kontrolle des Systems und erweiterten Logging- und Wartungsmöglichkeiten haben Administratoren effiziente Instrumente bei Pflege und Betrieb des Lock-Keepers zur Hand (s. auch Abb. 1). Dadurch lässt sich der Lock-Keeper noch leichter in bestehende IT-Infrastrukturen und Managementprozesse integrieren.

Der Lock-Keeper wird bereits in mehreren Branchen und Ländern zum Schutz von Unternehmensnetzwerken eingesetzt. Erfolgreich bewährt hat sich der Lock-Keeper zum Beispiel bei der Absicherung von E-Mail-Systemen verschiedener Großbanken, zum Schutz von Datenbanksystemen oder im Rahmen der Installation mehrstufiger Sicherheitsarchitekturen in Regierungsstellen.

## 10. Konzept für den sicheren Betrieb eines WLAN

*Lokale Funknetze erfreuen sich in Firmen immer größerer Beliebtheit, ermöglichen sie doch den Betrieb von Laptops und Handheld-Computern (Palms) ohne lästige Verkabelung. Dadurch bleibt der Vorteil solcher Geräte, die ungehemmte Bewegungsfreiheit, erhalten. Neben Firmennetzen ermöglichen immer mehr öffentliche Gebäude (Flughäfen, Cafés) einen Zugang ins Internet über WLAN. Das Institut für Telematik hat in einem Projekt erforscht, welche Sicherheitsaspekte im Zusammenhang mit der Vertraulichkeit der übertragenen Daten und dem Schutz vor unerwünschten Eindringlingen zu beachten sind. Außerdem wurde ein Konzept für den Betrieb entwickelt.*

## 10. A Security-Concept for a WLAN

*Wireless LANs (WLANs) gain increased popularity by companies. They enable the operation of laptops and handheld computers (palms) without annoying cabling. This allows to preserve the advantages of such devices, i.e. unrestricted freedom of movement. Beside offices, more and more public buildings like airports or coffee bars enable the access to the internet via WLANs. The Institute for Telematics has explored various security aspects concerning the confidence of the transmitted data and the protection against undesired intruders. Moreover it has developed a concept for the operation of an in-house WLAN.*

Der WLAN-Standard (IEEE 802.11b) definiert mit dem WEP-Protokoll (Wired Equivalent Privacy) eine Möglichkeit der verschlüsselten Kommunikation zwischen Funk-Karten und Basis-Station. Die zur Zeit üblichen Verfahren (WEP 40 und WEP 128) leiden unter einem generellen Problem: Der Aufbau des Schlüssels, der zur Verschlüsselung der übertragenen Daten herangezogen wird, weist strukturelle Schwächen auf. So kann durch statistische Analysen des übertragenen Datenstromes dieser Schlüssel ermittelt werden. Einzige Voraussetzung ist, dass ausreichend Daten zur Analyse überragen werden.

Laut einigen Studien kann dies unter Umständen längere Zeit dauern. Aber angesichts der vorhandenen kriminellen Energie mancher Nutzer sollte dies nicht als beschwichtigendes Argument für den Einsatz von WEP herangezogen werden. Besonderes Gewicht bekommt ferner der Umstand, dass Tools im Internet erhältlich sind, die eine Entschlüsselung automatisiert vornehmem. Niemand muss sich heutzutage noch in die Spezifikationen und Publikationen hineinlesen, um diese Schwäche auszunutzen: Ein einfacher Doppelklick auf die Hacker-Anwendung und genügend Zeit reichen aus. Als Konsequenz aus diesem Umstand bleibt nur die Erkenntnis, dass weiter reichende Technologien verwendet werden müssen, um ein WLAN sicher zu betreiben.

Das Konzept des Instituts für Telematik zur Einführung des WLAN sieht eine Trennung von Internet, Intranet und WLAN-Netz durch eine Firewall vor (Abbildung 1). Um den Datenverkehr zwischen der Funk-Karte und Basisstation sicher zu machen, wird ein VPN-Tunnel (Virtual Private Network) zwischen dem WLAN-Gerät und der Firewall aufgebaut.

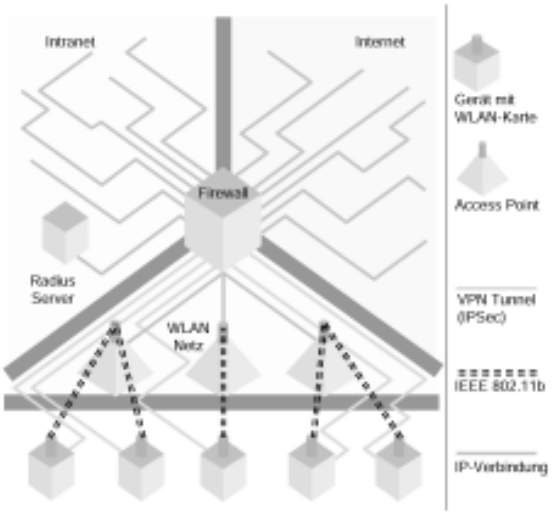



Abb.1: Trennung von Internet, Intranet und WLAN-Netz über eine Firewall

Virtual Private Networks werden verwendet, um in öffentlichen und nicht vertrauenswürdigen Netzen einen sicheren „Tunnel" zwischen zwei Kommunikationspartnern aufzubauen. Die Verschlüsselung, auf die VPN's aufbauen (z.B. IPsec) garantiert, dass kein anderer Teilnehmer des öffentlichen Netzes den Datenstrom zwischen den beiden Kommunikationspartnern entschlüsseln kann.

Der Zugang zu den Basisstationen ist im Allgemeinen nicht gesichert. Eine fremde Person kann also zunächst versuchen, eine Verbindung zwischen seinem Rechner und der Basisstation herzustellen, um dann von dort aus in das Netz einzudringen. Auf den Basisstationen können Listen gepflegt werden, die den Zugang zu der Basis-

station regeln. Dieses Feature ist vielerorts ausgeschaltet, aber selbst in eingeschaltetem Zustand nicht wirklich ein Hindernis, weil ein gültiger Listeneintrag durch Mithören des Datenstromes von autorisierten Teilnehmern ermittelt werden kann.

Schwieriger wird es, wenn Radius-Server im Spiel sind. Hier wird der Zugang zur Basisstation erst dann zugelassen, wenn vorher eine Authentifikation am Radius-Server stattgefunden hat. Hierzu müssen die Basisstationen das EAP (Extensible Authentication Protocol) oder LEAP (Lightweight Extensible Authentication Protocol) implementiert haben. Durch die Verwendung dieses Verfahrens ist es prinzipiell auch möglich, die Sicherheit des WEP-Protokolles zu erhöhen, da der WEP-Schlüssel bei jeder Anmeldung neu ausgehandelt wird. Damit wird das Risiko minimiert, eine so große Menge an Daten zu übertragen, dass eine Ermittlung des Schlüssels möglich ist. Voraussetzung ist allerdings, dass die Verbindung nicht permanent besteht.

Die Umsetzung der beschriebenen Konzeption (VPN, Firewall, Radius-Server) weist in der Praxis einige Probleme auf, da der Radius-Server sinnvollerweise im Intranet aufgestellt ist. Die Authentifikation erfolgt also vor der Etablierung des VPN-Tunnels zwischen PC und Firewall. Dies bedeutet, dass die Firewall Kommunikation zwischen den Basisstationen und dem Radius-Server zunächst zulassen muss, später aber nur diejenige Kommunikation erlauben darf, die zuvor über VPN übertragen wurde. Hier ist die Reihenfolge der eingesetzten Technologien, die nicht notwendigerweise vom gleichen Hersteller geliefert werden, entscheidend.

Zusätzlich möchte man den Anwender auch davor bewahren, zu viele Passworte anzugeben. Die Authentifizierung am Radius-Server sollte deshalb gleichzeitig mit der Anmeldung am Windows-Netzwerk im Intranet sowie mit dem Aufbau des VPN-Tunnels erfolgen.

Bei WLAN ergibt sich dabei ein weiteres Randproblem. Der Anwender kann sich möglicherweise in Bewegung befinden und aus dem Empfangsbereich einer Basis-Station in den Empfangsbereich einer anderen Basisstation gelangen (Abb. 2). Hier muss garantiert werden, dass der VPN-Tunnel über die neue Basisstation zur Firewall nicht „abreißt“ und die Kommunikation aufrecht erhalten wird. Dieses Verfahren ist unter dem Begriff „Roaming“ auch bei Handys bekannt.

Die Praxis hat gezeigt, dass eine Umsetzung des beschriebenen Konzeptes möglich ist. Allerdings sollte nicht verschwiegen werden, dass damit Randbedingungen an die verwendete Hardware und die verwendeten Betriebssysteme gestellt werden. Natürlich ist die Konzeption zunächst betriebssystemneutral, jedoch sind die Erfahrungen, die mit der Umsetzung mit einem bestimmten Betriebssystem gewonnen wurden, teilweise für andere Betriebssysteme ohne Nutzen. Dies betrifft vor allem den Bereich der Benutzer-Authentifikation. Ebenso sind Tools zum Management in verschiedenen Betriebssystem-Implementationen nicht notwendigerweise gleich. Allerdings hilft die Erkenntnis über die Zusammenhänge der beteiligten Komponenten bei der Umsetzung für andere Betriebssysteme ungemein.

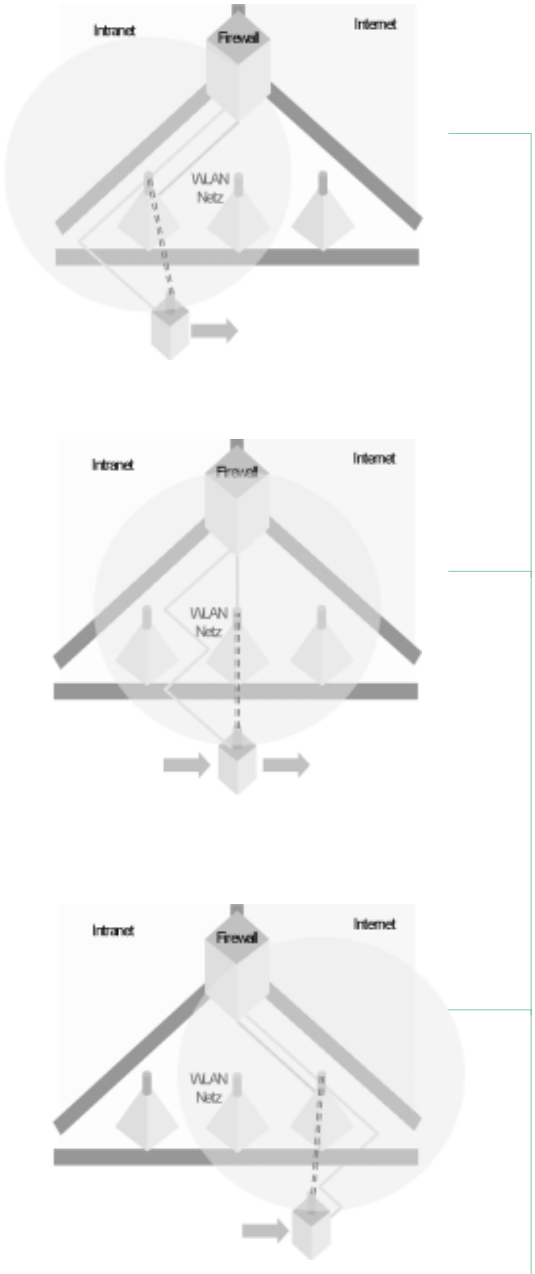



Abb. 2: Roaming im WLAN

# Dissertationen

In den Jahren 2001 und 2002 wurden drei Dissertationen von Instituts-Mitarbeitern verteidigt (Ernst-Georg Haffner, Harald Sack, Andreas Heuer). Im Folgenden werden diese Doktorarbeiten kurz erläutert. Sie können alle auf der Instituts-Website im Volltext als pdf-Dokument herunter geladen werden.

