Heft 63 · November 2003

DFN Mitteilungen

DFNRoaming
Unterwegs im Wissenschaftsnetz

Mapping Mars
G-WiN ermöglicht zeitnahe Auswertung von Bilddaten der Mars-Mission

Virtual-Silk-Highway
Konnektivität für die Wissenschaft in Zentralasien

INHALT

IMPRESSUM

Herausgeber
Verein zur Förderung eines Deutschen Forschungsnetzes e.V.
– DFN-Verein –
Anhalter Straße 1, 10963 Berlin
Tel 030 - 88 42 99 - 24
Fax 030 - 88 42 99 - 70
Mail dfn-verein@dfn.de
WWW http://www.dfn.de
ISSN 0177-6894

Redaktion
Kai Hoelzner (*kh*)

Gestaltung
VISIUS DESIGNAGENTUR, Berlin
info@visius-design.de

Druck
Trigger Offsetdruck, Berlin

Roaming für das Deutsche Forschungsnetz

In den letzten Jahren wurde an nahezu jeder Hochschule ein flächendeckender W-LAN Dienst aufgebaut. Zugangsberechtigt sind im Regelfall alle Hochschulangehörigen. Die Erfahrung zeigt, dass dieser Dienst eine hohe Akzeptanz bei allen Nutzern findet und in vielfältigen Anwendungen eingesetzt wird. Für die Hochschule ist dieser Dienst auch unter wirtschaftlichen Gesichtspunkten interessant: die Nutzer verwenden ihre eigenen Endgeräte und müssen nicht auf die der Hochschule zurückgreifen. Die sicherheitstechnischen Verfahren, mit denen unberechtigte Nutzer von einem Zugriff abgehalten werden, sind bekannt und werden wohl überwiegend eingesetzt. Die Leistungsfähigkeit des Deutschen Forschungsnetzes ist hinreichend bekannt und muss nicht weiter angesprochen werden. Es bietet sich also geradezu an, beide Elemente miteinander zu verbinden:

Angehörige von Mitgliedseinrichtungen des DFN bekommen über W-LAN Zugang zum Netz der Fremdhochschule und werden zu ihrer eigenen Hochschule durchvermittelt. Technisch ist dies kein Problem, sofern sich die Hochschulen auf ein gemeisames Zugangsverfahren einigen. Vorschläge hierzu werden vom DFN erarbeitet und allen Mitgliedshochschulen angeboten.

Prof. Dr. Gerhard Peter

Rektor der Fachhochschule Heilbronn
Leiter der Nutzergruppe "Hochschulverwaltung im DFN"

Die Autorisierung und Authentifizierung wird bei der Heimathochschule durchgeführt und erst bei der Freigabe wird eine endültige Verbindung hergestellt. Einige organisatorische Fragen bleiben noch zu klären: Sollen die der Fremdhochschule entstehenden Kosten durch die Heimathochschule erstattet werden? Zumindest für eine Einführungsphase sollte auf eine Verrechnung verzichtet werden, da von einem ausgeglichenen Datenverkehr ausgegangen werden kann. Auch muss gefragt werden, ob die login-Verfahren sicher genug sind. Es wäre gleichzeitig ein guter Zeitpunkt für die Einführung von fortgeschrittenen Signaturen. Parallel zur Einführung des Roaming-Dienstes sollte eine DFN-interne Infrastruktur zur Einführung einer zentralen Zertifikatsvergabe aufgebaut werden. Zusätzlich könnten sowohl die Zertifikate, die von einzelnen Hochschulen ausgegeben werden, gültig sein, als auch die Verwendung von qualifizierten Signaturen privater Anbieter ermöglicht werden.

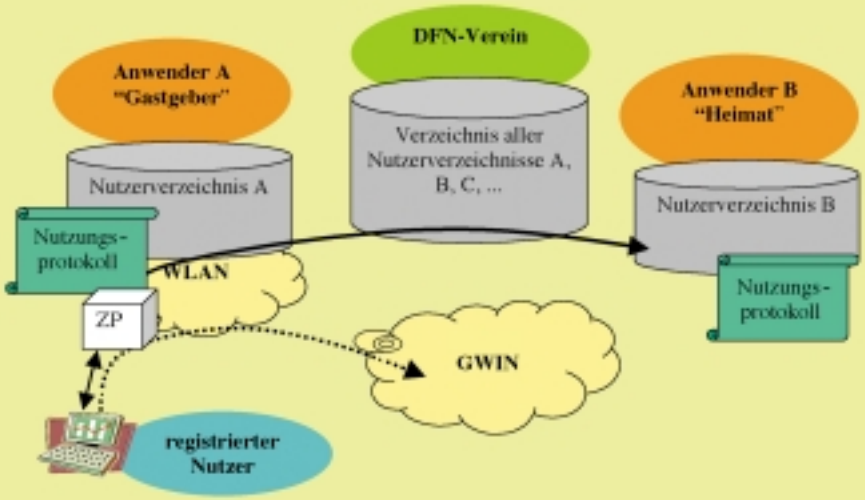
Der Aufwand für die Einführung eines solchen Roaming-Dienstes ist überschaubar. Die Verwendung fortgeschrittener Zertifikate ist in diesem Kontext sinnvoll. Der wichtigste Aspekt ist allerdings, dass es gelingt, viele Hochschulen für die Teilnahme zu gewinnen, auch wenn vordergründig zunächst einmal nur die Angehörigen einer fremden Hochschule davon profitieren. Für den reisenden Wissenschaftler wird ein funktionierender Roaming-Dienst eine wesentliche Erleichterung darstellen. Eine Ausdehnung auf Studierende bietet sich an, die Randbedingung sind aber noch zu klären.

DFNRoaming – Unterwegs ins Wissenschaftsnetz

Frei nach Shakespeare „Wo es Euch beliebt."

Mit der zunehmenden Verbreitung von transportablen Rechnern (Notebooks, Handhelds, etc) steigt der Bedarf nach einem ortungebundenen Zugang zum Wissenschaftsnetz und dem damit verbundenen Internet. Es gibt unmittelbar ein großes Interesse daran, „von unterwegs" seine eMails abzuholen oder Informationen aus dem WWW zu erhalten. Darüber hinaus wäre es auch oft sehr hilfreich, über eine gesicherte Verbindung auf interne Datenbanken der Bibliothek oder interne WWW-Server zugreifen zu können.
Bislang gibt es mit dem Roaming-Handbuch des DFN-Vereins (http://www.dfn.de, Suchwort: „Roaming") eine verlässliche und detaillierte Anleitung, wie über einen beliebigen Internetzugang eine gesicherte Verbindung zu den o.g. Diensten in der eigenen Einrichtung aufgebaut werden kann. In diesem Bild fehlte bislang noch das Puzzleteil, wie das Wissenschaftsnetz unterwegs schnell, unkompliziert und frei von laufenden Entgelten erreicht werden kann. Dieses Puzzleteil wird nun mit dem Leistungspaket „DFNRoaming" eingefügt und komplettiert das Leistungsangebot für den „reisenden Wissenschaftler".

Grundlegendes Konzept für DFN-Roaming ist ein verteiltes Authentifizierungssystem. Um als Nutzer von DFN-Roaming registriert zu sein, genügt es, sich genau einmal in seiner eigenen Einrichtung eine Kennung zu beschaffen. Mit dieser Kennung können dann alle WLAN-Netze der am Dienst teilnehmenden Anwender für den Zugang zum Wissenschaftsnetz genutzt werden. Die Authentifizierung findet dabei immer anhand der Informationen des Nutzerverzeichnisses der „Heimateinrichtung" statt. Die Abbildung erläutert diesen Zusammenhang.
Jeder Anwender pflegt ein Nutzerverzeichnis seiner registrierten Nutzer. Die registrierten Nutzer werden in der Regel eine Teilmenge der Nutzer sein, denen der Anwender Zugang zu seinem eigenen WLAN gewährt. Ein registrierter Nutzer bekommt Zugang zum G-WiN (gestrichelter Pfeil), wenn er am Zugangspunkt (ZP) eines dienstkonformen WLAN authentifiziert wird. Dies geschieht anhand seiner Kennung, die in der Regel eine Kombination aus Username/Passwort ist, aber auch ein digitales Zertifikat sein kann. Zur Prüfung der Kennung verwendet der Zugangspunkt das Nutzerverzeichnis des Anwenders (durchgezogener Pfeil), bei dem der Nutzer beschäftigt oder immatrikuliert ist (Heimat). Dort und nur dort ist festgelegt, ob ein Nutzer zugangsberechtigt ist oder nicht. Um das lokale Verzeichnis der Heimat des Nutzers zu finden, wird das vom DFN-Verein betriebene Verzeichnis aller Nutzerverzeichnisse (DFN-Toplevel Verzeichnis) verwendet. Vergleichbare Betriebskonzepte sind auch für kabelgebundene



Kurzmeldungen

DFN-Projekt gewinnt höchstdotierten Medienpreis

Das vom DFN-Verein im Rahmen seines Entwicklungsprogrammes aus Mitteln des bmb+f geförderte Projekt "Statistiklabor" des Centers für Digitale Systeme CeDIS der FU-Berlin wurde im September mit Europas höchstdotiertem Medienpreis, dem MEDIDA-PRIX ausgezeichnet. Das Preisgeld von 100.000 Euro ging zu gleichen Teilen an die Freie Universität Berlin und die Universität Basel, die für das Projekt "Pharma" ausgezeichnet wurde. Das unter der Leitung von Dr. Nicolas Apostolopoulos entwickelte "Statistiklabor" wird seit 1999 in verschiedenen Fakultäten deutscher Hochschulen eingesetzt. Es liefert Unterstützung für reguläre Veranstaltungen und auch für das Selbstlernen. Als aktives Prüfungsinstrument ist die Software inzwischen integraler Bestandteil der Ausbildung.

DENIC, SWITCH und nic.at ermöglichen künftig auch Umlaute in Domainnamen

Ab dem 1. März kommenden Jahres müssen die Müllers, Jägers oder Schröders in Deutschland nicht mehr auf Umschreibungen wie mueller.de ausweichen, wenn sie ihren Namen in der Internet-Domain verwenden wollen. DENIC, SWITCH und nic.at, die Registrierungsstellen für Domains in Deutschland, der Schweiz und Österreich, warten dann nämlich mit einer bedeutenden und praktischen Erweiterung für die Wahl möglicher Domains auf. Durch die Einführung des neuen Standards IDN (Internationalized Domain Name) sind dann nicht nur Umlaute erlaubt. Insgesamt 92 zusätzliche Buchstaben, vom französischen é bis zum dänischen ø werden dann die Domains bereichern.

Jochem Pattloch
E-Mail: pat@dfn.de

Ralf Paffrath
E-Mail: paffrath@dfn.de

DFN-Verein, Geschäftsstelle
Anhalter Straße 1
D-10963 Berlin

LANs denkbar und können in weiteren Ausbaustufen von DFNRoaming umgesetzt werden.

Das Leistungspaket DFNRoaming wird als Ergänzung zum DFNInternet Dienst erbracht. Die Leistungen von DFNRoaming sind mit den Entgelten für den DFNInternet Dienst abgegolten. Zwischen dem DFN-Verein und den Nutzern von DFNRoaming bestehen keine vertraglichen Beziehungen.

Die Leistung des Pakets DFNRoaming umfasst Betrieb und Pflege des DFN-Toplevel Verzeichnisses, Zertifizierung und Registrierung der Nutzerverzeichnisse, Pflege eines Informationsangebots zu betrieblichen, technischen und rechtlichen Fragen (Wissensdatenbank und moderierte Mailingliste), Koordinierung der Integration des Dienstes in internationale Infrastrukturen sowie Koordinierung der möglichen Zusammenwirkung mit kommerziellen Anbietern von vergleichbaren Diensten.

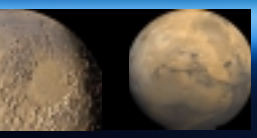
Zur Mitwirkung der Anwender gehört im wesentlichen der Betrieb eines WLAN, das den registrierten Nutzern aller teilnehmenden Anwender einen Zugang zum Wissenschaftsnetz ermöglicht sowie die Betreuung der bei ihm registrierten Nutzer durch Firstlevel Support, Schulung und Konfiguration von Endgeräten.

Technologisch wird DFNRoaming als verteilte Struktur von RADIUS-Servern realisiert. Als Protokoll kommt das international standardisierte Protokoll IEEE 802.1X zum Einsatz. Die Entscheidung für diesen technischen Ansatz beruht auf der Prämisse, ein gut skalierendes, nicht proprietäres technisches System zu schaffen, dass leicht in die bereits an vielen Stellen im Aufbau befindlichen europäischen Strukturen integriert werden kann.

DFNRoaming wird zum 1.1.2004 in den Pilotbetrieb gehen. In dieser Phase sollen z.B. Erfahrungen gesammelt werden, wie der Parallelbetrieb oder der Übergang von teilweise bereits bestehenden proprietären Authentifizierungsverfahren zum Standard IEEE 802.1X realisiert werden kann.

Der DFN-Verein will mit seinem neuen Leistungspaket DFNRoaming ein weiteren Baustein zu einem maßgeschneiderten DFNInternet Dienst hinzufügen. Die Idee von vielen „Internettankstellen“ für den reisenden Wissenschaftler rückt damit einen deutlichen Schritt näher und wird zunehmend von einer Vision zur Realität.

Weiterführende Informationen zu diesem Artikel finden Sie im Internet unter http://www.dfn.de unter dem Suchwort „DFNRoaming“.



Mapping Mars

Gigabit-Wissenschaftsnetz ermöglicht die zeitnahe Auswertung von Bilddaten der Mars-Mission

Nach Erkenntnissen bisheriger Marsmissionen gab es auf unserem Nachbarplaneten vor etwa 3,5 Milliarden Jahren eine Klimaveränderung, die aus einem vermutlich warmen und feuchten Himmelskörper einen Wüstenplanten machte. Die Fragen nach Wasservorkommen und der eventuellen Entstehung primitiver Lebensformen konnten trotz intensiver Forschung bislang nicht beantwortet werden. Die Mission soll durch Erkundung aus dem Orbit und durch Untersuchungen auf der Marsoberfläche vom Landegerät aus Aufschluss über die Klimageschichte des roten Planeten geben, die Rolle und den Verbleib von Wasser klären und schließlich nach mikrobiologischen Lebewesen suchen. Die Wissenschaftler erhoffen sich im Rahmen der vergleichenden Planetologie Parallelen zur Erde herstellen zu können, die beispielsweise genauere Aussagen über die langfristige Entwicklung unseres Planeten möglich machen würden. Deutschland ist mit drei Experimenten an der Mission beteiligt: dem Mars Radio Science Experiment „MaRS“, dem an Bord des Landers mitgeführten Bohrer „Pluto“ sowie unter der Leitung von Prof. Dr. Gerhard Neukum mit der Hochleistungskamera „HRSC“.

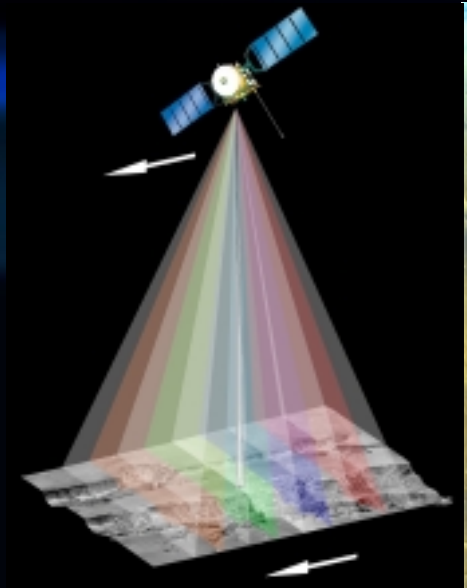
Die hochauflösende Stereokamera HRSC (High Resolution Stereo Camera), die an Bord der Mars-Mission zum roten Planeten unterwegs ist, wurde ursprünglich bereits für die russische „Mars 96 Mission“ entwickelt, jedoch bei einem Fehlstart im November 1996 zerstört. Bald darauf wurde eine modifizierte, auf Flugzeugen einsetzbare Version entwickelt. Die Flugzeugkamera HRSC-AX kam vom Mai 1999 bis zum Oktober 2001 im Rahmen des DFN-Gigabit-Testbed-Projektes „FIGARO-Fernerkundung im Wissenschaftsnetz“ zum Einsatz und wurde mehrere Jahre lang erprobt.

Die weiterentwickelte HRSC-Kamera, die sich an Bord der Mars Express Sonde befindet, hat die Erde am Abend des 02. Juni 2003 an Bord einer Sojus Fregat Trägerrakete vom russischen Weltraumbahnhof Baikonur/Kasachstan aus verlassen und wurde in den Erdorbit gebracht, von wo aus sie wenige Stunden später die Reise zum Nachbarplaneten antrat. Das Ziel ihrer Reise, den Mars-Orbit, wird die HRSC voraussichtlich am Heiligabend 2003 erreichen.

Anders als Film- oder Fotokameras verwendet die HRSC zur Aufnahme der Bilder Bildzeilen, durch die die Oberfläche beim Überflug „gescannt“ wird. Von den insgesamt neun Sensoren sind vier für die Erfassung in verschiedenen Spektralbereichen ausgelegt, die Daten der restlichen fünf Sensoren können aufgrund ihrer speziellen geometrischen Ausrichtung (vgl. Abb.) auch zur räumlichen Bestimmung von Digitalen Oberflächenmodellen (DOM) eingesetzt werden, d.h. für jeden Punkt auf der Oberfläche kann auch seine Höhe berechnet werden. Bei der Überquerung der Oberfläche mit der HRSC entstehen mehrere, teilweise überlappende Flugstreifen mit jeweils neun Datensätzen, deren Verarbeitung, Interpretation und Auswertung auf der Erde in einer verteilten Umgebung zwischen der DLR und verschiedenen Hochschulinstituten stattfindet. In ähnlicher Konfiguration wurde die verteilte Bildbearbeitung erstmals im Gigabit-Testbed erprobt.

Am marsnächsten Punkt der elliptischen Umlaufbahn (Perizentrum) beträgt der Abstand vom Raumschiff zum Mars 270 Kilometer. Bei dieser Höhe über dem Mars ist die Auflösung der 9 Bildstreifen 12 Meter für jeden der 5184 Pixel pro Zeilensensor. Die Bildstreifenbreite beträgt 52 Kilometer und die Mindeststreifenlänge 300 Kilometer. Ein Super Resolution Channel wird hierbei wie eine Lupe eingesetzt. Er liefert im Perizentrum 2,3 Kilometer x 2,3 Kilometer große Bilder in der Mitte der Bildstreifen, die Oberflächendetails mit einer Auflösung von 2,3 Meter pro Pixel abbilden. Diese SRC- Aufnahmen erhalten ihren besonderen Wert durch den geologischen Kontext der Umgebung, welcher durch die Bilder des hochauflösenden Stereokopfes geliefert wird.

Vor der Datenübertragung zur Erde werden die Bilder in einer „HRSC Digital Unit“ nach einem JPEG-ähnlichen Verfahren komprimiert und im Mars-Orbiter zwischengespeichert und dann zur ESA-



Hydrothermale Aktivität durch Vulkanismus: Spuren auf der Marsoberfläche deuten auf katastrophale Fluten in der Vergangenheit hin

Bildquelle: DLR

Antenne nach Australien übertragen. Tag für Tag werden auf diese Weise 0,5 bis 6 Gigabit Daten zur Erde gesendet, wobei die Bandbreite der Satelliten-Übertragung wesentlich von der Entfernung Erde-Mars abhängt. Die Bilddaten der Marsoberfläche machen etwa 40 Prozent der gesamten Missionsdaten aus, die von sechs weiteren Instrumenten am Bord des Orbiters sowie vom Lande-Modul auf der Marsoberfläche stammen.

Von Australien aus werden die HRSC-Daten zum ESOC (European Space Operations Center) in Darmstadt uebertragen und nach Instrumenten sortiert. Die HRSC-Daten werden anschließend zum DLR-Institut für Weltraumsensorik und Planetenerkundung in Darmstadt übertragen und dort systematisch prozessiert und dann über das Gigabit-Wissenschaftsnetz zur weiteren Verarbeitung und Analyse an das HRSC-Team im Institut für Planetenforschung des DLR in Berlin Adlershof übertragen. In Adlershof werden die Daten radiometrisch, photometrisch und geometrisch korrigiert, wobei die Helligkeits- und Kontrastunterschiede aus den verschiedenen Überflügen sowie die Verzerrungen und die Seiten- und Höhenverschiebungen der Bildpunkte, die in Folge der Eigenbewegung der Satelliten-Kamera auf der Mars-Umlaufbahn unvermeidlich sind, ausgeglichen werden.

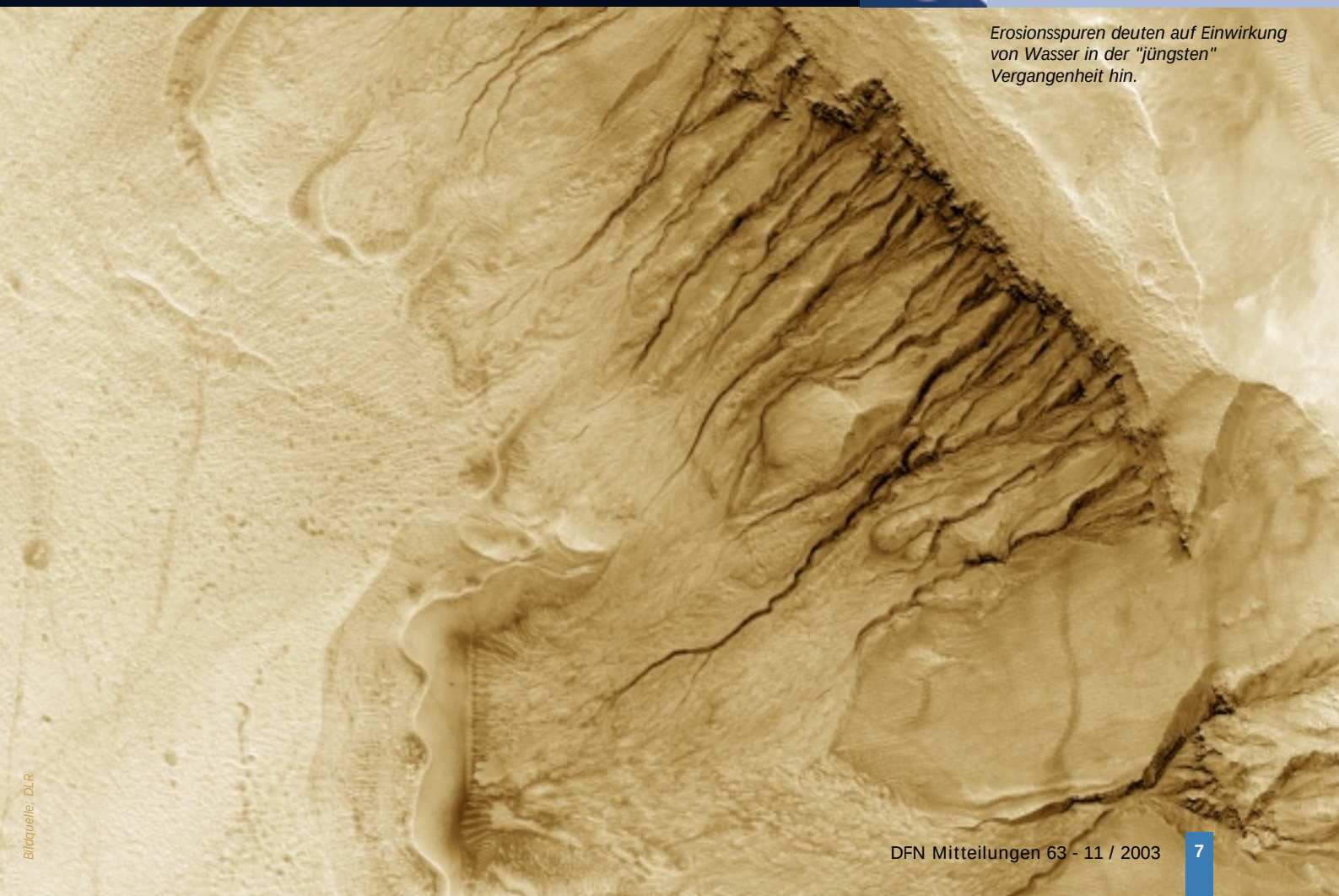
Anschließend werden die Daten über eine 155 Mbit/s-Verbindung zum Gigabit-Wissenschaftsnetz zur Weiterbearbeitung zur Technischen und zur Freien Universität Berlin, zur TU-Dresden, TU-München und zu einer Reihe weiterer Institute weltweit übertragen und zu speziellen Darstellungsformen der Marsoberfläche weiterverarbeitet. Am Dresdener Institut für Kartographie etwa hat man sich auf dreidimensionale Oberflächenmodelle spezialisiert, wärend am Kartografie-Institut der TU-Berlin eine „topografische Bilder-Karte“ der Mars-Oberfläche im Maßstab 1:200.000 erstellt wird, in der die „Orthobilder“, die im wesentlichen einer Luftbildkarte entsprechen, durch topografische Namen und Spezifikationen sowie durch Relief-Informationen ergänzt werden. An der TU-München wiederum werden die Lageparameter des Mars-Orbiters anhand der „Stereo-Daten“ der Kamera, die eine räumliche Bestimmung der Fluglage und -höhe während des Filmens erlauben, korrigiert. Die Datenmenge der aufbereiteten Bilder, die Adlershof täglich verlassen, beträgt zwischen 2,4 und 30 Gbit/Tag und wird an insgesamt 40 Institute weltweit versendet. Während der geplanten Projektlaufzeit von einem Marsjahr – dies entspricht etwa 2 Erdenjahren – werden auf diese Weise zwischen einem und zwei Terabyte Ausgangsdaten zur Weiterverarbeitung versendet. Im Zuge der Weiterverarbeitung z.B. zu dreidimensionalen Ansichten der Marsoberfläche oder zur topografischen Bilder-Karte wird sich die Menge der Mars-Daten, die über das Deutsche Forschungsnetz übertragen werden, noch um ein Vielfaches steigern.

