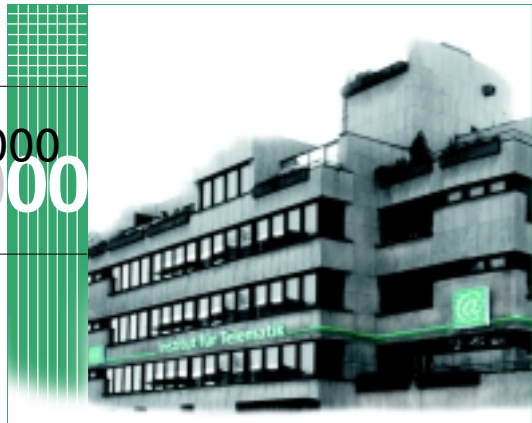
Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Tätigkeitsbericht 2000

Tätigkeitsbericht 2000



Christoph Meinel
Thomas Engel

Impressum

Impressum

Verantwortlich

Christoph Meinel und Thomas Engel

Redaktion

Lutz **Gollan**

Layout

Uwe Becker

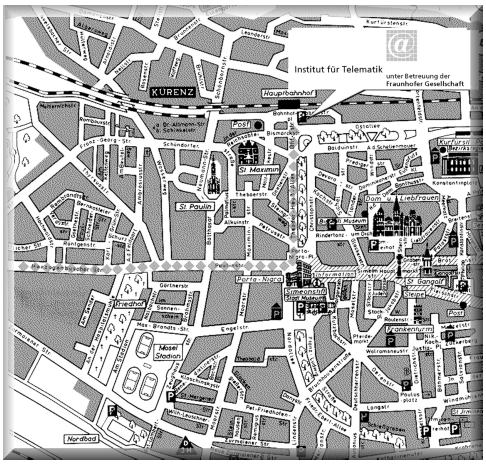
Anschrift der Redaktion

Institut für Telematik e.V.
Pressestelle
Bahnhofstraße 30-32
D-54292 Trier

E-Mail: info@ti.fhg.de

Telefon+49 (0) 651-97551-0

Telefax+49 (0) 651-97551-12



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Tätigkeitsbericht 2000

Tätigkeitsbericht 2000

Inhalt

T wie Telematik

T wie Trust

T wie Trier

T wie TI

Vorwort

Vorwort

Auch im dritten Jahr des am 1. Januar 1998 gegründeten Instituts für Telematik kann im Jahresbericht über eine Vielzahl von Erfolgen der Wissenschaftlerinnen und Wissenschaftler dieser noch jungen Einrichtung berichtet werden. So zum Beispiel über

- die ersten zwei Patente des Instituts,
- die ersten erfolgreich abgeschlossenen Promotionen von Institutsangehörigen,
- mehr als 30 von internationalen Jurys ausgewählte Forschungsberichte auf großen internationalen Tagungen,
- erfolgreich bearbeitete, zukunftsträchtige Kooperationsprojekte mit Partnern aus Wirtschaft und Gesellschaft und
- die Durchführung wichtiger Veranstaltungen.

Das alles spielt sich ab auf dem zukunftsträchtigen Feld der im Institut umfassend bearbeiteten Telematik, die durch die rasante Entwicklung der neuen Informations- und Kommunikationstechnologien und die ungeheure Nachfrage in Wirtschaft und Gesellschaft vorangetrieben wird. Dem Fraunhofer-Ideal folgend, das erfolgreiches angewandtes Forschen im Kontext konkreter Projektaufträge empfiehlt, war das Institut auch im Jahr 2000 wieder ein Ort der international beachteten anwendungsorientierten Forschung zum Nutzen von Wirtschaft und Gesellschaft.
Wir wünschen Ihnen beim Durchblättern und Lesen des Berichts viel Freude. Bestimmt gibt es auch in Ihrem Umfeld interessante Telematik-Probleme, die einer Lösung harren. Wir würden uns freuen, wenn Sie dazu Kontakt mit uns aufnehmen würden. Gerne suchen wir gemeinsam nach Lösung enfür diese Probleme.

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

Trier, im April 2001

Univ.-Prof. Dr. sc. Christoph Meinel

Dr. Thomas Engel

Das TI im Profil

Das TI im Profil

Grundsätzliches

Das Institut für Telematik in Trier befasst sich mit den vielfältigen, neuen Potenzialen, die sich aus der Verschmelzung von Telekommunikation und Informatik für die Nutzung der weltweit verteilten und elektronisch verfügbaren Daten ergeben. Es erforscht und entwickelt Möglichkeiten, wie man an jedem Ort und zu jeder Zeit auf die in den weltweit verbreiteten Computernetzwerken vorhandenen Informationen effizient zugreifen, mit diesen sicher umgehen und sie intelligent nutzen kann. Abläufe in Wirtschaft, Verwaltung, Verkehr und Gesundheitswesen können durch die Ergebnisse unser praxisorientierten Arbeit wesentlich rationeller gestaltet werden. Dabei streben wir danach, die Anwendung so einfach und nutzerfreundlich wie möglich zu machen.

Mit der Fraunhofer-Gesellschaft verbunden und als eingetragener Verein verfasst, ist das Institut für Telematik eine außeruniversitäre Forschungs- und Entwicklungs-Institution, die in ihrer Ausrichtung in Deutschland einmalig ist. 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 der Verfassung des Instituts für Telematik ist es fachlich und wirtschaftlich unabhängig, beschäftigt hervorragend qualifizierte Mitarbeiter mit einem sehr hohen Leistungsanspruch. Das Institut ist fachlich sehr flexibel und kann permanent neue Forschungsthemen aufgreifen. Nur 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, und Weitere wichtige Projekte). Wir agieren in der Bugwelle neuester technologischer Entwicklungen und wollen durch das ‚Ausreizen' technischer Potenziale 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 drei Jahren Arbeit weist unsere wissenschaftliche Bilanz zwei Patente, zwei Promotionen und fast 70 Fachbeiträge zu internationalen Konferenzen auf – eine Leistung, die auch weltweit 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. Das Institut bietet damit einen Ort, an dem die akademische Elite durch anwendungsbezogene Pro-

jekte schnell und gezielt auf die Tätigkeit als Führungskräfte der Wirtschaft vorbereitet wird.

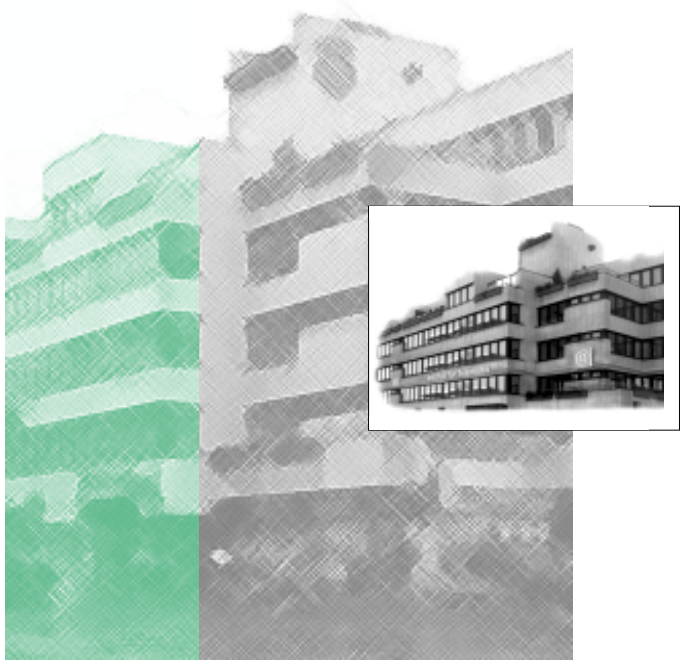
Telematik

Die Telematik hat sich erst Anfang der 90er Jahren 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 Potenzials 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.

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

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 enge Verbindungen zu den Instituten der Fraunhofer-Gesellschaft.

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 hoch leistungsfähigen PCs bzw. mit Workstations ausgestattet.
Am Institut für Telematik sind Standleitungen in verschiedene Netze (B-WIN, 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 strategischen 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:

- Universität Trier, insbesondere zur Abteilung Informatik, zum Zentrum für Wissenschaftliches elektronisches Publizieren (WEP) und zum DFG-Graduiertenkolleg „Mathematische Optimierung“
- Fraunhofer Gesellschaft und Fraunhofer Management Gesellschaft, München
- Polytechnische Hochschule Turin
- University of Colorado at Boulder, USA
- Computer Career Institute, Clark University, Massachusetts
- Dagstuhl, Internationales Begegnungs- und Forschungszentrum für Informatik
- Dresdner Bank AG, Frankfurt
- DREGIS – Dresdner Global IT-Services GmbH, Frankfurt
- ABBL - Association des banques et banquiers, Luxembourg
- IAL, Luxemburg
- Krankenhaus der Barmherzigen Brüder, Trier
- Ministerium für Bildung, Wissenschaft und Weiterbildung, Mainz
- Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau, Mainz
- Stadt Trier
- Industrie- und Handelskammer Trier
- Handwerkskammer Trier
- Vereinigung Teletrust Deutschland e.V., Erfurt
- Initiative Gesundheitstelematik Deutschland e.V., Köln

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

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:

- Universität Trier
- Stiftung Innovation des Landes Rheinland-Pfalz
- ABBL - Association des banques et banquiers, Luxemburg
- Deutsche Forschungsgemeinschaft (DFG)
- Nikolaus Koch Stiftung, Trier
- IAL, Luxemburg
- Mutterhaus der Borromäerinnen, Trier
- Krankenhaus der Barmherzigen Brüder, Trier
- University of Colorado at Boulder, USA
- Trierischer Volksfreund
- Stiftung Burgen, Schlösser, Altertum, Koblenz
- Dateninformationszentrum Rheinland-Pfalz, Mainz
- Ministerium für Inneres und Sport, Mainz
- Sozialministerium Baden-Württemberg, Stuttgart
- Technologiebeirat des Landes Rheinland-Pfalz
- Dresdner Bank AG, Frankfurt
- AGIS Allianz Gesellschaft für Informatik Service, München
- ZFE Siemens AG, München
- Firma UNILUX, Salmtal
- GWI Research, Trier
- Sybase, Düsseldorf
- WGZ-Bank Luxembourg S.A.
- Global Access
- Institut für Mittelstandsforschung InMIT, Trier
- DG BANK Luxembourg S.A.
- Caritas Trägergesellschaft Trier
- Industrie- und Handelskammer Trier
- Handwerkskammer Trier
- Euro Info Center, Trier

Handelnde Personen

Handelnde Personen

Die erfolgreiche Arbeit des Instituts für Telematik resultiert in hohem Maße aus der Kompetenz der Entscheidungsträger und wissenschaftlichen Mitarbeiter des Instituts, die alle über eine sehr hohe fachliche Qualifikationen verfügen. Sie wäre aber auch nicht denkbar ohne die tatkräftige Unterstützung durch die Vereinsmitglieder und das Kuratorium.

Institutsleitung

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

Stellvertreter: Dr. rer. nat. Thomas Engel

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

Prof. Dr. sc. 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 Informatik an die Universität Trier berufen.
Christoph Meinel ist Autor, Mitautor und Herausgeber von 8 Büchern und mehr als 100 wissenschaftlichen Veröffentlichungen in renommierten wissenschaftlichen Zeitschriften und bei internationalen Kongressen. Sein Hauptinteresse gilt den Forschungsgebieten Komplexitätstheorie, VLSI-Design und Telematik.
Prof. Dr. sc. Meinel ist Direktor des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP) an der Universität Trier und Mitglied verschiedener Aufsichtsräte und internationaler Konferenzprogrammkomitees. 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). Nicht zuletzt ist er 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 weiterhin Herausgeber des elektronischen Kolloquiums ECCC.
Prof. Dr. sc. Meinel war Mitglied des Technologiebeirats des Landes Rheinland-Pfalz und aktiv an der Arbeit des Forums Info 2000 der Bundesregierung Deutschland beteiligt.

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

Von 1987 bis 1992 studierte Dr. 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 TI.
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).

Führungskreis

Dr. rer. nat. Bernd Dusemund

Bis 1992	Studium der Physik an der Uni Saarbrücken
Abschluss	Dipl.-Physiker
1992-1993	wissenschaftlicher Mitarbeiter INM, Homburg;
1993-1999	Wissenschaftlicher Mitarbeiter an der Universität Saarbrücken
Seit 1999	Wissenschaftlicher Mitarbeiter am Institut für Telematik
Projekte:	Verantwortlich tätig im Bereich Smartcards und Trustcenter

Dipl. –Inform. Ernst Georg Haffner

1987	Studium der Informatik/Mathematik an der Uni Kaiserslautern,
Abschluss bis 1997	Dipl.-Inform. Tätigkeit in einer Unternehmens-EDV-Zentrale
seit 1997	Wissenschaftlicher Mitarbeiter am Institut für Telematik
Projekte:	Verantwortlich tätig in den Bereichen: Middleware, Hyperlinkmanagement, High-Security-Architekturen (LockKeeper)

Dipl. –Phys. 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

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 1995	Dipl.-Inform. Systemberater, Schwerpunkt: Administration von großen Lotus-NotesDomänen
seit 1998	Wissenschaftlicher Mitarbeiter am Institut für Telematik
Projekte:	Verantwortlich tätig im Bereich: Systementwicklung im Bereich Middleware

Mitarbeiter

Im Jahre 2000 beschäftigte das Institut 24 wissenschaftliche Mitarbeiter. 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

Mitarbeiter des Instituts für Telematik

Florence Absolu, M.A.
Dipl. Phys. Oliver Baldus
Dipl. Math. oec. Torsten Becker
Dipl. Phys. Dr. rer. nat. Bernd Dusemund
Dipl. Bibl. Michael Düro, M.A.
Dipl. Ing. Paul Ferring
Dr. iur. Lutz Gollan
Dipl. Inform. Ernst-Georg Haffner
Dipl. Phys. Andreas Heuer
Dipl. Inform. Frank Losemann
Dr. rer. nat. Sergey Khludov
Dipl. Inform. Kais Louizi
Dipl. Ing. Eugeni Lutschichin
Dipl. Ing. Ali Mabrouk
Dipl. Inform. Mariana Podesta
Dipl. Wirtsch.-Ing. Carsten Radke
Dipl. Inform. Uwe Roth
Dipl. Designer (FH) Andreas Laubenthal
Dipl. Inform. Changtao Qu
Dipl. Inform. Harald Sack
Wolfgang Thies
Dipl. Inform. Lutz Vorwerk
Dipl. Inform. Arno Wagner
Dr. rer. soc. Zhongdong Zhang

Systemadministration

Dipl. Math.oec. Jochen Bern
Dipl. Inform. Zheng Liu

Sekretariat/Verwaltung

Annelie Pauly
Carmen Galbraith
Waltraud Sauter-Herges
Barbara Huberty

Wissenschaftl. Hilfskräfte, Praktikanten

Julia Bäuerlein
Heiko Barth
Benjamin Bölter
Mariette Colling
Stefan Dewald
Esther de Leeuw
Hristov Filkov
Michail Gvantmakher
Daniel Görgen
Harald Haak
Jan Hirschler
Ewgenij Huebner
Thomas Hoffmann
Carmen Leopold
Maik Jarre
Martin Meinel
Tobias Meinel
Mihail Minev
Martin Mitev
Gerhard Müllenheim
Andreas Meyer
Maja Milicic
Michael Noll
Christine Orth-Theis
René Possin
Rüdiger Schlegel
Sebastian Schneider
Markus Treinen
Monika Trapp
Thomas Wagner
Till Zoppke
Zuo Xiaoping

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 Kompetenzen aus und nehmen wichtige Positionen in Politik, Gesellschaft, Wirtschaft und Wissenschaft ein.

Mitglieder

• Bitburger Brauerei Th. Simon
vertreten durch den Geschäftsführer
Alfred Müller

• Dr. rer. nat. Thomas Engel
Stellvertretender Direktor des Instituts für Telematik

• Handwerkskammer Trier
vertreten durch den Hauptgeschäftsführer
Ass. Hans-Hermann Kocks

• Industrie und Handelskammer Trier
vertreten durch den Hauptgeschäftsführer
Dr. Wolfgang Scheider

• Prof. Dr. sc. Christoph Meinel
Professor für Informatik der Universität Trier

• RWE Energie AG
vertreten durch den Direktor der RWE Energie AG, Regionalversorgung Trier, Dipl.-Inform. Josef Poll

• 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. Christoph Meinel
Universität Trier, FB IV – Informatik (Vorstandsvorsitzender)

• Dr. rer. nat. Thomas Engel
Institut für Telematik (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 Bildung, Wissenschaft und Weiterbildung, Rheinland-Pfalz, Mainz

Stellvertretender Kuratoriumsvorsitzender

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

Mitglieder des Kuratoriums (alphabetisch)

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

• Dr. Guido Hertwich
Leiter Telematik Forschung und Technologie, Daimler Benz AG, Berlin

• Univ.-Prof. Dr. Dieter Maaß
Univ.-Präsident i.R., Vorstandsvorsitzender a.D. des DFN-Vereins, Kaiserslautern

• Ministerialdirigent Josef Mentges
Ministerium für Bildung, Wissenschaft und Weiterbildung, Rheinland-Pfalz, Mainz

• Alfred Müller
Geschäftsführer der Bitburger Brauerei Th. Simon GmbH, Bitburg

• Paul Schuh
Conseiller de direction 1ère classe des Ministère des Communications, Luxembourg

• Dr. Hermann Josef Spital
Bischof von Trier

• Univ.-Prof. Dr. Peter Schwenkmezger
Präsident der Universität 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

Personell verbundene 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 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

Konkret geht es hier im Kernbereich der theoretischen Informatik um die Charakterisierung des Ressourcenbedarfs für konkrete Berechnungen. Schwerpunkt der Forschung ist die Frage nach bessern 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-wertigen) 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 Kommunikationszentrum 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. Christoph Meinel

Geschäftsführer: Dipl.-Inform. 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 2000 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

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
- Adaptive Datenkompression mit JAVA
- System zur elektronischen Arztbriefschreibung
- Interaktive multimediale Patientenakte
- Intranet-basierte PACS-Systeme

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:

- Firewalling (High-Security)
- Virtual Private Networks VPN
- Elektronische Modellierung von Datenzugriffshierarchien
- Trust-Center - Zertifizierungstellen nach Signaturgesetz
- Zertifikat-Management
- Datenverschlüsselung
- 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

Patienten-CD-System

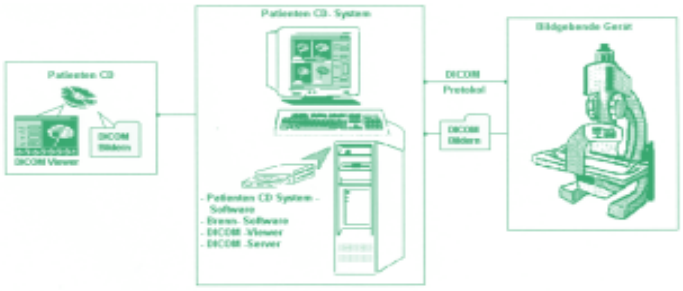
Patienten-CD-System

Projekt Patienten-CD-System

Die Vernetzung von Krankenhäusern, Rehabilitationszentren und Arztpraxen sowie die Ausnutzung neuer Möglichkeiten der Informations- und Telekommunikationstechnologien macht in medizinischen Einrichtungen neue Arbeitsabläufe möglich. Fachkollegen verschiedener Einrichtungen und an unterschiedlichen Orten können über das Internet und/oder Intranet miteinander kommunizieren, Daten austauschen und auf umfangreiche verteilte Datenbanken zugreifen, um schnell an notwendige Informationen zu gelangen.

