Institut für Telematik

unter Betreuung der
Fraunhofer-Gesellschaft

Tätigkeitsbericht 2001

Tätigkeitsbericht 2001

Progress Report 2001

Impressum

Impressum

Verantwortlich

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

Redaktion

Hans-Joachim Allgaier, M.A.

Layout

Dirk Neuses

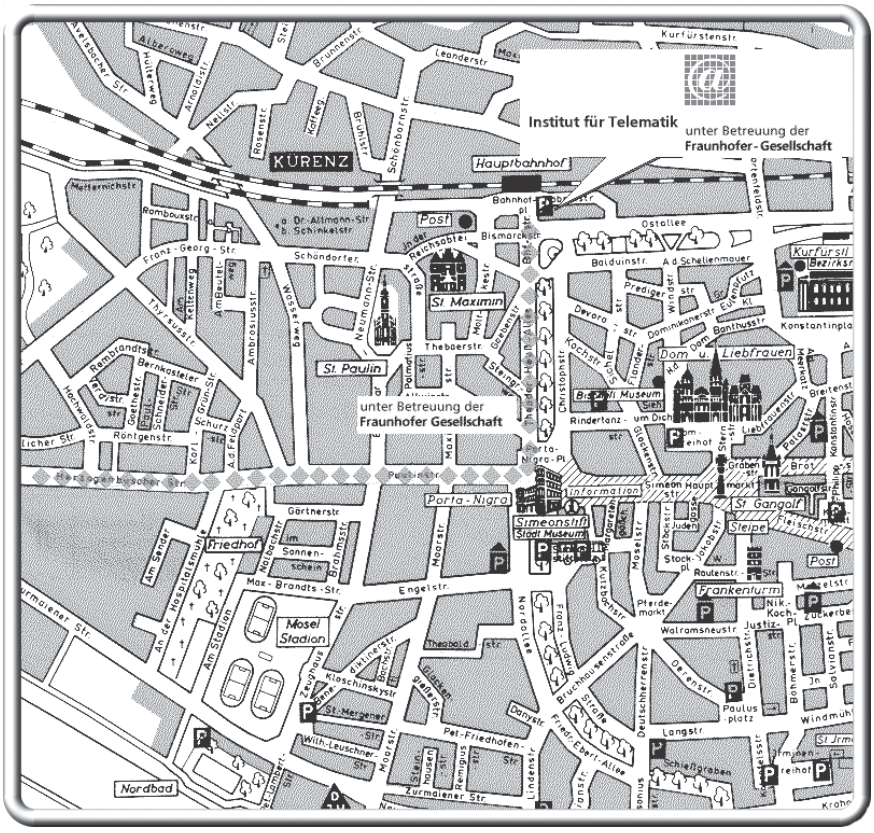
Anschrift der Redaktion

Institut für Telematik e.V.
Presse und Öffentlichkeitsarbeit
Bahnhofstraße 30-32
D-54292 Trier

E-Mail: allgaier@ti.fhg.de

Telefon+49 (0) 651-97551-19

Telefax+49 (0) 651-97551-12



Institut für Telematik
unter Betreuung der
Fraunhofer-Gesellschaft

Tätigkeitsbericht 2001

Tätigkeitsbericht 2001

Progress Report 2001

Inhalt

Inhalt

Vorwort

Im vierten Jahr seines Bestehens konnte das junge Institut für Telematik an die bisherigen Erfolge seiner wissenschaftlichen Tätigkeit anknüpfen und diese ausbauen. Vor allem gelang es, durch gezielte Kommunikationsmaßnahmen unsere Bekanntheit und damit das Interesse an unseren Leistungen zu verstärken. Gleichwohl ging - konjunkturell bedingt - im Jahr 2001 die Zahl der Projektaufträge aus der Wirtschaft deutlich zurück. Doch schon in den Frühjahrsmonaten des Jahres 2002 konnten die Planwerte wieder erreicht werden. So setzen wir unsere Arbeit fort, die unserer Wirtschaft wichtige Entwicklungsimpulse geben soll und bilden hochqualifizierten IT-Nachwuchs, den Deutschland so dringend braucht, sehr wirtschaftsnah aus.

Dies wird in der Öffentlichkeit gewürdigt. Man bezeichnet unser von der Fraunhofer-Gesellschaft betreutes, gemeinnütziges Institut mittlerweile als „führendes Spitzenforschungs- und Entwicklungszentrum fürs Internet", das auch für die hohe Qualität beim Consulting und bei der Realisierung von Praxis-Lösungen bekannt ist. Wir gelten in Wirtschaft und Wissenschaft als erfahrener und kompetenter Partner für Hightech-Projekte in dem Bereich, wo Telekommunikation und Informatik verschmelzen.

Derzeit beschäftigen wir in Trier ca. 25 Wissenschaftler verschiedener Disziplinen und Nationalitäten und eine etwa gleich große Zahl von wissenschaftlichen Hilfskräften. Ein Entwicklungsplan, der auf den Empfehlungen einer vom rheinland-pfälzischen Ministerium für Wissenschaft, Weiterbildung, Forschung und Kultur eingesetzten hochrangigen Evaluationskommission beruht und vom Kuratorium des Instituts gebilligt wurde, sieht vor, dass sich diese Zahl weiter erhöhen wird. Für neue Projekte der grundlagenorientierten Vorlaufforschung und der wirtschaftsnahen Auftragsforschung im Bereich der neuen Informations- und Kommunikationstechnologien steht das Institut für Telematik somit gut gerüstet bereit. Lassen Sie es uns deshalb bitte wissen, für welche telematischen Fragestellungen in Ihrem Umfeld wir eine Antwort finden helfen sollen.

Bis dahin wünschen wir viel Freude bei der Lektüre dieses Tätigkeitsberichts.

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

Trier, im Mai 2002

Foreword

In the fourth year of its existance the Institute for Telematics is able to continue and improve the previous successful results of its scientific activity. First of all, thanks to our targeted communication measures we have managed to become a well known research and development center and, consequently, to increase the interest in our results. Nevertheless, due to economic factors, in 2001 there was a considerable drop in the number of project tasks from the industrial and commercial sectors. However, planned values were reached as early as springtime months of 2002. Thus, we have continued our activities to give our economy a strong impetus for its development and we also provide training of a highly qualified IT generation that German economy needs so badly.

The effort is highly appreciated by the general public. Our institute, which is in care of the Fraunhofer-Gesellschaft, is described as a "leading research and development center for the Internet" and is also known for its top quality consulting and practical solutions. In industry and science we are regarded as an experienced and competent partner for high-tech projects in the areas that unify telecommunications and information technology, with computers, cellular phones and Internet acting together in new applications.

At the moment, in Trier we employ about 25 scientists specialized in different disciplines and of different nationalities, and there is a similar number of research assistants. According to our development plan, which is based on recommendations of a high-ranking evaluation committee set up by the Rhineland-Palatinate Ministry of Science, Higher Education, Research and Culture, and approved by the Institute Committee, the above figures will go up. The Institute of Telematics is well prepared for new projects of both basic research and industry-related and mission-oriented research in the field of new information and communication technologies. Therefore, just let us know which telematic issues specific for your environment we are supposed to help you address.
By then, we wish you a lot of pleasure while reading this progress report.

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

Trier, May 2002

Das Institut im Profil

nstitut im Profil

Grundsätzliches

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

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

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

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

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

Nach vier Jahren Arbeit weist unsere wissenschaftliche Bilanz zwei Patente, vier Promotionen und gut 80 Fachbeiträge zu internationalen Konferenzen auf – eine Leistung, die auch weltweit zu hoher Reputation führte.

Institutsphilosophie

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

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

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

Telematik

Die Telematik hat sich erst Anfang der 90er 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.

Telematik befasst sich mit dem Einsatz informatorischer Komponenten, Verfahren und Systeme, 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.

Entwicklungsgeschichte auf einen Blick

01.11.1997	Gründung des Trägervereins
01.01.1998	Gründung des Instituts
27.04.2000	Erste Promotion
04.09.2000	Erstes Patent erteilt
22.11.2000	Zweites Patent erteilt
10.04.2001	Zweite Promotion
10.05.2001	Mitgliedschaft in der Initiative D21
07.06.2001	Erstes Symposium online im Internet
01.09.2001	Beginn Zusammenarbeit Uni Peking
04.12.2001	Kuratorium beschließt Ausbau

Entwicklung des Instituts

Anfang Dezember 2001 hat das Kuratorium des Instituts-Trägervereins einem Entwicklungs- und Business-Plan der Institutsleitung zugestimmt. Er beruht auf den im Frühjahr 2001 unterbreiteten Vorschlägen einer renommierten Gutachter-Kommission, die das rheinland-pfälzische Wissenschaftsministerium mit der Evaluierung des Instituts beauftragt hatte. Eckpunkte sind eine Vertiefung der Forschungsleistungen, eine noch engere Verzahnung der wissenschaftlichen Arbeit mit Universitäten und Forschungseinrichtungen der Region sowie eine straffere Aufbau- und Ablauforganisation.

Der Business Plan sieht konkret vor, die Zahl der fest angestellten Wissenschaftler in den nächsten fünf Jahren deutlich zu erhöhen. Pro Wissenschaftler-Stelle soll es noch weitere Arbeitsplätze für Doktoranden und wissenschaftliche Hilfskräfte geben. Bei steigendem Jahresbudget soll sich der Anteil der staatlichen Grundförderung laut Plan von 30 auf 40 Prozent erhöhen. Diese wachsenden finanziellen Leistungen des Landes fördern sehr wesentlich die für das Institut typische Verknüpfung von grundlegender Vorlaufforschung mit der Auftragsforschung für Wirtschaft und Gesellschaft.

Insgesamt sehen die Gutachter das Institut für Telematik in einer „Mittlerstellung“ zwischen Universitäten und Forschungsinstituten einerseits und Anwendern in Wirtschaft und öffentlichen Bereichen andererseits. Selbst an die Gründung von start-up-Firmen kann nach dem Urteil der Gutachter gedacht werden. Ferner empfehlen Gutachter und Kuratorium dem Institut, sich mittelfristig in Forschungs- und Entwicklungsprojekte der Europäischen Union einzubinden.

Entstehung

Das Institut für Telematik hat unter Leitung von Univ.-Prof. Dr. sc. nat. Christoph Meinel am 1. Januar 1998 seine Arbeit aufgenommen. Institutionelle Voraussetzungen waren schon früher geschaffen worden. Auf Grund der sehr erfolgreichen Entwicklung der 1996 gegründeten und von Prof. Meinel geleiteten Trierer Außenstelle des heutigen Fraunhofer-Instituts für Wirtschafts- und Technomathematik wurde am 1. November 1997 der Trägerverein „Institut für Telematik e.V." gegründet. Ziel dieses Vereins ist die „Förderung der anwendungsnahen Grundlagenforschung und der angewandten Forschung ... auf allen Gebieten, die für die Telematik bedeutsam sind" sowie die Unterhaltung eines eigenen Forschungsinstituts. Zum Vorsitzenden des Vereins wurde Univ.-Prof. Dr. sc. nat. Christoph Meinel, Lehrstuhlinhaber im Fach Informatik an der Universität Trier, gewählt und mit dem Aufbau eines eigenständigen Instituts für Telematik beauftragt. Die Fraunhofer Management-Gesellschaft in München wurde mit der Geschäftsbesorgung betraut, ein Auftrag, der heute von der Fraunhofer-Gesellschaft selbst ausgeführt wird. Das Institut für Telematik verfügt so über gute Verbindungen zu den Instituten der Fraunhofer-Gesellschaft.

Technische Ausstattung

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

Sämtliche Arbeitsplätze der Wissenschaftler, des technischen Personals, der Sachbearbeiter und der wissenschaftlichen Hilfskräfte sind mit hochleistungsfähigen PCs bzw. mit Workstations ausgestattet.

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

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

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

- Ministerium für Wissenschaft, Weiterbildung, Forschung und Kultur, Mainz
- Universität Trier, insbesondere zur Abteilung Informatik und zum Zentrum für Wissenschaftliches Elektronisches Publizieren (WEP)
- IT-Services s.à.r.L., Luxemburg
- ITM Services AG, Essen
- Dresdner Bank AG, Frankfurt
- Allianz AG, München

- DREGIS – Dresdner Global IT-Services GmbH, Frankfurt
- Polytechnische Universität, Beijing
- Handwerkskammer Trier
- Industrie- und Handelskammer Trier
- ABBL - Association des banques et banquiers, Luxemburg
- Computer Career Institute, Clark University, Massachusetts
- Dagstuhl, Internationales Begegnungs- und Forschungszentrum für Informatik
- Fraunhofer-Gesellschaft, München
- IAL, Luxemburg
- Initiative Gesundheitstelematik Deutschland e.V., Köln
- Institut Supérieur de Technologie, Luxemburg
- Krankenhaus der Barmherzigen Brüder, Trier
- Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau, Mainz
- Polytechnische Hochschule Turin
- Stadt Trier
- University of Colorado at Boulder, USA
- Teletrust Deutschland e.V., Erfurt

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

Projektpartner und Kunden

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

Folgende Institutionen und Unternehmen gehören zu unseren Projektpartnern:

- ABBL - Association des banques et banquiers, Luxemburg
- AGIS Allianz Gesellschaft für Informatik Service mbH, München
- Allianz AG, München
- Aufsichts- und Dienstleistungsdirektion Rheinland-Pfalz, Trier
- Caritas Trägergesellschaft Trier
- CERF-net Germany, Frankfurt
- Dateninformationszentrum Rheinland-Pfalz, Mainz
- Deutsche Forschungsgemeinschaft (DFG)
- Deutsches Forschungsnetz (DFN)
- DREGIS – Dresdner Global IT-Services GmbH, Frankfurt
- Dresdner Bank AG, Frankfurt
- DZ BANK Luxemburg S.A.
- Euro Info Center, Trier
- Global Access GmbH, Frankfurt
- GWI Research, Trier
- Handwerkskammer Trier
- IAL, Luxemburg
- Industrie- und Handelskammer Trier
- Institut für Mittelstandsforschung INMIT, Trier
- ITM Services AG, Essen
- IT-Services s.à.r.L., Luxemburg
- Krankenhaus der Barmherzigen Brüder, Trier
- Ministerium für Inneres und Sport, Rheinland-Pfalz, Mainz
- Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau, Mainz
- Mutterhaus der Borromäerinnen, Trier
- Nikolaus Koch Stiftung, Trier
- Polytechnische Hochschule Turin
- Quorum Medical AG, Schweiz
- Stiftung Burgen, Schlösser, Altertum, Koblenz
- Sozialministerium Baden-Württemberg
- Stadt Trier
- Stiftung Innovation des Landes Rheinland-Pfalz
- Technologiebeirat des Landes Rheinland-Pfalz
- Trierischer Volksfreund
- Union Investment GmbH, Frankfurt
- University of Colorado at Boulder, USA
- Universität Trier
- Teletrust Deutschland e.V., Erfurt
- WGZ-Bank Luxemburg, S.A.
- ZFE Siemens AG, München

Handelnde Personen

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

Prof. Dr. rer. nat.
Thomas Engel

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

Christoph Meinel studierte von 1974 bis 1979 Mathematik und Informatik an der Humboldt-Universität zu Berlin. Nach einem Promotionsstudium an der Humboldt-Universität wurde ihm 1981 der Titel des Dr. rer. nat. verliehen. Von 1981 bis 1990 war er als wissenschaftlicher Assistent an der Sektion Mathematik der Humboldt-Universität zu Berlin und am Institut für Mathematik der Akademie der Wissenschaften in Berlin tätig. 1988 habilitierte er sich dort mit einer Arbeit aus dem Bereich der Komplexitätstheorie. Nach einem Forschungsaufenthalt an der Universität des Saarlands und einer Lehrstuhlvertretung an der Universität Paderborn wurde er 1992 zum ordentlichen Professor (C4) für „Theoretische Konzepte und neue Anwendungen der Informatik" an die Universität Trier berufen. Christoph Meinel ist Autor, Mitautor und Herausgeber von 9 Büchern und mehr als 200 wissenschaftlichen Veröffentlichungen in renommierten wissenschaftlichen Zeitschriften und bei internationalen Kongressen. Sein Hauptinteresse gilt den Forschungsgebieten Telematik, VLSI-Design, Komplexitätstheorie. Prof. Meinel ist Direktor des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP) an der Universität Trier und Mitglied verschiedener Aufsichtsräte und internationaler Konferenzprogramm-Kommittees. So gehört er z.B. dem Aufsichtsrat des Internationalen Begegnungs- und Forschungszentrums für Informatik auf Schloss Dagstuhl an und ist Sprecher der Fachgruppe Komplexität der deutschen Gesellschaft für Informatik (GI). Prof. Meinel ist als Veranstalter verschiedener wissenschaftlicher Symposien und internationaler Tagungen in Erscheinung getreten. Unter seiner Leitung wurde z.B. 1999 die weltweit bedeutende STACS-Konferenz in Trier ausgerichtet. Er ist Veranstalter der Trierer Symposien des Instituts für Telematik und Herausgeber des elektronischen Kolloquiums ECCC. Prof. Meinel war Mitglied des Technologiebeirats des Landes Rheinland-Pfalz und ist Gründungsvorstand der Initiative der Software- und Serviceanbieter (ISS) Rheinland-Pfalz. Er vertritt das Institut für Telematik im TeleTrust Deutschland e.V. und in der Initiative Gesundheitstelematik Deutschland e.V (IGD).

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

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

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

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

Führungskreis

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
1999	Promotion zum Dr. rer .nat
Seit 1999	Wissenschaftlicher Mitarbeiter am Institut für Telematik
Projekte:	Verantwortlich tätig im Bereich Smartcards und Trustcenter

Dr. rer. nat. Ernst Georg Haffner (bis 31.08.2001)

1987	Studium der Informatik/Mathematik an der Uni Kaiserslautern,
Abschluss:	Dipl.-Inform.
bis 1997	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)
2001	Promotion zum Dr. rer. nat.

Dr. rer. nat. Andreas Heuer

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

Dipl.–Inform. Frank Losemann

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

Dipl.–Inform. Uwe Roth

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

Mitarbeiter

Ende des Jahres 2001 beschäftigte das Institut 25 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.

Abb. 1: Mitarbeiter des Instituts für Telematik

Wissenschaftliche Mitarbeiter und Stipendiaten

Absolu, Florence, M.A.
Dr. Akatova, Elena
Dipl.-Inform. Baluch, Ali Raza
Dipl.-Math. oec. Becker, Torsten
Dr. rer. nat. Birkel, Ulf
Dr. rer. nat. Dusemund, Bernd
Dipl.-Ing. Ferring, Paul
Dr. rer. nat. Haffner, Ernst-Georg
Dr. rer. nat. Heuer, Andreas
Huang, Wanjun, MSc
Ji, Hu, MSc
Jiang, Chunyan, MSc
Gevantmakher, Mikhail
Dipl.-Inform. Louizi, Kais
Dr. iur. Gollan, Lutz
Dipl.-Inform. Losemann, Frank
Dipl.-Ing. Mabrouk, Ali
Dipl.-Inform. Podesta, Mariana
Dipl.-Inform. (FH) Müller, Ralf
Neuses, Dirk
Dipl.-Inform. Roth, Uwe
Dr. rer. nat. Sack, Harald
Dipl.-Inform. Schmitt, Michael
Dr. rer. nat. Tork, Joachim
Dipl.-Inform. Vorwerk, Lutz

Systemadministration

Dipl.-Math. oec. Bern, Jochen
Lentes, Bernd
Sand, Michael
Vieten, Michael
Dipl.-Inform. Liu, Zheng

Sekretariat/Verwaltung

Dipl.-Ing. (FH) Huberty, Barbara
Schröter, Anja

Wissenschaftliche Hilfskräfte

Barth, Heiko
Becker, Uwe
Berg, Karl
Boelter, Benjamin
Burghagen, Angela
Densborn, Ruth
Dewald, Stefan
Filkov, Hristo
Fischer, Daniel
Himbert, Isabell
Janetzki, Viktoria
Kloss, Bernhard
Leeuw, Esther Lee de
Ma, Mingchao
Meinel, Tobias
Minev, Mihail
Mitev, Martin
Muellenheim, Gerhard
Noll, Michael
Peters, Stefan
Possin, Rene
Scherer, Thomas
Schlegel, Rüdiger
Schmelzer, Christian
Schneider, Sebastian
Scholtes, Ingo
Schön, Michael
Trocha, Thomas
Wagner, Thomas
Woll, Romy
Ye, Fanglin
Zimmermann, Holger

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
- Prof. 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 Schneider, ab 01.11. Arne Rössel
- Univ. Prof. Dr. sc. nat. 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. nat. Christoph Meinel
  Universität Trier, FB IV – Informatik (Vorstandsvorsitzender)
- Prof. Dr. rer. nat. Thomas Engel
  (Stellvertretender Vorstandsvorsitzender)

Kuratorium

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

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

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

Kuratoriumsvorsitzender

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

Stellvertretender Kuratoriumsvorsitzender

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

Mitglieder des Kuratoriums (alphabetisch)

- Dr. Gunther Frank
  Geschäftsführer DREGIS - Dresdner Global IT-Services GmbH, Frankfurt/Main
- Univ.-Prof. Dr. Dieter Maaß
  Univ.-Präsident i.R., Vorstandsvorsitzender a.D. des DFN-Vereins, Kaiserslautern
- Ministerialdirigent Josef Mentges
  Ministerium für Wissenschaft, Weiterbildung, Forschung und Kultur, Rheinland-Pfalz, Mainz
- Alfred Müller
  Geschäftsführer der Bitburger Brauerei Th. Simon GmbH, Bitburg
- Dr. Thomas Rochel
  Vorsitzender der Geschäftsführung, Saarbrücker Zeitung, Saarbrücken
- Paul Schuh
  Conseiller de direction 1ère classe des Ministère des Communications, Luxembourg
- Univ.-Prof. Dr. Peter Schwenkmezger
  Präsident der Universität Trier
- Lucien Thiel
  Direktor der ABBL - Association des banques et banquiers, Luxemburg
- Dr. Friedrich Wöbking
  Vorstandsmitglied der Allianz Versicherungs-AG und der Allianz Lebensversicherungs-AG, München

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 besseren oberen und unteren Schranken.

2. BDD-basierte Datenstrukturen für logische Funktionen

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

Die Aufgaben des WEP:

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

Leitung des WEP

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

Geschäftsführer: Dr. rer. nat. Harald Sack

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

Kompetenzbereiche

Die Telematik ist ein sehr junges und sich rasant entwickelndes Forschungs- und Entwicklungsgebiet. Im Berichtsjahr 2001 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.