Weitere Informationen und erste Bilder der Mars Mission finden sich im Web unter: http://www.dlr.de/dlr/Raumfahrt/Missionen/marsexpress/marsexpress_ge.html

Ab voraussichtlich Anfang Januar werden unter dieser Adresse auch die ersten Aufnahmen der Marsoberfläche bereitgestellt werden.

Kai Hoelzner
DFN-Verein

Hoelzner@dfn.de



Erosionsspuren deuten auf Einwirkung von Wasser in der "jüngsten" Vergangenheit hin.

Bildquelle: DLR

Closing The Gap –

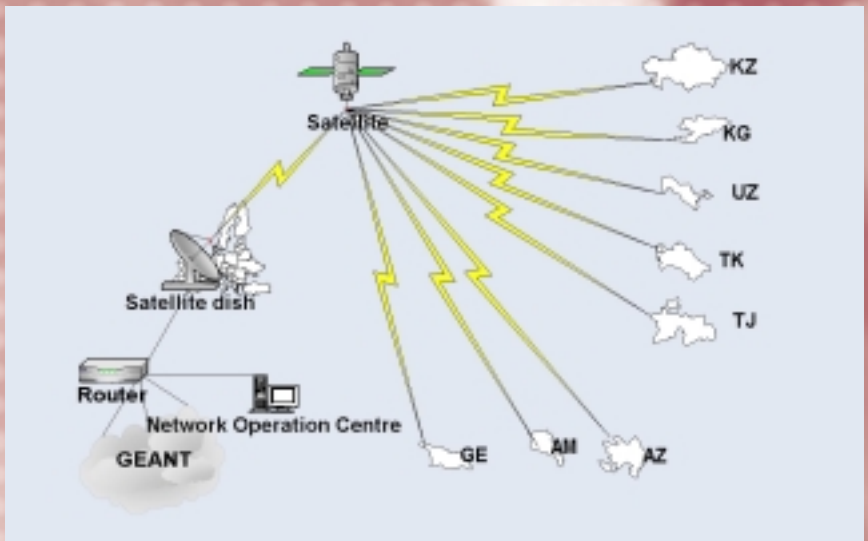
Das „Virtual-Silk-Highway-Projekt“, kurz „SILK-Projekt“, hat sich zum Ziel gesetzt, mittels Satelliten-Technologie kosteneffektive und robuste Konnektivität für die Wissenschaften in Zentralasien und in der Kaukasusregion bereitzustellen und damit den Informationsaustausch der Wissenschaften untereinander und mit der weltweiten Wissenschaftscommunity zu fördern. Das SILK-Projekt verfolgt dabei nicht allein technische Ziele. Es versteht sich vielmehr auch als Werbung für eine offene Gesellschaft, für demokratische Prozesse und eine Verbesserung der Bildungssysteme im Kaukasus und in Zentralasien. Nicht zuletzt will das seit 2001 laufende und auf vier Jahre angelegte Projekt Wissenschaftler aus untereinander zerstrittenen Staaten wie Armenien und Aserbaidschan an einen Tisch bringen und Politikern, die der Idee einer „offenen Gesellschaft“ und den Möglichkeiten der Informationstechnologie skeptisch gegenüber stehen, vom Nutzen der Kommunikationstechnologie überzeugen. Das Schließen der digitalen Kluft zwischen den informationsreichen und informationsarmen Ländern soll dabei helfen, Frieden und Sicherheit im Kaukasus und Zentralasien zu stabiliesieren.

Internet versus Brain Drain

Im Schatten der militärischen und politischen Aufgaben der NATO steht seit 45 Jahren ihr wissenschaftliches Engagement. Jahrzehntelang bezogen sich die Aktivitäten ausschließlich auf die Mitgliedsstaaten des Verteidigungsbündnisses. Seit Anfang der 90er Jahre hat sich die Strategie der NATO in Sachen Wissenschaftsförderung gewandelt. Mit den Programmen „Science for Peace“, „Life-Science“ und „Computer Network Infrastructure“ bemüht sich das Bündnis seither, den Brain Drain einzudämmen, den die Mitgliedsstaaten der ehemaligen Sowjetunion erleiden, seit die Rote Fahne in der Neujahrsnacht 1991/92 vom Dach des Kremls niedergeholt wurde. Auch osteuropäische Staaten, die noch nicht Mitglieder der Allianz waren, konnten seitdem als „Partnerländer“ am Science-For-Peace-Programm partizipieren. Mitte der 90er Jahre schließlich weitete die NATO ihr Programm auch auf die sogenannten „STAN“-Länder aus, die jenseits des Kaspischen Meeres zum südlichen Gürtel der vormaligen Sowjetunion gehören. Mit jährlich etwa 2,5 Mio. US-Dollar wird seither unter der Leitung von Walter Kaffenberger, NATO-Programmdirektor für Computer-Networking, der Aufbau von Rechner- und Netzinfrastrukturen in Ost-Europa und Zentralasien gefördert, wobei sich die Ausrichtung auf lokale Netzwerke sukzessive in Richtung eines Aufbaus von Wide-Area-Strukturen verschiebt. Ein Drittel dieses Etats wird derzeit für das SILK-Projekt bereitgestellt.

Kaukasische Kabel

Während Russland seit August diesen Jahres über eine 622Mbit/s Verbindung nach Helsinki ins NordUNet verfügt, von wo aus eine Verbindung ins GÉANT besteht, haben die Hochschulen und Akademien in der Kaspi-Region bislang



das „Virtual-Silk-Highway-Projekt“

keine physischen Leitungen, die sie mit den westeuropäischen Forschungsnetzen verbinden. Dies liegt nicht etwa daran, dass Glasfasern ein rares Wirtschaftsgut am Südrand der ehemaligen Sowjetunion wären. De facto sind eine Vielzahl optischer Leitungen im Kaukasus und ebenso in den „STAN-Ländern“ vorhanden. Eine davon ist die Glasfaser, die 1994 von Siemens verlegt wurde und Hamburg mit Shanghai verbindet. Unglücklicherweise wurde diese Faser, die über mehrere Tausend Kilometer mitten durch die Seidenstraßen-Region läuft, mit der damals als innovativ geltenden ISDN-Technik ausgestattet. Für eine heutige Nutzung zur Datenübertragung müssten sämtliche Vermittlungsstellen technisch umgerüstet werden – eine Investition, die angesichts dürftiger Rentabilitätsaussichten und großer administrativer Probleme in mehreren Anrainerstaaten derzeit wenig Aussicht auf Verwirklichung hat.

Ein weiteres, nicht zu unterschätzendes Hemmnis für die Erschließung Zentralasiens mit Internetverbindungen ist zum Beispiel die Unsitte, funktionstüchtige Datenleitungen aus dem Erdboden zu reißen, um an den im Innern vermuteten Kupferstrang zu gelangen. Zwar ist die Enttäuschung der illegalen Recycling-Unternehmer groß, wenn sich im Innern kein Metallkern findet, doch selbst für die feine Siliziumfaser gibt es noch Verwendungsmöglichkeiten: Von Zeit zu Zeit tauchen Bündel dieser Lichtleiter als dekorative Lampen auf den Basaren der Region auf. Als Ergebnis dieser Situation sind breitbandige Internetverbindungen meist nur zu horrenden Konditionen zu haben, so dass sich die Wissenschaftler Kaukasiens und Zentralasiens national wie international mit Bandbreiten von 64 Kbp/s bis 384 Kbp/s für die gesamte Forschungs- und Bildungscommunity eines Landes begnügen müssen.

Die Situation der nationalen Forschungsnetze

Die nationalen Infrastrukturen der SILK-Länder sind so unterschiedlich wie die Kulturen, die entlang der Seidenstraße aneinandergeknüpft sind. Während im ölreichen Aserbaidschan gleich zwei NRENs konkurrieren und zumindest in den Städten gut ausgebaute Mobilfunknetze vorhanden sind, verfügt das am gegenüberliegenden Ufer des Kaspischen Meeres angrenzende Turkmenistan auch heute noch über kein eigenes Wissenschaftsnetz. Seit dem ersten Ping, der 1997 von Turkmenistans Hauptstadt Aschchabad ins globale Internet ging, nahm die Entwicklung der I.u.K.-Technik in Turkmenistan einen höchst wechselhaften Verlauf. Zwar versuchte seit 1998 eine kleine Zahl von kommerziellen ISPs mit Erlaubnis des Kommunikationsministeriums eine Alternative zum Internet-Monopolisten Turkmentelekom zu etablieren, doch wenige Jahre später zogen sich diese Initiativen wieder zurück und warten nach Aussage des UNDP-Berichtes über die Lage der IT-Entwicklung in Turkmenistan auf „einen günstigeren Moment, den Turkmenischen Markt zu betreten“. Lediglich ein einziges privates Unternehmen war 2002 noch am Markt tätig, doch im Mai diesen Jahres wurde auch diesem die benötigte staatliche Lizenz entzogen, so dass Turkmentelekom heute als einziger ISP des Landes übrig geblieben ist.

Einen entgegengesetzten Verlauf wiederum nahm die Entwicklung in Usbekistan, wo bis zum Jahr 2002 noch kein NREN im eigentlichen Sinne existierte. Durch eine breit angelegte Initiative der Regierung und dank der konsequenten Arbeit des Teams um Vadim Navotny, Direktor der Usbekischen Forschungsnetz-Initiative UZSCINET, wurde vor kurz-

Schwierige Namensfindung

Bildhafte Namen sind für Forschungsprojekte heute das Salz in der Suppe. Ursprünglich sollte das SILK-Projekt „Alexander-Project“ heißen, benannt nach Alexander dem Großen, Herrscher von Mazedonien, der die Grenzen des griechischen Reiches im vierten Jahrhundert vor Christus bis auf den indischen Subkontinent ausdehnte. Doch anders als in Europa, wo Alexander als Begründer eines Weltreiches gilt, der interkulturelle Ehen und andere „moderne“ gesellschaftliche Ideen verfolgte, ist der Klang seines Namens für die Nachfahren der einst unterworfenen Völker ungefähr so anheimelnd wie hierzulande der Name Attila. Der Vorschlag, auf den Namen eines Eroberers zu Verzichten und das Projekt „Virtual-Silk-Highway“ zu nennen, kam schließlich von Asomiddin Atoev, Internet Project Director der Central Asian Development Agency (CADA) in Tadschikistan. Entgegen der weit verbreiteten Ansicht, bei der Seidenstraße handele es sich um eine lineare Strecke zwischen China und Europa, eine Art „Route 66“ der Antike, stellt die Seidenstraße ein weitverzweigtes Netz von Karawanenwegen dar, dessen Endpunkte in Karatschi und Bombay genauso wie in Rangoon, Hongkong und Hanoi zu finden sind. Das Handelsnetz „Seidenstraße“ existierte seit etwa 100 vor Christus und diente dem Transport der Luxuswaren Wolle, Gold, Mandeln und Seide. Wie die meisten alten Handelswege war die Seidenstraße nicht nur die wichtigsten Transportwege für Waren, sondern auch die Wege der Kommunikation, über die Informationen über fremde Welten ausgetauscht wurden.

em ein Durchbruch bei der Etablierung einer Kommunikationsinfrastruktur für die Wissenschaft erzielt. In einer Kooperation zwischen UNDP und George Soros' „Open Society Institute" wird derzeit in Usbekistan ein NREN aufgebaut, das künftig mehr als 100 Forschungs- und Bildungseinrichtungen mit Internetzugängen versorgen wird. Zusätzlich unterstützt die Firma CISCO Systems Usbekistan wie auch sämtliche andere SILK-Staaten durch Einrichtung einer „Networking Academy", in der bis heute mehr als 60 Studenten in Computer-Networking-Technologie unterrichtet wurden um in den Instituten des Landes beim Aufbau und Betrieb von Netzwerken mitzuhelfen.

Insgesamt mögen die Bandbreiten, mit denen sich die Netzwerker in Zentralasien begnügen müssen, manche Europäer an die Internet-Gründerzeit der Achtziger Jahre erinnern. Dennoch bestehen deutliche Unterschiede: Wesentlich konsequenter als die Westeuropäer profitieren die Wissenschaftler der SILK-Länder vom Know-how der Hochtechnologie-Nationen. Ganz selbstverständlich plädiert z.B. Asomiddin Atoev aus Tadschikistan für den Einsatz von Open-Source-Produkten: „Anstatt überteuerte Office-Pakete anzuschaffen", so Atoev, „ist es für die SILK-Teilnehmer weitaus sinnvoller, die knappen finanziellen Mittel in Hardware zu investieren".

Internationale Anbindungen

Getreu dem Motto, dass die einfachsten Technologien bei schwierigen Aussenbedingungen am effektivsten sind, setzt das SILK-Projekt auf stabile und bewährte Satellitenübertragungen. „Im Vergleich zu den fragilen Glasfasern verfügen Satelliten über extrem lange Entwicklungs- und Lebenszyklen: Allein sieben Jahre braucht die Entwicklung eines neuen Raumflugkörpers. Die Nutzungszeit im Orbit beträgt nicht selten eineinhalb Jahrzehnte", erläutert Hans Frese, Vorsitzender des Arbeitskreises Telekommunikation im Deutschen Elektronen Synchronotron (DESY) in Hamburg die Rahmenbedingungen seiner Arbeit. Frese ist einer der geistigen Väter des SILK-Projekts. Schon zu Zeiten des Eisernen Vorhanges organisierte er analoge Standleitungen zwischen der Sowjetunion und Deutschland. Bereits 1988 bedienten sich Hochenergiephysiker am DESY und deren russische Kollegen in Moskau einer 1200 Baud-Verbindung via Frankfurt an der Oder, um miteinander zu kommunizieren. 1993 wurde diese Leitung durch eine Satellitenverbindung mit der wesentlich höheren Bandbreite von 512 Kbit/s ersetzt. Satellitengestützte Zusammenarbeit begann kurze Zeit später auch mit dem Armenischen YerPhi-Physik-Institut in Eriwan .
Die Bandbreite, die bei einer Übertragung via Weltraum auf einem Satelliten zur Verfügung steht, nimmt sich mit insgesamt gut einem Gbit/s gegenüber den Kapazitäten in Glasfasernetzen zwar bescheiden aus, dennoch sprechen gewichtige Argumente für diese Technik: Abgesehen davon, dass in den meisten Teilnehmerstaaten des SILK-Projekts mangels Leitungen keine terrestrische Alternative besteht, benötigt der Betrieb eines Satelliten nur minimalen Wartungsaufwand. Zudem können an jedem Ort in kürzester Zeit Verbindungen bereitgestellt werden, die im Rahmen der gegebenen (Bandbreiten)-Möglichkeiten schnell und leicht skalierbar sind.
Der derzeit genutzte Eurasiasat-1, der im Januar 2001 an Board einer Ariane IV-Rakete vom Französischen Weltraumbahnhof Guyana in den Orbit gebracht wurde, fungiert neben seinen wissenschaftlichen Zwecken auch als Fernsehsatellit. Die SILK-Daten nutzen bis zum Jahr 2004 24 Mbit/s von der Gesamtbandbreite des Satelliten, die laufenden Kosten für die Mitnutzung betragen jährlich etwa 800.000 US-Dollar.

Die Daten aus den acht SILK-Staaten laufen sternförmig auf einen zentralen Verteilerpunkt am DESY in Hamburg zu. Von Hamburg aus wird der Datenverkehr über das DESY in das Deutsche Forschungsnetz übergeben und anschließend in Frankfurt mit dem GÉANT verbunden. Das gesamte System wird durch das „SILK Network Management, Monitoring and Control Centre" (NMMC) überwacht. Die Road-Map des Projektes sieht vor, jedes der angeschlossenen Länder bis zum Jahr 2005 mit einer „Minimal"-Bandbreite von 3Mbit/s zu versorgen, wobei den Teilnehmern gestattet ist, die ungenutzten Bandbreiten anderer Teilnehmerländer kurzfristig auszuschöpfen. Um die geringen Bandbreiten optimal zu nutzen, wurden die Teilnehmer nicht nur mit der Satellitentechnik, sondern ebenso mit Caching-Engines ausgestattet. Bevor eine Download via Satellit beginnt, prüft das System, ob die nachgefragten Daten in der Vergangenheit bereits einmal heruntergeladen wur-

Links zu den angeschlossenen NRENs:		
Armenien	ARENA	http://www.arena.am (engl.)
Aserbaidschan	AZRENA	http://www.azrena.org (ru./engl.)
Georgien	GRENA	http://www.grena.ge (ru./engl.)
Kasachstan	KAZRENA	http://www.kazrena.kz (ru.)
Kirgisische Republik	KRENA	http://aknet.kg/ (ru.)
Tadschikistan	TARENA	http://www.tarena-tj.org
Turkmenistan		z.Zt. kein Webangebot
Usbekistan	UZSCINET	http://www.uzsci.net (ru./engl.)

Weitere Informationsquellen:		
SILK-Projekt	Silk-Projekt-Seite	www.silkproject.org (engl.)
CEENET	Netzwerkorganisation für Osteuropa und Zentralasien	http://www.ceenet.org (engl.)
UNDP	United Nations Development Programm	http://www.undp.org/
OSI	Open Society Institute	http://www.soros.org/

den und im Caching-Modul verfügbar sind. Das NMMC stellt sicher, dass die Satelliten-Bandbreite in allen Teilnehmerländern in akzeptablen Grenzen bleibt und sich die Teilnehmer untereinander keine Kapazitäten streitig machen. Darüber hinaus können durch das NMMC zu besonderen Anlässen zusätzliche Bandbreiten zur Verfügung gestellt oder die Charakteristiken der Caching-Engines verändert werden. Neben dem NMMC verfügt SILK über ein russischsprachiges Network Operation Centre (SILK-NOC), das vom Hamburger DESY aus einen Help Desk anbietet und die Kontakte zum Satelliten-Provider Eurasia-Sat unterhält.

Kai Hoelzner
DFN-Verein

Hoelzner@dfn.de

Hilfe zur Selbsthilfe

Obwohl SILK eine Reihe von Verbesserungen für die technische Kommunikation der teilnehmenden Staaten darstellt, versteht sich das Projekt lediglich als ein Anstoß für weitere Entwicklungen, die in der Kaukasusregion und in Zentralasien erhofft werden. Denn trotz Caching und Bandbreitensharing sind die Übertragungsraten via Satellit knapp bemessen. Die Strategie des SILK-Projektes ist es jedoch nicht, sämtliche Bandbreitenbedürfnisse in den angeschlossenen Ländern zu befriedigen. SILK soll für die Teilnehmerländer lediglich ein erstes Fenster zum Europäischen Forschungsbackbone sein. Die Teilnehmerstaaten haben im SILK-Projekt die Option, aus eigenen Mitteln zusätzliche Bandbreiten zuzukaufen. Darüber hinaus ist es Teil des Projektes, dass sich die Projektbeteiligten bereits während der Projekt-Laufzeit auf die Suche nach alternativen Finanzmitteln und Management-Lösungen begeben, durch die die Satelliten-Infrastruktur auch nach Beendigung der Projektlaufzeit weiter betrieben werden kann. Hierzu dienen unter anderem eine Reihe von Workshops und Events, die mit prominenter Beteiligung in den Teilnehmerstaaten durchgeführt werden und helfen sollen, das Projekt in den einzelnen Ländern zu befördern. Der Erfolg dieser Strategie zeigt sich derzeit an der Entwicklung Usbekistans. Er zeigt sich noch stärker im Anbetracht der Tatsache, dass selbst der Turkmenische Präsident Sapamurat Niyazov, in den Medien besser bekannt als „Turkmenbashi“, trotz größter Vorbehalte gegen das Internet die Teilnahme Turkmenistans am SILK-Projekt ausdrücklich begrüßt.

WLAN-Roaming im Europäischen Wissenschaftsbereich

Problemstellung

Die zunehmend flächendeckende Verfügbarkeit von drahtlosen Datennetzen (WLANs, IEEE 802.11) an vielen Hochschulen und Forschungseinrichtungen – aber auch daheim, in Hotels, Tagungszentren, Flughäfen, Cafés u.ä. – wird die derzeitige Arbeitsweise und die Arbeitsmöglichkeiten vieler Wissenschaftler und Studenten verändern, indem sie es technisch ermöglicht, eine weitgehend durchgängige Konnektivität (d.h. Zugang zu Internet-Ressourcen) herzustellen. Mitarbeiter und Studierende können dann räumlich weniger eingeschränkt und damit wesentlich flexibler mit ihren mobilen Endgeräten (Notebooks, PDAs) arbeiten.

Allerdings ist die alleinige Existenz von WLANs in vielen Hochschulen nicht ausreichend, um ortsunabhängig Konnektivität (sogenanntes Roaming) bereitstellen zu können. Die Nutzung eines „fremden" WLAN wird z.B. explizite administrative Schritte erfordern, die nicht ad-hoc erreichbar sind. Dies ist besonders nachteilig bei benachbarten Hochschulen und Forschungseinrichtungen, zwischen denen Mitarbeiter und Studierende täglich pendeln können sollen, ohne daß hierdurch der durchgängige Netzzugang – meist zum jeweiligen WLAN – erschwert wird, aber auch bei Arbeitstreffen, Konferenzen und Gastaufenthalten störend. Internet-Konnektivität (Netzzugang) oder gar die Erreichbarkeit der auf dem eigenen Campus gewohnten Arbeitsumgebung (Email, Groupware, Fileserver etc.) „von außen" ist daher nur durch Zusatzvorkehrungen zu erlangen, die einrichtungsübergreifend organisiert werden müssen. Der von den Gastnutzern dabei genutzte Bandbreitenanteil wird sich im Normalfall im Promille-Bereich des Anschlusses der Einrichtung befinden; ein Billing bzw. gegenseitiges Verrechnen ist aus gegenwärtiger Sicht nicht erforderlich. Geeignete Accountingsysteme können das absichern, werden hier aber nicht näher betrachtet.

Es bedarf also einer technischen Lösung, die ein weitgehend transparentes Roaming zwischen all jenen Einrichtungen ermöglicht, die ihren Nutzern ohne individuelle vorherige Anmeldung gegenseitig Zugang zum jeweiligen WLAN gestatten wollen. Hierzu hat sich unter der Schirmherrschaft von TERENA, der europäischen Dachorganisation nationaler Forschungsnetze, eine Arbeitsgruppe mit dem Ziel etabliert, eine Roaming-Architektur für die Forschungsgemeinde in Europa zu definieren und zu testen. Zunächst hat die Arbeitsgruppe Anforderungen an derartige Roaming-Lösungen ausgearbeitet sowie verschiedene Roaming-Technologieszenarien zusammengetragen. Drei Verfahren haben sich herauskristallisiert und werden gegenwärtig evaluiert sowie in Bezug auf ihre Interoperabilität untersucht. Über die bisherigen Ergebnisse der Arbeitsgruppe wird im folgenden zusammenfassend berichtet.

Anforderungen an Roaming-Lösungen

Die nachfolgenden allgemeinen Anforderungen an eine Roaming-Lösung wurden von der Arbeitsgruppe definiert:

• **Der Ansatz muß skalieren.** Es wird angenommen, daß sich tausende Einrichtungen in Europa (und ggf. weltweit) an einer Roaming-Lösung beteiligen. Dies darf weder Komponenten überlasten noch dazu führen, daß bereits beteiligte Institutionen für jede neu hinzukommende eine Änderung ihrer Konfiguration ausführen müssen. Gleichzeitig sollte die Lösung bevorzugt auf bereits vorhandene zentrale/dezentrale Infrastruktur aufsetzen (Investitionsschutz).