## Ernst-Georg Haffner: Request Prediction and Hyperlink Proposals – Methodologies and Mathematics behind Web Applications

*Seit der Einführung des World Wide Web (www) im Internet wächst die Nutzung des Internet in atemberaubenden Maße. Das lässt auch den Bedarf an effizienten Anwendungen steigen. Einerseits wird die Verkürzung von Antwortzeiten gewünscht, andererseits die automatische Generierung von Vorschlägen, wie man mit "Hyperlinks" Verbindungen zu anderen Webseiten schaffen kann. Auf den ersten Blick scheinen diese beiden Anwendungen kaum Gemeinsamkeiten aufzuweisen, doch in seiner Dissertation weist Ernst-Georg Haffner nach, dass mittels ähnlicher mathematischer und methodologischer Strategien Lösungen für beide Probleme gefunden werden können. Ferner werden Wege aufgezeigt, wie mögliche Synergie-Effekte genutzt werden können.*

*Since the introduction of the World Wide Web service the use of the "net of all nets" has been increasing to a breathtaking level. Consequently, there has been an increasing demand for efficient applications. On one hand, there is a request for shorter and shorter response times, and on the other, for an automatic generation of proposals addressing the issue of methods of connecting to other websites via hyperlinks. At first glance, it seems that the two applications have nothing in common, but Ernst-Georg Haffner shows in his dissertation that by similar mathematic and methodological strategies it is possible to find solutions to both problems. Methods of the use of possible synergy effects will be shown in the future.*

Im Rahmen seiner Dissertation entwickelt und beschreibt der Wissenschaftler eine mathematische Methode, mit der die bevorstehende Nutzung von Internet-Seiten vorherzusagen ist. Dadurch können Wartezeiten beim Aufruf von Inhalten im weltweiten Computernetz erheblich vermindert werden.

Auf Basis der mathematisch berechneten Nutzungswahrscheinlichkeit werden Server im Internet künftig in der Lage sein, aufwendige Rechenoperationen und Datenübermittlung bereits vorzunehmen, bevor der Anwender überhaupt die Seiten abruft. Der einzelne Internet-Nutzer hat dann den Vorteil kürzerer Antwortzeiten, ohne dass andere Teilnehmer gleichzeitig Leistungseinbußen hinnehmen müssten. Ferner ist es möglich, dass ein Computer bestimmte Daten schon abfragt, bevor der Anwender mit seiner eigentlichen Internet-Sitzung beginnt.

Das Modell von Ernst-Georg Haffner bezieht in die Vorausberechnung der Internet-Nutzung unter anderem Zufälligkeits-Faktoren, mittlere Anforderungshäufigkeiten, Umfang und Anteil von teilweise vorhersagbaren Elementen einer Benutzersitzung sowie Kostenaspekte ein. Auch der Zeitablauf und das Altern von Datensätzen gehen in das Verfahren zur Prognose des Abrufs von Internet-Inhalten ein.

Ernst-Georg Haffner fand zudem heraus, dass die „Request Prediction" mathematisch und methodisch erstaunliche Gemeinsamkeiten hat mit der automatischen Erzeugung von Vorschlägen zur sogenannten „Verlinkung" von Internet-Inhalten durch Redaktionssysteme. Der Wissenschaftler entwickelte sein Hyperlink-Proposal-Modul auf der methodischen Basis des sogenannten "fallbasierten Schließens".

Die Dissertation von Ernst-Georg Haffner kann auf der Website des Instituts für Telematik unter der Adresse http://www.telematik-institut.de/publikationen/dissertationen/diss_haffner.html als pdf-Dokument heruntergeladen werden.

## Harald Sack: Improving the Power of Ordered Binary Decision Diagrams by Integrating Parity Nodes

*Sowohl die Zahl der eingesetzten Computersysteme wächst weltweit sehr stark, als auch die Komplexität der darin integrierten Schaltkreise. Die Industrie sieht sich gezwungen, in immer kürzerer Zeit immer leistungsfähigere und kleinere Mikrochips zu immer niedrigeren Kosten zu produzieren. Um bei diesem Produktivitätsdruck absolut korrekt arbeitende Prozessoren zu gewährleisten, braucht es Entwicklungs-Werkzeuge und -Methoden, die den Schaltkreisentwurf auf einer höheren Ebene der Abstraktion ermöglichen und die dazu notwendigen Arbeitsschritte auf den unteren Abstraktionsebenen weitgehend automatisieren. In seiner Dissertation definiert und beschreibt Harald Sack ein mathematisches Verfahren, mit dem Chiphersteller schon in der Entwicklungsphase von Mikroprozessoren und integrierten Schaltkreisen deren Fehlerfreiheit sicherstellen können. Dadurch lassen sich die mit Hardware-Fehlern gelegentlich verbunden hohen finanziellen Risiken ausschließen.*

*With the fast increasing number of computer systems set up throughout the world, integrated circuits have been growing more and more complex. The industry is forced to make microchips which must be ever more efficient, ever smaller in size, but made in shorter and shorter time and at a smaller and smaller cost. In order to ensure, in the above described circumstances of constant pressure on productivity, the absolutely correct operation of processors, it is necessary to provide development tools and methods ensuring the circuit design on a higher level of abstraction and a comprehensive automation of the necessary worksteps on the lower level of abstraction. In his dissertation, Harald Sack defines and describes a mathematical method enabling manufacturers of chips to ensure a perfect condition of microprocessors and integrated circuits even in their development stage. Thus, it is possible to eliminate high financial risks which occasionally occur due to a hardware failure.*

Für das Auffinden von Hardware-Designfehlern (*Verifikation*) war bislang die sogenannte *Simulation* die eingesetzte Methode der Wahl. Sie versuchte bei einem zu überprüfenden Schaltkreis, alle möglichen Eingabekombinationen hinsichtlich der von diesen berechneten Ausgaben zu testen. Heutige Schaltkreise sind aber von so hoher Komplexität, dass selbst alle Zeit der Welt nicht ausreichend wäre, um mit dieser Methode ein Endergebnis zu erzielen. Daher werden nicht alle möglichen Kombinationen überprüft, sondern es wird ein als signifikant angesehener Testzyklus festgelegt, nach dessen erfolgreichem Abschluss mit einer hohen Wahrscheinlichkeit von Korrektheit ausgegangen werden kann.

Seither ist die Kette aufgetretener Fehler in Mikroprozessoren nicht abgerissen. Doch nicht immer sind die Folgen so spektakulär wie damals. Zu praktisch allen aktuellen Prozessoren existieren Listen mit bekannten, aufgetretenen Fehlern, doch mindern diese die Einsatzfähigkeit der Chips nur in geringem Maße. Trotzdem ist es gerade bei sicherheitskritischen Anwendungen in Flug- oder Kraftfahrzeugen wichtig, Hardware-Fehler bereits möglichst früh im Designprozess zu erkennen. Hierfür ist das von Harald Sack entwickelte neue formale Verfahren zur Computer gestützten automatischen Schaltkreis-Überprüfung eine wichtige Voraussetzung. Es erweitert die bislang zur Computer unterstützten Darstellung der Funktionalität angewandte Datenstruktur der geordneten binären Entscheidungsdiagramme- OBDDs -, indem er deren Ausdrucksfähigkeit durch Hinzunahme sogenannter Parity-Operatoren stark erhöht. Harald Sack weist nach, dass die so entstandene Datenstruktur der Parity-OBDDs wesentlich leistungsfähiger ist als die bisher mit großem Erfolg eingesetzten binären Entscheidungsdiagramme. Darüber hinaus hat der Wissenschaftler ein sehr umfangreiches Softewarepaket entwickelt, mit dem Parity-OBDDs industriell zum Einsatz gebracht werden können.

Die Dissertation von Harald Sack kann auf der Website des Instituts für Telematik unter der Adresse http://www.telematik-institut.de/publikationen/dissertationen/diss_sack.html als pdf-Dokument heruntergeladen werden.

# Andreas Heuer: Web Präsenz Management im Unternehmen – Entwicklung und Einsatz eines Java-basierten Online-Redaktionssystems

*Das Publizieren von Dokumenten im World Wide Web (WWW) stellt in der Regel hohe Anforderungen an die informationstechnische Ausbildung derer, die mit dieser Aufgabe betraut sind. Verantwortlich für die Inhalte der Dokumente, das Layout und die Verknüpfungen in den Hypertexten sind üblicherweise die Spezialisten einer Web-Redaktion, aber nicht die Mitarbeiter, die über die höchste Kompetenz für die Inhalte verfügen. Dadurch entstehen häufig Engpässe bei der Einstellung von Dokumenten und Probleme mit deren Aktualisierung. Im Gegensatz dazu ermöglicht Ein von Andreas Heuer als Chefentwickler geschaffenes neues Redaktionssystem es nun auch Sachbearbeitern/Autoren, die keinerlei Fachkenntnisse für die Erstellung von Webseiten besitzen, direkt von ihrem Arbeitsplatz aus Dokumente für die Veröffentlichung im Internet zu erstellen. Das in der Dissertation von Andreas Heuer beschriebene System nennt sich jDAPHNE (Java Distributed Authoring and Publishing of Hypertext in a Network Environment).*

*Generally, WWW document publishing is very demanding when it comes to IT-related education of those entrusted with the task. Usually, it is a web editorial staff that is responsible for the document contents, layout and hypertext linking, but not the employees having a highest level of competence for the contents. Therefore, there are often bottlenecks while creating a document as well as problems with its updating and refreshing. Thanks to a new editing system, which was developed by the chief developer, Andreas Heuer, even specialist/authors without any expertise in website creation can now make documents to be published on the Internet, and they can do it directly at their desks. The system described in the dissertation written by Andreas Heuer is called JDAPHNE (Java Distributed Authoring and Publishing of Hypertext in a Network Environment).*

Das webbasierte System der neuesten Generation baut auf offenen Standards auf und ist unter allen gängigen Betriebssystemen und Umgebungen lauffähig, sofern ein JAVA-Engine und eine Datenbank vorhanden sind. jDAPHNE ermöglicht die Verwaltung der Web-site- Dokumente nach einem festzulegenden Workflow. Auf diese Weise werden die Mitarbeiter ihrem Fachgebiet entsprechend nur in einzelne Abschnitte des Publikationsvorgangs eingebunden. Mit jDAPHNE ist also eine wirkliche Arbeitsteilung auf dem Weg zur Web-Präsenz möglich.

Die Sachbearbeiter greifen über ihren gewohnten Webbrowser (z.B. Internet Explorer, Netscape Communicator) von ihrem Arbeitsplatzrechner aus auf das Content Management-System zu. Die Erstellung der Dokumente erfolgt dann jeweils mittels des vertrauten Editor-Programms, z.B. MS Word oder Star Writer. Die Dokumente durchlaufen, bevor sie im Internet sichtbar werden, einen zuvor festgelegten Workflow, welcher der inhaltlichen und technischen Qualitätssicherung dient. Er kann vom Administrator des Redaktionssystems vorab selbst konfiguriert und somit der gewünschten Kontrollstruktur im Unternehmen angepasst werden. Die Endkontrolle obliegt dem Webmaster. Nur wenn er ein Dokument als formal korrekt abzeichnet, wird es auf der Website veröffentlicht. jDAPHNE verwaltet den Inhalt und das Layout eines Dokumentes getrennt. Beide werden erst beim Export des Dokumentes in das Internet zu einer vollständigen Webseite zusammengefügt. Dabei ist es allen Beteiligten, vom Sachbearbeiter bis hin zum Webverantwortlichen, jederzeit möglich, sich die endgültige Internet-Ansicht eines Dokuments anzuschauen. Durch strikte Trennung von Inhalt und Layout stellt jDAPHNE die einheitliche Darstellung der Inhalte im Internet sicher. Dabei können einzelnen Teilbereichen der Internet-Präsenz verschiedene Layouts zugeordnet werden.