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

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

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

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

2. Kompetenzbereich: Elektronisches Publizieren

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

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

- Online-Redaktionssysteme für Internet und Intranet
- Multilinguale Multiautorensysteme

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

3. Kompetenzbereich: Telemedizin

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

- Mobile Datenerfassung in der Medizin
- DICOM-Bildmanagement und DICOMZIP
- DICOM-Präsentationssystem
- Adaptive Datenkompression mit JAVA
- System zur elektronischen Arztbriefschreibung
- Interaktive multimediale Patientenakte
- Intranet-basierte PACS-Systeme
- Patienten CD-System
- Patientenreminder
- Umfrage Teleradiologie

4. Kompetenzbereich: Sicherheit in offenen Datennetzen

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

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

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

- Trust-Center - Zertifizierungstellen nach Signaturgesetz
- Sicherheitspolicies
- Sicherheitsaudits
- Lock-Keeper und Firewalling
- Tiger Team
- Virtual Private Networks VPN
- Elektronische Modellierung von Datenzugriffshierarchien
- Public-Key-Infrastruktur
- Zertifikat-Management
- Digitale Signaturen
- Electronic Commerce
- Mobile Commerce

5. Kompetenzbereich: Systementwurf und -analyse

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

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

Lock-Keeper

Lock-Keeper

Lock-Keeper – eine patentierte Schleusen-Technologie für höchste Sicherheitsansprüche

Die Sicherheitsgefahren aus dem Internet sind noch lange nicht gebannt, werden sogar immer umfangreicher. Fast regelmäßig erregen Meldungen über „Hackerangriffe" die Öffentlichkeit. Moderne Schutzssysteme sind vor allem in Unternehmen mit hohen Sicherheitsanforderungen gefragt, um sensible Daten vor Ausforschung und Missbrauch zu schützen. Für die Abwehrmaßnahmen werden unterschiedliche Sicherheitsstufen (Security Levels) bei den jeweilig erlaubten Anwendungen definiert und umgesetzt. Je höher die Sicherheitsanforderung, desto stärker die Restriktionen bei den möglichen Anwendungen. Standardlösung in diesem Bereich sind die sogenannten „Firewalls". Doch diese trennen das interne Rechnernetz eines Unternehmens nicht von der Außenwelt, sondern analysieren und filtern lediglich die übermittelten Datenpakete. Deshalb ist es nicht auszuschließen, dass durch Softwarefehler der Firewall oder des Betriebssystems, mangelnde Kenntnisse des Bedienungspersonals oder fehlerhafte Konfiguration die „Brandmauern" in ihrer Schutzfunktion gefährdet oder sogar außer Kraft gesetzt werden. Absolute Sicherheit vor Online-Attacken erhält man nur, indem man die kommunizierenden Netze physikalisch voneinander trennt. Aber wie kann man die Trennung der Netze mit einem gleichzeitig gewährleisteten Datenaustausch in Einklang bringen? Das Institut für Telematik fand in der patentierten Lock-Keeper Architektur (Patentnummer 198 38 253) die Antwort auf diese Frage. Das Land Rheinland-Pfalz zeichnete die Erfindung für hochsicheren Datenaustausch mit dem Erfinderpreis 2001 aus.

Lock-Keeper – a Patented Locking Technology for the Highest Security Requirements

Not only have the Internet security risks been threatening us for long, but, they have become even more widespread. Reports on "hacker attacks" disturb the general public on a practically regular basis. The most important requirement to be fulfilled by the state-of-the-art security systems, especially in companies with high security requirements, is to ensure the protection of confidential data prior to disclosure and misuse. Defense measures include defining and implementation of various security levels for the approved application. The higher the security requirement, the stronger the restriction for possible applications. Firewalls are a standard solution for this area. However, they do not separate the internal computer network of a company from the outside world, but simply analyze and filter the transmitted data packets. Therefore, we must not rule out the possibility that the protective function of firewalls may be at risk or even disabled due to a defect in the firewall software or operating system, incompetence of the operator, or incorrect configuration. Absolute security from an online attack may only be ensured by physically separating the networks from one another during the communication. But, how is it possible to match the separation of networks to the data exchange which is guaranteed at the same time? The Institute for Telematics has found a solution to the problem in a patented lock-keeper architecture (patent number 198 38 253). The highly secure data exchange invention was awarded the 2001 Invention Prize by the state of Rhineland-Palatinate.

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

Das Lock-Keeper-Prinzip wurde am Institut für Telematik mit dem Ziel entwickelt, Daten zwischen einem internen, hochsicheren Netzwerk und einem externen, weniger sicheren Netz wie z.B. dem Internet austauschen zu können, ohne dabei eine-wenn auch nur kurzfristig bestehende – direkte Verbindung aufbauen zu müssen. In Anlehnung an den eher schlichten Ablauf, die Da-

ten zwischen den beiden Netzwerken per Diskette zu transferieren, entstand die Idee, eine Lösung zu entwickeln, die diesen „Austausch per Diskette“ automatisiert durchführen kann.

Genial einfacher Mechanismus

Der Lock-Keeper basiert auf dem genauso altbekannten wie genial einfachen Mechanismus, der Schleuse. Wie bei einer Schiffsschleuse werden beim Lock-Keeper die Daten so durchgeleitet, dass zu keinem Zeitpunkt eine direkte Verbindung zwischen dem inneren und dem äußeren Netzwerk besteht.

Die Lock-Keeper-internen Komponenten sind an einer patentierten Schaltplatine angeschlossen, und zwar so, dass maximal zwei der drei Lock-Keeper-PCs gleichzeitig miteinander kommunizieren können. Dies gewähren sogenannte Schaltrelais (elektronische Schalter) auf der Platine, welche die Verbindung auf Hardware-Ebene in definierten Intervallen umschalten.

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

Die Schleusentechnologie des Lock-Keeper ist somit gegen Online-Attacken immun, da das zugehörige Sicherheitskonzept nicht etwa berechtigte von nicht-erlaubten Anfragen trennt (wie bei einer Firewall), sondern grundsätzlich – unabhängig von einer optionalen Analyse – jeglichen Datenverkehr zwischen den inneren und dem äußeren Netzwerk abbricht, zwischenspeichert und hierdurch alle direkten Angriffsmöglichkeiten unterbindet. Umgekehrt bedeutet dies natürlich auch, dass bestimmte Dienste, die auf eine direkte und unmittelbare Verbindung zwischen den Computer-Netzwerken nicht verzichten können, durch den Lock-Keeper nicht oder nur sehr schwer bereitgestellt werden können.

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

Erfahrungen im praktischen Einsatz

Der Lock-Keeper wird bereits erfolgreich in unterschiedlichen Branchen und Ländern zum Schutz von Unternehmensnetzwerken eingesetzt. Praktische Einsatzgebiete des Lock-Keepers sind beispielsweise die Absicherung von E-Mail-Systemen verschiedener Großbanken, Schutz von Datenbanksystemen oder die Installation mehrstufiger Sicherheitsarchitekturen in Regierungsstellen. Das gemeinsame Ziel dieser Projekte ist der Schutz von unternehmenskritischen internen Netzwerken vor äußeren Angriffen.

Das Institut für Telematik berät auf Grund seiner umfangreichen Erfahrung und Kompetenz Unternehmen, Behörden und andere auf Hochsicherheit angewiesene Institutionen bei der Konzeption, der Realisierung und dem Ausbau von komplexen Sicherheits-Infrastrukturen. Durch Definition unterschiedlicher Sicherheitslevel werden dabei die individuellen Anforderungen an den Quality-of-Service mit den jeweiligen Sicherheitsbedürfnissen in Einklang gebracht. Eine möglichst breit angelegte Palette einsetzbarer Sicherheitskomponenten wird vorgeschlagen. Neben und in Erweiterung zu klassischen Firewalls stellt das Institut auch Lock-Keeper-Lösungen bereit, um absolut sicheren Datenaustausch zu gewährleisten.

Für künftige Ausbaustufen seiner Lock-Keeper-Schleusentechnologie arbeitet das Institut derzeit daran, zeitverzögert auch solche Dienste bereitzustellen, die gewöhnlich eine unmittelbare Verbindung zwischen den datenaustauschenden Netzen erfordern. Die Einschränkungen im Bereich des Quality-of-Service könnten damit vermindert werden.

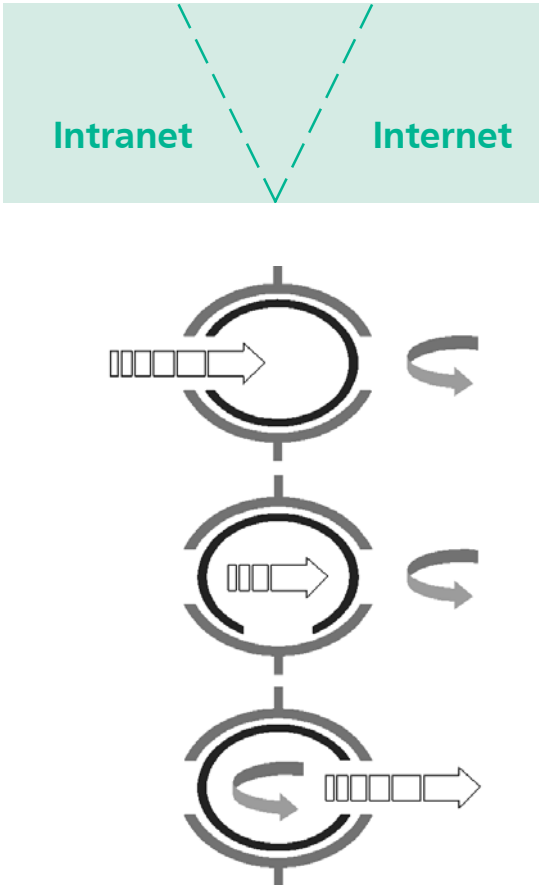


Abb. 1: „Dreischrittiges Schleusenprinzip": Lock-Keeper-Datenaustausch zwischen Intra- und Internet

Bild-Komprimierung

mprimierung

DICOMZIP – effektive und verlustfreie Komprimierung digitaler medizinischer Bilder

Entwickelt vom Institut für Telematik setzt das patentierte DICOMZIP-Verfahren (Patentnummer 19944213) mit seiner hohen und praktisch verlustfreien Komprimierung neue Standards in der digitalen Verarbeitung medizinischer Bilder im international anerkannten DICOM 3-Format. Basierend auf der Idee der adaptiven Kompression, bei der die jeweiligen Vorteile verschiedener herkömmlicher Bildkompressionsverfahren angewendet werden, können die Bilder mit DICOMZIP stark komprimiert und anschließend per e-Mail über das Inter-/Intranet versendet werden.

DICOMZIP – Effective and Loss-Free Compression of Digital Medical Images

Thanks to its high and loss-free compression, the patented DICOMZIP algorithm (patent number 19944213), which was developed by the Institute for Telematics, sets new standards for the digital processing of medical images in the internationally accepted DICOM 3 format. Based on the idea of adaptive compression supported by certain advantages of various standard algorithms of image compression, images can be extremely compressed by DICOMZIP and then sent by e-mail via the Internet/Intranet.

Die digitale Bildverarbeitung im Gesundheitswesen ist durch außerordentlich große Datenmengen pro Bild bzw. Bildsequenz, hohen Bedarf an Speicherplatz und nach wie vor inakzeptabel lange Übertragungszeiten sowohl im Bereich der Unfallmedizin als auch beim Outsourcing medizinischer Datenarchivierung gekennzeichnet. DICOMZIP wurde für die Anwendung in der medizinischen Bildverarbeitung mit dem Ziel entwickelt, die genannten Mängel abzustellen und gleichzeitig den hohen Anforderungen in der Telemedizin an Geschwindigkeit und Bildqualität Rechnung zu tragen. So lässt sich ein mit DICOMZIP komprimiertes Bild bzw. ein ganzes Verzeichnis um 70% bis 90% schneller über das Internet versenden und verursacht einen im gleichen Maße verringerten Speicherplatzbedarf.

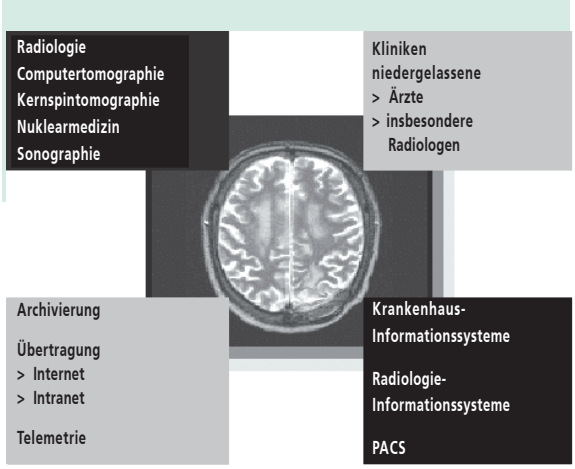


Abb. 1: Einsatzfelder von DICOMZIP

Das Funktionsprinzip

1. Das Originalbild wird in zwei Bilder aufgeteilt. Das erste Bild besteht aus den höchsten Bit-Ebenen des Originalbildes, das zweite Bild aus den niedrigsten. Die Einteilung der Bit-Ebenen in die beiden Klassen erfolgt aufgrund der Analyse des Mittelwertes der Segmentparameter für jede Bit-Ebene.
2. Das erste Bild wird analysiert und daraus eine Einteilung des zweiten Bildes in zwei Bereiche abgeleitet, wobei der erste Bereich die Informationen zum eigentlichen Untersuchungsobjekt (Region des Interesses) beinhaltet und der zweite Bereich ohne jedes Interesse für die Diagnose ist, da er keinerlei wichtige Bildinformationen beinhaltet.

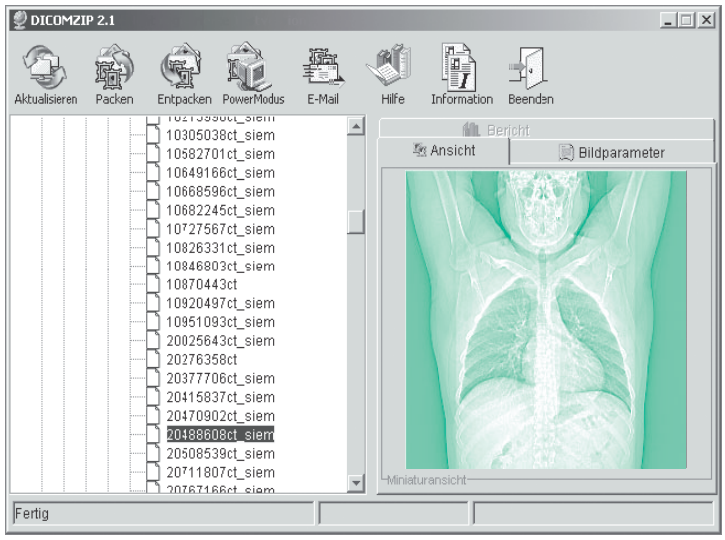


Abb. 2: Datei Explorer/Bildansicht

3. Im dritten Schritt wird der erste Bereich mittels des LZW-Verfahrens (GIF), also verlustfrei, komprimiert. Der zweite Bereich wird mit tels des JPEG-Verfahrens kodiert. Dabei wird der erste Bereich des zweiten Bildes verlust frei (und folglich mit einem kleineren Kompressionsfaktor) komprimiert, während der zweite Bereich mit der irrelevanten Informati on mit einem hohen Kompressionsfaktor kom primiert wird.

4. Zum Abschluss werden die bei der Kompression erzeugten LZW-Daten und JPEG-Daten zu einer Datei kombiniert, die somit sämtliche komprimierten Bilddaten enthält.

Die mit DICOMZIP komprimierten Bilder haben in der Regel eine Größe von nicht mehr als 10 % bis 30 % des Orginalbildes (Faktor 1:10 bis 1:3). Die maximal erzielbare verlustfreie Komprimierung richtet sich dabei u.a. nach der Art (CT, CR, DS usw.), dem Bildinhalt (Hintergrundanteil) und der Qualität des Originalbildes.

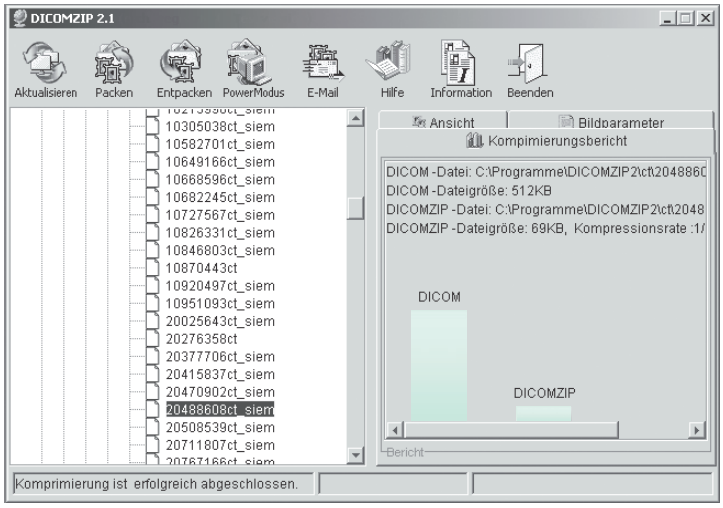


Abb. 3: Komprimierungsbericht

Risiko-Management-Systeme

agement-Systeme

Neues Risiko-Management-Tool für Banken

Die weltweit zunehmende Zahl an Finanz-Transaktionen bietet für Anleger große Chancen, aber – wie vor allem die jüngere Vergangenheit gezeigt hat – auch nicht unerhebliche Risiken. Zins-, Aktien- und Wechselkursschwankungen, aber auch Länder- und Kreditrisiken mit ihrer Ausfall-Problematik bringen die Gefahr hoher Verluste mit sich. Wer sich zum Beispiel als professioneller Anlageberater im starken Wettbewerb behaupten will, muss die verfügbaren Analysedaten aus verschiedenen Quellen intelligent miteinander verknüpfen und schnell und präzise auswerten. Das stellt höchste Anforderungen an die Informationstechnologie und –Infrastruktur eines Finanzdienstleisters. Wenn Flexibilität in den Datenanbindungen und Datenstrukturen genauso gewährleistet ist wie intuitive Benutzung, kann ein zukunftssicheres Risiko-Management-System entstehen, wie ein Projekt des Instituts für Telematik zeigt.

New Risk Management Tool for Banks

The increasing number of financial transactions worldwide has resulted in great opportunities for investors, but also, as we witnessed not long ago, in considerable risks. Changes in interest rates, stocks and exchange rates, together with international and credit risks with their loss-related problems bring along a risk of large losses. Those who wish to establish themselves as professional investment consultants in today's highly competitive environment must be able to ensure that the analysis data, which is available from different sources, is cleverly linked and used in a fast and precise manner. Therefore, providers of financial services are faced with high requirements when it comes to information technology and infrastructure. As suggested in one of the projects of the Institute for Telematics, when flexibility of data link and data structures is guaranteed exactly the same as intuitive use, it is possible to have a risk management system with a guaranteed future.

Bei dem Auftrag einer großen deutschen Fondsgesellschaft, ein Risiko-Management-Tool zu schaffen, ging es darum, den Fondsmanagern folgende Möglichkeiten in die Hand zu legen:

- Steuerung von Wertpapierrisiken
- Überwachung von Kenngrößen
- Berechnung und Simulation von Risikogrößen
- Berücksichtigung von Wertpapierkategorien.

Dies soll es erleichtern, Wertpapiere nach ihren unterschiedlichen Wertsteigerungspotentialen und Risiken zu klassifizieren.

Das Projekt musste mehreren Rahmenbedingungen gerecht werden: Flexible Datenanbindung, flexible Datenstrukturen sowie intuitive Benutzbarkeit sollten garantiert sein.

Flexible Datenanbindung

Eine wichtige Anforderung an das Institut für Telematik war es, eine flexible Datenanbindung zu schaffen, die es auch in Zukunft erlaubt, mit jeder Art von neuer Middleware zusammen zu arbeiten. Unter Middleware versteht man diejenigen Software-Programme eines IT-Systems, die zwischen Informationsanbietern (in der Regel Datenbanken) und Informationskonsumenten vermittelnd tätig sind. Das Institut für Telematik löste diese Aufgabe mit der Einführung einer Abstraktionsebene (Interface), für die eine konkrete Datenanbindung in der Art von Treiber-Programmen realisiert wurde. Nicht zuletzt dadurch besteht hoher Investitionsschutz für die Risiko-Management-Tool-Anwendung.

Flexible Datenstrukturen

Bei dem Projekt waren sehr unterschiedliche Wertpapier-Gattungen zu berücksichtigen. Deutlich wurde, dass die Festlegung der Wertpapier-Gattungen mit Ihren Dimensionen nicht notwendigerweise festgeschrieben ist. Einer zunächst starren Übernahme der gegenwärtigen Strukturen wird künftig eine ständige Anpassung folgen. Dabei ist die Aufnahme neuer Wertpapier-Gattungen ebenso wahrscheinlich wie die Anpassung bestehender.

Um diese Anforderungen zu erfüllen, entschied sich das Institut für Telematik für die zur Zeit flexibelste Doku-mentenstruktur: das XML-Format. Es erleichtert die Verarbeitung, die Analyse und den Austausch entsprechend formatierter Daten.

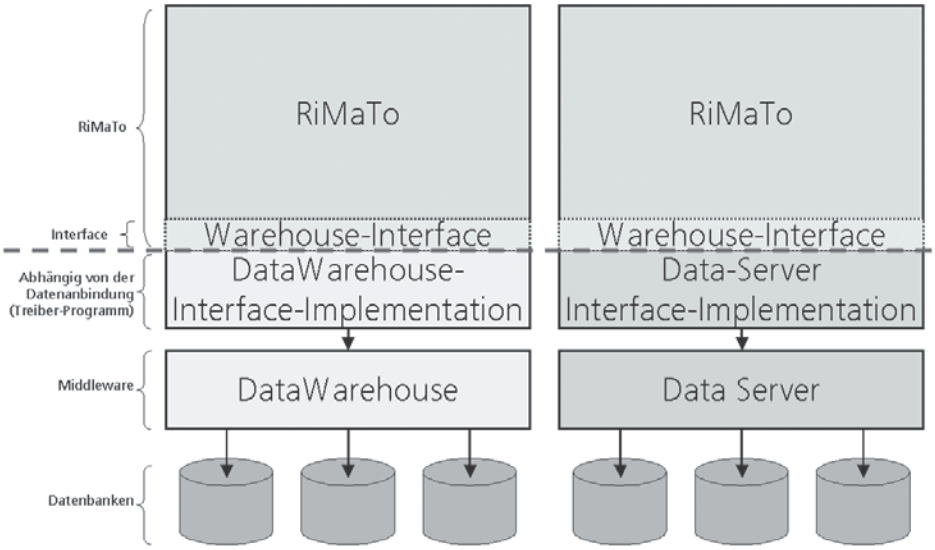


Abb. 1: Abstrahierung der Daten-Anbindung über eine definierte Treiber-Schnittstelle. RiMaTo: Abkürzung für Risiko-Management-Tool

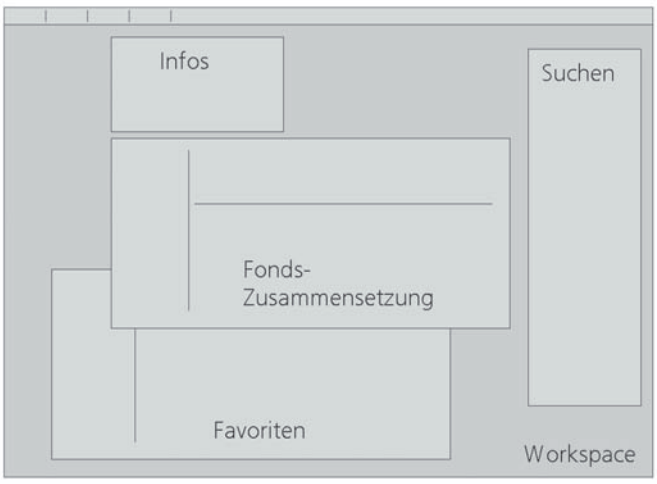


Abb. 2: Schematischer Aufbau der RiMaTo-Arbeitsoberfläche

Intuitive Benutzbarkeit

Anwendungen besitzen nicht nur einen funktionalen Aspekt, sondern werden auch unter dem Gesichtspunkt der intuitiven Benutzbarkeit bewertet. Bei der Entwicklung des Risiko-Management-Tools legte das Institut für Telematik deshalb viel Wert darauf, Anwendungsabläufe ständig zu hinterfragen und mit den Erkenntnissen aus den Beta-Tests zu vergleichen.