• **Der administrative Aufwand für den Betrieb soll gering sein.** Zwar ist es vorstellbar, daß in der eigenen Einrichtung ein einmaliger Konfigurationsschritt erforderlich ist, um einen Nutzer für den Roaming-Verbund zuzulassen, aber es wäre inakzeptabel, wenn dieser Schritt bei jedem Netzzugang von einem anderen Ort aus wiederholt werden müsste. Zugleich wäre es sinnvoll, die Roaming-Lösung in vorhandene AAA-Infrastrukturen (Authentication, Authorization, Accounting) zu integrieren.

• **Die Lösung muß rechtlich zulässig sein.** Es darf zu keinen regulatorischen Überschreitungen kommen. Die Lösung muß in allen Europäischen Forschungsnetzen einsetzbar sein.

• **Sicherheitskonzepte der beteiligten Einrichtungen (u.a. bzgl. Zugangskontrolle/-beschränkung) müssen gewahrt bleiben.** Die Sicherheit der eigenen Institution darf von den Maßnahmen einer anderen Einrichtung nicht beeinträchtigt werden, sonst wird sich verständlicherweise niemand beteiligen.

• **Die Nutzung muß zurechenbar sein.** Es muß eine Möglichkeit bestehen, im Bedarfsfall unzulässige Aktionen den verursachenden Nutzern zuordnen und diese ggf. sperren zu können. Ein anonymer Zugang könnte für Spam, DoS-Attacken (Denial of Service) o.ä. mißbraucht werden. Die zugelassene Nutzergruppe setzt sich aus allen Mitgliedern der beteiligten Einrichtungen mit Roaming-Berechtigung, also aus Nutzern aller Europäischen Forschungsnetze, zusammen. Damit wird eine rechtliche Beziehung zwischen Anbieter und Nutzer hergestellt.

• **Der Dienst sollte für alle Nutzer verfügbar sein,** ggf. also auch für drahtgebundene Endgeräte. Er sollte sich auf alle gängigen Betriebssysteme erstrecken. Den Nutzern sollte ein Durchgriff auf die gewohnten Dienste auf dem eigenen Campus möglich sein. Sie müssen auch als Gast z.B. eigene ergänzende Sicherheitsmechanismen wie SSH und VPN-Verbindungen nutzen können (entweder direkt oder „on-top").

• **Die eingesetzten Verfahren müssen zwingend auf Standards basieren.** Sie dürfen sich zudem nicht auf IPv4 beschränken, IPv6 muß integrierbar sein.

Eine Roaming-Lösung soll die o.g. Anforderungen möglichst umfassend erfüllen, aber auch auf vorhandene Infrastruktur aufsetzen. Daher sind die derzeit an Hochschulen und Forschungseinrichtungen bestehenden WLAN-Sicherheitskonzepte einzubeziehen.

Entwicklung von Sicherheitskonzepten für WLANs

Drahtlose Netze sind generell als unsicher einzustufen. Weder läßt sich der Sendebereich klar begrenzen noch die Gemeinsamkeit der Nutzung vermeiden – „shared media". Es wurde zudem schnell erkannt, daß die Sicherheitskonzepte der „ersten Stunde" unzureichend sind [1]:

Der Netzwerkname (SSID, Service Set ID) muß auf den Klienten und den Zugangspunkten (AP, Access Point) übereinstimmen, wird im Klartext übermittelt und ist damit leicht abhörbar.

Die initiale, statische Variante der WEP-Verschlüsselung (Wired Equivalent Privacy) ist unsicher. Zum einen kann der genutzte Schlüssel mit wenig Aufwand ermittelt werden und liegt teilweise im Klartext vor, zum anderen steht nur eine begrenzte Menge gemeinsamer Schlüssel für alle lokalen Nutzer bereit, die den oder die Schlüssel alle kennen müssen – „shared secret".

Eine Zugangsbeschränkung über die MAC-Adresse der WLAN-Karte läßt sich zum einen relativ einfach umgehen, da MAC-Adressen nicht fälschungssicher sind (MAC address spoofing), zum anderen läßt sie nur unscharfe Rückschlüsse auf den tatsächlichen Nutzer zu, wenn sie nicht mit User Credentials (Nutzername, Passwort) im Nutzerverzeichnis kombiniert wird. Zudem ist eine Registrierung aller Karten bzw. Zugangsgeräte sehr aufwendig und problematisch im Besuchsfall.

So sind die WLAN einsetzenden Einrichtungen bislang gezwungen, eigene Sicherheitslösungen (z.B. lokales VPN, lokales IEEE 802.1X) aufzusetzen, um die oben genannten Ziele bzw. eine Teilmenge davon zu erreichen. Im Ergebnis gibt es viele unterschiedliche Ansätze und Produkte, die nun entweder zu koppeln oder komplett zu ersetzen sind, will man den Endnutzern ein weiträumiges Roaming ermöglichen.

Bestandsaufnahme von Roaming-Ansätzen im wissenschaftlichen Umfeld

Die Bestandsaufnahme der TERENA-Arbeitsgruppe zeigte drei wesentliche Ansätze für Zugangsverfahren [2, 3, 4], jeweils benannt nach der zugrunde liegenden Technologie, die derzeit in verschiedenen Forschungsnetzen eingesetzt und inzwischen zugleich als Basis für das dortige Roaming verwendet werden – teilweise lokal, teilweise in regionalen Verbünden oder bereits auf der Ebene des nationalen Forschungsnetzes:

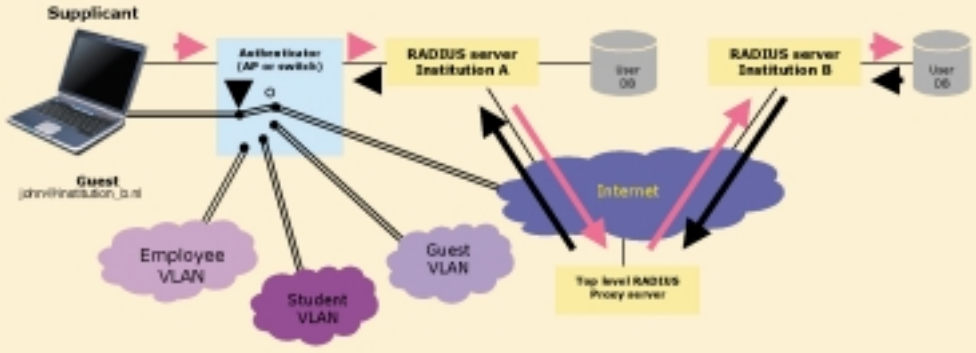
- **IEEE 802.1X.** Dieses seit Juni 2003 als Standard verfügbare portbasierte Verfahren beschreibt die Authentifizierung an der äußeren Grenze („edge") eines Netzes. Diese findet auf Layer 2 statt; Layer-3-Konnektivität (IP) wird erst erlangt, nachdem sich der Client („supplicant") gegenüber der Netzkomponente („authenticator") ausgewiesen hat. Dies ist hier ein WLAN-Access Point (AP), sonst ein Switch o.ä. Der AP kann z.B. mit einer RADIUS-Hierarchie gekoppelt werden, die dann die eigentliche Authentifizierung übernimmt (Abb.1).
Das eingesetzte EAP/EAPoL (Extensible Authentication Protocol, RFC 2284) ist ein Trägerprotokoll, in das verschiedene Mechanismen eingepasst werden können, z.B. TLS (Transport Layer Security, dafür ist eine PKI erforderlich!), TTLS (Tunneled TLS) oder PEAP (Protected EAP). Hier gibt es eine beträchtliche Vielfalt. Die nachfolgende Verschlüsselung erfolgt über dynamische, d.h. zur Laufzeit hinreichend häufig wechselnde WEP-Schlüssel.

IEEE 802.1X ist bei den Teilnehmern der Arbeitsgruppe auf Grund des zukunftsträchtigen Potentials auf großes Interesse gestoßen. Eine Referenzinstallation ist bei SURFnet zu finden [5]. SURFnet hat in den Niederlanden auf der Basis von TTLS einen nationalen Verbund inkl. RADIUS-Hierarchie initiiert, dem sich inzwischen mehrere Firmen und Hochschulen angeschlossen haben. Dabei kommt eine in einem Kooperationsprojekt speziell

C. Bormann, R. Paffrath, N. Pollem, J. Rauschenbach

Ansprechpartner in der DFN-Geschäftsstelle:
Dr. Jürgen Rauschenbach
E-Mail: jrau@dfn.de

Abbildung 1: IEEE 802.1X-Schema (Quelle: SURFnet)



erstellte 802.1X-Client-Software zum Einsatz (Freeware), die Forschungseinrichtungen zur Verfügung gestellt werden kann.

Das noch neue Verfahren hat inzwischen Eingang in viele Produkte gefunden. Die Standardisierung ist abgeschlossen und die benötigte Client-Software ist für die gängigen Plattformen verfügbar und in einige Betriebssysteme bereits integriert (Windows 2000, XP, MAC OS X 10.3). Heute eingesetzte Access Points unterstützen 802.1X mit wachsender Tendenz, für viele APs kann 802.1X nachinstalliert werden.

Auch wenn hier die Entwicklung und Integration schnell fortschreitet, ist aus gegenwärtiger Sicht davon auszugehen, daß es auf absehbare Zeit etablierte Campusnetze bzw. WLAN-Installationen geben wird, die 802.1X nicht oder nicht durchgängig unterstützen.

Gemessen an den Anforderungen kann festgestellt werden, daß 802.1X bzw. die zugehörige Infrastruktur gut skaliert, die Sicherheitskriterien erfüllt werden und die Verfügbarkeit ausreichend ist.

- **VPN** (Virtual Private Network). Basierend auf den Randbedingungen eines unsicheren Zugangsnetzes einerseits und der fehlenden Nutzer-basierten Anmeldung andererseits haben viele der „frühen" Campus-WLANs eine VPN-basierte Lösung implementiert. Dabei wird das WLAN-Zugangsnetz (docking network) als VLAN vom restlichen Campusnetz abgetrennt; der Klient erreicht andere Netze erst nach dem erfolgreichen Aufbau eines VPN-Tunnels zu einem verbindenden VPN-Gateway (Abb.2).

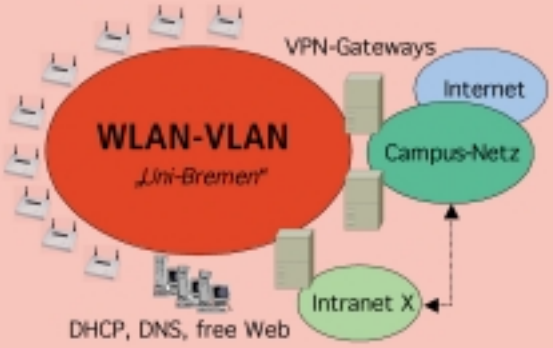


Abbildung 2: VPN-Ansatz

VPN-basierte Ansätze sind an vielen Hochschulen in Europa zu finden. Referenzlösungen gibt es in Deutschland [6], Portugal und der Schweiz (dort national als SWITCHmobile [7]). VPNs sind in der Regel übersichtlich und vergleichsweise einfach aufzusetzen, da es sich um homogene Lösungen handelt (frei verfügbare und kommerziell vertriebene Produkte).

Dadurch, daß mehrere Gateways eingebunden werden können, können auch unterschiedliche VPN-Varianten angeboten (meist PPTP und IPsec, dazu ggf. SSH) bzw. unterschiedliche Zugangsrechte auf unterschiedliche Gateways abgebildet werden. Die jeweiligen Clients sind analog 802.1X für alle gängigen Plattformen verfügbar – teilweise integriert, teilweise nachzuinstallieren.

Für die Einrichtung von Roaming muß ein Nutzer im besuchten Netz Zugang zu seinem VPN-Server im Heimatnetz erlangen. Wenn das gewährleistet werden kann, ist der Nutzer nicht von der VPN-Lösung im besuchten Netz abhängig. Alle am Verbund teilnehmenden VPN-Gateways sind über entsprechende Access-Listen freigeschaltet. Diese haben jedoch den Nachteil, daß alle teilnehmenden Einrichtungen eine neue Version der Liste einspielen müssen, wenn eine weitere Einrichtung dazukommt. In dieser Form skaliert die Lösung nicht und müßte für den europaweiten Einsatz modifiziert werden. (Siehe unten.)

Gemessen an den Anforderungen kann man feststellen, daß das Verfahren ein hohes Sicherheitsniveau bietet, gut anwendbar ist, sich bzgl. Roaming aber mit Skalierungsproblemen auseinandersetzen muß.

- **Web.** Die Architektur eines Web-basierten Authentifizierungssystems ist sehr einfach. Weder die APs/Switches noch die Geräte der Nutzer benötigen besondere Funktionen (ein Web mit SSL ist ausreichend, einzig ein „Access Control Device" als Verbindung zwischen Zugangsnetz und Außenwelt kommt noch hinzu). Der Nutzer bekommt via DHCP eine IP-Adresse zugewiesen und öffnet seinen Browser, der zu einer Authentifizierungsseite umgeleitet wird. Ein Formular erscheint; dort sind die Nutzerdaten (Name, Passwort, gegebenenfalls weitere Angaben) einzutragen. Nach erfolgreicher Authentifizierung erfolgt die Freischaltung bzw. Zuweisung einer routbaren IP-Adresse. Abbildung 3 zeigt den schematischen Ablauf einer Authentifizierung nach dem Web-Verfahren.

Die Web-Methode ist auch in öffentlichen Hotspots üblich. Da bei Verwendung von HTTP die Nutzer/Passwort-Information im Klartext versendet wird, wird unbedingt SSL/TLS empfohlen. Aber auch damit bleibt ein Sicherheitsrisiko (Nutzer muss Server-Zertifikat prüfen – viele Einrichtungen haben keine von den Browsern ohne weiteres akzeptierte Zertifikate). Eine SSL/TLS-Zertifikat-Infrastruktur bzw. -PKI ist derzeit nicht vorhanden und müßte erst aufgebaut werden.

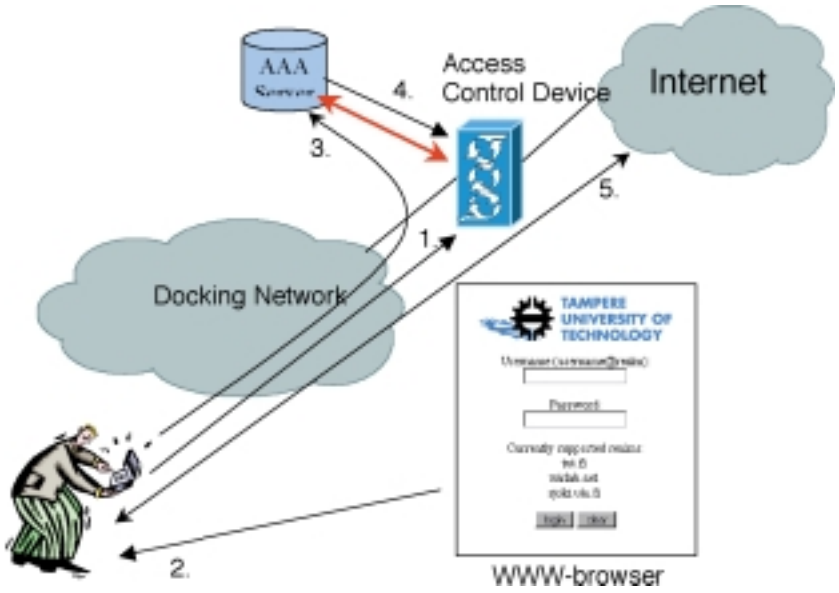
Eine Web-basierte Referenzinstallation ist in Finnland zu finden [8]. Der Zugangs-Server (Access Control Device) ist in diesem Fall ein Linux-PC, aber bzgl. des Basissystems gibt es kaum Einschränkungen. Auch kommerzielle Lösungen sind verfügbar (Nomadix, Vernier).

Gemessen an den Anforderungen kann zusammengefaßt werden, daß das Verfahren skaliert, sehr einfach zu nutzen ist, an der Sicherheit aber erhebliche Abstriche zu machen sind, da u.a. die Verschlüsselung der auf der Verbindung übertragenen Daten dem Nutzer selbst überlassen bleibt.

Roaming-Interoperabilität
Nach der Beschreibung der unterschiedlichen Verfahren stellt sich nun die Frage, wie die bestehenden Lösungen wechselseitig interoperieren können – wie also z.B. ein Nutzer, auf dessen eigenem Campus eine VPN-basierte Lösung im Einsatz ist, auf einem Campus zurecht kommt, auf dem der Zugang mittels IEEE 802.1X geregelt wird und umgekehrt – und welche Schritte ggf. erforderlich wären, um die einzelnen Ansätze auf einen regionalen/nationalen Kontext zu skalieren. Die Untersuchungen zu diesem Thema sind in der TERENA-Arbeitsgruppe noch nicht abgeschlossen. Die Ergebnisse werden im Bericht „Preliminary selection for inter-NREN roaming" dargestellt werden, der noch in diesem Jahr veröffentlicht werden wird.

Das Roaming zwischen Einrichtungen, die jeweils das gleiche Verfahren anwenden, ist einfacher als gemischte Kombinationen. In der homogenen 802.1X-Kombination sollte die Authentifizierung problemlos funktionieren, wenn der zuständige RADIUS-Server im Verbund und damit auch entfernt erreichbar ist. Das gilt analog auch für Einrichtungen, die den Web-basierten Zugang nutzen. Damit ist auch eine Kombination möglich. Die 802.1X- und die Web-basierte Lösung können für die Überprüfung der Zugangsdaten jeweils auf eine – gemeinsame – RADIUS-Hierarchie zurückgreifen. RADIUS-Server mit der geeigneten Funktionalität gibt es sowohl als Produkt (z.B. Radiator) als auch als Freeware (FreeRadius). Lokale RADIUS-Server sind oftmals ohnehin vorhanden und können sehr gut auch für das internationale Roaming genutzt werden.

Abbildung 3: Web-basierte Authentifizierung (Quelle: TUT)



Das Web-basierte Verfahren bietet sich grundsätzlich als Ergänzung einer 802.1X-Infrastruktur oder auch einer VPN-Infrastruktur an, da es ggf. von allen Gästen genutzt werden kann, die nicht über die entsprechende Klienten-Software verfügen.

Für das VPN-basierte Roaming ist der Zugang zum VPN-Gateway im Heimatnetz Voraussetzung. Als Lösung ist ein Vorschlag namens CASG (Controlled Address Space for Gateways) in der Diskussion, der das Skalierungsproblem entschärfen soll. Er ermöglicht, aus einem besuchten Zugangsnetz heraus transparent auf die Gateways der anderen Institutionen und damit auch auf jene auf dem eigenen Campus zuzugreifen, ohne die Gateways einzeln in die Zugangs-Listen aufnehmen zu müssen. Dieser Ansatz erfordert die Zuweisung von IP-Adressräumen, für den Endnutzer ist dieser Aufwand jedoch nicht sichtbar. Bei länder-basierten CASGs bliebe ein gewisser Konfigurationsaufwand zu leisten, sobald ein weiteres nationales Forschungsnetz hinzukommt.

Durch den Verbindungsaufbau zu einem VPN-Gateway auf dem eigenen und nicht dem besuchten Campus können die beteiligten Einrichtungen beliebig verschiedene VPN-Technologien einsetzen: die Clients der Endnutzer müssen nur auf die eigenen Gateways abgestimmt sein und brauchen im Roaming-Fall nicht gewechselt zu werden.

Zusammenfassung
Im Wissenschaftsbereich sind verschiedene Zugangslösungen für mobile Endgeräte im Einsatz. Das einfachste und kostengünstige ist das Web-basierte Verfahren, allerdings mit Problemen in Bezug auf Sicherheit. Die gegenwärtig am häufigsten anzutreffenden sind die VPN-basierten Verfahren. Sie gewährleisten ein hohes Sicherheitsniveau und sind relativ einfach anzuwenden, haben jedoch gewisse Skalierungsprobleme. 802.1X zzgl. RADIUS-Infrastruktur skaliert gut und hat ausgezeichnete Zukunftsaussichten. Aus diesen Gründen hat sich der DFN-Verein dafür entschieden, eine Roaming-Infrastruktur auf der Basis von IEEE 802.1X und RADIUS zu unterstützen (s.a. Artikel zum DFNRoaming).

Die Kopplung der genannten Verfahren ist möglich und mittelfristig auch zwingend erforderlich, will man alle Hochschulen und Forschungseinrichtungen einbeziehen. Die Bewertung und Umsetzung verschiedener Kombinationen ist in der TERENA-Arbeitsgruppe noch nicht abgeschlossen.

[1] http://www.bsi.bund.de/literat/doc/wlan/
[2,3,4] http://www.terena.nl/tech/task-forces/tf-mobility/DelAndDoc.html (Deliverable D, E, F)
[5] http://www.surfnet.nl/innovatie/wlan/
[6] http://www.wbone.org/
[7] http://www.switch.ch/mobile/
[8] http://www.atm.tut.fi/tut-public-access/

Neue Wege kooperativen Lernens – Das Paderborner Jour-Fixe-Konzept

Für die erfolgreiche Entwicklung und Erforschung von Methoden der kooperativen Wissensorganisation ist neben der Entwicklung geeigneter Werkzeuge und Theorien insbesondere ihre Einbettung in die tägliche Praxis der Aus- und Weiterbildung eine wichtige Voraussetzung. Für den von uns verfolgten Ansatz ist hierbei zentrales konzeptuelles und organisatorisches Element der Jour-Fixe. Begleitend zur Vorlesung stellen die Studierenden ihre semantischen Gestaltungs- und Strukturierungsfortschritte eines virtuellen Wissensraums zu festen Terminen, dem so genannten Jour-Fixe, vor. Hierzu nutzen sie ein spezielles kooperatives Shared Whiteboard, das im Rahmen des vom DFN-Verein geförderten open-sTeam-Projekts entwickelt wurde. Damit ist die Aufbereitung eines vorlesungsbezogenen Themas in kleineren Gruppen von Studierenden und seine Präsentation in einer Reihe von Jour-Fixe-Terminen Teil der späteren Prüfungsleistung. Der vorliegende Artikel stellt das Jour-Fixe-Konzept als integralen Bestandteil der Paderborner Lehre vor und schildert am Beispiel der Veranstaltung „Konzepte Digitaler Medien“ erste Erfahrungen in der Praxis.

Prof. Reinhard Keil-Slawik

Prof. Thorsten Hampel
Heinz Nixdorf Institut, Universität Paderborn
Fürstenallee 11
33102 Paderborn
Germany
E-Mail: {hampel|rks|}@upb.de

Kooperatives Lernen und Lehren braucht Werkzeuge und Konzepte

Seit der Antike ist die Vorlesung das klassische Modell der Wissensvermittlung an Universitäten. Der Lehrende trägt sein Wissen – heute unterstützt von Tafelbildern oder Folien – seiner Zuhörerschaft vor. Klassisch übertragen die Zuhörenden die vorgetragenen Ideen – Stichpunkte oder Tafelbilder in ihre persönlichen Unterlagen. Der Lehrende nimmt entsprechend die Funktion eines Mentors für ein Sachgebiet ein, Wissen wird vorstrukturiert, in verträgliche „Häppchen“ aufbereitet und vermittelt eine Orientierung und Struktur für die Lernenden. Gleichzeitig definiert sich durch die Vorlesung der für eine spätere Prüfung relevante Stoff, sie erfüllt die wichtige Funktion der Eingrenzung eines Themengebietes – Wissen wird handhabbar.

Die Vorlesung ist damit auch weiterhin ein essentieller Bestandteil moderner und neuartiger Lehr- und Lernprozesse; sie erfüllt die Funktion der Vorstrukturierung eines Sachgebietes, sie gibt Anleitungen zur Erschließung und hebt Relevantes hervor.

Begleitend zur Vorlesung exstieren eine Reihe ergänzender und in ihrer Arbeitsweise sehr vielfältige Lehr- und Lernkonzepte wie Seminare, Übungen oder Tutorien. In Übungen oder Tutorien wird das in der Vorlesung präsentierte Wissen vertieft und um Beispiele und Aufgaben angereichert; es steht das Üben von Einzelproblemen im Vordergrund. In der Praxis sind alle oben genannten Ausbildungsformen zumeist recht unverknüpft. Vorlesung und Übung finden in verschiedenen Räumlichkeiten und zu unterschiedlichen Zeitpunkten statt. Die Gruppe der Lernenden in der Vorlesung ist zumeist recht groß im Vergleich zu den Übungsgruppen oder Gruppen von Tutorien. In dieser Form ergeben sich vollständig divergente Gruppenbildungsprozesse zwischen Vorlesung und Übung. Zudem unterschieden sich meist die Dozenten und Übungsgruppenleiter – ein Wissensaustausch und gegenseitige Bezüge sind zwingend notwendig, jedoch gelingt es in vielen Fällen nur schlecht, Vorlesungsinhalte stetig mit Übungsinhalten, Beispielen und verschiedenen Sichten auf das Wissen zu verknüpfen.

