DFN Mitteilungen

73 | Dezember 2007

Neudefinition der Zeiteinheit

Fasergeführte optische Frequenzübertragung im X-WiN

Feuerprobe für DFN-PKI

Die Zertifizierungsstelle der FH Landshut in der DFN-PKI

Inhalt

IMPRESSUM

Herausgeber
Verein zur Förderung
eines Deutschen Forschungsnetzes e.V.
DFN-Verein
Stresemannstr. 78, 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
www.visius-design.de

Druck
D+S GmbH

Vorwort

Dr. Achim Bachem

Sprecher des Gauss Centre for Supercomputing und Vorstandsvorsitzender des Forschungszentrums Jülich

Im April haben Vertreter von HPC-Einrichtungen aus 14 europäischen Ländern in Berlin ein Memorandum of Understanding unterzeichnet, in dem sie sich dem gemeinsamen Ziel verpflichtet haben, eine nachhaltige paneuropäische HPC-Infrastruktur der höchsten Leistungsklasse aufzubauen. Deutschland wird in dieser Partnership for Advanced Computing in Europe - kurz PRACE - durch das Gauss Centre for Supercomputing vertreten.

Die gemeinsame Initiative ist ein großer Schritt für die europäische Wissenschaft. Herrschte vor kurzem noch das Gefühl, es fehle hierzulande an den Infrastrukturen und damit an den Möglichkeiten, die nordamerikanische Forschungseinrichtungen zu bieten haben, so stellt man heute fest: Wissenschaft hat in Europa Konjunktur.

In ungewohnt kurzer Zeit ist es gelungen, das Gauss Centre for Supercomputing (GCS) zu gründen. Mit diesem Schulterschluss der deutschen Höchstleistungsrechenzentren entsteht derzeit Europas leistungsstärkster Supercomputing Zentrum Rechenverbund.

Das Ziel des GCS ist, den Zusammenschluss auf nationaler Ebene nun auch europaweit zu vollziehen und mit PRACE ein gesamteuropäisches Konzept für den Aufbau eines europäischen Höchstleistungsrechenzentrums auf den Weg zu bringen.

Eine der Voraussetzungen für PRACE ist die Möglichkeit, in Europa über leistungsfähige Netze zu verfügen und ohne Engpässe über den gesamten Kontinent hinweg Daten zu transportieren. Das dies heute möglich ist, verdanken wir der Tatsache, dass die Entwicklung der Wissenschaftsnetze mit gleicher Energie vorangetrieben wird, wie die der Höchstleistungsrechner.

Noch niemals in der Vergangenheit hatten wir so gute Bedingungen, weltweit zusammenzuarbeiten und Ressourcen ortsunabhängig zu teilen. Darin liegt ein großes Versprechen für die Wissenschaft insgesamt.

Was das Gauss Centre for Supercomputing mit dem Deutschen Forschungsnetz über die nahe liegenden Aspekte des technischen Zusammenspiels verbindet ist von sehr grundsätzlicher Natur: Beide organisieren Zusammenarbeit und setzen auf die Nachhaltigkeit und auf die Stärke von Gemeinschaften.

Aktuell schiebt sich das Gauss Centre for Supercomputing mit seinem neuen Supercomputer JuGene am Standort Jülich an die Spitze der europäischen Rechenzentren und nimmt in der aktuellen TOP500-Liste der schnellsten Rechner den ersten Platz in Europa und den zweiten Platz in der Welt ein.

Herzliche Grüße

Ihr Achim Bachem

DFN-VPN

Große Bandbreiten zu festen Zielen

Sei es für die feste Kopplung mehrerer Supercomputer, für einen Verbund zur Datensicherung oder für die Verschmelzung mehrerer Standorte zu einem virtuellen Campus. Immer wenn eine Datenkommunikation zwischen vorher festgelegten Zielen erfolgen soll, sind fest geschaltete Verbindungen mit DFN-VPN die ideale Möglichkeit, um datenintensive Anwendungen zu bedienen. Schon im G-WiN wurden auf der Basis des dort bereitgestellten Punkt-zu-Punkt-Dienstes und für erste GRID-Projekte Virtuelle Private Netze (VPN) zur Unterstützung von besonderen Anforderungen an Datenkommunikations-Anwendungen neben dem DFNInternet-Dienst bereitgestellt. Mit den neuen Möglichkeiten der Plattform des X-WiN wurde diese Entwicklung ausgebaut. Der Beitrag beschreibt einige Beispiele von VPNs im X-WiN und soll Anregung für weitere Anwendungsfälle geben.

Anforderungen und Voraussetzungen

Virtuelle Private Netze (VPN) im X-WiN sind Netze, die auf der Basis der Plattform des X-WiN unabhängig vom DFNInternet-Dienst Nutzerdaten übertragen. Besondere Anforderungen an diese Netze sind zum Beispiel:

- hohes, anwenderspezifisches Datenaufkommen zwischen einer begrenzten Anzahl von Endpunkten
- zeitkritische Anwendungen

Mit dem X-WiN als Baukasten von unterschiedlichen technischen Optionen wurde eine geeignete Plattform für die bedarfsgerechte Gestaltung unterschiedlichster Anforderungen geschaffen. Es stehen mehr als 6.300 km Glasfasern zwischen den gegenwärtig 49 Standorten zur Verfügung. Über die eingesetzte DWDM-Technik können leistungsfähige Verbindungen (etwa mit 1GE oder 10GE) zwischen jedem dieser Standorte geschaltet werden. Modernste Routertechnik ergänzt die effektive Vermittlung von Bandbreiten bis zu 10 Gbit/s. Das Betriebsmodell des X-WiN begünstig den Aufbau von VPNs, da der DFN-Verein selbst als Netzbetreiber fungiert.

Im X-WiN wurden bisher folgende VPN-Grundtypen realisiert:

- VPN-Verbindungen werden nur über die optische Plattform des X-WiN bereitgestellt (optische VPNs).
- Die VPN-Verbindungen werden über die Routerplattform des X-WiN als Layer 2-VPN bereitgestellt.
- Die VPN-Verbindungen werden über die X-WiN-Infrastruktur als Intranet-VPN der Anwender genutzt.

Optische VPNs

VPNs, die über eigene Wellenlängen des X-WiN betrieben werden, werden auch als optische VPNs bezeichnet. Die Anwender schließen ihre Endgeräte direkt an die bereitgestellten Wellenlängen an. Die optischen Parameter der Anwenderschnittstellen sind single mode mit 1310 nm. Damit können vom DWDM-Gerät aus Anwender im Umkreis von ca. 10 km ohne zusätzliche Verstärkertechnik angeschlossen werden. Befinden sich die Endstellen des VPN nicht direkt an einem X-WiN-Standort, so werden die Wellenlängen durch eine geeignete Zugangsverbindung weitergeführt. Das können entweder Fasern oder gleichartige Wellenlängen eines anderen Betreibers sein. Die bereitgestellten Wellenlängen werden vom Betreiber der DWDM-Geräte überwacht und Störungen an den Überwacher gemeldet. Nutzer des VPN haben die Möglichkeit, Störungen „Rund-um-die-Uhr" an die Hotline des X-WiN-Überwachers zu melden. Bei Eingang von Störungsmeldungen werden die im Betriebshandbuch des X-WiN festgelegten Aktionen zur Störungsbehebung eingeleitet. Ein Nachteil der Punkt-zu-Punkt-Verbindung besteht darin, dass z. B. durch einen Faserbruch die Verbindung unterbrochen wird. Da Faserreparaturen gelegentlich zeitaufwendig sind, kann es dabei zu längeren Unterbrechungen kommen. Die im X-WiN eingesetzte DWDM-Technik ist aber in der Lage, durch sogenannte optische Protektion innerhalb von Millisekunden auf einen zuvor festgelegten Ersatzpfad zu schalten. Das Vorhalten eines Ersatzpfades ist mit zusätzlichen Kosten für das VPN verbunden.

Eines der ersten optischen VPNs war der Hochleistungsrechner-Verbund zwischen dem Konrad-Zuse-Zentrum (ZIB) in Berlin und dem Regionalen Rechenzentrum in Hannover (RRZN), das schon im G-WiN auf Wellenlängen des damaligen Kernnetzes realisiert wurde und nun im X-WiN zwischen den beiden Standorten am ZIB und RRZN (HAN) mit 1 GE geschaltet ist. Die optische Protektion dieser Wellenlänge hat schon oft wegen Störungen und Wartungen der Fasern für eine sichere Verbindung gesorgt. Da der Ersatzpfad aber deutlich länger als der Arbeitspfad ist, erhöhen sich dann allerdings die Laufzeiten.

Eines der leistungsfähigsten VPN wurde für die Kopplung europäischer Supercomputer im Rahmen des DEISA-Projektes aufgebaut (Distributed European Infrastructure for Supercomputing Applications). Für diese Forschungsinfrastruktur wurden über die DWDM-Infrastruktur des

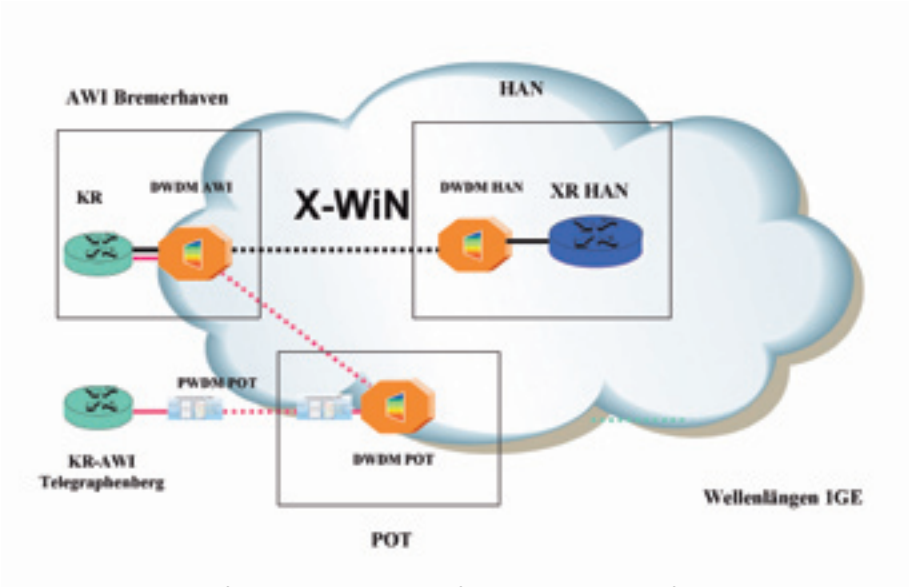
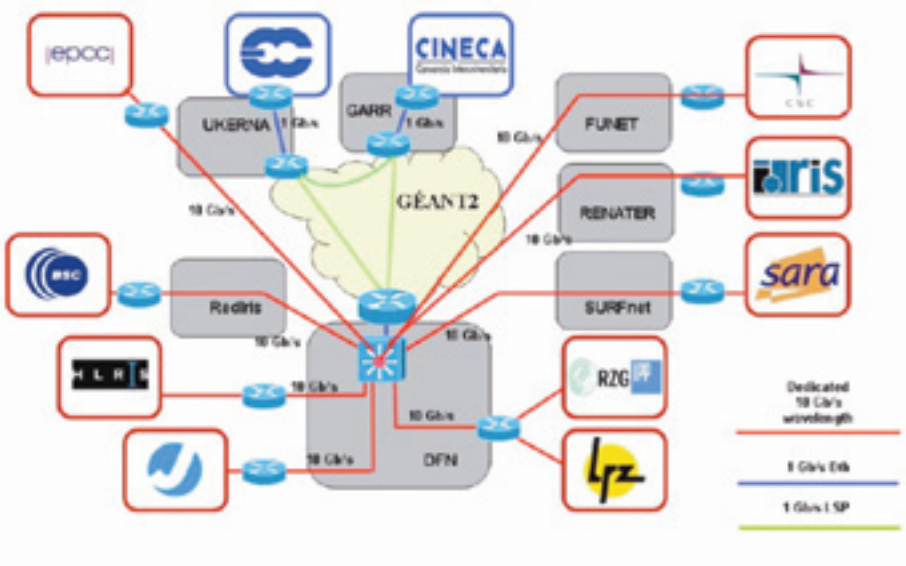


Abb. 1: Das VPN des Alfred-Wegener-Instituts für Polar- und Meeresforschung.

X-WiN mehrere 10GE-Punkt-zu-Punkt-Verbindungen zum DEISA-Switch am X-WiN-Standort in Frankfurt am Main geschaltet. Ein Teil dieser Wellenlängen wird in benachbarte Wissenschaftsnetze weitergeführt. Die VPN-Verbindungen im X-WiN sind optisch geschützt. Abbildung 2 zeigt die DEISA Infrastruktur.

Zwei interessante Lösungen wurden für die Einrichtungen der Alfred-Wegener-Institute (AWI) in Potsdam und in Bremerhaven sowie der Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig und Berlin geschaffen. Vom AWI auf dem Telegrafenberg in Potsdam wird über passive WDM-Geräte eine GE-Verbindung auf die DWDM-Technik am Standort an der Universität Potsdam (POT) geschaltet. Von dort geht es über eine GE-Verbindung zum Standort am AWI Bremerhaven (siehe Abbildung 1). Die beiden AWI-Einrichtungen nutzen die VPN-Verbindung sowohl für den internen Verkehr als auch für den Internet-Zugang des AWI Potsdam, der am AWI Bremerhaven ins X-WiN geleitet wird. Die beiden PTB-Einrichtungen nutzen die VPN-Verbindung nur für den internen Verkehr.

Abb. 2: Das VPN des europäischen Supercomputerverbundes DEISA erstreckt sich über sieben nationale Forschungsnetze und verbindet elf Einrichtungen in verschiedenen Ländern.



Layer2-VPNs

Für Anwendungen, deren Bandbreiten Anforderungen geringer als ein Gbit/s sind oder die sich nicht über Standorte realisiert lassen, die über DWDM-Technik des X-WiN verfügen, bilden die sogenannten Layer2-VPNs eine erfolgreiche Alternative. Auf der Basis von Ethernet-Verbindungen werden über die X-WiN-Routerinfrastruktur die geforderten Layer2-Verbindungen hergestellt. Der Vorteil diese VPNs ist, dass ihre Anschluss-Verbindungen in die aktive Überwachung des X-WiN einbezogen sind. Die Layer2-Tunnel durch das Kernnetz des X-WiN werden bei Ausfall einer Kernnetzverbindung auf andere Wege umgeschaltet, da die Signalisierung und das Forwarding über die Router-Infrastruktur erfolgt.

Ein typisches Beispiel eines Layer2-VPNs sind die Verbindungen der Standorte der Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) in Bonn, Berlin und Braunschweig mit Garching (Abbildung 3). Das VPN wurde ebenfalls schon im G-WiN über 34 Mbit/s-Verbindungen des damaligen Punkt-zu-Punkt-Dienstes realisiert. Da dieser Dienst im X-WiN nicht mehr genutzt werden konnte, wurde als Nachfolger das Layer-2-VPN aufgebaut. Die 3 Einrichtungen der GRS sind mit 50 Mbit/s Fastethernet-Verbindungen an die nächsten X-WiN-Router angeschlossen, die Garchinger Einrichtung mit 1GE. Zwischen den Standorten ist ein vollvermaschtes Netz geschaltet, über das ausschließlich interner Datenverkehr ausgetauscht wird.