In jDAPHNE integriert ist eine Hyperlinkmanagement-Funktion, die nach fehlerhaften Querverweisen sucht und diese zur Korrektur vorschlägt. Solche Link-Konsistenz-Überwachungen werden

präventiv eingesetzt: Bevor ein Dokument aus der Web-Präsenz entfernt oder in seiner URL modifiziert wird, kann jDAPHNE alle durch diese Aktion betroffenen Dokumente filtern und modifizieren. Dadurch wird das Auftreten von Inkonsistenzen im Voraus vermieden und das Risiko „toter Links" bei der Pflege des Dokumentenbestands deutlich minimiert.

Die Dissertation von Andreas Heuer kann auf der Website des Instituts für Telematik unter der Adresse http://www.telematik-institut.de/publikationen/dissertationen/diss_heuer.html als pdf-Dokument heruntergeladen werden.

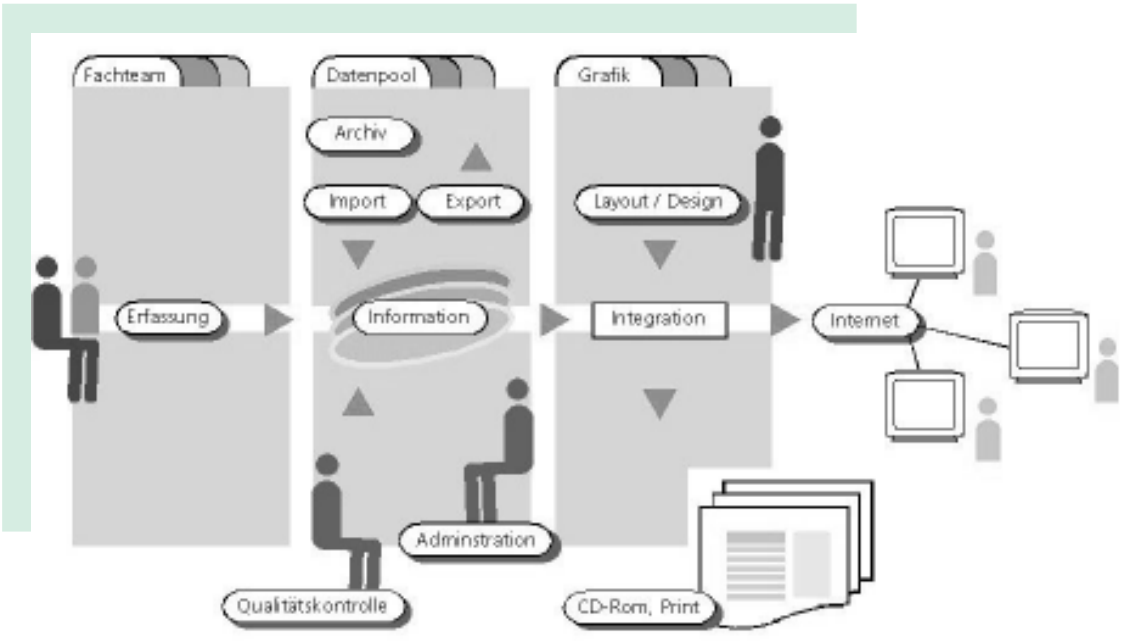




*Abb. 1:* Das Redaktionssystem JDaphne im Überblick, der qualitätsgesichterte Informationsfluss von der Erfassung der Informationen über ihre Verarbeitung, Veredlung bis zur Publikation in verschiedenen Pulikationsmedien.

# Trierer Symposien

Trierer Symposien

Regelmäßig veranstaltet das Institut für Telematik wissenschaftliche Symposien zu aktuellen Entwicklungen im Bereich der Telematik. Es will mit diesen Symposien ein Forum bieten, in dem Vertreter der Forschung und Entwicklung im Bereich der Informations- und Kommunikations-Technologien und Praktiker aus den Hochschulen und Bildungsinstitutionen gemeinsam über die Potentiale der modernen Informations- und Kommunikationstechnik diskutieren.

## Übersicht der Symposien seit Gründung des Instituts:

**Sichere Telemedizin**
14. und 15. November 2002

**Digitales Geld**
20. und 21. Juni 2002

**Digitale Signaturen**
15. und 16. November 2001

**Mobile Commerce**
07. und 08. Juni 2001

**Smart Cards**
23. und 24. November 2000

**Virtuelle Hochschule**
04. und 05. Mai 2000

**Televerwaltung**
11. und 12. November 1999

**Elektronisches Publizieren**
25. und 26. März 1999

**Telemedizin**
08. und 09. Oktober 1998

14.-15.11.2002
**Trierer Symposium**

## Sichere Telemedizin

Das 9. Trierer Symposium des Instituts für Telematik, dessen Schirmherrin Frau Malu Dreyer (Ministerin für Arbeit, Soziales, Familie und Gesundheit) war, beschäftigte sich mit dem Thema „Sichere Telemedizin". Es richtete sich an leitende Persönlichkeiten im Bereich Gesundheitswesen und bot ein Forum der Information nicht nur für Experten aus Medizin, Telekommunikation und Informatik, sondern auch für jeden, der ganz allgemein am elektronischen Austausch von Gesundheitsdaten über offene Netze interessiert war. Das Symposium gab Entscheidern aus Ärzte- und Apothekerschaft, Pflegeberufen, Rettungsdiensten, Verwaltungen, Krankenversicherungen, Interessensverbänden, Wirtschaft und Politik einen Einblick in neueste Erkenntnisse, einen Überblick über aktuelle Anwendungen und einen Ausblick auf künftige Entwicklungen.

Die Telemedizin, also der elektronische Austausch medizinischer Daten wie Bilder, Befunde und Messergebnisse über große Entfernungen hinweg, hat viele faszinierende Anwendungsmöglichkeiten. Sie überschreitet die Grenzen der herkömmlichen, meist papiergebundenen Kommunikationsabläufe und macht es dank des Internets zum Beispiel möglich, ungeachtet von Entfernungen schnell weitere Experten hinzuzuziehen, Untersuchungsdaten, Operationen und einzelne medizinische Bilder live zu übertragen sowie elektronische Patientenakten, Arztbriefe und Rezepte zu übermitteln.

Allerdings werden die Möglichkeiten der Telemedizin bisher nur in Ansätzen ausgeschöpft - meist in vereinzelten, über die gesamte Bundesrepublik verstreuten Pilotprojekten. Wie andere Mitgliedsstaaten der Europäischen Union sind wir noch weit entfernt von einem flächendeckenden Ausbau der telematischen Infrastruktur im Gesundheitswesen.

Das Symposium hatte die Programmschwerpunkte

- Austausch von Patientendaten
- Verwaltung medizinischer Daten
- Chipkarten für das Gesundheitswesen
- E-Health – Werkzeuge und Anwendungen

20.-21.06.2002
**Trierer Symposium**

## Digitales Geld

Das 8. Trierer Symposium des Instituts für Telematik beschäftigte sich mit dem Thema Bezahlvorgänge im Internet. Unter dem Motto „Digitales Geld" diskutierten Forscher und Entwickler aus dem Bereich der Informations- und Kommunikationstechnologien sowie Praktiker aus Wirtschaft, Verbänden und Institutionen kritisch über Chancen und Risiken elektronischer Zahlungsmechanismen, über die Einsatzmöglichkeiten der entsprechenden Technologien und über die gesellschaftlichen Rahmenbedingungen.

Der immer populärer werdende elektronische Handel von Waren und Dienstleistungen über das Internet sowie das ungebrochen wachsende Interesse am Online-Banking machen es notwendig, die Verfahren für die elektronische Abwicklung der Zahlungsvorgänge zu überprüfen und gegebenenfalls zu optimieren - unter wirtschaftlichen, ergonomischen und nicht zuletzt auch unter Sicherheitsgesichtspunkten. Eine besondere Herausforderung im E-Commerce stellen vor allem die Zahlungen zwischen Endkunden und Händlern dar, weil beim Online-Shopping oft noch keine etablierte Geschäftsbeziehung mit entsprechendem Vertrauensverhältnis existiert. Noch immer hat die Mehrheit der deutschen Internet-Käufer erhebliche Sicherheitsbedenken und will vor allem Daten von Kreditkarten und Bankkonten nicht dem World Wide Web anvertrauen.

„Revolution auf Raten". Mittlerweile existieren viele sehr unterschiedliche elektronische Bezahlverfahren. Hier umfassende Transparenz zu schaffen, die verschiedenen Methoden systematisch zu vergleichen, einen aktuellen Überblick über die tatsächliche Nutzung in der Praxis zu gewinnen und Prognosen für die zukünftige Entwicklung zu ermöglichen, war Ziel des Trierer Symposiums „Digitales Geld".

Das Symposium hatte die Programmschwerpunkte

- Sicherheit der Verfahren und Rechtsrahmen für Nutzer
- Perspektive der Finanzdienstleister
- Tendenzen und neue Entwicklungen

15.-16.11.2001
**Trier Symposium**

## Digitale Signaturen

Das 7. Trierer Symposium unter dem Titel „Digitale Signaturen“ bot ein Forum, in dem Vertreter der Forschung und Entwicklung im Bereich der Informations- und Kommunikationstechnologien, sowie Praktiker aus Wirtschaft und Verwaltung gemeinsam über die Chancen und Risiken des digitalen Unterschreibens von elektronischen Daten, die Einsatzmöglichkeiten der Technologien und die Randbedingungen kritisch diskutierten.

Aufgrund der wachsenden Bedeutung der elektronischen Kommunikation tritt die Problematik der heute noch recht mangelhaften Absicherung deutlich zutage. Eine Sicherung des Datenaustauschs muss vielschichtig sein: die Identität der Kommunikationspartner muss eindeutig feststellbar sein, es muss sichergestellt sein, dass jede während der Übermittlung unbefugte Veränderung der Daten bemerkt wird, und gegebenenfalls müssen Daten „gerichtsfest“ sein.

Die Entwicklung der Digitalen Signatur ist dabei die vielversprechendste Antwort auf die gestiegenen Sicherheitsanforderungen der netzgestützten Kommunikation. Als elektronisches Gegenstück zur Handunterschrift ist sie heute weltweit auch von den Gesetzgebern weitestgehend anerkannt. Sie stellt die verlässlichste Methode zur Sicherung der elektronischen Kommunikation dar.

Das Prinzip der Digitalen Signaturen ist dabei allgemein anerkannt - die Umsetzung ihres Einsatzes erweist sich in vielen Gebieten jedoch als problematisch.

Derzeit sind die meisten Methoden proprietär, d.h. in vielen Fällen können digitale Signaturen, die mit Hilfe eines bestimmten Anbieters erstellt worden sind, nicht mit der Software und Hardware eines anderen Anbieters überprüft werden. Diese Lücke muss kurzfristig geschlossen werden.

Das Symposium hatte die Programmschwerpunkte

- Technologie und Infrastrukturen
- Digitale Signaturen und E-Commerce
- Digitale Signaturen und öffentliche Verwaltung
- Zukunftserwartungen und -entwicklungen

07.-08.06.2001
**Trierer Symposium**

## Mobile Commerce

Das Institut für Telematik lud beim Trierer Symposium „Mobile Commerce“ Vertreter der Forschung und Entwicklung im Bereich der Informations- und Kommunikationstechnologien und Praktiker aus Wirtschaft und Verwaltung ein, gemeinsam über die Potentiale der modernen Informations- und Kommunikationstechnik im Bereich der mobilen Anwendungen, ihren Ausprägungen und deren Randbedingungen bezüglich der Sicherheit zu diskutieren.