In Hinblick auf die notwendige Stärkung sogenannter Schlüsselqualifikationen wie z.B. die Fähigkeit, Wissen praktisch anwenden und eigenständig Bezüge herstellen zu können, erscheinen die obigen Probleme besonders schmerzvoll. Hieran hat sich auch durch die Einführung „neuer Medien“ zunächst wenig geändert. Auch im Zeitalter des Hypertextes lassen computergestützte Lernprozesse nur wenig soziale Aktivitäten erkennen. Speziell das WWW degeneriert zum Ort nicht sequentiellen Lesens, in dem nur den Verweisen im vorbereiteten Hypertext gefolgt wird. Die Ursprungsidee des „nicht sequentiellen Schreibens“ nach Ted Nelson (Nelson, 1989) als wesentlicher Bestandteil des Konzepts von Hypertext ist in der aktuellen Praxis des E-Learning kaum verwirklicht. Entsprechend werden Lernenden keinerlei Möglichkeiten eröffnet, eigene und fremde Texte integrieren zu können. Auch unter dem Blickwinkel der Einsatzmöglichkeiten kooperationsunterstützender Systeme in der Präsenzlehre ergeben sich nur wenige Anknüpfungspunkte an das bestehende Lehrkonzept. Zwangsläufig reduziert sich ihr Einsatz auf das zur Verfügung stellen von Vorlesungsfolien oder bestenfalls auf die teilweise Unterstützung organisatorischer und inhaltlicher Aspekte des Übungsbetriebes.

Zwar können mittels kooperationsunterstützender Systeme beispielsweise Prozesse der Anmeldung zu Vorlesungen und Übungen oder auch Übungsabgaben vereinfacht werden , doch auch hier gelingt es in der Praxis kaum, Möglichkeiten des gemeinsamen Bearbeitens von Dokumenten geeignet zu unterstützten. Die Reduzierung des Hypertextes auf nicht-sequentielles Lesen bleibt weitgehend erhalten, Lernen bleibt eine individuelle, wenig soziale Aktivität.

Noch verstärkt wird das obige Defizit durch die weiterhin praktizierte klare Trennung von Vorlesung, Übung und Prüfung. Dieser Trennung aus individuellen und gemeinsamen, sozialen Lernprozessen steht das Konzepts des kooperativen Wissensraums (vgl. Hampel, 2002a und Hampel & Keil-Slawik, 2002) entgegen. Erst durch Einbeziehung verschiedener Formen des Lernens und der Zusammenarbeit in Gruppen begleitend zu einer Lehrveranstaltung ergibt sich die Notwendigkeit der Unterstützung durch Werkzeuge der kooperativen Wissensorganisation.
Auch der allgemein zu beobachtende Trend zu Verfahren des Blendet Learning, also der Zusammenführung von Präsenzlehre und Fernlernen, wird in der Beibehaltung der schon angedeuteten strikten Trennungen aus Vorlesung, Übung und Prüfung zur Farce. Nur das Überdenken von Vorlesungs- Übungs- und Prüfungskonzepten schafft einen notwendigen Freiraum in der Entwicklung neuer Wege der kooperativen Wissenskonstruktion.
Ziel der Paderborner Forschungen ist es, innovative Konzepte, Werkzeuge und Theorien der kooperativen Wissensorganisation und neue Formen des E-Learnings zu entwickeln und diese in der täglichen Praxis zu erproben und zu evaluieren. Hierbei können wir auf eine langjährige Erfahrung in der Entwicklung lernförderlicher Infrastrukturen zurückgreifen (Keil-Slawik, 1999).
Der kooperative Wissensraum wird zum wichtigen Unterstützungsinstrument kooperativer Lernprozesse. Im Konzept der Medienfunktionen (Hampel 2002a) werden zugleich wesentliche notwendige Handlungsfunktionen an Materialien definiert. Hier sind insbesondere das Arrangieren, also die Anordnung des Semantischen Raums, das Herstellen von Verweisen und Annotationen essentiell.

Der Paderborner Jour Fixe-Ansatz

Bezug nehmend auf die Defizite möchte der vorliegende Artikel unser Konzept des Jour-Fixe verdeutlichen. Der Jour-Fixe-Ansatz versucht in der Verbindung aus Methoden der kooperativen Wissensorganisation, des Erarbeitens und semantischen Strukturierens von Wissen in Gruppen und der Einbeziehung klassischer Vorlesungsanteile auch neue Formen des Ablegens von Prüfungsleistungen zu entwickeln.
Jour-Fixe bedeutet zunächst von der Herkunft des Wortes her eine regelmäßige Zusammenkunft, ein „fester Tag“ zu dem etwas vorgelegt oder vorgezeigt werden muss.

Wir verstehen unter dem Jour-Fixe Ansatz neben der festgelegten regelmäßigen und wiederkehrenden Zusammenkunft speziell den Aspekt des Vorstellens eines Sachverhaltes in Form einer „freien Aussprache“ und des gegenseitigen Austauschens und Kommentierens.
Der Jour-Fixe erfüllt damit die Funktion der regelmäßigen Zusammenkunft und des Austauschs, also die Präsentation, Verknüpfung, Kommentierung und Diskussion von Inhalten, sowie die regelmäßige Bewertung und Kontrolle des Fortschritts in der Strukturierung und Aufbereitung eines Wissensbereiches. Entsprechend sieht das verfolgte Konzept des Jour-Fixes eingebunden in den Veranstaltungsablauf die folgenden Komponenten vor:

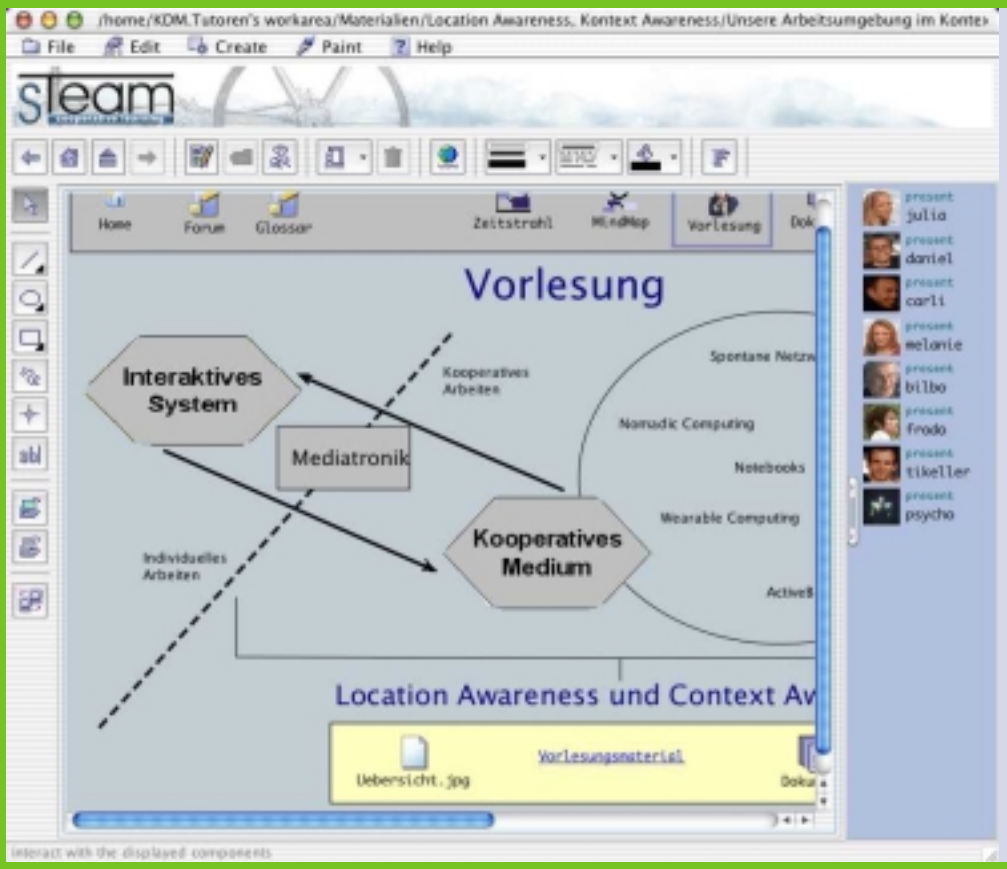


Abbildung 1: Ein Semantischer Raum: Kooperative Strukturierung des Raums mittels eines Shared Whiteboards

1) Vorlesungsanteile: Materialien werden durch den Dozenten vorgetragen; es werden wesentliche Leitideen vermittelt, Verknüpfungen zwischen Wissensbereichen hergestellt und Wissen maßgeblich vorstrukturiert. Vorlesungsfolien, Beispiele und ergänzender Text werden in einem netzgestützten Wissensareal zur Vorlesung abgelegt und damit den Zuhörern zur Verfügung gestellt. Idealerweise stehen diese Unterlagen schon vor dem eigentlichen Vorlesungstermin zur Verfügung, d.h. sie können von den Zuhörern parallel zur Vorlesung mit persönlichen Kommentaren und Anmerkungen versehen werden. (Im optimalen Fall wird dieser Prozess wiederum von einem kooperationsunterstützenden System geeignet unterstützt.

2) Strukturierung/Gruppenarbeit:
Übungsanteile: Studierende strukturieren in kleineren Gruppen Teilbereiche des präsentierten Vorlesungsstoffs, die die wesentlichen Kernideen und Methoden der Vorlesung wiedergeben. Übungsbeispiele, ergänzender Text, Referenzen und Quellen werden in einem dauerhaften, für einzelne Lernende und Gruppen von Lernenden frei zur Verfügung stehenden semantischen Wissensräumen verwaltet. Lernende können in einem derartigen Umfeld auch Kommunikationsmechanismen wie Nachrichtenbretter o.ä. nutzen um sich mit Mit-Lernenden auszutauschen.

3) Jour-Fixe: Wesentlicher Bestandteil der Aufbereitung und Vermittlung des Vorlesungsstoffes sind eine Reihe von bis zu fünf Jour-Fixe-Terminen. Hier müssen Studierende in kleinen Gruppen ein Kernthema der Vorlesung bearbeiten und in Form eines virtuellen Wissensraums aufbereiten. In einer Folge von so

genannten Jour-Fixe Zusammenkünften wird das aufbereitete Wissen der Gruppe regelmäßig allen Vorlesungsteilnehmern präsentiert. In der zeitlichen Verteilung der Jour-Fixes auf den Vorlesungsverlauf ergibt sich in den kurzen (zumeist nur 15-minutigen Vorstellungen) der einzelnen Gruppen zu jedem Jour-Fixe eine Entwicklungslinie der Aufbereitung eines Themengebiets in Form des virtuellen Wissensraums. Ein semantischer virtueller Wissensraum lässt sich hierbei als zentrales Element durch ein grafisches, als auch synchrones Werkzeug strukturieren

4) Prüfung/Jour-Fixe: Der Jour-Fixe, speziell die Vorstellung eines in der Gruppe aufbereiteten Übungsraumes, ist integraler Bestandteil der zu erbringenden Teil-Prüfungsleistung. Entsprechend erfolgt eine Vorstellung des aufbereiteten Wissensareals in der Gruppe in Kombination mit einem kurzen Fachgespräch.

Zentrales Element und in dieser Form neu ist damit die Verbindung aus Jour-Fixe und virtueller Wissensorganisation. Lernende müssen parallel zur Vorlesung ihr erlerntes Wissen konkret auf einen speziellen Aspekt, ein Themengebiet der Vorlesung anwenden und zuspitzen. Dieses Themengebiet wird mittels verschiedener Werkzeuge in einer Weise strukturiert, dass es den anderen Teilnehmern der Vorlesung hilft sich in dem gesamten Vorlesungsstoff zurechtzufinden.
Bewusst findet die Vorstellung des Wissensraumes und seiner Stufen der Strukturierung an mehreren Terminen statt. Lernende sollen in die Lage versetzt werden auch nicht vollständig ausgereifte Zwischenstufen ihrer Orientierung in einem Themengebiet vorzustellen und damit Raum für Fragen und Anregungen anderer Teilnehmer der Vorlesung schaffen. Idealerweise vernetzten sich die Themen auf diese Weise in einer Zusammenarbeit unterschiedlicher Jour-Fixe-Gruppen. Kontrastiv zum klassischen Seminar steht nicht allein der Seminarvortrag oder die Seminarleistung im Vordergrund, sondern mehr und mehr auch der Prozess des gemeinsamen Strukturierens eines Wissensgebiets.
Dies kann entsprechend den verschiedenen thematischen Ausrichtungen auf ganz unterschiedliche Art und Weise erfolgen. Zentral für das verfolgte Jour-Fixe-Konzept ist damit die semantische Strukturierung eines virtuellen Wissensraums in der Gruppe.

Semantische Strukturierung von Wissensräumen
Semantische/thematische Strukturierung bedeutet hierbei zusätzlich eine räumliche Strukturierung, d.h. der Raum oder die Fläche nimmt eine wichtige Funktion in der Strukturierung unterschiedlicher Elemente ein. So kann beispielsweise durch räumliche Nähe eine Beziehung zwischen verschiedenen Elementen ausgedrückt werden. Unterschiedliche Formen von Diagrammen (geometrische Achsen) können Angrenzungen eines Themengebietes verdeutlichen. Ergebnis ist eine grafische Orientierungskarte, welche zur Navigation in einem Themengebiet Verwendung finden kann.
Verschiedene Formen grafischer Strukturierungsweisen eines Wissensgebietes umfassen damit:
- Semantische Achsen und Dimensionen: Hierzu zählen zeitliche Abfolgen durch Darstellung eines Zeitstrahls genauso wie Auszeichnungen durch unterschiedliche Farbigkeit, Symbolik oder hierarchische Strukturen durch Eltern-Kinder-Beziehungen.
- Semantische Räume: Diese umfassen thematische Hintergrundbilder, Strukturierung durch semantische Anordnung von Elementen, ihre Gruppierung und Nähe oder Auszeichnungen und strukturelle Verweise. Häufigstes Element sind hier geometrische Distanzbeziehungen: räumliche Nähe drückt beispielsweise semantische Zusammengehörigkeit aus. Ein weiteres wichtiges Strukturierungselement kann hier schon die Beachtung der Leserichtung sein.

Idealerweise bedeutet Navigation hierbei auch eine Rückmeldung über die Position eines Nutzers auf der Karte bzw. entsprechende Information über seine Position innerhalb des Wissensgebietes.
Wir nennen das entstehende Konzept Semantische Karte (Hampel & Selke 1999).
Weiteres konzeptionelles Element des verfolgten Ansatzes ist die grafische Strukturierung eines Wissensbereiches als alternative Sicht auf den Wissensraum. Damit lassen sich über verschiedenste Werkzeuge (im Falle des genutzten sTeam-Systems über einen WWW-Browser, ein Shared Whiteboard und einen Java-Client) verschiedene Zugänge (synchron und asynchron) auf ein und denselben Wissensraum schaffen. Die Semantische Karte steht nicht unverbunden zu anderweitigen Werkzeugen, sie erlaubt es Materialien, Dokumente, grafische und diskursive Elemente (Annotationen) in synchronen als auch asynchronen Arbeitsweisen zu strukturieren.

Erfahrungen des Jour-Fix-Konzeptes
Im folgenden sei die Idee des Jour-Fix-Ansatzes an einem konkreten Beispiel aus der Vorlesung „Konzepte Digitaler Medien“ aus dem Sommersemester 2003 verdeutlicht. Die Vorlesung führt in unterschiedliche Kernkonzepte der Entwicklung digitaler Medien vom interaktiven System bis zum kooperativen Medium ein. Als Jour-Fix -Themen wurden entsprechend Themenbereiche wie Hypertext, interaktive Systeme, virtuelle Gemeinschaften, MUDs/MOOs-Chat etc. vergeben.
Das folgende Beispiel (vgl. Abbildung 1 und 2) zeigt den virtuellen Wissensraum der Gruppe „Location Awareness und Kontext Awareness“.
Die Gruppe bestand aus drei Studierenden, die sich mit unterschiedlichsten Aspekten der gegenseitigen Wahrnehmung (Awareness) beschäftigten. Maßgebliches Ziel hierbei ist ganz unterschiedliche Zugänge zum Thema Awareness zu schaffen und dabei unterschiedliche Bezüge zu den Themen der Vorlesung und den anderen Jour-Fix-Gruppen herzustellen. Verwendung findet hierbei das sTeam-Shared Whiteboard (vgl. www.open-steam.org.) welches es der Gruppe erlaubt in synchroner, als auch asynchroner Arbeitsweise, verschiedene grafische Elemente zu arrangieren, Verweise zu erzeugen, Materialien abzulegen etc. Durch Aktivieren eines Links werden Materialen in der Webschnittselle, im einfachsten Fall im Browser, angezeigt und können durch den so genannten sTeam-Application Launcher mit den üblichen Office-Anwendungen direkt bearbeitet werden.

Ergebnis der Wissensstrukturierungsprozesse der Gruppe „Awareness“ sind eine Reihe verknüpfter Wissensareale. Der Zugang beginnt mit einer ersten grafischen Differenzierung des Begriffs. Von hier aus gelangt man in einen weiteren Raum, der unterschiedliche semantische Karten zum Bereich der Awareness bereitstellt. Hier findet sich ein thematischer Zugang über einen Zeitstrahl und ein Begriffsnetzwerk, sowie die Darstellung der Materialien aus der Vorlesung. Ergänzend wurde ein Glossar beigefügt, welches in Form eines Diskussionsbrettes die wesentlichen Begrifflichkeiten erläutert. Hier können zu einer Begriffsdefinition alternative Formulierungen und Quellen gesammelt und in Bezug gesetzt werden, sowie Referenzen (Dokumente) der Ursprungsquellen hinzugefügt werden. Speziell die Möglichkeit, Definitio-

nen in Gruppen zu entwerfen und diese gegenseitig zu kommentieren und zu bewerten, stellen wichtige Mechanismen der Zusammenarbeit dar und sind damit integraler Bestandteil des Jour-Fixe-Konzepts.

Alle oben gezeigten Zugänge zum Thema Awareness wurden parallel zum Vorlesungszeitraum erstellt und in einer Reihe von Jour-Fixes den anderen Gruppen vorgestellt. Hierdurch ergab sich

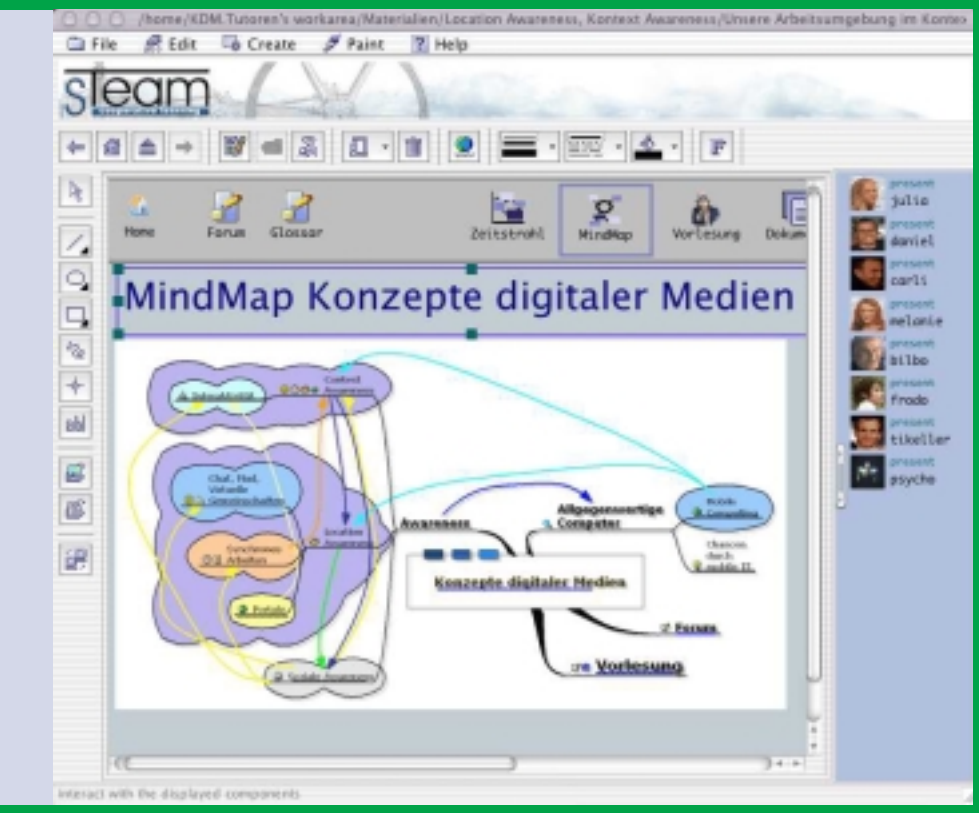


Abbildung 2: Als Teil des Jour-Fixes einer Gruppe von Studierenden erstellte Mind-Map zur Einordnung des Begriffes der Awareness in die Struktur der Vorlesung

eine gute Verknüpfung in der Zusammenarbeit der verschiedenen Gruppen und damit eine gewollte Verknüpfung der verschiedenen Themenbereiche. Das in Abbildung 2 gezeigte und ebenfalls von den Studierenden erstellte Begriffsnetzwerk (Mindmap) macht dies auf eindrucksvolle Weise deutlich. Die Präsentation eines Zwischenergebnisses im Jour-Fixe kann dabei auch den Charakter eines kurzen Vortrages besitzen, ist aber maßgeblich durch den Diskurs in der Gruppe geprägt. Derartige Diskussionen zu den Beziehungen und Verknüpfungen der Themen untereinander können zudem in verschiedenen, den jeweiligen Wissensräumen zugeordneten Diskussionsbereichen fortgeführt werden.
Einen wesentlichen Anteil der späteren notwendigen Prüfung nimmt die Vorstellung und Diskussion des Wissensraums ein. Am Beispiel zum Wissensraum „Awareness“ zeigt sich, dass als wesentlicher Maßstab der Bewertung der Grad der gelungenen Abgrenzung und Einordnung des Themengebietes in den Gesamtkontext der Vorlesung angesehen werden kann. Hier zeigt sich, wie in der als Beispiel herangezogenen Gruppe gelungen, dass ganz unterschiedliche Zugänge und Einordnungsmöglichkeiten zu dem jeweiligen Themengebiet existieren können und sollten und Lernenden entsprechend die Einführung in das Themengebiet durch eine Reihe von Semantischen Karten innerhalb des Wissensraums maßgeblich vereinfacht werden kann.
Als Ergebnis einer ersten formativen Evaluation (Befragung der Studierenden in kurzen informellen Gesprächen) lässt sich ein positives Resümee des gewählten Jour-Fixe-Konzepts ziehen. Das Veranstaltungskonzept wurde von den Studierenden insgesamt sehr positiv aufgenommen. Die themenbezogene Zusammenarbeit in kleineren Gruppen und die regelmäßige Vorstellung zu den Jour-Fixes wurde als angenehm und produktiv empfunden. Hierbei wurde insbesondere die Möglichkeit positiv hervorgehoben als Teil des Prüfungsgespräches die strukturierten Wissensräume in der Gruppe vorstellen zu können.

Verwandte Arbeiten

Die vorgestellten Arbeiten lassen sowohl enge Bezüge zu verschiedenen Ansätzen des E-Learning, speziell im Bereich des CSCL (vgl. beispielsweise Wessner et. al. 1998 und Schuckmann et. al. 1996) erkennen, beziehen sich aber insbesondere auf Forschungen der grafischen und semantischen Strukturierung von Wissensräumen (vgl. hierzu insbesondere die Arbeiten von Harrison & Dourish, 1996) In letzterem Bereich seien insbesondere innovative Werkzeuge der synchronen Zusammenarbeit, d.h. der Kopplung von Sichten auf grafische Materialien (Shared Whiteboards etc.) genannt. (Vgl. hierzu insbesondere die Arbeiten von Chabert et. al. 1998 und Roseman & Greenberg, 1996). Neu und in dieser Form in der Literatur nicht vorhanden ist die Zusammenführung aus Methoden der Dokumentenverwaltung, das heißt Bereichen des CSCW (vgl. Greif 1988) und semantisch-grafischen Strukturierungsformen der kooperativen Wissenskonstruktion.