Den Fondsmanagern konnten schließlich folgende einfach zu bedienende Anwendungsmöglichkeiten zur Verfügung gestellt werden:

- Persönliche Fonds-Favoriten-Liste
- Erweiterte Suche von Produkten aller Kategorien
- Informationen zu den Produkten
- Verwaltung von mehreren Fonds-Profilen zu einem Fonds
- Transaktions-Simulation
- Erstellung von Order-Listen
- Globale Auswahl der verwendeten Sprache

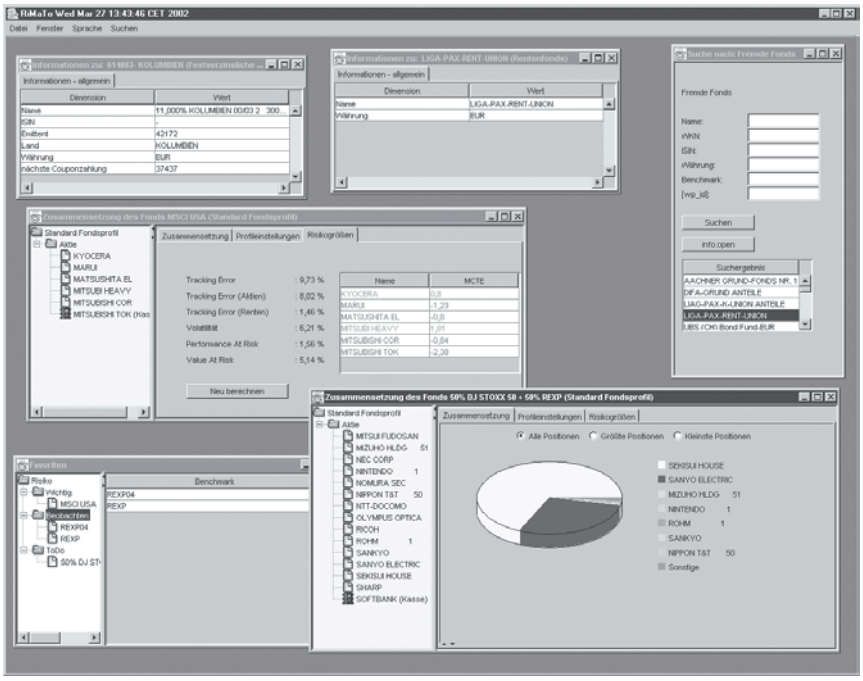


Abb. 3: RiMaTo in Aktion

Weitere wichtige Projekte

In der Folge stellen wir eine Auswahl weiterer interessanter Projekte vor, an denen 2001 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. Web-basiertes Personalmanagement mit dem Smart Data Server

Die Strukturen der Informationstechnologie-Systeme in Unternehmen und Behörden sind hochgradig heterogen. Das hängt mit starkem Wachstum und schneller Veränderung im Lauf der Zeit zusammen. Neue Technologien kommen zum Einsatz, ohne dass jeweils die existierende Infrastruktur komplett ersetzen werden würde. Geichzeitig wachsen die Anforderungen an die IT-Strukturen: Daten aus verschiedenen Quellen müssen kombiniert, sichere Zugänge über das Internet zu den Daten des Intranets geschaffen werden. Standard-Lösungen gibt es praktisch nicht. Vielmehr sind jeweils Anpassungen an die individuelle IT-Struktur notwendig. Doch bei allen unterschiedlichen Anforderungen gibt es auch Gemeinsamkeiten, die in einer Integrations-Plattform zusammengefasst werden können. Diese Integrations-Plattform ist Mittler zwischen den Informationsanbietern (in der Regel Datenbanken) und den Informationskonsumenten (jede Art von Client: Anwendungsprogramm, Java-Applet, Web-Server mit Java Servlets/Perl, o.ä.). Für solche als „Middle-Tier" (Zwischenschicht) bezeichneten Integrationsplattformen hat das Institut für Telematik eine neue, flexible Lösung entwickelt - den „Smart Data Server" (SDS). Er hat sich im Praxiseinsatz beim Personalmanage-ment einer Landesbehörde bereits bewährt.

Web-Based Personnel Management with Smart Data Server

Structures of IT systems in companies and government offices are extremely heterogeneous. This is due to intensive growth and a fast course of time. New technologies are being used although the existing infrastructure has not been fully replaced first. At the same time, requirements for IT structures are growing: data from different sources must be combined, and safe accesses to the respective Intranet data must be provided via the Internet. Generally speaking, there are no standard solutions. Instead, it is necessary to offer possibilities of adjustments according to an individual IT structure. On the other hand, no matter how different these requirements may be, they still have some common characteristics which may be combined in an integration platform. The respective integration platform is a mediator between the information provider (as a rule, a data bank) and information user (any type of client: application program, Java-Applet, Web server with Java Servlets/Perl, or other). For the so-called middle tier integration platforms, the Institute for Telematics has developed a new flexible solution – Smart Data Server (SDS). It has already proved its worth while used in regional authorities personnel management.

Der Smart Data Server des Instituts für Telematik zeichnet sich durch mehrere Vorzüge aus. Hier seien nur einige stichwortartig aufgelistet:

- Modularer Aufbau
- Einfaches Hinzufügen von auf das eigentliche Problem fokussierten Komponenten/ Modulen
- Zugriff der Komponenten auf die Server-Umgebung über Services
- Damit verbunden ist eine einfache Anpassung an verschiedene Einsatzumgebungen/ Infra strukturen
- Netzwerke von SDS sind möglich zur Lasten-/ Aufgaben-Verteilung

Das zu entwickelnde System musste solche Verfahrensweisen berücksichtigen. Auch war es wichtig, bei positiver Antragsbescheidung einzelne Datenbanken der Behörde zu aktualisieren.

Das Verfahren zur Eingabe der Antragsdaten ist dynamisch. Der Benutzer wird über eine Reihe von Web-basierten Dialogen geführt, deren Inhalt sich aus den vorangegangenen Eingaben, sowie Daten, die in einer Datenbank vorliegen, zusammen setzt. Auf der letzten Dialogseite bestätigt der Benutzer seine Angaben.

Eine besondere Herausforderung war es, einen Weg zu finden, wie die Formulardaten in das Intranet der

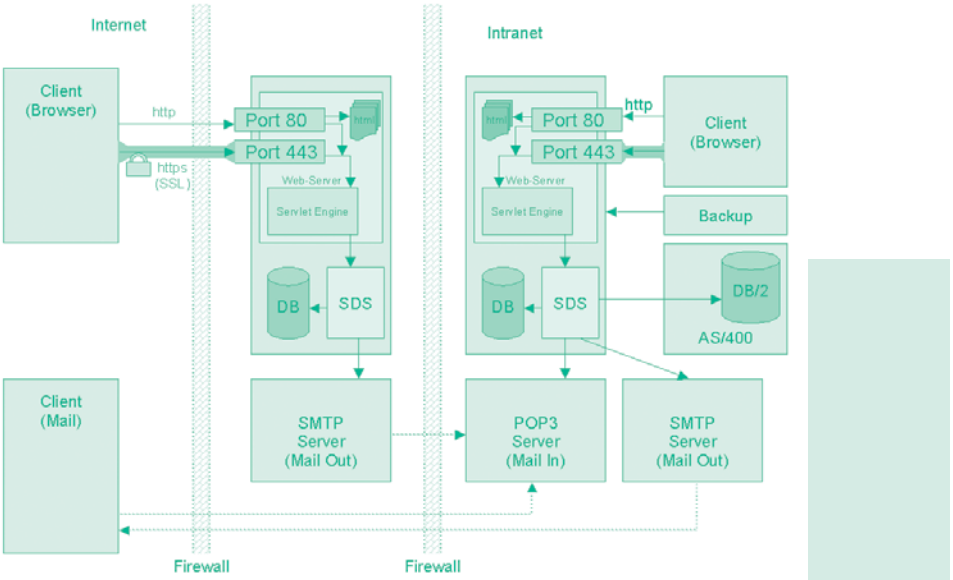


Abb 1: SDS in der 'demilitarisierten Zone' für den Zugriff von Lehrern über das Internet.
SDS im Intranet für den Zugriff von Sachbearbeitern

Ausgangspunkt für die SDS-Entwicklung war das Projekt einer Landesbehörde. Sie wollte allen teilzeitbeschäftigten Lehrern die Verlängerung ihrer Verträge über das Internet möglich machen. Dabei handelt es sich um einen jährlich wiederkehrenden Vorgang, bei dem tausende von Lehrern eine Verlängerung ihrer Verträge beantragen müssen. Bislang geschah dies in Papierform. Durch die Einführung der Antragstellung über das Internet kann die Antragsbearbeitung nun beschleunigt stattfinden, da die Daten des Antragstellers schon in ausreichendem Maße vorliegen und bis zur Bescheiderstellung vollständig elektronisch bearbeitet werden. Die Bearbeitung der Anträge beschränkt sich hauptsächlich auf die Zustimmung oder Ablehnung durch die vorgesehenen Mitarbeitergruppen sowie auf die Korrektur möglicher Falschangaben.

Von der Antragsstellung bis zur Erstellung der Bescheide sind viele verschiedene Persongruppen an dem Genehmigungsprozess beteiligt. Abhängig von den jeweiligen Antragsdaten kann der Weg des Antrages innerhalb der Behörde unterschiedlich sein.

Behörde überführt werden, da wegen der Sicherheits-Policy eine direkte Kommunikation zwischen Internet und Intranet nicht erlaubt ist. Hierbei konnte jedoch der SDS seine Flexibilität unter Beweis stellen. Er gewährleistet, dass bei einer späteren Anpassung der Sicherheits-Policy (Erlauben von direkter Kommunikation) keine Neuentwicklungen vorgenommen werden müssen. Es besteht also Investitionsschutz.

Eine weitere wichtige Leistung war es, die Beteiligung am Genehmigungsprozess auch solchen Personengruppen zu ermöglichen, die keinen direkten Zugang zum Intranet der Behörde besitzen (Schulleiter). Auch hier konnte ein adäquate Lösung entwickelt werden.

Erfreulich ist die Bereitschaft der Pädagogen, die neue Möglichkeit der Antragstellung über das Internet auch zu nutzen. Mehrere tausend Teilzeit-Lehrer wählten bereits diesen Weg – ohne sich darüber bewusst zu sein, dass der Prozess auf modernster Middle-Tier-Technologie basiert.

2. Public Key Infrastrukturen (PKI) – Ideale Sicherheitssysteme für Banken

Banken setzen besonders viel Informationstechnologie ein. Diese abzusichern, ist ein immer wichtiger werdendes Anliegen.
In Banken arbeiten sehr viele IT-Systeme unterschiedlicher Hersteller, Größe und Architektur miteinander zusammen. Sie alle sollen von einem einheitlichen Sicherheitssystem geschützt werden. Dessen funktionale Ziele sind in der Regel Authentizität, Integrität, Vertraulichkeit und Nachvollziehbarkeit. Voraussetzung dafür, diese Ziele zu erreichen, ist die sichere Identifikation der Benutzer bzw. Kommunikationspartner. In großen vernetzten, heterogenen und teils verteilt administrierten IT-Systemen, wie man sie in Banken findet, bietet der Einsatz einer Public Key Infrastruktur (PKI) dafür eine ideale, standardbasierte Lösung, welche die Kommunikation auch über unsichere Netze wie das Internet absichern kann. Gearbeitet wird dabei mit einem Zwei-Schlüssel-System. Die einmaligen und sich ergänzenden Schlüssel dafür erzeugt und verwaltet ein Trust Center. Diese Zertifizierungsstelle arbeitet als „elektronischer Notar".

Public Key Infrastructures (PKI) – Perfect Security Systems for Banks

Since banks in particular have a lot of IT equipment installed, ensuring its security is their major concern. At banks you can often find a great variety of IT systems operating together regardless of the fact that they differ in brands, sizes and architectures. All of those systems must be safeguarded by means of a uniform security system. Generally, its functional aims include authenticity, integrity, reliability and adaptability. The correct identification of the user, that is, communication partner is a prerequisite for the fulfillment of the above goals. In case of large networked, heterogeneous and partly distributed administered IT systems that we find in banks, the implementation of the Public Key Infrastructure (PKI) provides a perfect standard solution enabling communication also via unsafe networks such as Internet. In this case, a two-key system is used. The unique and complementary keys are made and managed by a trust center. The certification place operates as an "electronic notary".

Aufgabe eines Projektteams des Instituts für Telematik war 2001 die Einführung, der Ausbau und die Betriebsunterstützung einer geschlossenen Public Key Infrastruktur in einem großen, international operierenden Finanzdienstleistungs-Konzern. Vor allem ging es um einen automatischen Zertifikatserneuerungsprozess und das Zusammenspiel der internen PKI mit anderen offenen Public Key Infrastrukturen. Schon seit 1997 hat das Institut bei einer großen europäischen Bank das Grundsystem einer PKI und viele weitere Komponenten dafür konzipiert und geliefert.

Umfassende Kompetenz und reichhaltige Praxiserfahrung des Partners sind – so hat es sich gezeigt – für die Auftraggeber von PKI-Projekten entscheidende Erfolgsfaktoren bei der Realisierung. Denn wegen vieler Schnittstellen zu anderen Systemen und ineinandergreifender Prozesse ist das Risiko des Scheiterns ohnehin vergleichsweise hoch. Manche solcher PKI-Projekte sind anderenorts schon wegen zu hoher Betriebskosten durch allgemeinen Verwaltungs- und Wartungsaufwand eingestellt worden oder nie aus dem Pilotstadium herausgekommen.

Aus den vielen Aspekten, die der Betrieb einer PKI z.B. in einer Bank hat, seien hier nur zwei besonders wichtige herausgegriffen:
Administrierbarkeit und Anwendernutzen.

Administrierbarkeit

Alle PKI-bezogenen Aufwendungen in Form von Investitionskosten und Arbeitszeit müssen in direktem Verhältnis zum Nutzen gesehen werden. Dieser liegt im Beitrag zum Sicherheitssystem, in Produktivitätssteigerungen und in Kosteneinsparungen durch Vermeidung von Mehrfachentwicklungen. Dieser Nutzen ist bei Infrastrukturen aber nur schwer transparent oder messbar zu machen, da er sehr vielschichtig ist. Manche Eigenschaften helfen, eine PKI kostengünstig zu betreiben, verursachen aber zunächst auch höhere Entwicklungskosten. Diese können nur durch Einsparungen im Betrieb der PKI und bei der weiteren Anwendungsentwicklung mit und für diese PKI gerechtfertigt werden.

Ein Beispiel, das die Vorteile einer administrationsarmen PKI besonders deutlich macht, ist die Genehmigung von Zertifikatsanträgen. Jeder Anwender, der die Vorteile eine PKI nutzen will, benötigt

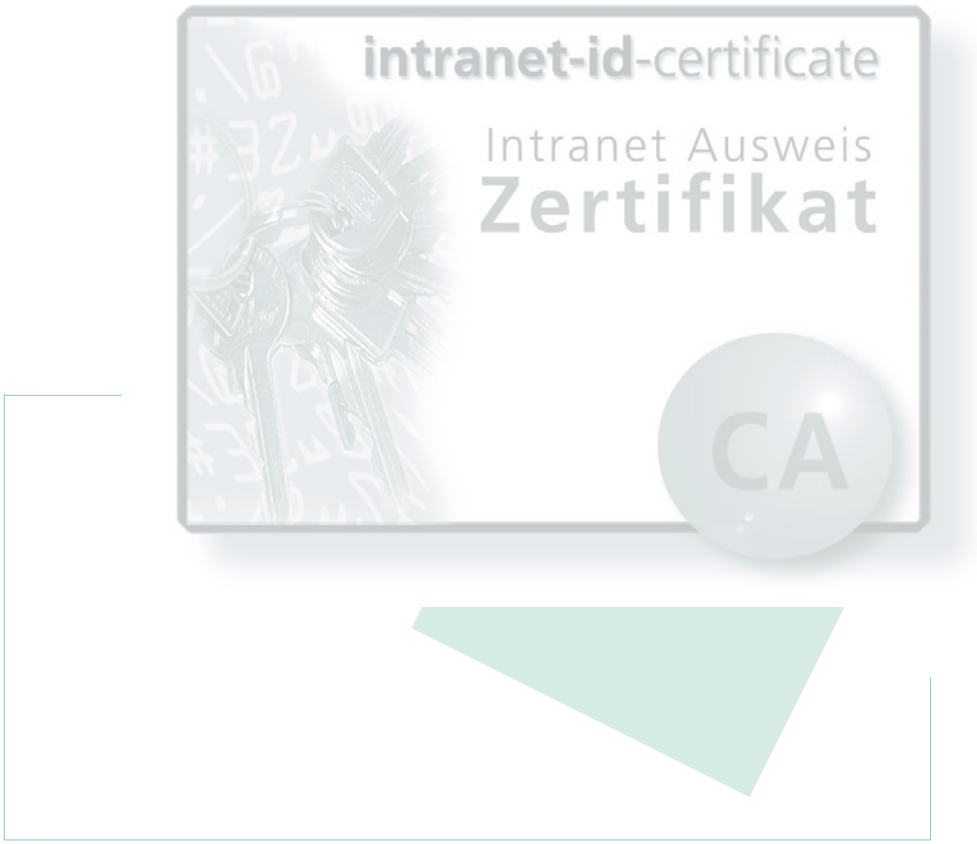
ein Zertifikat. Die Daten in diesem Zertifikat (Name, E-Mail Adresse oder Personalnummer) müssen entweder vom Nutzer eingegeben werden oder aus verlässlichen Datenquellen kommen. Je weniger eingegeben werden muss, desto schneller - also kostengünstiger - können die Zertifikate erstellt werden.

Bestehende Datenquellen waren in unserem Projekt daher so in die PKI zu integrieren, dass möglichst wenig Benutzereingaben bei der Sicherheitsadministration erforderlich sind. Damit werden auch Medienbrüche und mögliche Fehleingaben vermieden. Eine entsprechende Gestaltung der Benutzerschnittstelle der PKI senkt den Schulungsbedarf und steigert die Sicherheit und Benutzerfreundlichkeit einer Zertifikatsmanagement-Anwendung.

Anwendernutzen

Eine PKI kann überall dort, wo sichere Identifizierung (Authentifikation) der Benutzer bzw. Mitarbeiter notwendig ist, Paßworteingaben ersetzen. Das ist zum Beispiel bei Zugriffen auf vertrauliche Informationen im Intranet sinnvoll oder dann, wenn auf den Benutzer abgestimmte Informationen bereitgestellt werden sollen. Der Schutz von Intranet-Ressourcen kann auf der Basis von Public Key Infrastrukturen benutzerfreundlich und für den Benutzer transparent gestaltet werden, wenn Techniken der digitalen Signatur mit einem sogenannten "Single-Sign-On" (SSO) oder Einmal-Anmelden eingesetzt werden.

Hierbei gibt es nur noch ein Paßwort pro Benutzer, das für alle entsprechenden Anwendungen gleichermaßen gilt. Mit diesem Passwort identifiziert man sich nur noch einmal pro Sitzung gegenüber seinem eigenen Web-Browser bzw. dem Betriebssystem. Die Zugriffsprotokolle werden dann - je nach Einstellung - teil- oder vollautomatisch für den Benutzer abgewickelt. Durch den Einsatz von Zertifikaten kann der Web-Browser seinen Benutzer bei Intranet-Servern anmelden, ohne ihn jedes Mal im Arbeitsfluss zu stören, indem er nach einem weiteren Paßwort fragt. Die Sicherheit wird in diesem Szenario erhöht, da keine Passworte mehr zwischen den Rechnern übertragen werden müssen, sondern ein auf Public-Key-Verschlüsselung basierendes Identifikations-Verfahren eingesetzt wird.



3. Tages-CA - eine Lösung für Smartcard-Betriebsausweise

Immer mehr Unternehmen rüsten ihre Mitarbeiter aus Sicherheitsgründen mit multifunktionalen Chipkarten (Smartcards) als Betriebsausweis aus. Gebäudezutritt und Anmeldung an Computersystemen sind dann ohne solche Smartcards nicht mehr möglich. Aber was passiert, wenn Smartcards vergessen, verloren oder gestohlen werden? Bis eine Ersatzkarte ausgestellt werden kann, vergehen drei bis vier Tage. Nicht nur Außendienstler, die für die Kundenberatung vor Ort auf ihren Smartcard gesicherten Notebook angewiesen sind, können sich derart lange Untätigkeit nicht leisten. Ein vom Institut für Telematik entwickelter Workflow macht die Mitarbeiter in höchstens dreißig Minuten wieder arbeitsfähig – per elektronischem Tagesausweis.

Surrogate CA – Solution for the Smart Card Employee Identification

For security reasons, an increasing number of companies provide their employees with multifunctional chip cards (smartcards) as employee identification. Access to facilities and login to computer systems is then impossible without such smartcards. But, what happens when your smartcard is forgotten, lost, or stolen? It takes three or four days to issue a substitute card. Employees working outside the office and using their smartcard secured notebooks to provide their clients with on-site consulting services are among those who cannot afford long periods of idleness. A workflow developed by the Institute for Telematics, makes it possible for an employee to go back to work again in a 30 minutes' time at the most – thanks to an electronic daily identification.

Erfahrungsberichte aus der Unternehmenspraxis zeigen, dass bei IT-Systemen, die ohne Smartcards arbeiten, von 50.000 Benutzern pro Tag durchschnittlich etwa 15 ihre Paßworte zurücksetzen lassen. Das ergibt im Monat fast 400 Verzögerungen im Arbeitsablauf, die je nach Erreichbarkeit der Administratoren jeweils etwa 5 bis 15 Minuten dauern. Leicht kommen so bis zu 100 unproduktive Mannstunden pro Monat zusammen...

Bei Smartcards jedoch ist das Zurücksetzen des Paßworts gar nicht möglich, denn kein Administrator soll die Karte entsperren und damit in fremdem Namen digitale Unterschriften leisten können. Die Karte muss also komplett ersetzt werden, wenn die Benutzer das Paßwort der Smartcard vergessen. Auch das Vergessen der Smartcard selbst sowie deren Verlust, Diebstahl oder Beschädigung führen zu Ersatzbedarf.

Einen solchen Betriebsausweis nach herkömmlichem zentralisierten Verfahren zu ersetzen, dauert mit Versand und Übergabe in der Regel mindestens drei Tage. Einfache Ersatzkarten helfen zwar für den Gebäudezutritt, sind für die Anmeldung am eigenen Benutzerkonto des IT-Systems nicht geeignet, da sie dem Konto nicht zugeordnet sind.

Ist die Karte nicht verfügbar, wird meist auch erst am nächsten Tag eine Verlustmeldung geschrieben, damit es keinen unnötigen Ärger gibt, wenn sich die Karte doch noch wiederfindet. Es vergeht also noch ein weiterer Tag ungenutzt, bis der Mitarbeiter nach einem Verlust der Smartcard wieder richtig arbeiten kann.

Lösung

Das Institut für Telematik hat als Lösung für all diese Probleme einen Workflow entwickelt, der den Mitarbeiter in 15 bis 30 Minuten wieder arbeitsfähig macht. Dies geschieht durch die Aus-

gabe kurzlaufender Zertifikate („Tages-CA"), die online auf dem Computer oder einer neuen Smartcard installiert werden können.