Am Anfang dieses Jahrhunderts verschmelzen Wirtschaft und digitale Technik, unsere heutige Gesellschaft wird zur Informationsgesellschaft. Durch diese Fusion sind Informationen zum Produktionsmittel geworden. Es sind zahlreiche Formen von elektronischen Diensten entstanden. E-Commerce, E-Business, E-Goverment etc. sind die ersten Anwendungsgebiete der neuen Entwicklungen.

Das Internet mit seinen Daten und der Mobilfunk überschneiden sich heute in revolutionärem Maße. Dadurch bewegt sich die Sprachkommunikation auf das Netz zu und erlaubt eine drahtlose, internetbasierte Datenkommunikation für den Massenmarkt.

Der Mobile Commerce will nützliche Informationen zu jeder Zeit an jedem Ort bereit stellen. Aber es gibt auch weitere Anforderungen. Eine davon ist die Sicherheit.

Mit der Weiterentwicklung und der wachsenden Kompliziertheit der Anwendungen entsteht eine zunehmende Bedrohung hinsichtlich der Sicherheit dieser Verfahren. Gleichzeitig versprechen jedoch neuartige Technologien unterschiedliche Sicherheitslösungen, um mit der Bedrohung fertig zu werden und die resultierenden Probleme zu überwinden.

Das Symposium hatte die Programmschwerpunkte

- Sicherheitsaspekte der mobilen Anwendungen
- Enabling-Technologien
- Einsatz von mobilen Agenten für die Automatisierung und Personalisierung der mobilen Anwendungen
- Künftige Entwicklungen

23.-24.11. 2000
**Trierer Symposium**

## Smart Cards

Das Institut für Telematik wollte mit dem 5. Trierer Symposium, diesmal zum Thema „Smart Cards" (Intelligente Chipkarten), ein Forum bieten, in dem Vertreter der Forschung und Entwicklung im Bereich der Informations- und Kommunikationstechnologien und Praktiker aus Wirtschaft und Verwaltung gemeinsam über die Potenziale der modernen Informations- und Kommunikationstechnik im Bereich der intelligenten Chipkarten und deren Einsatzfelder diskutieren konnten.

Während die bislang vorherrschenden Magnetstreifenkarten und „einfachen" Chipkarten lediglich dem Speichern von Informationen dienen, ermöglichen die intelligenten („smart") Chipkarten die Durchführung von Rechenoperationen und damit von komplexen Anwendungen direkt auf der Karte. Die daraus folgenden Einsatzmöglichkeiten werden derzeit entwickelt und getestet und zeigen die ersten Erfolge. Die durch die innovative und expandierende Forschung vorangetriebene Technik wird zur zukünftigen Verbreitung der Smart Cards mit ihren vielfältigen Verwendungsmöglichkeiten beitragen und mittelfristig die Magnetstreifenkarten ablösen.

Durch die Vorstellung von konkreten Projekten, die ihren Forschungsschwerpunkt auf verschiedene Aspekte dieser Thematik gelegt hatten, wurde im Trierer Symposium ein konstruktiver Austausch der Erfahrungen ermöglicht. Neben der sich an die Vorträge anschließenden Gelegenheit zur Diskussion wurde auch bei einem gemeinsamen Abendessen ausführlich Gelegenheit zum informellen Austausch gegeben.

Das Symposium hatte die Programmschwerpunkte

- Aufbau und Wirkungsweise von Smart Cards
- Karten im Gesundheitswesen
- Bürger- und Kundenkarte
- Mobilität durch Smart Cards
- Künftige Entwicklungen

04.-05.05.2000
**Trierer Symposium**

## Virtuelle Hochschule

Das Institut für Telematik wollte mit dem Symposium „Virtuelle Hochschule" ein Forum bieten, in dem Vertreter der Forschung und Entwicklung im Bereich der Informations- und Kommunikationstechnologien und Praktiker aus den Hochschulen und Bildungsinstitutionen gemeinsam über die Potenziale der modernen Informations- und Kommunikationstechnik im Bereich der Aus- und Weiterbildung an Hochschulen und ihrem Umfeld diskutieren konnten.

Die Einbeziehung multimedialer Informations- und Kommunikationstechnologien in bestehende oder neue Ansätze zur Vermittlung von Wissen und als Ergänzung zu klassischen Unterrichtsformen ist ein vieldiskutiertes Thema. Das Symposium sollte die Chance bieten, einen Erfahrungsaustausch in Gang zu setzen, der sowohl die zugrundeliegenden Techniken und die multimediale Aufbereitung von Materialien thematisierte, als auch notwendige neue Organisationsformen und –modelle konkretisierte.

Gerade die globale Verfügbarkeit entsprechend aufbereiteter Materialien und das einerseits daraus erwachsende Szenarium des weltweiten Wettbewerbs der Bildungseinrichtungen, und andererseits der unübersichtlich vielfältigen Auswahl für den Lernenden, stellen ein Spannungsfeld dar, das die Chancen und Risiken dieser Entwicklung durchaus andeutet.

Das Symposium hatte die Programmschwerpunkte

- Lebenslanges Lernen
- Virtueller Campus
- Virtueller Hörsaal
- Digitale Bibliothek

11.-12.11.1999
**Trierer Symposium**

## Televerwaltung

Das Institut für Telematik bot mit dem Trierer Symposium Televerwaltung ein Forum, in dem Vertreter aus Forschung und Entwicklung mit Praktikern aus Politik und Verwaltung über die Potenziale der neuen Informations- und Kommunikationstechnologien im Bereich der Verwaltung diskutieren konnten. Neben wissenschaftlichen Untersuchungen und technischen Entwicklungen sollten konkrete aktuelle Projekte in der Verwaltung vorgestellt werden.

Das Symposium am 11. und 12. November '99 hatte die Schwerpunkte Telematiksysteme und Netzinfrastrukturen für Televerwaltung, Aspekte der Sicherheit in offenen Netzen, Projekte der Televerwaltung und Rationalisierungseffekte und Qualitätsverbesserung durch Televerwaltung. Zu allen Programmschwerpunkten wurden führende Experten als Referenten eingeladen.

Auf dem Weg in die Informations- und Wissensgesellschaft hat die Modernisierung der öffentlichen Verwaltung und der Verwaltung von Unternehmen einen besonderen Stellenwert. Anwendungsgebiete sind beispielsweise die elektronische Akteneinsicht, das elektronische Wählen, die elektronische Unterstützung von Beschaffungsvorgängen, die elektronische Antragsbearbeitung und die Telearbeit zur Flexibilisierung von Arbeitsprozessen.

Die Programmschwerpunkte waren

- Projekte und Vorhaben I
- Karten und Trustcenter
- Konzepte
- Organisierte Sicherheit
- Telearbeit
- Projekte und Vorhaben II

25.-26.03.1999
**Trierer Symposium**

## Elektronisches Publizieren

Das Institut für Telematik hatte mit dem "Trierer Symposium für Elektronisches Publizieren" ein Forum geschaffen, in dem Vertreter der Forschung und Entwicklung im Bereich des Elektronischen Publizierens und Praktiker aus Verlagswesen und Wirtschaft gemeinsam über die Potentiale der modernen Informations- und Kommunikationstechnik im Bereich des Elektronischen Publizierens diskutieren konnten.

Ziel des am 25. und 26. März '99 veranstalteten Symposiums war es, Entscheidungsträger aus den Medien, dem Bibliothekswesen und der universitären Forschung sowie Experten aus dem Bereich der Technik zusammenzubringen, um die Potenziale der neuen Informations- und Kommunikationstechnik für die Anwendung im Bereich des Publizierens zu diskutieren. Dabei sollten auch Probleme im Bereich der Erstellung und der Verbreitung von Publikationen sowie deren organisatorische, rechtliche wie auch betriebswirtschaftliche Eigenheiten erörtert werden.

Zahlreiche Referenten aus Forschung und Entwicklung sowie Praktiker aus Politik und Verwaltung analysierten die Potenziale, Einsatzmöglichkeiten und technischen Voraussetzungen des Elektronischen Publizierens:

Die Programmschwerpunkte waren

- Bibliotheken
- Verlagswesen
- Retrodigitalisierung
- Geschäftsmodelle

**08.-09.10.1998**
**Trierer Symposium**

# Telemedizin

Das Institut für Telematik richtete am 8. und 9. Oktober das „Trierer Symposium" mit dem Thema „Internet-Technologie in der Medizin" aus. Mit dieser Veranstaltung schuf das Institut ein Forum, das Vertreter aus Forschung und Entwicklung und medizinische Praktiker nutzten, um sich über aktuelle Entwicklungen zu informieren und diese miteinander zu diskutieren.

Der Schwerpunkt des Symposiums lag auf der Bedeutung der Internet-Technologie für die Telemedizin. Dabei sollten auch die Risiken und Sicherheitsbedenken im Zusammenhang mit der Vernetzung medizinischer Institutionen diskutiert werden. Die große Zahl der Teilnehmer - 60 Personen aus allen Teilen Deutschlands, aus Luxemburg und den Niederlanden waren angereist - und die angeregten Diskussionen nach den Vorträgen und in den Pausen zeigten, daß dieses Ziel voll und ganz erreicht wurde.

Ein Dutzend Gastreferenten aus Forschung und Entwicklung sowie Praktiker aus Politik und Verwaltung diskutierten über den aktuellen Stand und denkbare zukünftige Einsatzmöglichkeiten der Telemedizin und deren Umsetzung.

Die Programmschwerpunkte waren

- Informationssysteme im Krankenhaus
- Sicherer Datenaustausch im Gesundheitswesen
- Wissensbasierte Systeme

# Messeauftritte

## Arab Health

Das Institut für Telematik in Trier stellt sich mit Forschungs- und Entwicklungsbeiträgen den Herausforderungen des Wandels von der Industrie- zur Wissensgesellschaft und will im Rahmen konkreter praktischer Projekte deren visionäre Ziele verwirklichen helfen. Das Spektrum der Institutstätigkeit reicht dabei von der anwendungsorientierten Grundlagenforschung in Informatik und Telekommunikation bis zur Entwicklung maßgeschneiderter Problemlösungen für Handel, Banken, Industrie, Medizin und Verwaltung.

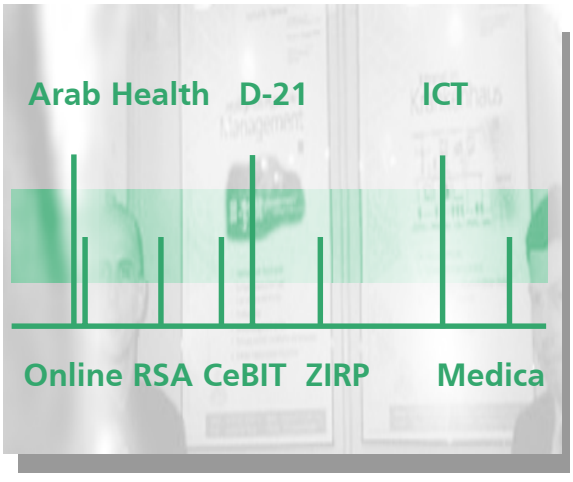
Das Institut für Telematik ist im Jahre 2002 auf verschiedenen Messen als Aussteller in Erscheinung getreten. Es gelang, für innovative Produkte Aufmerksamkeit zu wecken und Anwender und Firmen über die Potenziale der Exponate detailliert zu informieren.

Die Messeaktivitäten haben sich - für die Besucher und Interessierten und für uns gleichermaßen - vollauf gelohnt. Wir stellen jeweils kurz die verschiedenen Exponate vor.

Das Institut präsentierte vom 26. bis 29. Januar auf der Gesundheitsfachmesse „Arab Health 2002“ im World Trade Center von Dubai, der Hauptstadt der Vereinigten Arabischen Emirate, seine jüngsten Entwicklungen im Bereich der Telemedizin.