Zusammenfassung

Zusammenfassend können unsere ersten Erfahrungen mit dem Jour-Fixe-Konzept in Verbindung mit der Nutzung des kooperationsunterstützenden Systems sTeam als sehr positiv bewertet werden. Sicherlich gilt es auch zukünftig, wie die tägliche Praxis zeigt, eine Vielzahl kleinerer technischer und konzeptueller Probleme zu überwinden. Diese bewegen sich auf technischer Seite beispielsweise in den Bereichen der Schaffung geeigneter technischer Infrastrukturen zur Nutzung der bereitgestellten Werkzeuge und der Integration dieser Werkzeuge in die gewohnte Arbeitsumgebung der Lernenden.
Auf konzeptioneller Seite gilt es zudem die Verbesserung der Orientierbarkeit und Navigierbarkeit innerhalb der Struktur verknüpfter Wissensräume voranzutreiben. – Hierbei handelt es sich um ein Thema, welches eng mit Fragestellungen der Entwicklung geeigneter Mechanismen der gegenseitigen Wahrnehmung (Awareness) verknüpft ist. Weiterhin sind die Gestaltungsmöglichkeiten Semantischer Karten, speziell in Formen der kooperativen Zusammenarbeit zu verbessern.
Auch die Nutzung von synchronen Werkzeugen auf unterschiedlichen Endgeräten, speziell unter den Anforderungen steigender Mobilitätsanforderungen gilt es zukünftig zu beachten. Die zur Umsetzung genutzte Open-Source sTeam-Plattform bietet hier sicherlich genügend Entwicklungs- und Gestaltungsoptionen.
In dem eingeschlagenen Weg der Verbindung von Entwicklung und Erforschung von Konzepten und Werkzeugen der kooperativen Wissensorganisation mit der Neugestaltung organisatorischer

Abläufe einer Lehrveranstaltung, welche in Teilbereichen bis zu der cirrucularen Einbettung reicht, lässt sich wie gezeigt eine neue Qualität der Lehre verwirklichen. Das Jour-Fixe-Konzept ist sicherlich ein guter Weg, um sowohl erprobte Wissensvermittlungsprozesse, wie die Vorlesung, mit freien offenen Ausbildungsformen des Explorierens und Erarbeitens von Wissensbereichen in Gruppen zu verknüpfen. Hierzu werden Werkzeuge und Umgebungen der kooperativen Wissensorganisation benötigt, die einen derartigen offenen Wissenskonstruktionsprozess, auch in Gruppen geeignet unterstützten.

Danksagung

Wir möchten an dieser Stelle allen danken, die an der Erprobungsphase unseres Jour-Fixe-Ansatzes beteiligt waren, insbesondere Daniel Büse, der viel Mühe in die Verbesserung unseres Shared Whiteboards investiert. Zudem sei allen Entwicklern des sTeam-Systems gedankt, speziell Thomas Bopp und Ludger Merkens.

References

Chabert, A., Grossman, E., Jackson, L.S., Pietrowiz, S.R., Seguin, C. (1998). Java object-sharing in Habanero. Communications of the ACM 41(6) 1998, 69–76.

Greif, I. (1988). Computer Supported Cooperative Work: A Book of Readings. San Mateo: Morgan Kaufmann Publishers, 1988.

Hampel, T. (2003). Our Experience With Web-Based Computer-Supported Cooperative Learning – Self-Administered Virtual Knowledge Spaces in Higher Education. In: Proc. of Site 2003 – Society for Information Technology and Teacher Education - International Conference. Charlottesville (Va.), USA: Association for the Advancement of Computing in Education, 1443-1450.

Hampel, T. (2002a). Virtuelle Wissensräume. – Ein Ansatz für die kooperative Wissensorganisation, University of Paderborn, Fachbereich 17 – Informatik, PHD-study.

Hampel, T. (2002b). sTeam- Providing Primary Media Functions for Web-Based Computer-Supported Cooperative Learning. Proceedings of ED-MEDIA 2002. Charlottesville (Va.), USA: Association for the Advancement of Computing in Education, 692–697.

Hampel, T. & Keil-Slawik, R. (2002). sTeam: Structuring Information in a Team - Distributed Knowledge Management in Cooperative Learning Environments. ACM Journal of Educational Resources in Computing 1(2).

Hampel, T. (2001). TRES FACIUNT COLLEGIUM – Paderborn's Collaboration Centred Approach for New Forms of Learning. In: Price, J., Willis, D., Davis, N., Willis, J. (Hrsg.): Proceedings of SITE 2001, Charlottesville (Va.), USA: Association for the Advancement of Computing in Education March 5-10, 2001, Orlando, Florida, USA, 52–57.

Hampel, T. & Selke, H. (1999). Customizing the Web – Two Tools for individual and collaborative use of hypermedia course material. In: Collis, B., Oliver, R. (eds): Proceedings of ED-MEDIA 99. Charlottesville: Association for the Advancement of Computing in Education, 634–639.

Harrison, S., Dourish, P. (1996). Re-Placeing Space: The Roles of Place and Space in Collaborative Systems. In: Ackerman, M.S. (Hrsg.): Proceedings of the ACM 1996 Conference on Computer Supported Cooperative Work (CSCW'96), November 16-20, Boston, USA. New York: ACM Press 1996, 67–76.

Keil-Slawik, R. (1999). Evaluation als evolutionäre Systemgestaltung. Aufbau und Weiterentwicklung der Paderborner DISCO (Digitale Infrastruktur für computerunterstütztes kooperatives Lernen). In: Kindt, Michael (Hrsg.): Projektevaluation in der Lehre – Multimedia an Hochschulen zeigt Profil(e). Reihe: Medien in der Wissenschaft, Bd. 7. Münster: Waxmann 1999, 11–36.

Nelson, T.H. (1989). Replacing the Printed Word: A Complete Literary System. In: Lavington, S.H. (Hrsg.): Information Processing 80. Amsterdam: Publishing Company, 1980, 1013–1023.

Roseman, M. and Greenberg, S. (1996). Building Real Time Groupware with GroupKit, A Groupware Toolkit. ACM Transactions on Computer Human Interaction 3(1) 1996, 66–106.

Schuckmann, C., Kirchner, L., Schümmer, J., Haake, J.M. (1996). Designing Object-Oriented synchronous groupware with COAST. In: Ackerman, M.S. (Hrsg.): Proceedings of the ACM 1996 Conference on Computer Supported Cooperative Work (CSCW'96), November 16-20, Boston, USA. New York: ACM Press 1996, 30–38.

Wessner, M., Beck-Wilson, J., Pfister, H.R.. (1998). Clear - A Cooperative Distributed Learning Environment. In: Ottmann, T., Tomek, I.: Proceedings of ED-MEDIA / ED-TELECOM 98. Freiburg, Germany, Charlottesville: Association for the Advancement of Computing in Education 1998 (Vol.II), 1876–1877.

Pro Print

Print-On-Demand für die Wissenschaft

Seit mehr als fünf Jahren werden in Deutschland an fast jedem Universitätsstandort Dokumentenserver zur Verbreitung und Aufbewahrung digitaler wissenschaftlicher Literatur aufgebaut. Es wurden und werden Promotionsordnungen an Universitäten geändert, um die kostengünstige Veröffentlichung von Dissertationen in digitaler Form zu ermöglichen. Ebenso werden historische Quellen digitalisiert, um diese über das Internet zugänglich zu machen. Daneben werden elektronische Zeitschriften aufgebaut, die langfristig den Weg aus der so genannten Zeitschriftenkrise weisen sollen. Ziel all dieser Projekte ist es, Informationen kostengünstig und weltweit verfügbar zu machen.

Matthias Schulz

Computer- und Medienservice
Humboldt-Universität zu Berlin
Unter den Linden 6
10099 Berlin

E-Mail: info@proprint-service.de
ProPrint-Service:
http://www.proprint-service.de

Aus Nutzersicht besteht der Bedarf an einer integrierten Rechercheoberfläche, mit der die einzelnen Dokumentenserver komfortabel durchsucht werden können, ohne sie manuell ansteuern zu müssen. Eine Vernetzung der Dokumentenserver ist dafür die Voraussetzung.
Dokumentenserver als elektronische Langzeitarchive werden gedruckte Informationen nicht entbehrlich machen - im Gegenteil: Der Wunsch nach dem gedruckten Dokument wächst bei den Nutzern solcher Informationssysteme. Dieses Bedürfnis bezieht sich in vielen Fällen jedoch nicht auf das gesamte Dokument, sondern lediglich auf Ausschnitte, einzelne Aufsätze, Kapitel, Zitate o.ä. Ziel von ProPrint ist es, ein verteiltes Drucksystem zu schaffen, damit nur der Teil ausgedruckt wird, den der Nutzer tatsächlich benötigt.
Mit dem Ziel, Wissenschaftler effektiv mit Informationen zu versorgen, entwickelte der Computer- und Medienservice der Humboldt-Universität zu Berlin und der Staats- und Universitätsbibliothek Göttingen (SUB) im Rahmen des DFN-Programms „Einsatz von Netzdiensten im Wissenschaftlichen Informationswesen“, gefördert mit Mitteln des BMBF, den Dienst ProPrint.

Was ist ProPrint?

- Mit ProPrint können Dokumentenserver virtuell zusammengeschlossen werden. Das heißt, der Bestand dieser Server kann mit einer einzigen Suchmaske durchsucht werden.
- ProPrint erweitert das Dienstleistungsangebot jedes angeschlossenen Dokumentenservers um eine Print-On-Demand-Komponente.
- ProPrint bietet einen Workflow, der Bibliotheken beim elektronischen Publizieren unterstützt. Mit ProPrint kann die technische Qualität der elektronischen Dokumente gesteigert werden. Dies dient vor allem dazu, die Voraussetzungen für die Langzeitverfügbarkeit der elektronischen Dokumente auf zertifizierten Dokumentenservern zu schaffen und zu verbessern.

ProPrint stellt eine Software bereit, mit der ein Print-On-Demand-Dienst in einer Bibliothek oder wissenschaftlichen Einrichtung installiert werden kann.
Von Ende 2000 bis Mitte 2003 arbeiteten Entwickler des Computer- und Medienservice der Humboldt-Universität zu Berlin und der Staats- und Universitätsbibliothek Göttingen (SUB) am Aufbau des ProPrint-Dienstes. Ein LAMP-System bot dabei die softwaretechnische Grundlage. Dieses System setzt sich aus folgenden Komponenten zusammen: Linux als Betriebssystem, dem Apache-Webserver, einer MySQL-Datenbank und PHP als Programmiersprache. Mit dieser Entscheidung wurde insbesondere die Nachnutzung des Systems in den Blick genommen, da alle verwendeten Softwarekomponenten frei zur Verfügung stehen. Darüber hinaus stand die konsequente

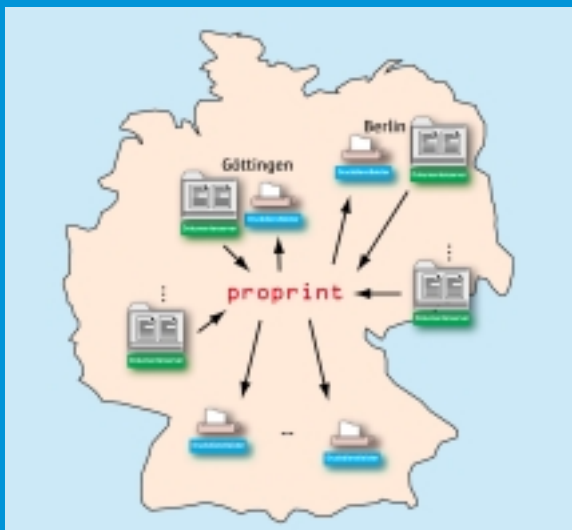


Abbildung 1: Schema des ProPrint-Service

Verwendung von Standards sowohl für die Kommunikation zwischen den Dokumentenservern als auch für Dokumentformate und Metadaten im Mittelpunkt der Projektarbeit.
Um Nutzern Recherchemöglichkeiten über Dokumentenservergrenzen hinaus anzubieten, können verschiedene Techniken zum Einsatz kommen. Genannt seien die verteilte Suche und das Harvesting. Beim ProPrint-System wird das Harvesting von Metadaten mit dem Open Archives Protocol for Metadata Harvesting (OAI-PMH) verwendet.
Das OAI-Protokoll ermöglicht einen effizienten Austausch von Metadaten und impliziert eine funktionale Aufteilung in Anbieter von (Dokumenten und) Metadaten, so genannte Dataprovider , und darauf aufbauende Dienste (Serviceprovider). Das OAI-PMH basiert auf dem grundsätzlichen Prinzip des so genannten Harvesting , bei dem im Gegensatz zum Ansatz des Cross Searching eine asynchrone Suche durchgeführt wird. Das heißt, der Serviceprovider fragt in regelmäßigen Abständen die Metadaten der Dataprovider ab und speichert diese in seiner lokalen Datenbank. Konkrete Suchanfragen (z.B. von Endnutzern) werden im Falle des Harvesting-Ansatzes ausschließlich mit Hilfe der Datenbank beantwortet.

Das OAI-Protokoll basiert auf weithin bekannten und verbreiteten Standards. Es setzt auf das Hypertext Transfer Protocol (HTTP) auf und verwendet zur Kodierung der Metadaten und der sonstigen in den Antworten enthaltenen Informationen die eXtensible Markup Language (XML). Wiewohl sich das OAI-Protokoll zur Übertragung von Metadaten in beliebigen (durch ein XML-Schema definierten) Formaten eignet, ist Dublin Core aus Gründen der Interoperabilität als Minimalstandard in das OAI-PMH aufgenommen worden. OAI-kompatible Datenprovider müssen in der Lage sein, für ihre Metadaten zumindest Dublin Core auszuliefern. Damit sind die Kommunikation und der tatsächliche Austausch von Metadaten zwischen beliebigen OAI-kompatiblen Daten- und Serviceprovidern ohne weitere zusätzliche Vereinbarungen sofort möglich. Die zentrale ProPrint-Suchmaschine ist im Sinne von OAI der Serviceprovider, und die einzelnen Dokumentenserver sind Datenprovider.

Voraussetzung für die OAI-Kompatibilität eines Dokumentenservers ist dessen Fähigkeit, Dublin Core als Metadatenformat auszuliefern. Für die Beschreibung weiterer Metadaten, die für den ProPrint-Dienst erforderlich sind, wurden innerhalb dieses Metadatenformates weitere Elemente mit einem gesonderten Namensraum definiert. Dieser Namensraum enthält auch Elemente des DIEPER-Metadatensatzes. Die ProPrint-Erweiterung des Metadatenformates, der ProPrint-Metadatensatz, umfasst Informationen für besondere Seitenformate, Vertriebsinformationen und Teile eines Dokumentes (Kapitel, Unterkapitel). Die Entwicklung der Elemente für die Beschreibung von Teilstrukturen konnte nicht von physisch vorliegenden Papierseiten einer gedruckten Publikation ausgehen, wie dies das Metadatenformat des Göttinger Digitalisierungszentrums (GDZ) für Digitalisate vorsah. Da bei den digitalen Dokumenten der Dokumentenserver der Humboldt-Universität und der SUB-Göttingen keine physischen Papierseiten vorlagen, wurde das Metadatenformat für Teilstrukturen auf logischen Einheiten (Kapitel, Unterkapitel ...) aufgebaut.

Über die zentrale ProPrint-Suchmaschine haben die Forschenden und Studierenden so einen unbegrenzten Zugang zu elektronischen Dokumenten. Aber nicht nur über den zentralen Zugang kann der ProPrint-Dienst genutzt werden, sondern jeder angeschlossene Dokumentenserver kann einen ProPrint-Button auf seinen Internetseiten anbringen. Damit erweitert sich das Dienstleistungsangebot der Bibliothek um einen Print-On-Demand-Dienst. Nur das Anbringen eines speziellen Links ist dafür notwendig, was ohne zusätzliche Programmierung realisierbar ist.

Zum Stand des elektronischen Publizierens

In Zusammenarbeit mit der DINI-Arbeitsgruppe „Elektronisches Publizieren“ wurde eine Befragung zum Stand des elektronischen Publizierens in Deutschland durchgeführt. Ergebnis dieser Befragung war, dass eine Vielzahl von Bibliotheken sich dem Thema des elektronischen Publizierens widmet, allerdings in sehr unterschiedlicher Art und Weise. In den meisten Fällen werden die elektronischen Dokumente in Datenbanken oder dem OPAC erschlossen und gespeichert. Das bevorzugte Dokumentformat für Textdokumente ist PDF. Dass die Dokumente nach festgelegten Richtlinien der Betreiber der Dokumentenserver aufgenommen werden, konnten nur 40% der Befragten bejahen. Die Erschließung mit Metadaten, die Aufschluss über den bibliographischen, administrativen und technischen Status geben, wird nur in 23% der Fälle vorgenommen.

Resultat der Befragung war, dass gemeinsam mit der DINI-Arbeitsgruppe die Ergebnisse dazu genutzt wurden, Kriterien für ein DINI-Zertifikat für Dokumenten- und Publikationsserver zu diskutieren und festzulegen. Die Erteilung des Zertifikates umfasst unter anderem eine Prüfung der Servertechnik und eine Qualitätsprüfung der elektronischen Dokumente. Dabei wird besonders Wert auf die Erstellung, Erschließung und Archivierung der elektronischen Dokumente gelegt.

Standardisierung der Anforderungen an das Format der Dokumente

Der Dokumentenaustausch zwischen Dokumentenservern kann nur gewährleistet werden, wenn Übereinkünfte zu Formaten und deren technischer Qualität bestehen. ProPrint setzt das PDF-Format von Adobe als Austauschformat ein. Jedoch kann die technische Qualität dieses Formates unterschiedlich sein. Bei der Erstellung dieses Formates können Fehler unterlaufen, die die weitere Verwendung des Dokumentes ausschließen. Außerdem ergeben sich durch Versionswechsel Kompatibilitätsprobleme.

Welche Fehler auftreten können und welche Aspekte unbedingt für einen standardisierten Austausch erfüllt sein müssen, wurde in einer umfangreichen PDF-Testreihe ermittelt. An diesem Test beteiligten sich die Dokumentenserver von OPUS - Stuttgart und das Universitätsrechenzentrum der TU Chemnitz.

Betrachtet wurden

- die Einbettung von Schriften,
- die PDF-Versionen, die jeweiligen PDF-Erstellungstools und
- etwaige Sicherheitseinstellungen.

Zum Abschluss wurde eine Auswahl von Dokumenten zum konkreten Druck an einen Druckdienstleister gegeben und auf fehlerhafte Darstellungen überprüft. Die durch den Test ermittelten Fehler führten zu den Empfehlungen der DINI-Arbeitsgruppe „Elektronisches Publizieren“ zum Thema Print-on-Demand, die folgende Checkliste für elektronische Dokumente enthält:

- **Einbetten von Schriften und Vorkontrolle der Dokumente:** Wenn PDF als Archivierungsformat verwendet werden soll, sind grundsätzlich alle verwendeten Schriften während der Umwandlung in das PDF-Format über den Distiller oder andere Software-Tools einzubetten. Dies erhöht zwar die Dateigröße und ist wegen der längeren Ladezeit weniger für die Webbetrachtung geeignet, aber zur Archivierung von wissenschaftlichen Publikationen sollte auf jeden Fall gewährleistet werden, dass die PDF-Dateien auf jeder Plattform gelesen werden können, zumal ohne eingebettete Schriften das Dokument keine feste optische Erscheinung hat und somit nicht plattformunabhängig nutzbar ist.

Ein zwingend notwendiger Schritt vor dem Einstellen der Dokumente auf dem Server ist eine vorangegangene gründliche Kontrolle durch den Betreiber des Dokumentenservers oder eine andere Institution.

- **Keine Sicherheitseinstellungen bei PDF-Dokumenten:** Um die Archivierung von Dokumenten im PDF-Format zu ermöglichen, sollten Sicherheitseinstellungen und Benutzungsbeschränkung grundsätzlich ausgeschlossen werden. Nutzungseinschränkungen können in jedem Fall umgangen werden, indem die PDF-Datei über Ghostscript in eine Postscript-Datei gewandelt und daraus anschließend durch den Acrobat Distiller

oder ein anderes Tool ein neues PDF-Dokument generiert wird („redestillieren"). Die Nutzungsbeschränkungen sind deshalb weitestgehend nutzlos und behindern den sinnvollen Einsatz zusätzlicher elektronischer Dienstleistungen. Die Sicherheitseinstellungen sind für Dokumente, die durch ProPrint nutzbar sein sollen, grundsätzlich auszuschließen.

• **Kontrolle der Farbigkeit von Texten:** Es sollte aus der Sicht der zukünftigen Leser bei der Abgabe der Dokumente darauf geachtet werden, dass keine Schrift unnötigerweise in Farbe erscheint. Automatische Funktionen in MS Word formatieren z. B. eine URL blau. Diese Funktionalitäten sind auszuschalten. Die Autoren sind darauf aufmerksam zu machen und sollten aufgefordert werden, ein neues PDF-Dokument zu liefern, denn jede dieser Seiten würde als Farbseite erkannt und als solche bei dem Druckdienstleister beauftragt. Dies würde den Preis der Seite um ein Vielfaches erhöhen, ohne dass ein ersichtlicher Nutzen entstehen würde.

• **Format bei Print-on-Demand:** Den meisten Dokumenten ist gemein, dass die Schriftgröße jeweils so gering ist, dass ein Ausdruck im DIN A5-Format nicht sinnvoll erscheint. Der Text wäre nicht mehr angenehm leserlich. Darum sollte für den Ausdruck grundsätzlich das DIN A4-Format vorgesehen werden. Sollte der Ausdruck in DIN A5 gewünscht sein, ist die Schriftgröße beim Seitenlayout entsprechend zu berücksichtigen.

Die Entwicklung und Einrichtung des ProPrint-Service

Der ProPrint-Webservice wurde in einfach zu erfassenden Webseiten gestaltet, die komplett dynamisch erstellt werden. Bei der Implementierung wurden folgende Vorgaben umgesetzt:

• **Metadaten:** Bildung eines zentralen, für alle Dokumentenserver einheitlichen Metadatensatzes, der darüber hinaus für viele noch in Zukunft denkbare Dokumenttypen und Objekte vorbereitet ist, wie beispielsweise geographische Karten. Dafür wurde in Anlehnung an Dublin Core (DC) ein ergänzender ProPrint-Namespace und ein ProPrint-Application Profile gebildet. Die Metadaten müssen dazu vom ProPrint-Webservice regelmäßig und automatisch mit den Dokumentenservern abgeglichen werden.

• **Dokumente:** Dieser Bereich kann in zwei Gruppen eingeteilt werden: die Gruppe der Dokumente, die von den Betreibern der Dokumentenserver verwaltet werden und die Gruppe von Dokumenten, die auf dem ProPrint-Server für die Druckdienstleister als druckreife Vorlagen vorbereitet werden. Das ProPrint-System muss hierbei (mittels sog. „mergen", also einem Verbinden der zugrunde liegenden Originaldateien), letztgenannte Dokumente aus den erstgenannten erzeugen können.
Rechteverwaltung: Anwender, Administratoren und Druckdienstleister werden nach ihrem Nutzungsprofil unterschieden und haben unterschiedliche Zugriffsrechte auf Bereiche und Inhalte des ProPrint-Dienstes. Diese Rechte werden durch Nutzer mit entsprechenden Vergaberechten zugewiesen (Rechte-Administratoren).

• **Druck und Vertrieb:** Die dezentralen Druckdienstleister vertreiben die Dokumente in gedruckter und gebundener Form an den ProPrint-Nutzer. Ergänzt wird der direkte Weg über den Versand bei gleichzeitiger Rechnungsstellung durch die SUB-Göttingen. Hierfür steht ein Workflow zur Verfügung, in dem die Druckdienstleister und die Rechnungsstelle der SUB-Göttingen eingebunden sind.

• **Rechnungsverfahren:** Alle für die Rechnungsstellung relevanten Daten werden im ProPrint-System zentral erfasst und gespeichert. Die Dokumente werden auf ihre Seitenzahl und ihre Farbigkeit ausgelesen. Dementsprechend wird der Preis pro Seite mittels eines Preisschemas für s/w- und farbige Seiten ermittelt. Das ProPrint-System generiert eine Rechnungsvorlage, die druckbar ist und bereits alle Preise sowie eine eindeutige Rechnungsnummer enthält, welche aus einem vom SAP-Rechnungswesen reservierten Kontingent stammt.
Die Administration des ProPrint-Webservice erfolgt über die direkte Arbeit auf dem Server und über eine Internetschnittstelle. Folgende Funktionen sind durch diese Schnittstelle administrierbar:

- Test/Sprache (u.a. werden die Hilfetexte der ProPrint-Webservice Seiten hier verwaltet),
- Nutzerverwaltung,
- OAI-Server (Einbindung von OAI-Servern in den ProPrint-Webservice),
- Zeitplan/Tasks,
- Druckdienste (Einbindung von Druckdienstleistern),
- Rechnungsnummern (Verwaltung der Rechnungsnummer der einzelnen Transaktionen).

Was bietet ProPrint in der Zukunft?

Heute sind über 4000 verschiedene Dokumente aus dem Bestand der Dokumentenserver der Humboldt-Universität zu Berlin und der Staats- und Universitätsbibliothek Göttingen mit ProPrint verfügbar. Darunter befinden sich Monographien, Zeitschriften, digitalisierte Dokumente aus historischen Beständen, Habilitationen, Dissertationen und Konferenzbeiträge von drei nationalen und internationalen Konferenzen. ProPrint steht für ein offenes System. Das heißt, dass jeder Betreiber eines Dokumentenservers diesen Dienst nutzen kann. ProPrint beschränkt sich dabei nicht nur auf öffentliche Einrichtungen, sondern richtet sich auch an kommerzielle Content-Provider.
Mit der evaluierten ProPrint-Software werden im nächsten Jahr weitere Dokumentenserver und Dokumentenarchive an das ProPrint-System angeschlossen.