Zwischen Ärzten, die in der Radiologie tätig sind, werden zur Zeit große Datenvolumen in dem Original-DICOM-3-Format[1] per CD-Medien ausgetauscht. Ein Grund dafür sind die erheblichen Einschränkungen bei der Datenübertragung über das Internet (z.B. unzureichende Sicherheit und lange Übertragungszeiten). Alle bisherigen Lösungen dieses Problems sind unmittelbar entweder mit hohen Kosten oder zeitaufwendigen fachbezogenen Personalschulungen und mit massivem Widerstand des betroffenen medizinischen Personals verbunden.

Die Erfahrung aus der Zusammenarbeit mit mehreren Krankenhäusern in Trier brachte das Institut für Telematik auf die Idee, ein benutzerfreundliches und vollautomatisiertes System zum Archivieren medizinischer Bildern aller Art auf CD–Medien zu entwickeln, das insbesondere einen breiten Zugang zu den archivierten digitalen Bildern und deren unkomplizierte Nutzung ermöglicht.
Dieses System (im Weiteren Patienten-CD-System genannt) besteht aus einem bereits früher am Institut für Telematik entwickelten DICOM–Viewer[2], einem Patienten–CD-Schreibmodul[3] und einer DICOM-Server[4]-Software.



Block Schema des Systems

Das Verfahren eignet sich zur Langzeitarchivierung sowohl von Radiologie- als auch von Ultraschallaufnahmen. Die Patienten-CD vereinfacht nicht nur die Archivierung medizinischer Bilder, sie spart auch Kosten und ermöglicht einen einfachen und sicheren Datenaustausch.
Der interessierte Patient kann seine medizinischen Bilddaten auf CD mit nach Hause nehmen und am heimischen PC selbst betrachten.

Das Patienten-CD-Schreibmodul ist eine JAVA[5]–Anwendung. Damit können aktiv oder passiv digitale medizinische Bilder direkt von den bildgebenden Geräten empfangen werden. Mit seiner Hilfe werden über den eingebauten CD-Rekorder nicht nur Bilder im Original-DICOM-3-Format direkt auf einen CD-Rohling gebrannt, sondern auch der zu ihrer späteren Betrachtung notwendige DICOM-Viewer. Die Aufnahmegeschwindigkeit hängt allein von dem verwendeten CD-Brenner ab. Mit den zur Zeit üblichen CD-Brennern können Rohlinge innerhalb von 6 –7 Minuten mit 650 MB Daten beschrieben werden. Das entspricht einer Kapazität von bis zu 3000 digitalen medizinischen Bildern. Die mit dem Patienten-CD-System beschriebenen CD-Rohlinge können später in allen handelsüblichen CD-Laufwerken gelesen werden . Nach dem Einlegen ins Laufwerk startet die CD automatisch und bietet mehrere Handlungsalternativen zur Auswahl: Hilfe, Infos, Bildbetrachtung usw.

Das Patienten-CD-System bietet damit dem Arzt eine schnelle und bequeme, z.B. nach Patientennamen geordnete Übersicht über die vorhandenen Bilder bzw. Bildserien. Außerdem stellt es dem Arzt die wichtigsten Bildparameter zu Verfügung.

[1] DICOM ist eine Abkürzung für „Digital imaging and communications in medicine". DICOM kann als Mulimedia-Standard in der Medizin bezeichnet werden.
[2] DICOM Viewer ist eine Software zum Lesen und Visualisieren von DICOM–Daten
[3] Patienten–CD Schreibmodul ist eine Software zum komfortablen Schreiben von DICOM–Daten auf CD-Medien
[4] DICOM –Server ist eine Software, die DICOM–Daten von einem medizinischen bildgebenden Gerät (z.B. Röntgengerät) empfängt, um diese Daten weiter verarbeiten zu können.
[5] JAVA: Objektorientierte Programmiersprache, die im Internet sehr verbreitet ist.

Ausgewählte Bilder/Bildserien lassen sich per Knopfdruck sehr komfortabel auf die CD-Medien schreiben. Zur Vereinfachung der Arbeit mit dem Patienten-CD-System dient eine mitgelieferte Hilfefunktion, die sehr ausführliche Informationen und Tipps zum bequemen Arbeiten mit dem Programm bereitstellt.
Der DICOM-Viewer für das Patienten-CD-System ist ein leistungsfähiger JAVA-basiertes Programm zum Betrachten von digitalisierten medizinischen Bildern aller Art, die in dem inzwischen international weit verbreiteten DICOM-3-Format bereitgestellt werden. Der DICOM–Viewer stellt alle nötigen Werkzeuge zur Verfügung, um ein Bild oder eine Bildersequenz im DICOM-3-Format mit einer hohen Auflösung darstellen und bearbeiten zu können.

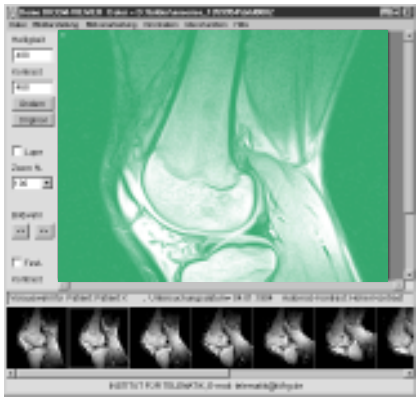
Oberfläche des Patienten-CD Viewers für die Betrachtung der Bilder

DICOM-Viewer Funktionen:

- 2D-Darstellung medizinischer Daten
- Schnittbild-Erzeugung aus Volumendatensätzen
- Videoanimationen in verschiedenen Bildfrequenzen
- Inversion eines Bildes
- Veränderung von Kontrast und Helligkeit des Bildes
- Geometrische Transformation
- Grauwert-, Distanz-, Winkelmessung
- Zoom
- Vorschau auf Bilder des aktiven Verzeichnisses
- Lupe mit verschiedenen Vergrößerungsraten
- Miniaturansicht aller Bilder des aktiven Verzeichnisses

Vorteile des Patienten-CD-Systems gegenüber den herkömmlichen Archivierungsmethoden:

1. benutzerfreundlich
2. schnell und arbeitssparend
3. niedrige Betriebkosten
4. hohe Kompatibilität mit den gängigen Betriebssystemen.
5. digitale medizinische Bilder von einer Patienten-CD können an jedem PC ohne spezielle Visualisierungsprogramme betrachtet werden, und zwar ohne Qualitätsverlust.
6. um das Patienten-CD-System bedienen zu können, braucht man keine speziellen Vorkenntnisse. Das Erlernen dauert maximal eine halbe Stunde.



DICOM Viewer

Bisher wurden über 50.000 verschiedene DICOM-Bilder bewertet, die mit radiologischen Geräten unterschiedlicher Hersteller (z.B. Siemens, Philips, AGFA) produziert wurden. Die große technische Zuverlässigkeit des Systems konnte damit unter Beweis gestellt werden.

LuxTrust

LuxTrust

Eines der Schwerpunktgebiete der Tätigkeit des Instituts für Telematik ist die Sicherheit von Daten in offenen Netzen. Hierbei setzt das Institut auf hochsichere und moderne Lösungen, die zum einen flexibel, zum anderen skalierbar sind. Im Laufe der letzten Jahre hat sich herausgestellt, dass sogenannte „Public-Key-Infrastrukturen" (PKI), die auf sogenannten „digitalen Signaturen" und „asymmetrischer Verschlüsselung" beruhen, die gewünschten Eigenschaften bei hoher Verfügbarkeit und hochgradiger Sicherheit. PKIs können in den unterschiedlichsten Bereichen verteilter Anwendungen eingesetzt werden und eignen sich aufgrund ihrer Sicherheits-Features insbesondere für den Bankenbereich.
Das Institut für Telematik kann in den entsprechenden Projekten bezüglich der notwendigen Infrastruktur und der Sicherheitsstandards auf seine Erfahrungen mit dem hausinternen TI-Trustcenter (TI-TC) zurückgreifen. Dieses wird. u.a. für die konkrete Projektarbeit als Test-CA eingesetzt und ermöglicht so realistische Test-Szenarien, die in der Praxis beim Auftraggeber umgesetzt werden können.
Die diesbezüglichen Kompetenzen des Instituts für Telematik wurden im Jahr 2000 unter anderem in das Projekt LuxTrust eingebracht.

Ausgangslage

Seit 1999 wird in Luxemburg, dem zentralen europäischen Bankenplatz neben Frankfurt, der Aufbau einer hochsicheren Computernetz-Infrastruktur für die Absicherung des elektronischen Geschäftsverkehrs konzipiert. Den vor Ort ansässigen international tätigen Banken ist dabei bewusst, dass die Schaffung einer gemeinsamen Infrastruktur mit der Unterstützung des Landes deutliche Vorteile bietet im Vergleich zu singulären und proprietären, möglicherweise nicht miteinander kompatiblen Lösungen.

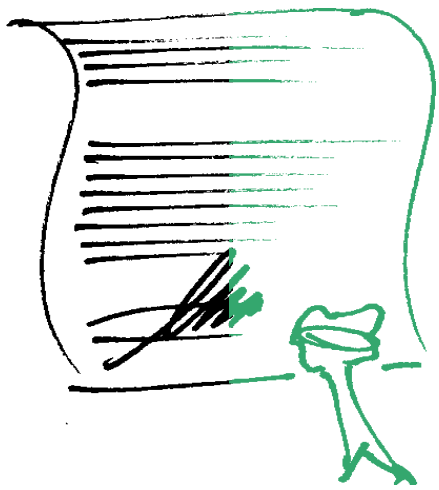
Projektziel

Nachdem die Banken die Chancen, aber auch die Gefährdungen des netzgestützten elektronischen Geschäftsverkehrs erkannten, waren durch das Institut für Telematik in enger Zusammenarbeit mit den Auftraggebern mögliche Problemlösungen zu erörtern. Es ging um Entscheidungsgrundlagen aus technischer, rechtlicher und betriebswirtschaftlicher Sicht.

Projektphasen

Im umfangreichen Projekt „LuxTrust" des Instituts für Telematik wurden zu Beginn die Anforderungen des Bankenplatzes Luxemburg an den Bau und die Infrastruktur einer hochsicheren, umfassenden E-Commerce-Lösung analysiert. Hierbei wurde deutlich, dass ein gemeinsames Trustcenter als Rückgrat einer landesweiten Public-Key-Infrastruktur (PKI) ein sowohl sichereres als möglicherweise auch kostengünstigeres Modell sein könnte.

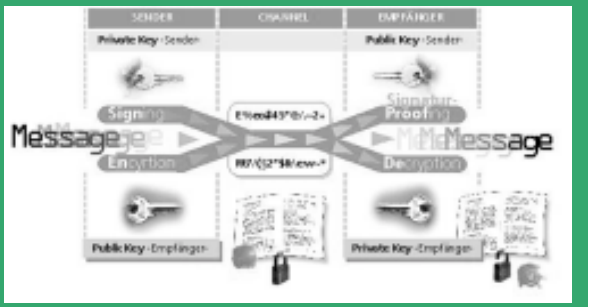
In der nächsten Projektphase wurden die benötigten technischen und infrastrukturellen Komponenten definiert. Abschließend prüfte das Institut

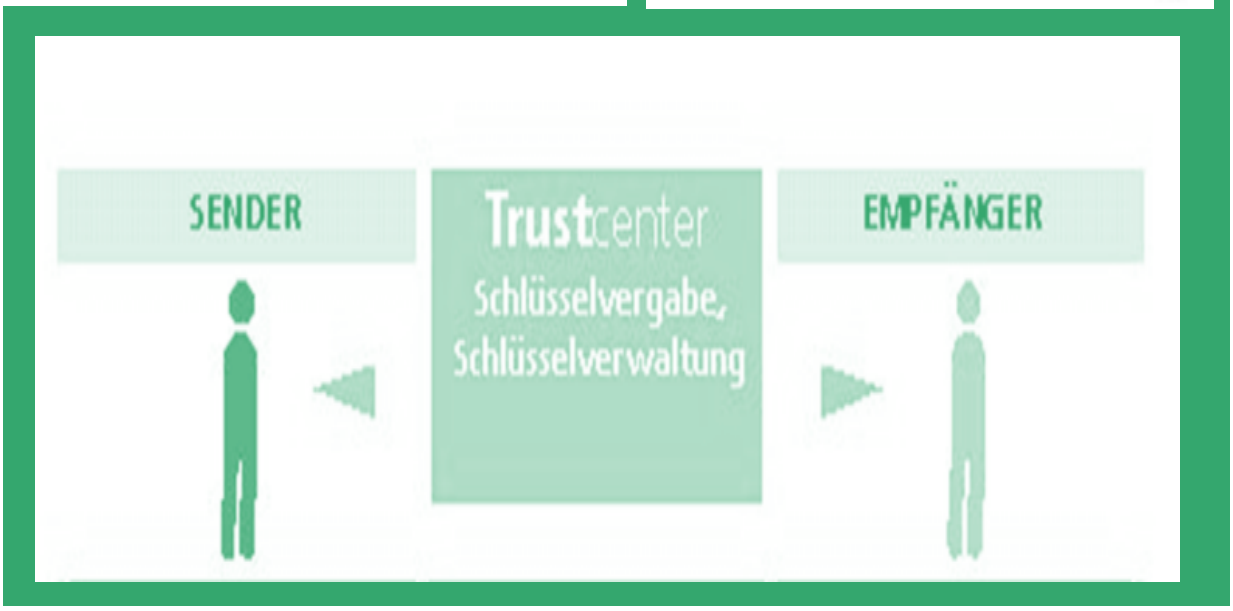


die realisierbaren Lösungsmöglichkeiten für diese Komponenten.
Drei grundsätzliche Konzepte standen hierbei zur Auswahl: singuläre und z.T. proprietäre Lösungen der einzelnen Banken, vollständige Auslagerung des Baus und des Betriebs eines gemeinsamen Trustcenters oder die Errichtung und der Betrieb eines eigenen Trustcenters mit ausgewählter Unterstützung durch Dritte.

Entscheidungsgrundlage

Alle drei Konzepte wurden vom Institut für Telematik gleichwertig analysiert. Auch angesichts der finanziellen Bedeutung der Entscheidung war eine betriebswirtschaftliche Begleitung („Business-Case") der Lösungsmodelle erforderlich. Hierbei griff das Institut für Telematik auf die renommierte internationale Unternehmensberatung PricewaterhouseCoopers (PwC) zurück, die mit Unterstützung des Instituts für Telematik das Kosten-Nutzen-Verhältnis der einzelnen Konzepte analysierte.
Im Vordergrund der Tätigkeit des Instituts für Telematik stand die Definierung eines „goldenen", offenen Standards für die bestmögliche Sicherheit einer Lösung. Dabei wurden sowohl die informationstechnologischen, infrastrukturellen (Stichwort: Policy) und rechtlichen Anforderungen bestimmt. Die weltweit führenden Anbieter von PKI-Lösungen waren anschließend eingeladen, in einem mehrtägigem Workshop die verfügbaren Produkte und Leistungen vorzustellen. Anschließend analysierte das Institut für Telematik mit Unterstützung von PwC diese Lösungen und führte sie in einer fünfbändigen, umfassenden Dokumentation für die Auftraggeber zusammen. Die im letzten Stadium des Projekts gewonnen Erkenntnisse und Empfehlungen wurden abschließend präsentiert.





Virtuelle Hochschule

Virtuelle Hochschule

Ausgangslage

Die zunehmende Vernetzung der Gesellschaft verschafft der modernen Informations- und Kommunikationstechnik vor allem im Bereich der Aus- und Weiterbildung an Hochschulen und ihrem Umfeld neue Möglichkeiten. Eine in den Bildungseinrichtungen aber auch in den Haushalten ständig zunehmende Zahl von Rechnern mit Internet-Zugang ermöglicht die örtlich und zeitlich nicht mehr gebundene Wissensvermittlung und –überprüfung. Wie multimediale Informations- und Kommunikationstechnologien in bestehende oder neue Ansätze zur Vermittlung von Wissen einbezogen und als Ergänzung zu klassischen Unterrichtsformen genutzt werden können, wird daher derzeit viel diskutiert. Es handelt sich um ein über die Hochschulen hinaus auch für Politik und Gesellschaft bedeutsames Thema, dem sich das Institut für Telematik auch im Jahr 2000 intensiv gewidmet hat.

Sicherheitsaspekte einer virtuellen Universität

Um eine virtuelle Universität zu verwirklichen, bedarf es einerseits eines vertieften Verständnisses für die spezifischen Inhalte und das Zusammenwirken der verschiedenen Komponenten, die das Lernen über Entfernungen verlangen. Andererseits müssen auch die inhärenten Schwächen des Internets berücksichtigt werden, vor allem was die Wahrung der Privatsphäre der Teilnehmer und den sicheren Datentransfer betrifft.