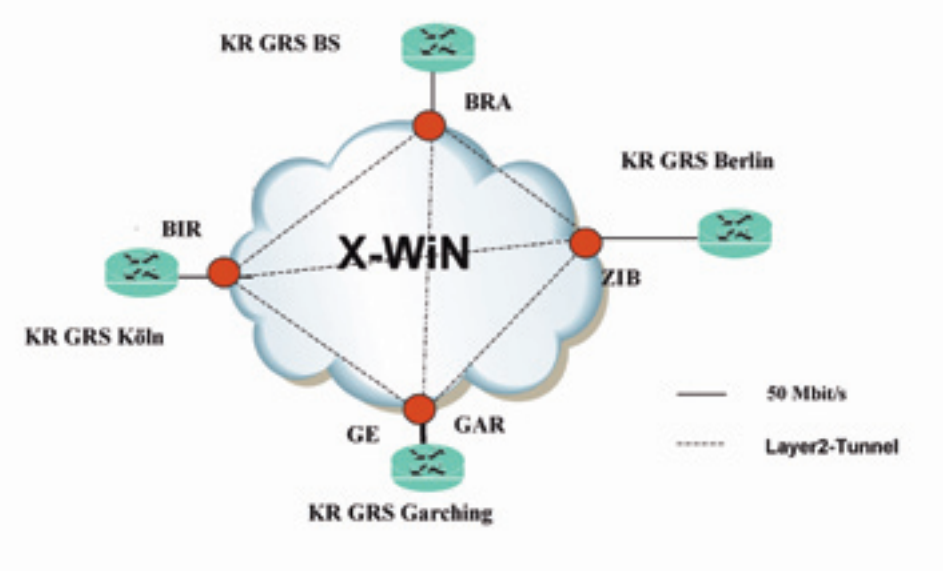


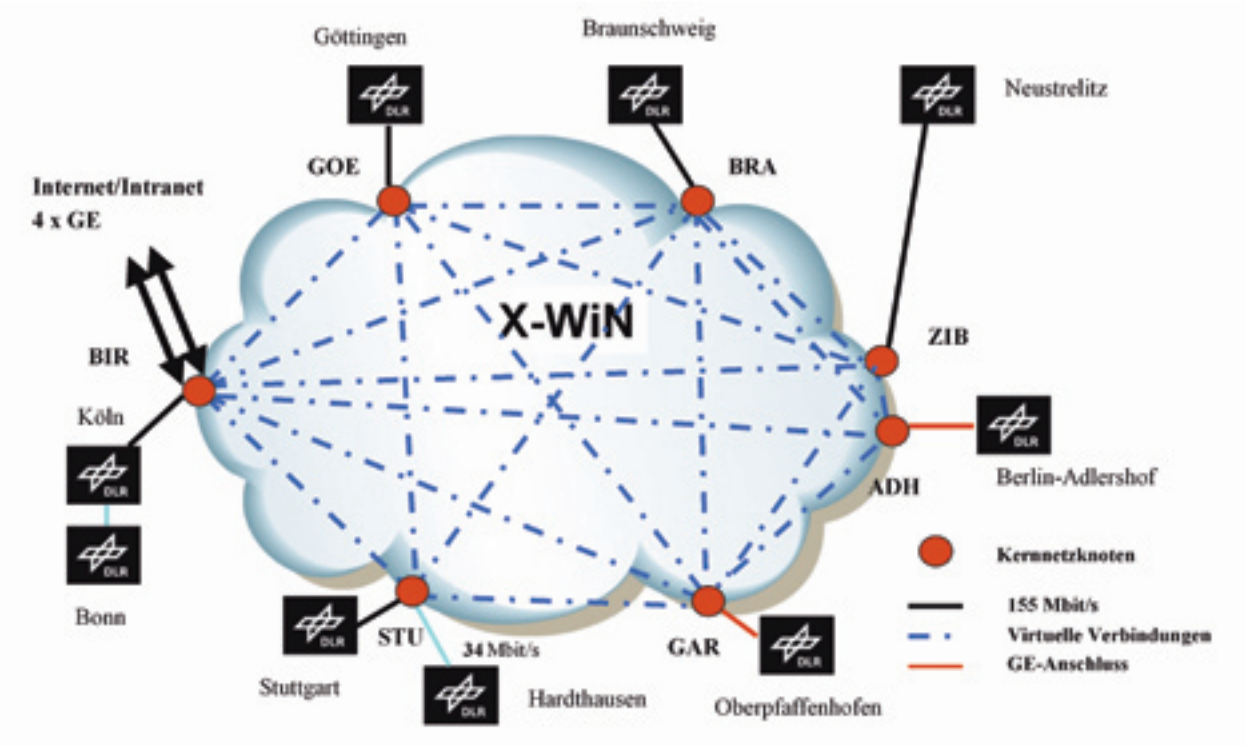
Abb. 3: Das Layer2-VPN der Gesellschaft für Anlagen- und Reaktorsicherheit: Alle Standorte sind voll miteinander vermascht.

Ein weiteres Beispiel ist das VPN für die beiden Max-Planck-Institute für Plasmaphysik in Garching und Greifswald. Zusätzlich zu den Internet-Dienst-Anschlüssen an den beiden Standorten wird ein 600 Mbit/s-Layer2-Tunnel zwischen beiden Einrichtungen zum Austausch von Backup-Daten genutzt. In Vorbereitung ist für den gleichen Zweck ein VPN zwischen der Universität Kassel und der Universität Frankfurt am Main.

Intranet-VPNs

Schon im G-WiN gab es Anforderungen von Anwendern, ihren verteilten Standorten den Zugang zum Internet nur an einem dieser Standorte zu gestatten und

Abb. 4: Das VPN der DLR besteht seit 2001 und verbindet neun größere Standorte und eine Reihe kleinerer Einrichtungen.



die anderen Standorte im Sinne eines Intranets auf diesen Standort zuzuführen. Für den sogenannten Haupt-Anschluss wurde eine entsprechende InternetDienst-Kategorie gewählt, die anderen Standorte wurden mit den geforderten Bandbereiten an den nächsten Standort des Wissenschaftsnetzes angeschlossen. Die Verbindung zum Hauptanschluss wurde in Verantwortung des Anwenders über entsprechende Tunnel realisiert. Alle Anschlüsse des VPNs sind in die Überwachung einbezogen.

Ein Beispiel für diesen VPN-Typ ist das Netz für das Deutsche Zentrum für Luft- und Raumfahrt (DLR). Die neun DLR-Standorte sind mit unterschiedlichen Bandbreiten von 34 Mbit/s bis zu 1 Gbit/s an die nächstgelegen X-WiN-Standorte angeschlossen. Die geschalteten Bandbreiten können voll genutzt werden. Der Verkehr aller DLR-Standorte wird zu den Servern der DLR in Birlinghoven geführt. Dort erfolgt dann auch der Übergang zum DFN-Internet-Dienst. Abbildung 4 zeigt das DLR-VPN.

Ein weiteres VPN diese Art nutzt das Forschungszentrum Jülich mit den Außenstandorten in Rostock und Berlin.

Ausblick

Die aufgeführten Beispiele zeigen die Vielfalt der VPNs im X-WiN. Natürlich sind auch Kombinationen der hier geschilderten Grundtypen möglich. Für Teilnehmer des Deutschen Forschungsnetzes, die DFN-VPN in Anspruch nehmen wollen, erstellt die Geschäftsstelle des DFN-Vereins ein technisches Konzept und ermittelt die damit verbundenen Kosten.

Hans-Martin Adler

DFN-Verein
adler@dfn.de

Seit 2001 in Betrieb: Das VPN der DLR

Die DLR ist einer der Vorreiter bei der Nutzung von VPNs im Wissenschaftsnetz. Schon im Jahr 2001 kurz nach dem Start des G-WiN, hat die DLR mit der Vernetzung ihrer Standorte begonnen. Anfangs ging es dabei in erster Linie um den reinen Datentransport. Heute hingegen stehen die Vorteile von VPNs in punkto Datensicherheit und die Virtualisierung von Netzen im Vordergrund. Aktuell existieren neun größere Standorte, die mit bis zu 1 Gbit/s untereinander vernetzt sind, sowie eine Reihe kleinerer Standorte. Darunter sind auch auch einige, die mit einer Bandbreite von bis zu 100 Mbit/s per Standleitung an die nächsten größeren Standorte angeschlossen sind.

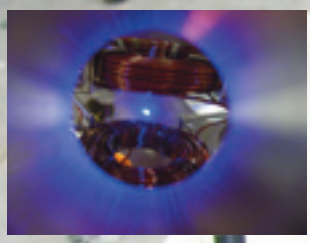
Auf der Basis der physischen Transportkanäle werden in der DLR verschiedene Netze realisiert, die z.B. unterschiedliche Sicherheitsniveaus haben. Neben dem geschützten Intranet der DLR, zu dem ausschließlich Mitarbeiter Zugang haben gibt z.B. ein „öffentliches" Netz für Besucher, die sich über ihr eigenes, virtuelles Netz in der DLR bewegen. Darüber hinaus gibt es auch ein Fremdfirmen-LAN, das von Firmen genutzt wird, die auf dem Campus der DLR angesiedelt sind, aber organisatorisch nicht zu ihr gehören. So finden sich relativ viele Ausgründungen, die an DLR Standorten residieren, aber eigene GmbHs geworden sind.

Derzeit sind es 5.000 Mitarbeiter und insgesamt 10.000 Rechner, die die verschiedenen Netzwerke nutzen. Für alle LANs gibt es eine gemeinsame Schnittstelle nach außen. Dies ist der zentrale Internetzugang in Birlinghoven.

Für den Betrieb des VPN werden in der DLR kaum Ressourcen oder zusätzliche Stellen benötigt. Da über die jahrelange Erfahrung ein großes Know-How vorhanden ist, werden nur ein paar technische Ressourcen, wie etwa Router mit Hardware-Verschlüsselung und VPN-Encrypt-Modulen benötigt.

Technisch gesehen handelt es sich beim VPN der DLR um ein voll vermaschtes Netz ohne zentralen Knoten, bei dem alle Standorte direkt untereinander verbunden sind. Dadurch hat das Netz außerordentlich geringe Latenzzeiten, was spürbar wird, wenn externe Fileserver oder anspruchsvolle AV-Anwendungen über das Netz genutzt werden, da zentrale Knoten die Datenströme z.B. bei VoIP oder Videoconferencing beeinträchtigen können.

Das Deutsche Forschungsnetz hat für Wissenschaftseinrichtungen beim Thema VPN gleich mehrere Vorteile: So ist das X-WiN fast an allen Wissenschaftsstandorten verfügbar, was die Kosten bei der Beschaffung von Fasern verringert. Eine große Rolle spielt auch die internationale Verknüpfung mit den Wissenschaftsnetzen anderer Nationen. Wissenschaftseinrichtungen haben mit dem DFN die Flexibilität, bei Bedarf Standorte im Ausland einzubinden. Darüber hinaus hat das X-WiN eine sehr hohe Betriebsstabilität und verfügt über die Leistungsparameter, die in der Wissenschaft benötigt werden.



Neudefinition der Zeiteinheit

Fasergeführte optische Frequenzübertragung im X-WiN

Eine Uhr, egal ob Sonnenuhr, Sanduhr, Pendeluhr, Quarzuhr oder Caesium-Atomuhr, besteht immer aus zwei Komponenten: Einem Oszillator, der möglichst gleichmäßig schwingt, und einem Zähler, der diese Schwingungen mitzählt und nach einer gewissen Anzahl zum Beispiel den Sekundenzeiger um eine Einheit weiter bewegt.

Dabei gilt, dass je schneller der Oszillator einer Uhr schwingt, desto genauer geht die Uhr. Während die Sonnenuhr als frühester vom Menschen genutzter Zeitmesser mit einer Frequenz von einem Tag „schwingt", übernimmt bei der Atomuhr die Strahlungsfrequenz des Caesium-Atoms die Aufgabe des Pendels. Dieses Pendel geht mit 9.192.631.770 Schwingungen so genau, dass die Caesium-Uhr nur alle 30 Millionen Jahre eine Abweichung von 1 Sekunde hat.

Eine weitere Steigerung der Genauigkeit wird mit Atomuhren erreicht, deren Oszillator mit der Frequenz sichtbaren Lichtes schwingt. Licht mit einer Wellenlänge von 500 Nanometern hat eine Fre-

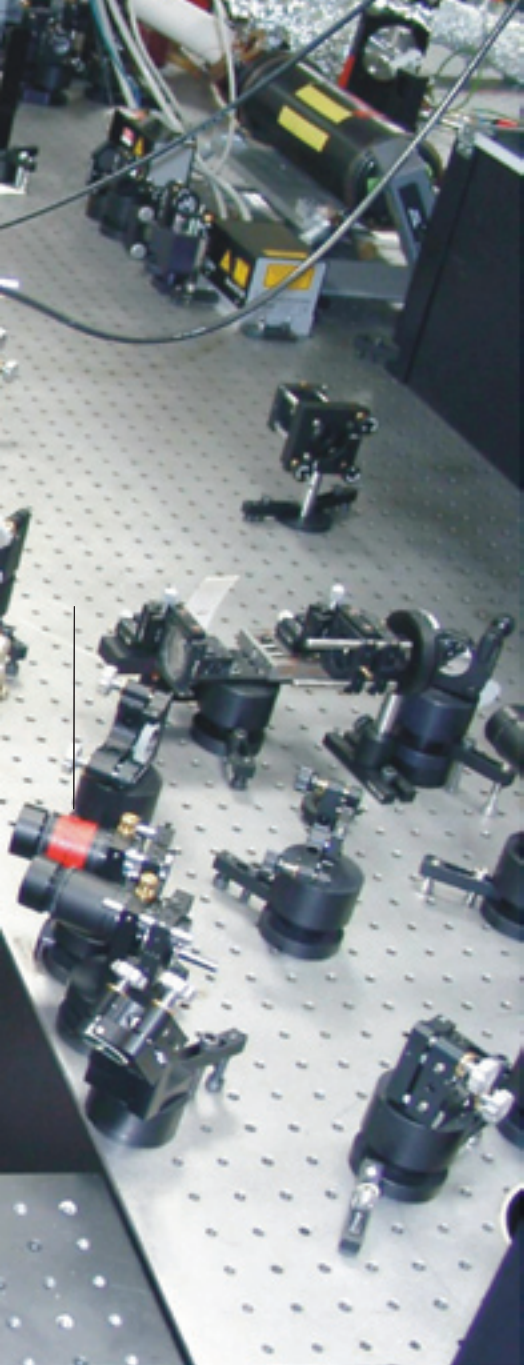


Abbildung 1: *Vakuumapparatur für die neue Generation der Atomuhren (optische Gitteruhr) der PTB. Das Detailbild zeigt in einer magnetoptischen Falle gespeicherte Atome.*

Abbildung 2: *Nach jedem Umlauf in der Spiegelanordnung eines Titan:Saphir Lasers (unten links) verlässt eine Kopie des umlaufenden Pulses den Laser durch einen teildurchlässigen Spiegel. Der dadurch entstehende Pulszug lässt sich mithilfe der Frequenzkammtechnik derart mit der Welle eines Einfarbenlasers (oben links) synchronisieren, dass beispielsweise genau eine Million Zyklen dieses Lasers zwischen zwei Pulsen liegen. Ist dies erreicht, so muss nur noch die Anzahl der kurzen Pulse pro Zeiteinheit, die jetzt im Gigahertzbereich liegt und damit einer elektronischen Erfassung zugänglich ist, gezählt und die sich daraus ergebende Frequenz mit einer Million multipliziert werden. Der Name der Technik rührt daher, dass der spektrale (Frequenz-) Gehalt des von dem Pulslaser emittierten Lichtes eine Struktur aufweist, die einem Kamm mit scharfen äquidistanten „Zinken" ähnelt.*

quenz von 600.000 Gigahertz und erlaubt damit eine wesentlich feinere Unterteilung der Zeitskala als herkömmliche Atomuhren. Das große Problem war lange Zeit allerdings, dass es keine Möglichkeit gab diese Schwingungen direkt mit elektronischen Geräten zu zählen (Die besten elektronischen Frequenzzähler arbeiten bis zu ein paar hundert Gigahertz). Aufwändige Frequenzketten, wie sie nur in Staatsinstituten realisiert werden konnten, erlaubten es zwar, eine gezielte Frequenz hochgenau zu messen, aber der Siegeszug der optischen Uhren begann erst mit der am Max-Planck-Institut für Quantenoptik in Garching entwickelten Frequenzkammtechnik, für die Professor Theodor Hänsch 2005 den Nobelpreis für Physik erhielt.

Ein Frequenzkamm besteht aus einem Ultrakurzpulslaser, der Pulse mit einer Dauer von wenigen zehn Femtosekunden in immer genau gleichem zeitlichen Abstand emittiert. Die Schwierigkeit, die extrem schnellen Schwingungen des Lichtes zu zählen, wird bei der Frequenzkammtechnik mit folgendem Trick überlistet: Hochfrequentes sichtbares Licht wird einer (niederfrequenten) Frequenzkomponente des Frequenzkamms zugeordnet, deren Frequenz in einem ganzzahligen Verhältnis zur optischen Frequenz steht, z.B. genau ein Millionstel beträgt, und daher mit elektronischen Mitteln erfasst werden kann.

Damit lassen sich Frequenzmessungen höchster Präzision durchführen und hochgenaue „optische Atomuhren" realisieren, die in naher Zukunft zu einer Neudefinition der Basiseinheit „Sekunde" führen werden. Neben neuen Anwendungen in der Geologie sind damit beispielsweise auch neue Erkenntnisse zu fundamentalen physikalischen Theorien zu erwarten.

Übertragung von Referenzmessungen

Um das Potenzial optischer Uhren voll auszuschöpfen, ist es erforderlich, diese mit z.T. unterschiedlichen optischen Frequenzen und an unterschiedlichen Standorten betriebenen Uhren direkt miteinander vergleichen zu können. Ähnlich wie bei dem Problem elektronischer Messungen von Frequenzen mit höherer „optischer" Genauigkeit stößt auch die Übermittlung der optischen Frequenzen schnell an ihre Grenzen, weil jeder elektronische Übertragungsweg die Präzision der übermittelten Messungen beeinflussen würde. Herkömmliche Frequenzvergleiche mit Hilfe von Mikrowellennormalen und Satelliten können die erforderliche Genauigkeit und Stabilität nicht gewährleisten. Außerdem steht diese Technologie aufgrund der Komplexität der erforderlichen Messeinrichtungen und Datenaufbereitung wiederum nur den Staatsinstituten zur Verfügung.

Um die überragende Stabilität optischer Uhren für andere Anwender nutzbar machen zu können, wird daher die Suche nach einer für größere Entfernungen geeigneten Vergleichsmethode zu einem der zentralen Punkte der neuen Generation von Atomuhren. Für Fragestellungen in der Metrologie, fundamentalen Physik und Astronomie ist ein Frequenzvergleich mit einer Unsicherheit im Bereich von $< 10^{-15}$ innerhalb Europas oder auch transatlantisch von großer praktischer Relevanz.