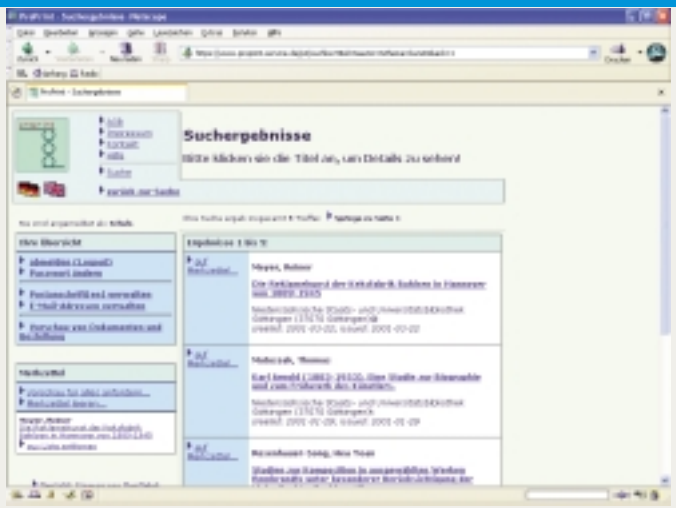


Abbildung 2: Suchmaske des ProPrint

SINN

Wissenschaftliche Information, frei, offen und redundant verteilt

Der DFN e.V. hat von Februar 2001 bis Oktober 2003 das Projekt 'SINN: Suchmaschinennetzwerk im Internationalen Naturwissenschaftlichen Netz' [1] gefördert. Ziel dieses Projektes war es, ein international verteiltes Netz von interagierenden Portalen aufzubauen. Am Beispiel des Physik-Portals PhysNet [2] wurden hier Techniken und Methoden entwickelt und erprobt, wie man nachhaltig Netzwerke von Fachportal-Servern im internationalen Kontext aufbauen und betreiben kann. Ein spezieller Schwerpunkt lag dabei auf der Entwicklung eines Suchmaschinen-Systems, das die verteilte Architektur der Portal-Server nutzt, bzw. in diese eingebettet ist, und auf offenen Standards basiert.

Von der Link-Liste zum internationalen Fachportal

Bereits ab 1993, in den Kinderjahren des WWW, begannen Wissenschaftler an zahlreichen Physik-Instituten, eigene Web-Server zu installieren und Link-Listen der Server anderer Institutionen zusammenzustellen. Mit dem rasanten Wachstum des WWW wurde es jedoch schnell klar, dass es keiner Institution alleine möglich sein würde, vollständige Link-Listen zu erstellen und laufend zu aktualisieren. 1996 initiierte dann die European Physical Society EPS [3] eine erste Bündelung dieser verteilten Informationsquellen und der verteilten Arbeitskraft zur Pflege der Link-Listen in ein Portal der ersten Generation. Zunächst europaweit wurden jene Wissenschaftler zusammengebracht, die im Auftrage ihrer nationalen Physik-Fachgesellschaften solche Listen erstellten und pflegten. Deren zwar räumlich begrenzten aber aktuellen und laufend gepflegten Link-Listen wurden automatisiert in ein gemeinsames Portal eingespielt, welches so ohne zusätzlichen administrativen Aufwand von den Beteiligten gefüllt wurde. Auf diese Weise entstand des Kern des heutigen PhysNet.

Um die globale Ausdehnung dieses Systems zu ermöglichen und voranzutreiben, mussten gemeinsame Qualitätskriterien definiert werden. Diese wurden im August 2000 in einer Charter [4] festgehalten und von allen am Portal beteiligten Institutionen verabschiedet. Auf diesem organisatorischen und inhaltlichen Fundament konnte dann im Februar 2001 das Projekt SINN aufsetzen.

Verteilte Inhalte, verbesserte Akzeptanz

Die Erfahrungen beim Betrieb des PhysNet-Dienstes haben gezeigt, dass ein entscheidendes Kriterium für die Akzeptanz des Dienstes ist, die angebotenen Inhalte nicht an einem Orte zentral zu sammeln und vorzuhalten. Je dezentraler die Struktur ist, desto größer ist die Akzeptanz des Dienstes, sowohl bei den Nutzern als auch bei den Betreibern. Ziel des SINN-Projektes war daher auch, das in PhysNet vorhandene Netzwerk von Personen und Institutionen zu nutzen und den Ausbau des Dienstes zu einem wirklich verteilten internationalen Fachportal konsequent fortzusetzen.

Der Aufbau dieses Portal-Netzwerkes erfolgte schrittweise. In einem ersten Schritt wurden die Web-Seiten des Dienstes an verschiedenen Standorten gespiegelt. Dazu musste ein inkrementelles Verfahren so implementiert werden, dass es möglichst einfach und vor allem selbsterklärend unter möglichst jedem Unix/Linux-System installier- und automatisierbar ist. Akzeptanz findet ein solches Verfahren nur, wenn es vollkommen transparent ist und auch den technisch meist unerfahrenen Entscheidungsträgern an den Spiegelstandorten leicht erklärbar ist. Pakete wie 'wget' schieden von vornherein als zu komplex für diese Aufgabe aus. Der Durchbruch in diesem Projektteil wurde erreicht, als alle Kommunikation des 'Mirrorings' auf das in jedem Browser implementierte und jedem Beteiligten aus der alltäglichen Arbeit vertraute HTTP umgestellt wurde.

Michael Hohlfeld **Thomas Severins**

Kontakt: Michael Hohlfeld
Institute for Science Networking Oldenburg GmbH
an der Carl von Ossietzky Universität Oldenburg
Email: michael.hohlfeld@isn-oldenburg.de

Seit 2002 spiegelt nun ein Perlskript [5], das weniger als 100 Zeilen Programmcode enthält und sich vollkommen selbsterklärend installiert, alle Web-Seiten des PhysNet-Dienstes.

Weltweit gibt es derzeit 15 solcher Spiegel. Der jeweils erste laufende Spiegel-Server eines Landes bekommt dabei die Möglichkeit, die Domain cc.physnet.net, mit "cc" dem Country-Code, zu verwenden. Diese Domains lassen sich einerseits leicht merken und tragen andererseits zu einem einheitlichen Erscheinungsbild des Portal-Netzwerkes und damit auch zu einer Erhöhung der Nutzerakzeptanz bei, wie sich aus der Zeitreihenanalyse der Spiegelnutzungen ablesen lässt. Knapp 30 Prozent der Nutzung sind derzeit auf die Spiegel-Server verteilt [6].

Die Analyse des Nutzerverhaltens, mit der die Akzeptanz des Dienstes erfasst werden sollte, um sie zielgerichtet optimieren zu können, war ein wesentlicher Aufgabenbereich des Vorhabens. Bei der Erfassung der dafür nötigen Daten hat es sich als nicht machbar erwiesen, Log-Files oder deren Auswertungen zwischen den vielen Beteiligten in solch einem Netzwerk auszutauschen. Noch so enge Vereinbarungen zwischen sonst zuverlässigen Partnern erlauben es nicht, derartige Informationen langfristig stabil und lückenlos auszutauschen. Als sinnvoller, gangbarer Weg hat sich das im kommer-

ziellen Web verbreitete Verfahren, des Einbindens von "blinden" Bildern in die Web-Seiten herausgestellt. Verknüpft man diese zum Beispiel mit Hilfe von Apache Server-Side-Includes noch mit Informationen über den Domainnamen des Spiegel-Servers, dann hat man an einem Master-Server alle gewünschten Informationen in dessen Log-Files verfügbar. Die Funktion dieses Master-Servers kann im Prinzip jeder der beteiligten Spiegel-Server jederzeit übernehmen.

Gemeinsame Pflege, gespiegelte Web-Seiten, verteilte Suchmaschine

Nachdem also die Pflege der Web-Seiten unter den Mitgliedern des PhysNet organisiert, die verteilten Inhalte zu einem Portal unter einem einheitlichen, nutzerfreundlichen Layout versammelt und dieses dann global verteilt gespiegelt wurde, war der nächste Schritt, ein Netzwerk von Suchmaschinen in diesem System zu implementieren, um die Inhalte nicht nur surfbar, sondern auch verteilt suchbar zu erschließen und vorzuhalten.

Bereits 1996 wurde im PhysNet eine Suchmaschine installiert, die auf der Harvest-Software [7] beruht. Die Wahl einer geeigneten Software fiel seinerzeit auf dieses Open-Source-Produkt, weil es einerseits gut mit sehr heterogenen Inhalten zurecht kommt, andererseits eine strikte Trennung zwischen dem Einsammeln der Inhalte in eine Datenbank (Gatherer) und dem Nachweis der Inhalte, also der Datenbank-Nutzer-Schnittstelle (Broker) vorsieht. Außerdem erlaubt es diese Software, Netzwerke von Suchmaschinen aufzubauen und war daher auch als Basis für das SINN-Vorhaben geeignet.

Harvest ist eine Suchmaschine, keine Meta-Suchmaschine. Es ist also nicht möglich, die Anfragen der Nutzer zu splitten, auf verschiedene Systeme zu verteilen um anschließend die Antworten wieder für den Nutzer sinnvoll zusammenzuführen. Will man dieses erreichen - und dies ist ja Ziel des SINN-Projektes -, so ist zunächst eine logische Ebene oberhalb der bisherigen Nutzerschnittstellen zu installieren. Diese weitere logische Ebene sollte dann auch die Möglichkeit bieten, Statusinformationen zu transportieren, um sicherzustellen, dass Anfragen nur an Teilnehmer des Netzes gerootet werden, die auch zügig antworten können.

Als Sprache innerhalb eines solchen Netzwerkes bietet sich das vom W3C noch nicht endgültig standardisierte XML-Query [8] an. Im Rahmen des Projektes SINN wurde die W3C-Mitgliedschaft des DFN Vereins genutzt, um aktiv in der entsprechenden Arbeitsgruppe daran mitzuarbeiten, dass diese Sprache nicht nur für die Kommunikation zwischen hochstrukturierten XML-Datenbanken, sondern auch zur Kommunikation zwischen heterogeneren WWW-Suchmaschinen nutzbar ist.

Zwar ist XML-Query noch nicht endgültig verabschiedet, für das PhysNet gibt es jedoch schon eine Middleware, DXQ [9], welche die Kommunikation innerhalb eines Suchmaschinen-Netzwerkes basierend auf der Harvest-Software erlaubt (siehe Abb. 1).

Dieses Netzwerk kann um jede Suchmaschine und Datenbank erweitert werden, sofern diese XML-Query nativ unterstützen, was leider noch bei keiner Datenbank der Fall ist. Es gibt lediglich Prototypen, die beweisen, dass dies prinzipiell möglich ist, sobald XML-Query standardisiert ist.

Für die Nutzer des PhysNet-Dienstes ist dann von diesem Suchmaschinen-Netzwerk und seiner wesentlich intelligenteren Struktur natürlich nur das Nutzerinterface zu sehen. Aber auch jetzt profitiert der Nutzer bei der automatischen Weiterleitung auf den für ihn am schnellsten erreichbaren und antwortenden Spiegel-Server von einem Teil der schon implementierten Software, die später auch bei der Verteilung der Suchanfragen an die verteilten Broker Anwendung findet.

Schlussbemerkung

Beim Betrieb eines verteilten Informationsdienstes wie dem PhysNet ist neben dem Einsatz geeigneter Techniken und Standards und der genauen Analyse des Nutzerverhaltens die Organisation der verteilten Arbeitskraft eine der wesentlichen Aufgaben.
Das Projekt SINN hat gezeigt, dass eine konsequente Einbindung aller Beteiligten in solchen globalen Projekten zum Erfolg führt.

Referenzen/Links:

[1] SINN-Projekt: www.isn-oldenburg.de/projects/SINN/
[2] PhysNet: www.physnet.net
[3] Eiropean Physical Society EPS: www.eps.org
[4] PhysNet-Charter: de.physnet.net/PhysNet/charter.html
[5] Physnet-Mirror-Script: de.physnet.net/PhysNet/bin/newbuild.pl

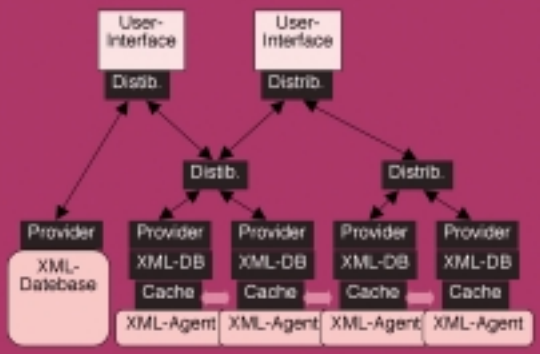


Abbildung 1: Die in SINN entwickelte Middleware ermöglicht den Aufbau kaskadierender Netzwerke von Datenquellen (Provider), intelligenten Knoten (Distributor) und Nutzerschnittstellen. Eine Anfrage wird über das User-Interface in XML übersetzt, durch die Distributoren an alle verfügbaren, aktiven Provider weitergeleitet und von diesen beantwortet.
Die Antworten werden von den Distributoren zusammengefasst, wozu ein Rankingalgorithmus über das Nutzer-Interface vorgegeben werden kann. Die Provider können untereinander Informationen austauschen. Anfragen, Antworten und Rankingalgorithmen sind im Netz in XML-Query kodiert.

[6] PhysNet-Spiegel-Nutzung: de.physnet.net/PhysNet/mirrorstat.html
[7] Harvest-Software: harvest.sourceforge.net
[8] W3C XML-Query Working Group: http://www.w3.org/XML/Query
[9] Christian Thiemann, Michael Schlenker, Thomas Severiens: Proposed Specification of a Distributed XML-Query Network, 13. Sep. 2003, www.isn-oldenburg.de/projects/SINN/DXQ-Spec.html
arxiv.org/abs/cs.DC/0309022

Das IRT-Objekt in der RIPE-Datenbank

Ein neuer Service für GWiN-Anwender

Marco Thorbrügge
DFN-CERT GmbH
Heidenkampsweg 41
D-20097 Hamburg/Germany
thorbruegge@cert.dfn.de
http://www.dfn-cert.de

Bei Sicherheitsvorfällen ist es für ein CERT wichtig, schnell den richtigen Ansprechpartner für eine bestimmte IP-Adresse oder einen Adressraum zu ermitteln, um ihm beispielsweise mitzuteilen, dass bei ihm eingebrochen wurde oder von einem seiner Systeme ein Angriff ausgeht. In den allermeisten Fällen bedeutet dies, eine WHOIS-Abfrage in der Datenbank eines der regionalen Internet Registrierungsdiensten zu starten. Das Problem: immer wieder stoßen CERTs auf veraltete Einträge, nicht mehr gültige Mailadressen oder Telefonnummern. Die Folge: die Vorfallsbearbeitung verzögert sich, wertvolle Minuten oder gar Stunden werden mit der Recherche im Web oder per Telefon vergeudet. Eine etwaige „heiße Spur“ ist bis dann längst erkaltet.

Die Einführung des IRT-Objekts in der RIPE-Datenbank

Um dieses Manko, welches vor allem bei nationenübergreifenden Vorfällen ins Gewicht fällt, zumindest für den europäischen Bereich zu beseitigen, wurde in Terenas Task force for Computer Incident Response Teams (TF-CSIRT) eine Erweiterung des RIPE-Datenbankstandards entwickelt. Die RIPE-Datenbank bietet das Backend für das WHOIS-Tool und liefert zu einer IP-Adresse Informationen über den Inhaber. Sie wird von RIPE betrieben, dem Internet-Registrar, der für die Vergabe von IP-Adressen im europäischen Raum verantwortlich ist. Die Idee war, die Datenbank dahingehend zu erweitern, dass zu einer IP-Adresse neben den Informationen über den Eigner auch Kontaktinformationen über das zuständige Notfallteam abfragbar sind. Ist es schon nicht möglich, korrekte Daten über den Eigner zu bekommen, so können Informationen zumindest schnell an das richtige CERT geschickt werden.

Eine handvoll europäischer Notfallteams, unter ihnen das DFN-CERT, verwirklichte diese Idee in Zusammenarbeit mit RIPE. Inzwischen existiert diese Zusatzinformation in der RIPE Datenbank in Form des sogenannten IRT-Objektes, welches Kontakinformationen von CERTs beherbergt. Neben den üblichen Einträgen wie ADMIN-C oder TECH-C finden sich grundsätzlich Informationen über die Erreichbarkeit des Teams in dem Objekt: Telefon, Fax, E-Mail und Postanschrift. Darüber hinaus sind Informationen über die PGP-Keys enthalten, die für die sichere Kommunikation mit diesem Team verwendet werden können. Verlinkt werden die IRT-Objekte von einem INETNUM-Objekt, also dem Hauptobjekt für eine IP-Adresse bzw. einen Adressraum. Abfragbar sind diese Informationen entweder auf der RIPE-Webseite direkt oder mit dem RIPE-WHOIS-Tool und dem Parameter “-c” (auf ftp.ripe.net/tools/).

Verlinkung im DFN bereits durchgeführt

Seit Anfang Oktober sind sämtliche INETNUM-Einträge bei RIPE, für die der DFN-Verein der Maintainer ist, mit dem IRT-Objekt des DFN-CERT verlinkt. Für neue GWiN Anwender wird diese Verlinkung automatisch durchgeführt werden.

Für die Ermittlung des korrekten Notfallteams für eine IP-Adresse wird WHOIS verwendet:

```
marco@dummy:/> whois -h
whois.ripe.net -c -r 192.76.176.5

inetnum:      192.76.176.0 -
              192.76.176.255
netname:      DFNZPL-NET
descr:        DFN-Verein
descr:        Anhalter Str. 1
descr:        D-10963 Berlin
country:      DE
admin-c:      MW238
tech-c:       JR433
tech-c:       KL565
status:       ASSIGNED PI
mnt-by:       DFN-LIR-MNT
mnt-irt:      IRT-DFN-CERT
changed:      porten@vm.gmd.de
              19910621
changed:      poldi@dfn.de 19960507
changed:      poldi@dfn.de 19990806
changed:      poldi@dfn.de 20031008
source:       RIPE
```

In einem zweiten Schritt können nun die Kontaktinformationen des DFN-CERT, ebenfalls mittels WHOIS, abgefragt werden:

```
marco@dummy:/> whois -h
whois.ripe.net irt-dfn-cert

irt:          IRT-DFN-CERT
address:      DFN-CERT GmbH
address:      Heidenkampsweg 41
address:      D-20097 Hamburg
address:      Germany
phone:        +49 40 80 80 77 555
fax-no:       +49 40 80 80 77 556
e-mail:       dfncert@cert.dfn.de
signature:    PGPKEY-6DFC4771
encryption:   PGPKEY-6DFC4771
admin-c:      TI123-RIPE
tech-c:       TI123-RIPE
auth:         PGPKEY-6DFC4771
remarks:      Emergency telephonenum-
              ber +49 4080 8077 555
              (GMT+1/GMT+2 with DST)
remarks:      http://www.trusted-intro-
              ducer.org/teams/dfn-
              cert.html
remarks:      This is an accredited IRT
              (level 2)
irt-nfy:      dfncert@cert.dfn.de
notify:       tiirt@stelvio.nl
notify:       dfncert@cert.dfn.de
mnt-by:       TRUSTED-INTRODUCER-MNT
changed:      ripe-dbm@ripe.net
              20030814
source:       RIPE
```

DFN-PCA Schlüssel- und Zertifikatinformationen

Qualitätskontrolle
Die Korrektheit und Vollständigkeit der Informationen über ein Notfallteam stellt der Service "Trusted Introducer" (TI, www.ti.stelvio.nl) sicher. Dieser Zertifizierungsdienst für Notfallteams übernimmt die Generierung und Aktualisierung des IRT-Objektes für Level 2-Teams wie das DFN-CERT. Dies ist sinnvoll, da der TI als vertrauensbildende Instanz immer die aktuellen Daten über ein Level 2-Team hat, denn es gehört zu den Aufgaben eines Level 2-Teams seine Informationen in der TI-Datenbank immer aktuell zu halten. Mitarbeiter des TI haben bei der Erstellung der Spezifikationen für das IRT-Objekt sehr eng mit RIPE zusammengearbeitet und sind deshalb in der Lage diesen Service für das DFN-CERT anzubieten.

Alles klar?
Bitte prüfen Sie nach oben angegebenem Schema, ob die Verlinkung mit dem DFN-CERT in der RIPE-Datenbank für Ihren IP-Adressbereich erfolgreich war. Bei Rückfragen wenden Sie sich bitte an hostmaster@dfn.de.

Die Policy Certification Authority im DFN (DFN-PCA) arbeitet unter dem Dach der DFN-CERT GmbH. Aufgabe der DFN-PCA ist der Aufbau einer DFN-weiten Public Key Infrastruktur (PKI). Dazu wurde eine Zertifizierungsstelle für die Standards PGP und X.509/SSL aufgebaut. Um die Authentizität von durch die DFN-PCA ausgestellten Zertifikaten prüfen zu können, werden die nachfolgenden Informationen benötigt. Das Wurzelzertifikat zu X.509/SSL ist für den Zeitraum von 2001 - 2010 gültig. Für PGP wurden für die Ende 2003 ablaufenden Zertifikate bereits neue erzeugt, die ab dem 1.1.2004 gültig werden. Alle weiteten Informationen zur DFN-PCA finden Sie unter: www.dfn-pca.de.