Voraussetzungen für die sichere virtuelle Universität

Nur wenn bei der Verwendung des Internets als Hauptkommunikationskanal für alle Beteiligten Sicherheit und Privatsphäre umfassend garantiert werden, wird es möglich sein, eine virtuelle Universität erfolgreich zu betreiben. Deshalb müssen folgende Voraussetzungen erfüllt sein:

· *Vertraulichkeit*: Durch die Verschlüsselung von Daten wird die Privatsphäre der Nachrichtenübermittlung gewahrt.
· *Authentifikation*: Der Absender der Nachricht wird eindeutig identifiziert. Es wird ausgeschlossen, dass sich jemand eine falsche Identität zulegt oder sich als eine andere Person ausgibt.
· *Integrität*: Die versandte Nachricht erreicht unverändert den Adressaten.
· *Unwiderrufbarkeit*: Der Sender kann die Autorenschaft einer Nachricht, die er gesendet hat, im Nachhinein nicht abstreiten.

Modell der virtuellen Universität

Sämtliche dieser Eigenschaften können durch den Aufbau einer Public-Key-Infrastruktur (PKI), wie sie das Institut für Telematik anbietet, nachhaltig erreicht werden. In unserem Modell einer virtuellen Universität, das auf den jahrelangen Erfahrungen des Instituts im Bereich der Zertifikatsverwaltung bei Banken beruht, wird - auf offenen Standards basierend - eine PKI mit folgenden Komponenten geschaffen:

Ein sicheres *elektronisches Studienbuch* wird für jeden Studierenden eingerichtet. Es beinhaltet die relevanten persönlichen Informationen wie Name, Immatrikulationsdatum und die abgelegten Scheine und Prüfungen.

Ein *Zertifikats-Server* gibt den Teilnehmern die Möglichkeit, Zertifikate für die Kommunikation zu beantragen und diese auf ihrem Rechner oder einer Smart Card zu installieren. Dadurch wird bei Aufsuchen der virtuellen Universität im Netz die Eingabe von Passwörtern überflüssig.

Ein *Directory-Server* verwaltet die Zertifikate der Studierenden und Lehrenden sowie der Verwaltungsmitarbeiter zentral und speichert sie für alle nachprüfbar.

Ein *Zeitstempeldienst* verschafft die Möglichkeit, Dokumente mit einer Zeitmarke zu versehen. Dies ist für die Abgabe von Hausarbeiten und Diplomarbeiten („Abgabeschluss“) unerlässlich.

SmartCards, Disketten oder auch *Festplatten* können als persönliche Sicherheitsumgebung für die Speicherung privater Schlüssel und zur Aktivierung der Zertifikate dienen.

Zertifikate und Zeitstempeldienst – Basis für die sichere Kommunikation

Die Zertifikate der Teilnehmer und der virtuellen Universität sowie der Zeitstempeldienst können zu folgenden Aufgaben genutzt werden:

- Zugriff auf das elektronische Studienbuch
- Signieren von Scheinen und Prüfungsergebnissen
- Signieren und Verschlüsseln von E-Mails
- Erwerb von Studienunterlagen
- Antragstellung bei der Uni-Verwaltung
- Verschlüsselter Versand der Kreditkartennummer für Gebührenzahlung
- Versendung persönlicher privater Informationen zur Universitätsverwaltung
- Verteilung von Forschungsergebnissen
- Einsicht in persönliche Daten von Studenten nur durch berechtigte Personen
- Zeitstempel, um die Existenz elektronischer Dateien zu einen bestimmten Zeitpunkt zu dokumentieren
- Anträge auf Aufnahme in Kurse mit einer begrenzten Teilnehmer-Zahl

Ausgewiesene Kompetenz des Instituts für Telematik

Während bislang die Vermittlung der Lerninhalte im Vordergrund der Konzepte zur virtuellen Hochschule steht, bietet das Institut für Telematik ein umfassendes Infrastruktur-Modell zur Umsetzung dieser Ansätze, das den modernen Ansprüchen an die sichere und vertrauliche Kommunikation in offenen Datennetzen gerecht wird. Die u.a. im Bankenbereich bewiesene Kompetenz des Instituts bei der Schaffung und dem Betrieb einer PKI mit mehreren zehntausend Teilnehmern ist dabei ein Garant für den Erfolg dieses Modells.

Weitere wichtige Projekte

Weitere wichtige Projekte

In der Folge stellen wir eine Auswahl interessanter Projekte vor, an denen 2000 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.

1. Online- Redaktionssystem

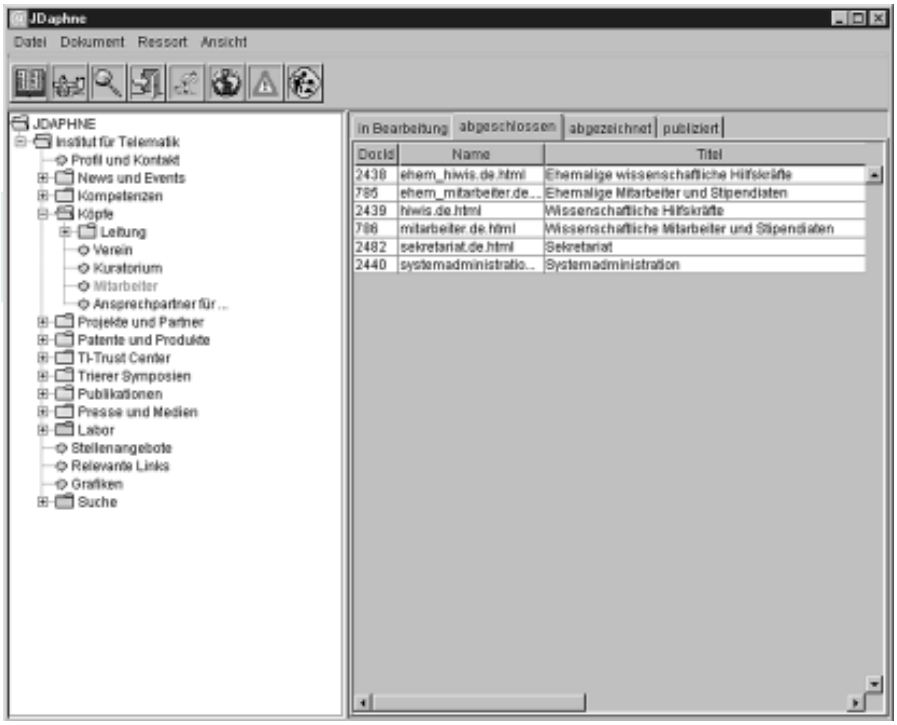
JDAPHNE

JDAPHNE (Java Distributed Authoring and Publishing of Hypertexts in Network Environments) ist ein vom Institut für Telematik entwickeltes Web-Präsenz-Content-Management-System (WCMS). Das interaktive und dynamische System für den Praxisalltag zeichnet sich dadurch aus, dass alle Komponenten, sowohl auf Server- als auch auf Client-Seite, mit allen gängigen Betriebssystemen zusammen arbeiten. Um diese Plattform-Unabhängigkeit zu gewährleisten, sind die Hauptkomponenten auf der Server-Seite in JAVA implementiert. Auf der Client-Seite wird die Plattform-Unabhängigkeit durch den Einsatz von HTML und einem JAVA-Applet erreicht. Der Client muss deshalb nur über einen Web-Browser verfügen. Das Applet selbst läuft im Web-Browser in einer definierten Umgebung, einem frei verfügbaren Plugin, ab.

Rollenbezogene Zugriffskontrolle

Die Zugriffskontrolle im WCMS erfolgt über Rollen und Verzeichnisse. Über die Rollen werden die Berechtigungen zu bestimmten Aktionen, z.B. Schreiben, Lesen oder Publizieren vergeben. Für die inhaltlichen Berechtigungen werden Verzeichnisse, im weiteren als Ressorts bezeichnet, herangezogen. Diese Verzeichnisse sind nicht direkt an einzelne Benutzer gekoppelt, sondern an Gruppen. Über die Zugehörigkeit zu einer oder mehreren Gruppen erhält jeder Benutzer somit die Berechtigung, in den zugeordneten Ressorts zu arbeiten, d.h. auf die Dateien darin zuzugreifen. Welche Arbeitsschritte im Einzelnen erlaubt sind, ist von der Rolle abhängig, die der Benutzer inne hat. Über die Rollen und Resorts lässt sich eine beispielsweise an die Unternehmenshierarchie angepasste Rechtevergabe vornehmen. Während die Erfassung und Modifikation von Inhalten durch die Sacharbeiter mit der zugehörigen Rolle „Autor" erledigt wird, sorgt die übergeordnete Ebene, im Unternehmen die Ebene mit inhaltlicher Verantwortung (im WCMS als „Freigabe-Berechtigter" bezeichnet) für die inhaltliche Kontrolle.
Die Gesamtübersicht über den Stand der Web-Präsenz wird von der Rolle des „Webmasters" erwartet. Mit Zugriff auf alle Ressorts versehen

obliegt es den Inhabern dieser Rolle, die von den „Freischaltungs-Berechtigten“ abgezeichneten Dokumente im Internet zu publizieren. Die mit den einzelnen Rollen verbundenen Berechtigungen lassen sich innerhalb des Systems sehr fein einstellen. Zusammen mit der Ressortstruktur und den Gruppen lassen sich so die Mitarbeiter des Unternehmens flexibel mit Zuständigkeiten und Berechtigungen für die Pflege der Web-Präsenz versehenn.



Dokumenten-Workflows

Die Konzeption des WCMS sieht verschiedene Workflows für die verwalteten Dokumente vor. Weil sehr stark mit den Rollen verknüpft, lassen sich die Workflows nur über die Vergabe entsprechender Berechtigungen gestalten. Der normale Workflow für ein Dokument ist zum Beispiel dreistufig: Das Dokument wird bearbeitet und vom Autor fertiggestellt. Der „Freistellungs-Berechtigte“ zeichnet es ab. Der „Webmaster“ publiziert es dann. Der hier exemplarisch dargestellte Workflow bildet ein Sechs-Augen-Prinzip ab. Um ein Vier-Augen-Prinzip zu praktizieren, könnte es beispielsweise dem „Freistellungs-Berechtigten“ erlaubt werden, selbst Dokumente zu publizieren. Alternativ können von dem Autor als fertig gemeldete Dokumente auch von ihm selbst abgezeichnet werden und dann direkt vom Web-Master publiziert werden. Wie an diesem Beispiel skizziert, lassen sich für alle im Rahmen des WCMS anfallenden Workflows entsprechende Rollenvergaben vornehmen. Im Zusammenspiel mit „Aufgaben-Listen“, die für die Rolleninhaber aufgestellt werden, lassen sich flexible Arbeitsabläufe schaffen, die einfach geändert und angepasst werden können.

Ressort-Struktur

Wie im Zusammenhang mit der rollenbezogenen Zugriffskontrolle schon erwähnt, werden die Informationen durch „Ressorts“ inhaltlich gegliedert. Diese sind in etwa mit den Verzeichnissen im Dateisystem zu vergleichen. Ressorts können ineinander geschachtelt werden und bieten somit die Möglichkeit zur feingliedrigen Verwaltung der Informationen. Jeder Informationsbaustein wird fest einem Ressort zugeordnet. Diese primäre Ordnung wird wie bei einem Dateisystem in einem hierarchischen Baum präsentiert. Den Informationsbausteinen können aber auch sekundäre Zugehörigkeiten gegeben werden. Anhand dieser sekundären Zugehörigkeiten, die nicht wie die Ressorts Teil der rollenbezogenen Zugriffskontrolle sind, lassen sich alternative Darstellungen beim Publizieren aufbauen. Während in der Normaleinstellung die Ressortstruktur auch in der fertigen Web-Präsenz sichtbar wird, z.B. in der Navigation, lassen sich über die sekundären Zugehörigkeiten von der Ressortstruktur unabhängige Darstellungen erzeugen.

2. Bildkomprimierung

Ausgangslage

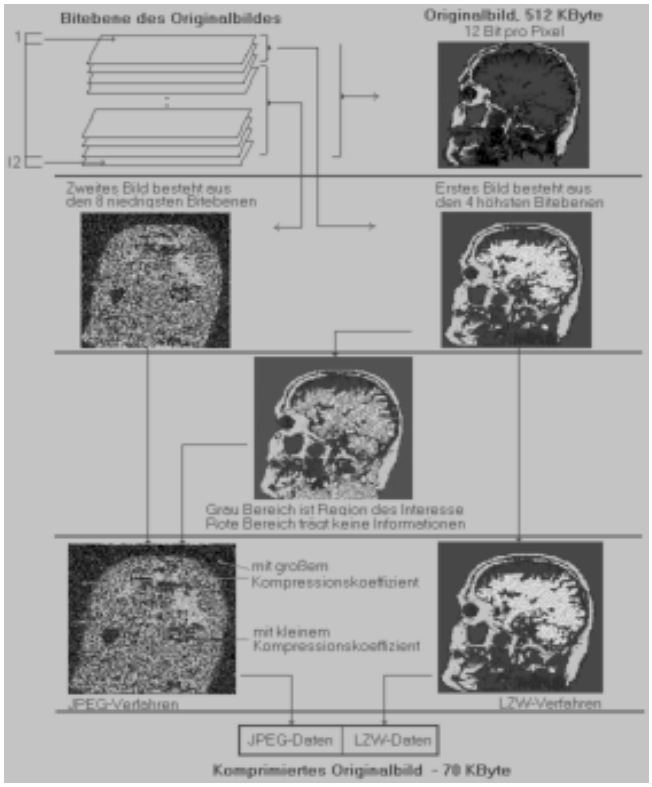
Krankenhäuser und Arztpraxen sind derzeit nicht in der Lage, medizinische Bilder einfach und schnell über das Internet auszutauschen. Hauptverantwortlich dafür sind der große Datenumfang zwischen zehn und 150 Megabyte pro Bild, der für erhebliche Übertragungszeiten sorgt, und die in der Medizin nicht akzeptablen Verluste bei herkömmlicher Bildkomprimierung.

Vorteile

Mit äußerst geringem Rechenaufwand können so sehr hohe Verdichtungsraten erzielt und gleichzeitig eine praktisch verlustfreie Bildwiedergabe gewährleistet werden, wie sie der medizinische Standard verlangt. Ein wesentlicher Vorteil liegt darin, dass die Ärzte die übermittelten Patienten-Bilder mit jedem herkömmlichen Browser betrachten könnten.

Patentierte Technologie

Eine Erfindung, für die das Institut für Telematik im Jahr 2000 in Deutschland Patentschutz erhielt, stellt eine bisher unerreichte Verdichtung der digitalen Daten von Patienten-Bildern sicher. Die Datenmenge schrumpft dabei bis zu einem Zwanzigstel zusammen. Dadurch benötigt die Bild-Übermittlung von Arzt zu Arzt übers Internet nicht mehr bis zu drei Stunden, sondern nur wenige Sekunden – wichtig vor allem in der Notfall-Medizin.



Es gelang, die bei sonstigen schnellen Bildkomprimierungs-Verfahren auftretenden Einbußen an Bildqualität zu vermeiden. Im Prinzip wird das Originalbild - zum Beispiel aus einer Röntgen- oder Computertomographie-Untersuchung - in zwei Bilder zerlegt. Das eine zeigt den eigentlichen Bildinhalt, das andere unwesentliche technische Bestandteile, sogenanntes Hintergrundrauschen. Da beide Bilder jeweils unterschiedliche Bedeutung aufweisen, wird für jedes dann das jeweils spezifisch geeignetste Verfahren der Komprimierung angewendet. Ein verlustfreies Verfahren verdichtet das Hauptbild zu einer GIF-Datei, das verlustbehaftete JPEG-Verfahren reduziert das „Rausch-Bild" auf ein Minimum. Am Ende werden beide Bilder wieder zusammengefügt und abgeschickt.

3. Lock-Keeper Patent

Ausgangslage

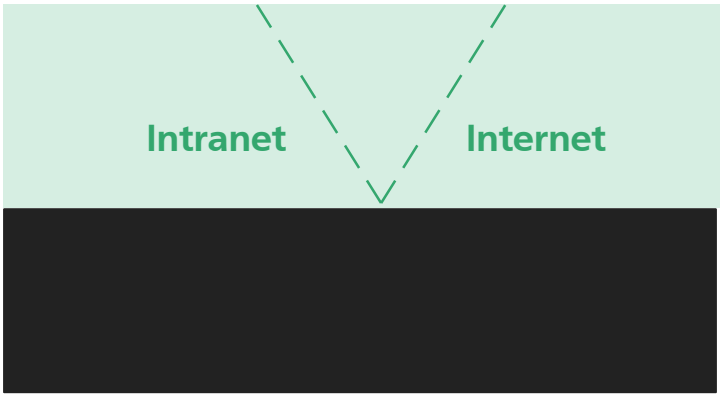
Firewalls schützen zwar Netzwerke gegen Attaken krimineller Eindringlinge, bieten jedoch aufgrund ihrer Komplexität und schwierigen Wartbarkeit keinen absoluten Schutzen gegen Online-Angriffe. Die Lock-Keeper-Technologie setzt hier an und positioniert sich damit im Segment hochsicherer Netzwerkarchitekturen. Im Jahr 2000 wurde für den Lock-Keeper das deutsche Patent mit der Nummer 198 38 253.7-31 erteilt. Die Nachricht über die Patent-Erteilung sorgte für die bisher größte Publizität des Instituts in Printmedien und Rundfunk.

Technologie

Die Lock-Keeper-Technologie wurde am Institut für Telematik entwickelt und setzt die Idee der „Schleuse" auf dem Gebiet hochsicheren Datentransfers um. Zu keinem Zeitpunkt besteht eine direkte Verbindung zwischen zwei datenaustauschenden Netzen, sondern, je nach Zustand der „Schleusentore", findet der Informationsaustausch nur jeweils mit einem der Kommunikationspartner statt. Die Datenverbindungen werden hierbei jeweils physikalisch getrennt. Während des kurzen Aufenthalts in der Schleuse werden die Daten überprüft.
Online-Attacken auf interne Unternehmensdaten sind durch das Lock-Keeper-System ausgeschlossen. Seine fortschrittliche Architektur erlaubt es, den durch die Schleuse entstehenden Zeitversatz bei Datenaustausch und Datenprüfung vergleichsweise gering zu halten.