Eine Möglichkeit, Frequenznormale mit höchster Genauigkeit untereinander zu vergleichen und höchstpräzise Frequenzen an Industrie und Forschungseinrichtungen weiterzugeben, ist die Übertragung hochstabiler optischer Frequenzen über Glasfasern, wie sie für die optische Telekommunikation verwendet werden. Sie sind unterirdisch verlegt, gut geschützt und weisen eine geringe Dämpfung von etwa 0,25 dB pro Kilometer für Strahlung im nahen Infrarot-Bereich auf.

Glasfasern als Übertragungskanäle

Das Konzept zum Vergleich optischer Uhren per Glasfaser ist in der Physikalisch Technischen Bundesanstalt PTB in Braunschweig entwickelt und bereits an einer Glasfaserstrecke erprobt worden.

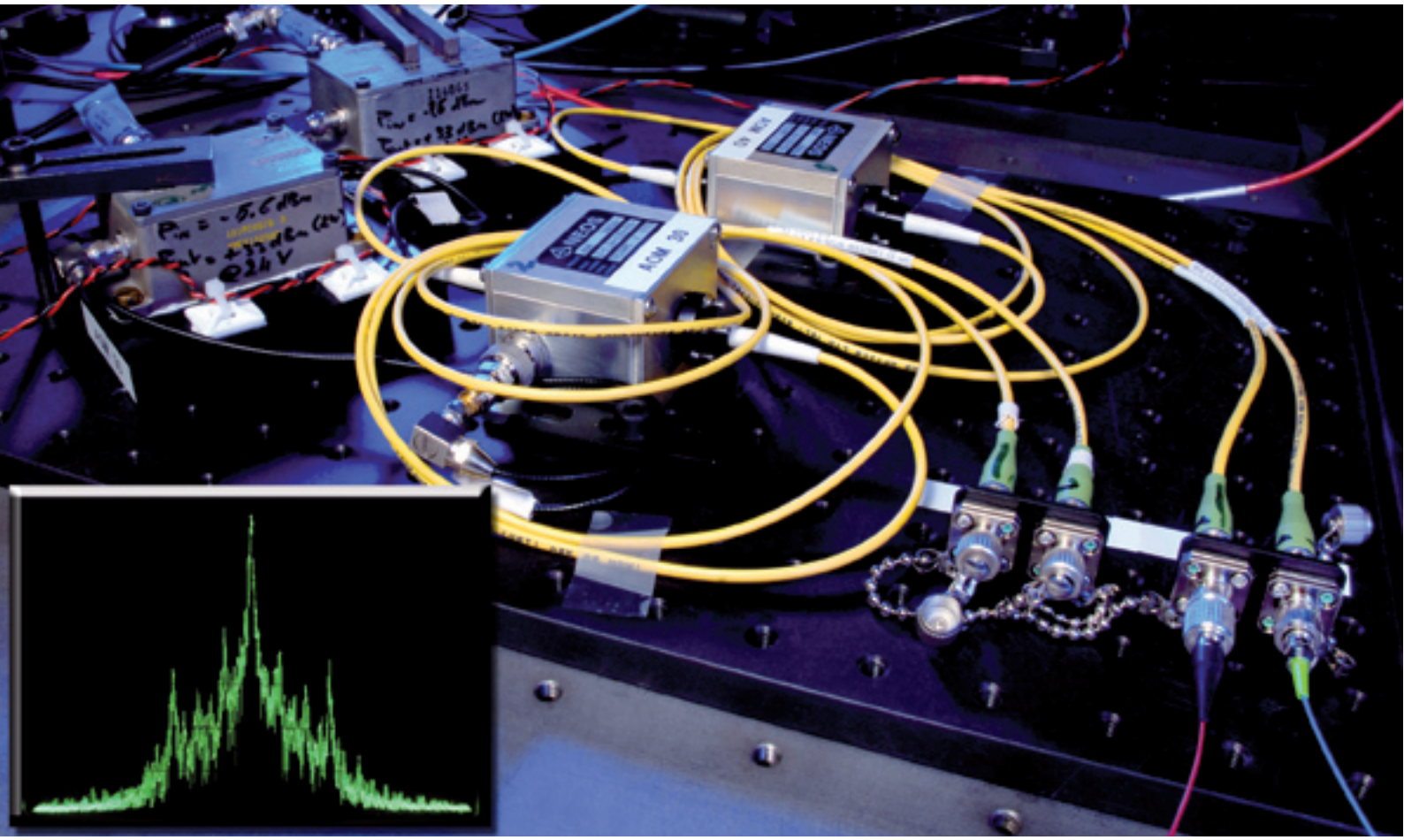


***Abbildung 3**: Interferometer mit fasergekoppelten, akusto-optischen Modulatoren detektiert Schwankungen der optischen Weglänge in der Übertragungsfaser.*

Hierbei wurde ein Dauerstrichlaser (cw-Laser) mit einer Wellenlänge nahe 1.5 µm mit Hilfe eines Frequenzkammgenerators phasenverfolgbar an die optische Uhr gekoppelt, so dass die optische Frequenz des cw-Transferlasers als Träger für die Frequenzinformation der optischen Uhr genutzt werden kann.

Eine so synthetisierte optische Frequenz wurde bereits im Rahmen einer internationalen Kooperation in eine Glasfaserstrecke von 86 km Länge eingespeist, die zwei Forschungsinstitute in Paris miteinander verbindet. Durch zusätzliche Faserspulen wurde die Strecke bis auf insgesamt 211 km verlängert.

Ein Problem musste das Froscherteam allerdings zuvor lösen: Wegen mechanischer, akustischer und thermischer Einflüsse auf die optische Faser schwankt die optische Weglänge, was sich am Ende der Übertragungsstrecke durch Frequenzfluktuationen bemerkbar macht. Diese Einflüsse wurden zunächst in Laborexperimenten simuliert und die gewonnenen Erkenntnisse an einem Testsystem, einem ca. 50 km langen Glasfaserring in Braunschweig überprüft. Auf Grundlage der gewonnenen Erfahrungen konnten dann die Störungen auf der Glasfaserstrecke in Paris interferometrisch erfasst und um etwa drei Größenordnungen unterdrückt werden, so dass die glasfasergestützte Frequenzübertragung eine Unsicherheit von etwa $1\ 10^{-17}$ erreichte.

Mit der Umsetzung und Übertragung einer optischen Trägerfrequenz steht der PTB ein weltweit einzigartiges Verfahren zum Vergleich von Frequenznormalen auch über weite Strecken zur Verfügung.

Es eröffnet gleichzeitig die Möglichkeit, Referenzfrequenzen an Forschungslaboratorien zu verteilen und für grundlegende Fragestellungen der Physik nutzbar zu machen.

Das X-WiN als wissenschaftliche Kooperation

Die Vision eines von der PTB initiierten Projektes ist nun, über die Glasfaser-Plattform des X-WiN des Deutschen Forschungsnetzes DFN eine Infrastruktur zu schaffen, die weitreichende Möglichkeiten für die zukünftige Übertragung und den Vergleich der Frequenz optischer Uhren bietet.

Ziel des Projektes ist die Realisierung einer optischen Verbindung zur Übertragung möglichst schwankungsarmer Frequenz-/Zeitinformation zwischen der PTB und anderen Instituten, die über ein optisches Frequenznormal und einen Frequenzkamm verfügen. Als Kooperationspartner der PTB kommen in Deutschland insbesondere drei Institute in Frage: das Institut für Quantenoptik der Universität Hannover, das Institute of Optics, Information and Photonics (Max Planck Research Group) der Universität Erlangen-Nürnberg und das Max-Planck-Institut für Quantenoptik in Garching.

Das X-WiN unterhält direkte Verbindungen zwischen Kernnetzknoten in den Rechenzentren der Universitäten Hannover und Erlangen und zum Max-Planck-Rechenzentrum in Garching. Da in aller Regel bereits Glasfasertrassen zwischen den

beteiligten Instituten und den Rechenzentren (Netzknoten) vorhanden sind, lassen sich Verbindungen mit den optischen Uhren der PTB relativ einfach realisieren.

Betrachtet man jedoch die physikalischen Rahmenbedingungen dieses ehrgeizigen Projektes, so erkennt man sofort, dass es aufgrund der Dämpfung der Signale nicht möglich ist, Distanzen von vielen 100 Kilometern in einem Schritt zu überbrücken. Die Übertragungsstrecke benötigt etwa alle 100 - 150 km ein Signalkonditioniermodul in Form eines phasengekoppelten cw-Lasers oder einer schmalbandigen Verstärkerstufe, das das akkumulierte Rauschen abstreift und das Nutzsignal verstärkt. Bei einer Faserlänge von ca. 800-900 km werden daher voraussichtlich 5 - 6 solcher Transfermodule benötigt.

Die Verfügbarkeit des X-Win erlaubt die relativ einfache Vernetzung der deutschen Forschungsstandorte, aber in einer zukünftigen Ausbaustufe könnten auch unter Einbeziehung weiterer nationaler Forschungsnetze wie RENATER oder UKERNA Institute innerhalb Europas, wie das Laboratoire Systèmes de Référence Temps-Espace (SYRTE) in Paris mit 1200 km Faserlänge oder das National Physical Laboratory (NPL) in London, eingebunden werden.

Ausblick

Ähnlich der klassischen Zeitverteilung über GPS oder DCF77, mit dem viele herkömmliche Uhren und Wecker per Funk die „richtige Zeit" empfangen, kann die Verbreitung einer optischen Referenz per Glasfaser unter dem Stichwort „Meter aus der Steckdose" zur Rückführung der Wellenlänge bzw. Frequenz optischer Strahlung eine breite Anwendung in Forschung und Industrie finden.

In der angewandten Längenmesstechnik ermöglicht die Übertragung über das Wissenschaftsnetz die Rückführung der Längeneinheit für die Interferometrie, und in der Breitband-Kommunikationstechnik selbst könnten rauscharme Referenzsignale zur Synchronisation zur Verfügung gestellt werden.

Darüber hinaus könnte das Verfahren auch im Rahmen von Very-Long-Baseline-Interferometrie (VLBI) eingesetzt werden. VLBI ist eine Methode der Radioastronomie für Messungen mit höchster räumlicher Auflösung und Positionsgenauigkeit. Sie dient sowohl für astronomische Beobachtungen als auch für geodätische Untersuchungen im Gebiet der Erdmessung. Hierbei werden Signale einzelner Antennen zusammen mit sehr genauen Zeitreferenzen gespeichert und später rechnerisch korreliert. Dadurch ist es möglich, Interferenzen über interkontinentale Entfernungen oder sogar mit Antennen im Weltraum (Weltraum-VLBI) zu erhalten. Durch Anmessen mehrerer Quasare wird eine Art Vermessungsnetz aufgebaut. Weil sich die einzelnen Laufzeitunterschiede der Messungen durch die Erdrotation dauernd ändern, kann mit Hilfe präziserer Zeitreferenzen außer den Koordinaten der Quasare auch der momentane Rotationspol und die astronomische Zeit wesentlich genauer bestimmt werden als bisher.

In der Frequenzmetrologie werden aufwändige Schwungrad-Oszillatoren zur Überbrückung von Laufzeitschwankungen entfallen. Vor allem wird der Zugang entfernt liegender Anwender zu hochpräziser Referenzfrequenz möglich.

Mit dem hier beschriebenen Verfahren können stabile optischen Frequenzen mit einer Qualität verteilt werden, wie sie sonst nur Forschungsinstituten zur Verfügung steht.

Damit kann ein Anwender auch vor Ort mit Hilfe des Frequenzkamms direkt seine eigene elektrische Referenzfrequenz erzeugen, die alle bisher zur Verfügung stehenden Quellen an Stabilität bei weitem übertrifft.

Die Verwendung bestehender Glasfaserinfrastruktur, wie sie in den nationalen Forschungsnetzen vorgehalten wird, ermöglicht in Zukunft eine Erweiterung zu einem EuroNetz, in dem alle optischen Uhren in Europa untereinander verglichen werden können.

Dr. Harald Schnatz

Physikalisch Technische Bundesanstalt Braunschweig

Dr. Gesine Grosche

Physikalisch Technische Bundesanstalt Braunschweig

Katharina Predehl

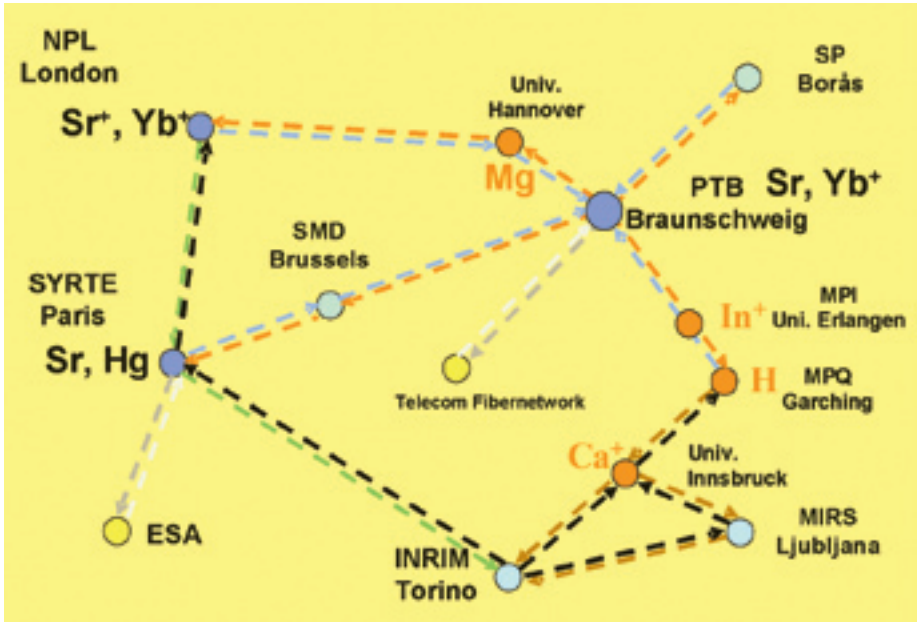
Max Planck Institut für Quantenoptik Garching

Dr. Ronald Holzwarth

Max Planck Institut für Quantenoptik Garching

Kontakt: Harald.Schnatz@ptb.de

Abbildung 4: *Vision eines europäischen Glasfasernetzwerkes zum Vergleich optischer Uhren*



Nie mehr unscharf

Neues vom DFN-Videokonferenzdienst

Der DFN-Verein ist in ein neues Zeitalter gestartet: High Definition (HD) heißt das Zauberwort. Nachdem das Label „HD ready" in der Consumer Welt schon länger auf jedem Fernseher prangt, haben auch die Hersteller von Videokonferenz-Systemen nachgezogen. Wir merken es an den Anfragen unserer Nutzer und an den Angeboten auf dem Markt: HD ist in aller Munde. Der DFN-Verein hat sich dieser Herausforderung gestellt und in die entsprechende Infrastruktur investiert. Im folgenden werden die neuen Angebote im Videokonferenzdienst (DFNVC) erläutert.

Videokonferenzen in High Definition Qualität

Ausgangspunkt war die rege Nachfrage von DFNVC-Nutzern nach Testergebnissen von Videokonferenzsystemen aus dem HD-Bereich. Die aktuellen Arbeiten des Kompetenzzentrums für Videokonferenzdienste (VCC) in Dresden betrafen im letzten Jahr– was die Tests von VC-Systemen betrifft – fast ausschließlich HD-Systeme der verschiedenen Hersteller (LifeSize, Polycom, Aethra, Tandberg, Sony). Insofern ist absehbar, dass der Marktanteil an HD-fähigen Systemen in den DFN-Einrichtungen stetig zunehmen wird. Will man sich mit diesen Systemen an einer Multipoint-Konferenz beteiligen, bedarf es einer leistungsstarken MCU's mit den entsprechenden Funktionen.

Der DFN-Verein hat im letzten halben Jahr nicht nur die MCU-Kapazität, sondern auch die MCU-Qualität gesteigert, indem die bisherigen Codian MCUs 4220 gegen High Definition MCUs 4520 ausgetauscht wurden (Abb. 1). Die Codian 4500- Serie ermöglicht derzeit als einzige MCU auf dem Markt hochauflösende Videokonferenzen mit HD-Qualität. HD bedeutet derzeit in Videokonferenzen eine Bildauflösung von 1280x720p Bildpunkten mit 30 Bildern pro Sekunde (fps). Das Ganze erfolgt mit dem Bandbreite-sparenden Protokoll H.264 im Continuous Presence Mode, d.h., bis zu 16 Teilnehmer können gleichzeitig dargestellt

***Abb. 1:** Codian HD MCU*

werden. Einen Eindruck für die verschiedenen Bildauflösungen von QCIF (176x144) über CIF (352x288) und 4CIF (704x576) bis zu HD720p kann man sich mit Hilfe der Abb. 3 verschaffen. Codian hat angekündigt, in Zukunft auch HD720p mit 60 fps und Full HD (1920x1080p) mit 30 fps zu unterstützen. Die Datenübertragung über das Protokoll H.239 erfolgt ebenfalls in HD

***Abb. 2:** Szenarien von Videokonferenzen mit integrierter Datenübertragung*

***Abb. 3:** Eindruck von den Bildschirmauflösungen QCIF, CIF, 4CIF und HD720p*
Copyright © Codian 2006

Dual Video Qualität (Abb. 2). Den Nutzern des DFNVC-Dienstes stehen insgesamt 120 Video-Ports und 120 Audio-Ports auf den neuen MCUs zur Verfügung.