DFN-PCA: PGP-Schlüsselinformationen

Low-Level Policy

PCA (Wurzelzertifikat):

Benutzer-ID:
DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003) <http://www.dfn-pca.de/>
Schlüssel-ID: F2D58DB1
Schlüssellänge: 2048 Bits • Erstellungsdatum: 2001/11/20
Fingerprint: DE 31 69 0D BC 6A E7 79 4D CD A1 B5 81 80 FE 7B

Benutzer-ID:
DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005) <http://www.dfn-pca.de/>
Schlüssel-ID: FDCB1C33
Schlüssellänge: 2048 Bits • Erstellungsdatum: 2003/10/26
Fingerprint: 96 B0 AD 7F B8 DC 00 18 DC A0 70 53 1C 3B 4D A5

User-CA:

Benutzer-ID:
DFN-User-CA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003) <http://www.dfn-pca.de/>
Schlüssel-ID: 7A9D7B59
Schlüssellänge: 2048 Bits • Erstellungsdatum: 2001/11/20
Fingerprint: 7A 0A DC 7B D6 B3 91 1D E6 75 6F E0 A7 43 AA 48

Benutzer-ID:
DFN-User-CA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005) <http://www.dfn-pca.de/>
Schlüssel-ID: BB62BBA7
Schlüssellänge: 2048 Bits • Erstellungsdatum: 2003/10/26
Fingerprint: 4F 89 24 B6 71 D4 7B 92 D3 9E AA EB D3 A1 28 ED

DFN-PCA Kommunikationsschlüssel (gültig bis 31.12.2003):

Benutzer-ID:
DFN-PCA, ENCRYPTION KEY <dfnpca@pca.dfn.de>
Schlüssel-ID: E77ADB85
Schlüssellänge: 2048 Bits • Erstellungsdatum: 1998/04/21
Fingerprint: 48 BE 74 79 7F 5D BD 4C 65 2B 98 53 DD 5A 03 05

DFN-PCA Kommunikationsschlüssel (gültig für 2004):

Benutzer-ID:
DFN-PCA (2004), ENCRYPTION Key <dfnpca@dfn-pca.de>
Schlüssel-ID: 94E799B5
Schlüssellänge: 2048 Bits • Erstellungsdatum: 2003-11-07
Fingerprint: A9 F8 2D C4 09 CC DA 7F DC 67 8F E5 28 DE AA AC

DFN-PCA: X.509/SSL-Zertifikatinformationen

X.509 Policy

DFN Top Level CA Generation 1 (Wurzelzertifikat):

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1429501 (0x15cffd)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA, \
            CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
    Validity
            Not Before: Dec 1 12:11:16 2001 GMT
            Not After : Jan 31 12:11:16 2010 GMT
    Subject: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA, \
              CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
    Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
    X509v3 extensions:
            X509v3 Basic Constraints: critical
                    CA:TRUE
    X509v3 Subject Key Identifier:
            06:0B:FA:B5:F8:48:78:A3:20:B1:0B:3E:CF:A0:D0:C4:D1:7F:7D:D0
    X509v3 Authority Key Identifier:
            keyid:06:0B:FA:B5:F8:48:78:A3:20:B1:0B:3E:CF:A0:D0:C4:D1:7F:7D:D0
            DirName:/C=DE/O=Deutsches Forschungsnetz/OU=DFN-CERT GmbH/OU=DFN-PCA \
                    /CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
            serial:15:CF:FD
    X509v3 Key Usage:
            Certificate Sign, CRL Sign
    Netscape Cert Type:
            SSL CA, S/MIME CA, Object Signing CA
    X509v3 CRL Distribution Points:
            URI:http://www.dfn-pca.de/certification/x509/g1/data/crls/root-ca-crl.crx
            URI:http://www.dfn-pca.de/certification/x509/g1/data/crls/root-ca-crl.crl
    Netscape Revocation Url:
            https://www.dfn-pca.de/cgi/check-rev.cgi?
    Netscape CA Policy Url:
            http://www.dfn-pca.de/certification/policies/x509policy.html
    Netscape Comment:
            The DFN Top-Level Certification Authority
    X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.11418.300.1.1
                    CPS: http://www.dfn-pca.de/certification/policies/x509policy.html