Einsatzgebiete

Die Lock-Keeper-Technologie kann ergänzend zu bereits existierenden Firewall-Systemen eingesetzt werden, um hochsichere Teilnetze gegen Online-Attacken sicher zu schützen. Insbesondere dann, wenn ein passiver Informationsaustausch (z.B. Transfer sicherheitsrelevanter Dokumente, E-Mails u.a.) genügt, empfiehlt sich der Einsatz des „Lock-Keepers", der mit vergleichsweise geringem Konfigurationsaufwand höchste Sicherheitsvorgaben erfüllt. Darüber hinaus kann der Lock-Keeper ebenso als hochsicherer Einstieg in den Datenaustausch zwischen Intranet und Internet fungieren. Bis Personal und Infrastruktur für den Einsatz gemanagter Firewallsysteme bereitsteht, kann der Lock-Keeper bereits als Lösung für den E-Mail-Austausch eingesetzt werden.



Der zeitversetzte und softwareunabhängige Lock-Keeper-System (LKS) gewährleistet den hohen Sicherheitsstandard beim Datenaustausch

Abb. *Aufbau der Lock-Keeper-Komponenten*

Ausblick

Die Funktion des Lock-Keepers basiert auf dem Prinzip der Schleuse, die zahlreiche Internet-Protokolle abwehrt. Die künftige Weiterentwicklung dieser Technologie zielt darauf ab, die Reduktion im „Quality of Service" zu verringern und zugleich Bandbreite und Durchsatz der Daten zu erhöhen.

4. Digitaler Zeitstempel

Ausgangslage

Mit einer Geschwindigkeit wie nie zuvor verbreitet sich die elektronische Datenverarbeitung in immer mehr Bereichen. Ob in Schulen, Krankenhäusern, Verwaltung oder Unternehmen - der Computer wird für zentrale Aufgaben wie elektronischer Schriftverkehr, Ausstellung von Urkunden, Archivierung von Daten, Buchhaltung, etc. mehr und mehr eingesetzt.
Bei der Unterzeichnung eines herkömmlichen Dokumentes in Papierform bestätigen die Unterzeichner, eventuelle Zeugen oder - je nach Notwendigkeit - auch ein Notar sowohl die Gültigkeit der enthaltenen Daten als auch den Zeitpunkt, zu dem das Dokument erstellt wurde.
Doch die digitale, körperlose Form wichtiger Dokumente und Urkunden bringt in dieser Beziehung einige Schwierigkeiten mit sich: Einerseits sollen alle Aufgaben von physischen Dokumenten erfüllt, andererseits aber auch die Integrität der Inhalte wie auch die Beweiskraft gewährleistet sein.
So will zum Beispiel ein Notar beweisen können, dass ein elektronisch aufgesetztes Testament zu einem bestimmten Zeitpunkt in exakt dieser Form existiert hat.

Der digitale Zeitstempel

Abhilfe für dieses Problem schafft der digitale Zeitstempel, der ein elektronisches Dokument ebenso markiert wie ein herkömmlicher Datumsstempel auf Papier. Das Institut für Telematik hat im Rahmen eines Forschungsprojektes ein solches Verfahren realisiert und auch die institutionellen Voraussetzungen einer Time Stamping Authority (TSA) als Teil eines Trust Centers geschaffen.

Das Verfahren

Ziel des Projektes war es, ein Verfahren zu entwickeln, das es dem Benutzer auf einfachem Wege möglich macht, ein elektronisches Dokument digital „zeitstempeln" zu lassen.
Der Anwender kann über ein benutzerfreundliches Applet (ein im Browser laufendes Java-Programm) bequem einen Zeitstempel für sein elektronisches Dokument anfordern.
Dabei wird das Dokument zunächst mit einem durch spezielle Algorithmen ermittelten numerischen Wert, dem sogenannten „Hash-Code", versehen, um das Dokument zu identifizieren.
Dieser Wert ist einzigartig und kann nur an Hand des Dokumentes selbst (und zwar genau in dieser Form) reproduziert werden. Wenn schon nur ein Zeichen des Dokumentes verändert wird, verändert sich zwangsläufig auch der resultierende Hash-Wert.
Das aktuelle und nicht verfälschbare Datum zu erhalten, ist eine anspruchsvolle Aufgabe, da sich Datum und Uhrzeit bei Computern in der Regel ohne viel Aufwand im Betriebssystem oder in BIOS ändern lassen. Weil die Beweiskraft des Dokumentes jedoch mittelbar von der Korrektheit des Erstellungsdatums abhängt, werden Datum und Uhrzeit von einem speziellen Zeitstempel-Server der TSA geliefert. Somit können sie nicht von Dritten beeinflusst oder manipuliert werden.
Die auf diese Weise ermittelten Daten werden nun mit den Daten des Dokumenteninhabers und der Identifikation des Zeitstempelservers zu dem eigentlichen Zeitstempel zusammengeführt.
Um die Authentizität und die Integrität des Zeitstempels selbst zu gewährleisten, wird nun der Zeitstempel mit dem Zertifikat der TSA signiert, bevor er an den Benutzer zurückgeschickt wird.

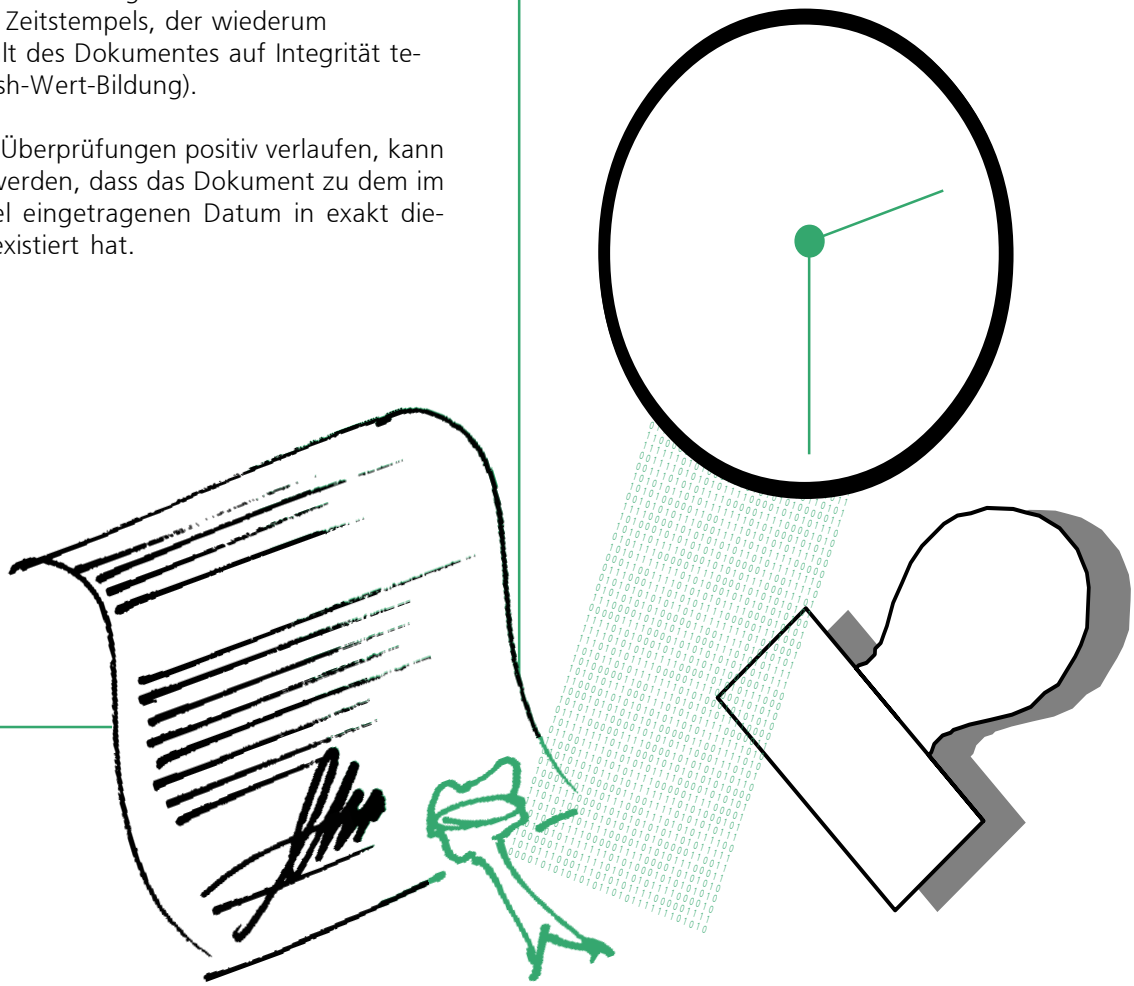
Jede Datenübertragung zwischen Client und Server erfolgt verschlüsselt, damit alle Daten während der Kommunikation vor Manipulation bzw. Einsichtnahme Dritter geschützt sind.

Verifikation

Die Benutzeroberfläche bietet ebenfalls einen leicht zu bedienenden Mechanismus zur Überprüfung des Zeitstempels.
Ein mehrstufiges Verifikationsverfahren überprüft nicht nur den Zeitstempel in Bezug auf das spezifische Dokument, sondern auch die Authentizität des Zeitstempels sowie die Korrektheit der Signatur und die Gültigkeit des Zertifikates:

- das Zertifikat der TSA, das den Inhaber des öffentlichen Schlüssels identifiziert und bestätigt, wird auf Gültigkeit überprüft.
- mit dem öffentlichen Schlüssel wird die Zeitstempel-Signatur auf Validität (Gültigkeit) getestet
- die Signatur bestätigt schließlich die Korrektheit des Zeitstempels, der wiederum
- den Inhalt des Dokumentes auf Integrität testet (Hash-Wert-Bildung).

Wenn alle Überprüfungen positiv verlaufen, kann bestätigt werden, dass das Dokument zu dem im Zeitstempel eingetragenen Datum in exakt dieser Form existiert hat.



5. Weiterentwicklung der Smart Card-Technologie

Smart Card Technologie

Karten sind dem Anwender und Bürger schon seit geraumer Zeit vertraut in Form von Krankenkassenkarten oder Geldkarten, Parkhauskarten oder Kreditkarten. Ihre Funktionalität basiert hauptsächlich auf dem Abspeichern von persönlichen Informationen, die mit entsprechenden Terminals ausgelesen werden können. Ein inhärenter Mangel ist die Sicherheit und Vertraulichkeit der Daten, die darauf enthalten sind. Moderne Karten mit integrierten Chips sind in der Lage, kryptographische Operationen auf der Karte auszuführen.
Mit ihnen lassen sich Anwendungen auf der Karte realisieren, die höchsten Sicherheitsanforderungen genügen, und des weiteren mehrere Anwendungen auf einer Karte vereinen können. Die Sicherheit stützt sich auf die geschützte Verwahrung eines dem Besitzer eindeutig zugeordneten privaten digitalen Schlüssels. Die Zuordnung geschieht in einem Trustcenter, das über eine sehr hohe Sicherheitsinfrastruktur verfügt. Im Zusammenspiel zwischen Trustcenter und der Verwendung solcher Karten, sind Anwendungen realisierbar, wie elektronische Dienstausweise, Arztkarten oder Anwendungen im sensiblen Finanzbereich, die bisher aus sicherheitstechnischen Erwägungen nicht realisiert werden konnten. Zusätzlich werden diese Karten im Bereich Mobilfunk zunehmend an Bedeutung gewinnen, bei der sich mit Hilfe sichere Authentisierung zum Beispiel Zugangskontrollen mit Hilfe eines Mobiltelefons realisieren lassen. Auch hier steht die ganze Palette der oben genannten Anwendungen prinzipiell zur

Verfügung und schafft mit seiner Unabhängigkeit von der direkten Anbindung an einen Rechner neue Nutzungsmöglichkeiten. Da hier zusätzlich Standortinformationen direkt vorliegen, sind speziell angepasste Servicefunktionen realisierbar.
Hochmoderne Karten lassen sich zunehmend mit vertrauten Entwicklungsumgebungen wie der Java – Programmiersprache ansteuern und entwickeln. Das verspricht eine breite Einsatzmöglichkeit und eine hohe Interoperabilität. Das Institut für Telematik beschäftigt sich mit der Entwicklung solcher Anwendungen unter Verwendung den neuesten Chipkartengenerationen. Es werden Testszenarien entworfen und neue Anwendungsfelder erschlossen. Die Kombination mit biometrischen Verfahren wird Gegenstand weiterer Forschungen sein.

6. Studie zum Spam-Problem

Die zunehmende Verbreitung des Internets und dessen Akzeptanz in der Bevölkerung haben es möglich gemacht, Informationen in einem bislang nicht gekannten Umfang zu verbreiten. Der Nutzen für die Bevölkerung ist offensichtlich. Es sind aber auch neue Gefahren entstanden, die berücksichtigt werden müssen. Unternehmen und Behörden sind zunehmend auf die Infrastruktur des Internets angewiesen. Es reicht bis in diese Organisationen und Institutionen hinein. Ein Ausfall der Infrastruktur führt in den meisten Fällen zu hohen Kosten. Ist die Nichtverfügbarkeit zudem noch von Datenverlusten begleitet, können irreparable Schäden entstehen, die ein Unternehmen in seiner Existenz bedrohen.

In der Vergangenheit haben der Melissa-Virus und einige seiner Nachfolger gezeigt, wie schnell bösartige Programme sich auf der ganzen Welt verteilen und Schaden anrichten können. Ein weiteres Beispiel war die Attacke auf die Web-Server von bekannten Unternehmen, die ihre Haupteinnahmen ausschließlich durch den Vertrieb von Produkten über ihre Präsenz im Internet bestreiten (eBay, Amazon u.a.). Das systematische Attakkieren von Web-Servern und anderen Internet-Diensten über sogenannten Distributed Denial-of-service-Attacken stellen eine der Hauptgefahren im Internet dar.

Im Rahmen einer Studie für die *Allianz Gesellschaft für Informatik Service mbH* (AGIS) in München wurden zunächst die Begriffe, die in diesem Zusammenhang verwendet werden, definiert. Dadurch konnte eine Basis für eine folgende Diskussion über Maßnahmen zur Abwehr der Gefahren geschaffen werden.

Die Studie, aus der ein Preprint hervorgegangen ist („Was Sie noch nie über Spam wissen wollten, aber gezwungen waren zu erfahren"), erläutert die Begriffe

- **Mailbombe**
- **Trojanische Pferde**
- **Viren**
- **Würmer**
- **Spam**
- **Spoofing**
- **Denial of Service (DoS)**
- **Distributed Denial of Service (DDoS)**

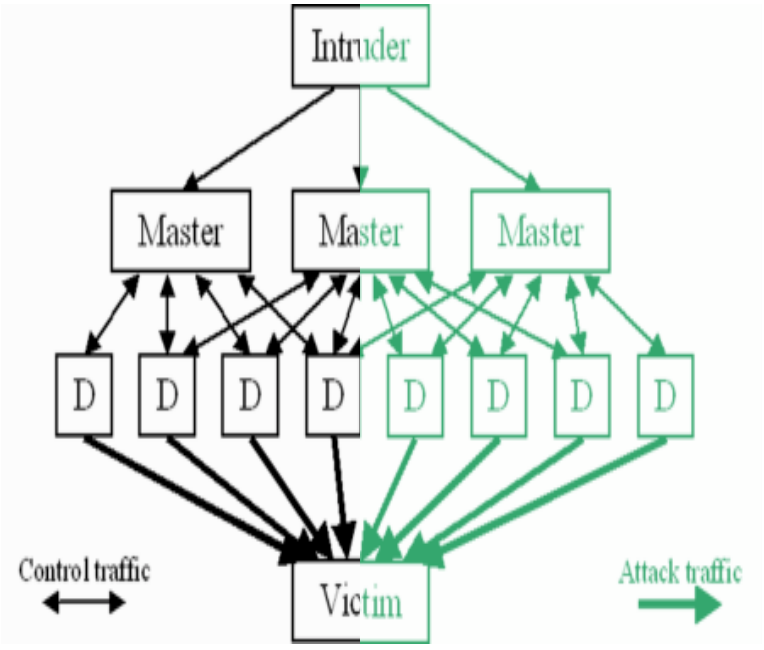


Abbildung: Funktionsweise eines DDoS

7. Projekt Website Management

Ausgangslage

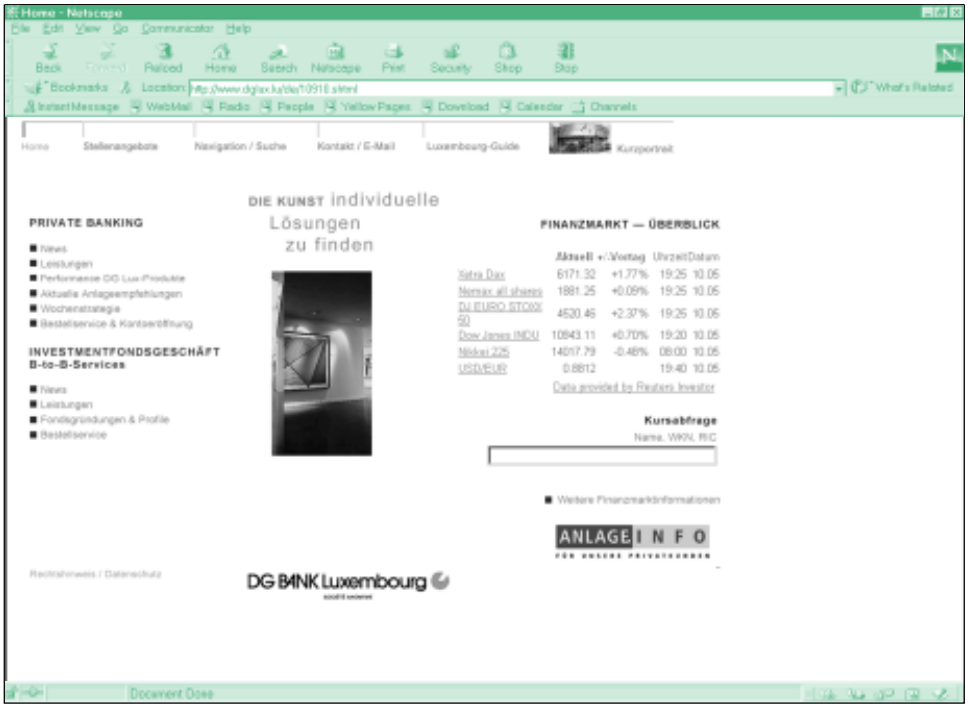
Im Rahmen des Auftrags einer Luxemburger Großbank zur Dynamisierung ihres Online-Auftritts wurde das vom Institut für Telematik entwickelte Redaktionssystem DAPHNE erweitert und angepasst. Darüber hinaus dienen JavaScript-Programme dazu, Kursdaten und News des Informationsproviders unmittelbar in die Unternehmens-Website zu integrieren.