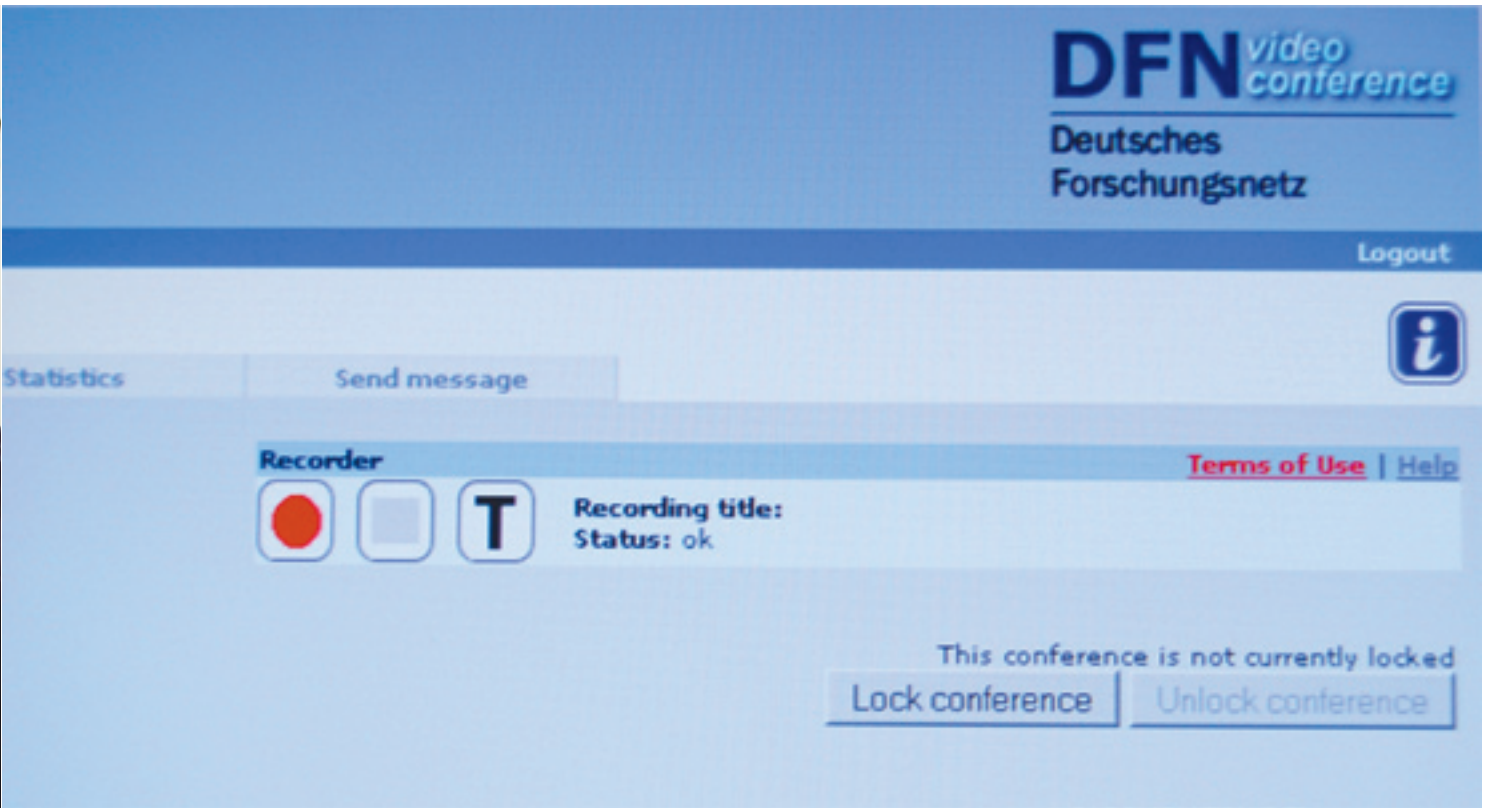
Auflösung Input	Auflösung Output
QCIF (Quarter CIF) - 144p	CIF (Common Intermediate Format) - 288p
CIF - 288p	4CIF - 567p
448p	672p
480	HD720p

***Tabelle 1:** Verbesserung der Auflösung mit ClearVisionTM*

Zum ersten Mal ist es möglich, alle Endsysteme nach ihren jeweiligen Fähigkeiten an den Konferenzen zu beteiligen, und sowohl für HD-Systeme als auch für SD- (Standard Definition) Systeme die bestmögliche Qualität herauszuholen. Wie wird das erreicht? Das neueste Feature der Codian MCU 4500 Serie nennt sich ClearVision™ und erhöht die Auflösung und Qualität älterer Videokonferenz-Systeme bis auf das 4-fache (Tabelle1). Dies ist unter anderem durch die starke Prozessorleistung der 4500-Serie möglich.

Die Qualität der HD-Systeme wird erstmalig nicht reduziert, wenn sich qualitativ schlechtere Systeme in der Konferenz befinden. Bisher konnten HD-Systeme in diesem Fall nur maximal 4CIF empfangen, jetzt können sie mit dem Codian Feature 720p empfangen und werden somit optimal genutzt. Aber auch die SD-Systeme erfahren durch die verbesserte Auflösung eine wesentliche Qualitätssteigerung. Und erstmalig kann die MCU viele SD Bilder zu einem großen HD Bild kombinieren.

***Abb. 4:** Aufzeichnung von Videokonferenzen über die MCU-Oberfläche.*



Aufzeichnen von Videokonferenzen

Für die Aufzeichnung von Konferenzen steht seit kurzem ein in den DFNVC-Dienst integrierter Codian IPVCR-Recorder zur Verfügung. Maximal können bis zu 5 Konferenzen parallel aufgezeichnet werden. Die Bedienung des Recorders erfolgt sehr einfach über den Button „Steuerung" auf dem DFNVC-Portal, über den der Konferenzadministrator - wie bisher schon gewohnt – die Konferenz steuern kann. Auf der MCU-Oberfläche befindet sich nun ein zusätzliches Bedienungsfeld für das Starten und Beenden einer Aufzeichnung sowie für die Eingabe eines Aufnahmetitels (Abb. 5 und 6). Beim Start der Aufnahme wird 30 Sekunden lang im Videobild der Teilnehmer ein Hinweis auf die Aufzeichnung eingeblendet, und während der gesamten Aufnahme ist im Videobild links oben ein roter Punkt eingeblendet. Der Konferenzadministrator muss vor dem Starten der Aufzeichnung den Nutzungsbedingungen zustimmen.

Nach Beendigung der Aufnahme steht die Datei 14 Tage über das Webinterface in MPEG-1 (Fernsehformat mit 720x576 Bildpunkten) oder im Codian-Format zum Download bereit. Danach wird sie automatisch gelöscht. Der Zugang auf das DFNVC-Portal ist selbstverständlich passwortgeschützt. Und noch ein Hinweis zur Qualität der Aufzeichnungen: Der Recorder ist HD-fähig und kann Videobilder in HD-Qualität (720p) aufzeichnen.

Für Teilnehmer, die sich über ein ISDN-System in eine Videokonferenz einwählen, gibt es ebenfalls eine Verbesserung. Mit den neuen Codian ISDN-Gateways der Serie 3200 stehen leistungsstärkere Systeme zur Verfügung, die höhere Bandbreiten und eine verbesserte Audio- und Video-Qualität ermöglichen.

Insgesamt erfreut sich der DFNVC-Dienst wachsender Beliebtheit, was sich in stark gestiegenen Nutzungszahlen gegenüber dem Vorjahr ausdrückt. 145 Einrichtungen nutzen derzeit das Dienstangebot des DFN-Vereins. Mit den neuen Funktionen und Qualitäten des Dienstes wird das Angebot für die DFN-Nutzer noch attraktiver. Wie in der Vergangenheit können Sie sich bei Fragen rund um den Dienst an die DFN-Geschäftsstelle wenden. Das VCC in Dresden unterstützt Sie bei der Auswahl von VC-Systemen und stellt umfangreiche Testergebnisse auf den Webseiten bereit.

Abb. 5: Videokonferenz ohne ClearVisionTM.

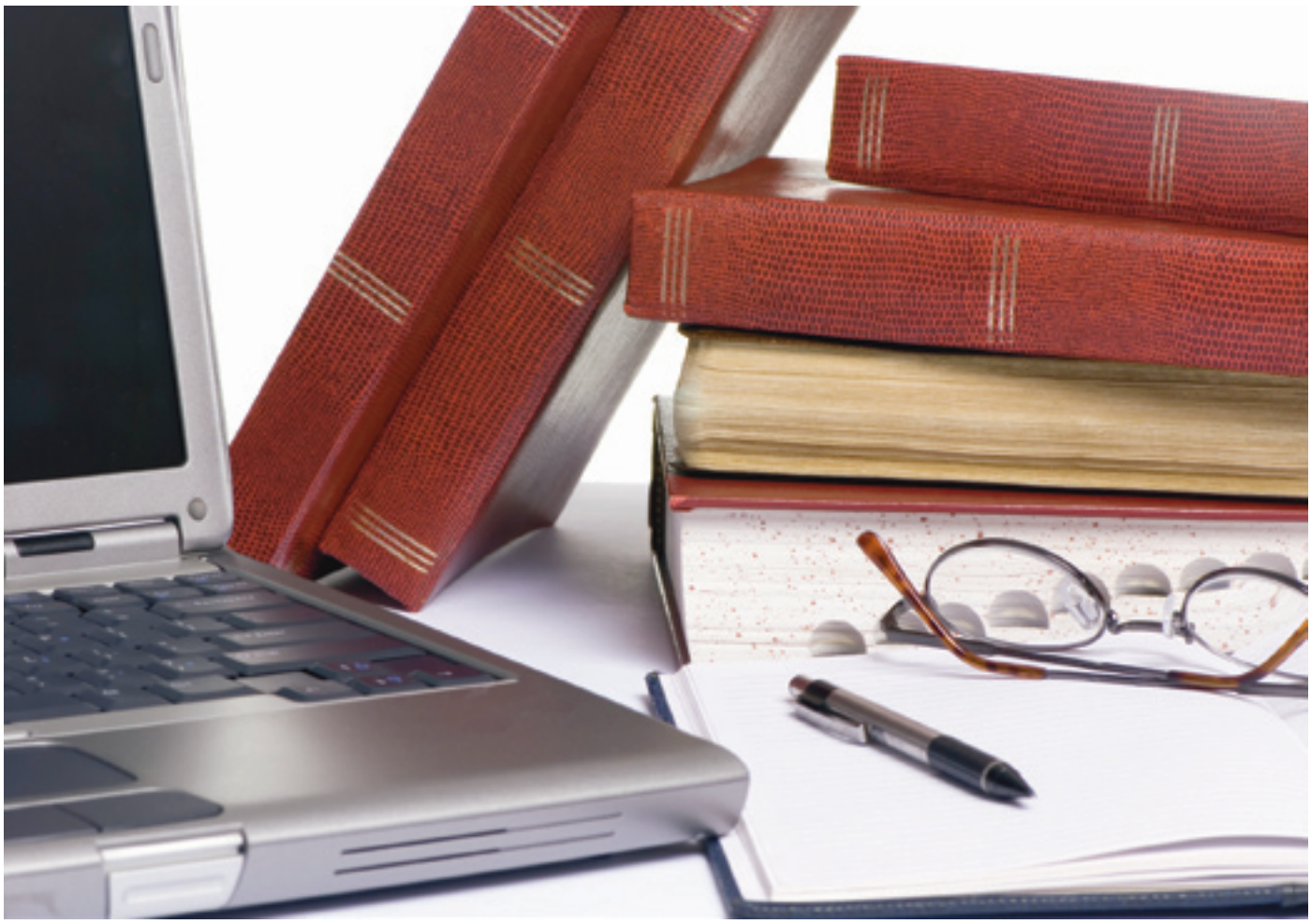
Abb. 6: Videokonferenz mit ClearVisionTM.

Weitere Informationen zum Dienst:

http://www.vc.dfn.de
http://vcc.zih.tu-dresden.de
EMail: hotline@vc.dfn.de
Telefon: 0711-63314-214

Gisela Maiß

DFN-Verein
maiss@dfn.de



Start frei für DFN-AAI

DFN-AAI geht in den Produktionsbetrieb

Im November 2007 wurde der Produktionsbetrieb der DFN-AAI aufgenommen. Nachdem im voraus bereits eine Reihe von Einrichtungen erfolgreich mit ihren Installationen das DFN-Testsystem durchlaufen und auch die vertraglichen Regelungen mit dem DFN-Verein getroffen hatten, war durch die Freigabe der für den Betrieb notwendigen zentralen Komponenten der Weg frei für den Start der Produktionsföderation. Damit ist ein wesentlicher Meilenstein für den Aufbau der DFN-AAI erreicht. Bereits seit Frühjahr 2007 lag der Vertrag für die Teilnehmer an der DFN-AAI vor, seit Oktober gibt es nun auch den entsprechenden Vertrag für die Ressourcenanbieter. Hierzu wurde der Vertrag der Kollegen des Schweizer Forschungsnetzes SWITCH als Vorbild genommen und auf DFN-Verhältnisse angepasst. Bereits kurz nach Veröffentlichung der Verträge gibt es sowohl von Teilnehmern aus dem Forschungsbereich als auch von kommerziell tätigen wissenschaftlichen Informationsanbietern eine Reihe von Unterzeichnern, die die DFN-AAI nutzen.

Technische Komponenten

Alle für den Betrieb notwendigen technischen Komponenten wie die Metadatenverwaltung, der WAYF-Server und das Testsystem stehen pünktlich zum Start des Dienstbetriebes zur Verfügung. WAYF-Server und Testsystem befinden sich schon seit einigen Monaten in Betrieb und werden eifrig genutzt. Das Web-Portal wurde um eine Komponente für die Metadatenverwaltung erweitert. Damit sind die Administratoren der teilnehmenden Einrichtungen in der Lage, ihre Metadaten selber in die DFN-Datenbank einzutragen und zu pflegen. Das nachgeschaltete System erzeugt daraus automatisch die aggregierte Metadatendatei aller AAI-Teilnehmer, die dann DFN-weit verteilt wird.

Bibliothekswesen und Verlage als erste Anwender

Zahlreiche Kontakte auf der diesjährigen Buchmesse in Frankfurt zeigten, dass die Bibliotheken und Verlage zu Recht in dem Rufe stehen, Vorreiter in Sachen

„Shibboleth" zu sein. Viele Verlage bieten bereits Zugangsmöglichkeiten zu ihrem Informationsangebot mittels des Shibboleth-Verfahrens an und sind auch schon Teilnehmer an einigen europäischen und amerikanischen Föderationen. So stieß der DFN-Verein auf offene Ohren mit dem Angebot, Verlage in die DFN-Föderation aufzunehmen. Inzwischen liegen bereits unterzeichnete Verträge international tätiger Verlage vor, und es haben auch schon erfolgreiche Tests zwischen den Service-Providern der Verlage und DFN-IdPs stattgefunden.

Zu den ersten Teilnehmern an der Produktionsföderation des DFN zählen Bibliotheken aus Baden-Württemberg. Aufgrund erfolgreicher Vorarbeiten im REDI-Projekt konnten eine Anzahl von Teilnehmern problemlos in die DFN-AAI übernommen werden.

Auf dem deutschen Bibliothekarstag im Juni 2008 in Mannheim wird DFN-AAI ein Schwerpunktthema sein. Im Rahmen der Vortragsveranstaltungen, durch Vorführungen und einem Messestand wird der DFN-Verein gemeinsam mit der Universitätsbibliothek Freiburg hierzu umfassend informieren.

Software-Verteilung

Die kontrollierte Verteilung lizensierter Software mit Hilfe der Verfahren der DFN-AAI ist Gegenstand eines Projektes der Firma Microsoft und der Universität Würzburg. Während auf der technischen Seite Fortschritte erzielt wurden - die Einbindung der Server in die DFN-AAI wurde erfolgreich getestet - umfasst die Menge der Microsoft-Produkte, die zur Verfügung gestellt werden sollen, einige wichtige Software-Komponenten noch nicht. Hierzu sind noch weitere Gespräche mit Firmenvertretern von Microsoft nötig.

E-Learning

In einigen Ländern der Bundesrepublik sind E-Learning-Systeme im Einsatz, die landesweit von Hochschulen genutzt werden. Für den effizienten Einsatz von E-Learning-Systemen in der DFN-AAI soll ein gemeinsamer Attributsatz entwickelt werden, der länderübergreifend DFN-weit abgestimmt ist. Zu diesem Zweck wird Anfang 2008 ein Treffen mit Interessenten stattfinden, die ein passendes Attributschema erarbeiten sollen.

D-Grid

Innerhalb des D-GRID stellt das C3-Projekt eine treibende Kraft für den Einsatz von Shibboleth zu Grid-Zwecken dar. In enger Absprache mit den Betriebsverantwortlichen des DFN-Vereins gehörten die Systeme des C3-Grid zu den ersten, die das DFN-Testsystem erfolgreich durchlaufen haben, und auch zu den ersten, die in die Produktionsföderation überführt wurden. Weitere Grids werden folgen.