### DICOM Zip

Das Bildkomprimierungsverfahren DICOM Zip senkt die Übertragungszeit von medizinischen Bildern von mehreren Stunden auf wenige Minuten - wichtig vor allem in der Notfallmedizin. Trotz starker Bildkompression ist kein Verlust an Informationen sichtbar. Das Originalbild wird in zwei Bilder mit unterschiedlichen Bit-Ebenen zerlegt. Das eine Bild enthält relevante Informationen, die mit einem kleinen Kompressionsfaktor als GIF-Datei komprimiert werden. Das andere Bild mit für die Diagnose unbedeutenden Informationen wird dagegen sehr stark komprimiert im JPEG-Format. Die Zusammenführung zu einer Datei mit sämtlichen Bildinformationen macht dann die sekundenschnelle Komprimierung der Bilddokumente möglich.




## D-21 Jahreskongress

In Leipzig fand am 28. Juni der Jahreskongress der D-21-Initiative statt. Das Institut war mit folgenden Exponaten vertreten:

### Lock-Keeper

Siehe RSA 2002

### Zeitstempeldienst

Siehe CeBIT 2002

## RSA 2002

Vom 19. bis 21. Februar fand in San José die weltweit bedeutendste e-Security-Konferenz und Messe statt. Das Institut war mit folgendem Exponat vertreten.

### Lock-Keeper

Der Lock-Keeper ist eine patentierte Hardware-Lösung zum Schutz gegen Online-Hacker. Wenn die Sicherheitsansprüche eines Unternehmens zum Austausch von Daten über das Internet die Möglichkeit klassischer Firewalls übersteigen, empfiehlt sich der Einsatz des Lock-Keepers, der mit geringem Konfigurationsaufwand höchste Sicherheitsvorgaben erfüllt. Seine Funktionsweise entspricht dabei dem Passieren einer Schleuse: Zu keinem Zeitpunkt besteht eine direkte Verbindung zwischen Intranet und Internet, sondern je nach Zustand der „Schleusentore" findet der Informationsaustausch nur jeweils mit einem der Kommunikationsteilnehmer statt.

## Online 2002

In Düsseldorf fand vom 28 - 31. Januar die Online 2002 statt. Das Institut war mit folgenden Themen verteten:

### Lock-Keeper

siehe RSA 2002

### Palm-Fahrtenbuch

siehe CeBIT 2002

### Zeitstempeldienst

siehe CeBIT 2002

## CeBIT 2002

In Hannover fand vom 13. bis 20. März die CeBIT statt. Das Institut war mit folgenden Exponaten vertreten:

### Lock-Keeper

Siehe RSA 2002

### Smart Data Server

Die Integrationsplattform für heterogene Informationstechnologie-Strukturen kann in Unternehmen und Behörden als besonders leistungsfähiger Vermittler zwischen Informations-Anbietern und -Nutzern dienen, der bei Infrastrukturänderungen ansonsten fällige Neuprogrammierungen überflüssig macht. Der Smart Data Server weist eine besondere Kompaktheit und Anpassungsfähigkeit im Vergleich zu anderen Middleware-Lösungen auf. Der modular aufgebaute SDS arbeitet sehr schnell und hat eine höhere Performance.

### Palm-Fahrtenbuch

Exemplarisch für den Palm wurde ein mit Daten aus dem Global Positioning-System GPS arbeitendes Programm entwickelt. Es ermittelt die meisten Daten einer Autofahrt automatisch. Umständliche und zeitraubende manuelle Eingaben entfallen. Die Daten können problemlos auf Computer überspielt und von dort zur Vorlage beim Finanzamt ausgedruckt werden.

### Zeitstempeldienst

Elektronischer Nachfolger des klassischen Post-Eingangsstempels im Büro. Er bestätigt beim Dokumentenaustausch übers Internet verlässlich, dass zum Beispiel ein Vertrag, eine Steuererklärung oder eine Ausschreibungsunterlage zu einem bestimmten Zeitpunkt so und nicht anders vorgelegen haben. Der digitale Zeitstempel ist auch für die fristgerechte Online-Übermittlung von Dokumenten an Gerichte oder Hochschulen wichtig.

### Dicom Zip

Siehe Arab Health

## Telemedicine & Telecare 2002

In Luxemburg trat das Institut für Telematik auf der Fachmesse Telemedicine & Telecare 2002 vom 10. bis 12. April mit diesen Exponaten auf:

**DICOM Zip**
siehe Arab Health

**Patienten-CD-System**
Das System ermöglicht es, digitale medizinische Bilder innerhalb kürzester Zeit auf eine CD zu brennen und sie dem Patienten mitzugeben. Es handelt sich um einen handelsüblichen CD-Rohling, auf dem nicht nur die während einer ärztlichen Untersuchung gewonnenen Aufnahmen im international spezifizierten DICOM 3-Format, sondern auch ein leistungsfähiger Viewer zum Betrachten der Bilder gespeichert werden. Das Patienten-CD-System kann auch zur Erstellung einer mobilen, übertragbaren medizinischen Patientenakte in der Radiologie verwendet werden.

## ZIRP- 'Wirtschaft und Hochschule'

In Trier fand am 28.Mai die Veranstaltung Zukunftsinitiative Rheinland-Pfalz (ZIRP) im Bildungszentrum der Handwerkskammer Trier statt. Das Institut beteiligte sich an dieser Veranstaltung mit folgenden Exponaten:

**Zeitstempeldienst**
siehe CeBIT 2002

**Lock-Keeper**
Siehe RSA 2002

## ICT Regensburg

Auf der „International Conference on Telemedicine" vom 22. bis 25. September in Regensburg war das Institut für Telematik mit folgenden Exponaten vertreten:

**3D-Generator**
Optimiert z.B. die Diagnosemöglichkeit von Verletzungen oder Erkrankungen im Bereich der Zahnwurzeln. Dabei transformiert die Software die 2D-Röntgenbilder der hufeisenförmigen Struktur des Kiefers in ein dreidimensionales Objekt. Das 3D-Objekt kann als Serie zweidimensionaler DICOM-Bilder gespeichert werden. Für die Orientierung bei der Spezifikation einer Schnittebene wird ein transparenter Würfel mit der Schnittebene visualisiert. Die Schnittebene kann durch Parameter angepasst werden. Mit Hilfe der Schnittebene ist es möglich, durch das Innere des Objektes zu „wandern". Das Objekt kann zusätzlich frei rotiert werden.

**DICOM Zip**
Siehe Arab Health

**Patienten-CD**
Siehe Arab Health

## Medica 2002

An der Medica 2002, die vom 20. bis 23. November in Düsseldorf stattfand, beteiligte sich das Institut für Telematik mit diesen Exponaten:

### 3D-Generator

siehe ICT Regensburg

### DICOM Management Suite

Die DICOM Management Suite besteht aus einem modular aufgebauten, leistungsfähigen Archivierungs- und Bildverwaltungssystem. Die Software hat folgende Komponenten:

**DICOM View** – ein leistungsfähiger JAVA-basierter DICOM-Viewer
**DICOM Disk** – das Archivierungssystem für medizinische Bilder
**DICOM Mail** – sicherer Versand von einzelnen Bildern bzw. ganzen Bildserien
**DICOM Zip** – patentiertes Verfahren zur verlustfreien Hochleistungskompression von DICOM-Bildern
**DICOM Beam** – Präsentations- und Schulungssystem für die Besprechung von Untersuchungsergebnissen
**DICOM Send** – Versand von DICOM-Bildern über das DICOM-Protokoll
**DICOM Repair** – Tool zur Behebung von Problemen beim Öffnen von DICOM-Dateien
**DICOM Print** – Client-Server zur Ausgabe von Bildern auf DICOM-Druckern
**DICOM Edit** – Editieren von DICOM-Dateien
**DICOM Base** – Objektorientierte Datenbank

### Patienten-CD

siehe Arab Health

# Publikationen & Vorträge

Mitarbeiter des Instituts für Telematik traten 2002 mit zahlreichen Publikationen und Vorträgen an die Öffentlichkeit. Das Institut nutzte neben diversen hochrangigen Publikationsmedien auch die Möglichkeit, mittels selbst herausgegebener und sowohl in Papierform als auch über das WWW zur Verfügung gestellter Preprints über wichtige Vorarbeiten zu informieren. Zu erwähnen sind auch die der Öffentlichkeit zugänglichen Kolloquiumsvorträge, die regelmäßig im Institut für Telematik stattfinden.

## Publikationen 2002

### Veröffentlichungen in Tagungsbänden

Mitarbeiter des Instituts für Telematik haben im Jahre 2002 mit Vorträgen zu verschiedenen Themen an internationalen Konferenzen, Symposien und Workshops teilgenommen. Das Institut war unter anderem auf folgenden Veranstaltungen aktiv vertreten:

- WSEAS Intern. Conf. on Multimedia, Internert and Video Technologies, Skiathos (Greece)
- Medical Imaging 2002, San Diego (USA)
- IMSA 2002, Honolulu (USA)
- ICDIA 2002, Shanghai (China)
- EuroPACS 2002 , Oulu (Finnland)
- WWW2002, Honolulu (USA)
- IADIS Intern. Conf. on WWW/Internet Lissabon (Portugal)
- SIGUCCS 2002, Providence (USA)
- SCI 2002, Orlando (USA)
- JCIS 2002, Durham (USA)
- IMAGE 2002, Brisbane (Australia)

### Titel der Konferenzbeiträge

W. Huang, U. Roth, Ch. Meinel
*Improvement to the Smart Data Server with SOAP*
*Proc. of the 2nd WSEAS International Conference on MULTIMEDIA, INTERNET and VIDEO TECHNOLOGIES, WSEAS ICOMIV 2002*, Skiathos (Greece), 2002, pp.107-111

L. Vorwerk, Ch. Meinel
*A Practical Approach to Store DICOM-conform Presentations of Radiological Images*
*Proc. PACS Design and Evaluation: Engineering and Clinical Issues vol. 4685, Medical Imaging 2002*, San Diego (USA), 2002, pp. 299-306

L. Vorwerk, C.Jiang, Ch. Meinel
*Application for repairing and presenting DICOM objects, Internet and Multimedia Systems and Applications*
*Proc. IMSA 2002*, Hawaii (USA), 2002, pp. 318-323

C. Jiang, L. Vorwerk, Ch. Meinel
*Deformation and Construction of 3D Medical Image*
*Proc. ICDIA 2002*, Shanghai (China), 2002, pp.48-53

L. Vorwerk, C. Jiang, Ch. Meinel
*Security Requirements for Telemedical Applications regarding DICOM-image-management in a PACS*
*Proc. Europacs 2002*, Oulu (Finnland), 2002, pp.66-69

C. Jiang, L. Vorwerk, Ch. Meinel
*Standardizing DICOM File and Rendering 3D Medical Image*
*Proc. Europacs 2002*, Oulu (Finnland), 2002, pp.225

L. Vorwerk, C. Jiang, Ch. Meinel
*Secure Transfer of Digital Images and Related Data*
*Proc. WWW2002*, Honolulu (Hawaii, USA), 2002, pp. k.A.