Damit die Ausgabe schnell erfolgen kann, wird vermieden, eine zentrale Abteilung in den Ausgabeprozess einzubeziehen. Zwei Mitarbeiter aus der selben Abteilung, die Ihren Kollegen persönlich kennen und selbst noch über funktionierende Zertifikate verfügen, beantragen stellvertretend das Ersatz-Zertifikat. Je nach Sicherheitsanweisungen des Unternehmens können aber auch Vorgesetzte mit in den Workflow eingebunden werden. Generell wird der organisatorischer Zustimmungs- und Entscheidungs-prozess in der Software des Instituts für Telematik nachgebildet.

Der Mitarbeiter kann dabei angeben, ob er sein Zertifikat nur vergessen oder verloren hat. Bei Verlust wird die alte Smartcard gesperrt und eine neue vollautomatisch beantragt. Je nachdem, ob die Karte ersetzt werden muss oder nicht, sind die Ersatzzertifikate für ein bis fünf Tage gültig.

Die Praxis zeigt, dass wesentlich mehr Karten vergessen werden als verloren gehen. Die im Workflow der Tages-CA gefundene Ersatzlösung rettet also viel wertvolle Arbeitszeit. Und weil der Schaden begrenzt wird, können Mitarbeiter viel offener mit dem Problem einer verlorenen Smartcard umgehen. Das Unternehmen ist in der Lage, rechtzeitig die richtigen Maßnahmen einzuleiten, zum Beispiel Karten mit unklarem Zustand zu sperren, damit diese nicht durch unehrliche Finder missbraucht werden können.

Im Berichtsjahr 2001 hat das Institut für Telematik sein Konzept einer Tages-CA in eine große Application Service Providing (ASP) Infrastruktur integriert. Diese bietet über einen ganz normalen Web-Browser und ein Zusatzmodul (Plug-In) Zugriff auf Standardanwendungen. Durch ASP müssen Anwendungen nicht mehr auf einzelnen Rechnern installiert werden, sondern werden über das Netz in einer Server-„Farm" ausgeführt. Der Benutzer sieht davon nichts - er kann wie gewohnt mit den Programmen arbeiten. Durch ASP sinkt der Installations- und Pflegeaufwand für Software auf Arbeitsplatzstationen. Außerdem werden Einsparungen durch ein verbessertes Lizenzmanagement erwartet.

Um nun die Benutzer bei der Anmeldung an ihrem Rechner und der zentralen ASP-Umgebung sicher zu identifizieren, werden Zertifikate auf Smartcards eingesetzt. Zertifikate sind dabei für einen Betriebsausweis so etwas wie maschinenlesbare Erweiterungen. Diese werden für jede Smartcard und jeden Benutzer individuell erstellt und auf der Karte gespeichert. Mit Zertifikaten funktioniert die Anmeldung sicherer als nur mit Paßworten, da diese bei der Übertragung abge-
den könnten.

4. Studie zu Digitalen Signaturen gibt Marktüberblick

Wer in Deutschland elektronische Unterschriften einsetzen will, die den strengen Anforderungen des Gesetzes entsprechen, kann sich an mehr als ein Dutzend Anbieter wenden. Grundsätzlich ist davon auszugehen, dass bei den Anbietern sogenannter qualifizierter elektronischer Signaturen, die den herkömmlichen Handunterschriften mittlerweile rechtlich weitestgehend gleichgestellt sind, gleich sicher gearbeitet wird. Doch bleiben für IT-Entscheider, die über die Einführung entsprechender Systeme zu befinden haben, genauso wie für Anwender wichtige Fragen zu klären: Welche Chipkarten werden eingesetzt, welche Signiersoftware wird angeboten, wie werden die Schlüssel gespeichert? Antworten auf diese und andere Fragen liefert eine Studie, die das Institut für Telematik angefertigt hat, um Grundlagen- und Fach-Kenntnisse für die Bewertung der angebotenen Lösungen zu vermitteln.

A Study of Digital Signature Provides a Market Overview

In Germany, those who wish to use electronic signatures in compliance with the stringent regulations, can turn to more than a dozen suppliers. Basically, we assume that one can start work immediately in case of suppliers of the so-called certified electronic signatures which have meanwhile become to the greatest possible extent legally equal to usual handwritten signatures. However, for the people making IT-related decisions and approving the implementation of certain systems, as well as for the users, the following important questions need clarifying: which chip cards are to be used, which signature software is offered, and how are the keys stored? Answers to these, and other, questions are provided in the study made by the Institute for Telematics in order to acquire both the basics and technical expertise necessary for the evaluation of any offered solutions.

Neben den Fragen, was genau das Signaturgesetz 2001 und die dazugehörige Signaturverordnung 2001 von den Anbietern fordern, muss der IT-Entscheider auch die Prinzipien der Digitalen Signaturen, der Zertifikatsmodelle und der Überprüfungsmechanismen nachvollziehen können. Einen umfangreichen Grundlagenteil zu liefern, war daher Bedingung für die universell einsetzbare Marktübersicht.

Ziel der Studie

Das Institut für Telematik mit seiner langjährigen Projekterfahrung im technischen und rechtlichen Bereich der Public-Key-Infrastrukturen und der Digitalen Signaturen legte Wert darauf, dass die Studie zum einen die Anforderungen des Signaturgesetzes 2001 und der Signaturverordnung 2001 an die Zertifizierungsdiensteanbieter und deren Produkte in Deutschland darstellt, zum anderen deren Produkte und Dienste erläutert. Diese unterscheiden sich teilweise nur im Detail. Dies kann jedoch weitreichende Folgen haben, die dem Interessierten aufgrund des Grundlagenteils der Studie leicht nachvollziehbar sind.

Inhalt der Studie

Neben der Einführung in die Technologie und die gesetzlichen Anforderungen informiert die Studie (aktualisierte Fassung: Stand Mai 2002) über die in Deutschland existierenden

- akkreditierten Zertifizierungsdiensteanbieter,
- akkreditierten Zeitstempeldienstanbieter und
- Zertifizierungsdiensteanbieter, die ihre Tätigkeit behördlich angezeigt haben.

Pro Anbieter bietet die Studie einen kompakten Überblick an über u.a. die Produkte zur Schlüsselerzeugung, die Art der Schlüsselspeicherung, die einsetzbare Signiersoftware, die Kosten pro Jahr, weitere Leistungen des Anbieters und die einsetzbaren Chipkartenleser.

Aufgrund der grundsätzlichen Informationen im ersten Teil eignet sich die Studie auch als Einstieg für technische Laien. Experten werden die Ergebnisse schätzen, wenn sie einen umfassenden Überblick über die aktuellen Anbieter am Markt und deren Lösungen suchen, der einen schnellen Vergleich ermöglicht.eee

	Telesec	Signtrust	Bundesnotar-kammer[1]	Datev[2] , StB- und RA-Kammern[3]	Medizon	TC Trustcenter[4]	D-Trust[5]
Eigenes Trustcenter	ja	ja	nein	ja	nein	ja	ja
Komponente zur Schlüsselerzeugung	Schlüsselgenerator TC-SG Deutsche Telekom	Schlüsselgenerator KG-DPAG Deutsche Post	wie Signtrust	wie Telesec	wie Signtrust	Smart Card StARCOS, Giesecke & Devrient (G&D)	Smart Card MICARDO Public, Orga ("D-TRUST-CARD")
Schlüsselspeicherung und Signatur-Erstellung	PKS-Card Deutsche Telekom	SEA-Card Deutsche Post	wie Signtrust	e:secure-Card	wie Signtrust	Smart Card StARCOS, G&D	Smart Card MICARDO Public, Orga
Systemvoraussetzung	MS Windows 95, NT 4.0	MS Windows 95, 98, NT 4.0, 2000	wie Signtrust	MS Windows 95a, 98 SE, NT 4.0, 2000	wie Signtrust	MS Windows 98, NT, 2000	MS Windows 95, 98, NT, 2000
Darstellung zu signierender Daten	TCrypt-SigGDeutsche Telekom	Plug-In eTrust Mail für MS Outlook, Lotus Notes R5	wie Signtrust	Datev GERVA, Funktionsbibliothek DVSigE2 mit MS Outlook, Outlook Express, Eudora light	wie Signtrust	SecSignerSec-Com-merce	ID2/Smarttrust Personal i.V.m. MS Outlook
Überprüfung signierter Daten	TCrypt-SigGDeutsche Telekom	Plug-In Signtrust eTrust Mail für MS Outlook, Lotus Notes R5	wie Signtrust	Datev GERVA, Funk-tionsbiblioth-ek DVSigE2 mit MS Outlook, Out-look Express, Eudora light	wie Signtrust	SecSignerSec-Com-merce	ID2/Smarttrust Personal i.V.m. MS Outlook
Empfänger-Voraussetzung	wie Signierender	wie Signierender	wie Signtrust	alternativ kostenl. Datev GERVA Viewer	wie Signtrust	wie Signierender	S/MIME-fähiger E-Mail Client und Root-Zertifikat
Sicherer Verzeichnis-Dienst	ÖVTC-Verzeichnis-Dienst Deutsche Telekom	DIR-DPAG Deutsche Post	wie Signtrust	OCSP-Responder Secunet	wie Signtrust	TC-DIRTC Trustcenter	OCSP-Responder Secunet
Zeitstempeldienst	(für PKS-Nutzer)	DIR-TSS Deutsche Post	wie Signtrust	über OCSP-Responder Secunet	TSSTimeproof	n.a.	n.a.
Kosten	· Chipkarte einschließ-lich Attribut-Zertifikat: 27,35 · Jährlich: 49,83	· Chipkarte inkl. Nutzungsgebühr für ein Jahr: 61,36 · Jährlich: 25,56	· Chipkarte inkl. Nutzungsgebühr für ein Jahr: 25,56 · Jährlich: 25,56 · zzgl. Notargebühren	n.a.	· Chipkarte inkl. Nutzungsgebühr für ein Jahr: 150,- · Jährlich: 75,-	n.a.	· Chipkarte inkl. Nutzungsgebühr für 3 Jahre: 49,-
Internet-Adresse	www.telesec.de	www.signtrust.de	www.bnotk.de	www.zs.datev.de	www.medizon.de	www.trustcenter.de	www.d-trust.de

Abb. 1: Stand: März 2002, Quelle: Institut für Telematik (www.ti.fhg.de)
Aufgeführt sind alle Zertifizierungsdienste-Anbieter, die nach dem deutschen Signaturgesetz als Trust Center („Elektronischer Notar") arbeiten dürfen. Sie stellen Zertifikate aus. Das sind Bescheinigungen, die einer Person einen öffentlichen Schlüssel zuordnen und die Identität der Person bestätigen.

[1] Kundenkreis beschränkt auf Notare etc.
[2] Kundenkreis beschränkt auf Steuerberater- und Rechtsanwalts-Kammern etc.
[3] Steuerberaterkammern Nürnberg, Saarland, Bremen, Stuttgart, München, Berlin; Rechtsanwaltskammern Bamberg, Koblenz; diese nutzen alle das Trustcenter der DATEV
[4] Schlüsselerzeugung auf Speichermedium
[5] Schlüsselerzeugung auf Speichermedium
[6] einziger Anbieter eines ausschließlichen Zeitstempeldienstes ist Authentidate (www.authentidate.de)

5. Zeitstempeldienst: Elektronische Ablösung des Post-Eingangsstempels

Bei elektronischen Dokumenten ist heute nicht nur permanente Verfügbarkeit wichtig, sondern auch der Nachweis, dass sie zu einem bestimmten Zeitpunkt so und nicht anders vorgelegen haben. Unternehmer wollen zum Beispiel juristisch sicher beweisen können, dass ein elektronisch aufgesetzter Vertrag zu einem bestimmten Zeitpunkt in exakt dieser Form abgeschlossen wurde. Und wer eine elektronische Steuererklärung abgibt, will die fristgerechte Einreichung dokumentiert sehen. Das Institut für Telematik hat eine dem herkömmlichen Post-Eingangsstempel ebenbürtige elektronische Lösung entwickelt, die einfach zu bedienen, aber trotzdem hochsicher ist: einen Zeitstempeldienst.

Time Stamping Service: Electronic Substitute for the Post Receipt Stamp

As regards electronic documents, today it is not only important that they are available on a permanent basis, but they must also provide evidence that they existed in the particular form and at a specified time and not otherwise. Businessmen, for example, want to be able to produce sufficient legal evidence confirming that the electronically drawn contract was concluded in an exactly specific form and at the exactly specific time. Anyone filing an electronic income tax return will see a submission documented within the stipulated period. The Institute for Telematics has developed an easy-to-use but extremely secure electronic solution equivalent to a standard postal receipt stamp.

Zwar gibt es am Markt schon vergleichbare Software und Infrastrukturen von anderen Anbietern. Dem Institut für Telematik war jedoch eine Eigenentwicklung wichtig, die sich durch den Vorteil geringer Programmgröße, hohen Benutzerkomforts und Software-Implementierung mittels offener Standards auszeichnet. Der digitale Zeitstempel, der auf den Verfahren der digitalen Signaturen beruht, erwies sich dabei als tauglichste Lösung.

Funktionsweise

Das auf den Benutzer-Computer herunterzuladene Programm (ohne Java-Umgebung nur wenige hundert Kilobytes groß) erstellt auf Knopfdruck eine praktisch einmalige Kurzform („Hash-Wert“) derjenigen Datei, die einen Zeitstempel erhalten soll. Aufgrund der dabei verwendeten Einweg-Funktion ist es unmöglich, diesen elektronischen „Fingerabdruck“, der aus einer nicht lesbaren Zeichenfolge besteht, in die Originaldatei zurück zu verwandeln. Der elektronische Fingerabdruck wird über eine verschlüsselte Internet-Verbindung (https) an den Zeitstempel-Server im hochsicheren Trust Center des Instituts für Telematik in Trier gesendet. Dort, beim „elektronischen Notar“ , wird der Zeitstempel angebracht. Die Zeit bezieht der Server dabei über die Atom-Uhr in Braunschweig.

Wenige Augenblicke später wird die Antwort, die den Zeitstempel und die Signatur des Zeitstempels enthält, über eine ebenfalls verschlüsselte Internet-Verbindung an den Benutzer zurück gesendet. Dieses Verfahren ermöglicht eine eindeutige und zweifelsfreie zeitliche Zuordnung der entsprechenden Dokumente. Auf dem selben Weg lässt sich durch einen beliebig oft wiederholbaren Datenabgleich zwischen Sender und Zeitstempel-Server jederzeit überprüfen, ob das Dokument zwischenzeitlich verändert worden ist. Somit dürfte es bei Firmen und Behörden in Zukunft keine Probleme mehr beim Vergleich der verschiedenen Dateiversionen eines elektronisch gespeicherten Dokumentes geben.
Das Zeitstempelsystem kann auch die Sicherheit im Bereich der Computer-Logfiles deutlich verbessern. Diese dokumentieren fortlaufend sicherheitsrelevante Ereignisse. Wünschenswert ist hier, dass Logs im Nachhinein nicht manipuliert werden können bzw. dass etwaige Manipulationen bemerkt werden.

Technik

Gemäß seiner Philosophie setzt das Institut für Telematik bei der Entwicklung auf offene Standards. Sowohl die Anwendung zum Anfordern und Überprüfen des Zeitstempels durch den Benutzer als auch der Zeitstempel-Server im Institut für Telematik wurden in der offenen Programmiersprache JAVA programmiert. Dies garantiert zum einen die Plattformunabhängigkeit der Software, zum anderen können die Programme problemlos an spezielle Anforderungen von Kunden angepasst oder erweitert werden.

6. Telemedizin – das mobile Patienten-Informationssystem Cura Call

Viele Menschen scheuen den Weg zum Arzt, weil sie ihre Gesundheit nicht als akut bedroht ansehen. Dennoch ist es zum Beispiel im Rahmen der Vorsorge und für die Einhaltung von Impfterminen wichtig, regelmäßig den Arzt zu konsultieren. Besonders gilt das zum Beispiel für Kleinkinder (Impftermine, Früherkennung) und ältere Menschen (Vorbeugung). Auch Frauen benötigen von einem bestimmten Alter an gesonderte, geschlechtsspezifische Untersuchungen. Leider zeigt sich in den letzten Jahren eine gewisse Müdigkeit der Bevölkerung bei der Teilnahme an Schutzimpfungen und Vorsorge-Untersuchungen. Empfohlene Termine werden immer öfter nicht registriert oder einfach nicht eingehalten. Um hier helfend einzugreifen, hat das Institut für Telematik zusammen mit der Firma ITMS AG (Essen) das automatische Benachrichtigungs-System „Cura Call" entwickelt.

Telemedicine – the Cura Call Mobile Information System for Patients

Many people shy away from seeing their doctor unless they feel acutely ill. However, it is important to consult your doctor regularly either as a preventative measure or to keep a vaccination appointment, for example. Even more so in case of small children (vaccination terms, early diagnosis) and the elderly (prophylactic measures). Having reached certain years of age, women too must have some sex-specific tests. Unfortunately, over the past few years there has been a kind of tiredness on part of citizens when it comes to having vaccination and preventive tests. There have been more and more people failing to make, or to simply keep their recommended appointments. To offer help, the Institute for Telematics and the company ITMS AG (Essen) have developed an automated information system, called "Cura Call".

Mit dem Cura Call-System können Ärzte ihren Patienten zur gegebenen Zeit automatisch eine SMS oder eine elektronische Mail senden. Diese erinnert den Patienten spätestens eine Woche vor einem anstehenden Termin daran, sich mit der Arztpraxis in Verbindung zu setzen und einen Besuchstermin zu vereinbaren.

In der Arztpraxis brauchen nicht mehr zunächst alle Patientendaten manuell ausgewertet werden, um anschließend dann Briefe zu versenden. Das Cura Call-System entlastet das Praxis-Personal von solch zeitraubender und kostspieliger Verwaltungsarbeit. Per Mausklick werden aus einer zuvor aufgebauten Datenbank die passenden Patientendaten ausgelesen und eine Sammelnachricht konstruiert, die der Provider in die einzelnen SMS-Nachrichten aufsplittet und anschließend versendet.

Sollte der Patient nicht reagieren, so wird er automatisch auch ein zweites Mal an den Arzt-Termin erinnert.

Technisch wird die Cura Call-Lösung unter open-source-Software betrieben, wobei eine Konvertierung auf andere Betriebssysteme in Vorbereitung ist. Die Daten der Patienten werden mit Hilfe eines Lesegerätes für die Krankenkassenkarte eingelesen und zusätzlich mit der Nummer des Mobil-Telefons des Patienten bzw. mit der E-Mail-Adresse versehen.

Der Verbindungsaufbau zum Telekommunikationsnetz erfolgt über Modem oder eine eingebaute ISDN-Karte. Steht die Verbindung zum Internet, braucht es nur wenige Sekunden, um alle Nachrichten zu versenden.

Weiterentwicklungen

Zur Zeit wird das System weiter entwickelt, um noch spezifischer auf die individuellen Bedürfnisse der Patienten reagieren zu können. So speichert das System nicht nur die Termine der üblichen Vorsorge-Untersuchungen und Impfungen, sondern es erinnert den Patienten bezogen auf einen bereits wahrgenommenen Termin auch im passenden Zeitintervall an die Folge-Besuche beim Arzt. Ein Standard-Beispiel dafür ist die Erinnerung an die Tetanus-Schutzimpfung, weil dabei im Verlauf eines Jahres unter Einhaltung eines bestimmten Rhythmus' mehrere Impfungen verabreicht werden müssen, um den bestmöglichen Schutz zu erreichen.

Die Idee eines solchen Konzeptes lässt sich auch auf andere Gebiete der Gesundheitsversorgung übertragen. Denkbar ist zum Beispiel eine Erinnerung an die zeitgenaue Einnahme bzw. Verabreichung von Medikamenten.

7. Patienten-CD: Medizinische Bilder am PC betrachten und kompakt archivieren

Das Institut für Telematik hat ein Patienten-CD-System entwickelt, das Medizinern den schnellen und benutzerfreundlichen Aufbau einer mobilen, übertragbaren Patientenakte sowie die kompakte, übersichtliche Langzeitarchivierung von Bilddaten ermöglicht.

Patient CD: Trouble-Free Viewing of Medical Images on PC and Archiving of Compacted Images

The Institute for Telematics has developed a CD system for patients providing doctors with a possibility of fast and user-friendly creating of cellular and transferable patient records, as well as compact and clear long-term archiving of image data.

Bilder aus Röntgen-, CRT-, MRT- und Ultraschall-Untersuchungen können mit dem Patienten-CD-System einfacher und preiswerter archiviert werden als bisher. Zudem wird der Datenaustausch leichter. Die bei einer Untersuchung auf einen herkömmlichen CD-bzw. DVD-Rohling geschriebenen medizinischen Bilder können an jedem herkömmlichen Personal-Computer in hervorragender Qualität und ohne Qualitätsverlust betrachtet werden. Dafür sorgt eine leistungsfähige Betrachtungssoftware, die auf der Patienten-CD gespeichert ist.

Gespeichert werden die Bildserien auf der CD-ROM im international anerkannten „DICOM 3"-Format. Das auf der Patienten-CD gespeicherte Betrachtungsprogramm erlaubt z.B. die Vergrößerung per Lupen-Funktion, das Messen von Abständen und Winkeln sowie die Veränderung des Kontrastes. Das Patienten-CD-System beinhaltet eine integrierte Hilfefunktion, die Tipps zum schnellen und komfortablen Arbeiten ohne große Vorkenntnisse gibt. Das Archivprogramm auf CD-ROM-Basis zeichnet sich auch durch hohe Kompatibilität mit gängigen Betriebssystemen aus.

Die Vorteile des Patienten-CD-Systems für den Arzt sind beträchtlich:

- preisgünstiges und Hersteller unabhängiges System zur Archivierung von digitalen Bilddaten
- unkomplizierter Datenaustausch und Kommunikation mit Kollegen durch CD-Weitergabe
- Ausweitung des Patienten-Serviceangebotes.

Auch für den Patienten weist das Patienten-CD-System viele Vorteile auf:

- jederzeitiger Zugriff auf die persönlichen Bilddaten
- Möglichkeit der Weitergabe an den behandelnden Arzt
- Vermeidung von Mehrfachuntersuchungen
- Verwendung im Familien- und Freundeskreis.

Jede Patienten-CD enthält bereits den zur Bildbetrachtung notwendigen DICOM Viewer. Dies gewährleistet für Arzt und Patient überall und jederzeit die unmittelbare Verfügbarkeit der archivierten Patientenbilder.

8. Mobile Computing - automatische Fahrtenbuch-führung mit Handheld und GPS

Die Verbreitung mobiler Kleingeräte (Handys, Handhelds etc.) hat in den letzten Jahren erheblich zugenommen. Das Institut für Telematik entwickelt spezielle Anwendungen für diese Geräte, um die Vorteile dieser neuen Technologien nutzerfreundlich und praxisgerecht zur Verfügung stellen zu können. So war zum Beispiel die Führung eines Fahrtenbuchs bislang eine lästige, umständliche und zeitraubende Angelegenheit. Eine Vielzahl von Angaben musste bisher von Hand in das Fahrtenbuch eingetragen werden. Um diese mühevollen Aufzeichnungen auf ein Minimum zu reduzieren, wurde am Institut für Telematik ein elektronisch geführtes, GPS-unterstütztes Fahrtenbuch für PalmOS®-Handhelds entwickelt - eine große Erleichterung für jeden, der die Kosten für Autofahrten abrechnet.