Ausblick

Für das Jahr 2008 hat sich der DFN-Verein eine Reihe von Aufgaben vorgenommen, um den Dienst DFN-AAI weiter voran zu treiben:

- Der Ausbau der DFN-Föderation soll durch Hinzunahme weiterer Teilnehmer und Ressourcenanbieter vorangetrieben werden.

- Die Betriebsinfrastruktur von DFN-AAI soll durch Redundanzmaßnahmen höchstmögliche Verfügbarkeit erlangen.

- Das Informationsangebot auf dem Web-Server (http://www.aai.dfn.de) soll benutzerfreundlicher strukturiert werden.

- Für E-Learning soll ein Attributsatz abgestimmt werden.

- Die neue Software-Version Shibboleth 2.0 soll sobald wie möglich in Betrieb genommen werden.

Ulrich Kähler

DFN-Verein
kaehler@dfn.de

Call for Papers

1. DFN-Forum Kommunikationstechnologien "Verteilte Systeme im Wissenschaftsbereich" am 28. und 29. Mai 2008

Der Verein zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN-Verein) veranstaltet gemeinsam mit der TU Kaiserslautern am 28. und 29. Mai 2008 das 1. DFN-Forum Kommunikationstechnologien. Mitveranstalter sind die Zentren für Kommunikation und Informationsverarbeitung in Forschung und Lehre e.V. (ZKI) und die Gesellschaft für Informatik e.V. (GI).

Call for Papers

Das 1. DFN-Forum Kommunikationstechnologien „Verteilte Systeme im Wissenschaftsbereich" ist eine Plattform zur Darstellung und Diskussion neuer Forschungs- und Entwicklungsergebnisse aus dem Bereich TK/IT. Das Forum dient dem Erfahrungsaustausch zwischen Wissenschaftlern und Praktikern aus Hochschulen, Großforschungseinrichtungen und Industrie.
Die Vorträge umfassen i.d.R. eine Zeitspanne von 25 Minuten + 5 Minuten für die Diskussion. Es wird um Beitragseinreichungen zu den nachfolgend aufgeführten Themenkreisen (TK) gebeten:

TK I: Neue Netztechnologien und Infrastruktur

- Future Internet (Clean-Slate versus Evolution)
- Drahtlose Zugangstechnologien (UMTS, WLAN ...)
- Layer-2 Technologien (Carrier-Grade Ethernet, …)
- Selbstorganisation und -management Overlaynetze (P2P)

TK II: Grid-Technologien

- Virtualisierung
- Kollaboration und Wissensmanagement
- D-Grid: Community Grids, Betriebsmodelle, Business-Projekte und Nachhaltigkeit
- Management von Grids
- Grids im Rechenzentrumsumfeld
- Service orientierte Architekturen
- Strategien zum VO-Management
- SLA im Grid-Umfeld

TK III: Anwendungsarchitekturen und Dienste

- Integrationseffekte VoIP/IT
- Video-/Web-Conferencing
- Mobiles Web
- Medienunterstützung in F&L
- Multimodale Schnittstellen/Interaktion
- Innovative Anwendungen
- Application Service Provisioning

TK IV: ITC Management

- Autonomous Management
- Management Policies
- Authentication and Authorisation
- Identity Management
- Sicherheit
- Management von Grids, Grids im Rechenzentrumsumfeld

Programmkomitee

Marcus Brunner, NEC
Alexander Clemm, Cisco
Gabi Dreo (Co-Chair), Universität der Bundeswehr München
Thomas Eickermann, Forschungszentrum Jülich
Markus Fidler, TU Darmstadt
Alfred Geiger, T-Systems SfR
Wolfgang Gentzsch, D-Grid Initiative
Hannes Hartenstein, Universität Karlsruhe
Dieter Hogrefe, Universität Göttingen
Ulrich Lang, Universität zu Köln
Paul Müller (Co-Chair), TU Kaiserslautern
Bernhard Neumair (Co-Chair), GWDG Göttingen
Gerhard Peter, Hochschule Heilbronn
Christa Radloff, Universität Rostock
Erwin P. Rathgeb, Universität Duisburg-Essen
Helmut Reiser, LRZ München
Peter Schirmbacher, Humboldt-Universität, Berlin
Manfred Seedig, Universität Kassel
Rene Wies, BMW Group

Beitragseinreichung

Bitte reichen Sie Ihre Beiträge zu den angegebenen Themenkreisen bis zum 06.01.2008 ein unter:
http://dfn2008.uni-kl.de/

Die Vortragsanmeldung sollte beinhalten:

1. Eine Seite (Deckblatt): Themenkreis (TK), zu dem der Vortrag angemeldet wird, Name, Vorname, Akad. Titel, Hochschule/Firma, Telefon, E-Mail und Dienstanschrift des Vortragenden (Hochschule/Firma, Abteilung, Straße/Postfach, PLZ und Ort), entsprechende Angaben zu Co-Autoren.

2. Den Beitrag (max. 10 Seiten) im PDF-Format (Details zum Format der endgültigen Fassungen siehe die obige Web-Adresse)

Die angenommenen Beiträge werden in einem gedruckten Konferenzband veröffentlicht, der im GI-Verlag erscheinen wird.

Wichtige Termine

- Einreichung der Beiträge:
  06. Januar 2008
- Autorenbenachrichtigung:
  29. Februar 2008
- Abgabe der endgültigen Fassung:
  20. März 2008

Aktuelles aus dem Wissenschaftsnetz

W-LAN Karte der Uni Hamburg in Google Earth

Wer an der Universität Hamburg den nächsten Hotspot sucht, findet seit Mitte November alle Access Points der Uni bei Google-Earth. Die WLAN-Standorte werden auf der Webseite des Rechenzentrums als Placemark-Datei für die Software Google Earth™ zum Download angeboten. Voraussetzung für das Betrachten der Placemark-Datei ist die Installation von Google Earth™ in einer aktuellen Version. Ist Google Earth™ bereits installiert, besteht eine Verknüpfung der Dateien vom Typ „kmz", so dass die Datei „uhh_ap.kmz" automatisch in Google Earth™ geladen wird.

Wird Google Earth™ über die „uhh_ap.kmz" Datei geöffnet, so wird eine Darstellung gewählt, in der sämtliche Access-Points der Universität gezeigt werden. Soll ein bestimmter Bereich der Übersicht vergrößert dargestellt werden, so reicht ein Doppelklick auf das gewünschte Gebiet, und der gewählte Kartenausschnitt wird vergrößert.

Sind in einem Gebäude mehrere APs untergebracht, so werden diese übereinander abgebildet. Klickt man auf diese Symbole, werden die Symbole auseinandergefächert dargestellt (siehe Abb. unten). Bei einem weiteren Klick auf eines der Symbole öffnet sich ein Fenster mit weiteren Informationen, wie etwa der Nummer des Raumes, in dem der Access-Point installiert ist. Des weiteren weisen Links direkt auf relevante Internetseiten des RRZ zum Thema „Öffentliche Netzzugänge und WLAN" an der Universität Hamburg.

Die Standortdaten der universitären Access-Points werden vom Rechenzentrum in einer Datenbank gepflegt. Ein stündlich laufender cronjob fragt die Datenbank nach den installierten APs ab und übergibt das Resultat an ein Python-Skript, welches wiederum die Placemark-Datei generiert.

Gästen der Universität kann der Zugang zum Datennetz gewährt werden, wenn ihre Heimatinstitution am Roaming-Dienst des Deutschen Forschungsnetzes teilnimmt. Derzeit ist an der Universität Hamburg das CASG-Verfahren implementiert. Das eduroam-Verfahren nach dem 802.1x-Standard befindet sich in der Erprobung.

http://www.rrz.uni-hamburg.de/kommunikation/netzzugaenge/wlan-standorte.html

X-WiN: 5 Petabyte-Schwelle in Sichtweite

Im Oktober 2007 betrug das Gesamtvolumen der von den Einrichtungen über das X-WiN empfangenen Daten 4,777 Petabyte. Das transportierte Volumen im X-WiN hat sich damit gegenüber dem Vorjahreswert annähernd verdoppelt. Nach einer leichten Stagnation im Frühjahr hat die Netznutzung seit Sommer 2007 wieder überdurchschnittlich stark zugenommen. Etwas mehr als 1 Petabyte wurden aus dem GÉANT2 und über Global Upstream aus dem weltweiten Internet empfangen.

Die Steigerung der Nutzungsintensität verteilt sich insgesamt gleichmäßig über alle Anschlusskategorien, wobei die 600-Mbit/s-Anschlüsse mit 626 Terabyte Datenimport den relativ größten Anteil am Netzverkehr verbuchen. Insgesamt waren im Oktober 455 Wissenschaftseinrichtungen direkt an das X-WiN angeschlossen.

DFNInternet: mehr Leistung ab 2008

Ab dem 1.1.2008 wird für alle Kategorien des DFNInternet-Dienstes die Leistung bei gleichem Entgelt erhöht. Gleichzeitig steht den Anwendern der Kategorie I 06 neben einer Anbindung mit STM-1 auch wahlweise ohne zusätzliches Entgelt eine Anbindung mit Gigabit-Ethernet (GE) zur Verfügung. Mit der Umstellung auf die neuen Bandbreiten wurde bereits in diesem Jahr begonnen.

Cross-Border-Fibre zwischen Frankreich und Deutschland

Am 15. Januar 2008 wird eine Glasfaserverbindung eingeweiht, die vom badischen Kehl ins französische Strasbourg führt und die Wissenschaftsnetze Deutschlands und Frankreichs direkt miteinander verbindet. Die Hochleistungs-Datenverbindung zwischen dem französischen RENATER (Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche) und dem X-WiN wird sowohl für die Spitzenforschung zur Verfügung stehen als auch den grenzübergreifenden Datenverkehr beflügeln.

Cross-Border-Verbindungen spielen eine zunehmend wichtige Rolle beim internationalen Datenverkehr zwischen den Forschungsnetzen. Deutschland verfügt bis dato über CBF-Verbindungen mit Polen, mit der Schweiz und den Niederlanden. Eine weitere Verbindung zum luxemburgischen Forschungsnetz RESTENA befindet sich in Vorbereitung.

Mehr als 500 Hochschulen und Forschungseinrichtungen allein in Deutschland können über diese 'Cross-Border-Fibre' mit den Wissenschaftlern in Frankreich direkt verbunden werden. Die physische Verbindung der Netze ermöglicht nicht nur Übertragungsgeschwindigkeiten im vielfachen Gigabit-Bereich, sondern erlaubt auch die Kopplung von wissenschaftlichen Großgeräten über Ländergrenzen hinweg.

Die feierliche Inbetriebnahme der Cross-Border-Fibre findet am 15. Januar 2008 an der Universität Strasbourg statt. Die Veranstaltung ist öffentlich - das französische Wissenschaftsnetz RENATER und der DFN-Verein laden Sie hierzu herzlich ein.

Weitere Informationen in Kürze unter http://www.dfn.de/

Existierende und geplante Cross-Border-Verbindungen zwischen den europäischen Wissenschaftsnetzen.

DFN@home - Einwahl jetzt auch übers Handy

DFN@home ermöglicht Nutzern einen Zugang zum internen Netz ihrer Einrichtung über Telefon-/ISDN bzw. über DSL. Ein Nutzer erhält eine IP-Adresse aus dem Netz seiner Einrichtung und kann so als Angehöriger seiner Einrichtung authentifiziert werden. Seit Oktober wird DFN@home mit einem neuen Vertragspartner, der ‚Inter.net Germany' betrieben. Als zusätzliche Option des Dienstes steht seit dem Wechsel die Einwahl auch aus dem Ausland und aus Mobilfunknetzen unter der Nummer +49 30 254 420 zur Verfügung.

Administratoren-Tool und neue Standortliste für DFNRoaming

Die Landkarte der Roaming-Standorte im Deutschen Forschungsnetz füllt sich zusehends. Für DFNRoaming gibt es seit kurzem eine überarbeitete Standortliste sowie eine Liste aller eduroam-Standorte in Deutschland. Beide Dienste ermöglichen Wissenschaftlern das roamen im ganzen europäischen Forschungsnetzverbund. Einziger Unterschied ist, dass DFNRoaming auf nationaler Ebene VPNs und Web Redirects unterstützt, deren Unterstützung von eduroam nicht mehr fortgeführt werden.

Neu bei DFNRoaming ist ein Diagnose Tool, das Administratoren die Möglichkeit bietet, ihre Konfiguration zu testen. Das Tool befindet sich zur Zeit in der Pilotphase. Der Zugriff auf dieses Tool wird über Zertifikate abgesichert.

http://www.dfn.de/de/dienstleistungen/dfnroaming/

http://www.eduroam.de

Happy Birthday, SWITCH

Schweizer Forschungsnetz feiert zwanzigsten Geburtstag

Dass er einmal ein landesweites Hochleistungsnetz aufbauen und betreiben würde, davon hat Thomas Brunner, Managing Director des Schweizer Forschungsnetzes SWITCH, als kleiner Junge nicht geträumt. Wie viele andere Kinder wollte auch er einmal Lokomotivführer werden. Heute liest sich die Geschichte des Internets für den passionierten Bahnfahrer Brunner fast wie die Geschichte des Schienenverkehrs. Genau wie das Netz hatte sich die Bahn im 19. Jahrhundert binnen weniger Jahrzehnte zu einem weit vernetzten Transportmittel entwickelt, welches die Reisezeiten in Europa und Nordamerika drastisch verkürzte. Sie wirkte dabei als Katalysator der industriellen Revolution, weil sie die infrastrukturellen Voraussetzungen für die Entwicklung der Industrie schuf und selbst eine gewaltige Nachfrage nach deren Produkten erzeugte. Im Oktober 1987, als das Schweizer Forschungsnetz SWITCH gegründet wurde, war eine ähnliche Entwicklung auch in der Welt der Netze vielleicht schon zu erahnen, vorauszusehen war sie allerdings nicht.

SWITCH wird gegründet

Bereits 1978, neun Jahre vor der Gründung von SWITCH, hatten Wissenschaftler damit begonnen, über ein Forschungsnetzwerk für die Schweiz nachzudenken. Netzzugänge für die Wissenschaft wurden zu dieser Zeit wie in vielen anderen Ländern von EARN, dem European Academic Research Network, realisiert. 1984 entwickelten Mitglieder der Commission pour l'Informatique de la Conférence Univérsitaire Suisse (CICUS) die Idee eines nationalen Forschungsnetzwerks für die Schweiz. 1985 entschloss sich CICUS, das Swiss TeleCommunication System for Higher Education and Research mit der einprägsamen Marke SWITCH zu gründen. Ein Impulskredit des Bundes in Höhe von 15 Millionen Franken ermöglichte es 1986, dass die Gründung von SWITCH Formen annahm.

Im gleichen Jahr trug Jon Postel, Gründer der Internet Assigned Numbers Authority (IANA), auf Antrag von Prof. Dr. Bernhard Plattner von der ETH Zürich die Top Level Domain .ch ins DNS ein. Weil Plattner nach der Gründung von SWITCH deren Geschäfte „ad interim" führte und weil SWITCH den Auftrag hatte, das Schweizer Hochschul- und Forschungsnetz aufzubauen, übertrug Plattner die Domain von der ETH auf SWITCH. Von nun an war SWITCH nicht nur für die Vernetzung der Wissenschaft, sondern auch für die Verwaltung der Domain-Namen unter .ch zuständig.

SWITCHMail als erste netzwerkbasierte Dienstleistung

Im ersten Jahr nach der Gründung stand die Konstituierung der Organe und der Aufbau der Geschäftsstelle der Stiftung im Zentrum. Prof. Dr. Jürgen Harms, der durch sein nationales und internationales Engagement wesentlich zur Gründung der Stiftung beigetragen hat, wurde erster Präsident. In dieser Funktion begleitete er die Geschäfte der Stiftung bis ins Jahr 2000. Harms besetzte die Position des Geschäftsführers mit Peter Gilli. Bis zum Ende des ersten vollen Geschäftsjahres konnte ein kleines, aber schlagkräftiges Team aufgebaut werden, das über die notwendige Erfahrungen in der Vernetzung von Organisationen mit Telekommunikations-Technologien verfügte.

Es war die Geburtsstunde des SWITCHlan. Mit der Vernetzung der ersten beiden Standorte Zürich und Lausanne wurde ein Grundstein dafür gelegt. Konzeptionelle Arbeiten, Ausschreibungen für die Infrastruktur und wegweisende Entscheidungen zur verwendeten Hardware sind diesem Schritt vorausgegangen.

Bereits im Gründungsjahr wurden die ersten E-Mails über die Infrastruktur von SWITCH zwischen den Schweizer Hochschulen ausgetauscht. Weil es 1987 noch keinen einheitlichen Standard für Mails gab, stellte der elektronische Briefwechsel über verschiedene anwenderspezifische Plattformen eine große Herausforderung dar. SWITCHMail mit ihren internationalen Verknüpfungen war die erste netzwerkbasierte Dienstleistung, die den Schweizer Hochschulen angeboten wurde.

Bereits 1989 alle Universitäten am SWITCH1

Schon bevor SWITCH ins Leben gerufen wurde, gab es in der Schweiz Verbindungen zwischen einzelnen Hochschulen. Zwischen den beiden Eidgenössischen Technischen Hochschulen in Zürich und Lausanne und dem Paul-Scherrer-Institut in Villigen (PSI) existierten bereits 2 Mbit/s schnelle Mietleitungen. Vor allem die Anwender von DEC-VMS-Systemen hatten ihre Rechner über diese Mietleitungen und das öffentliche X.25-Netz der damaligen Telecom PTT verbunden.