U. Roth, E.-G. Haffner, Ch. Meinel
*The Internal Workflow of the Smart Data Server*
*Proc. IADIS International Conference WWW/Internet 2002*, Lisbon (Portugal), 2002, pp. 572-576

V. Schillings, Ch. Meinel
*tele-TASK - Teleteaching Anywhere Solution Kit*
Proc. SIGUCCS 2002, Providence (Rhode Island, USA), 2002, pp. 130-133

Ch. Meinel, H. Sack, V. Schillings
*Course Management in the Twinkle of an Eye*
Proc. SIGUCCS 2002, Providence (Rhode Island, USA), 2002, pp. 281-283

M. Ma, Ch. Meinel
*A Proposal for Trust Model: Independent Trust Intermediary Service (ITIS)*
Proc. IADIS 2002, Lisbon (Portugal), 2002, pp. 785-790

L. Gollan, Ch. Meinel
*Digital Signatures for Automobiles?!*
Proc. SCI 2002, Orlando, (Florida, USA), 2002, pp. 225-230

E.-G. Haffner, U. Roth, Ch. Meinel
*A Hyperlink-Proposal Mechanism to Exemplify Cognitive Algorithms for Web-Applications*
Proc. JCIS 2002, Durham, (North Carolina, USA), 2002, pp. 517-520

L. Vorwerk, Ch. Meinel
*DICOM Based Presentation System Engrane*
Proc. IMAGE 2002, Brisbane (Australia), 2002 (to be published)

**Herausgeberschaft und Mitherausgeberschaft an Proceedingsbänden**

Ch. Meinel, F. Rudolf
*„Sichere Telemedizin"*
*Proceedings Trierer Symposium „Sichere Telemedizin"*, Trier, Institut für Telematik, ISSN 1433-8106, 2002

Ch. Meinel, F. Rudolf
*„Digitales Geld"*
*Proceedings Trierer Symposium „Digitales Geld",* Trier, Institut für Telematik, ISSN 1433-8106, 2002

Ch. Meinel, M. Bittner, U. Sandl, I. Münch
*„eSecurity, Net-Security & Trusted eCommerce"*
*Proceedings Online 2002*, Düsseldorf, 2002

**Veröffentlichungen in Zeitschriften**

Ch. Meinel, L. Gollan
*Der elektronische Personalausweis? - Elektronische Signaturen und staatliche Verantwortung*
Internet-Zeitschrift für Rechtsinformatik, Web-Dok. 223/2002, Abs. 1-15

**Technische Berichte des Instituts**

Preprint 2002-10
*Sicherheitsrisiken und Schwachstellenanalyse von IT-Systemen*
Ch. Meinel, M. Schmitt

Preprint 2002-09
*Digitale Signaturen in der Verwaltung*
Ch. Meinel, L. Gollan

Preprint 2002-08
*Trierer Symposium Sichere Telemedizin, Proceedings*
Ch. Meinel, F. Rudolf

Preprint 2002-07
*Generieren von diagnostischen 3D-Objekten aus deformierten 2D-DICOM Bildern*
L. Vorwerk, Ch. Jiang, Ch. Meinel

Preprint 2002-06
*Patientenreminder*
B. Dusemund, Ch. Meinel

Preprint 2002-05
*Secure E-Document Container*
L. Gollan, A. Heuer, Ch. Meinel, T. Engel

Preprint 2002-04
*Digitale Signaturen für Kraftfahrzeuge*
Ch. Meinel, L. Gollan

Preprint 2002-03
*tele-TASK – Teleteaching Anywhere Solution Kit*
Ch. Meinel, V. Schillings

Preprint 2002-02
*Trierer Symposium Digitales Geld, Proceedings*
Ch. Meinel, F. Rudolf

Preprint 2002-01
*Digital Signatures for Automobiles!?*
Ch. Meinel, L. Gollan

**Studien**

M. Schmitt, M. Noll, G. Müllenheim, B. Lentes, M. Vieten, Th. Engel, Ch. Meinel
*Firewalls und Intrusion-Detection-Systeme Technologien und Produkte*

L. Gollan, Th. Engel, Ch. Meinel
*Digitale Signaturen*

T. Becker, B. Dusemund, L. Gollan, F. Losemann, L. Vorwerk, Ch. Meinel
*Public-Key Infrastrukturen - Konzepte und Produkte*

## Patente

Um die innovative fachliche Leistungskraft des Instituts für Telematik unter Beweis zu stellen, wurden drei Entwicklungen auf dem Gebiet der Sicherheit offener Netze bzw. der Telemedizin zum Patent angemeldet und erteilt:

- *Datenverbindung zwischen zwei Rechnern und Verfahren zur Datenübertragung zwischen zwei Rechnern („Lock-Keeper")* (Patentnummer: 198.38.253),
- *Verfahren zum Komprimieren eines digitalen Bildes mit mehreren Bitebenen* (Patentnummer: 199.44.213)
- *Verfahren und Vorrichtung zum digitalen Signieren digitaler Information* (Patentanmeldungsnummer: 102.34.815.4)

## Institutskolloquien 2002

15.11.2002
Frank Losemann
*PKI im Gesundheitswesen*
Symposium „Sichere Telemedizin"

06.11.2002
Uwe Roth
*The Internal Workflow of the Smart Data Server*

11.09.2002
Mikhail Gevantmakher
*Entwicklungen für die Telemedizin - DICOM-Manager*

04.09.2002
Idris Hamid Arrahmane
*Zope - ein Web Application Server und Content Management System*

28.08.2002
Wanjun Huang
*Improvement to the Smart Data Server with SOAP*

24.07.2002
Torsten Becker
*IT-Sicherheitskriterien im Vergleich*

22.07.2002
Chunyan Jiang
*Deformation and Construction of 3-D Medical Image*

17.07.2002
Michael Schmitt
*CERT Infrastrukur Deutschland*

26.06.2002
Benjamin Bölter, Bernd Dusemund
*Starcos Karte Management Tool*

19.06.2002
Martin Mitev
*Multiple Database Connectivity*

05.06.2002
Lutz Vorwerk, Ingo Scholtes
*Beispielimplementation einer objektorientierten Datenbank mit integrierter Verschlüsselung*

22.05.2002
Ralf Müller
*Risiko Management Toolkit*

15.05.2002
Stefan Dewald
*Redaktionssystem JDaphne im Institut für Telematik*

08.05.2002
Zhang Xinhua
*Beijing Technique Careerman Computer Application Level Test System*

24.04.2002
Ma, Mingchao
*Trust Management and Trust Service Based on Public Key*

17.04.2002
Lutz Vorwerk
*Mobiles PACS mit DICOM-konformer und benutzerorientierter Konfigurationsverwaltung*

10.04.2002
Bernd Dusemund
*CuraCall - Patientenreminder*

13.03.2002
Michael Schmitt
*Firewalls - Technologische Grundlagen*

06.03.2002
Torsten Becker
*Vorstellung des GPS-Fahrtenbuchs des TI*

06.03.2002
Mikhail Gevantmakher
*DICOMZIP*

27.02.2002
Max Mühlhäuser (Technische Universität Darmstadt)
*Ubiquitous Computing - Herausforderung oder „Hype"?*

20.02.2002
Lutz Gollan
*Digitale Signaturen - Zertifizierungsdiensteanbieter in Deutschland*

13.02.2002
Andreas Heuer
*Confidential Internet Mail*

06.02.2002
Ali Raza Baluch
*Telecommunication and Network Systems*

06.02.2002
Ji Hu
*Security Management System for E-commerce*

21.01.2002
Michael Noll
*„Lock-Keeper" Technologie*

## Gäste am Institut für Telematik 2002

Dr. Rainer Baumgart
Secunet Security Networks AG, Essen
*Elektronische Zahlungsmechanismen unter Sicherheitsgesichtspunkten*

Kay Leibold
Uni Karlsruhe, Institut für Wirtschaftspolitik und Wirtschaftsforschung
*Internet-Zahlungssysteme aus Sicht des Konsumenten - Ergebnisse der Online-Umfrage IZV5*

Dr. Stefan Werner
Credit Suisse (Deutschland) AG, Frankfurt/Main
*Rechtliche Aspekte von E-Payment-Systemen*

Maren Geisler
Verbraucherzentrale Bundesverband e.V., Berlin
*Nutzen und Risiken von Internet-Bezahlsystemen aus Verbrauchersicht*

Horst Förster
x-Business Consultance, Erftstadt
*Digitales Geld verdienen - Der deutsche Handel und das Online-Shopping*

Daniel Gläser
Stiftung Warentest, Berlin
*Fallstudie Micropayment - Auswahlkriterien und Akzeptanz beim Verbraucher*

Jochen Siegert
EURO Kartensysteme EUROCARD und eurocheque GmbH, Frankfurt/Main
*Kreditkarten: gegenwärtige und zukünftige Nutzung*

Hermann Seiler
Deutsche Bank AG, Frankfurt
*Die Macht der Standards - Voraussetzungen / Anforderungen für ein marktdurchdringendes Bezahlverfahren*

Dr. Joachim Beckert
Hypovereinsbank, Luxemburg
*Die Notwendigkeit eines sicheren Online-Bezahlsystems - Verhältnis von Aufwand und Nutzen aus Sicht der Akteure*

Dieter Bartl
Informatikzentrum der Sparkassenorganisation, Bonn
*Der zukunftssichere Transaktionsstandard für das Online-Banking*

Fabian G. Siegel
FIRSTGATE Internet AG, Köln
*Preisfindung für den Vertrieb digitaler Dienstleistungen und Güter*

Thomas Nisbach
ALLCASH Serviceges. f. elektronische Zahlungssysteme mbH, Moers
*Bezahlen in der Zukunft*

Patrick Braun
paybox Deutschland AG, Raunheim/Frankfurt
*Payment goes mobile – paybox*

Dr. Malte Krüger
PaySys Consultancy GmbH, Frankfurt/Main
*Grenzüberschreitendes Bezahlen im gemeinsamen Markt des mobilen Europas*

Dr. Thomas Schall
International Center for Telemedicine, Regensburg
*Perspektiven der Telemedizin – Entwicklungen, Trends, Visionen*

Bruno Struif
Fraunhofer-SIT, Darmstadt
*Die Health Professional Card für Ärzte und Apotheken*

Volkhard Sendatzki
BKK Bundesverband, Essen
*eRezept-Konzeption der Betriebskrankenkassen*

Dittmar Padeken
Bundesministerium für Gesundheit, Bonn
*Flächendeckende gesundheitstelematische Infrastruktur - Anspruch und Wirklichkeit 2002*

Bertram Bresser
Fraunhofer-IBMT, St. Ingbert
*PaDok – ein Ansatz für die kooperative elektronische Fallakte*

Dr. Gerhard Nitz
Kanzlei Dierks & Bohle, Berlin
*Rechtliche Anforderungen an Datenschutz und Datensicherheit*

Dr. Klaus Kern
Ministerium für Arbeit, Soziales, Familie und Gesundheit, Mainz
*Umfrageergebnisse zur Telemedizin in Rheinland-Pfalz*

Prof. Dr. Klaus Lowitzsch
Neurologie Klinikum Ludwigshafen
*Teleradiologie-Stroke-Units in Rheinland-Pfalz*

Yoshinori Tsukawaki
SAS Japan Inc., Zürich
*Mobile Patientenakte in Japan*

Yoshiaki Okuda
SAS Japan Inc., Zürich
*Mobile Patientenakte in Japan*

Dr. Claus-Werner Brill
Werbe- und Vertriebgesellschaft der Deutschen Apotheker, Eschborn
*Die Telematik-Konzeption der ABDA*

Jürgen Sembritzki
Zentrum für Telematik im Gesundheitswesen, Krefeld
*Die Bedeutung von Normung und Standardisierung im Gesundheitswesen*

Dr. Bernd Blobel
Institut für Biometrie und medizinische Informatik, Magdeburg
*Standards für sichere Telemedizin (EHR, XML, HL7, DICOM)*

Dr. Stephan Schug
Zentrum für Telematik im Gesundheitswesen, Krefeld
*Gesundheitsportale: Validierte Gesundheitsinformationen im Internet*

Dr. med. Guido Noelle, Lohmar
*Thesen zur patientenzentrierten Telemedizin*

Dr. Georgi Graschew
Charité, Humboldt-Universität zu Berlin
*Telechirurgie im Operationssaal der Zukunft*

Dr. Christoph Goetz
KV Bayerns
*Kryptographische Verfahren im Gesundheitswesen*

Thomas Weber
Deutsches Zentrum für Luft- und RaumfahrtLR, Köln
*Vision: Telemedizin in Luft- und Raumfahrt*

Rainer Herzog
MobiHealth, Ericsson GmbH, München
*Vision: Wireless Body Area Networks (BAN) – Killerapplikation für UMTS?*

# Medienresonanz

## 2002 Medienresonanz erneut gesteigert

Im Jahr 2002 stieß die Tätigkeit des Instituts für Telematik auf noch höheres Medieninteresse als im Vorjahr. Sowohl Fernsehen und Hörfunk als auch Printmedien griffen Themen aus der Institutsarbeit auf. Bemerkenswert war vor allem, dass viele Medien von sich aus, ohne dass es eines Impulses aus Trier bedurft hätte, auf das Institut zukamen und dessen Kompetenz für die Vorbereitung und Realisierung von Beiträgen nutzten. Deutschlands bedeutendste Nachrichtenagentur dpa führte im Verlauf des Jahres mehrere Gespräche mit der Institutsleitung. Dies führte zu einem hohen Multiplikationseffekt vor allem im Bereich der Tageszeitungen. Aber auch ausländische Medien wie z.B. die BBC nahmen sich Trierer Telematik-Themen an. Auf den folgenden Seiten präsentieren wir eine Auswahl von Medien, die sich mit der Instituts-Tätigkeit beschäftigten, und von Themen, die dabei eine Rolle spielten.