Technologie

Das Redaktionssystem DAPHNE, ein Akronym für Distributed Authoring and Publishing of Hypertexts in Network Environments, bietet eine effektive Möglichkeit, Dokumente unterschiedlichen Typs zu erstellen, zu verwalten und für das Einstellen ins Internet vorzubereiten. Auf den Komfort vertrauter Programme muss nicht verzichtet werden. Ebenso ist ein verteiltes Arbeiten mehrerer Benutzer, gegliedert nach Rollen, möglich.

Im Rahmen des Luxemburger Großbank-Projekts wurden zahlreiche Fortschritte gegenüber der früheren Versionen des Programmpaktes erzielt. Link-Kontrollen wurden verbessert, Ressortstrukturen und Navigationselemente der neuen Website integriert.
Zudem wurde auf der Basis von JavaScript eine Schnittstelle für das Einlesen und Darstellen von Informationen eines großen Datenproviders angelegt.

Die künftige Entwicklung auf dem Sektor Online-Redaktionssysteme werden vom Nachfolgeprodukt JDAPHNE geprägt, einer reinen Java-Kodierung des Vorgängers DAPHNE. Hier sind ausgefeilte Mechanismen zum Hyperlink- und Ressortmanagement bereits integriert.

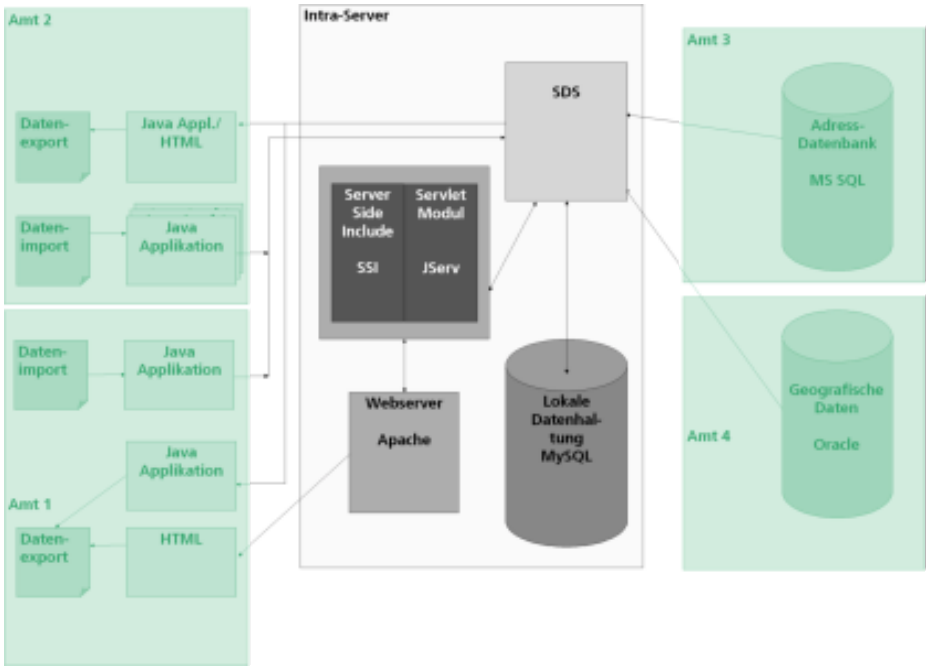


8. Smart Data Server (SDS) für kommunale Stadtverwaltung

Die IT-Strukturen in Behörden sind hochgradig heterogen. Die Gründe dafür sind einleuchtend: IT-Strukturen wachsen und ändern sich mit der Behörde. Im Wandel der Zeit werden neue Technologien eingesetzt, ohne die existierende Infrastruktur komplett ersetzen zu können. Investitionsschutz und Migrationkosten spielen dabei eine ausschlaggebende Rolle. Dabei werden die Anforderungen an die IT-Strukturen nicht weniger: Daten verschiedener Datenquellen müssen kombiniert werden, um Synergieeffekte ausnutzen zu können.
Eine allgemeingültige Lösung dieser Problematik ist nicht möglich, jede Lösung muss an die individuelle IT-Struktur angepasst werden.
Doch so unterschiedlich die Anforderungen auch sein mögen, es gibt Gemeinsamkeiten, die in einer Integrations-Plattform zusammengefasst werden können. Diese Integrations-Plattform ist Mittler zwischen den Informationsanbietern (i.a. Datenbanken) und den Informationskonsumenten und wird als „Middle-Tier" (Zwischenschicht) bezeichnet. Die am Institut für Telematik entwickelte Middle-Tier-Plattform „Smart Data Server" (SDS) zeichnet sich durch verschiedene Aspekte aus. Hier sind nur einige stichwortartig aufgelistet.

- Modularer Aufbau
- Einfaches Hinzufügen von problemorientierten Komponenten
- Zugriff der Komponenten auf die Server-Umgebung über Services
- Damit verbunden eine einfache Anpassung an verschiedene Einsatzumgebungen
- Netzwerke von SDS sind möglich zur Lasten-/Aufgaben-Verteilung

Im Rahmen eines Projektes mit einer kommunalen Stadtverwaltung wurde die SDS-Plattform zur Verknüpfung von Daten aus verschiedenen Ämtern konzipiert und implementiert. Dabei sollte einem bestimmten Amt (hier Amt 1) Daten dreier weitere Ämter (Amt 2, 3, 4) verfügbar gemacht werden, um durch deren Kombination Mehrwerte für das Amt zu erlangen. Die Daten aus Amt 2 lagen bis zu diesem Zeitpunkt nur unstrukturiert



in nicht-elektronischer Form vor. Um sie verfügbar zu machen, mussten Mechanismen geschaffen werden, diese Daten in eine neu geschaffene Datenbank einzupflegen. Exportmechanismen sollten es auch Amt 2 ermöglichen, auf die historisierten Daten zurückgreifen zu können, um neben dem Aufwand als Datenlieferant auch einen Nutzen zu erhalten.
Amt 3 und 4 stellten Daten zur Verfügung, auf die nur lesend zugegriffen werden sollte. Die Kombination von Adressdaten aus Amt 3 mit geografischen Daten aus Amt 4 versprach die größten Synergieeffekte. Aber auch Amt 1 selbst kann prinzipiell Datenlieferant sein. Zugriffe auf Daten können als Fallbeispiele für zukünftige Anfragen hinterlegt werden.
Mit dem SDS als Middle-Tier-Architektur war es möglich, eine auf Internet-Technologie basierende Struktur zu konzipieren, die den Zugriff auf Daten verschiedenster Ursprungsquellen transparent verfügbar macht und zwar über Standard-PC mit Standard-Programmen (Internet-Browser wie z.B. Netscape oder Internet-Explorer).

8. Telemedizin: I²RIS

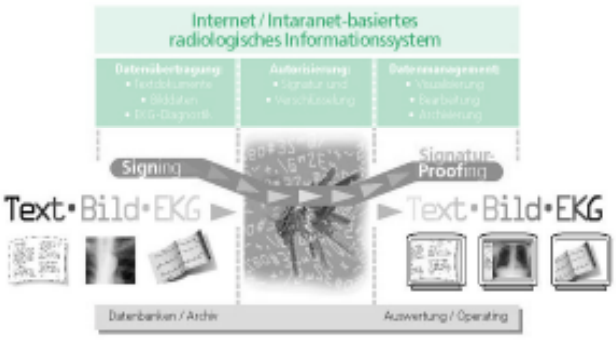
Problemstellung

Die modernen Kommunikationstechnologien erfordern im medizinischen Sektor anwendungstaugliche und effiziente Lösungen zum Austausch von vielfältigen visuellen Daten für Statistik, Begutachtung und Auswertung. Im Vordergrund stehen dabei die Internet-/Intranet-bezogenen Anwendungen für dieses gewaltige Anwendungsfeld.
Z.B. erfordert die moderne Bildübertragung eine effiziente Bildkompression bei höchstmöglicher Bildqualität als Bedingung für ein reibungsloses online-management für Medizinpraxis und Ausbildung.

I²RIS ein neues System für die Telemedizin

Intranet/Internet-basierte Anwendungen eröffnen weitreichende Möglichkeiten für Kommunikation und Datenvisualisierung. Viele beispielhafte Internet-Anwendungen haben gezeigt, dass mit geringem Aufwand benutzerfreundliche und mächtige Kommunikations-Systeme erstellt werden können.
Mit dem Internet/Intranet-orientierten radiologischen Informationssystem, kurz *I²RIS*, stellt das Institut für Telematik, Trier ein stabiles und einfach zu bedienendes System zur Übertragung, Visualisierung und Bearbeitung von medizinischem Bildmaterial im DICOM-Format vor. Mit Hilfe von *I²RIS* kann der Arzt mit allgemeinem Internet- bzw. Intranetzugang-Krankenhaus alle notwendigen Daten über einen Patienten aus dem DICOM-Archiv eines Krankenhauses bekommen. Dazu zählen insbesondere alle radiologischen Aufnahmen verschiedener DICOM-Modalitäten. So entstehen unschätzbare Vorteile durch die ortsunabhängige Arbeit für die Ärzte. Die Echtzeit-Konsultation via Internet mit weit entfernten Arztkollegen wird auf diesem Weg realisierbar. Darüberhinaus kann die digitale Kommunikation bis hin zum Patienten augedehnt werden, sofern dies sinnvoll, angemessen und praxisorientiert erfolgt. Technische Voraussetzung dafür ist der gewöhnliche Internetanschluss.
Das System *I²RIS* ist am Institut für Telematik entwickelt und auf der Basis von Standardnetzwerkprotokollen und unter Verwendung des DICOM-Standards konzipiert worden. Die Komponenten des Systems wurden in der plattformunabhängigen Programmiersprache Java implementiert. Denn das Systems orientiert sich an schon existierenden, offenen Standards. Die dadurch erreichten Vorteile des Systems liegen dabei auf der Hand :

- einfache Bedienung, schnelle Erlernbarkeit
- einfache Struktur, wartungsarm, kostengünstig
- hohe Übertragungsgeschwindigkeit
- sehr kurze Übertragungszeiten von großen Bildern
- praxiserprobte Sicherheitstechnik
- keine unberechtigten Zugriffe oder Manipulationen
- hohe Stabilität und
- hohe Betriebssicherheit des Systems



Der einzige spezifische Installationsvorgang betrifft den Web-Server, da auf ihm die spezifische *I²RIS*-Software installiert werden muss. Dabei wird eine Benutzerdatenbank mit Benutzerdaten sowie die Servlet- und Applet-Klassen, die die Datenverwaltung auf den DICOM-Modalitäten und die Kommunikation mit dem Client organisieren, installiert. Die Viewer-Software wird serverseits betrieben, so daß auf dem Client des Arztes lediglich ein Internet-Browser benötigt wird.

Der Bildbetrachter (Viewer) von *I²RIS* bietet alle im ärztlichen Alltag nötigen Funktionen (Kontrastierung, Vergrößern, Invertieren, Kommentierung u.a.) zur Bildbetrachtung und -bearbeitung. In nur ca. 15 Minuten läßt sich die bewußt einfach gehaltenen Anwendung auch von Computerneulingen erlernen.

Durch das neuartige und eigens am Institut für Telematik entwickelte Verfahren der Dateikomprimierung kann - ohne Minderung der Bildqualität auch für hochauflösende Graphiken eine hohe Übertragungsgeschwindigkeit erzielt werden.
Jede Datenübertragung zwischen Client und Server erfolgt aus Datenschutzgründen verschlüsselt, so dass alle patientenbezogenen Daten vor unberechtigter Einsichtnahme oder Manipulation geschützt sind. Zur Verschlüsselung wird ein asymmetrischer Kodierungsalgorithmus (RSA) verwendet. Der öffentliche Schlüssel wird nach Anfrage und erfolgreicher Überprüfung des Internet-Benutzers vom SSL-fähigen Web-Server generiert und getrennt vom Applet an den Browser übertragen. Zwar ist auch eine manuelle Überprüfung möglich, jedoch sollte idealerweise die Überprüfung persönlicher Daten des Internet-Benutzer automatisch mittels Zertifikatsmechanismus realisiert werden.
Bei jeder Authentifizierung und Sendung wird ein neues generiert, so dass eine hinreichend große Sicherheit vor unberechtigtem Zugriff garantiert wird. Passwort und Schlüssel, sowie die persönlichen Daten des Anwenders, werden in einer Benutzerdatenbank gespeichert, wobei das Administrationspersonal nur Einsicht in die Personendaten der User nehmen kann. Paßsswörter und Schlüssel können nur vom berechtigten User eingesehen und geändert werden.

DICOM Bilder

Personen Daten

EKG Auswertung

Trierer Symposien

Trierer Symposien

Regelmäßig veranstaltet das Institut für Telematik wissenschaftliche Symposien zu aktuellen Entwicklungen im Bereich der Telematik.

Das Institut für Telematik 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.

Durch die Vorstellung von konkreten Projekten, die ihren Forschungsschwerpunkt auf verschiedene Aspekte dieser Thematik gelegt haben, wird ein konstruktiver Austausch der Erfahrungen ermöglicht. Neben der sich an die Vorträge anschließenden Gelegenheit zur Diskussion hat sich der gemeinsame Informationsaustausch in entspannter Athmosphäre und während einem gemeinsamen Abendessen als äußerst positiv erwiesen.

Übersicht der Symposien seit Gründung des Instituts:

Telemedizin
8. und 9. Oktober 1998

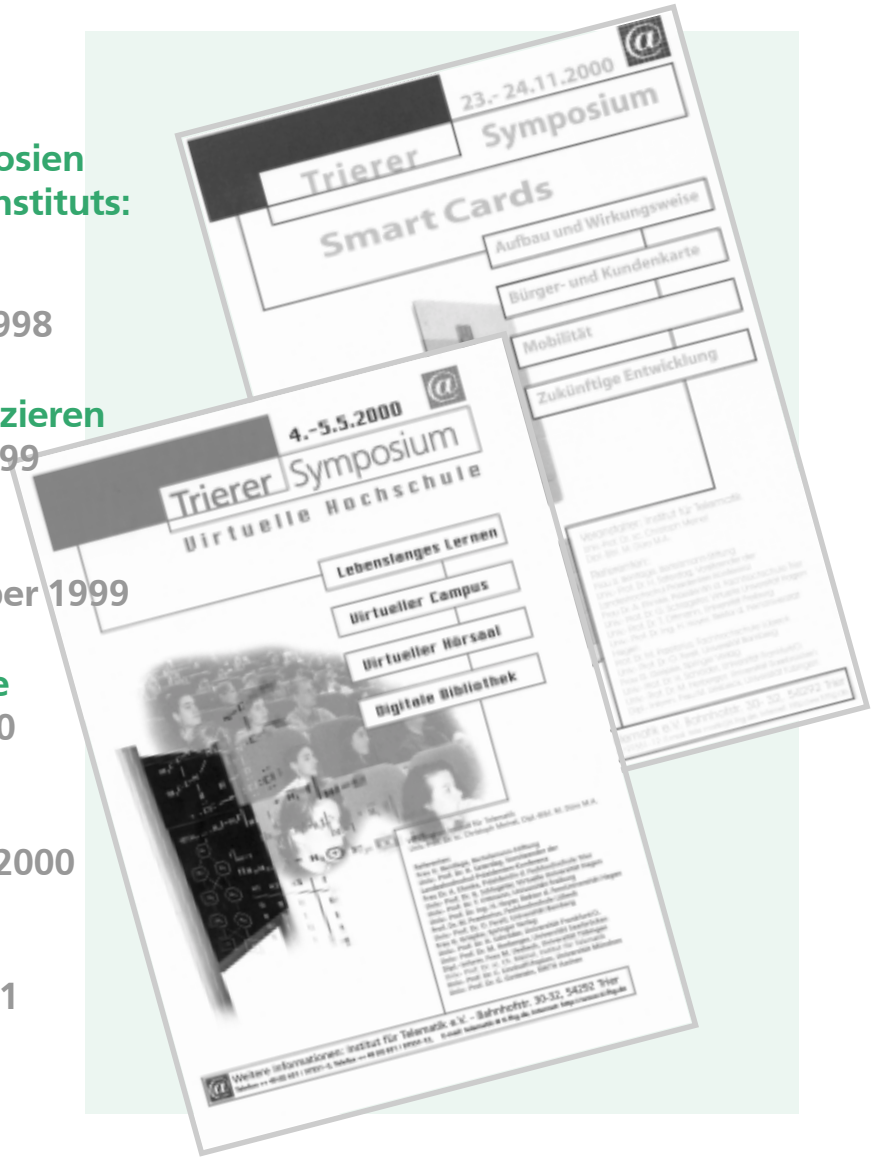
Elektronisches Publizieren
25. und 26. März 1999

Televerwaltung
11. und 12. November 1999

Virtuelle Hochschule
04. und 05. Mai 2000

Smart Cards
23. - 24. November 2000

Mobile Commerce
07. und 08. Juni 2001



08.-09.10.1998
Trierer Symposium

Telemedizin

Das Institut für Telematik richtete am 8. und 9. Oktober 1998 das „Trierer Telemedizin 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.