SWITCH musste auf diese bestehenden Anwendungen Rücksicht nehmen, gleichzeitig aber dafür sorgen, dass die interuniversitären Verbindungen den neuen technischen Standards genügten. Zu diesem Zweck wurde ein Multiprotokollnetzwerk aufgebaut, das auf Routern basierte. In Anlehnung an das LAN (Local Area Network), das Rechner innerhalb einer Hochschule verband, wurde das neue Netzwerk SWITCHlan genannt. Dieser Name sollte signalisieren, dass von nun an auch Rechner an verschiedenen Hochschulen miteinander kommunizieren konnten. Das Bindeglied zwischen SWITCHlan und dem Netzwerk der einzelnen Universitäten war das SWITCHAccess System (SAS). Das Konzept war erfolgreich: Bis Ende 1989 waren alle Schweizer Universitäten und das Kernforschungszentrum CERN mit 64 oder 128 Kbit/s angeschlossen. Das Kernnetz, bestehend aus den beiden eidgenössischen technischen Hochschulen, dem PSI sowie den Universitäten Lausanne und Zürich, bestand aus einer 2-Mbit/s-Verbindung.

SWITCH wird Registrierungsstelle für TLDs

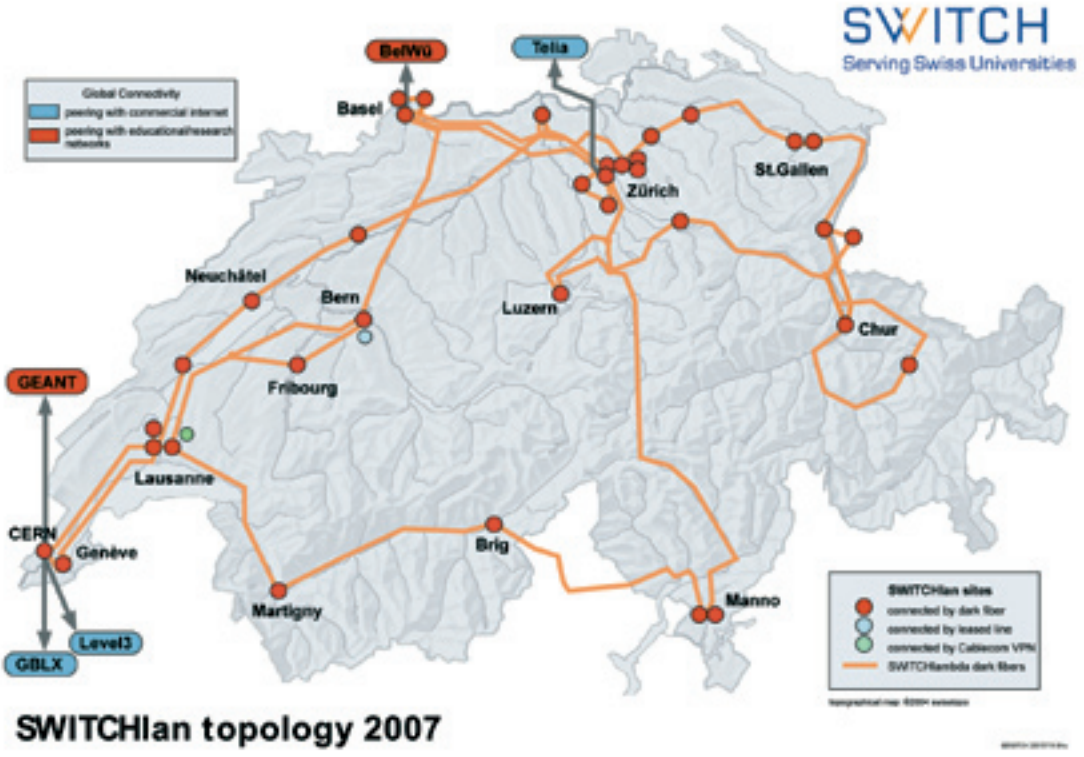
Seit seiner Gründung zeichnete SWITCH auch für die Registrierungen der Schweizer Top-Level-Domains verantwortlich. In den Anfangsjahren hatten die Domainverwalter allerdings denkbar wenig zu tun: Die ersten Schweizer Domain-Namen waren ethz.ch, cern.ch und switch.ch, später folgten die Domain-Namen für die Schweizer Hochschulen. Noch hatten nur Universitäten und eine Handvoll großer Unternehmen Zugang zum Internet, entsprechend gering war das Interesse an Domain-Namen. Um einen .ch-Domain-Namen zu beantragen, genügte es, das ausgefüllte Antragsformular per E-Mail, Fax oder Brief bei SWITCH einzureichen. So einfach die Kontaktaufnahme war, so streng waren am Anfang die Vergaberegeln: Pro Firma oder Organisation durfte nur ein Domain-Name registriert werden, und der Domain-Name musste dem Namen der Firma möglichst ähnlich sein. Natürliche Personen waren als Halter von Domain-Namen gar nicht vorgesehen – was eine Privatperson mit einem Internet-Domain-Namen anfangen sollte, das konnte man sich 1990 noch nicht vorstellen. Bis Ende 1994 waren gerade einmal 300 Domain-Namen registriert.

Am CERN wird das www erfunden

Fast drei Jahrzehnte wurde das Internet fast ausschließlich von Wissenschaftlern und Militärs benutzt. Man musste komplizierte Befehle eingeben, und wer den richtigen Befehl nicht kannte, stand, wie die Schweizer sagen, „am Berg". 1991 änderte sich das mit einem Schlag: Die unansehnliche Raupe Internet verwandelte sich – notabene in der Schweiz – in einen fröhlichen Schmetterling, ins World Wide Web.

Schuld daran war Tim Berners-Lee. Er kreierte, eher zufällig und aus einer Not heraus, am Kernforschungszentrum CERN in Genf das World Wide Web. Bereits im März 1989 hatte Berners-Lee in einem ersten Vorschlag «Information Management: A Proposal» die Grundzüge des World Wide Web skizziert. Ziel seiner Arbeit war es, den auf der ganzen Welt verstreuten Kernphysikforschern des CERN ein Kommunikationsinstrument in die Hand zu geben. «Das Dokument war ein Versuch, das CERN-Management davon zu überzeugen, dass ein globales Hypertextsystem im Interesse von CERN ist», kommentierte Berners-Lee das Papier später.

Zusammen mit dem Programmierer Robert Cailliau überarbeitete er den Vorschlag und reichte ihn im Oktober 1990 erneut ein. Während im ersten Papier nur zweimal von «einem Web» die Rede war, sprachen die beiden Autoren im zweiten Papier bereits explizit von «World Wide Web». Nur Wochen später begann Lee damit, eine erste Version des World Wide Web zu programmieren. Bereits an Weihnachten 1990 war das Web mit einem textbasierten Browser demonstrierbar.



SWITCH wird IP-Netz

Die kommenden Jahre brachten mit der Entwicklung erster Browser und kurz darauf mit der Veröffentlichung erster Webverzeichnisse immer mehr Usability ins World Wide Web. 1995 feierte SWITCH fünf Jahre Internetanschluss in der Schweiz. Die Anzahl registrierter Domain-Namen unter .ch und .li stieg auf 1257 an. Inzwischen war ein Mitarbeiter der Netzwerkgruppe von SWITCH zu hundert Prozent mit der Registrierung und Verwaltung von Domain-Namen beschäftigt und es gab erste Pläne, den Datendurchsatz auf 34 bis 155 Mbit/s zu erhöhen. Der aggregierte Datenverkehr aller Hochschulen in der Schweiz durchbrach Mitte des Jahrzehnts die 1 Gbit/s-Grenze.

Beim Management des Verkehrs hatte man zum Leidwesen der Netzwerker nach wie vor mit sehr heterogenen Systemen und Umgebungen in den Universitäten zu tun. Das SWITCH Access System (SAS) schob sich deshalb als Bindeglied zwischen das SWITCHlan und die Netzwerke der einzelnen Universitäten. Das wichtigste Protokoll im SWITCH-Netz war zu Beginn DECnet IV . Bald kam das Internet Protocol (IP) und 1993 das ISO CLNS hinzu. Wie viele andere Wissenschaftsnetze verwandelte sich SWITCH vom Multiprotokoll-Netzwerk in ein reines IP-Netz und schaltete 1998 das alte DECnet ab.

Erste Glasfaser zwischen Zürich und Genf

Ein Sorgenkind in punkto Netzwerkkapazität war angesichts beständig steigender Volumina im Netz vor allem die Verbindung Zürich–Genf: Die Spitzenlast auf dieser Verbindung überschritt regelmäßig 100 Mbit/s. 1999/2000 sollte ein Ausbau der Bandbreite dieser meistbelasteten Verbindung von 155 auf 622 Mbit/s stattfinden. Es stellte sich aber heraus, dass nur ein Ausbauschritt direkt auf 2,5 Gbit/s preislich und technologisch sinnvoll war. Das Ergebnis war eine erste Hochgeschwindigkeitsverbindung als Pilotbetrieb zwischen ETH Zürich und dem CERN.

Kurz vor Weihnachten 2000 begann SWITCH mit den ersten Tests im Gigabit-Bereich. Parallel dazu hat SWITCH den Einsatz von eigenen Glasfasern geprüft. Noch vor Ende des Jahres schloss SWITCH einen Vertrag für den Kauf eines Glasfaserpaares zwischen Zürich und Genf. Ab August 2001 sollte diese Glasfaserleitung mit einer Kapazität von mehreren 10 Gbit/s als Hochgeschwindigkeitsverbindung in das Netzwerk integriert werden und die gemietete Pilotstrecke ablösen.

SWITCH wird zu SWITCHlambda

Mit der ersten eigenen Glasfaserverbindung zwischen Zürich und Genf nahm SWITCH innerhalb Europas eine Pionierrolle ein. Verlegt entlang der Autobahn Genf–Lausanne–Bern–Basel–Zürich verbindet sie bis heute das CERN in Genf mit den Universitäten Lausanne, Bern, Basel und Zürich sowie den eidgenössischen technischen Hochschulen in Lausanne und Zürich. Die Initialkonfiguration umfasste mehrere optische Kanäle mit 1 Gbit/s-Übertragungsrate und verwendet die DWDM (Dense Wavelength Division Multiplexing) Technik.Ihr optisches System wurde von Anfang an für 16 Kanäle à 10 Gbit/s ausgelegt. Die den Hochschulen zur Verfügung stehende

Der vorliegende Artikel enthält Passagen aus der Jubiläumsausgabe des SWITCHjournals „20 Jahre SWITCH". Das Journal findet sich als PDF unter der Adresse http://www.switch.ch./de/about/publications.html

Bandbreite konnte dadurch in den Folgejahren mit vergleichsweise geringen Investitionen erhöht werden und mit den steigenden Anforderungen Schritt halten.

Die Glasfaserleitung war Teil des Projekts SWITCHlambda. Ziel des Projekts war ein schweizweites Glasfasernetz, das alle Universitäten, Hochschulen und Fachhochschulen erschließt. In den Jahren nach 2001 sollte dieses Netzwerk in Etappen realisiert werden. Im Jahr 2006 ging als letzte große Teilstrecke die Verbindung von Lausanne durchs Wallis und weiter via Domodossola nach Manno als Zweitwegverbindung für das Tessin in Betrieb, so dass SWITCH im Journal vom Juni 2006 melden konnte: «Rings Closed!»

Schnittstelle zur Zukunft

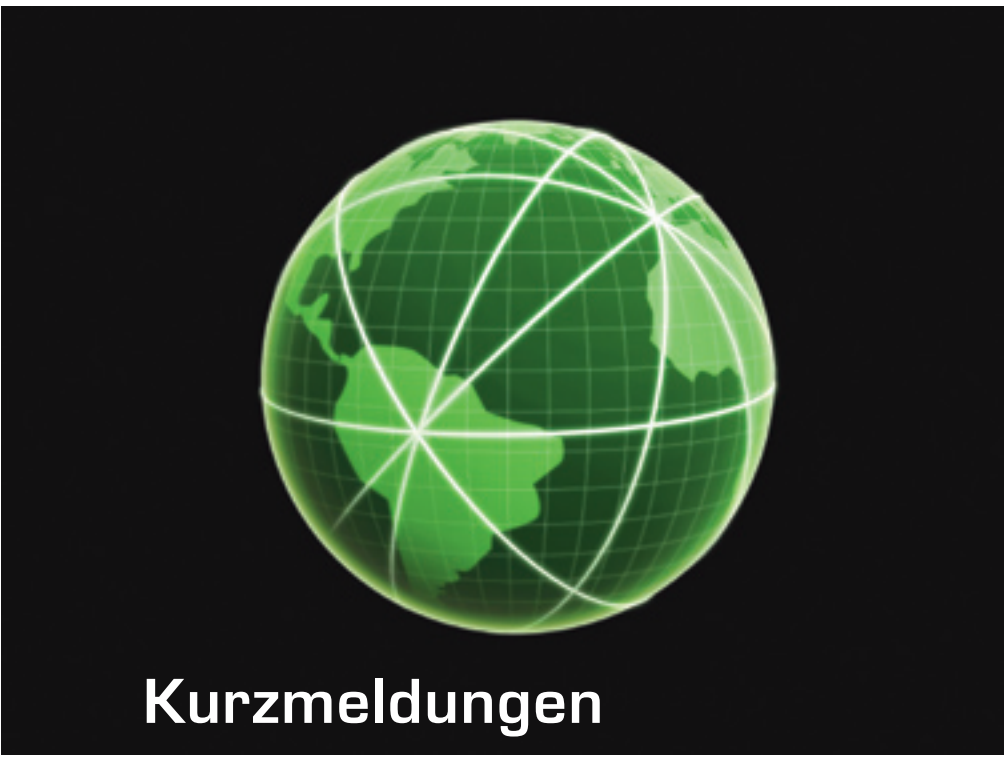
Mehr als 80 Mitarbeiter bieten den Hochschulen und Forschungseinrichtungen in der Schweiz ein breites Spektrum an Dienste und Services an. Und lange schon dreht es sich dabei nicht mehr nur um Konnektivität. Auf der Basis von SWITCHlambda werden laufend neue, innovative Dienste ersonnen und zur Betriebsreife gebracht. So wurde das SWITCH e-Conferencing-Portal von verschiedenen ausländischen Schwesterorganisationen lizenziert. Einen ebenso guten „Riecher" hatte SWITCH etwa beim Thema Streaming: SWITCH erkannte schnell den Trend zu Podcasting und entwickelte deshalb ein Exportmodul, das die Erzeugung von Podcasts spielerisch einfach gestaltet. Gleichzeitig befasste sich SWITCH mit den pädagogischen Aspekten und entwickelte zusammen mit E-Learning-Fachleuten eine speziell für die Bildung geeignete Form von Vorlesungs-Podcasts. Aufgezeichnete Streams können sowohl in einer hoch auflösenden als auch in einer für portable Abspielgeräte optimierten Variante vom Server geladen werden. Die iPod-Version wechselt dabei zwischen Sprecher und Präsentation und fördert so die Aufmerksamkeit. Der SWITCH-Approach zur automatischen Erstellung solcher Podcasts gilt immer noch als einzigartig.

„Wenn ich groß bin, will ich einmal Netzwerker werden!"

Noch ist es schwer, sich vorzustellen, dass künftige Generationen statt „Lokomotivführer" einmal „Netzwerker" als Berufswunsch angeben. Dass dies dereinst doch möglich werden kann, darum bemüht sich der „SWITCH Junior Web Award", dessen Preisverleihung am 16. November aus Anlass der Jubiläumsfeierlichkeiten stattfand. Mehr als 100 Klassen mit rund 2000 Schülerinnen und Schülern hatten eigene 119 Websites kreiert und dabei viel über den Umgang mit dem Internet, mit Programmen, mit der Sprache und den vielfältigen Aspekten des Internets gelernt.

Mittlerweile geht der „Junior Web Award" in seine zweite Runde. Die Websеiten, die die Kids im ersten Jahr gebaut haben, finden sich unter der Adresse http://www.juniorwebaward.ch/

(kh)



Kurzmeldungen

Radioastronomen nutzen P2P-Services im GÉANT2

Unter dem Projektnamen „EXPReS" arbeiten derzeit vier der größten radioastronomischen Forschungseinrichtungen Europas in einem Projekt zur High-Speed-Astronomie zusammen, um ein komplexeres und genaueres Bild vom Universum zu erhalten.