Mobile Computing – Automated Driver's Logbook Keeping with a Handheld and GPS Support

Over the past few years, the widespread use of small devices (cellular phones, handhelds, etc.) has been considerably increasing. The Institute of Telematics has been developing special applications for the above devices so that the advantages of the new technologies are made available in a user-friendly and practical way. For example, the driver's logbook keeping was, until recently, a most annoying, awkward and time-consuming work to do. A large number of data had to be entered manually. To minimize the tiresome record work, the Institute for Telematics has developed an electronically kept and GSP supported driver's log for PalmOS® handhelds – a great relief for anyone in charge of calculating the cost of drive.

Dieses Fahrtenbuch ermittelt die meisten Daten einer Autofahrt automatisch. Im Gegensatz dazu müssen Nutzer konventioneller Fahrtenbuch-Programme bislang immer erst selbst die Tachometer-Daten ablesen und dann zusammen mit zahlreichen anderen wichtigen Informationen manuell eingeben. Diese Vorgehensweise ist jedoch vielen Autofahrern so unbequem, dass sie dem Finanzamt kein Fahrtenbuch vorlegen, sondern die für sie ungünstigere Pauschalversteuerungslösung wählen. Die automatische Fahrtenbuchführung für Palm-Nutzer hingegen reduziert solche manuellen Eingaben auf das Minimum.

Eintragungen	elektronisches **Fahrtenbuch** ohne GPS	elektronisches **Fahrtenbuch** mit GPS
Datum und Uhrzeit	automatisch	automatisch
KM-Stand (Fahrtbeginn)	automatische Übernahme des aktuellen Kilometerstands	automatische Übernahme des aktuellen Kilometerstands
KM-Stand (Fahrtende)	muss eingegeben werden	**automatische Berechnung**
Gefahrene Kilometer	automatische Berechnung	automatische Berechnung
Name des Fahrers	automatisch Übernahme des letzten Eintrags	automatisch Übernahme des letzten Eintrags
Reiseroute	muss eingegeben werden	**automatische Ermittlung**
Reisezweck	muss eingegeben werden	muss eingegeben werden

Abb.1: Daten eines Fahrtenbuches

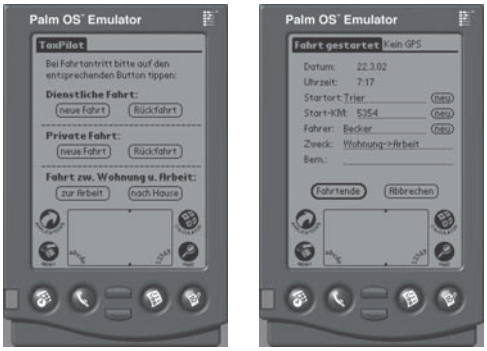


Abb. 2: Das Fahrtenbuchprogramm auf einem Handheld

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

Das Verfahren funktioniert folgendermaßen: Zu Beginn der Fahrt drückt der Nutzer auf „Start". Das elektronische Fahrtenbuch zeigt ihm das aktuelle Datum und die Uhrzeit. Als Startort-Angabe wird das Ziel des letzten Eintrags vorgeschlagen, als Kilometerstand der zuletzt gespeicherte Wert. Diese in einem Formular erscheinenden Angaben können vom Anwender manuell geändert werden. Nach Fahrtende tippt der Nutzer auf „Stopp". Es öffnet sich ein neues Formular mit der aktuellen Datums- und Zeitangabe. Mit den

vom GPS-Empfänger gelieferten Daten ermittelt das elektronische Fahrtenbuch nun automatisch den Kilometerstand bei Fahrtende und das Reiseziel. Manuell müssen nur noch der Fahrername eingegeben (vorgeschlagen wird zunächst immer die Angabe des letzten Eintrags) und der Fahrtzweck ausgewählt werden.

Die Daten werden im Handheld gespeichert und mittels eines mitgelieferten Programms (sogenanntes Conduit) beim nächsten Synchronisationsvorgang des Handhelds (HotSync®) auf den PC übertragen. Vom PC aus können die Daten mit der mitgelieferten Software betrachtet und zur Vorlage beim Finanzamt ausgedruckt werden.

Ideenreich musste bei der Umsetzung der GPS-Koordinaten in Ortsnamen vorgegangen werden: Da dies eine größere Datenbank benötigt, als sie

Abb. 4: Das Fahrtenbuch in Aktion

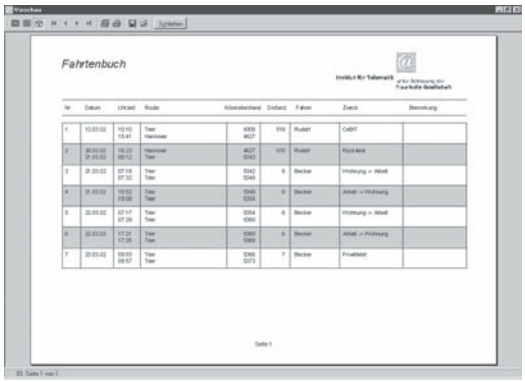


Abb. 3: Ansicht des Fahrtenbuchs am PC

das Palm-System speichern kann, zeigt das elektronische Fahrtenbuch zunächst nur Großstädte automatisch an. Da aber die Geo-Daten der kleineren angefahrenen Orte ebenfalls gespeichert werden, lernt das Programm automatisch die neuen, vom Fahrer manuell ergänzten Ortsnamen.

Vermarktungspartner des Instituts für Telematik ist das Essener Unternehmen ITM Service AG (www.dicomzip.de).

Global Positioning System

Das Global Positioning System (GPS) basiert auf einem Verbund von mehr als 24 nichtstationären Satelliten. Sie sind so angeordnet, dass von jedem Punkt der Erdeoberfläche mindestens zwölf dieser Satelliten am Horizont „sichtbar" sind.

Diese Satelliten funken permanent ihre aktuelle Position und die genaue Uhrzeit zur Erde. Ein GPS-Empfänger kann - freie Sicht zu mindestens drei Satelliten vorausgesetzt - diese Signale auswerten und somit seine eigenen Positionsdaten bestimmen.

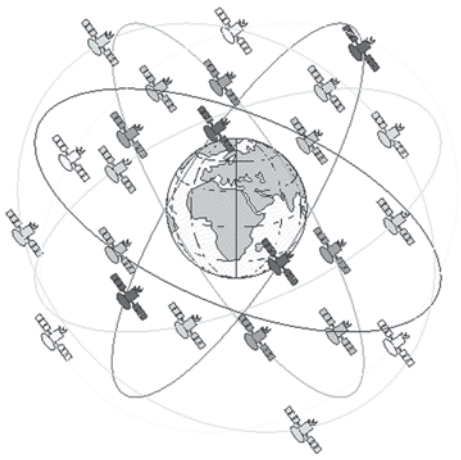


Abb. 5: Anordnung der GPS-Satelliten

9. E-Learning: Uni-Vorlesungen live und auf Abruf am Heim-PC mitverfolgen

Das Wissen um die Technik des Internets breit zu fördern sowie eine möglichst einfache Zugangstechnik für Online-Vorlesungen über Internet-Themen zu entwickeln und bereit zu stellen, hat sich das Trierer Institut für Telematik gemeinsam mit der örtlichen Universität zur Aufgabe gemacht. Von der Wohnung oder vom Büro aus soll jeder PC-Nutzer mit geeignetem Internetanschluss - ob interessierter Laie, Fachspezialist oder eingeschriebener Student - Lehrveranstaltungen komfortabel und kostenlos mitverfolgen können.

E-Learning: University Lectures Live and on Call on the Home PC

One of the common tasks of the Trier Institute for Telematics and the local university is to improve the general knowledge of the Internet technology, and to develop and prepare an extremely straightforward access to online lectures via the Internet topics. Whether a lay person interested in the subject, a specialist, or a regular student, every PC user with an adequate Internet connection can follow courses free of charge and while comfortably sitting at home or in an office.

Im Wintersemester 2001/2002 wurden zum Beispiel Trierer Informatik-Vorlesungen zu dem Thema „Technische Grundlagen des Elektronischen Publizierens“ live und online im World Wide Web übertragen. Trotz der damals noch vergleichsweise komplizierteren Zugangstechnik gab es eine beträchtliche Resonanz: Aus 18 Ländern „klickten“ sich Teilnehmer weltweit ein und weit mehr als 1000 Zugriffe auf die archivierten Vorlesungsmaterialien wurden zu Semesterende gezählt. Die technischen Voraussetzungen waren sehr hoch. Benötigt wurde ein Java fähiger PC und zumindest ein DSL-Anschluss mit Multicastunterstützung oder – besser noch – eine Standleitung. Ferner war die Installation spezieller Software erforderlich.

Um den technischen Fortschritt weiter voran zu treiben, wurde noch im Verlauf des Wintersemesters eine Lösung entwickelt, die eine drastische Vereinfachung des Zugangs zu solchen Online-Vorlesungen ermöglicht. Sie heißt „tele-TASK“. Das steht für Teleteaching Anywhere Solution Kit. Eingesetzt wird diese Technik seit Sommersemester 2002. Jeweils dienstags und donnerstags können sich „e-Learner“ zwischen 8 und 10 Uhr vom Heim- oder Büro-PC aus in den Hörsaal V 301/302 der Uni Trier „klicken“, um die Vorlesung „Informationssicherheit im Internet“ in Ton und Bild live mitzuverfolgen. So werden die ureigenen Möglichkeiten des Internets genutzt, um die vielfältigen und zum Teil gravierenden Sicherheitsprobleme im weltweiten Computer-Netzwerk einer breiten Öffentlichkeit verständlich zu machen. Durch das sogenannte „Teleteaching“ ist die Teilnahme an der Vorlesung auch für solche Interessenten möglich, die in dieser Zeit nicht vor Ort sein könnten oder sonst gar keine Berechtigung zur Teilnahme an Uni-Veranstaltungen hätten. Einzige Voraussetzung: Ein Internetanschluss mit ISDN- oder - noch besser - DSL-Verbindung und das in jedem gängigen Browser verfügbare Standard-Programm „Real Player“.

Übermittelt werden nicht nur – wie sonst üblich – Live-Bild und -Ton vom Dozenten, sondern simultan dazu auch die Lehrinhalte, welche die Studenten im Hörsaal an die „elektronische Tafel“ projiziert bekommen. Sogar die handschriftlichen Ergänzungen, die der Dozent während der Vorlesung auf die elektronische Tafel (Smart Board) schreibt, können vom „e-Learner“ am PC mitverfolgt werden. Zusätzlich hilft ihm eine Navigationsleiste, auf sehr einfache Weise zu einzelnen, ihn besonders interessierenden Teilen der Vorlesung zu surfen. Zusätzlich werden die Trierer Vorlesungen aufgezeichnet und archiviert, damit sich jeder auch später noch in den Stoff vertiefen und sich die Studenten intensiver auf Prüfungen vorbereiten können.

Die höheren Kennziffern für die tatsächliche Nutzung des Trierer Teleteaching-Angebots beweisen bereits im Mai 2002, dass die einfachere Zugangstechnik Hürden abgebaut hat. Schon nach sechs Terminen wurden weit mehr als 2000 Zugriffe auf Live- bzw. On-Demand-Inhalte verzeichnet. Positive Resonanz seitens der Studenten, ein Fernsehbericht sowie unter anderem ein Artikel in der britischen Tageszeitung „The Times“ bestätigen den Fortschritt.

Weitere Informationen über die Online-Vorlesungen befinden sich auf der Homepage des Instituts für Telematik http://www.ti.fhg.de/publikationen/online-vorlesungen/index.html oder sind unter http://www.tele-task.de zu finden.

10. Sicherheits-Anforderungen an den Betrieb lokaler Funknetze (WLAN)

Lokale Funknetze (Wireless Local Area Networks, WLAN) bieten - einfach gesagt - geeigneten mobilen Endgeräten die Möglichkeit, kabellos Daten mit Firmennetzwerken oder dem Internet auszutauschen. Die Vorteile solcher Funknetze liegen hauptsächlich im schnelleren Auf- und Ausbau der notwendigen Infrastruktur. Ein gewichtiger Nachteil ist allerdings das Sicherheitsproblem. Welche Lösungsmöglichkeiten es dafür gibt, hat das Institut für Telematik in einem Projekt erforscht.

Security Requirements for the Operation of Local Radio Telephone Networks (WLAN)

In plain words, local radio telephone networks (Wireless Local Area Networks, WLAN) provide the cellular terminals with a possibility of a wireless data exchange with corporate networks or with the Internet. Advantages of such radio networks in particular ensure a faster setting up and upgrading of the necessary infrastructure. A serious drawback is the issue of security. In one of its projects, the Institue for Telematics dealt with possible solutions to the problem.

Unter Wireless LAN (WLAN) versteht man im Allgemeinen ein Funknetz, dass auf dem Standard des Institute of Electrical and Electronics Engineers IEEE 802.11b basiert. Anwender können dadurch zum Beispiel einen Laptop in einem geschlossenen Firmennetz oder im offenen Internet betreiben, ohne dass eine Kabelverbindung die Bewegungsfreiheit einschränkt.

WLAN-Vorteile

Wireless LAN haben unbeschrittene Vorteile gegenüber den „normalen" Netzen. Da die übliche Verkabelung entfällt, kann wesentlich schneller die notwendige Infrastruktur aufgebaut und erweitert werden. Wo bei konventionellen Kabelnetzen zu jedem einzelnen Netzteilnehmer eine separate Verbindung geschaffen werden muss, reicht bei WLAN die Verkabelung einiger Basisstationen (Access-Points), die auf empfangstechnisch optimale Punkte verteilt werden. Steht diese Infrastruktur, ist das Hinzufügen neuer Teilnehmer zum Netz ohne Probleme möglich. Einzig eine Funk-Karte (WLAN-Karte) muss in den Laptop/PC eingebaut werden. Bei der Benutzung unterscheidet sich die Anwendung dann nicht mehr vom Einsatz einer normalen Netzwerkkarte.

WLAN-Nachteile

Allerdings gibt es auch negative Seiten. Der WLAN-Standard garantiert eine Übertragungsrate bis maximal 11MBit/s, die sich alle Laptops bzw. PC's teilen müssen, die über die selbe Basis-Station mit dem Funknetz verbunden sind. Zwei gleichzeitige Nutzer haben dann also nur noch eine Übertragungsrate von gut 5MBit/s, drei nur noch von knapp 4MBit/s und so weiter. Auch wirkt sich die Entfernung und die Gebäudeformation zwischen Basis-Station und Funk-Karte negativ auf die Leistung aus. Mit Basis-Stationen sollte also nicht gespart werden, wenn man an den Aufbau eines WLAN nachdenkt.

Ein noch gewichtigerer Aspekt bei lokalen Funknetzen ist jedoch die Sicherheit. Der WLAN-Standard definiert mit dem WEP-Protokoll (Wired Equivalent Privacy) eine Möglichkeit der verschlüsselten Kommunikation zwischen Funk-Karten und Basis-Station. Zur Zeit sind zwei Variationen des WEP-Protokolles üblich: WEP 40 und WEP 128. Beide Verfahren leiden unter dem prinzipiellen Problem, dass durch Mithören des Datenstromes der Schlüssel berechnet werden kann, mit dem die Daten zwischen Basis-Station und Funk-Karte verschlüsselt werden. Inzwischen sind sogar Werkzeuge im Internet erhältlich, die es auch technisch nicht versierten Personen ermöglichen, den Schlüssel zu knacken und damit den Datenverkehr abzuhören. Somit ist eine Absicherung allein durch das WEP-Protokoll nicht geeignet.

Sicherheitslösungen

Eine höhere Sicherheit ergibt sich durch die Verwendung von Virtual Private Networks (VPN). VPN werden verwendet, um in öffentlichen Netzen einen sicheren „Tunnel" zwischen zwei Kommunikationspartnern aufzubauen. Als Beispiel kann man sich zwei Firmenstandorte vorstellen (z.B. einer in Europa und einer in Asien). Standleitungen zwischen diesen Orten sind viel zu teuer. Preiswert hingegen sind Standleitungen ins Internet. Mit VPN wird das Internet zur Übertragung der Daten zwischen den Firmenstandorten

genutzt. Die Verschlüsselung garantiert, dass kein anderer Internetnutzer den Datenstrom entschlüsseln kann. Durch VPN erscheinen die beiden Firmennetze wie ein einziges großes privates Firmennetz.

Eine weitere Möglichkeit, WLAN sicherer zu machen, ist die Verwendung von Radius-Servern für die Autorisierung. Sie sichern zunächst den Zugang zu den Basisstationen, bieten also für die Abhörsicherheit zunächst keinen Vorteil. Unterstützen die Basisstationen jedoch das EAP (Extensible Authentication Protocol) oder LEAP (Lightweight Extensible Authentication Protocol), kann der Radius-Server dazu beitragen, die bei der WEP-Kommunikation verwendeten Schlüssel zwischen Basisstation und Funkkarte neu auszuhandeln. Da zur Berechnung des verwendeten WEP-Schlüssels durch Abhören eine bestimmte Anzahl von abgehörten Datenpaketen benötigt wird, erhöht das häufige Neu-Aushandeln der Schlüssel den Aufwand für einen potentiellen Angreifer erheblich und reduziert damit das Risiko.

Individuelle Beratung durch das Institut für Telematik

Das Institut für Telematik hat 2001 die Infrastruktur für die Einführung eines WLAN im Institut konzipiert. Ziel war weniger die Umsetzung aller denkbaren technischen Möglichkeiten, sondern zunächst die Definition der gewünschten und erwarteten Eigenschaften und Sicherheitsaspekte, die mit einem solchen Funknetz verbunden sind. Wie weit können zusätzliche Komponenten in der Konzeption die Sicherheit erhöhen oder ein Mehr an Fähigkeiten bereitstellen und was kostet dies? Kann auf einige Eigenschaften unter Umständen verzichtet werden? All diese Fragen wurden in einer Matrix zunächst aufgelistet und anschließend priorisiert. Auf Grundlage dieser Liste konnte in einem letzten Schritt ein WLAN-Komplex konzipiert werden, der die hohen Ansprüche des Instituts für Telematik an Service und Sicherheit erfüllt und gleichzeitig in einem vernünftigen finanziellen Rahmen bleibt. Da andere Priorisierungen und finanziellen Rahmenbedingungen zu anderen WLAN-Komplexen führen, muss bei jeder Planung ein maßgeschneiderter Entscheidungsprozess neu durchgeführt werden. Das Institut bietet dafür seine Expertise an.

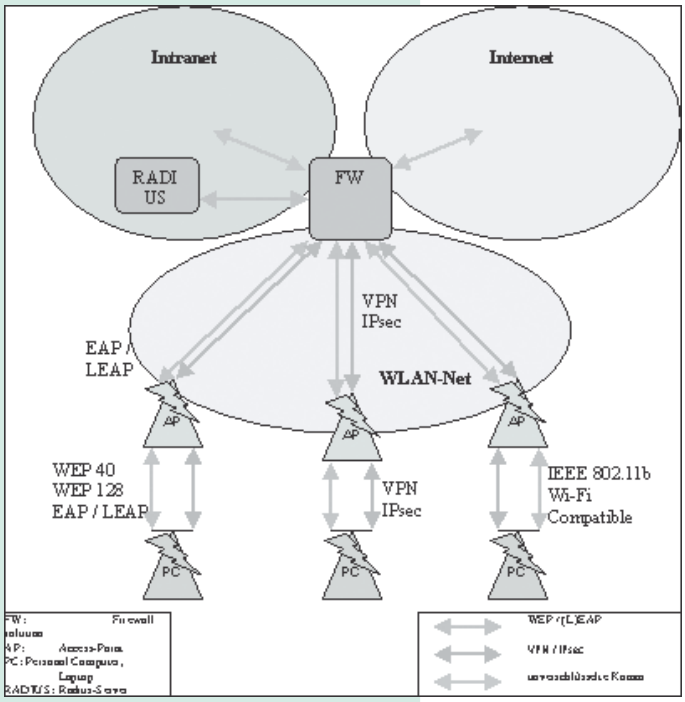


Abb. 1: Trennung von Internet, Intranet und WLAN-Netz. Radius-Authentifikation. WEP-Verschlüsselung. VPN-Tunnel mittels IPsec.

11. Telefonieren über das Internet - Computer-Telefonie-Integration und Voice over IP

Werden Telefongespräche über Computer- und Datennetze übertragen, spricht man von der „Voice over IP"-Technik (VoIP). Dabei kommt das allgemein übliche Internet-Protokoll (TCP/IP) zum Einsatz, um die Sprachdaten als Datenpakete zu übertragen. Es lassen sich aber auch die Fähigkeiten von Computern und Telefonen kombinieren. Der Fachbegriff dafür ist „Computer-Telefonie-Integration" (CTI). Hier geht es um die funktionelle Integration beider Techniken. Wie man zum Beispiel einen Linux-PC als Telefonanlage für VoIP einsetzen könnte, hat das Institut für Telematik erforscht.

Making Telephone Calls via the Internet – Computer Telephony Integration and Voice over IP

Voice over IP (VoIP) is when telephone conversations are transmitted via the computer network and data network. In that case, the commonly implemented Internet protocol (TCP/IP) is used to ensure that voice data is transmitted as data packets. Moreover, possibilities of computers and telephones can be combined. Technically, this is called "computer telephony integration" (CTI). It is about a functional integration of both technologies. The Institute for Telematics studied, for example how a Linux PC could be used as a telephone device.

Voice over IP-Telefonie

Bei VoIP konkurrieren zwei Standards. Zum einen gibt es die Rahmenempfehlung H.323 „Packet-based multimedia communication systems" der International Telecommunication Union (ITU) in Genf. Wie der Begriff „multimedia" schon andeutet, beschränkt sich der Standard H.323 nicht auf reine Telefonie, also Sprache (Audio), sondern beschreibt die Übertragung und Signalisierung von Audio, Video und Daten über paketbasierte Netze. Der Standard sieht auch Videokonferenzen vor. Insofern stellt der Begriff „Voice over IP" eine Einschränkung der tatsächlich vorgesehenen Möglichkeiten dar.

Der zweite, in der Vergangenheit weniger bedeutende Standard, ist das so genannte Session Initiation Protocol (SIP). Es wurde von der Internet Engineering Task Force (IETF) ausgearbeitet und basiert auf dem Hypertext Transfer Protocol HTTP. Welcher der beiden Standards sich letztendlich durchsetzen wird, ist im Moment noch nicht abzusehen. Beide haben ihre Vor- und Nachteile. So braucht SIP z.B. weniger Ressourcen und ist deshalb für portable Endgeräte besser geeignet. Ein dauerhaftes Nebeneinander ist durchaus denkbar.

Computer-Telefonie-Integration

Die Computer-Telefonie-Integration (CTI) erlaubt es, die Fähigkeiten von Computern und Telefonen zu kombinieren. CTI macht es Computeranwendungen möglich, Telefonverbindungen aufzubauen, zu beenden und weiterzuleiten. Umgekehrt können aber auch Telefonverbindungen Computeranwendungen beeinflussen und als Eingabe dienen. Die Möglichkeit der gegenseitigen Einflussnahme ist der eigentliche Mehrwert und erlaubt es, Arbeits- und Kommunikationsabläufe im Büro rationeller zu gestalten.

Projekt: Linux-PC als Telefonanlage für VoIP

Wie man ein normales ISDN-Telefon nutzen kann, um günstig über das Internet zu telefonieren, hat das Institut für Telematik in einem Projekt untersucht. Die Graphik zeigt den verwendeten Aufbau.