Folgende 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:

- Dr. G. Dietzel , Bundesgesundheitsministerium
- Prof. Dr. J. Dudeck, Institut für Medizinische Informatik, Justus-Liebig-Universität Gießen
- Dr. U. Engelmann, Deutsches Krebsforschungszentrum, Heidelberg
- Dr. S. Hludov, Institut für Telematik
- Prof. Dr. K. Kuhn, Universität Marburg und Leiter der GMDS-AG Krankenhausinformationssysteme
- Dr. G. Mann , GSF-Forschungszentrum für Umwelt und Gesundheit, München
- Dr. D. Mart , Luxembourg
- Dr. S. Müller, Institut für Telematik
- Prof. Dr. K. Pommerening , Johannes Gutenberg-Universität, Mainz , Leiter der GMDS-AG Datenschutz
- Dipl. Inform. J. Sembritzki, Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik Deutschland
- Dipl. Inform. C. Schröter, Institut für Telematik
- Dr. M. Skalej, Universitätsklinikum Tübingen

Die Programmschwerpunkte waren:

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

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 Potenziale der modernen Informations- und Kommunikationstechnik im Bereich des Elektronischen Publizierens diskutieren konnten.

Ziel des am 25. und 26. März ‘99 stattgefundenen 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 und
- Geschäftsmodelle

11.-12.11.1999
Trierer Symposium

Televerwaltung

Das Institut für Telematik wollte mit dem Trierer Symposium Televerwaltung ein Forum bieten, 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 Programmschwerpunkte 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

4. - 5.5.2000
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.
Durch die Vorstellung von konkreten Projekten, die ihren Forschungsschwerpunkt auf verschiedene Aspekte dieser Thematik gelegt hatten, wurde 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 Lebenslanges Lernen, Virtueller Campus, Virtueller Hörsaal und Digitale Bibliothek. Zu allen Programmschwerpunkten wurden führende Experten als Referenten eingeladen.

Eine detaillierte Auflistung der Gastreferenten und der Vortragsthemen beim Symposium Virtuelle Hochschule finden Sie auf den Seiten 45 - 46 unter der Rubrik:
(Gäste am Institut für Telematik 2000)

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" und „Künftige Entwicklungen". Zu allen Programmschwerpunkten wurden erneut führende Experten als Referenten eingeladen.

Eine detaillierte Auflistung der Gastreferenten und der Vortragsthemen beim Symposium Smart Cards finden Sie auf den Seiten 45 - 46 unter der Rubrik:
(Gäste am Institut für Telematik 2000)

Messeauftritte

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 2000 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; fehlt eine nähere Erklärung, so ist bei einer früheren Messen nachzuschauen.

Online 2000

In Düsseldorf fand vom 31.1. bis 3.2. die Online 2000 statt. Das TI war mit folgendem Exponat präsent:

Lock-Keeper: High Security-Datenaustausch zwischen Intranet und Internet

Wenn die Sicherheitsbedürfnisse eines Unternehmens zum Austausch von Daten über das Internet die Möglichkeiten klassischer Firewalls übersteigen, empfiehlt sich der Einsatz vom Lock-Keeper, 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 einer Seite der Kommunikationsteilnehmer statt.

CeBIT 2000

In Hannover fand vom 24.2. bis 1.3. die CeBIT statt.
Das TI war mit folgenden Exponaten vertreten:

Information Broker: internetbasiertes Portfoliomanagement: Intelligentes Datenmanagement mit dem Smart Data Server (SDS)

Heterogene Datennetze und Datenbankanbindungen bestimmen die heutige IT-Landschaft. Zum effizienten Handling des Informationsflusses stellt der Smart Data Server (SDS) als Framework für verteilte Anwendungen eine Plattform bereit, um unterschiedliche Anforderungen modular, flexibel und skalierbar zu ermöglichen.

Intelligentes Hyperlink-Management
Die Verwaltung von Hyperlinks großer Web-Sites ist äußerst schwierig. Ebenso stellt auch das Erstellen neuer, sinnvoller Links ein Problem dar. Unser intelligentes Hyperlink-Management-System bietet Hilfe zum Auffinden von Broken-Links und zur Konsistenzerhaltung von Links. Neu ist die Möglichkeit, Link-Vorschläge zu Dokumenten automatisch generieren zu lassen. Das System unterstützt neben Mehrsprachigkeit auch das Versionsmanagement von Sites. Durch die interne Trennung von Dokumentenpool und Meta-Daten können neue Funktionalitäten einfach in das System integriert werden.

Medica 2000

In Düssedorf fand vom 22. bis 25.11.2000 die Medica statt.

Intranet im Krankenhaus: offene Standards und modulare Systeme

Die Bedeutung von Intranet im Krankenhaus nimmt immer weiter zu. Auf dem Weg in die Informationsgesellschaft haben auch kleinere Krankenhäuser die Potenziale des Intranets erkannt. Das Intranet dient zum einen als Informationsforum, zum anderen unterstützt es die flexible Integration mit offenen Standards und modulare Systemen. Offene Standards ermöglichen die Kommunikation zwischen den verschiedenen Servern und modularen Systemen. Die Integration zwischen den verschiedenen Teilsystemen kann durch Kommunikationsserver realisiert werden.

Trust Center – Multifunktionskarten für die Finanzindustrie

Die Entwicklung neuer, billiger und leistungsfähiger Mikroprozessorchips und miniaturisierter Speicherbausteine mit großem Speicherbereich bietet eine Grundlage für multiple Applikationsszenarien. Die in dieser Karte eingesetzte Sicherheitstechnik auf höchstem Sicherheitsniveau bildet das fehlende Element für sicheren, d.h. rechtsverbindlichen, elektronischen Daten-, Zahlungs- und Geschäftsverkehr im Internet. Neben der digitalen Signatur und den elektronischen Zahlungsfunktionen können zusätzliche lokale Anwendungen, wie z.B. Ausweisfunktionen, Telefonfunktion u.a., auf den Chip geladen werden.

Lock-Keeper: High Security-Datenaustausch zwischen Intranet und Internet

Siehe Text: Online 2000 auf nebenstehender Seite

DICOM-Viewer: Java basierte Implementierung von Übertragungs- und Visualisierungsverfahren für DICOM-Bilder

Der Zweck des Intranet-/Internet-basierten, radiologischen, modularen Informationssystems für Kliniken, Krankenhäuser und niedergelassene Ärzte ist der interne und externe Zugriff auf alle DICOM-Daten, die von den verschiedenen bildgebenden Abteilungen produziert und archiviert werden. Dieser Zugriff wurde durch den DICOM-Standard und die Verwendung der modernen plattformunab-hängigen Programmiersprache Java und der Intranet-/Internet-Technologie erreicht. Die Hauptkomponente des Systems bildet ein PACS. Ein PACS besteht aus bildgebenden Modalitäten, einem Archivierungssystem und miteinander in Verbindung stehenden PCs.

Der Kern des Archivierungssystems ist eine relationale Datenbank für Patientendaten mit zugehörigem Dateisystem für die Bilder.

I²RIS - Ein neues System für die Telemedizin

Mit dem **I**nternet/**I**ntranet- orientierten **r**adiologischen **I**nformations**s**ystem, kurz I²RIS, stellt das Institut ein neuartiges, stabiles und leicht zu bedienendes System zur Übertragung, Visualisierung und Bearbeitung von medizinischem Bildmaterial im DICOM Format vor. Mit Hilfe von I²RIS kann der Arzt, der über einen Zugang zum Internet (oder zum Intranet des Krankenhauses) verfügt, alle notwendigen Daten über einen Patienten, inklusive aller radiologischen Aufnahemn, von den verschiedenen DICOM Modalitäten oder aus dem DICOM Archiv eines Krankenhauses erhalten.
Das System wurde auf der Basis von Standardnetzwerkprotokollen und unter Verwendung des DICOM Standads konzipiert. Die Komponenten des Systems wurden in der plattformunabhängigen Programmiersprache JAVA implementiert. Der einzige spezifische Installationsvorgang betrifft den Webserver, auf dem die I²RIS Software installiert werden muss.

Publikationen & Vorträge

Mitarbeiter des Instituts für Telematik traten 2000 mit zahlreichen Publikationen und Vorträgen an die Öffentlichkeit. Das Institut nutzt 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 2000

Veröffentlichungen in Tagungsbänden

Mitarbeiter des Instituts für Telematik haben im Jahre 2000 mit Vorträgen zu verschiedenen Themen an internationalen Konferenzen, Symposien und Workshops teilgenommen. Das Institut war unter anderem auf folgenden Veranstaltungen aktiv vertreten:

- 13th IEEE CBMS'2000, Houston, Texas, USA, 2000
- 1st IEEE International Conference on Management of Innovation and Technology, ICMIT'2000, Singapore, Malaysia, 2000
- 1st International Conference on Internet Computing, IC'2000, Las Vegas, Nevada, USA, 2000
- 4th IEEE International Enterprise Distributed Computing Conference, EDOC'00, Makuhari, Japan, 2000
- ACM SIGUCCS Fall 2000 User Service Conference, Richmond, Virginia, USA, 2000
- Applied Informatics, IASTED AI2000, Innsbruck, Austria, 2000
- CACIC 2000, Ushuaia, Argentinien, 2000
- Computer Graphics, Visualization and Interactive Digital Media'2000, Plzen - Bory, Czech Republic, 2000
- CRIS'2000, Helsinki, Finnland, 2000
- ECIS'2000, Wien (Österreich), 2000
- GI Jahrestagung, Berlin, 2000
- IEEE/ACM IWLS'2000, Dana Point, USA, 2000
- Informatiktage 2000, Fachwissenschaftlicher Informatik-Kongress, Bad Schussenried, Deutschland, 2000
- International Conference on Advances in Information Systems, ADVIS'2000, LNCS1909, Izmir, Türkei, 2000
- International Conference on Electronic Commerce and Web-Applications, EC-Web00, LNCS1875, Greenwich, Großbritannien, 2000
- International Conference on Internet Computing, IC00, Las Vegas, Nevada, 2000
- MEDICOM 2000, Remagen, Deutschland, 2000
- ONLINE'2000, Düsseldorf, Deutschland, 2000
- SPIE's International Symposium on Medical Imaging, San Diego, USA, 2000
- Symposium on Applied Computing, ACM SAC2000, Como, Italien, 2000
- Visual Communications and Image Processing (VCIP) 2000, 20-23 June 2000, Perth, Austra lien, 2000
- WISE'2000, Hong Kong, China, 2000
- World Conference on the WWW and Internet, AACE WebNet 2000, San Antonio, USA, 2000

Titel der Vorträge

C. Qu, T. Engel, Ch. Meinel
Implementation of a WebDAV-based Collaborative Distance Learning Environment
ACM SIGUCCS Fall 2000 User Services Conference, Richmond, (Virginia, USA), 2000.

A. Heuer, F. Losemann, Ch. Meinel
Signed Preservation Of Online References
World Conference on the WWW and Internet, AACE WebNet 2000, San Antonio, (Texas, USA), 2000.

C. Qu, T. Engel, Ch. Meinel
Implementation of a Document Management System Based on WebDAV Protocol
1st IEEE International Conference on Management of Innovation and Technolgoy (ICMIT'2000), Singapore, 2000.

U. Roth, A.Heuer. E.-G. Haffner, Ch. Meinel
A Search-Engine-Topology to Improve Document Retrieval on the Web
World Conference on the WWW and Internet, AACE WebNet 2000, San Antonio, (Texas, USA), 2000.

E.-G. Haffner, U. Roth, A. Heuer, T. Engel, Ch. Meinel
Link Proposals with Case-Based Reasoning Techniques
World Conference on the WWW and Internet, AACE WebNet 2000, San Antonio, (Texas, USA), 2000.

M. Podesta, Ch. Meinel
Integration of a Public Key Infrastructure in a Virtual University
CACIC 2000, Ushuaia (Argentinien), 2000.

C. Qu, T. Engel, Ch. Meinel
Implementation of an Enterprise-level Groupware System Based on J2EE Platform and WebDAV Protocol
4th IEEE International Enterprise Distributed Computing Conference EDOC'00, Makuhari (Japan), 2000.

L. Vorwerk, Ch. Meinel
Integration of TLS in an Intern/Intranet/based Application
MEDICOM 2000, Remagen, (Germany), 2000.

E.-G. Haffner, U. Roth, A. Heuer, T. Engel, Ch. Meinel
What do Hyperlink-Proposals and Request-Prediction have in Common?
First Biennial International Conference on Advances in Information Systems ADVIS'00, Izmir (Turkey), 2000.

E.-G. Haffner, U. Roth, A. Heuer, Ch. Meinel
Advanced Studies on Link Proposals and Knowledge Retrieval of Hypertexts with CBR
1st International Conference on Electronic Commerce and Web Technologies EC-Web 2000, Greenwich, (United Kingdom), 2000.

A. Heuer, F. Losemann, Ch. Meinel
Logging and Signing Document Transfers on the WWW - A Trusted Third Party Gateway
1st International Conference on Web Information Systems Engineering, WISE'2000, Hong Kong (China), 2000.

E.-G. Haffner, T. Engel, Ch. Meinel
Integration der Schleusentechnik „Lock-Keeper" in moderne Sicherheitsarchitekturen
GI-Jahrestagung Informatik 2000, Workshop: „Sicherheit in Mediendaten", Berlin (Germany), 2000.

Z. Zhang, T. Engel, U. Roth, Ch. Meinel
Web Site Design Using a Web-Based Authoring and Publishing System
1st International Conference on Internet Computing, IC'2000, Las Vegas (Nevada, USA), 2000, pp. 113-118.

A. Heuer, E.-G. Haffner, U. Roth, Ch. Meinel
A Hyperlink Focused Browse Assistent for the World Wide Web
1st International Conference on Internet Computing, IC'2000, Las Vegas (Nevada, USA), 2000, pp. 79-84.

E.-G. Haffner, U. Roth, A. Heuer, T. Engel, Ch. Meinel
Advanced Techniques for Analyzing Web Server Logs
1st International Conference on Internet Computing, IC'2000, Las Vegas (USA), 2000, pp. 71-78.

Ch. Meinel, A. Wagner
WWW.BDD-PORTAL.ORG
IEEE/ACM IWLS'2000, Dana Point (USA), 2000.

B. Lüpken, F. Losemann, T. Engel, Ch. Meinel
Functional Integration Test of Mass Processes with Electronic Signatures in Public Administrations
European Conference on Information Systems, ECIS'2000, Wien (Österreich), 2000.

L. Vorwerk, T. Engel, Ch. Meinel
A Proposal for a Combination of Compression and Encryption
SPIE Visual Communications and Image Processing, Perth (Australia), 2000.

S. Khludov, L. Vorwerk, Ch. Meinel
Internet-Orientated Medical Information System for DICOM-Data Transfer, Visualization and Revision
13th IEEE CBMS'2000, Houston (Texas, USA), 2000, 293-296.

L. Vorwerk, Ch. Meinel
A Multimedia-Editor for Making Findings in Radiology
13th IEEE CBMS'2000, Houston (Texas, USA), 2000, pp. 297-302.

Ch. Meinel, Ch. Stangier
Speeding Up Image Computation by using RTL Information
FMCAD'2000, Austin (Texas, USA), 2000.

H. Sack, Ch. Meinel
Functional Extension of Decision Diagrams in Practice
FMTOOLS'2000, Reisenburg (Germany), 2000, pp. 195-196.

Ch. Meinel, Ch. Stangier
Accelerating Techniques for OBDD-based Formal Verification of Sequential Systems
FMTOOLS'2000, Reisenburg (Germany), 2000, pp. 129-134.

E.-G. Haffner, U. Roth, T. Engel, Ch. Meinel
Modeling of Time and Document Aging for Request Prediction - One Step Further
ACM Symposium on Applied Computing, SAC'2000, Como (Italy), 2000.

Ch. Meinel, A. Wagner
WWW.BDD-PORTAL.ORG - A Basis for Cooperative Research in EDA
CRIS'2000, Helsinki (Finland), 2000.

E.-G. Haffner, U. Roth, T. Engel, Ch. Meinel
Optimizing Requests for the Smart Data Server
Applied Informatics, IASTED, AI'2000, Innsbruck (Austria), 2000.

L. Vorwerk, F. Losemann, T.Engel, Ch. Meinel
Constructing a Secure HIPACS with Structured Reporting
SPIE - Medical Imaging 2000, San Diego (USA), 2000.

L. Vorwerk, S. Khludov, Ch. Meinel
Concept for Increased Security for Internet/Intranet-Based Administration of Patient Data
WSCG'2000, Plzen (Czech Republic), 2000.

Ch. Meinel, L. Vorwerk, T. Engel
Trustcenter und Multifunktionskarten
ONLINE'2000, Düsseldorf (Germany), 2000, pp. C410.03 - C410.12.

H. Sack, E. Dubrova, Ch. Meinel
Representation of Multiple-Valued Functions with Mod-p Decision Diagrams
IEEE IWLS'2000, Dana Point (California, USA), 2000, pp. 341-348.

Ch. Meinel, A. Wagner
WWW.BDD-PORTAL.ORG
IEEE IWLS'2000, Dana Point (California, USA), 2000, pp. 349-353.

H. Sack, E. Dubrova, Ch. Meinel
Mod-p-DDs: A Data-Structure for Multiple-Valued Functions
30th IEEE ISMVL 2000, Portland (Oregon, USA), 2000

Ch. Meinel, A. Wagner
WWW.BDD-PORTAL.ORG - An Electronical Basis for Cooperative Research in EDA
CRIS 2000, Helsinki (Finland), 2000

Herausgeberschaft und Mitherausgeberschaft an Proceedingsbänden

Ch. Meinel, L. Gollan (Eds.)
„Smart Cards"
Proceedings Trierer Symposium „Smart Cards", Trier, Institut für Telematik, ISSN 1433-8106, 2000.

Ch. Meinel, M. Düro (Eds.)
„Virtuelle Hochschule"
Proceedings Trierer Symp. „Virtuelle Hochschule", Trier, Institut für Telematik, ISSN 1433-8106, 2000.

Ch. Meinel, M. Lawo, F. Veit, M. Suilmann (Eds.)
„Telekommunikation - Sicherheit & Security Management"
Proceedings ONLINE'2000, Congress IV, Düsseldorf, ONLINE-Verlag, Velbert, ISBN 3-89077-209-9, 2000.

Ch. Meinel, O. Bendel (Eds.)
„Televerwaltung"
Proceedings Trierer Symposium Televerwaltung, Trier, Institut für Telematik, ISSN 1433-8106, 1999.