Immer leistungsfähigere Netze ermöglichen schnellere Korrelation gemeinsam gewonnener Daten und lassen immer präzisere Beobachtungen kosmischer Phänomene am Rand des Universums zu. Gemeinsam mit dem GÉANT2 haben das italienische GARR, Englands JANET und Polens PSNC mittels Punkt-zu-Punkt-Verbindungen ein Radioastronomie-VPN geschaltet, das vier der größten Teleskope Europas koppelt. Dadurch entsteht ein virtuelles Radioteleskop, das die Leistungen der einzelnen Teilnehmer bündelt und tiefer und genauer ins All horchen kann als jemals zuvor. Die vier teilnehmenden Teleskope befinden sich im italienischen Medicina, im polnischen Torun sowie im britischen Jodrell Bank und Cambridge.

http://www.expres-eu.org/

Europäisches Forschungsnetz-Kompendium

Das von der europäischen Forschungsnetzkonferenz TERENA jährlich zusammengestellte Kompendium der nationalen Forschungsnetze Europas ist erschienen. Die 2007er Edition hält Daten von fast 50 Wissenschaftsnetzen Europas und angrenzender Regionen bereit. Es bietet Informationen zu Nutzern, technischen Plattformen, Verkehrszahlen, angebotenen Diensten und Services sowie zu den Betreiber-Organisationen. Jedem, der tiefer in die Materie „Forschungsnetz" einsteigen möchte, bietet das Kompendium eine Fülle an Informationen über die Welt der Wissenschaftsnetze. Bei der Lektüre fällt vor allem der stetige Zuwachs bei der Nutzung von Dark Fibre und die zunehmende Anzahl von Cross-Border-Fibres ins Auge. Ein klarer internationaler Trend ist auch die Tendenz zu mehr Bandbreite und leistungsfähigeren Diensten bei gleichbleibenden Entgelten.

In der Geschäftsstelle des DFN-Vereins steht Interessenten eine kleine Anzahl gedruckter Ausgaben zur Verfügung. Eine .pdf-Version mit sämtlichen Informationen ist selbstverständlich online verfügbar:

www.terena.org/activities/compendium/

Σ-Net: Lettlands Forschungsnetz mit neuem Namen

Das lettische Forschungsnetz, das bislang unter dem Namen LATNET firmierte und seit seiner Gründung 1992 die Wissenschaft in der baltischen Republik mit Internet-Services versorgt hat, hat sich nun einen neuen Namen gegeben. Der Name Sigma-Net steht für veränderte Ziele, die sich die Forschungsnetzwerker Lettlands gesetzt haben: Noch mehr Kooperation mit den Forschungsnetzen anderer Länder, mehr Service-Qualität und neue Dienste und Services wie ein eigenes CERT oder die Unterstützung von Grids stehen auf dem Programm. Das Summenzeichen Sigma repräsentiert die Bündelung aller Ressourcen und Kräfte bei der Bewältigung dieser Aufgaben.

http://www.sigmanet.lv/

Forschungsnetz für Bosnien-Herzegowina

Das Forschungsnetz von Bosnien-Herzegowina wieder zu beleben ist das Ziel eines Treffens hochrangiger Politiker und Wissenschaftler des Landes, das am 20. November 2007 in Sarajevo stattfand. Aktuell verfügt die Balkan-Republik über kein in Betrieb befindliches landesweites Forschungsnetz, das den Forschungs- und Bildungseinrichtungen des Landes Internet-Dienste anbieten könnte.

Fast 50 Teilnehmer diskutierten in Sarajevo Möglichkeiten und Erfordernisse, um die bosnischen Schulen und Hochschulen ans Netz zu bringen. Eingeladen waren neben Vertretern der Universitäten auch Politiker, kommerzielle Netzwerkbetreiber und Vertreter von Telefongesellschaften. Daneben nahm auch eine Delegation der Europäischen Kommission und des Executive Committee des europäischen GÉANT2 teil.

Bosnien Herzegowina hat derzeit vier Hochschulen in Sarajevo, Tuzla, Mostar und Biha und eine Vielzahl von höheren Bildungsreinrichtungen, die z.T. berufsvorbereitenden Charakter haben. BiHARNET, das einstige nationale Forschungsnetz wurde 1998 in Betrieb genommen, beendete seinen Betrieb aber bereits im Dezember 2000 aus finanziellen Gründen.

TUD-Informatiker gewinnen Bandbreitenwettbewerb auf Supercomputing-Konferenz

In einem Wettbewerb, der auf der diesjährigen Supercomputing-Konferenz in Reno (Nevada, USA) stattfand, gewann ein internationales Team mit Beteiligung Dresdner Informatiker den ersten Preis. Das Team bestand aus Wissenschaftlern der Indiana University, der TU Dresden, des Rochester Institute of Technology, des Oak Ridge National Labs und des Pittsburgh Supercomputing Center.

Im sogenannten „Bandbreitenwettbewerb" müssen die Teilnehmer die Grenzen der Netzwerk- und Computertechnologie demonstrieren. Ziel ist die Ausnutzung der Netzwerkbandbreite zwischen Speichersystemen vor Ort und den weltweit verteilten Forschungseinrichtungen, wobei der Nutzen für echte Anwendungen demonstriert werden muss. Die weltweit führenden Institutionen stehen hier im Wettbewerb, um die Leistungsfähigkeit von Hard- und Software zu demonstrieren.

Unter Ausnutzung eines speziellen Speichersystems der Indiana University - des sogenannten Data Capacitors - gelang es dem Team, eine Transferrate von bis zu 18,21 Gigabit/s von maximal möglichen 20 Gigabit/s zu erzielen. Dies entspricht der Übertragung von 195 CDs pro Minute. Von Dresden aus ging hierbei ein etwa 4 Gbit/s großer Datenstrom durch das X-WiN, das GÉANT2 und das Internet2 bis zur Indiana University. Bemerkenswert ist nicht zuletzt, dass für den Rekord keine gesonderten Verbindungen im X-WiN geschaltet werden mussten. Die Datenströme liefen über den 10-Gbit/s-Anschluss der TU-Dresden und wurden durch den normalen Netzbetrieb nicht beeinträchtigt.

Das Team demonstrierte während des Bandbreitenwettbewerbs mehrere Anwendungen unter anderem der Performance-Analyse einer Strömungssimulation der Technischen Universität Dresden. Dabei kam die Software Vampir und VampirTrace zum Einsatz, die am Dresdner Zentrum für Informationsdienste und Höchstleistungsrechnen (ZIH) entwickelt wird. Die Indiana Universität steuerte eine Modellierung und Analyse von Amyloid-Proteinen bei, von denen angenommen wird, dass sie die Ursache von Alzheimer sind. Zwei weitere Anwendungen waren die Verwaltung von Röntgenstrukturanalysedaten und die Verwaltung von gescannten Sanskrit-Schriften aus dem 14. Jahrhundert.

Allen Projekten ist gemein, dass sie mit sehr großen Datenmengen umgehen und diese übertragen müssen. Zur Speicherung dieses Datenvolumens konzentrierte sich das Team auf die Verwendung des Lustre-Dateisystems. Die Ausnutzung dieser Technologie über große Entfernungen ist zukunftsweisend für die weltweite Verwaltung riesiger Datenmengen.
(kh)

Dalai Lama im X-WiN

Universität Münster streamt Besuch des Oberhauptes der Tibeter über das Deutsche Forschungsnetz

Anlässlich des Besuches des Dalai Lamas am 20. und 21. September 2007 in der Westfälischen Wilhelms-Universität in Münster (WWU) setzte das Zentrum für Informationsverarbeitung ZIV erstmals im größeren Stil Streaming-Technik zur Live-Audio und Live-Video-Übertragung ein.

In der Aula und im Senatssaal des Schlosses zu Münster, wo der Dalai Lama auftrat, war aus räumlichen und aus Sicherheitsgründen nur eine begrenzte Anzahl an Besuchern zugelassen. Deshalb wurde die Veranstaltung mit hochwertiger Video- und Audiotechnik aufgenommen und über das LAN der Hochschule in andere Hörsäle im Schloss sowie ins Foyer im Fürstenberghaus übertragen. Zusätzlich wurde ein Hörsaal im Schloss für die internationale Presse hergerichtet und mit Live-Bild und -Ton versorgt. Auch bei der Rede des Dalai Lama in der Aula lief im Hintergrund auf der großen Leinwand das Live-Bild der Kameraaufnahmen. Insbesondere hier kam es auf eine zuverlässige und hochwertige Bildqualität mit geringer Übertragungsverzögerung an. Erstmalig bei dieser Veranstaltung wurden die Audio- und Videosignale nicht analog, sondern digital über das LAN der WWU, d.h. über das Internet Protokoll (IP) gestreamt.

Streaming auf dem Campus

Bei der angestrebten „DVD-Qualität" werden allgemein Übertragungsraten von bis zu 12 MBit/s benötigt. Für hochwertige und zuverlässige Übertragungen wurden Hardware-Encoder der Firmen Scientific Atlanta (Cisco Systems, D9032) sowie Teracue (ENC-100) verwendet, die die Audio- und Video-Signale in Echtzeit in IP-Pakete umwandeln und sie zu Set-Top-Boxen schicken. Dies sind spezielle Decoder, welche einen eingehenden IP-Stream in analoge Audio- und Video-Signale zurückwandeln, um sie auf direkt angeschlossenen Beamern und Lautsprecheranlagen präsentieren zu können. Für die Veranstaltung wurden Set-Top-Boxen von Cisco Systems (Modell: Digital Media Player 4300G) und Amino (Modell: AmiNET110) verwendet. Damit die Encoder den IP-Stream nur einmal ins Intranet senden mussten, wurde mit IP-Multicast übertragen. So konnten im Prinzip beliebig viele Decoder ein und denselben Multicast-Stream empfangen und gleichzeitig wiedergeben.

Livestream ins Internet

Das Streaming ins Internet ist mit den oben genannten Qualitäten und Techniken lediglich eingeschränkt möglich: Ein wesentlicher Grund dafür ist, dass ISPs nur selten IP-Multicast anbieten. Für das Streaming ins Internet mussten Server eingesetzt werden, die die live eingehenden IP-Streams *gleichzeitig* einer großen Anzahl Nutzern anbieten. Im Gegensatz zur effizienten Multicast-Übertragung wird über einen Streamingserver für *jeden* Nutzer eine eigene IP-Unicast-Verbindung aufgebaut. Bei entsprechend hoher Nutzerzahl kommt dabei schnell ein sehr hoher Bandbreitenbedarf für die Streamingserver zusammen

Für die Festveranstaltung wurde zur Videokodierung der H.264/MPEG-4 AVC Standard verwendet. Die Audiokodierung erfolgte mittels MPEG-4 AAC. Je nach zur Verfügung stehender eigener Internet-Bandbreite konnte der Nutzer zwischen einem Angebot in hoher Qualität (rund 1 MBit/s) und mittlerer Qualität (rund 200 KBit/s) auswählen. Zur Encodierung wurden zwei Apple-Macintosh-Rechner mit dem Programm „Broadcaster" verwendet.

Vorraussetzung für die Nutzung ist, dass auf dem Rechner des Betrachters ein entsprechender Streaming-Client („Player") installiert ist. Die Livestreams des ZIV können mit aktuellen Versionen des Apple QuickTime Player oder des VLC Media Players angeschaut werden. Beide Programme bieten Browser-Plugins, so dass der Stream innerhalb der ZIV Livestream-Player Seite verfolgt werden kann. Für Probleme mit der Plug-In-Wiedergabe gibt es einen Button, welcher die URL anzeigt, die mit QuickTime oder VLC auch außerhalb des Browsers geöffnet werden kann.

Guido Wessendorf

Westfälische Wilhelms-Universität Münster
Zentrum für Informationsverarbeitung

wessend@uni-muenster.de

Entscheidend für eine gute Übertragung zu vielen gleichzeitigen Nutzern ist die Anbindung der Streamingserver mit hoher Bandbreite. Für den Besuch des Dalai Lamas hatte das ZIV in Zusammenarbeit mit dem DFN-Verein zwei leistungsfähige Streaming-Server direkt an einen Router des X-WiN-Kernnetzstandortes in Münster angebunden. Jeder dieser Server war mit 2 GBit/s Anschlussgeschwindigkeit angebunden, d.h. es standen alleine 4 GBit/s nur für das Internet-Angebot zur Verfügung! WWU-intern standen den Nutzern zwei weitere Server, jeweils auch mit 2 GBits/s angeschlossen, zur Verfügung.

Das ZIV plant, das Livestream-Angebot für Campus- und Internet-Streaming weiter auszubauen. Derzeit läuft hierzu eine Evaluation der zu beschaffenden Encoder und Decoder. Ideal wären Systeme, die sowohl für das Campus-Streaming als auch für die Übertragung ins Internet gleich gut geeignet sind.

http://www.uni-muenster.de/ZIV/inforum/2007-4/a01.html

Bild: Forschungszentrum Jülich

IBM Blue Gene/P in Jülich

Ein weiterer Schritt in Richtung Petascale Computing

Als im Jahr 2004 die IBM Blue Gene Technologie verfügbar wurde, erkannte das Forschungszentrum Jülich (FZJ) schnell das Potential dieser Architektur für Anwendungen aus dem Capability-Computing. Eine Schlüsselfunktion dieser Architektur ist die Skalierbarkeit in Richtung PetaFlop-Computing, mit geringem Energieverbrauch, geringem Platzbedarf und einem hervorragenden Preis-Leistungs-Verhältnis.

Bereits im Sommer 2005 wurde in Jülich ein einzelnes Blue Gene/L Rack mit 2.048 Prozessoren getestet. Schon bald wurde offensichtlich, dass es viel mehr Anwendungen als erwartet gibt, die effizient auf der Blue Gene Architektur gerechnet werden können. Angesichts der Tatsache, dass das System in Bezug auf die Prozessorgeschwindigkeit, die Speicherlatenz und die Netzwerk-Performance gut ausbalanciert ist, skalieren viele Anwendungen sehr gut bis zu einer großen Zahl von Prozessoren. Daher wurde im Januar 2006 das System auf 8 Racks mit 16.384 Prozessoren erweitert. Die Finanzierung dazu erfolgte durch die Helmholtz-Gemeinschaft.

Das 8-Rack-System ist nun seit fast zwei Jahren erfolgreich im Einsatz. Heute lassen etwa 30 sorgfältig ausgewählte Forschungsprojekte ihre Anwendungen auf dem System laufen. Die Job-Größen bewegen sich zwischen 1.024 und 16.384 Prozessoren. Während eines Blue Gene Scaling Workshops am FZJ konnten einige wichtige Anwendungen mit Hilfe von Experten des Argonne National Laboratory, von IBM und aus Jülich optimiert werden. Dabei stellte sich heraus, dass all diese Anwendungen sämtliche 16.384 Prozessoren der Maschine erfolgreich nutzen können.

Aufbauphase des Jugene-Rechnersystems

Bild: Forschungszentrum Jülich

Wissenschaftler der Computational Science aus vielen Forschungsbereichen nahmen die Chance wahr, sich um Rechenzeit auf dem System Blue Gene/L zu bewerben, um ungelöste Fragestellungen bearbeiten zu können, die bisher auf anderen Rechnern nicht möglich waren. Wegen des großen Nutzerandrangs und im Einklang mit der Strategie, das Leadership-Class-Computing zu stärken, beschloss das Forschungszentrum Jülich, ein leistungsstarkes Blue Gene-System der nächsten Generation zu beschaffen. Im Oktober 2007 wurde ein 16-Rack-System Blue Gene/P mit 65.536 Prozessoren installiert, das durch die Helmholtz-Gemeinschaft und das Land Nordrhein-Westfalen finanziert wurde. Mit einer Peak-Performance von 222,8 TFlop/s ist die Jülicher Blue Gene/P, mit Spitznamen JUGENE, gegenwärtig der leistungsstärkste Supercomputer in Europa.

Die wichtigsten Unterschiede zwischen Blue Gene/P und Blue Gene/L betreffen den Prozessor und die Netzwerke (s. Tabelle 1), wogegen der prinzipielle Aufbau von Blue Gene/L unverändert für Blue Gene/P übernommen wurde. Die wesentlichen Merkmale von Blue Gene/P sind:

- 4 PowerPC® 450 Prozessoren werden in einem vollständigen 4-fach SMP-Chip (Knoten) kombiniert, der hybride Programmiermodelle mit MPI und OpenMP erlaubt (bis zu vier Threads pro Knoten).
- Das Netzwerk-Interface ist vollständig DMA-fähig (Direct Memory Access), wodurch die Performance erhöht und die Prozessorlast während des Message-Handlings reduziert wird.
- Der verfügbare Speicher pro Prozessor wurde verdoppelt.
- Das externe I/O-Netzwerk wurde von 1 auf 10 Gigabit Ethernet aufgestockt.

Diese Verbesserungen schlagen sich auch in der Performance für die Anwendungen nieder. Beispielsweise läuft ein Programm aus der theoretischen Elementarteilchenphysik auf Blue Gene/P mit 31,5% der Peak-Performance im Vergleich zu 26,3% auf Blue Gene/L. Außerdem wird der vergrößerte Hauptspeicher von 2 GB pro Knoten neue Anwendungen für Blue Gene/P erschließen.

JUGENE ist Teil des dualen Supercomputer-Komplexes in Jülich und ist eingebunden in eine gemeinsame Speicher-Infrastruktur, die ebenfalls erweitert wurde. Der Hauptbestandteil dieser Infrastruktur ist das neue Jülich Storage-Cluster *(JUST),* das im dritten Quartal 2007 installiert wurde und die Online-Plattenspeicherkapazität um den Faktor 10 auf ca. 1 PetaByte erhöhte. Die maximale I/O-Bandbreite von 20 GB/s wird durch 29 Storage Controller erreicht im Verbund mit 32 IBM Power5 Servern. *JUST* ist an die Supercomputer über eine neue Switch-Technologie angebunden, die auf 10-Gigabit Ethernet basiert. Das System übernimmt die Fileserver-Funktionen für das GPFS (General Parallel File System) und stellt sie den Nutzern in Jülich und innerhalb der internationalen DEISA-Infrastruktur bereit.