Die Versuchsanordnung verwendet zwei Rechner mit dem Betriebssystem Linux und eingebauter Netzwerk-und ISDN-Karte. An zwei verschiedenen Standorten übernehmen die Rechner jeweils die Funktion eines so genannten VoIP-Gateways in das Internet, bilden also eine Brücke vom Telefonnetz zum Internet. Das interne lokale Netzwerk (LAN) des Instituts übernimmt im Versuchsaufbau zunächst die Rolle des Internets. An beiden Standorten ist eine Telekommunikations-Anlage installiert, über die weiterhin Gespräche über das öffentliche Telefonnetz geführt werden können.

Der Wählvorgang geschieht wie folgt: Teilnehmer A hebt ab und wählt die Durchwahl „seines" Linux-Gateways. Anschließend gibt er als Nachwahl die Rufnummer des gewünschten Gesprächspartners an. Diese Rufnummer beinhaltet sowohl die Information zur Identifikation des zu erreichenden Gateways als auch die Information zur Iden-

tifikation des gewünschten Gesprächspartners B. Hebt letzterer ab, wird die Verbindung aufgebaut und das Gespräch kann beginnen.

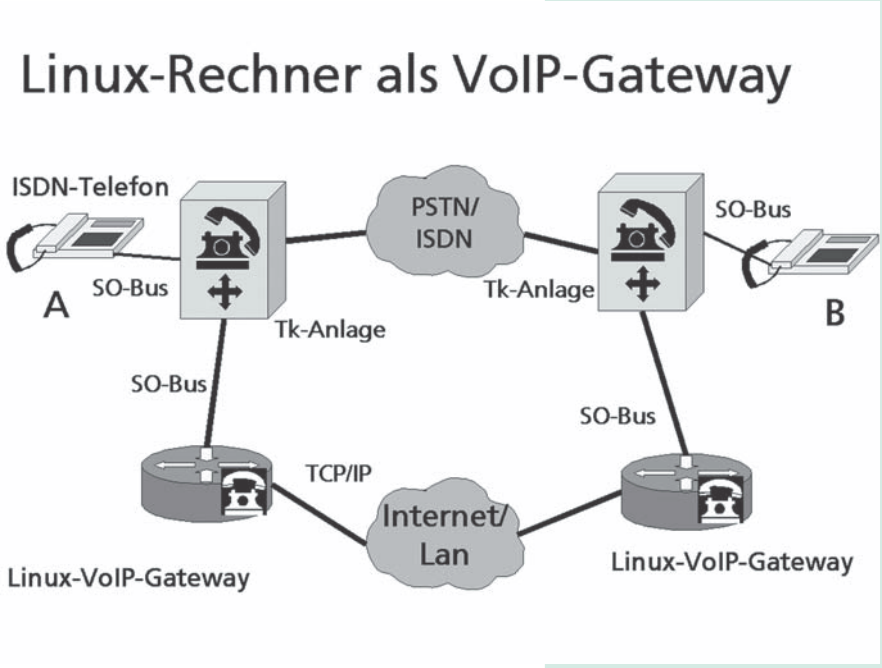


Abb. 1: VoIP - Verbindung mit VoIP-Gateways parallel zum Telefonnetz

Fazit

Das noch etwas komplizierte Prozedere macht den Forschungs- und Entwicklungsbedarf deutlich, den es auf dem Gebiet von VoIP und CTI noch gibt. Wünschenswert wäre zum Beispiel, dass das Telefon von Teilnehmer A direkt mit dem Gateway verbunden ist. In einer Datenbank müssten zudem die Rufnummern der zu erreichenden Teilnehmer gespeichert sein. Das Linux-Gateway könnte dann selbstständig entscheiden, ob der gewünschte Teilnehmer per VoIP über das Internet oder auf dem bisher üblichen Weg über das öffentliche Telefonnetz (ISDN oder analog) angewählt wird. Im Idealfall müsste sich der Anrufende dann nicht mehr darum kümmern, welchen Weg sein Gespräch nimmt.

Ein langfristiges Ziel im Bereich VoIP und CTI sollte es sein, jedem PC-Benutzer ein „VoIP-Gateway" auf seinem Arbeitsplatzrechner zur Verfügung zur stellen. Dieses sollte jedoch nicht nur auf VoIP, also auf Sprachübertragung, begrenzt sein, sondern Multimedia-Anwendungen einschließen. Daten-, Audio- und Videoübertragung werden dann in die alltäglich verwendeten Büroanwendungen wie z.B. in den E-Mail-Client integriert werden können.

Dissertationen

Im Jahr 2001 wurden drei Dissertationen von Institutsmitarbeitern verteidigt (Ernst-Georg Haffner) oder eingereicht (Harald Sack, Andreas Heuer). Im Folgenden werden diese Doktorarbeiten kurz erläutert.

Ernst-Georg Haffner:

Request Prediction and Hyperlink Proposals – Methodologies and Mathematics behind Web Applications

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

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

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

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

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

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

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

Harald Sack:

Improving the Power of Ordered Binary Decision Diagrams by Integrating Parity Nodes

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

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

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

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

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

Andreas Heuer:

Web Präsenz Management im Unternehmen – Entwicklung und Einsatz eines Java-basierten Online-Redaktionssystems

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

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

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

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

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

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

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

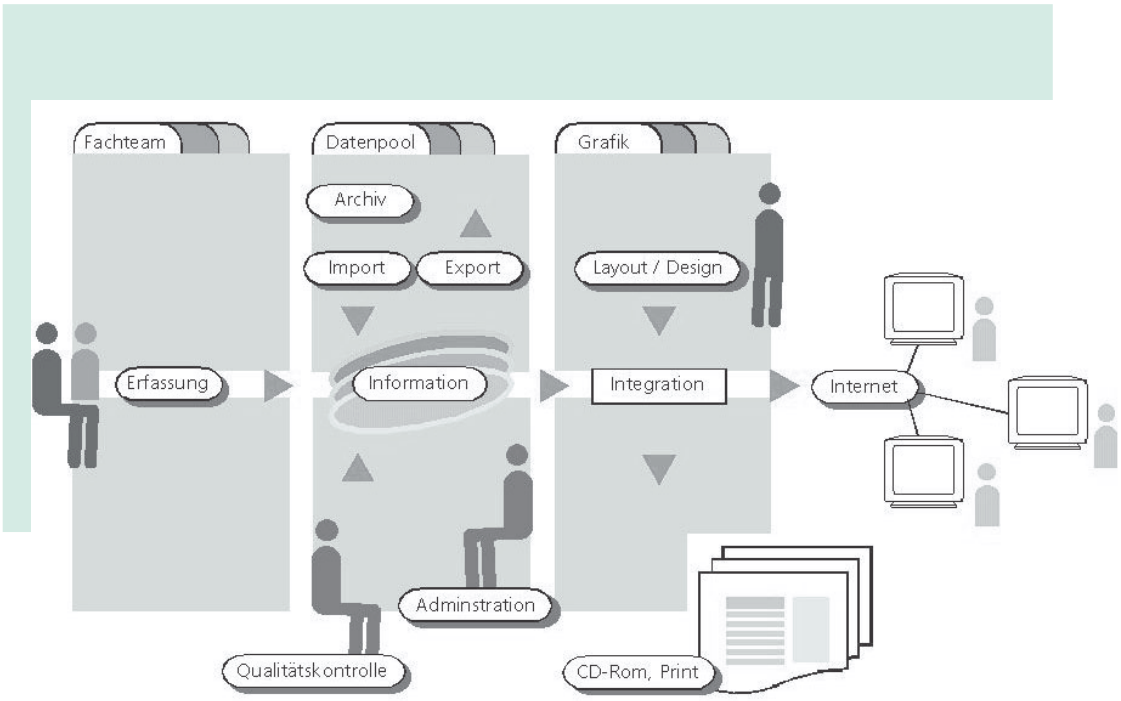


Abb. 1: Das Redaktionssystem jDaphne im Überblick: qualitätsgesichterter Informationsfluss von der Erfassung der Informationen über ihre Verarbeitung und Veredlung bis zur Publikation in verschiedenen Pulikationsmedien

Trierer Symposien

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 Kommunikationstechnologien 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 eines gemeinsamen Abendessens als äußerst positiv erwiesen.

Digitale Signaturen
15. und 16. November 2001

Mobile Commerce
7. und 8. Juni 2001

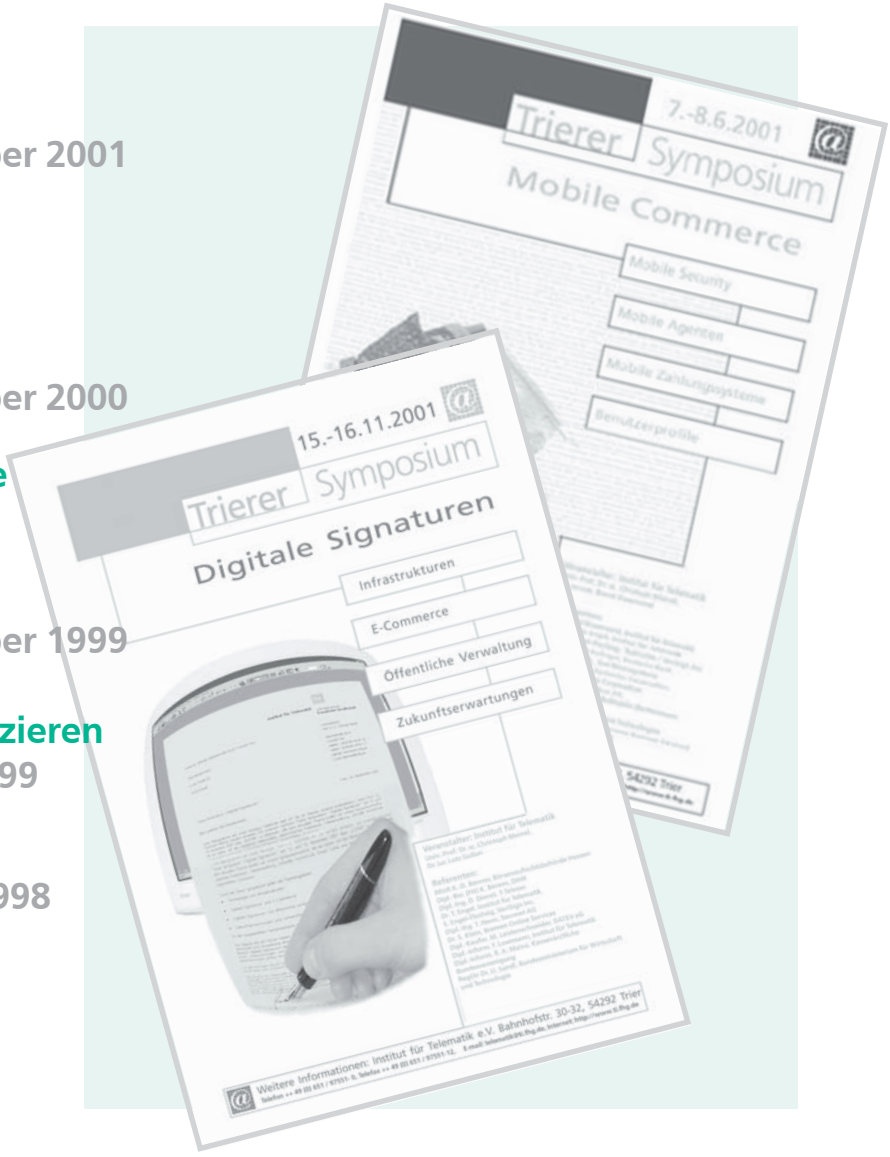
Smart Cards
23. und 24. November 2000

Virtuelle Hochschule
4. und 5. Mai 2000

Televerwaltung
11. und 12. November 1999

Elektronisches Publizieren
25. und 26. März 1999

Telemedizin
8. und 9. Oktober 1998



Trierer Symposium
15.-16.11.2001

Digitale Signaturen

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

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

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

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

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

Das Symposium hatte die Programmschwerpunkte

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

Trierer Symposium
7.-8.6.2001

Mobile Commerce

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

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

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

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

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

Das Symposium hatte die Programmschwerpunkte

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

Trierer Symposium
23.-24.11. 2000

Smart Cards

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

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

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

Das Symposium hatte die Programmschwerpunkte

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

Trierer Symposium
4.-5.5.2000

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
- Digitale Bibliothek

Trierer Symposium
11.-12.11.1999

Televerwaltung

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

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

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

Die Programmschwerpunkte waren

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

Trierer Symposium
25.-26.3.1999

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

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

Die Programmschwerpunkte waren

- Bibliotheken
- Verlagswesen
- Retrodigitalisierung
- Geschäftsmodelle

Trierer Symposium
8.-9.10.1998

Telemedizin

Das Institut für Telematik richtete am 8. und 9. Oktober 1998 das „Trierer Symposium“ mit dem Thema „Internet-Technologie in der Medizin“ aus. Mit dieser Veranstaltung schuf das Institut ein Forum, das Vertreter aus Forschung und Entwicklung und medizinische Praktiker nutzten, um sich über aktuelle Entwicklungen zu informieren und diese miteinander zu diskutieren.

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

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

Die Programmschwerpunkte waren

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


Trierer Symposium
Digitale Signaturen
15.-16.11.2001
Infrastrukturen
E-Commerce
Öffentliche Verwaltung
Zukunftserwartungen
Trierer Symposium
Mobile Commerce
7.-8.6.2001
Trierer
Elektronisches Publizieren
Verlagswesen
Bibliotheken
Retrodigitalisierung
Geschäftsmodelle

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 2001 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.

Online 2001

In Düsseldorf fand vom 31. Januar bis 1. Februar die Online 2001 statt. Das Institut war mit folgenden Themen vertreten:

Lock-Keeper

Die erst kürzlich patentierte Hardware-Lösung des Instituts zum Schutz gegen Hacker stellt die „leading edge" der Netzwerktechnologien dar. Wenn die Sicherheitsbedürfnisse eines Unternehmens zum Austausch von Daten über das Internet die Möglichkeiten klassischer Firewalls übersteigen, empfiehlt sich der Einsatz des Lock-Keepers, der mit geringem Konfigurationsaufwand höchste Sicherheitsvorgaben erfüllt. Seine Funktionsweise entspricht dabei dem Passieren einer Schleuse: Zu keinem Zeitpunkt besteht eine direkte Verbindung zwischen Intranet und Internet, sondern je nach Zustand der „Schleusentore" findet der Informationsaustausch nur jeweils mit einer Seite der Kommunikationsteilnehmer statt.

Mobile Anwendungen

Am Anfang dieses Jahrhunderts sind wir Zeugen eines unvergleichlichen Verschmelzungsprozesses, der Verschmelzung der Wirtschaft mit der digitalen Technik. Unsere heutige Gesellschaft ist dadurch gekennzeichnet, dass sie eine Informationsgesellschaft geworden ist. Durch diese Fusion ist Information zum Produktionsmittel geworden. Dadurch sind zahlreiche Formen von elektronischen Diensten entstanden. E-Commerce, E-Business, E-Goverment etc. sind die ersten Formen dieser Fusion. Heutzutage überschneiden sich zwei wichtige Technologien, das Internet mit seinen Daten und der Mobilfunk. M-Commerce (auch bekannt als Wireless Electronic Commerce) beabsichtigt einen Großteil seriöser Anforderungen früherer Geschäfte zu erfüllen: Informationen zu jeder Zeit an jedem Ort. Noch gibt es unterschiedliche Anforderungen, resultierend aus der Natur dieses neuen Phänomenes, die in Erwägung gezogen werden sollten. Eine dieser Anforderungen ist die Sicherheit. Mit der Entwicklung und der Kompliziertheit der Anwendungen entsteht eine wachsende Bedrohung hinsichtlich der Sicherheit dieser Anwendungen. Gleichzeitig versprechen einige Technologien unterschiedliche Sicherheitslösungen, um mit der Bedrohung fertig zu werden und die resultierenden Probleme zu überwinden.

CeBIT 2001

In Hannover fand vom 22. bis 28. März die CeBIT statt. Das Institut war mit folgenden Exponaten vertreten:

Lock-Keeper
Siehe Text Online 2001

DICOM DISC
Siehe Text Medica 2001

Smart Cards
Die Smart Cards - „intelligente" Chipkarten - unterscheiden sich von ihren Vorläufern, den Magnetkarten, erheblich. Konnten diese Informationen in nur geringem Umfange speichern, so bietet die Smart Card, die mit einem Mikroprozessor bestückt ist, ganz andere Möglichkeiten. Informationen können derart gespeichert werden, dass ein Auslesen unmöglich wird. Ein elektronischer Schlüssel zum Beispiel, der sicher auf der Karte abgelegt ist, ermöglicht es in Verbindung mit der Rechenkapazität des integrierten Prozessors, digitale Signaturen auf der Karte zu erstellen.

Das elektronische Studienbuch
Das Konzept der Virtuellen Hochschule stellt neue Anforderungen an die Sicherung der Identität der Studierenden und die Integrität der von und zu ihnen übermittelten Daten. Mit dem elektronischen Studienbuch können die bekannten Probleme des Zugangs zu den Virtuellen Hochschulen, die Ausstellung und Archivierung von Leistungsnachweisen, die Bezahlung der Kurse etc. sicher und dauerhaft gelöst werden.

Medica 2001

An der Fachmesse Medica, die vom 21. bis 24. November in Düsseldorf stattfand, beteiligte sich das Institut für Telematik mit diesen Exponaten:

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

DICOM DISC
Das Patienten-CD-System DICOM DISK ermöglicht Medizinern den schnellen und benutzerfreundlichen Aufbau einer mobilen, übertragbaren Patientenakte sowie die kompakte, übersichtliche Langzeitarchivierung von Bilddaten. Bilder aus Röntgen-, CRT-, MRT- und Ultraschalluntersuchungen können so einfacher und preiswerter archiviert werden. Zudem wird der Datenaustausch leichter. Die bei einer Untersuchung auf einen speziellen CD-ROM-Rohling gebrannten Bilder im DICOM 3-Format können an jedem herkömmlichen PC in hervorragender Qualität und ohne Informationseinbuße betrachtet werden.

Cura Call
Das mobile Patienten-Erinnerungssystem Cura Call registriert bei der Erfassung der Patientendaten in der Arztpraxis auch die Mobilfunk-Telefonnummer des Patienten. Automatisch erkennt die Cura Call-Software, wann ein Vorsorge- oder Impftermin ansteht und sendet dem Patienten rechtzeitig eine SMS mit Erinnerung, Absender und Rückrufnummer. Der Patient kann die Praxis unmittelbar zurückrufen und einen Termin festmachen. Das komplette Cura Call-Angebot besteht aus einem separaten PC, einem Kartenlesegerät, Modem, installierter Software und SMS-Versandservice.

Publikationen und Vorträge

Mitarbeiter des Instituts für Telematik traten 2001 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 2001

Veröffentlichungen in Tagungsbänden

Mitarbeiter des Instituts für Telematik haben im Jahre 2001 mit Vorträgen zu verschiedenen Themen an internationalen Konferenzen, Symposien und Workshops teilgenommen. Das Institut war unter anderem auf folgenden Veranstaltungen aktiv vertreten:

- ACM SIGDOG 2001, Santa Fe, USA, 2001
- ASP-DAC 2001, Yokohama, Japan, 2001
- ICCD 2001, Austin, USA, 2001
- IMAGE 2001, Brisbane, Australia, 2001
- Internet Computing 2001, Las Vegas, USA, 2001
- IT-Sicherheitskongress des BSI, Bonn, Germany, 2001
- IEEE/ACM IWLS 2001, Lake Tahoe, USA, 2001
- 7.Kongress der IuK-Initiative, Trier, 2001
- Photonics West, San Jose, USA, 2001
- Reed-Muller 2001, Starkville, USA, 2001
- WebNet 2001, Orlando, USA, 2001

Titel der Konferenzbeiträge

Christoph Meinel, Harald Sack, Volker Schillings
IDDS: An Interactive Decentralized Documentation System
Proc. ACM SIGDOG 2001, Santa Fe, USA, 2001.

Christoph Meinel, Harald Sack
Improving XOR-node Placement for Mod2-OBDD Minimzation
Proc. Reed-Muller 2001, Starkville, USA, 2001, pp. 51-56.

Christoph Meinel, Harald Sack
A Simple Heuristic for Mod2-OBDD Minimization Proc. IWLS´2001, Lake Tahoe, USA, 2001, pp. 304-309.

Frank Losemann, Andreas Heuer, Lutz Vorwerk, Thomas Engel, Christoph Meinel
Replacement of Lost User Certificates for Instant IS Access
Proc. Internet Computing 2001, Las Vegas, USA, 2001, pp. 951-956.

Lutz Vorwerk, Christoph Meinel
DICOM Based Presentation System Engrane
Proc. IMAGE 2001, Brisbane, Australia, 2001

Ernst-Georg Haffner, Uwe Roth, Andreas Heuer, Thomas Engel, Christoph Meinel
Managing Distributed Personal Firewalls with Smart Data Servers
Proc. WebNet 2001, Orlando, USA, 2001, pp. 466-471.

Uwe Roth, Kais Louizi, Ernst-Georg Haffner, Christoph Meinel
How Much Middle-Tier Do You Need?
Proc. WebNet 2001, Orlando, USA, 2001, pp. 1053-1056.

Lutz Gollan
Elektronische Signaturen und Sicherheitsanforderungen - Viel Lärm um fast nichts?
IuK-Konferenz, 7. Kongress der IuK-Initiative, Trier, 2001.

Christoph Meinel, Christian Stangier
Hierarchical Image Computation with Dynamic Conjunction Scheduling
Proc. ICCD´2001, Austin, USA, 2001, pp. 354-359.

Christoph Meinel, Christian Stangier
A new Partitioning Scheme for Improvement of Image Computation
Proc. ASP-DAC'2001, Yokohama, Japan, 2001, pp. 97-102.

Christoph Meinel, Christian Stangier
Hierarchical Image Computation with Dynamic Conjunction Scheduling
Proc. IWLS´2001, Lake Tahoe, USA, 2001, pp. 316-321.

Lutz Gollan, Christoph Meinel
Elektronische Signaturen - eine amerikanische und europäische Perspektive
Proc.7. IT-Sicherheitskongress des BSI, Bonn, Germany, 2001, pp. 97-112.

Lutz Vorwerk, Frank Losemann, Christoph Meinel
Suggestion for an Alternative of watermarking and digital Signatures
Proc. Photonics West, San Jose, USA, 2001, pp. 158-165.

Herausgeberschaft und Mitherausgeberschaft an Proceedingsbänden

Christoph Meinel
„Security & Public Key Infrastructures" Proceedings Online 2001, Düsseldorf, 2001

Christoph Meinel, Bernd Dusemund (Eds.)
„Mobile Commerce" Proceedings Trierer Symp. „Mobile Commerce", Trier, Institut für Telematik, ISSN 1433-8106, 2001

Christoph Meinel, Lutz Gollan (Eds.)
„Digitale Signaturen" Proceedings Trierer Symp. „Digitale Signaturen", Trier, Institut für Telematik, ISSN 1433-8106, 2001

Veröffentlichungen in Zeitschriften

Lutz Gollan, Christoph Meinel
Elektronischer Notar
Kommune21, Heft 7/2001, pp. 12-16.

Christoph Meinel, Stephan Waack
The „Log Rank" Conjecture for Modular Communication Complexity Computational Complexity (Birkhäuser Verlag), Heft 10/2001, pp. 70-91.