Ch. Meinel, S. Tison (Eds.)
„16th Annual Symosium on Theoretical Aspects of Computer Science"
Proceedings STACS 1999, Trier, Germany, 1999, LNCS Vol. 1563, Springer-Verlag, Heidelberg, New York, 1999.

M. Morvan, Ch. Meinel, D. Krob (Eds.)
„15th Annual Symposium on Theoretical Aspects of Computer Science"
Proceedings STACS 1998, Paris, France, 1998, LNCS Vol. 1373, Springer-Verlag, Heidelberg, New York, 1998.

Ch. Meinel, S. Müller (Eds.)
„Internet-Technologie in der Medizin"
Proceedings Trierer Telemedizin Symposium, Trier, Institut für Telematik, ISSN 1433-8106, 1998.

Veröffentlichungen in Zeitschriften

Ch. Meinel
Mod2OBDDs - a BDD Structure for Probalistic Verification
ENTCS 22 (2000).

Ch. Meinel, F. Somenzi, T. Theobald
Linear Sifting of Decision Diagrams and ist Application in Synthesis
IEEE Transactions on CAD, Vol. 19 (2000), No. 5, 521-533.

Ch. Meinel, T. Theobald:
Local Encoding Transformations for Optimizing OBDD-Representations of Finite State Machines
Formal Methods in System Design (2000)

Technische Berichte des Instituts
für Telematik, ISSN 1433-8106

Preprint 2000-01
Redaktionssystem DAPHNE
Zhongdong Zhang, Andreas Heuer, Zuo, Thomas Engel, Christoph Meinel

Preprint 2000-02
Die Lock-Keeper-Architektur
Ernst-Georg Haffner, Thomas Engel, Christoph Meinel

Preprint 2000-03
Techniques for Securing Networks against Criminal Attacks
Ernst-Georg Haffner, Thomas Engel, Christoph Meinel

Preprint 2000-04
Was Sie noch nie über Spam wissen wollten, aber gezwungen waren zu erfahren
Uwe Roth, Christoph Meinel

Preprint 2000-05
Trierer Symposium Virtuelle Hochschule. Proceedings
Christoph Meinel, Michael Düro

Preprint 2000-06
Trierer Symposium Virtuelle Hochschule. Abstracts
Christoph Meinel, Michael Düro

Preprint 2000-07
Trierer Symposium Smart Cards. Abstracts
Christoph Meinel, Lutz Gollan

Preprint 2000-08
Electronic Signatures. - An American and European Perspective -
Lutz Gollan, Christoph Meinel

Preprint 2000-09
Modell für den Einsatz von Java Cards im Gesundheitswesen
Lutz Vorwerk, Frank Losemann, Thomas Engel, Christoph

Preprint 2000-10
Mobile commerce
Ali Marbrouk, Christoph Meinel, Thomas Engel

Preprint 2000-11
Das Patienten-CD System
Sergej Khludov, Christoph Meinel, Gevantmakher

Preprint 2000-12
Trierer Symposium Smart Cards. Proceedings
Christoph Meinel, Lutz Gollan

Preprint 2000-13
The Necessity of a Public Key Infrastructure for a Virtual University
Marianna Podesta, Christoph Meinel

Preprint 2000-14
Integration der Schleusentechnologie Lock-Keeper™ in moderne Sicherheitsarchitekturen
Ernst Georg Haffner, Thomas Engel, Christoph Meinel

Preprint 2000-15
Security in Open Networks: The Functionality of a Public Key Infrastructure
Bernd Dusemund, Torsten Becker, Lutz Gollan, Thomas Engel, Christoph Meinel

Patente

Um die innovative fachliche Leistungskraft des Instituts für Telematik unter Beweis zu stellen, wurden zwei Entwicklungen auf dem Gebiet der Sicherheit offener Netze bzw. der Telemedizin zum Patent angemeldet, die mittlerweile erteilt wurden. Dabei handelt es sich zum einen um die

- *Datenverbindung zwischen zwei Rechnern und Verfahren zur Datenübertragung zwischen zwei Rechnern („Lock-Keeper")*

(Patentnummer: 198 38 253),

und zum anderen um ein

- *Verfahren zum Komprimieren eines digitalen Bildes mit mehreren Bitebenen*

(Patentnummer: 199 44 213) für die internetbasierte medizinische Bildkommunikation.

Vorträge 2000

19.01.2000
Christoph Meinel
Vorstellung des Instituts für Telematik

26.1. 2000
Dipl.-Inform. Lutz Vorwerk
Constructing a secure HIPACS with Structured Reporting

26.1.2000
Dipl.-Inform. Lutz Vorwerk
Concept for increased Security for Internet/Intranet - based Administration of Patient Data

31.01.2000
Christoph Meinel
Trustcenter und Multifunktionskarten

16.2.2000
Dipl. Wirtsch.-Ing. Carsten Radke
Aktivitäten im Web: Aktuelles, Auswertung der Statistiken, Redaktionssystem, neue Ideen.

18.02.2000
Christoph Meinel
Telematik - eine junge Wissenschaftsdisziplin

20.2.2000
Michael Schommer
CrytoKit - eine Java-Bibliothek kryptographischer Primitive

21.2.2000
Eugeni Lutschichin
TCP/IP-basiertes Kommunikationssystem mit integriertem Zeitstempeldienst

21.2.2000
Michael Schommer
CryptoKit-Talk, verschlüsselt kommunizieren übers Internet

17.03.2000
Christoph Meinel
BDDs - State-of-the-Art Data Structures for Boolean Functions

20.3.2000
Michael Düro, M.A.
Aufbau einer Digitalen Bibliothek mit Online-Redaktionssystemen

22.3.2000
Dipl.-Inform. Xiaping Zuo
Web-based Support for the Writing of a Report in an Organization

29.3.2000
Dipl. Inform Uwe Roth
Spam, Spam, Spam, Eggs and Spam

30.03.2000
Christoph Meinel
Institut für Telematik - Forschungs- und Entwicklungsprojekte

18.04.2000
Christoph Meinel
Notwendigkeit und Aufgaben eines Luxembourger Trust Centers

04.05.2000
Christoph Meinel
Eröffnungsvortrag Trierer Symposium "Virtuelle Hochschule"

22.05.2000
Christoph Meinel
BDD-basierte Datenstrukturen im Schaltkreisentwurf

26.05.2000
Christoph Meinel
WWW.BDD-Portal.Org - An Electronical Basis for Cooperative Research in EDA

31.5.2000
Dipl.-Ing. Paul Ferring
Voice over IP

7.6.2000
Dipl.-Inform Lutz Vorwerk
A Proposal for a Combination of Compression and Encryption

8.6.2000
Christoph Meinel
WWW.BDD-Portal.Org

21.06.2000
Christoph Meinel
Rechenschaftsbericht Institut für Telematik

Juni 2000
Christoph Meinel
Internet-Orientated Medical Information System for DICOM-Data Transfer, Visualization and Revision
13th IEEE CBMS' 2000, Houston/USA,

Juni 2000
Christoph Meinel
A Multimedia-Editor for Making Findings in Radiology

Juni 2000
Christoph Meinel
Smart Cards - The Personal Safe in an E-Commerce World

12.7.2000
Dipl.-Inform. Ernie Haffner
Modeling Time and Document Aging for Request Prediction

18.07.2000
Harald Sack
Development of an Mod2-OBDD package/ Accelerating OBDD minimization by Sampling/ Iterative Synthesis with OBDDs of Different Variable Orders

08.08.2000
Christoph Meinel
Vorstellung des Instituts für Telematik

16.8.2000
Florence Absolum, M.A.
Erlangung interkultureller Kompetenzen: ein neuer Weg

30.8.2000
Dipl.-Phys. Oliver Baldus
Holographische Datenspeicherung mit photoadressierbaren Polymeren

12.09.2000
Christoph Meinel
BDD-based Data Structures in VLSI

13.9.2000
Dipl.-Math. oec. Torsten Becker
Optimierung über der effizienten Menge eines Mehrzieloptimierungsproblems

27.9.2000
Zheng Liu
Vorstellung

3.10.2000
Christoph Meinel
Institute of Telematics - Research and Development Activities

18.10.2000
Dr. iur. Lutz Gollan
Private Sicherheitsdienste in der Risikogesellschaft

28.10.2000
Harald Sack
Implementation of a WebDAV-based Collaborative Distance Learning Environment

10.11.2000
Christoph Meinel
Rechenschaftsbericht des Instituts für Telematik

15.11.2000
Dipl.-Inf. Kais Louizi
Design und Entwicklung eines XML-basierten CORBA Test-Clients für den Einsatz in der Prozeß-automatisierung

15.11.2000
Christoph Meinel
Implementation of a Document Management System Based on WebDAV Protocol

23.11.2000
Christoph Meinel
Einführungsvortrag

24.11.2000
Dr. Bernd Dusemund
Smartcards und ihre Verwendung in einem Trust-center

28.11.2000
Christoph Meinel
BDD-basierte Datenstrukturen für sequentielle Schaltkreise

20.12.2000
Christoph Meinel
Trust Center-Infrastructure, Specifications and Standards

Gäste am Institut für Telematik 2000

Dipl.-Ing. Markus Ullmann,
BSI, Bonn
Online-Zugriffe, wenn die Grenzen der Lockkeeper-Architektur erreicht sind

Ulrike Bentlage,
Bertelsmann-Stiftung
Studium Online: Ein Szenario für das Jahr 2005

Ministerialdirigent Dr.Peter Krug,
Mainz
Lebenslanges Lernen als Motor eines sich verändernden Bildungssystems

Univ.-Prof. Dr. Helmut Hoyer,
FernUniversität Hagen
Die FernUniversität auf dem Weg zur Virtuellen Universität

Prof. Dr. Michael Praetorius,
FH Lübeck
Das Bundesleitprojekt Virtuelle Fachhochschule

Univ.-Prof. Dr. Otto K. Ferstl,
Universität Bamberg
Die Virtuelle Hochschule Bayern

Univ.-Prof. Dr. Thomas Ottmann,
Universität Freiburg
The Virtual University in the Upper Rhine Valley

Prof. Dr. Paul Müller,
RHRZ Kaiserslautern
Das Projekt Virtueller Campus Rheinland-Pfalz

Univ.-Prof. Dr. Hartmut Schröder,
Universität Frankfurt/Oder
"Widok" - Ein virtuelles Doktorandenkolloquium im Internet zum Forschungsbereich "Interkulturelle Kommunikation"

Dipl.-Inf. Mechthild Uesbeck,
Universität Tübingen
Ein Kompaktsystem zur Generierung Web-basierter Trainings-Systeme fuer die Aus- und Weiterbildung - vorgestellt am Tübinger Medizin-System MURMEL

Univ.-Prof. Dr. Maximilian Herberger,
Universität Saarbrücken
Das internationale Online-Seminar: Erfahrungen und Perspektiven

Univ.-Prof. Dr. Claudia Linnhoff-Popien,
Universität München
LMU München - RWTH Aachen: Die Vorlesung Telekommunikationssysteme

Dr. Reginald Ferber,
FernUniversität Hagen
Das CUBER Projekt: Kursbroker in einem Netz europäischer Fern-Universitäten

Univ.-Prof. Dr. Günter Gottstein,
Universität Aachen
Das multimediale Lehrbuch Werkstoff-wissenschaften

Dipl.-Inf. Harald Sack,
Geschäftsführer WEP Trier
Electronic Colloquium on Computational Complexity - ECCC

Gudrun Griepke,
Springer Verlag
LINK: Elektronisches Publizieren in einem wissenschaftlichen Verlag

Wim Kuling,
Zorg en Zekerheid, Leiden/Niederlande
Parkinson Card

Dipl.-Inf. Jürgen Sembritzki,
ZTG Krefeld
ISO WG 5: Health Cards

Dr. Christoph Sutter,
TÜV Informationstechnik GmbH, Essen
Evaluierungen von Smart Cards

Dr. Martin Merck,
Sun Microsystems GmbH München
Java Cards

Hansjörg Röhrich,
RMV, Hochheim/Ts.
WAYflow und MobiChip

Dr. Ulrich Sporn,
T-Mobil, Bonn
Chipkarten im Mobilfunk - Entwicklungen und Trends

Dr. Harald Ahrens,
Curiavant Internet GmbH, Nürnberg
Das MEDIA@Komm-Projekt in der Region Nürnberg: Die Entwicklung und Einführung des Anwohnerparkausweises - erste Erfahrungen aus der Praxis

Walter Nink, Oberamtsrat,
Universität Trier
Die multifunktionale Chipkarte als Studienausweis der Universität Trier

Dr. Rainer Ulrich,
Fraunhofer - Institut für integrierte Schaltungen, Erlangen
Flexible, drahtlose multifunktionale Chipkarten - und was dann?

Dr. Franz Weikmann,
Giesecke & Devrient GmbH, München
Multifunktionale Chipkarten - Technik und Anwendungen

Prof. Dr. Arndt Bode,
Institut für Informatik Lehrstuhl für Rechnertechnik und Rechnerorganisation TU München
Architekturen für das Hochleistungsrechnen: Stand und Entwicklungslinien

Pressespiegel

Pressespiegel

UNIJOURNAL, Jahrgang 26 / 2000, Heft Nr. 2

Wissenschaftstag am Institut für Telematik

Hochkarätige Internet-Forschung in Trier: Präsentation der Projekte auf der CeBIT 2000

TRIER. Ursprünglich als Wissenschaftsnetz konzipiert, hat sich das Internet durch die Einführung multimedialer Übertragungsprotokolle inzwischen zu einem gigantischen Kommunikationsmedium entwickelt, das auch von kommerziellen Unternehmen, Dienstleistern, Industrie und Handel kräftig genutzt wird. Forschungs- und Entwicklungsarbeiten rund um die Internet-Technologie, wie sie am von Prof. Dr. Christoph Meinel geleiteten Trierer Institut für Telematik e. V. unter Betreuung der Fraunhofer Gesellschaft betrieben werden, sind darum hochaktuell und von unmittelbarer praktischer Bedeutung. In einer Forschungsnachlese '99, dem „TI-Wissenschaftstag", werden Forschungsprojekte des Instituts vorgestellt, die im Jahre 1999 Aufnahme in das wissenschaftliche Programm so renommierter internationaler Fachkongresse gefunden haben, wie etwa die WebNet '99 in Honolulu, ACM-SigDoc'99 in New Orleans, IMSA'99 und SIP'99 in Nassau, ASIS'99 in Washington, AP-Web'99 in Hongkong oder CARS'99 in Paris. Weiterhin wurden die Projekte auf der CeBIT 2000 präsentiert.
Der Wissenschaftstag fand am 23. März 2000 ab 14.00 Uhr in den Konferenzräumen des Instituts für Telematik in Trier statt. Vorgestellt wurden Beiträge zu den Themen
- Digitale Bibliotheken und Portale im Internet
- Online-Redaktion und Hyperlink-Management; Navigation im WWW; Neue Browser-Assistenten
- Smart Data Server – eine neue Server Architektur
- Lock-Keeper und Informationssicherheit
Komprimierung und Übertragung medizinischer Bilder

Straubinger Tagblatt, 20.04.2000

Informatik Studenten rechnen immer schlechter

Die Mathematik-Kenntnisse angehender Informatiker und Naturwissenschaftler lassen nach. „Das Niveau ist seit ungefähr zehn Jahren rückläufig", sagte der Leiter des von der Frauenhofer-Gesellschaft verwalteten Instituts für Telematik, Christoph Meinel. Viele Studenten hätten schon mit Bruchrechnen Probleme. „Das Vermitteln strukturierten und analytischen Denkens kommt in der Schule zu kurz."

Bonner Generalanzeiger, 20.04.2000

Mathe-Kenntnisse lassen seit zehn Jahren nach

TRIER. Die Mathematik-Kenntnisse angehender Informatiker und Naturwissenschaftler lassen nach. „Das Niveau ist seit ungefähr zehn Jahren rückläufig", sagte der Leiter des von der Frauenhofer-Gesellschaft verwalteten Instituts für Telematik, Christoph Meinel, in Trier in einem dpa-Gespräch. Viele Studenten hätten schon mit Bruchrechnen Probleme. „Das Vermitteln strukturierten und analytischen Denkens kommt in der Schule zu kurz." An technische Fächer, die wie die Diplom-Informatik als schwierig gelten, trauten sich deshalb viele Abiturienten nicht heran, bedauerte Meinel. Gerade für das Programmieren und die Administration großer Rechensysteme etwa in Unternehmen fehlten deshalb Fachkräfte.

Flensburger Tageblatt, 29.04.2000

Mathe-Kenntnisse lassen nach

TRIER (dpa) Die Mathematik-Kenntnisse angehender Informatiker und Naturwissenschaftler lassen nach. „Das Niveau ist seit ungefähr zehn Jahren rückläufig", sagte der Leiter des von der Frauenhofer-Gesellschaft verwalteten Instituts für Telematik, Christoph Meinel, in Trier. Viele Studenten hätten schon mit Bruchrechnen Probleme. „Das Vermitteln strukturierten und analytischen Denkes kommt in der Schule zu kurz." An technische Fächer, die wie die Diplom-Informatik als schwierig gelten, trauten sich deshalb viele Abiturienten nicht heran, bedauerte der Professor. Gerade für das Programmieren und die Administration großer Rechensysteme etwa in Unternehmen fehlten deshalb Fachkräfte. Im Aufwind sei dagegen die Wirtschaftsinformatik, bei der die Studierenden vor allem den Umgang mit Programmen lernten. Das Bildungssystem schwäche den Standort Deutschland.

Trierischer Volksfreund 4.5.2000

Virtueller Hörsaal ist in Trier schon Realität,

Hochschulen in der Region erproben den Einsatz von Multimedia für Forschung und Lehre – Symposium über virtuelle Universitäten

Von unserem Mitarbeiter ARNE LANGNER
TRIER.Im Trierer Hochschulalltag spielen das Internet und andere neue Medien bereits eine große Rolle. Um die Perspektiven für Forschung und Lehre geht es ab heute bei einem Symposium.