### www.t-online.de, 14.01.2003

**Schwerer Schlag für die deutsche Internetforschung**

Lästige Pflicht für Vielreisende: Jeder Kilometer muss für das Finanzamt per Hand ins Fahrtenbuch eingetragen werden. Kein Problem für die Tüftler des Trierer Instituts für Telematik. Sie entwickelten eine Lösung, die per PDA und Satellitennavigation alle Daten der Fahrt automatisch erfasst. Eine weitere Entwicklung der Trierer ist "Lock-Keeper", eine Schleuse, die Firmencomputer wirksam gegen Hackerattacken schützt. Mit solchen innovativen Projekten aus Deutschland könnte allerdings aufgrund der Wirtschaftsflaute bald Schluss sein.

**Forschung für die Praxis**

Dem Institut für Telematik in Trier gehen die Mittel aus. Die Hightech-Forschung im Bereich Internet muss damit eingestellt werden, wenn sich nicht noch ein Investor findet. Institutsleiter Professor Meinel äußerte großes Bedauern über die Entwicklung: "Das Institut für Telematik hat fünf Jahre lang nach amerikanischem Modell zukunftsträchtige und wirtschaftsnahe Hightech-Forschung rund ums Internet betrieben." Zahlreiche Patente, Preise, Veröffentlichungen und die Präsenz auf Technologiemessen dokumentieren die erfolgreiche Arbeit der Trierer.

**Forschung und Entwicklung für das Internet**

Seit der Gründung 1998 hat das Institut 120 Projekte mit einem Volumen von 5,8 Millionen Euro bearbeitet. Ein Defizit aus dem Jahr 2001 von 360.000 Euro konnte im vergangenen Jahr nicht ausgeglichen werden. Die 40 Mitarbeiter beschäftigen sich mit Hightech-Lösungen zur Verknüpfung von Computern, Mobilfunk und Internet. Im Oktober hat sich das Institut für den Betrieb der geplanten europäischen Top Level Domain .eu beworben.

**Aufträge blieben aus**

Das Institut wird von einem gemeinnützigen Verein getragen und finanziert sich aus öffentlichen Fördermitteln und Forschungsaufträgen aus der Wirtschaft. Wegen der schlechten Wirtschaftslage blieben jedoch seit dem Jahr 2001 Aufträge aus und das Land Rheinland-Pfalz musste seinen Zuschuss aufzustocken. Das Land ist nun nicht mehr bereit, die Kosten zu tragen und der Versuch, das Institut in die Universität Trier zu integrieren scheiterte, da die Uni das Risiko nicht tragen wollte. Die Träger des Vereins stellten daraufhin fest, dass die wirtschaftliche Grundlage für das Institut nicht mehr besteht. "Wenn sich im Verlauf des Liquidationsverfahrens nicht noch ein Investor findet oder sich der Haushalts- und Finanzausschuss des Landtags entscheidet, das Geld lieber in die Weiterarbeit des Instituts für Telematik zu stecken als in dessen Abwicklung, gehen für unsere Einrichtung definitiv die Lichter aus", bedauert Professor Meinel.

### www.chip.de, 14.01.2003

Fraunhofer Institut für Telematik droht das Aus

**Trier (ddp)** — Das auf Hightech-Forschung und -Entwicklung im Internet spezialisierte Institut für Telematik in Trier soll geschlossen werden. Nach Aussage von Institutsleiter Christoph Meinel hat der Trägerverein einen entsprechenden Beschluss gefasst. Ihm gehört neben dem Mainzer Wissenschaftsministerium auch die Stadt, die Universität, die Industrie- und Handelskammer und die Handwerkskammer Trier an.

Das Gremium habe mehrheitlich einer Bewertung des rheinland-pfälzischen Wissenschafts-Ministeriums zugestimmt, nach dem es keine genügend sichere wirtschaftliche Grundlage für das Fortbestehen des Instituts gebe, sagte Meinel. Für die Abwicklung des Liquidationsverfahrens sei ein Trierer Rechtsanwalt bestimmt worden, der ab dem morgigen Mittwoch tätig werde.

Aussagen von Meinel zufolge hatte der Haushalts- und Finanzausschuss des rheinland-pfälzischen Landtages Mitte Oktober eine vollständige Integration des Instituts in die Universität Trier empfohlen. Aufgrund eines hohen Eigenfinanzierungsanteils sei die Übernahme des bisher selbstständigen Instituts aber von der Universität als zu risikoreich angesehen worden.

**Info:** www.ti.fhg.de

### ARD Mittagsmagazin berichtet über das „Tigerteam" des Instituts für Telematik (30.07.2002)

### Trierischer Volksfreund,

**"Das falsche Signal"**

**Trägerverein des Instituts für Telematik beschließt Liquidation**

**Mit innovativen Lösungen hat sich das Institut für Telematik einen guten Namen gemacht. Nun droht das Aus. Foto: TV-Archiv/Friedemann Vetter**

TRIER. (j.s./wie) Das Trierer Institut für Telematik steht wegen finanzieller Schwierigkeiten vor dem Aus.

Der Trägerverein, dem neben der Stadt Trier unter anderem auch die Universität und die Kammern angehören, hatte, wie Institutssprecher Hans-Joachim Allgaier am Montag auf Anfrage mitteilte, am vergangenen Mittwoch den Beschluss zur Selbstliquidation gefasst. Die Mitglieder schlossen sich damit einer Bewertung des rheinland-pfälzischen Wissenschaftsministeriums an, nach der es keine genügend sichere Grundlage für das Fortbestehen des Instituts gebe. Das Land ist Hauptförderer des vor fünf Jahren gegründeten Instituts. Diese Einschätzung wird von den beiden Vorstandsvorsitzenden Professor Christoph Meinel und Professor Thomas Engel nicht geteilt. "Gerade in der gegenwärtigen Situation in Deutschland ist nicht zu verstehen, wenn nun das negative Signal ausgesendet wird. So etwas wollen wir uns hier nicht mehr leisten, solch ein innovatives Modell fördern

## eBanker, 26.09.2002


Stürmen Sie meine Bank, Herr Hacker!

## WDR Schulfernsehen, 20.03.2002

## Die Welt, 18.12.2002


Experte fordert elektronische Auto-Kennzeichen

## E-LEARNING, 27.11.2002


E-LEARNING

Einstein-Preis für Telematiker

PROVIDENCE/TRIER. (red) Das in Trier entwickelte E-Learning-System „Tele-Task" hat in den USA den „Einstein Award" verliehen bekommen. Die Trierer Wissenschaftler Professor Christoph Meinel und der Informatiker Volker Schillings nahmen die Auszeichnung auf einer Konferenz der weltweit größten Informatikergesellschaft „American Computing Machinery" (ACM) entgegen. Die neue Technik für Internetübertragungen wurde zum „außergewöhnlichsten und ideenreichsten" Projekt gekürt. Außer für Vorlesungen kann das Trierer Teleteaching-Modell auch für jede andere Art von Vortragsveranstaltungen genutzt werden. Entwickelt wurde Tele-Task (www.tele-task.de) in Meinels Arbeitsgruppe an der Uni Trier und am Trierer Institut für Telematik. Tele-Task überträgt außer Bildern und Ton in Großformat auch den verwendeten Präsentationsrechner mit Anschauungsmaterial, Grafiken und Computeranimationen als Video.

## ARD Text, 14.09.2002

547 ARD-Text 14.09.02 12:12:28

Gesundheit

Telemedizin kaum genutzt

Die Möglichkeiten der Telemedizin werden nach Einschätzung des Trierer Instituts für Telematik in Deutschland bislang nur ansatzweise genutzt.

Institutsleiter Prof.Christoph Meinel bemängelt, dass der elektronische Austausch von Gesundheitsdaten über große Entfernungen sich noch vorwiegend auf vereinzelte Pilotprojekte beschränke.

Deutschland sei noch weit entfernt von einem Flächen deckenden Ausbau der telematischen Infrastruktur im Gesundheitswesen, wie es die europäischen Regierungschefs vor zwei Jahren für Ende 2002 geplant hatten.

530 << Umwelt >> 548

## The British Journal of Healthcare Computing and Information Management, Mai.2002

### Dicomzip: images ten times faster and a tenth the size

The Hanover CeBIT exhibition in March saw the launch of Dicomzip, a revolutionary compression method that transmits medical images via the Internet at ten times the speed of conventional compression systems. Developed by Institut für Telematik of Trier, the process also reduces the storage space required for xray, tomography and ultrasonic image volumes, in some cases to about 10% of that needed in the past.

The Institut has found a way to combat the loss of image quality usually inherent in compressed data. Professor Christoph Meinel, the Director, explained: "We're basically dividing the original image into two pictures. One shows the actual contents of the image, the other contains unimportant technical components. Because both pictures have different structures, the most suitable compression process is utilised in each case."

With this technology, extremely high compression rates can be achieved while maintaining an image that is virtually identical with the original. A key benefit is that the software can run on any platform because it is a Java-based program that self installs and works regardless of the brand of hardware. Dicomzip will be marketed by ITM Services AG of Essen.

## PZ Pirmasenser Zeitung, 12.11.2002

### Meinel: „Es fehlt oft an Geld"

Zwei Drittel der Krankenhäuser nutzen keine Telemedizin

## NetworkWorld, 20.09.2002

### Unternehmen meiden das Thema Sicherheit

München (pi) – Die Wirtschaftskrise bremst den Ausbau der Sicherheits-Infrastrukturen. IT-Leiter versuchen Ausfällen, damit kein Investitionsbedarf sichtbar wird.

Deutsche Unternehmen können sich nach wie vor zu wenig um die Informationssicherheit. Diese Ansicht teilen sowohl Unternehmensberater als auch Wissenschaftler, die sich auf das Thema IT-Security spezialisiert haben. So wertete Informatikprofessor Christoph Meinel vom Trierer Institut für Telematik (ITM) Monate nach den Anschlägen von New York davon, dass die Wirtschaft angesichts knapper Budgets zurzeit am falschen Ende spare. Zwar ist die Bewusstsein für die Bedeutung von Sicherheitsmaßnahmen spürbar gestiegen, der praktisch fehle es vor allem an Mittelstand an Investitionen.

Nur bei Großunternehmen und Banken des Finanzbereichs sehe es besser aus. Meinels Thesen werden durch aktuelle Umfragen gestützt. So hat der Unternehmensberater Ernst & Young in einer Befragung herausgefunden, dass 80 Prozent der deutschen Firmen die Sicherheit ihrer IT-Infrastrukturen höchste Priorität, aber nur ein Drittel hat in den vergangenen zwölf Monaten mehr als etwa für die Sicherheit getan.