Christoph Meinel, Thorsten Theobald
Local Encoding Transformations for Optimizing OBDD-Representations of Finite State Machines Formal Methods in System Design, 18, pp. 285-301 (2001).

Technische Berichte des Instituts für Telematik, ISSN 1433-8106

Preprint 2001-11
Proceedings Trier Symposium „Digitale Signaturen" Lutz Gollan, Christoph Meinel

Preprint 2001-10
Anforderungsprofil für den „sicheren" Betrieb eines WLAN
Uwe Roth, Frank Losemann, Thomas Engel, Christoph Meinel

Preprint 2001-09
Trierer Symposium Digitale Signaturen, Abstracts
Lutz Gollan, Christop Meinel

Preprint 2001-08
SDS in der öffentlichen Verwaltung
Uwe Roth, Christoph Meinel

Preprint 2001-07
Studie Teleradiologie: Umfrage unter den Akutkrankenhäusern Baden-Württembergs 2000/2001 - Kurzfassung
Ulf Birkel, Lutz Gollan, Lutz Vorwerk, Christoph Meinel

Preprint 2001-06
Der DICOM Standard und seine Bedeutung für das europäische Gesundheitswesen
Lutz Vorwerk, Christoph Meinel

Preprint 2001-05
IT-Sicherheitszertifikate
Torsten Becker, Thomas Engel, Christoph Meinel

Preprint 2001-04
Trierer Symposium Mobile Commerce, Proceedings
Bernd Dusemund, Christoph Meinel

Preprint 2001-03
Die Schleusentechnologie „Lock-Keeper" und ihre Integration in moderne Sicherheitsarchitekturen
Ernst-Georg Haffner, Thomas Engel, Christoph Meinel

Preprint 2001-02
Trierer Symposium Mobile Commerce, Abstracts
Bernd Dusemund, Christoph Meinel

Preprint 2001-01
Computer-Telefonie-Integration und Packet-Based-Communication Systems
Paul Ferring, 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 2001

Ausser den genannten Vorträgen auf Tagungen und Kongressen haben Mitarbeiter des Instituts folgende Vorträge gehalten.

12.12.2001
Daniel Fischer, Bernd Dusemund
Client-Server basierte Zertifikatserstellung
Institutskolloqium

28.11.2001
Torsten Becker, Thomas Scherer
Aufbau eines internen Trustcenters mit OpenSSL
Institutskolloqium

21.11.2001
Christoph Meinel
Perspektiven im elektronischen Publizieren, Perspektiven in IT-Sicherheit
Dagstuhl, Perspektivenseminar

05.11.2001
Christoph Meinel
Sicherheit in offenen Netzen - Digitale Signaturen
Mannheimer IT-Tage, Mannheim

03.10.2001
Christoph Meinel
Actual BDD-Research in Trier
Universität Rom

26.09.2001
Christoph Meinel
Sicherheit in offenen Netzen: Schwachstellen und Angriffspunkte (3)
Institutskolloqium

19.09.2001
Bernd Dusemund
Aufbau eines LDAP-Servers
Institutskolloqium

18.09.2001
Christoph Meinel
IT-Security and Digital Signatures
Polytechnical University, Peking

29.08.2001
Christoph Meinel
Sicherheit in offenen Netzen: Schwachstellen und Angriffspunkte (2)
Institutskolloqium

22.08.2001
Christoph Meinel
Sicherheit in offenen Netzen: Schwachstellen und Angriffspunkte (1)
Institutskolloqium

24.07.2001
Christoph Meinel
ACERT - eine Konzeption für ein unternehmungsinternes CERT
Institutskolloqium

13.07.2001
Christoph Meinel
Gesundheitsportal für Trier
Regionale Gesundheitskonferenz, Trier

11.07.2001
Ingo Scholtes
Java Native Interface und Cygwin
Institutskolloqium

04.07.2001
Paul Ferring
Funktion und Architektur des Lock-Keepers
Institutskolloqium

27.06.2001
Torsten Becker
IT-Sicherheitszertifikate
Institutskolloqium

20.06.2001
Lutz Vorwerk
Engrane - Ein Lehrsystem für die Radiologie
Institutskolloqium
13.06.2001
Bernd Dusemund
Implementation eines Wap-Servers, Entwicklung von WML-Pages
Institutskolloqium

06.06.2001
Hristo Filkov
Erfahrungsbericht: Drag & Drop mit Java
Institutskolloqium

30.05.2001
Uwe Roth
Das Management des internen Workflows des Smart Data Servers (SDS2)
Institutskolloqium

23.05.2001
Lutz Gollan
7. Deutscher IT-Sicherheitskongress des BSI
Institutskolloqium

09.05.2001 (11:00)
Lutz Gollan
Elektronische Unterschriften - Eine amerikanische und europäische Perspektive
Institutskolloqium

02.05.2001 (16:30)
Lutz Gollan
Teleradiologie - Umfrage unter den Akutkrankenhäusern Baden-Württembergs
Institutskolloqium

20.04.2001
Christoph Meinel
Telematik - anwendungsgetriebene Forschung und Entwicklung
Universität Linz

06.04.2001
Mingchao Ma
Intelligent Agent for Modern Distance Education
Institutskolloqium

05.04.2001
Christoph Meinel
Telematik - junge Disziplin mit grenzenlosen Anwendungen

Telemedizin - Telematik im Gesundheitswesen
Donau-Universität Krems

04.04.2001
Christoph Meinel
Sicherheit in offenen Netzen

Elektronisches Publizieren - Portal-Sites und virtuelle Universitäten
Donau-Universität Krems

19.03.2001
Christoph Meinel
Aktuelle Telematikforschung und das Problem der Sicherheit in offenen Netzen
Universität Leipzig

14.03.2001
Andreas Heuer
Website Content Management, ein Überblick über den Arbeitsbereich
Institutskolloqium

07.03.2001
Lutz Gollan
Sicherheit in offenen Netzen: Elektronische Signaturen/Trust Center
Institutskolloqium

05.03.2001
Christoph Meinel
Telemedizin - Telematik im Gesundheitswesen
Humbodt-Universität, Berlin

28.02.2001
Ernst-Georg Haffner
Vorstellung des Technologiebereichs „Middleware“
Institutskolloqium

21.02.2001
Uwe Roth
Middleware-Technologie am Institut - Der Smart Data Server
Institutskolloqium

12.02.2001
Christoph Meinel
Telematik - junge Disziplin mit grenzenlosen Anwendungen
Jubiläum European Media Lab, Heidelberg

31.01.2001
Ernst-Georg Haffner
Request-Prediction and Hyperlink-Proposals Methodologies and Mathematics behind Web-Applications
Institutskolloqium

Gäste am Institut für Telematik 2001

Klaus-Dieter Benner
Börsenaufsichtsbehörde Hessen, Frankfurt
Nutzen und Risiken des Internet für den Handel an der Frankfurter Wertpapierbörse

Klaus Berens
Deutscher Industrie- und Handelskammertag, Bonn
Elektronische Signatur für sicheres eBusiness - Praktische Einsatzmöglichkeiten am Beispiel der IHK-Anwendungen

Detlef Dienst
T-Telesec, Netphen
Digitale Signatur - Wirkungsweise und Anwendungen

Stefan Engel-Flechsig
Radicchio/Verisign Inc.
Sicherheit in der mobilen Kommunikation

Bernhard Esslinger
Deutsche Bank
PKI in einem Großunternehmen, „bridge CA"

Thomas Groth
Sun Microsystems
Java-Technologie für eingebettete Systeme

Dr. Carlo Harpes
CETREL, Luxemburg
Sichere E-Mails: Banken und Zertifizierungsdiensteanbieter

Patrick Heinen
Semantec Corporation
Viren, Trojanische Pferde und Co.: Probleme und Lösungen

Danny Seiler, Frank Heinisch
Sonera Corporation
Mobile Geschäftsprozesse

Torsten Henn
Secunet AG, Siegen
SigG-Anwendungskomponenten - Lessons learned

Dr. Stephan Klein
Bremen Online Services
www.bremer-online-service.de - Der Vorreiter und Preisträger in der Pflicht

Bernd Kowalski
Initiative D21/Telekom, Berlin/Netphen
Förderung des Einsatzes von PKI-Komponenten und -Lösungen in der Praxis

Michael Leistenschneider
DATEV eG
Berufskammern als Zertifizierungsdiensteanbieter nach dem SigG

Reinhold A. Mainz
Kassenärztliche Bundesvereinigung, Köln
Elektronische Heilberufeausweise: Stand der Einführungsvorbereitungen und noch zu lösende Probleme

Dr. Armin Ratz
Dresdner Bank AG, Frankfurt
Konzernweites Zertifikatsmanagement

Dr. Ulrich Sandl
Bundesministerium für Wirtschaft und Technologie, Berlin
Das Konzept der digitalen Signatur in Theorie und Praxis

Ingo Schubert
Baltimore Technologies
Wireless PKI

Gregor Schulte
Ministerium des Innern und für Sport, Mainz
eGovernment und Elektronische Signatur in der Landesverwaltung Rheinland-Pfalz

Joachim Simon
Siemens Business Services
Mobile Banking and Brokerage

Torsten Witusch
Paybox AG
Die Geschäftsidee "Paybox"

Oliver Zeller
Secartis AG
Authentisierungsvarianten: Voice, Token, Biometrie

Medienresonanz

2001: Bislang stärkste Medienresonanz

Im Jahr 2001 hatte das Institut für Telematik eine so starke Resonanz in den Medien wie nie zuvor. Jede deutsche Nachrichtenagentur griff mindestens einmal Themen aus der Arbeit des Instituts auf. Diese Tatsache sowie der Versand von mehr als zwei Dutzend Medienmitteilungen an Publikums- und Fachmedien führte zu mehr als 120 Berichterstattungen. Nicht nur Printtitel, sondern auch elektronische Medien widmeten sich den Forschungs- und Entwicklungsergebnissen des Instituts. Mehrfach konnte Berichterstattung in Hörfunksendungen angestoßen werden. Mit einem Bericht über das Patienten-CD-System gelangte des Institut sogar in die Tagesschau des Ersten Deutschen Fernsehens. Auf den folgenden Seiten präsentieren wir eine Auswahl von Medien, die sich mit der Instituts-Tätigkeit beschäftigten und den Themen, die dabei eine Rolle spielten.

Handelsblatt, 15.02.2001

Konkurrenz für Firewall-Systeme

Trierer Datenschleuse wehrt Hacker ab

HANDELSBLATT, 15.2.2001

ab/wok TRIER. Ein neues Internet Schleusen-System des Trierer Instituts für Telematik soll Firmennetze besser vor Web-Gefahren schützen als bisherige Sicherheitsmechanismen wie Firewalls. „Mit unserer Datenschleuse besteht keine direkte Verbindung mehr zwischen einem Firmennetz und dem öffentlichen Internet", sagt Ernst-Georg Haffner vom Telematik-Institut, das der Fraunhofer-Gesellschaft angeschlossen ist.

„Unser System arbeitet wie eine Diskette, mit der Daten zwischen zwei verschiedenen PC hin und her transportiert werden", erläutert Haffner das patentierte so genannte Lock-Keeper-System. Mechanische Relais-Technik sorge in dem Lock-Keeper dafür, dass niemals eine physikalische Verbindung zwischen den Netzen besteht. So hätten Hacker von außen keinen direkten Zugriff auf das Firmennetz.

Derzeit kontrolliert zumeist eine so genannte Firewall den Netzverkehr am Grenzübergang zwischen Unternehmen und öffentlichem Internet. Eine solche „Brandschutzmauer" ist in der Regel ein separater Rechner, auf dem eine spezielle Internet-Überwachungssoftware läuft. Durch Überprüfung beispielsweise von Quell- und Zieladressen oder der angeforderten Dienste sollen unerwünschte Anfragen und Softwaresendungen wie Viren und Abhörprogramme abgehalten und eigene sensible Daten vor einem Zugriff geschützt werden. Experten kritisieren immer häufiger, dass solche Sicherheitslösungen vor allem den Datenverkehr von innen nach außen nur unzureichend schützen. Fehlerhafte Betriebssysteme, wissentlicher Datenmissbrauch, Schlampigkeit im Umgang mit Passwörtern oder ein falsch programmiertes Sicherheitsprogramm können dazu führen, dass zu schützende Informationen via Datenleitung ins Internet gelangen.

Der Trierer Lock-Keeper sorgt dafür, dass die Datenpakete eine Art Schleuse durchlaufen müssen. Hier können die Internet-Daten in Ruhe und ausführlich geprüft werden. Allerdings kann ein solches Durchschleusen bis zu 30 Sekunden dauern, weshalb der Lock-Keeper nicht unbedingt für alle Bereiche und Anwendungen geeignet ist. „Web-Surfen mit einer halben Minute Verzögerung macht keinen Spaß", muss Forscher Haffner zugeben. Daher sei die Trierer Lösung eher für Hochsicherheitsbereiche geeignet und mehr eine Ergänzung als ein Ersatz für die bisherigen Internet-Schutzlösungen.

Die Idee der physikalischen Trennung von Firmennetz und Internet ist auch nicht ganz neu. Ähnliche Ideen verfolgen bereits die israelischen Tech-

nologie-Firmen Whale Communications und Voltaire. Jörg Schneider vom Firewall-Marktführer Checkpoint sieht die Trierer Erfindung nicht als Konkurrenz: „Dass Software-Firewalls per Definition unsicherer und anfälliger als Hardware-Pendants sind, ist eine der ältesten Blender-Aussagen." Auch Dirk Husfeld vom Münchener IT-Sicherheitsspezialisten Genua ist skeptisch, ob die physikalische Trennung einen wirklichen Sicherheitsgewinn bringt. Letztlich müssten auch hier die Datenpakete überprüft weitergeleitet werden – nach den gleichen Regeln wie bei Firewalls.

Computer Zeitung Nr. 9, 01.03.2001

Physikalische Datenschleusen steigern die Internet-Sicherheit

Deutsche und israelische Security-Companies wollen sensible Bereiche im Firmennetz und im Internet physikalisch trennen. Dies soll bestehende Firewall-Lösungen ergänzen.

Der beste Schutz vor Internet-Gefahren wie Hackern und Viren ist, kein Internet-Zugang zu haben. Diese Binsenweisheit greift das junge Institut für Telematik in Trier mit ihrem patentierten Lock-Keeper auf, der sensible Bereiche eines Firmennetzes besser schützen soll als traditionelle Firewalls. „Denn diese trennen das interne Netz nicht physikalisch von der Außenwelt, sondern analysieren lediglich die übermittelten Datenpakete und können so möglicherweise doch von Hackern ausgetrickst werden", erklärt Ernst-Georg Haffner vom Trierer Institut, das mit der Fraunhofer-Gesellschaft zusammenarbeitet.

Für die Analyse ist mehr Zeit

Ihr Lock-Keeper arbeitet dagegen wie eine Schleuse, die Datenpakete von außen nach innen transportiert. Während des Schleusevorgangs können die Internet-Pakete ausführlich geprüft werden. Zur Anwendung kommt das System, das vom Luxemburger Unternehmen IT-Services vermarktet werden soll, etwa für den Mail-Austausch einer Bank. Realisiert wird die Schleuse mit zwei Linux-Rechnern, die mit speziellen Einschubkarten bestückt werden. Diese sorgen dafür, dass eine Verbindung entweder zwischen Innen- und Außenrechner oder aber zwischen Außen-Server und Internet besteht – und nie ein direkter Kontakt zwischen Innenrechner und Internet.

Nach einem ähnlichen Prinzip arbeitet die israelische Whale Communications, die derzeit ihr erstes deutsches Sales-Büro in Frankfurt eröffnet. Sie hat zur physikalischen Netztrennung ein spezielles Appliance namens E-Gap entwickelt. Dieses besteht aus einem analogen Schalter sowie einem RAM-Speicher mit zwei SCSI-Anschlüssen. Das System schaufelt die Daten zwischen Innen- und Außenrechner hin und her. Auf diesen läuft eine spezielle Shuttle-Software, die nur Anwendungsdaten durchlässt und darunterliegende Netzprotokolle wie TCP/IP abtrennt. „So werden Attacken generell abgeblockt, denn der Angreifer hat nie eine direkte TCP-Connection ins interne Netz", erklärt Whales CTO Carmi Merimovich. Shuttles gibt es für Web, Mail und Files.

Im Bereich der physikalischen Trennung arbeiten auch zwei weitere israelische Companies: Spearhead Technologies separiert Innen- und Außenrechner mit einem proprietären Bus-System. Voltaire teilt über eine Einschubkarte PCs in zwei Teile: Einen zum Surfen und einen für die interne Arbeit. Alle Anbieter positionieren ihre Lösungen als Ergänzung zur Firewall in Hochsicherheitsbereichen, die Administratoren am liebsten ganz vom Internet getrennt halten wollen.

Physikalische Netztrenner arbeiten wie ein Geldschalter bei der Bank, an dem niemals eine direkte Verbindung zwischen Außenwelt und dem Auszahler hinter der Panzerglasscheibe besteht. Die Internet-Pakete müssen zunächst eine Datenschleuse passieren, bevor sie interne Server mit sensiblen Daten erreichen. Dadurch sollen solche Lösungen in Hochsicherheitsumgebungen traditionelle Firewalls ergänzen.

Konkurrenten sind äußerst skeptisch

Klassische Firewall-Anbieter beäugen die neue Konkurrenz kritisch: Für Jörg Schneider vom Marktführer Checkpoint ist die Idee der galvanischen Trennung schlicht Blödsinn. „Die Aussage, Software-Firewalls seien unsicherer als ihre Hardwarependants, ist eine der ältesten Blenderaussagen und so alt wie der Firewall-Markt selbst." Auch Dirk Husfeld von der Münchner Genua ist skeptisch. Application-Level-Firewalls, die auf Anwendungsebene arbeiten, hätten ähnliche Funktionen und ließen keine direkte TCP-Verbindung nach innen zu. Einzige Ausnahme: wenn der Hacker über ein Sicherheitsloch gleich die Kontrolle über die gesamte Firewall erlangt. ab

Luxemburger Wort, 05.03.2001

Röntgenbilder in Sekunden durchs Internet

(dpa). – Mit stark verdichteten Bilddaten will das Trierer Institut für Telematik die Übertragungszeit von medizinischen Bildern per Internet von Stunden auf Sekunden verkürzen. Für das neue System zur Komprimierung der digitalen Daten sei bereits Patentschutz erteilt worden, teilte das Institut mit. Wichtig seien die schnelle Übermittlung vor allem in der Notfallmedizin.

Die Datenverdichtung sei ohne den sonst bei solchen Verfahren üblichen Verlust von Bildqualität erreicht worden. Nach dem neuen System werde das Originalbild beispielsweise einer Computertomographie in zwei Bilder zerlegt. Das eine zeige den eigentlichen Bildinhalt, das andere unwichtige technische Bestandteile des Hintergrundes, erklärte Institutsleiter Prof. Christoph Meinel. Mit äußerst geringem Rechneraufwand könnte so die hohe Komprimierung erzielt werden.

Ein Vorteil des Verfahrens besteht laut Meinel auch darin, dass die Ärzte die übermittelten Bilddaten mit jeder herkömmlichen Software zur Darstellung von Internet-inhalten betrachten könne.

Ärzte-Zeitung, 29.03.2001

Kompressionsverfahren für medizinische Bilder

Sonogramm wird in wenigen Minuten übermittelt

TRIER (rds). Wissenschaftler des Instituts für Telematik an der Universität Trier haben ein adaptives Kompressionsverfahren für die elektronische Übermittlung von Bildern zum Patent angemeldet. Dabei werden die individuellen Eigenschaften des zu verarbeitenden Originalbildes optimal berücksichtigt.

Röntgen- und besonders Computer- und Magnetresonanz-tomographische Bildfolgen benötigen durch ihre enorme Dateigröße – zehn bis 150 MB – über herkömmliche Netze wie ISDN sehr lange Übertragungszeiten. Zudem belegen sie sehr viel Speicherplatz im Archiv. So fällt zum Beispiel in einer Klinik pro Tag etwa ein Giga-Byte an zu archivierenden Bilddaten an. Ohne eine hochwirksame Bilddatenkompression, die aber die medizinisch relevante Bildinformation nicht reduzieren darf, ist die Übermittlung und Datenbankhaltung dieser Bilder kaum mehr machbar.

Bei dem jetzt zum Patent angemeldeten Kompressionsverfahren werden über eine Ortsfrequenzanalyse die diagnostisch relevanten Bildbereiche (ROI, Region of Interest) vom unwichtigen Hintergrund getrennt. Diese ROI-Zonen werden ohne Qualitätsverlust nach dem beim Bildformat GIF und dem Packformat ZIP genutzten LZW-Algorithmus (Lempel-Ziff-Welch), die übrigen Zonen mit Verlust nach dem JPEG-Standard komprimiert.

Das in weniger als fünf Sekunden erzeugte GIF-JPEG-Kombibild ist um den Faktor 7 bis 20 kleiner als das Original und kann mit jedem Web-Browser betrachtet werden. Dennoch ist das medizinische Qualitätskriterium (Signal-Rauschabstand > 40 dB in den ROI) erfüllt.

Bilder können schneller als bisher ausgetauscht werden

Besondere Bedeutung hat diese Entwicklung für die Telemedizin: Kollegen in Krankenhäusern und Arztpraxen können künftig medizinische Bilder einfacher und schneller auch über das Internet oder mit Hilfe von E-mails austauschen. Über künftige Funktelefonnetze mit Übertragungsraten bis zu zwei Mbit pro Sekunde gelingt zum Beispiel die Übermittlung eines Sonogramms vom Unfallort in die Klinik nur noch innerhalb von wenigen Minuten.

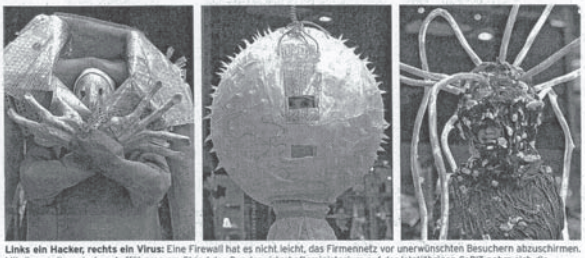
VDI Nachrichten, 23.02.2001

Firewall: Physikalische Trennung von Intranet und Internet schützt auch den Datenverkehr von Innen nach Außen

Computerdaten kommen in der Datenschleuse unter Quarantäne

VDI nachrichten, Düsseldorf, 23. 2. 01 -

Mit einer Datenschleuse als „Quarantänestation" soll der Datenaustausch zwischen firmeneigenem Computernetz (Intranet) und Internet sicherer werden. Computerviren oder vertrauliche Daten werden entdeckt, bevor sie von einem Netz ins andere gelangen können.



Links ein Hacker, rechts ein Virus: Eine Firewall hat es nicht leicht, das Firmennetz vor unerwünschten Besuchern abzuschirmen. Mit dieser allegorischen Aufführung am Stand des Bundeswirtschaftsministeriums auf der letztjährigen CeBIT nahm sich die Bundesregierung des Problems der Datensicherheit an. foto: AP

Nicht nur die Viren aus dem Internet sind es, die Systemadministratoren bei der Pflege von Firmennetzen Sorge bereiten. Nicht weniger kritisch sind unternehmensinterne Computerdateien, die unkontrolliert aus dem Intranet ins offene Internet gelangen.