Sowohl Chancen als auch Barrieren für die Zukunft des virtuellen Lehrens und Lernens hat das Online-Seminar des Trierer Medienwissenschaftlers Professor Dr. Hans-Jürgen Bucher verdeutlicht. Erstmals hatte er im vergangenen Wintersemester eine Lehrveranstaltung zum Thema Online-Journalismus auf der Grundlage des Teleteaching angeboten. In Kooperation mit der TU Ilmenau startete der Fachbereich Medienwissenschaft das Projekt im Oktober 1999. Die Zusammenarbeit lag nahe, da die Universität Ilmenau ebenfalls über einen Fachbereich Medienwissenschaft verfügt.
Mehrwert hatte die Veranstaltung auf vielfältige Weise. Die Trierer und Ilmenauer Studenten saßen einmal pro Woche jeweils zeitgleich im Seminarraum. Im virtuellen Hörsaal wurden Referate vorgetragen, die Teilnehmer konnten miteinander diskutieren. Ermöglicht wurde die Übertragung durch drei Kameras, die alle Bewegungen im Raum aufzeichneten.
Für dieses Unternehmen musste die Kapazität des Univesitätsrechners extra von zwei auf sechs Megabit erweitert werden. Die hohen Telefonkosten wurden teils von der Uni, teils von der Nikolaus-Koch-Stiftung getragen. Mittlerweile hat Bucher bei der Deutschen Forschungsgesellschaft (DFG) einen Antrag für einen eigenen Teleteaching-Raum gestellt. Ein positiver Bescheid liegt aber noch nicht vor.
Um allen Teilnehmern Zugriff auf die einzelnen Seminarprojekte und den Ablauf der Veranstaltung zu ermöglichen, wurde eine virtuelle Arbeitsplattform eingerichtet, auf der Daten und Texte abgelegt werden konnten. Außerdem war eine Kooperation über elektronische Post möglich.
Die Kompetenzen der Studenten im Online-Bereich wurden erweitert, wenn auch der Umgang mit der Sofware für viele am Anfang schwierig war. Das Reden vor der Kamera fiel ebenfalls nicht leicht, und der Arbeits- und Zeitaufwand für alle Teilnehmer war sehr hoch. Dennoch: „Es wurden Schlüsselqualifikationen vermittlelt, die für die Zukunft der Studierenden einfach wichtig sind", meint Bucher. „Die digitale Kontaktaufnahme wird integraler Bestandteil an den Universitäten werden."
An der Fachhochschule gibt es zwar noch keine vergleichbaren Projekte im Online-Bereich, aber auch dort wurden Weichen in diese Richtung gestellt. Vizepräsident Professor Dr. Gerd Diethelm: „Wir wollen demnächst auch Lehrstoff im Internet bereitstellen, der gegen eine geringe Gebühr hernuntergeladen werden kann."
Die Kosten für die Übertragung einer Lehrveranstaltung per Internet sieht er momentan als zu hoch an. Es gebe aber bereits erste Gespräche mit einer Trägergesellschaft für ein solches Projekt. Zum bereits erprobten Teleteaching-Projekt im Bereich Bauingenieurswesen sollen weitere Projekte hinzukommen.
Um die Zukunft des virtuellen Lehrens und Lernens geht es heute und morgen auch beim Trierer Symposium „Virtuelle Hochschule", das vom Institut für Telematik veranstaltet wird. Dabei diskutieren Experten aus Forschung und Lehre über lebenslanges Lernen, den virtuellen Campus und den virtuellen Hörsaal sowie digitalisierte Bibliotheken.

Trierischer Volksfreund 1.7.2000

Schnittstelle zwischen Wirtschaft und Wissenschaft

Das Trierer Institut für Telematik (TI) befasst sich mit den Entwicklungen und Problemen der Computerwelt

Von unserer Mitarbeiterin DENISE JUCHEM
TRIER. Das Internet wurde anfänglich zum Nachrichtenaustausch zwischen Universiäten entwikkelt. Mittlerweile hat sich die weltweit öffentliche Datenautobahn zu einem gigantischen Kommunikationsmedium entwickelt. Mit Chancen, aber auch vielen Gefahren.

Das Trierer Institut für Telematik (TI) befasst sich mit den Entwicklungen und Problemen der Computerwelt. Das Institut hat sich zum Ziel gesetzt, anwendungsnahe Grundlagenforschung zu betreiben.
Doch was ist unter dem Begriff „Telematik" zu verstehen? „Der Begriff Telematik ist ein Kunstwort", erklärt Ernst-Georg Haffner, Mitarbeiter des TI. „Das Wort setzt sich aus Telekommunikation und Informatik zusammen." Das TI, das von Professor Christoph Meinel geleitet wird, steht unter Betreuung der Frauenhofer Management Gesellschaft. „Das bedeutet, dass die Forscher nicht ins Leere forschen, sondern Anwendungen

in der Praxis finden", erklärt Erst-Georg Haffner. Die Leistungen des Instituts werden durch konkrete, zum überwiegenden Teil aus der Wirtschaft finanzierten Forschungs- und Entwicklungsaufträgen erbracht. Das Trierer Institut stellt somit eine effektive Schnittstelle zwischen Wissenschaft und Wirtschaft dar.
Die Entwicklung der Online-Dienste und vor allem des Internets schafft für die Nutzer vielfältige Risiken, da das Datennetz nicht unter Sicherheitsaspekten entwickelt wurde, sondern historisch gewachsen ist. Sicherheitsrisiken bestehen vor allem bei der Übertragung vertraulicher Daten, da die Übertragungswege für jedermann zugänglich sind. „Jeder Nutzer kann die Daten einsehen, manipulieren und im schlimmsten Fall missbrauchen", erklärt der Physiker Bernd Dusemund. Das TI hat verschiedene Projekte entwickelt und bearbeitet, um unberechtigte Zugriffe und die Manipulation von Daten zu verhindern.

Deutschland hat Vorreiterrolle

Eines dieser Projekte ist das so genannte Trust-Center. Die Datenübertragung in offenen Netzwerken erfordert die Verschlüsselung und sichere Authentifikation durch digitales Signieren. Die digitale Signatur muss die wesentlichen Merkmale einer Unterschrift wie Echtheit, Identität, Verifikation und Rechtsverbindlichkeit in elektronischer Form realisieren. Unberechtigte Zugriffe können durch Datenverschlüsselung verhindert werden. Jedem Nutzer wird ein kryptographisch erzeugtes elektronisches Schlüsselpaar zugewiesen, das aus einem geheimen und einem öffentlichen Schlüssel besteht. Damit können Dokumente verschlüsselt und elektronische Unterschriften erzeugt werden, die im Rechtsverkehr die Anforderungen handschiftlich signierter Dokumente erfüllen.
„Solche Trust-Center werden das Internet in Zukunft völlig verändern. Durch seine Sicherheit werden bald auch digitale Behördengänge möglich sein", erklärt Bernd Dusemund. Der Absender einer Nachricht erzeugt mit seinem geheimen, privaten Schlüssel, der weltweit nur einmal existiert, eine Signatur. Der Empfänger verifiziert die Signatur mit Hilfe des öffentlich abrufbaren Schlüssels des Absenders. Ist es möglich die Signatur zu entschlüsseln, dann steht fest, dass das Dokument nach dem Absenden nicht mehr verändert wurde und die Urheberschaft des Absenders nicht anzuzweifeln ist. Nur der authentische Absender konnte die digitale Unterschrift erzeugt haben, anderenfalls wäre eine Entschlüsselung mit einem offieziellen Schlüssel nicht möglich gewesen.
Zur Vergabe der Schlüssel bedarf es eines vertrauenswürdigen Dritten, der durch ein Zertifikat wie ein „elektronischer Notar" bestätigt, dass der öffentliche Schlüssel einmalig und fest einer bestimmten Person zugeordnet ist. Dieser vertrauensvolle Dritte ist das Trust-Center.
Das Trierer Institut für Telematik sieht sich als gemeinnützige Forschungs- und Entwicklungseinrichtung dafür prädestiniert, mittels des Trust-Centers die Erzeugung und Zertifizierung öffentlicher Schlüssel zu übernehmen und eine Gewähr für sichere und authentische Datenübertragung zu bieten. „Deutschland hat im Bereich der Trust-Center eine Vorreiterrolle eingenommen. Doch ein Problem stellt die unterschiedliche Gesetzeslage in anderen Ländern dar", erklärt Dusemund.

Trierischer Volksfreund 25/26.11.2000

Kluge Karten kommen

Trierer Institut stellt Einsatzmöglichkeiten vor

TRIER. (MvBL) Intelligente Chipkarten werden unser Leben künftig stark beeinflussen. Erste erfolgreiche Anwendungen zeigen, wie die digitale Zukunft aussehen könnte.

Am 23. und 24. November 2000 veranstaltete das Trierer Institut für Telematik e.V. ein Symposium über so genannte Smart Cards. Im Gegensatz zu den veralteten Karten mit Magnetstreifen verfügen die „klugen" Karten über einen kleinen Chip, wie er bereits auf der Geldkarte zu finden ist.
Harald Ahrens präsentiert das Media@Komm-Projekt des Städteverbunds Nürnberg. Das Rathaus der Zukunft müsse auf elektronischem Wege rund um die Uhr erreichbar sein, so Ahrens. Das Personal im öffenltichen Dienst könne durch elektronische Antragstellung und –bearbeitung von Routineaufgaben entlastet werden. Freiwerdende Arbeitszeiten kämen dem Bürger zugute.
Die digitale Signatur sei Dreh-und Angelpunkt aller Planungen rund um die smarten Karten. Mit dem 1997 in Kraft getretenen Signaturgesetz wurde zwar der Rahmen der digitalen Unterschrift abgesteckt, rechtsverbindlich sei die Unterzeichnung per Chipkarte allerdings noch nicht. Die längst überfällige Gleichstellung mit der händischen Unterschrift sei in Bälde zu erwarten.
Als erste funktionierende Nutzanwendung des Media@Komm-Projekts stellte Ahrens den online bestellbaren Anwohnerparkausweis vor. Personen und Adressdaten werden während der Antagstellung auf Plausibilität geprüft. Im letzten Schritt werden Wohnort und Parkberechtigungszone des

Antragstellers in einem Stadtplan eingezeichnet und angezeigt. Der Ausweis selbst wird noch per Post zugestellt.
Walter Nink von der Universität Trier stellte die multifunktionale Chipkarte vor. Zum Wintersemester 1997/ 98 wurde die „Tunika" (Trierer Universitätskarte) eingeführt. Mit dem Studienausweis können sich Studierende alle sechs Monate zurückmelden, die Bibliothek und den ÖPNV in Anspruch nehmen, Bescheinungungen ausdrukken und Anschriften ändern.
Nicht nur die Bezahlfunktion – die Tunika ist gleichzeitig Geldkarte – wird im kommenden Jahr erweitert werden. Mit der neuen Karte (ab Herbst 2001) wird man Klausurergebnisse abfragen können. Außerdem wird der Gebäudezutritt zu bestimmten Zeiten nur mit der Tunika möglich sein

Dresdner Neueste Nachrichten, 07.02.2001

Neues Schleusen-System soll Firmencomputer sicherer vor Hackern schützen als Firewalls ab

Trier (ots). Wissenschaftler aus Rheinland Pfalz haben ein System entwickelt, das firmeninterne Computer im Internet sicherer vor unberechtigten externen Zugriffen schützt als sogenannte „Firewalls". Für ihre Erfindung erhielten die Forscher des Trierer Instituts für Telematik jetzt Patentschutz, teilte die mit der Frauenhofer-Gesellschaft verbundene Institution mit. Ihre „Lock-Keeper" genannte Schleusenlösung legt „Hakkern" dadurch wirksam das Handwerk, dass niemals eine direkte physikalische Verbindung des firmeneigenen Netzes mit dem Internet zugelassen wird.

Institutsleiter Prof. Christoph Meinel (46): „Firewalls trennen das interne Rechnernetz eines Unternehmens nicht von der Außenwelt, sondern analysieren und filtern lediglich die übermittelten Datenpakete". Nach Worten des Trierer Telematik-Professors ist es deshalb nicht auszuschließen, dass duch Softwarefehler, mangelnde Kenntnisse des Personals oder fehlerhafte Konfiguration die Firewalls in ihrer Schutzfunktion gefährdet oder sogar außer Kraft gesetzt werden. „Unternehmen mit enorm hohen Sicherheitsbedürfnissen wie z.B. Banken wollen mit diesem Restrisiko nicht leben. Unser patentiertes Schleusen-System blockt alle Online-Attacken auf ein internes Rechnernetz hundertprozentig ab", erklärt Prof. Meinel. Das in seinem Institut entwickelte neue Verfahren soll auf der Computermesse CeBIT Ende März der Fachwelt vorgestellt werden.

Handelsblatt, 28.02.2001

Röntgenbilder schneller überragen
Trierer Forscher entwickeln Verfahren zur Datenkomprimierung

TRIER. Krankenhäuser und Arztpraxen können künftig medizinische Bilder einfacher und schneller über das Internet austauschen. Dafür sorgt eine Komprimierungstechnik, die sich das Forscherteam des Trierer Instituts für Telematik jetzt patentieren ließ. „Mit unserem Verfahren wird eine bisher unerreichte Verdichtung der digitalen Daten bei Patienten-Bildern erzielt", sagt der Leiter des Instituts für Telematik , Prof. Christoph Meinel. Die Übermittlung sei mit der neuen Technik um den Faktor 5 bis 15-mal schneller – je nach Größe des Bildes.
Für die Übermittlung von Diagnosebildern von Arzt zu Arzt per Internet und ISDN-Anschluss werden ohne Datenkompression heute noch bis zu drei Stunden benötigt. Diese Übertragungszeit werde nun auf wenige Minuten reduziert. Die Zeiteinsparung sei vor allem in der Notfall-Medizin wichtig, so Meinel.
„Die technische Herausforderung lag darin, dass die übermittelten Diagnosebilder beim behandelnden Arzt verlustfrei ankommen müssen", erläutert der Forscher. Dies sei nun gelungen. Mit der von den Trierer Wissenschaftlern entwickelten Technik werden die bei sonstigen Bildkomprimierungs-Verfahren auftretenden Einbußen auf ein Minimum verringert.
„Im Prinzip zerlegen wir das Originalbild aus einer Röntgen- oder Computertomographie-Untersuchung in zwei Bilder", erläutert der Institutsleiter. Das eine zeigt den eigentlichen Bildinhalt, das andere unwichtige technische Bestandteile des Hintergrunds. Die Verdichtung der Daten erfolgt schließlich mit zwei unterschiedlichen Komprimierungsverfahren. Dadurch würden mit einem äußerst geringen Rechenaufwand sehr hohe Verdichtungsraten erzielt und gleichzeitig eine praktisch verlustfreie Bildwiedergabe gewährleistet – „wie es in der Medizin verlangt wird", so Meinel. Wenn es überhaupt einen Verlust an Bildinformation gebe, sei der praktisch unsichtbar.
Die verwendete Komprimierungstechnik ist kompatibel mit den gängigen Standards. Das hat den Vorteil, dass die Ärzte die übermittelten Patienten-Bilder sofort mit jedem herkömmlichen „Browser", einer Software zur Darstellung von Internet-Inhalten, betrachten könnten, ohne auf ihren Rechnern eine spezielle Software installieren zu müssen.

Wege zum Institut

Wege zum Institut

Der Weg zu uns ist - über die Medien der Telekommunikation - nicht weit:

Internet

http://www.ti.fhg.de

E-Mail

telematik@ti.fhg.de

Telefon

+49 (0) 651-97551-0

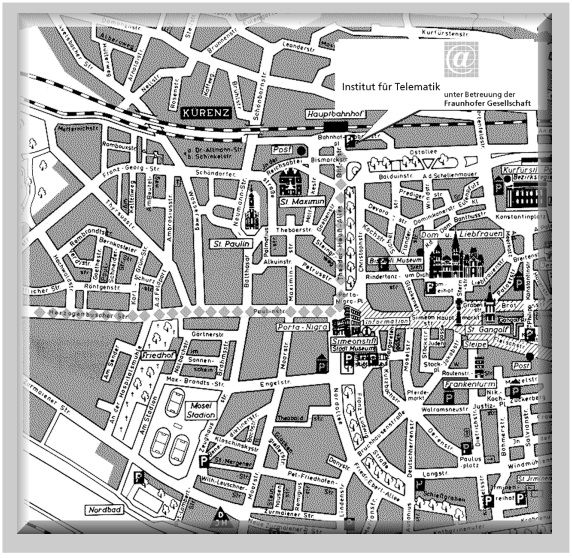
Telefax

+49 (0) 651-97551-12

Wenn Sie uns anschreiben oder in Trier persönlich besuchen wollen:

Anschrift

Institut für Telematik
Bahnhofstraße 30-32
D-54292 Trier



Anreise per Bahn

Mit dem Zug ist Trier zu erreichen über

- Luxemburg
- Köln über Gerolstein
- Koblenz
- Mainz über Koblenz
- Frankfurt über Koblenz
- Saarbrücken

Anreise mit dem Auto

Mit dem Auto erfolgt die Anreise von

- Luxemburg über die E 44/A 64
- Saarbrücken über die A 1
- Köln und Bitburg über die B 51
- Koblenz über die A 48/A1
- Mainz über die B 41
- Frankfurt über die B 41 oder über Koblenz

Anreise mit dem Flugzeug

Vom Flughafen Luxemburg bringt Sie der Airport-Liner direkt nach Trier. Die Reservierung muß 24 Stunden vor Anreise erfolgen.
Bequem können Sie auch mit Bus, Taxi oder Bahn Trier erreichen. Der Zug fährt stündlich und benötigt für die Strecke gute 40 Minuten. Direkt unter dem Flughafen von Frankfurt am Main befindet sich ein Bahnhof. Von diesem aus können Sie in knapp drei Stunden über Koblenz nach Trier gelangen.
Vom Flughafen Saarbrücken/Ensheim nehmen Sie ein Taxi an den Hauptbahnhof Saarbrücken; die anschließende Fahrt per Schnellzug nach Trier dauert gut eine Stunde.
Vom Flughafen Köln-Bonn fahren Shuttle-Busse zum Kölner Hauptbahnhof. Von dort gelangt man mit dem Zug in etwa drei Stunden nach Trier.

T wie TI

T wie TI

T wie TI

Bildquellen

Fotografien: Institut für Telematik, Trier