SHA1 Fingerprint = 8E:24:22:C6:7E:6C:86:C8:90:DD:F6:9D:F5:A1:DD:11:C4:C5:EA:81
MD5 Fingerprint = 3E:1F:9E:E6:4C:6E:F0:22:08:25:DA:91:23:08:05:03
```

Kurzmeldungen

Einsteigertarif für den Videokonferenzdienst des DFN-Vereins verlängert
Der bisher im Rahmen von DFNVC angebotene Einsteigertarif mit einer einmaligen Laufzeit von 6 Monaten wird ab sofort für ein ganzes Jahr angeboten. Damit soll interessierten Einrichtungen genügend Zeit gegeben werden, den Dienst auszuprobieren und bei ihren Nutzern bekannt zu machen.

BELWÜ wird Teil des DFN-Verbundes
Das Landeshochschulnetz BelWü ist seit dem Sommer Teil des bundesweiten DFN-Verbundes. Am 21. Juli des Jahres unterzeichneten Wissenschaftsmininster Prof. Peter Frankenberg für Baden-Württemberg und Prof. Eike Jessen für den DFN-Verein einen entsprechenden Vertrag. Insbesondere neuen Diensten mit höheren Qualitätsanforderungen kann damit in allen angeschlossenen Netzen eine einheitlich hohe Priorität eingeräumt werden. Gleichzeitig wird eine gemeinschaftliche Basis für wissenschaftliches Rechnen geschaffen.

DFNNetNews ab Dezember auch für lokale Newsgruppen
Ab Dezember 2003 können auf dem DFNNetNews-Server auch lokale Nutzergruppen mit voller Funktionalität eingerichtet werden. DFNNetNews wird als Zusatzdienst zu DFNInternet erbracht und bietet Anwendern und deren Nutzern einen zentralen Newsserver zum Lesen und Posten von Newsartikeln. Teilnehmer können dank DFNNetNews auf den Betrieb eigener Netnews-Server verzichten.

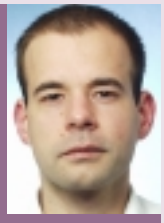
Die Auskunft über Verbindungsdaten gegenüber Strafverfolgungsbehörden

Mit Gesetz vom 20. Dezember 2001 sind die §§ 100g und 100h StPO in die Strafprozessordnung eingefügt worden. Sie stellen nunmehr seit ihrem Inkrafttreten am 1. Januar 2002 die Rechtsgrundlage für Auskunftsverlangen der Strafverfolgungsbehörden über Verbindungsdaten dar. Sie lösen § 12 Fernmeldeanlagengesetz (FAG) ab, gegen den unter dem Aspekt des rechtsstaatlichen Bestimmtheitserfordernisses verfassungsrechtliche Bedenken erhoben wurden. Im Zuge der Neuregelung wurden unter dem Blickwinkel des aus Art. 10 GG folgenden Fernmeldegeheimnisses die Anordnungsvoraussetzungen für den Auskunftsanspruch maßvoll angehoben. Die Neuregelung ermöglicht zeitlich befristet auch die Auskunft über künftige Verbindungsdaten. Der Umfang der Informationspflicht ist jedoch auf die Verbindungsdaten beschränkt, die ohnehin nach der Teledienstedatenschutzverordnung (TDSV) durch den Diensteanbieter erhoben, verarbeitet und genutzt werden dürfen.

Hinsichtlich ihrer materiellen Anforderungen differenziert die Regelung zwischen Straftaten von erheblicher Bedeutung und Straftaten, die mittels einer Endeinrichtung im Sinne des § 3 Nr. 3 TKG (z.B. Telefon, PC) begangen worden sind. Bei Straftaten die mittels einer Endeinrichtung begangen werden reicht es aus, wenn der Anordnung Gründe der Verhältnismäßigkeit nicht entgegenstehen. Grund für die vereinfachten Voraussetzungen ist, dass ansonsten kaum eine Möglichkeit der Verfolgung solcher Straftaten besteht. Wenn beispielsweise durch einen Dritten im Namen des dadurch Beleidigten die Schaltung einer kompromittierenden Anzeige in einem Online-Angebot veranlasst wird, wird dieser regelmäßig nur über die Verbindungsdaten bei seinem Provider zu identifizieren sein. Das LG Ulm (Az.:2Qs 2016/02) hatte am 21. März 2002 über einen solchen Fall zu entscheiden. Es war nur die durch den Zugangsprovider dynamisch zugewiesene IP-Adresse bekannt. Aufgrund der hohen Wahrscheinlichkeit der Individualisierung des Täters und dem Fehlen weiterer Ansatzpunkte für die Ermittlungen hielt das LG Ulm auch im Falle einer einfachen Beleidigung die Anordnung im Lichte des Fernmeldegeheimnisses für verhältnismäßig. Höher sind die Anforderungen, wenn eine Straftat nicht mittels einer Endeinrichtung begangen wurde. Das Erfordernis einer Straftat von erheblicher Bedeutung ist dabei reichlich unbestimmt. Zwar werden als Regelbeispiele die in § 100a StPO aufgezählten Tatbestände genannt. Dadurch wird aber lediglich klar, dass diese Taten jedenfalls als Straftaten von erheblicher Bedeutung anzusehen sind. Ungeklärt bleibt jedoch, welche weiteren Straftatbestände noch hierunter fallen können. Das LG Münster hat in einer Entscheidung vom 7. Januar 2002 (Az.: 8 Qs 2/02) festgestellt, dass ein einfacher Diebstahl jedenfalls nicht hierunter fällt.

Neben dem Vorliegen der materiellen Voraussetzungen wird eine richterliche Anordnung verlangt. Nur ausnahmsweise, wenn das Abwarten der richterlichen Entscheidung den Untersuchungserfolg ernstlich gefährden würde, kann die Anordnung durch den Staatsanwalt erfolgen. Allerdings bedarf es einer richterlichen Bestätigung innerhalb von drei Tagen. Daher gilt grundsätzlich, dass Auskunft über Verbindungsdaten nur dann erteilt werden muss, wenn eine richterliche Anordnung nach §§ 100g und 100h StPO vorliegt. Anderenfalls besteht grundsätzlich keine Verpflichtung zur Auskunft. Dies gilt jedoch nur für Verbindungsdaten. Über Bestandsdaten im Sinne des § 2 Nr. 3 Teledienstedatenschutzverordnung (TDSV) muss dennoch unter den Voraussetzungen von § 89 Abs. 6 Telekommunikationsgesetz Auskunft erteilt werden. Bei Bestandsdaten handelt es sich vor allem um personenbezogene Daten wie Name, Anschrift und Bankverbindung, die für die Begründung des Vertragsverhältnisses einschließlich dessen inhaltlicher Ausgestaltung erforderlich sind. Nach der gesetzgeberischen Begründung zu § 100g StPO handelt es sich bei IP-Adressen um Bestandsdaten. Dieses Urteil ist zu pauschal, da zwischen statischen und dynamischen IP-Adressen zu differenzieren ist. Eine statische IP-Adresse kann tatsächlich als Bestandsdatum angesehen werden, da sie zumeist über einen bestimmten Rechner einer bestimmten Person zugeordnet werden kann. Anders verhält es sich jedoch mit dynamischen IP-Adressen. Hier wird bei jeder neuen Verbindung eine neue IP-Adresse zugewiesen. Sie wird damit durch den Diensteanbieter nicht für den Bestand an Vertragsdaten erhoben, sondern mit Bezug auf einen bestimmten Verbindungsvorgang. Deshalb muss richtigerweise die Einordnung zu den Verbindungsdaten erfolgen. Daher fällt die Auskunft über dynamische IP-Adressen unter §§ 100g, 100h StPO und damit unter den Vorbehalt der richterlichen Anordnung.

Da die in §§ 100g und 100h StPO genannten Voraussetzungen Ausprägung des Schutzes des durch Art. 10 GG garantierten Fernmeldegeheimnisses sind, erfordert deren Beachtung strikte Einhaltung. Umso erstaunlicher ist die hierbei kürzlich durch den Fall AN.ON zu Tage getretene Praxis des Amtsgerichts Frankfurt am Main. Das Amtsgericht



Jan Köcher

Mitarbeiter der Forschungsstelle
"Recht im DFN"
Westfälische Wilhelms-Universität
Institut für Informations,-
Telekommunikations- und
Medienrecht (ITM)

dfn.recht@uni-muenster.de

hatte das AN.ON Projekt in einer Anordnung nach § 100g StPO verpflichtet, den Zugriff auf eine bestimmte IP-Nummer zu protokollieren. Die Vollziehung wurde kurz darauf durch das LG Frankfurt am Main ausgesetzt. Die bereits vorliegenden Aufzeichnungen wurden in den Räumen der TU Dresden als beteiligte Projektpartnerin aufbewahrt. Auf Antrag des ermittelnden BKA hat das Amtsgericht Frankfurt am Main sodann eine Anordnung auf Durchsuchung der Räumlichkeiten mit dem Ziel der Beschlagnahme der Aufzeichnungen erlassen. Damit hat sich das Amtsgericht über die Entscheidung des Landgerichts hinweggesetzt. Durch die Anordnung der Durchsuchung und Beschlagnahme der Aufzeichnung der Verbindungsdaten wurde der gesetzgeberische Ausgleich zwischen den Belangen des Fernmeldegeheimnisses und einer effektiven Strafverfolgung unterlaufen. Es ist davon auszugehen, dass das Amtsgericht bei seiner Entscheidung diese Wertungen nicht berücksichtigt hat. Hätten die Voraussetzungen für eine Anordnung nach § 100g StPO vorgelegen, hätte es des Umwegs über die Beschlagnahme nicht bedurft. Dagegen hilft auch der Einwand nicht, dass schließlich keine Auskunft begehrt wird sondern nur der körperliche Datenträger Gegenstand der Beschlagnahme ist. Durch das Wissen um die darauf gespeicherten Verbindungsdaten kommt diese Vorgehensweise der Durchsetzung eines Auskunftsbegehrens nach § 100g StPO gleich. Wenn die Beschlagnahme wie hier auf die Erlangung der Auskunft abzielt, dürfen die Voraussetzungen der §§ 100g und 100h StPO nicht unbeachtet bleiben. Daher ist eine Anordnung der Beschlagnahme von Datenträgern mit Verbindungsdaten nur dann rechtmäßig, wenn gleichzeitig die Voraussetzungen für eine Anordnung nach §§ 100g, 100h StPO gegeben sind. Man kann nur hoffen, dass die Obergerichte dies genauso sehen. Ansonsten verkommt das durch die Anti-Terror-Gesetzgebung ohnehin geschwächte Fernmeldegeheimnis zu einem Papiertiger.

Inzwischen hat das LG Frankfurt am Main (Az.: 5/8 Qs 26/03) entschieden, dass der Durchsuchungsbeschluss des AG Frankfurt eine rechtswidrige Umgehung der §§ 100g, h StPO darstellte. Das LG Frankfurt hat somit für Rechtssicherheit in diesem besonders sensiblen Bereich gesorgt.

- Im Ergebnis bleibt damit festzuhalten, dass eine Verpflichtung zur Auskunft über Verbindungsdaten gegenüber Ermittlungsbehörden grundsätzlich nur bei Vorliegen einer richterlichen Anordnung besteht.

- Die Auskunftsverpflichtung darf sich nur auf Daten beziehen, die nach der Teledienstedatenschutzverordnung durch den Diensteanbieter ohnehin erhoben werden dürfen.

- Es besteht dabei keine Verpflichtung die Daten für den Fall eines Auskunftsverlangens vorbeugend zu erheben.

- Eine Pflicht zur Erhebung von künftigen Verbindungsdaten für Zwecke der Ermittlung kann grundsätzlich nur durch eine richterliche Anordnung nach §§ 100g, h StPO begründet werden.

- Über Bestandsdaten muss unter den Voraussetzungen von § 89 Abs. 6 TKG den Ermittlungsbehörden jedoch Auskunft erteilt werden.

Am DFN-Verbund nahmen im Oktober 2003 463 Anwender und 297 Mitnutzer teil. 19 Anwender nutzen das Port-Dienstangebot. In 20 Clustern sind 53 Anwender angebunden. Von den 78 Änderungen der Zugangsleitungsbetreiber wurden 76 realisiert. Die restlichen beiden Umschaltungen stehen unmittelbar bevor. Es gab dabei keine wesentlichen Probleme. Im Monat Oktober lag das gesamte aus dem G-WiN exportierte Volumen bei 1.198 TByte, davon wurden an den Anwenderanschlüssen 525 TByte gemessen. Der daraus folgende jährliche Steigerungsfaktor lag im Oktober bei 1,20. Das importierte Datenvolumens lag an den Anwenderanschlüssen im Oktober bei 748 TByte/Monat. Damit ist wieder ein leichtes Ansteigen des Datenvolumens nach der Urlaubszeit zu verzeichnen.

Zur Verbesserung der IP-Performance für die Einrichtungen in NRW wurden zwischen dem Kernnetzknoten St. Augustin und Essen eine STM-16c-Verbindung und in Vorbereitung auf datenintensive GRID-Projekte im FZ Jülich ein Upgrade der Verbindung St. Augustin – Frankfurt/Main auf 10 Gbit/s beauftragt.

5039 Teilnehmer nutzen derzeit den WiNShuttle, davon sind 3894 Schulen. Von den WiNShuttle-Nutzern werden insgesamt 1314 eigene Domains betrieben, deren Nameservice vom WiNShuttle-Team bereitgestellt wird. Seit einiger Zeit werden auch DSL-Zugänge zum WiNShuttle angeboten. Voraussetzung ist, dass der Nutzer einen T-DSL-Anschluss bei der DTAG hat. Die Zuführung der DSL-Strecken aus dem DTAG-Netz ins G-WiN stellt die Telefonica Deutschland GmbH bereit (wie auch beim Dienst DFN@home). Zur Zeit sind 192 DSL-Zugänge zum WiNShuttle in Betrieb. Seit Juli 2003 ist das DSL-Angebot um eine Mehrplatzlösung auf Basis eines T-DSL 1500er Zugangs erweitert worden. Damit ist es möglich, von mehreren Arbeitsplätzen gleichzeitig via DSL und WiNShuttle auf das G-WiN zuzu-

Bericht zu Betrieb und Nutzung des DFN

greifen. Diese Lösung ist besonders für Schulen und andere Bildungseinrichtungen interessant. Im September wurde dieses Angebot von 41 Einrichtungen genutzt.

Für den VPN-Einwahldienst DFN@home sind derzeit ca. 14.000 Nutzer bei der Telefonica Deutschland GmbH registriert. 70 DFN-Einrichtungen nehmen derzeit am Dienst teil. DSL-Zugänge werden seit September 2002 bundesweit angeboten und von 50 Einrichtungen genutzt. Es sind ca. 1.500 DSL-Nutzer registriert. Die Werbeaktion zum Wintersemester an den Hochschulen hat in den ersten drei Wochen ca. 1.000 neue Nutzer gebracht.

Im Rahmen eines Corporate Network DFN bietet der DFN-Verein seinen Anwendern die Möglichkeit, im Vorgriff auf eine spätere Harmonisierung der Netze ihren Fernsprechdienst über die Infrastruktur der DTAG zu sehr günstigen Konditionen abzuwickeln. Dieses Angebot nutzen zur Zeit 161 Einrichtungen mit 768 Lokationen.

Der Regelbetrieb für den Dienst DFNVideoConference wird seit gut einem halben Jahr angeboten. Insgesamt haben sich 76 Einrichtungen für DFNVC angemeldet. Auf der Sitzung des Verwaltungsrates am 22.10.03 wurde beschlossen, den Einsteigertarif, der derzeit einmalig für 6 Monate mit einem Entgelt von 600,- EUR beauftragt werden kann, um 12 Monate zu verlängern. Im Oktober fanden insgesamt 2956 Konferenzen mit 3880 Teilnehmern statt. Die Nutzungszahlen zeigen einen deutlichen Anstieg gegenüber dem Vormonat. Bevorzugt wurden Bandbreiten über 384 Kbit/s. Bei der Dauer einer Konferenz häufen sich die Zeiten, die zwischen 20 Minuten und 2 Stunden liegen. Bei den MCU-Konferenzen wurde dem Konferenztyp „Continuous Presence“ häufig der Vorzug gegeben. 22% der Konferenzen nutzten T.120 (Application Sharing) bzw. haben die Option ausgewählt.

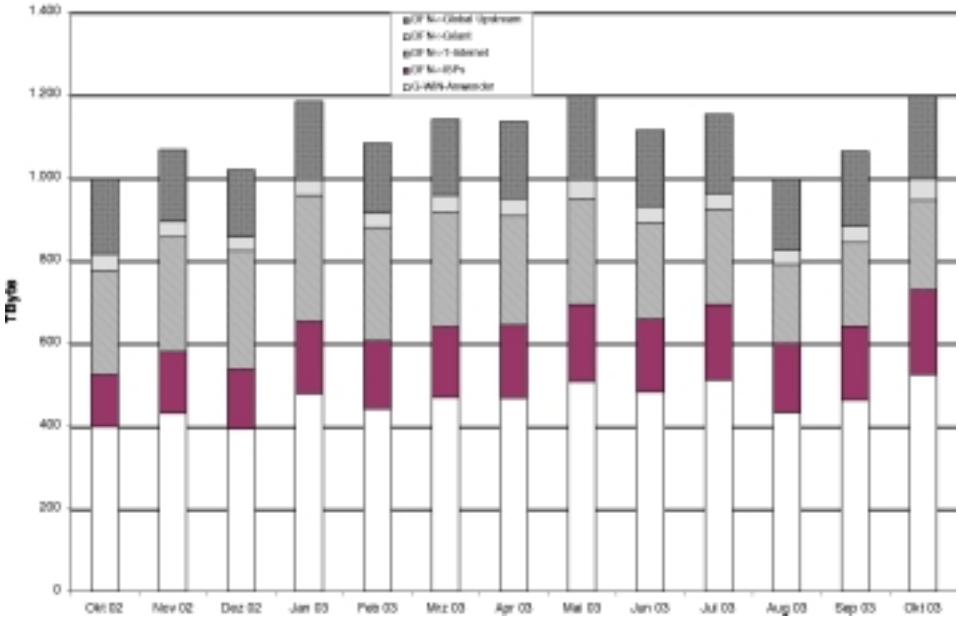


Abb1: Exportiertes Datenvolumen G-WiN Kernnetz

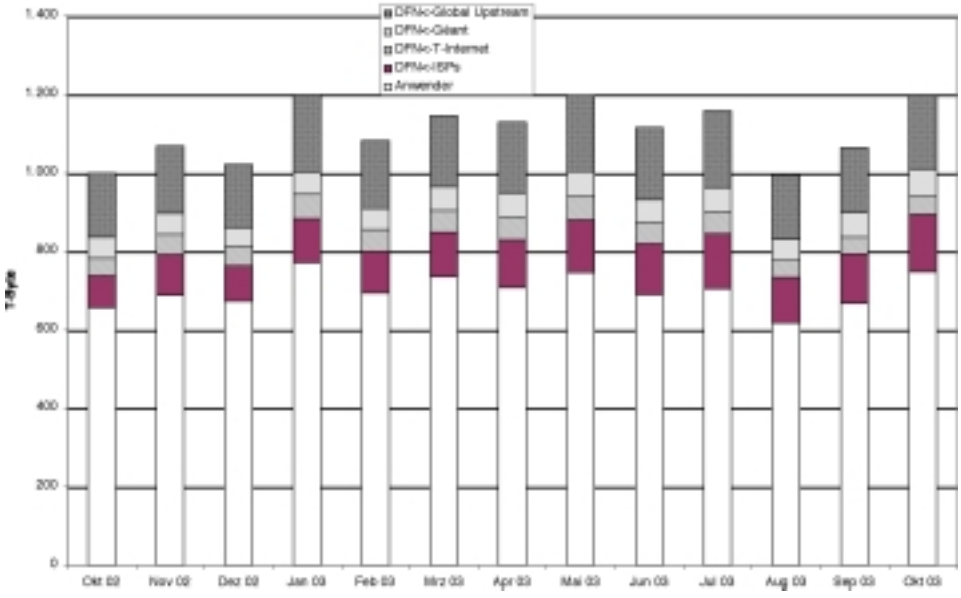


Abb2: Importiertes Datenvolumen G-WiN-Kernnetz

Zusätzlich zum DFNInternet Dienst wird der Dienst DFNNetNews angeboten. G-WiN Teilnehmer können mit DFNNetNews einen zentralen Newsserver zum Lesen und Posten von Newsartikeln nutzen und auf den Betrieb eines eigenen NetnewsServers verzichten. Der Dienst basiert auf dem Dienst News.CIS.DFN.DE, den die FU Berlin im Rahmen eines DFN-Projektes aufgebaut hat. Ab Dezember 2003 können lokale Nutzergruppen auf dem DFNNetNews-Server mit voller Funktionalität eingerichtet werden. Zur Zeit haben 27 Einrichtungen mit dem DFN-Verein einen Vertrag über die Nutzung des Dienstes abgeschlossen.

Übersicht über die Mitgliedseinrichtungen und Organe des DFN-Vereins (Stand 11.2003)

Laut Satzung fördert der DFN-Verein die Schaffung der Voraussetzungen für die Errichtung, den Betrieb und die Nutzung eines rechnergestützten Informations- und Kommunikationssystems für die öffentlich geförderte und gemeinnützige Forschung in der Bundesrepublik Deutschland. Der Satzungszweck wird verwirklicht insbesondere durch Vergabe von Forschungsaufträgen und Organisation von Dienstleistungen zur Nutzung des Deutschen Forschungsnetzes.

Als Mitglieder werden juristische Personen aufgenommen, von denen ein wesentlicher Beitrag zum Vereinszweck zu erwarten ist oder die dem Bereich der institutionell oder sonst aus öffentlichen Mitteln geförderten Forschung zuzurechnen sind.

Die Organe des DFN-Vereins sind
- die Mitgliederversammlung
- der Verwaltungsrat
- der Vorstand

Sitz des Vereins ist Berlin.

Die **Mitgliederversammlung** ist u. a. zuständig für die Wahl der Mitglieder des Verwaltungsrates, für die Genehmigung des Jahreswirtschaftsplanes, für die Entlastung des Vorstandes und für die Festlegung der Mitgliedsbeiträge. Derzeitiger Vorsitzender der Mitgliederversammlung ist Peter Grosse, Institut für Meereskunde an der Universität Kiel.

Die Mitgliederversammlung hat für 2003 folgende Mitgliedsbeiträge - abhängig vom Status des Mitglieds - beschlossen:

- für Hochschulen und andere Einrichtungen in Lehre und Forschung
  255,00 EURO/Jahr

- für staatliche geförderte Forschungseinrichtungen außerhalb der Lehre und vergleichbare Einrichtungen der öffentlichen Hand
  mit bis zu 100 Mitarbeitern
  1.025,00 EURO/Jahr
  mit über 100 Mitarbeitern
  2.560,00 EURO/Jahr

- für Wirtschaftsunternehmen,
  bis zu 20 Mitarbeitern
  1.025,00 EURO/Jahr
  bis zu 100 Mitarbeitern
  2.560,00 EURO/Jahr
  mit über 100 Mitarbeitern
  5.120,00 EURO/Jahr

Der **Verwaltungsrat** beschließt über alle wesentlichen Aktivitäten des Vereins, insbesondere über die technisch-wissenschaftlichen Arbeiten, und berät den Jahreswirtschaftsplan. Für die 7. Wahlperiode bis Ende 2005 sind Mitglieder des Verwaltungsrates:

- Prof. Dr. C. Eckert,
  Fraunhofer-Institut für Sichere Telekooperation, Darmstadt
- Prof. Dr. H.-G. Hegering (stellv. Vorsitzender),
  Leibniz-Rechenzentrum München
- Prof. Dr. W. Hiller,
  Alfred-Wegener-Institut für Polar- und Meeresforschung, Bremerhaven
- Prof. Dr.Dr.h.c. K. H. Hoffmann,
  Stiftung caesar, Bonn
- Prof. Dr. E. Jessen (Vorsitzender),
  Technische Universität München
- Prof.Dr. W. Juling,
  Universität Karlsruhe
- Dr. K.-P. Kossakowski,
  PRESECURE Consulting GmbH, Telgte
- Dr. B. Lix,
  Universität Duisburg-Essen
- Dr. F. Nolden, (stellv. Vorsitzender)
  UFZ-Umweltforschungszentrum Leipzig-Halle
- Prof. Dr. Gerhard Schneider,
  Universität Freiburg
- Dr. W. A. Slaby,
  Katholische Universität Eichstätt
- G. Springer,
  Technische Universität Ilmenau
- Prof. H. Wiese,
  FH Esslingen Hochschule für Technik, Esslingen

Der **Vorstand** des DFN-Vereins im Sinne des Gesetzes wird aus dem Vorsitzenden und den beiden stellvertretenden Vorsitzenden des Verwaltungsrates gebildet. Derzeit sind dies Prof. Dr. E. Jessen, Vorsitz, sowie Prof. Dr. H.-G. Hegering und Dr. F. Nolden.

Der Vorstand wird beraten von einem Technischen Ausschuß (TA), einem Betriebsausschuß (BA), und einem Ausschuss für Recht und Sicherheit (ARSi), der zugleich auch als Jungendschutzbeauftragter für das DFN fungiert. Ansprechstelle in Fragen des Jugendschutzes über e-mail: medieninhalte@dfn.de Tel.-Nr.: (030) 88 67 88 44

Technischer Ausschuss
- Thomas Brunner,
  SWITCH, Zürich
- Prof. Dr. Rüdiger Grimm,
  Technische Universität Ilmenau
- Stefan Heinzel,
  MPI für Plasmaphysik, Garching
- Prof. Dr. Uwe Hübner,
  Technische Universität Chemnitz (Vors.)
- Prof. Dr. Eike Jessen,
  Technische Universität München
- Dr. Burkhard Mertens,
  Forschungszentrum Jülich
- Prof. Dr. Helmut Pralle,
  Hannover
- Prof. Dr. Alexander Reinefeld,
  Konrad-Zuse-Zentrum für Informationstechnik, Berlin
- Dr. Ralf Schäfer,
  Fraunhofer Heinrich-Hertz-Institut für Nachrichtentechnik, Berlin
- Dr. Egon Verharen,
  Surfnet bv, Utrecht

Betriebsausschuss
- Dr. Holger Busse,
  Freie Universität Berlin, ZEDAT
- Dr. Hans Frese, DESY Hamburg
- Prof. Dr. Heinz-Gerd Hegering,
  Leibniz-Rechenzentrum München (Vorsitz)
- Dr. Wilhelm Held,
  Universität Münster
- Dr. Peter Holleczek,
  Universität Erlangen-Nürnberg
- Prof. Dr. Wilfried Juling,
  Universität Karlsruhe
- Frank Klapper
  Universität Bielefeld
- Edith Petermann,
  Universität Mannheim
- Dr. Christa Radloff,
  Universität Rostock
- Prof. Dr. Gerhard Schneider,
  Universität Freiburg
- Manfred Sedig, Universität Kassel
- Prof. Dr. Stenzel,
  Fachhochschule Köln

Ausschuss für Recht und Sicherheit
- Prof. Dr. Claudia Eckert, Technische Universität Darmstadt
- Prof. Dr. Thomas Hoeren,
  Universität Münster
- Dr. Klaus-Peter Kossakowski,
  PRESECURE Consulting GmbH, Teltge
- Dr. Frank Nolden,
  Umweltforschungszentrum Leipzig (Vorsitz)
- Dr. Bernhard Raiser,
  GeoForschungszentrum Potsdam
- Prof. Dr. Peter Schirmbacher,
  Humboldt-Universität Berlin
- Prof. Dr. Gerhard Schneider,
  Universität Freiburg

Der Vorstand bedient sich zur Erledigung laufender Aufgaben einer **Geschäftsstelle** mit Standorten in Berlin und Stuttgart. Sie wird von einer Geschäftsführung geleitet. Als Geschäftsführer wurden vom Vorstand Klaus Ullmann (wiss.-tech.) und Dr. Klaus-Eckart Maass (admin.) bestellt.

Anschriften
Verein zur Förderung eines Deutschen Forschungsnetzes e. V. - DFN-Verein -

Standort Berlin:
Anhalter Straße 1
D-10963 Berlin
Tel.: (030) 88 42 99 -23, -24 (Sekretariat)
Telefax: (030) 884 299-70
E-Mail: dfn-verein(@)dfn.de
Internet-Adresse:
www.dfn.de

Standort Stuttgart:
Lindenspürstraße 32
70176 Stuttgart
Tel.: (0711)633 14 140
Telefax: (0711) 633 14 133
Internet-Adresse:
www.noc.dfn.de

Ansprechpartner
Presse, Öffentlichkeitsarbeit:
K. Hoelzner
Betreuung der Entwicklung und Pilotierung neuer Dienste:
Dr. P. Kaufmann (kaufmann@dfn.de)
Administrative Fragen der Projektabwicklung:
E. Heller (heller@dfn.de)
Dienstleistungen: Allgemeine Nutzerberatung, Betriebstagung
U. Kähler (kaehler@dfn.de)
Domain-Adressen:
K. Leipold (leipold@dfn.de)
WiNShuttle:
B. Ackermann (baerbel.ackermann@dfn.de)
Rechnungen:
A. Pattloch für WiN (pia@dfn.de)
B. Schöller f. Sprachdienst (schoeller@dfn.de)
H. Först f. WiNShuttle (hfoerst@dfn.de)

Hotlines
für DFNInternet, DFNConnect und DFNATM:
in Vorbereitung
für WiNShuttle:
01805 / 252354
für DFN@home:
01805 / 38338
für DFNFernsprechen:
0911 / 5195340
für DFNNOC
0711-63314-112

Nutzergruppe "Hochschulverwaltung im DFN" ihre Sprecher bzw. Ansprechpartner
Prof. Dr. G. Peter, FH Heilbronn (Leiter)
Dr. J. Hötte, Universität Stuttgart

Forschungsstellen/Kompetenzzentren im DFN, ihre Leiter bzw. Ansprechpartner
- DFN-CERT: Zentrum für sichere Netzdienste GmbH
  Rolf Schaumburg
- Directory Kompetenzzentrum
  Peter Gietz, Universität Tübingen
- Kompetenzzentrum für Videokonferenzdienste
  Wolfgang Wünsch, TU Dresden
- Forschungsstelle Recht im DFN
  Prof. Dr. Thomas Hoeren, Universität Münster
- IPv6 Referenzzentrum
  Dr. Georg Richter, Universität Münster

Betriebsforen/Arbeitskreise und ihre Sprecher

CDC/OSI	M. Storz, LRZ München
Directory	F. Städler, FH Nürnberg
E-Mail/PRMD	F. Elsner, TU Berlin
E-Learning	Dr. N. Apostolopoulos, FU Berlin
Mobile IT	Dr. N. Klever, Univ. Bayreuth
IP über WiN	H. Becher, Univ. Rostock
IPv6	Dr.G.Richter, Univ. Münster
Multimedia-Dienste	H. Schulze, RRZN, Hannover
Security	S. Kelm, Secorvo GmbH

Der DFN-Verein hat derzeit folgende Mitglieder:

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Fachhochschule Aalen
Albstadt	Fachhochschule Albstadt-Sigmaringen
Amberg	Fachhochschule Amberg-Weiden
Aschaffenburg	Fachhochschule Aschaffenburg
Augsburg	Fachhochschule Augsburg
	Universität Augsburg
Bamberg	Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Berliner Elektronenspeicherring-Gesellschaft für Synchrotron-strahlung mbH (BESSY)
	BBB Management GmbH Campus Berlin-Buch
	Bundesanstalt für Materialforschung und -prüfung (BAM)
	Bundesinstitut für Risikobewertung und Veterinärmedizin (BgVV)
	Bundesministerium für Umwelt, Naturschutz u.Reaktorsicherheit
	Bundesministerium für Verkehr, Bau- und Wohnungswesen
	CDU Deutschlands
	Deutscher Beamtenbund (DBB)
	Deutsches Herzzentrum
	Deutsches Historisches Museum (DHM) GmbH
	Deutsches Institut für Normung e.V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	Fachhochschule für Sozialarbeit u. Sozialpädagogik Berlin
	Fachhochschule für Technik und Wirtschaft
	Fachhochschule für Wirtschaft
	Fachinformationszentrum Chemie GmbH (FIZ Chemie)
	Fraunhofer Heinrich-Hertz-Institut für Nachrichtentechnik Berlin GmbH (HHI)
	Freie Universität Berlin (FUB)
	Hahn-Meitner-Institut Berlin GmbH (HMI)
	Humboldt-Universität zu Berlin (HUB)
	Konrad-Zuse-Zentrum für Informationstechnik Berlin (ZIB)
	Landesbetrieb für Informationstechnik (LIT)
	Marconi Channel Markets GmbH
	Robert-Koch-Institut, Bundesinstitut für Infektionskrankheiten
	SCHERING AG
	Stiftung Preußischer Kulturbesitz
	Stanford-Universität in Berlin
	Technische Fachhochschule Berlin (TFH)
	Technische Universität Berlin (TUB)
	T-Systems Nova GmbH Berkom
	Umweltbundesamt
	Universität der Künste
	WIAS-Forschungsverbund Berlin e.V.
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum für Sozialforschung gGmbH (WZB)
Biberach	Fachhochschule Biberach, HS für Bauwesen und Wirtschaft
Bielefeld	Fachhochschule Bielefeld
	Universität Bielefeld
Bingen	Fachhochschule Bingen
Bochum	Fachhochschule Bochum, HS für Technik und Wirtschaft
	Evangelische FH Rheinland-Westfalen-Lippe
	Technische FH Georg Agricola für Rohstoffe, Energie und Umwelt
	Ruhr-Universität Bochum
Böblingen	Staatliche Akademie für Datenverarbeitung
Bonn	Bundesamt für Finanzen
	Bundesamt für Sicherheit in der Informationstechnik
	Deutsche Forschungsgemeinschaft e.V.
	Deutscher Akademischer Austauschdienst e.V. (DAAD)
	Universität Bonn
	IZ Sozialwissenschaften
Borstel	Forschungszentrum Borstel
Brandenburg	Fachhochschule Brandenburg
Braunschweig	Biologische Bundesanstalt für Land- und Forstwirtschaft
	Bundesforschungsanstalt für Landwirtschaft (FAL)
	Fachhochschule Braunschweig/Wolfenbüttel
	Gesellschaft für Biotechnologische Forschung mbH (GBF)
	Hochschule für Bildende Künste
	Physikalisch-Technische Bundesanstalt (PTB)
	Technische Universität Braunschweig
Breitenbrunn	Berufsakademie Sachsen, Studienakademie
Bremen	Hochschule Bremen
	International University Bremen
	Universität Bremen
Bremerhaven	Hochschule Bremerhaven
	Stadtbildstelle Bremerhaven
	Stiftung Alfred-Wegener-Institut für Polar- und Meeresforschung (AWI)
Chemnitz	Technische Universität Chemnitz
Clausthal	Clausthaler Umwelttechnik-Institut GmbH (CUTEC)
	Technische Universität Clausthal-Zellerfeld
Coburg	Fachhochschule Coburg
Cottbus	Brandenburgische Technische Universität Cottbus
Darmstadt	European Space Agency (ESA)
	Fachhochschule Darmstadt
	Gesellschaft für Schwerionenforschung mbH (GSI)
	Merck KGaA
	Technische Universität Darmstadt
	T-Systems Nova GmbH
	Zentrum für Graphische Datenverarbeitung e.V. (ZGDV)
Deggendorf	Fachhochschule Deggendorf
Detmold	Lippische Landesbibliothek
Diepholz	Private Fachhochschule für Wirtschaft und Technik, Vechta/Diepholz

Dortmund	UUnet Deutschland GmbH
	Fachhochschule Dortmund
	Universität Dortmund
Dreieich	PanDacom Networking AG
Dresden	Forschungszentrum Rossendorf e.V.
	Hannah-Ahrendt-Institut für Totalitarismusforschung e.V. (i.G.)
	Hochschule für Bildende Künste
	Hochschule für Technik und Wirtschaft Dresden (FH)
	Leibniz-Institut für Festkörper- und Werkstofforschung Dresden
	Institut für Polymerforschung Dresden e.V.
	Sächsische Landesbibliothek
	Technische Universität Dresden
Düsseldorf	Fachhochschule Düsseldorf
	Landesamt für Datenverarbeitung und Statistik des Landes NRW
	Universität Düsseldorf
Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Joh. A. Lasco Bibliothek Große Kirche Emden
Erfurt	Fachhochschule Erfurt
	Stiftung für Technologie- und Innovationsförderung Thüringen (STIFT)
	Universität Erfurt
Erlangen	Universität Erlangen-Nürnberg
Essen	Rheinisch-Westfälisches Institut für Wirtschaftsforschung
	Universität Duisburg-Essen
Esslingen	Fachhochschule Esslingen, Hochschule für Technik
Flensburg	Fachhochschule Flensburg
Frankfurt/M.	Die Deutsche Bibliothek Frankfurt
	Deutsches Institut für Internationale Pädagogische Forschung
	Fachhochschule Frankfurt am Main
	Fachinformationszentrum Technik e. V. (FIZ Technik)
	Phil.-Theol. Hochschule St. Georgen e. V.
	Stadt- und Universitätsbibliothek Frankfurt
	Universität Frankfurt am Main
Frankfurt/O.	Europa-Universität Viadrina Frankfurt/Oder
	IHP Innovations for High Perfomance Microelectronics/ Institut für innovative Mikroelektronik
Freiberg	TU/Bergakademie Freiberg
Freiburg	International Solar Energy Society (ISES)
	Universität Freiburg
Fulda	Fachhochschule Fulda
Furtwangen	Fachhochschule Furtwangen
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Gatersleben	Institut für Pflanzengenetik und Kulturpflanzenforschung
Geesthacht	GKSS-Forschungszentrum Geesthacht GmbH
Gelsenkirchen	Fachhochschule Gelsenkirchen
Gießen	Fachhochschule Gießen-Friedberg
	Universität Gießen
Göttingen	Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GwDG)
	IWF. Wissen und Medien GmbH
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes der Länder Göttingen
Greifswald	Ernst-Moritz-Arndt-Universität
Hagen	Fernuniversität – GH Hagen
	InterNett Hagen e.V.
	Fachhochschule Südwestfalen
Halle/Saale	Hochschule für Kunst und Design
	Martin-Luther-Universität Halle-Wittenberg
	Institut für Wirtschaftsforschung Halle
Hamburg	Bundesamt für Seeschiffahrt und Hydrographie (BSH)
	Deutsches Elektronen Synchrotron (DESY)
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	Hamburger Universität für Wirtschaft und Politik
	Hochschule für angewandte Wissenschaften Hamburg
	Heinrich-Pette-Institut für Experimentelle Virologie und Immunologie
	Hewlett Packard GmbH
	Hochschule für Bildende Künste
	Technische Universität Hamburg-Harburg
Hamburg	Universität der Bundeswehr Hamburg
	Universität Hamburg
Hannover	Bundesanstalt für Geowissenschaften und Rohstoffe (BGR)
	Evangelische Fachhochschule Hannover
	Fachhochschule Hannover
	Hochschule für Musik und Theater Hannover
	Hochschul-Informations-System-GmbH
	Medizinische Hochschule Hannover
	Niedersächsisches Landesamt für Bodenforschung
	Niedersächsische Landesbibliothek
	Tierärztliche Hochschule Hannover
	Universität Hannover
	Universitätsbibliothek Hannover und Technische Informations-bibliothek (TIB)
	Heide FH Westküste
Heidelberg	Network Laboratories, NEC Europe Ltd.
	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	Fachhochschule Heidelberg
	Springer-Verlag GmbH & Co. KG
	Universität Heidelberg
Heidenheim	Berufsakademie Heidenheim
Heilbronn	Fachhochschule Heilbronn mit Standort Künzelsau
Heyrothsberge	(Institut der Feuerwehr Sachsen-Anhalt)
Hildesheim	Fachhochschule Hildesheim/Holzminden/Göttingen
	Universität Hildesheim
Hof	Fachhochschule Hof
Ilmenau	Technische Universität Ilmenau
	Bundesanstalt für Wasserbau
Ingolstadt	Fachhochschule Ingolstadt
Jena	Fachhochschule Jena
	Friedrich-Schiller-Universität Jena
	Institut für Molekulare Biotechnologie e.V.
	Institut für Physikalische Hochtechnolgie e.V.
Jülich	Forschungszentrum Jülich GmbH
Kaiserlautern	Fachhochschule Kaiserslautern
	Universität Kaiserslautern
Karlsruhe	Badische Landesbibliothek
	Fachhochschule Karlsruhe
	Fachinformationszentrum Ges.f.wiss.-techn.Information mbH (FIZ Karlsruhe)
	Forschungszentrum Informatik an der Universität Karlsruhe
	Forschungszentrum Karlsruhe Technik + Umwelt
	Universität Karlsruhe
	Zentrum für Kunst und Medientechnologie
Kassel	Universität Kassel
Kempten	Fachhochschule Kempten
	DIZ Zentrum für Hochschuldidaktik der bayerischen Fachhochschulen
Kiel	Fachhochschule Kiel
	Forschungszentrum für marine Geowissenschaften der Universität zu Kiel, Geomar
	Institut für Meereskunde an der Universität Kiel
	Institut für Weltwirtschaft an der Universität Kiel
	Universität Kiel
Koblenz	Fachhochschule Koblenz
	Universität Koblenz-Landau
Köln	Deutsches Institut für Medizinische Dokumentation und Information (DIMDI)
	Deutsche Sporthochschule Köln
	Deutsches Zentrum für Luft und Raumfahrt
	Fachhochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln
	Universität zu Köln
Köthen	Hochschule Anhalt (FH) (Köthen, Bernburg, Dessau)
Konstanz	Fachhochschule Konstanz
	Universität Konstanz
Krefeld	Hochschule Niederrhein
Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e.V.
Landshut	Fachhochschule Landshut
Leipzig	Bundesamt für Kartographie und Geodäsie

Leipzig	Handelshochschule Leipzig
	Hochschule für Technik, Wirtschaft und Kultur Leipzig (FH)
	Institut für Troposphärenforschung e.V.
	Mitteldeutscher Rundfunk
	Umweltforschungszentrum Leipzig-Halle GmbH
	Universität Leipzig
Lemgo	Fachhochschule Lippe und Höxter
Lörrach	Berufsakademie Lörrach – Staatliche Studienakademie –
Ludwigshafen	Fachhochschule Ludwigshafen, HS für Wirtschaft
Lübeck	Fachhochschule Lübeck
	Medizinische Universität zu Lübeck
Lüneburg	Fachhochschule Nordost Niedersachsen (u. Hochschule Lüneburg)
	Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal (FH)
	Institut für Neurobiologie
	Otto-von-Guericke-Universität Magdeburg
Mainz	Fachhochschule Mainz
Mainz	IMM, Institut für Mikrotechnik Mainz GmbH
	Universität Koblenz-Landau
	Universität Mainz
Mannheim	Fachhochschule Mannheim, Hochschule für Technik und Gestaltung
	TÜV Energie- und Systemtechnik GmbH Baden-Württemberg
	Universität Mannheim
	Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW)
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Universität Marburg
Merseburg	Fachhochschule Merseburg
Mittweida	Hochschule Mittweida, University of Applied Sciences
Mosbach	Berufsakademie Mosbach, Staatl. Studienakademie
München	Bayerische Staatsbibliothek Bibliotheksverbund Bayern
	BT Ignite GmbH & Co.
	DECUS München e.V.
	Fachhochschule München
	Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung e. V. (FhG)
	GSF-Forschungszentrum für Umwelt und Gesundheit GmbH
	IFO-Institut für Wirtschaftsforschung e.V.
	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. (MPG)
	SIEMENS AG
	Technische Universität München
	Universität der Bundeswehr München
Müncheberg	Zentrum für Agrarlandschafts- und Landnutzungs-forschung (ZALF) e.V.
Münster	Fachhochschule Münster
	Institut für Angewandte Informatik an der Universität Münster
	Universität Münster
Neu Ulm	Fachhochschule Neu Ulm
Neubrandenburg	Fachhochschule Neubrandenburg
Nordhausen	Fachhochschule Nordhausen
Nürnberg	Fachhochschule Nürnberg
	Kommunikationsnetz Franken e.V.
Nürtingen	Fachhochschule Nürtingen
Oberursel	Dimension Data Germany AG + Co
Oberwolfach	Mathematisches Forschungsinstitut
Offenbach/Main	Deutscher Wetterdienst Offenbach
Offenburg	Fachhochschule Offenburg, HS für Technik und Wirtschaft
Oldenburg	Landesbibliothek Oldenburg
	Universität Oldenburg
Osnabrück	Fachhochschule Osnabrück
	Universität Osnabrück
Paderborn	HNF Heinz Nixdorf MuseumsForum GmbH
	Universität Gesamthochschule Paderborn
Passau	Universität Passau
Peine	Deutsche Gesellschaft zum Bau und Betrieb von Endlagern für Abfallstoffe mbH
Pforzheim	Fachhochschule Pforzheim, HS für Gestaltung, Technik und Wirtschaft
Potsdam	Deutsches Institut für Ernährungsforschung, Bergholz-Rehbrücke
	Fachhochschule Potsdam
	GeoForschungsZentrum Potsdam
	Hochschule für Film und Fernsehen „Konrad Wolf“
	Potsdam Institut für Klimafolgenforschung e.V. (PIK)
	Universität Potsdam
Ratingen	SUN Microsystems GmbH
Ravensburg	Berufsakademie Ravensburg
Recklinghausen	InfoTech Gesellschaft für Informations- und Datentechnik mbH
Regensburg	Fachhochschule Regensburg
	Universität Regensburg
Rosenheim	Fachhochschule Rosenheim
Rostock	Institut für Ostseeforschung
	Universität Rostock
Saarbrücken	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Birlinghovener Informationsdienste (ehemals GMD)
	Fachhochschule Bonn Rhein-Sieg
	Fraunhofer Gesellschaft e.V. -
	Ingbest Comchat AG-Security
Schmalkalden	Fachhochschule Schmalkalden
Schwäbisch-Gmünd	Pädagogische Hochschule
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Schwindegg	Bürgernetzverband e.V.
Senftenberg	Fachhochschule Lausitz
Siegen	Universität Siegen
Speyer	Deutsche Hochschule für Verwaltungswissenschaften Speyer
	Pfälzische Landesbibliothek Speyer am Rhein
Stralsund	Fachhochschule Stralsund
Stuttgart	Cisco Systems GmbH
	DaimlerCrysler AG
	Fachhochschule Stuttgart, HS der Medien
	Fachhochschule Stuttgart, HS für Technik
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte
Trier	Fachhochschule Trier, Hochschule für Technik, Wirtschaft und Gestaltung
	Universität Trier
Tübingen	Bundesforschungsanstalt für Viruskrankheiten der Tiere
	Universität Tübingen
Ulm	Fachhochschule Ulm, Hochschule für Technik
	Universität Ulm
Vechta	Hochschule Vechta
Wachtberg	Forschungsgesellschaft für angewandte Naturwissenschaften e.V., Wachtberg-Werthofen
Wedel	Hydromod GbR
Weidenbach	Fachhochschule Weihenstephan
Weimar	Bauhaus-Universität Weimar
Weingarten	Fachhochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz, Fachhochschule für Wirtschaft und Technik
Wiesbaden	Fachhochschule Wiesbaden
	Statistisches Bundesamt Wiesbaden
Wessling	T-Systems Solutions for Research GmbH
Wildau	Technische Fachhochschule Wildau
Wilhelmshaven	Fachhochschule Oldenburg/Ostfriesland/Wilhelmshaven
Wismar	Hochschule Wismar
Witten	Universität Witten/Herdecke
Wolfenbüttel	Herzog-August-Bibliothek
Worms	Fachhochschule Worms
	Wissenschaftliche Bibliothek der Stadt Worms
Würzburg	Fachhochschule Würzburg-Schweinfurt
	Universität Würzburg
Wuppertal	Bergische Universität Gesamthochschule Wuppertal
Zittau	Hochschule für Technik und Wirtschaft Zittau/Görlitz (FH)
	Internationales Hochschulinstitut
Zwickau	Westsächsische Hochschule Zwickau (FH)

TERMINE

03. bis 05. Februar 2004 **Hamburg**	**11. DFN-CERT/PCA Workshop 2004** *http://www.dfn-cert.de/events/ws/2004/*
09. bis 10. März 2004 **Berlin**	**40. Betriebstagung des DFN-Vereins** *http://www.dfn.de*
17. bis 19. März 2004 **Oxford, UK**	**16th IFIP International Conference on Testing of Communicating Systems** *http://www.testcom2004.org/*
18. bis 24. März 2004 **Hannover**	**CeBIT** *http://www.cebit.de*
17. bis 22. Mai 2004 **New York, USA**	**Thirteenth International World Wide Web Conference** *http://www2004.org/*
07. bis 10. Juni 2004 **Rhodos, Greece**	**TERENA Networking Conference 2004** *http://www.terena.nl*
15. Juni 2004 **Berlin**	**Festveranstaltung zur 48. Mitgliederversammlung "20 Jahr DFN"** *http://www.dfn.de*
16. Juni 2004 **Berlin**	**48. Mitgliederversammlung des DFN-Vereins** *http://www.dfn.de*