Fehlerhafte Betriebssysteme, wissentlicher Datenmissbrauch, Schlampigkeit im Umgang mit Passwörtern oder ein falsch programmiertes Sicherheitsprogramm: Es gibt zahlreiche Wege, wie zu schützende Informationen via Datenleitung unbemerkt das Firmengelände verlassen können.

Den unkontrollierten Datentourismus will das mit der Fraunhofer-Gesellschaft verbundene Trierer Institut für Telematik jetzt verhindern. Ihr „Lock-Keeper" bewirkt als Datenschleuse eine physikalische Trennung zwischen dem firmeneigenen Intranet und dem offenen Internet. Erst nachdem die Daten gewissermaßen unter Quarantäne genommen und für unbedenklich befunden wurden, können sie die Schleuse verlassen.

Um einen PC etwa vor Online-Attacken zu schützen hat man bislang zwei Möglichkeiten. Entweder man nimmt ihm Diskettenlaufwerk, CD-Rom und die Internetkarte, eben all das, was ihm die Verbindung zur Außenwelt ermöglicht, oder man entscheidet sich für eine Firewall-Software, die alle Datenpakete aus dem Internet filtert und analysiert, ehe sie zum Firmennetz durchgelassen werden. Durch Überprüfung beispielsweise von Quell- und Zieladressen oder der angeforderten Dienste sollen unerwünschte Anfragen und Softwaresendungen wie Viren und Abhörprogramme abgehalten und eigene sensible Daten vor einem Zugriff geschützt werden. Die Online-Kommunikation aber ist keine Einbahnstraße. Experten kritisieren immer häufiger, dass solche Sicherheitslösungen nur unzureichend auch den Datenverkehr von innen nach außen schützen.

Der „Lock-Keeper" unterscheidet sich nun wesentlich von den üblichen Firewalls auf Software-Basis. Dazu bedient er sich einer recht alten Hardware-Lösung, die sich in U-Booten und Raumstationen, aber auch in Infektions- und Laboreinheiten von Krankenhäusern und Forschungseinrichtungen bewährt hat: die Schleuse. „Der Lock-Keeper setzt mindestens zwei voneinander unabhängige Rechnersysteme voraus, einen Intranet-Server (INS) und einen Lock-Keeper-Server (LKS)", erklärt Institutsleiter Professor Christoph Meinel das wesentliche Merkmal. Zwischen beiden Servern befindet sich das innere Schleusentor und zwischen dem LKS und dem Internet das äußere Tor. Alle Daten aus dem Intranet werden zum INS gesendet und hier eingehend analysiert. Erst bei geöffneter innerer Schleuse gelangen die bereinigten Informationen auf den Lock-Keeper-Server. Er kann die Datenpakete erst dann weiter senden, wenn sich die innere Schleuse geschlossen hat. Dann erst baut der Lock-Keeper die Verbindung zum Internet auf, öffnet das zweite Schleusentor. Zwar können zu diesem Zeitpunkt berechtigte wie unberechtigte Zugriffe von außen auf den Lock-Keeper-Server erfolgen, dennoch aber bleibt das Computernetz des Unternehmens unangetastet, da keine physikalische Verbindung besteht, solange der Weg zum Internet geöffnet ist.

Wird dieser dann im letzten Schritt wieder verschlossen und der Weg vom Lock-Keeper-Server zum INS geöffnet, können infizierte Dateien zwar bis dorthin gelangen, sie können aber, je nach Wunsch, verschieden intensiv analysiert und gegebenenfalls vernichtet werden, ohne dass zeitgleich eine Online-Verbindung besteht, über die der INS manipuliert werden könnte. „Von höchster Bedeutung ist, dass zu keinem Zeitpunkt beide Schleusentore gleichzeitig geöffnet sind", sagt Meinel.

Die Trennung der Datennetze werde „physikalisch erzwungen", so dass selbst bei fehlerhafter Steuerungssoftware oder einem erfolgreichen Angriff auf eine der Lock-Keeper-Komponenten die Gesamtarchitektur nicht korrumpiert werden kann, was im übrigen auch für berechtigte Zugreifer gilt. „Aufgrund der physikalischen Gegebenheiten können auch Systemadministratoren keine Möglichkeit entwickeln, die Schleusentore gleichzeitig zu öffnen, um etwa eine schnellere Durchlaufzeit von Daten zu erzielen", erklärt Meinel und weist auf den Kostenfaktor hin: „Für die einfachste Lösung genügen gerade mal zwei PCs".

WOLFGANG KAPPLER

Trierischer Volksfreund, Nr. 125, 31.05.2001

Zukunft des M-Commerce

Trierer Tagung wird direkt im Internet übertragen

TRIER. Der „Mobile Commerce" ist Thema eines Trierer Symposiums Anfang Juni, das parallel im Internet übertragen wird. Das Institut für Telematik erwartet dazu führende Experten aus Wissenschaft und Wirtschaft.

Ein Dutzend Experten wird am 7. und 8. Juni sowohl den Tagungs-Teilnehmern in Trier als auch Interessenten aus aller Welt, die via Web-Cam verbunden sind, die Möglichkeiten moderner Kommunikationstechniken bei mobilen Anwendungen präsentieren. Wie Institutsleiter Professor Christoph Meinel mitteilte, soll vor allem geklärt werden, wie die immer komplizierteren Anwendungen die Sicherheit des drahtlosen elektronischen Geschäftsverkehrs bedrohen.

Der drahtlose Electronic-Commerce stehe noch am Anfang seiner Entwicklung, erläutert Professor Meinel. Vor einem Einsatz der breiten Masse müsste zunächst die Sicherheit gewährleistet sein, damit M-Commerce-Prozesse rechtlich unanfechtbar seien. Dazu gehöre der Schutz vor Viren-Attacken. Meinel kündigte für das Symposium die Vorstellung moderner Konzepte an, um mit den Gefährdungen des M-Commerce fertig zu werden und seine Sicherheit zu garantieren. Die Tagung setzt die Symposien-Reihe des Instituts für Telematik fort. Es soll ein Forum für hochrangige Wissenschaftler und Vertreter aus Wirtschaft und Verwaltung über die Potenziale der neuen Informations- und Kommunikationstechnologien im Bereich des M-Commerce sein.

● Institut für Telematik, Bahnhofstraße 30-32, 54294 Trier, Telefon 0651/97551-44, Internet: http://www.ti.fhg.de

Groupware Magazin Online, 07.06.2001

Initiative D21: Institut für Telematik engagiert sich

Das Institut für Telematik, eine mit der Fraunhofer-Gesellschaft verbundene rheinland-pfälzische Spitzenforschungseinrichtung, ist Fördermitglied der Initiative D21 geworden. Die 200 Mitwirkenden dieser Einrichtung verfolgen das Ziel, den Übergang von der Industrie- zur Informationsgesellschaft zu beschleunigen.

Durch seine Mitgliedschaft wolle das Institut für Telematik mithelfen, den aktuellen Rückstand Deutschlands in der Informationstechnologie gegenüber anderen Ländern aufzuholen, erklärte Institutsleiter Professor Christoph Meinel (47) zu Beginn des mCommerce-Symposiums in Trier. Experten aus Wissenschaft und Wirtschaf beschäftigen sich hier zwei Tage lang vor allem mit den Sicherheitsrisiken des drahtlosen elektronischen Geschäftsverkehrs. „Wir werden uns in verschiedenen Arbeitsgruppen aktiv engagieren", versprach der Trierer Telematik-Professor den versammelten mCommerce-Experten und bezeichnete die Initiative D21 als die größte private-public-partnership in Deutschland. Dem Beirat der Initiative steht Bundeskanzler Gerhard Schröder vor.

Das Mobile Commerce-Symposium im Trierer Institut für Telematik will die künftigen Möglichkeiten der modernen Informations- und Kommunikationstechniken im Bereich der mobilen Anwendungen präsentieren. Wie sein Leiter mitteilte, soll vor allem geklärt werden, wie die durch technische Weiterentwicklungen und immer kompliziertere Anwendungen bedrohte Sicherheit des drahtlosen elektronischen Geschäftsverkehrs gewährleistet werden soll.

Um an der sogenannten Multicast Backbone-Übertragung des Mobile Commerce-Symposiums am 7. Juni (14:00-18:00 Uhr) und am 8.Juni (9:00 - 14:00 Uhr) teilnehmen zu können, benötigt der Internet-User einen QuickTime Player (Version höher als 4.0) und den Internet Explorer. Auf der Website des Instituts für Telematik (http://www.ti.fhg.de) werden zusätzliche technische Hinweise gegeben

Diese Meldung stammt von Andrea Stickel / 07.06.2001

Welt am Sonntag, 10.06.2001

Die neue Datenschleuse Look-Keep soll Hackern das Handwerk legen

Konkurrenz für Firewalls

Hannover sg – Die scheinbar banalen Prinzipien sind oft die effektivsten. Das gilt auch für das neue Lock-Keep-Verfahren für den Schutz firmeneigener oder privater Netze, verspricht das Trierer Institut für Telematik, das die Datenschleuse entwickelt hat.

Herkömmliche Firewalls analysieren und filtern »übermittelte Daten aus dem Internet. Der Nachteil jedoch: Das firmeninterne Rechnernetz wird während des Datenverkehrs nicht von der Außenwelt getrennt. Durch Software-, Konfigurations- oder Bedienerfehler kann die Schutzfunktion somit beeinträchtigt und außer Kraft gesetzt werden.

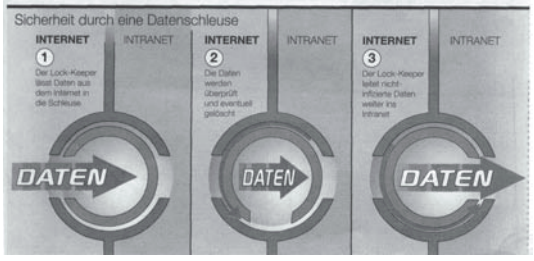
Die neue Schleusenlösung verhindert dagegen eine direkte physikalische Verbindung zwischen firmeneigenen Netzen und dem Internet. „Das von uns entwickelte Verfahren Lock-Keeper blockt alle Online-Attacken auf ein internes Rechnernetz durch physikalische Sicherheitsvorkehrungen hundertprozentig ab", sagt Institutsleiter und Patentträger Christoph Meinel.

Zwischen dem Intranet-Server (INS) und dem Internet setzt Mienel dazu den Lock-Keeper-Server (LKS) ein. Dieser hat in beide Richtungen zwei Schleusentore, die – wie in einer Wasserschleuse – zu keinem Zeitpunkt gleichzeitig geöffnet sind. Alle Daten, die aus dem Internet kommen, passieren zunächst das äußere Schleusentor und werden im Schleusenninnenraum analysiert. Infizierte Daten vernichtet das System sofort. Erst wenn der Datenwaschgang erfolgreich beendet und das äußere Tor verschlossen ist, öffnet sich das innere Schleusentor, um die Daten in das Firmennetz zu lassen.

Der Gegenverkehr funktioniert nach dem gleichen Prinzip. Denn nicht nur externe Datenangriffe machen den Datenschutzbeauftragten das Leben schwer. Zu oft geschieht der Datenverlust vertraulichen Datenmaterials auf dem umgekehrten Wege. „Jede zu schützende Information, die – gewollt oder ungewollt – ein Unternehmen verlässt, ist ein hoher Verlust. Deshalb ist der Lock-Keeper so konzipiert, dass selbst Systemadministratoren keine gleichzeitige Öffnung der Tore erzwingen können", erklärt Meinel.

Der Zeitversatz durch den Einsatz des Lock-Keeper ist minimal. Wer trotzdem auf eine extrem hohe Durchsatzrate angewiesen ist, kann die Schleuse ausschließlich im Sicherheitsbereich seines Unternehmens einsetzten. „Die Datenschleuse passt in einen Schuhkarton", sagt Meinel; für etwa 15 000 Mark sei der Lock-Keeper auch für mittelständische Firmen erschwinglich, bei sinkenden Preisen ebenso für private Haushalte. Damit kann das System in direkte Konkurrenz zu den Firewalls treten.

Erste Interessenten sind allerdings noch Großkunden wie Siemens und die Dresdner Bank. Das Lock-Keeper Patent ist das erste in der noch jungen Geschichte des 1998 gegründeten Instituts. 25 Forscher beschäftigen sich dort mit High-Tech-Projekten im Schnittbereich von Telekommunikation und Informatik. Eine zweite, noch geheim gehaltene Erfindung ist bereits beim Deutschen Patent- und Markenamt in München angemeldet. Weitere Informationen: www.ti.fhg.de



ARD-Text, 04.07.2001

Institut fordert digitale Signatur (1)

Das Trierer Institut für Telematik plädiert für die verstärkte Nutzung der elektronischen Unterschrift im E-Commerce.

Inzwischen gebe es zwar ausgereifte technische Verfahren, um Dokumente elektronisch zu unterschreiben und verschlüsselt zu versenden.

Dennoch existieren noch zu wenig Trust Center, die eine Voraussetzung dafür wären, dass der Handel via Internet sicher und rechtsverbindlich abgewickelt werden kann.

Heise Online Newsticker, 28.08.2001

Prognose-Modell soll Web auf Trab bringen

Ein Wissenschaftler des Instituts für Telematik in Trier hat eine mathematische Methode entwickelt, um die bevorstehende Nutzung von Internet-Seiten vorherzusagen. Dadurch könnten Wartezeiten beim Abruf von Inhalten im weltweiten Computernetz erheblich vermindert werden, sagte der Informatiker Ernst-Georg Haffner bei der Vorstellung seines Verfahrens.

Mit den in Haffners Modell berechneten Nutzungswahrscheinlichkeiten sollen Server im Internet künftig in der Lage sein, aufwendige Operationen und Datenübermittlung bereits vorzunehmen, bevor der Anwender überhaupt die entsprechenden Seiten abruft. "Der einzelne Internet-Nutzer hat den Vorteil kürzerer Antwortzeiten, ohne dass andere Teilnehmer gleichzeitig Leistungseinbußen hinnehmen müssen", betonte Haffner.

Das Modell des Trierer Telematikers bezieht in die Prognose der Internet-Nutzung unter anderem Zufälligkeits-Faktoren, mittlere Anforderungs-Häufigkeiten, Umfang und Anteil von teilweise vorhersagbaren Elementen einer Sitzung sowie Kostenaspekte ein. Auch der Zeitablauf und das Altern von Datensätzen werden in dem Verfahren berücksichtigt. Haffner fand zudem heraus, dass die "Request Prediction" mathematisch und methodisch erstaunliche Gemeinsamkeiten mit der automatischen Erzeugung von Vorschlägen zur Verlinkung von Web-Seiten durch Redaktionssysteme hat.

Forschungs- und Entwicklungsschwerpunkt des vor drei Jahren gegründeten Instituts für Telematik ist das Internet. Die gemeinnützige Einrichtung ist mit der Fraunhofer-Gesellschaft verbunden. (thd/c't)

Berliner Zeitung, 12.09.2001

Spitzenforschung fürs Internet wird ausgebaut

TRIER. Deutschlands einzige Forschungseinrichtung fürs Internet, das Trierer Institut für Telematik, kann dank erhöhter staatlicher Grundförderung stark ausgebaut werden. Dies teilte Institutsleiter Professor Christoph Meinel mit. Die rheinland-pfälzische Landesregierung hat sich nach Meinels Worten zu höheren Finanzzuweisungen bereit erklärt. Diese sollen nach dem Vorschlag einer Gutachter-Kommission in den nächsten fünf Jahren schrittweise von 0,9 auf 4 Millionen Mark anwachsen. Gleichzeitig soll die Zahl der Wissenschaftler mehr als verdreifacht werden. Sie werden sich noch stärker auf die Sicherheit im Internet konzentrieren, Schwerpunkte Banken und Telemedizin. *(bil.)*

Saarbrücker Zeitung, 20.09.2001

Drei Stipendien für China-Informatiker

Peking (ots). Das Trierer Institut für Telematik hat eine Kooperationsvereinbarung mit der Polytechnischen Universität Peking abgeschlossen. In einem ersten Schritt würden drei Promotionsstipendien für chinesische Informatik-Wissenschaftler eingerichtet, teilte der Institutsleiter, Professor Christoph Meinel (47) jetzt in der chinesischen Hauptstadt mit. Die ersten Absolventen aus Peking werden bereits am 1. Oktober in das deutsche Spitzenforschungsinstitut kommen und dort ihre Arbeit aufnehmen.

Wie Professor Meinel anlässlich der Feiern zum Beginn der Zusammenarbeit in der chinesischen Hauptstadt erläuterte, sollen künftig jedes Jahr mindestens drei weitere Doktoranden ihre Promotionsstipendien in Trier beginnen. Die chinesischen Experten bekommen ihr Stipendium in Höhe von 2000 Mark monatlich für die Dauer eines Jahres. Bei entsprechenden Fortschritten ist eine Verlängerung möglich. Auch Instituts-Mitarbeiter aus Trier sollen die Gelegenheit zu Aufenthalten in Peking bekommen.

Focus, 39/2001

INTERVIEW „In fünf Jahren nicht mehr ohne"

CHRISTOPH MEINEL, 47, ist Informatikprofessor und leitet das Institut für Telematik in Trier

FOCUS: Das Bundeswirtschaftsministerium hat einen einheitlichen Standard für digitale Signaturen in Auftrag gegeben. Wie viele inkompatible Systeme gibt es?

Meinel: Mindestens zwei nicht kompatible Lösungen von Post und Telekom. Bisher fehlt die einheitliche staatliche Linie, so wurde zum Beispiel das Steuererklärungssystem Elster mit wieder einer anderen Signatur entwickelt.

FOCUS: Warum ist die elektronische Unterschrift denn so wichtig?

Meinel: Sie garantiert, dass die elektronische Nachricht unverändert vom richtigen Absender kommt – die Voraussetzung, um Verträge allein übers Netz abzuschließen.

FOCUS: Seit 1998 läuft der Aufbau der Infrastruktur, warum führt die E-Unterschrift bisher ein Schattendasein?

Meinel: Es fehlt eine Signaturkarte, die im staatlichen, geschäftlichen und privaten Bereich einsetzbar ist. Ein Versäumnis der Bundesregierung war, die Bürger nicht direkt mit einem einheitlichen Signatursystem für Verwaltung und Steuererklärung auszustatten.

FOCUS: Ihre Prognose: Wann gehören digitale Signaturen zum Alltag?

Meinel: In fünf Jahren wird man ohne digitale Unterschrift nicht mehr auskommen.

Biophotonics International, 09/10 2001

New software makes digital archiving easier

TRIER, Germany — As hospitals and doctors move more toward using digital imaging systems, the problem of archiving the huge amounts of data in a user-friendly manner is becoming a concern.

In the case of x-rays, digital imaging exposes patients to less radiation and yields faster, more precise diagnoses. Digital images allow doctors to share information and combine images taken with different techniques. However, the data from these images is so voluminous — on average several dozen megabytes per record — that it can overload data links between specialists.

Researchers at The Institut für Telematik were experiencing these problems as they tried to collaborate with other area hospitals. To overcome these difficulties, they designed a fully automated, user-friendly system that archives files onto CDs. They turned burning CDs and viewing digital images, which usually require some technical ability, into something anyone can do. The user simply selects the pictures he or she wants to save on a CD.

The system has a writing module for compiling, viewing and archiving medical images onto a CD using Dicom, the standard international data format in the medical profession. It also includes a picture viewer that can reproduce and process a high-resolution image or sequence. Once a CD is burned, it can be viewed by any doctor or patient if the viewer software is burned onto the CD as well. ITM Services AG in Essen, Germany, is selling the system, which includes a computer, for between $6000 and $7000. □

Tagesschau 19.07.2001

ComputerBILD, Nr. 23/2001

Internet-Vorlesung

Der Trierer Informatik-Professor Christoph Meinel überträgt seine Vorlesung über Grundlagen, Funktionen und Möglichkeiten des Internets live – aber nicht im Fernsehen, sondern im weltweiten Datennetz. Im November werden die Vorlesungen jeweils Dienstags und Donnerstags zwischen 8.30 und 10 Uhr „gesendet". Vorkenntnisse sollen nicht erforderlich sein.

Infos: www.ti.fhg.de

N-TV.de CNN.de, 15.10.2001

Westdeutsche Allgemeine, 24.10.2001

Personalausweis fürs Netz

„Wir brauchen für das Internet eine Art Personalausweis", sagte Prof. Christoph Meinel vom Institut für Telematik, Trier. Es gebe zu viele Möglichkeiten, unter falscher Identität Informationen im Internet zu verbreiten oder Daten zu verfälschen. Sein Vorschlag für mehr Sicherheit in der digitalen Kommunikation: „Vorstellbar ist eine Chipkarte, die jeder an seinem Computer mit einem Lesegerät benutzen und damit die Daten signieren kann."

http:/www.ti.fhg.de (dpa)

Westfalenpost, 16.11.2001

Medizinische Bilder per Internet

Trierer Institut stellt neues Verfahren auf Medica in Düsseldorf vor

Trier/Düsseldorf. (dpa) In wenigen Sekunden statt Stunden sollen Ärzte künftig medizinische Bilder an Kollegen über das Internet verschicken können.

Für diese beschleunigte Übertragung von Röntgen-, Ultraschall- und Tomographiebildern hat das Institut für Telematik in Trier ein neues Bildkomprimierungsverfahren entwickelt. Vor allem für die Notfallmedizin sei das ein großer Schritt vorwärts, sagte Institutsleiter Professor Christoph Meinel. Das Verfahren wird vom 21. bis 24. November auf der internationalen Medizinmesse „Medica" in Düsseldorf vorgestellt.

Möglich sei ein schneller und benutzerfreundlicher Aufbau einer mobilen und übertragbaren Patientenakte und eine kompakte und übersichtliche Langzeitarchivierung von Bilddaten, erklärte der Wissenschaftler. „In Krankenhäusern wird noch immer viel Zeit mit dem personalaufwendigen Heraussuchen und Transport von Patientenakten verwendet", so Meinel. Das neue System ermögliche eine hohe Rationalisierung der Abläufe.

Wege zum Institut

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

Luxemburg
Vom Flughafen Findel bringt Sie der Airport-Liner-Dienst in ca. 45 Minuten direkt nach Trier. Die Reservierung muss 24 Stunden vor Anreise erfolgen und kann unter der Telefonnummer 0049 651 717273 vorgenommen werden. Sie können Trier aber auch mit Taxi, Bus oder Bahn gut erreichen. Der Zug fährt stündlich und benötigt für die Strecke gut 45 Minuten.

Frankfurt/Main
Direkt unter dem Rhein-Main-Airport befindet sich ein Bahnhof. Von dort aus können Sie über Koblenz in knapp drei Stunden nach Trier gelangen.

Frankfurt-Hahn
Die schnellste Möglichkeit, vom Flughafen in dem Hunsrück-Ort Lautzenhausen nach Trier zu gelangen, ist eine 40-minütige Taxifahrt nach Bullay und von dort aus eine Zugfahrt, die einen in rund 50 Minuten ans Ziel bringt.

Saarbrücken
Vom Flughafen Ensheim aus fahren Sie am besten mit dem Taxi zum Saarbrücker Hauptbahnhof und von dort aus in gut einer Stunde per Zug nach Trier.

Köln/Bonn
Mit einem Shuttle-Bus gelangen Sie vom Flughafen zum Kölner Hauptbahnhof. Von dort aus braucht der Zug etwa drei Stunden bis Trier.

Bildquellen

Fotografien: Institut für Telematik, Trier

Verarbeitung und Vervielfältigung