Meinel machte im Gespräch mit NetworkWorld deutlich, dass die Wechselwirkung zwischen der aktuellen Wirtschaftskrise und den Entwicklungen im Bereich IT-Sicherheit komplexer seien als auf den ersten Blick wahrzunehmen. «Es fällt zum Beispiel auf, dass immer dann, wenn möglichst kein Investitionsbedarf sichtbar werden soll, erklärt der Wissenschaftler. Dieses Denken sei vor allem deshalb bedauerlich, weil einmal erkannte Sicherheitslücken oft auch durch rein organisatorische Maßnahmen geschlossen

Fortsetzung auf Seite 5

## CeBIT News, 17.03.2002

ACADEMIC SUCCESS STORIES ON DISPLAY

## Neue Züricher Zeitung, 2.11.2002

**Fernvorlesung dank Streaming-Technik.** Chinesische Studenten können über das Internet erstmals an einer Informatikvorlesung aus Deutschland teilnehmen. Jeden Dienstag- und Donnerstagmorgen wird der Trierer Professor Christoph Meinel bis Ende Februar über Schwachstellen und Angriffspunkte der Internetsicherheit referieren. Zu seinem globalen Auditorium gehören auch etwa 24 Studenten der Polytechnischen Hochschule Peking, wie die Universität mitteilte. Die Vorlesung in englischer Sprache wird von Demonstrationen auf einem «Smart-Board» begleitet, einer Art Tafel mit elektronischem Stift. Dabei wird die Streaming-Technik von Realnetworks von technischen Erweiterungen der Universität Trier ergänzt. *(ap)*

## news.bbc.co.uk, 29.10.2002

BBC NEWS

Germans build web 'bridge' to Beijing

## www.waz.de, 19.09.2002

**Wählen übers Internet schwierig umzusetzen**

Trier (dpa) - Das Wählen per Mausklick am Computer oder mit Handy ist noch Zukunftsmusik. Zwar wäre das Wählen von zu Hause oder einem beliebigen Ort der Welt aus bequem. Doch anscheinend unüberwindbare rechtliche und finanzielle Hindernisse lassen die Praxis ins Ungewisse abdriften.

Ein junger Mann informiert sich an einem Computer in Frankfurt (Oder) über die Wahlprogramme der verschiedenen Parteien. Das Wählen per Mausklick am Computer oder mit Handy ist noch Zukunftsmusik.

»Wir sind weit entfernt von einem wahltauglichen Internet«, sagt der Internet-Wissenschaftler Christoph Meinel am Trierer Institut für Telematik. Gleichwohl müht sich eine Arbeitsgruppe unter Leitung des Bundesinnenministeriums, die Vision umzusetzen - als Ergänzung zum traditionellen Gang in die Wahlkabine. Schon zur nächsten Bundestagswahl 2006 sollen Computer und Internet zumindest so weit eingesetzt werden, dass die 80 000 Wahlbezirke vernetzt werden und jeder in einem beliebigen Wahllokal seine Stimme abgeben kann. In diesem Jahr werden in 29 deutschen Städten die ersten elektronischen Wahlgeräte aufgestellt.

Das Vorhaben einer Online-Stimmabgabe nennt der Informatiker Meinel ehrgeizig. Momentan seien Computer bei Wahlen nicht mehr als eine schnelle Auszählhilfe. »Wir sind nicht sicher vor Systemfehlern und Softwarefehlern und müssen jederzeit selbst mit einem Absturz rechnen - für eine Wahl muss die Möglichkeit der Stimmabgabe aber gesichert sein«, betont er.

Das Internet als Abstimmungsmöglichkeit werde bereits auf Betriebsratsebene und bei Studentenratswahlen getestet. Und Aktiengesellschaften in den USA nutzen die Online-Wahlverfahren längst für Abstimmungen in Hauptversammlungen.

## Luxemburger Wort, 23.08.2002

Cryptographie

**„Zunächst keine Gefahr"**

Der Trierer Informatik-Professor Christoph Meinel zum Plan eines US-Wissenschaftlers, den RSA-Schlüssel zu knacken

Sowohl durch Verwendung längerer Schlüssel als auch durch Entwicklung neuer Verschlüsselungsverfahren wird die Vertraulichkeit des Datenaustauschs über das Internet auch weiterhin gewährleistet bleiben. Mit diesem beruhigenden Hinweis hat der Trierer Informatik-Professor Christoph Meinel auf einen Bericht in der Frankfurter Allgemeinen Sonntagszeitung reagiert.

Danach soll angeblich ein „Chaos"-Knacker, falls er dem US-Mathematiker Daniel J. Bernstein gelingt, mit seiner geplanten neuen Rechenmaschine das Verschlüsselungssystem RSA zu knacken. Es ist weltweit seit 25 Jahren die wichtigste Geschäftsgrundlage für den elektronischen Handel und basiert auf der Tatsache, dass sich große Zahlen nur äußerst rechenaufwendig in ihre Primfaktoren zerlegen lassen. Die Ankündigung Bernsteins hatte in der Fachwelt für Aufsehen gesorgt.

Selbst wenn es der US-Mathematiker wirklich schaffe, bei gleichem Aufwand dreimal so lange natürliche Zahlen zu faktorisieren wie bisher, bräuchten Hacker und Geheimdienste mit dieser schnellen Technik noch längst „knacken digitales Generalschlüssel" in die Hand, betont Meinel. Der Direktor des unabhängigen Trierer Instituts für Telematik verweist darauf, dass es auch unter Kryptologen, also Experten für Chiffrierung, einen ständigen Wettlauf zwischen Verfahren und Gegen-Verfahren gebe. „Das RSA-Verfahren hat uns 25 Jahre lang geholfen. Jetzt sind eben wieder neue Anstrengungen fällig, um Systeme zu entwickeln, die den erhöhten Anforderungen gerecht werden", sagt Meinel.

Der Leiter des gemeinnützigen Spitzenforschungs- und Entwicklungszentrums fürs Internet macht ferner darauf aufmerksam, dass auch kommende Quanten-Computer die bisherigen Verschlüsselungstechniken in Frage stellen werden. Allerdings sind diese Rechner und ihre hohe Leistung derzeit noch Zukunftsmusik, meinte Meinel. Als Teil zwei der Doppelstrategie für den Erhalt vertraulicher geschäftlicher und privater Kommunikation über das Internet empfiehlt der Trierer Wissenschaftler zunächst eine Umstellung auf längere Schlüssel. Mit 2 048-stelligen Zahlen in Computer gerechter Binärschreibweise (2 048 Bit) sieht der Informatik-Professor die Nutzer auf der sicheren Seite. Die meisten mit der RSA-Technik verschlüsselten Daten werden derzeit mit 1024-Bit-Schlüsseln chiffriert. Auch das Bonner Bundesamt für Sicherheit in der Informationstechnik plädiert laut Presseberichten dafür, spätestens vom Jahr 2006 an nur noch Schlüssel der Länge 2 048 Bit zu benutzen.

Das als eingetragener Verein verfasste gemeinnützige und außeruniversitäre Institut für Telematik ist in seiner Ausrichtung in Deutschland einmalig. Nach gut vier Jahren Arbeit kann es schon auf zwei Patente, vier Promotionen und mehr als 80 Fachbeiträge zu internationalen Konferenzen verweisen. Die gut 50-köpfige Mannschaft rund um Professor Christoph Meinel entwickelt anwendungsfreundliche und praxistaugliche Hightech-Lösungen. M-Commerce, Internet-Intranet, Sicherheit der Datenkommunikation in offenen Netzen, Telemedizin, Elektronisches Publizieren, Systementwurf und -analyse - das sind die derzeitigen Tätigkeitsfelder des international beachteten Spitzenforschungsinstituts aus Trier. Es ist u.a. Mitglied der Initiative D21 und Träger des Erfinderpreises Rheinland-Pfalz.

www.ti.fhg.de

## www.super-illu.de, 25.08.2002

**Trier: Hilfe für US-Regierung beim Datenschutz**

München (ots) - Das Institut für Telematik hat der US-Regierung angeboten, zum Schutz von Rechnern im Internet die Hochsicherheits-Software Lock-Keeper einzusetzen. Damit könnte wichtige Computer in offenen Netzen "hundert Prozent zuverlässig gegen Attacken von Online-Hackern" abgesichert werden, sagte Instituts-Direktor Professor Christoph Meinel. Der Forscher reagierte damit auf Berichte in BBC und der Zeitung "Washington Post", wonach die US-Sicherheitsfirma PrismicTec sich schockiert darüber gezeigt habe, wie leicht es sei, in Netze des Pentagon einzudringen und auf vertrauliche Daten zuzugreifen. Der Leiter des Instituts für Telematik vermutet, dass der von Army-Sprecher Ted Drauchowski bestätigte Angriff nicht zu einem Ausspähen von sicherheitsrelevanten Informationen geführt hat. "Sever mit solch sensiblen Daten werden bislang meistens nicht ans Internet angeschlossen", erklärte Meinel. **Trierer Lock-Keeper sicherer als Firewalls** Würden die Rechner aber mit dem patentierten deutschen Lock-Keeper gesichert, sei dieser Coup möglich. Hackern wird mit dem Lock-Keeper dadurch verkauft das Handwerk gelegt, dass eine direkte physikalische Verbindung des Firmen-Netzes mit dem Internet niemals zugelassen wird. "Firewalls trennen das Internet eines Unternehmens nicht von der Außenwelt, sondern analysieren und filtern lediglich die übermittelten Datenpakete", erklärte Meinel. Deshalb sei es nicht auszuschließen, dass durch Softwarefehler, mangelnde Kenntnisse des Personals oder fehlerhafte Konfiguration die Firewalls in ihrer Schutzfunktion eingeschränkt oder sogar außer Kraft gesetzt werden. **Schleuse als physikalische Trennung** Das Lock-Keeper-System sorge hingegen dafür, dass die zwischen einem Firmen-Intranet und dem Internet übermittelten Daten eine Schleuse mit Rechner passieren müssten. Je nach Zustand der "Tore" findet der Informations-Austausch nur jeweils mit einem der Rechner statt. Während des Aufenthalts in der Schleuse können die zuvor Daten je nach den Sicherheits-Einstellungen der Firma überprüft werden.

## Focus-Magazin, 06.06.2002

INTERVIEW „Großes Durcheinander"

**PROFESSOR CHRISTOPH MEINEL** vom Institut für Telematik in Trier über die Chancen der digitalen Signatur

**FOCUS:** Das Geschäft mit der digitalen Signatur lohnt sich nicht, sagt die Deutsche Post, und schließt eines der größten Trust-Center für Signaturen. Steht damit die elektronische Unterschrift in Deutschland vor dem Aus?

**Meinel:** Es gibt ja, wie unsere soeben veröffentlichte Studie zeigt (www.ti.fhg.de), noch 14 andere Zertifizierungsanbieter. Aber auch die werden mit ihren verschiedenen Signaturen kein Geld verdienen.

**FOCUS:** Warum nicht?

**Meinel:** Weil potenzielle Kunden wie Krankenkassen abwarten, welche Signatur sich in der Praxis durchsetzt. Schuld an dem Signatur-Durcheinander ist der Staat: Er hat 1997 die Entwicklung der elektronischen Unterschrift aus der Hand gegeben und Wirtschaftsunternehmen überlassen. Deshalb gibt es bis heute keinen einheitlichen Standard – das lähmt das Geschäft.

**FOCUS:** Soll der Staat der digitalen Signatur auf die Sprünge helfen?

**Meinel:** Der Staat muss sich jetzt auf eine Signatur festlegen. Die kann zum Beispiel in einen Chipkarten-Personalausweis integriert werden. Er könnte – wie im Einwohnermeldewesen – eine staatliche Infrastruktur schaffen oder aber Trust-Center mit der Signaturausgabe betrauen. Dann kommen die Kunden, und die digitale Signatur setzt sich in Deutschland endlich durch.