Mit dem Upgrade der Supercomputer-Infrastruktur hat das Forschungszentrum Jülich den nächsten Schritt zum Petascale-Computing getan. Es stärkt damit den Anspruch Deutschlands, in Zukunft Standort eines der Europäischen Supercomputerzentren zu werden.

Dr. Michael Stephan
Division „High Performance Systems“,
Jülich Supercomputing Centre

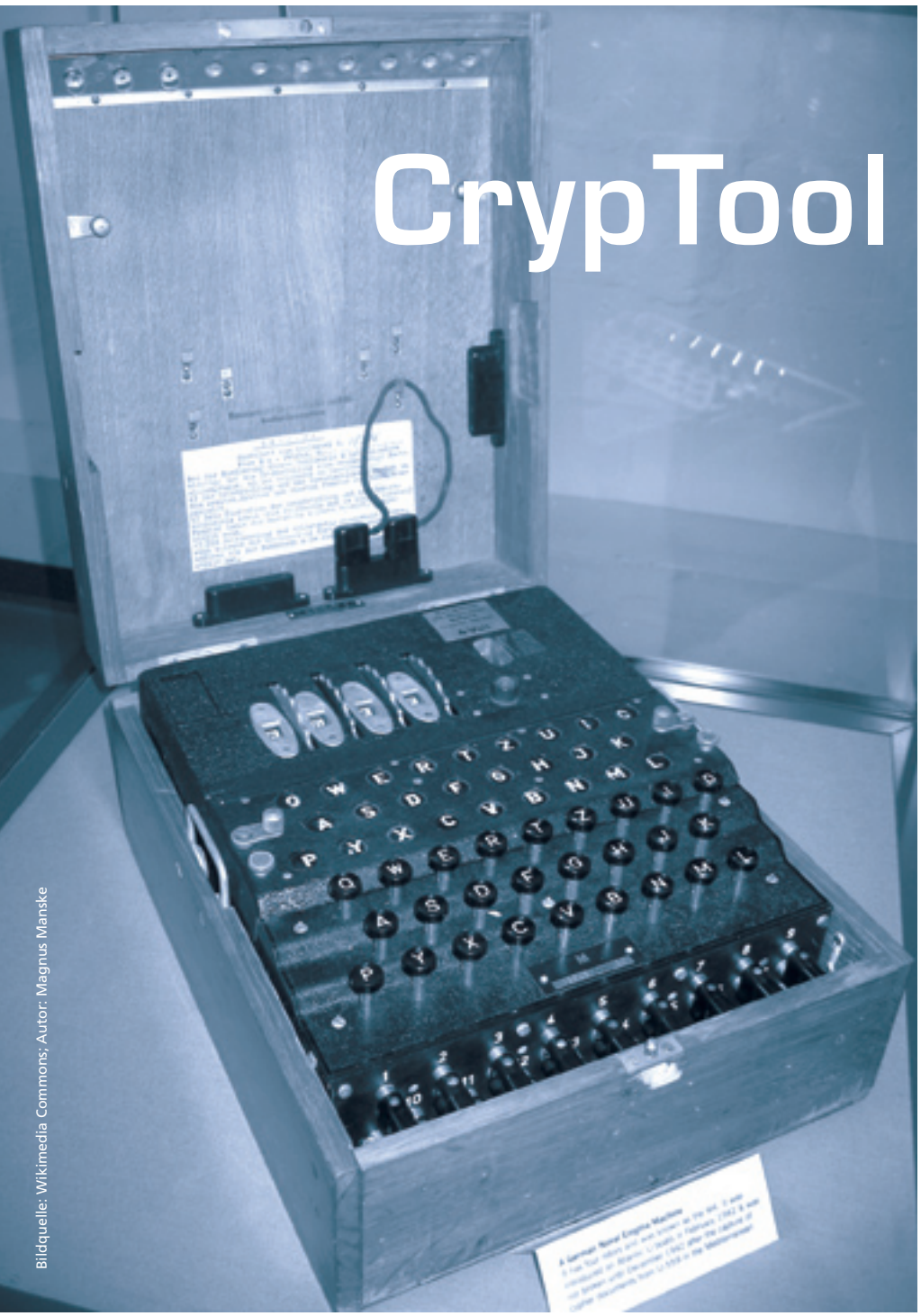
M.Stephan@fz-juelich.de

Klaus Wolkersdorfer
Head of the Division „High Performance Systems“, Jülich Supercomputing Centre

K.Wolkersdorfer@fz-juelich.de

	Blue Gene/L	Blue Gene/P
Eigenschaften der Knoten		
Prozessor	PowerPC® 440	PowerPC® 450
Prozessoren pro Knoten (Chip)	2	4
Prozessor Taktrate	700 MHz	850 MHz
Kohärenz	Durch Software gemanagt	SMP
L3 Cache	4 MB	8 MB
Physikalischer Hauptspeicher pro Knoten	512 MB	2 GB
Speicherbandbreite	5,6 GB/s	13,6 GB/s
Peak-Performance	5,6 GFlop/s	13,6 GFlop/s
Torus-Netzwerk		
Bandbreite	2,1 GB/s	5,1 GB/s
Hardware-Latenzzeit (für nächste Nachbarn)	200 ns (32B Paket) 1,6 µs	160 ns (32B Paket) 1,3 µs (256B Paket)
Netzwerk für globale Operationen		
Bandbreite	700 MB	1700 MB
Hardware-Latenzzeit (im schlechtesten Fall)	5,0 µs	3,0 µs

Tabelle 1: Blue Gene/L im Vergleich zu Blue Gene/P



Bildquelle: Wikimedia Commons; Autor: Magnus Manske

Ein E-Learning-Programm für Kryptologie

Zumeist unsichtbar kommen kryptographische Verfahren in vielen Bereichen des modernen Lebens zum Einsatz – vom Pay-TV, der Wegfahrsperre im Auto, dem Handy, der SSL-Verbindung beim Surfen, der Verschlüsselung beim Digital-Rights-Management bis zur bekanntesten Anwendung, der E-Mail. Und obwohl viele Menschen als Kind einmal versucht haben, Nachrichten zu verschlüsseln, finden nur sehr wenige Zugang zu den modernen Verfahren der Kryptographie. Mit dem seit 1998 entwickelten Open-Source-Programm „CrypTool" lassen sich klassische und moderne Kryptographie und Kryptoanalyse „spielerisch" erfahren. Dabei erklärt CrypTool nicht nur die Verfahren der Kryptographie, sondern bietet zusätzlich Analyse-Funktionen und Angriffs-Simulationen.

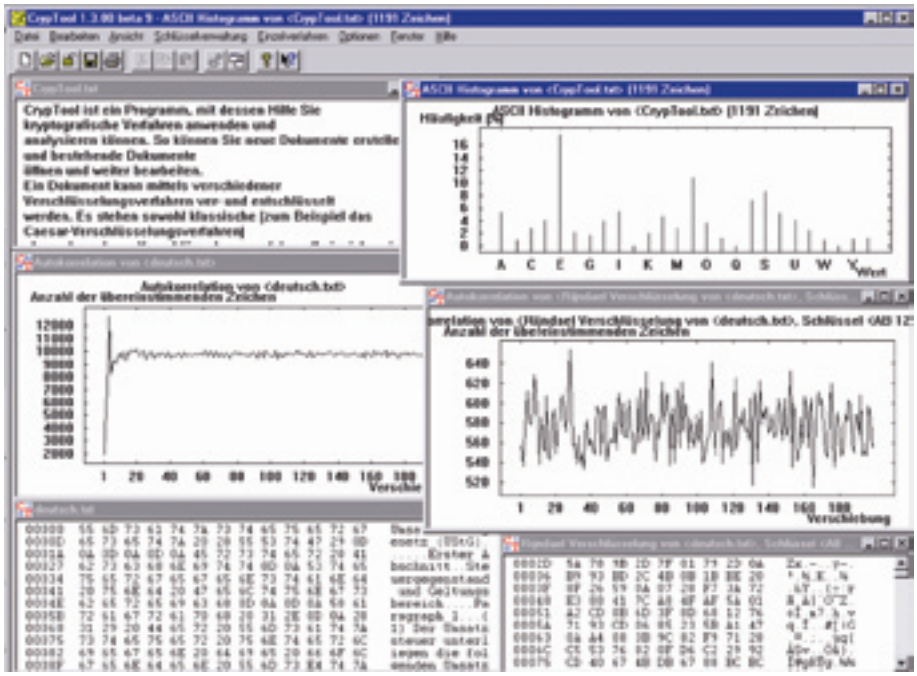
Seinen Ursprung hat CrypTool in der betrieblichen Ausbildung im Awareness-Programm einer Großbank, mit dem Ziel, Mitarbeiter für Fragen der Datensicherheit zu sensibilisieren. Seit dem offiziellen Projektstart an der Technischen Universität Darmstadt im Jahr 1998 wurde das Projekt mit einem Aufwand von mehr als 18 Mannjahren durchgeführt. Seit der Jahrtausendwende ist CrypTool inzwischen als Freeware verfügbar und befindet sich seit 2002 auf der Bürger-CD des Bundesamtes für Sicherheit in der Informationstechnik BSI mit Namen „Ins Internet – mit Sicherheit". Inzwischen wird CrypTool an vielen in- und ausländischen Schulen und Hochschulen in der Ausbildung/Lehre eingesetzt (in Themenfeldern wie Informatik, Kryptologie, Internetsicherheit und Digitale Signaturen).

Seit diesem Jahr ist CrypTool dreisprachig in deutsch, englisch und in polnisch verfügbar. Das Paket wird rund 3.000 mal pro Monat herunter geladen (davon entfallen 1/3 auf die englische Version). Rund 30 größtenteils ehrenamtliche Mitarbeiter verschiedener Firmen und Universitäten beschäftigen sich derzeit mit der Weiterentwicklung der Plattform. Weitere Projekt-Mitarbeiter und verwertbare vorhandene Sourcen sind dabei immer herzlich willkommen.

Was bietet CrypTool?

CrypTool ist ein Freeware-Programm, mit dem sich kryptographische Verfahren anwenden und analysieren lassen. CrypTool enthält eine sehr umfangreiche Online-Hilfe, die auch ohne tiefes Kryptowissen verstanden werden kann. Das Programm beinhaltet fast alle State-of-the-art-Kryptofunktionen und ermöglicht unter einer einheitlichen Benutzeroberfläche einen „spielerischen" Einstieg in die Kryptographie.

Dabei stehen sowohl klassische wie moderne Kryptoverfahren zur Verfügung. Unter den klassischen Verfahren finden sich zum Beispiel das Caesar-, das ADFGVX-, das Doppelwürfel- oder das Enigma-Verschlüsselungsverfahren. Unter den modernen das RSA-Verfahren das AES-Verfahren, die Hybridverschlüsselung und auf Gitterreduktion und Elliptischen Kurven basierende Verfahren.



In CrypTool stehen verschiedene Textanalyseverfahren zur Verfügung. Damit können die Schwächen von einfachen Verschlüsselungsverfahren aufgedeckt und diese teilweise auch automatisch gebrochen werden. Wird ein Dokument verschlüsselt, so wird das Ergebnis in ein Fenster geschrieben. Der Titel des Ergebnisfensters enthält den Namen des Ausgangsdokuments und den benutzten Schlüssel. Der Umgang mit Schlüsseln wird durch 2 Ikons erleichtert: Mit dem Ikon „Schlüssel anzeigen" lässt sich der benutzte Schlüssel aus einem Ergebnisfenster in einen internen Speicher kopieren. Beim Verschlüsseln eines weiteren Dokuments ist dann die Ikone „Schlüssel einfügen" in der Schlüsseleingabemaske aktiv. Nützlich ist dies vor allem bei komplexeren Schlüsseln (wie sie z.B. bei den homophonen Verfahren auftreten).

Analyse mit Hilfe von N-Grammen und umfangreicher Hilfefunktion

Für die klassischen Verschlüsselungsverfahren stehen automatische Analysen zur Verfügung, mit denen aus dem Chiffrat der Schlüssel und der Klartext ermittelt werden kann. Zur Unterstützung der eigenen Analyse von Dokumenten kann CrypTool von einem Dokument das Histogramm anzeigen, die Statistik beliebiger N-Gramme ermitteln und Entropie und Autokorrelation berechnen.

Bei CrypTool wurde darauf Wert gelegt, dass man sich an jeder Stelle im Programm mit der F1-Taste Kontext-sensitive Online-Hilfe holen kann. Zum Einarbeiten können sich Nutzer sehr einfach durch die Menüs bewegen und immer dann F1 drücken, wenn sie einen interessanten Eintrag sehen oder auf einen unbekannten Terminus stoßen.

Die umfangreiche Hilfe enthält die Erklärungen aller kryptographischen Grundbegriffe, eine Liste mit Literaturhinweisen aus dem Bereich Kryptographie, eine Zeittafel mit einem historischen Überblick, einen gut sortieren Index zu den behandelten Kryptographie-Themen sowie Tutorials für einen schnellen Einstieg.

E-Learning durch interaktive Einzelverfahren mit verständlichen Schritten

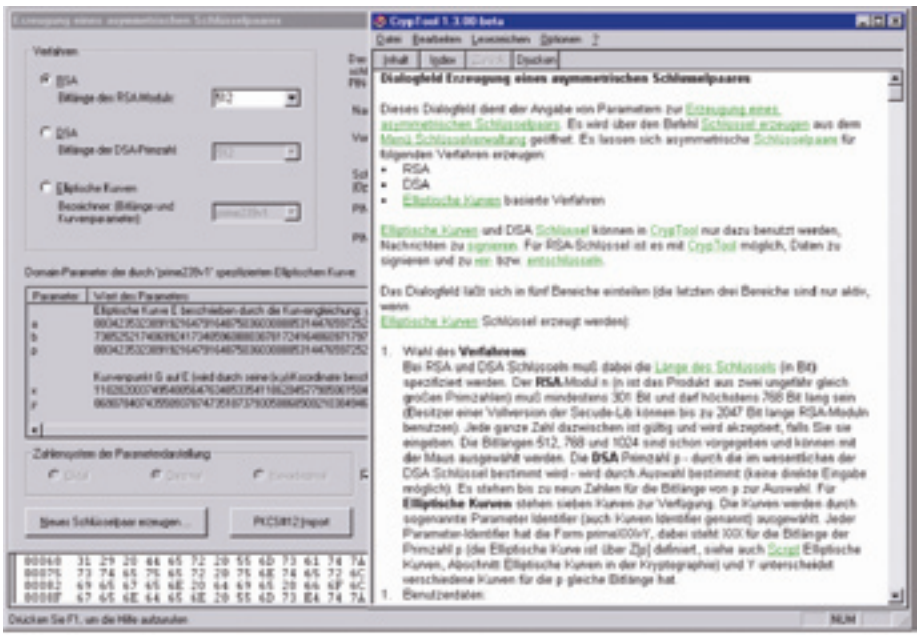
Die Verschlüsselungsfunktionen im Menü „Ver-/Entschlüsseln" sind so implementiert, dass sie möglichst effizient aufgerufen und durchgeführt werden können. Dagegen wurden die Funktionen im Menü „Einzelverfahren" schrittweise und interaktiv implementiert, so dass die E-Learning-Aspekte in den Vordergrund treten.

Im Menü Einzelverfahren werden verschiedene einzelne Verfahren und Protokolle angeboten, beispielsweise:

- Hashwerte berechnen und ihre Sensitivität demonstrieren.
- Message-Authentication-Codes (MACs) erstellen.
- Starke Schlüssel nach dem PKCS#5-Standard aus einem Passwort generieren.
- Dokumente komprimieren und wieder entkomprimieren – damit können die Auswirkungen der Komprimierung von Dateien im Vorfeld einer Verschlüsselung analysiert werden.
- Zufallsdaten erzeugen oder analysieren.
- Protokolle zur Authentisierung und Schlüsselvereinbarung (DH) demonstrieren.
- Einzelne Verschlüsselungsverfahren schrittweise vor- und zurück durchlaufen (mit ANIMAL).
- Verbreitete Codierungen wie base64 und uuencode anwenden.

Welche Funktionen in den Menüs ausgewählt werden können, hängt vom Typ des aktiven Dokuments ab. Die Menüs und Untermenüs von CrypTool werden

Die Fähigkeiten von CrypTool werden aktiv durch die umfangreiche Hilfe unterstützt.



dynamisch aufgebaut, abhängig davon, ob im Hauptfenster eine Datei geladen ist und ob die aktive Datei vom Typ Textdatei, Binärdatei oder Grafikanzeige ist. Inaktive Menüpunkte, die für das aktive Dokument nicht nutzbar sind, werden im CrypTool-Menü ausgegraut.

Schwerpunkt asymmetrische Verschlüsselung

Einer der Schwerpunkte in CrypTool sind asymmetrische Verschlüsselungsverfahren, die in vielen Bereichen, vor allem im Internet, die Grundlage für sichere Kommunikation darstellen. Ein asymmetrisches Kryptosystem besteht stets aus einem geheimen Teil, dem privaten Schlüssel, und einem öffentlicher Schlüssel. Der private Schlüssel ermöglicht es seinem Inhaber, Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren. Der öffentliche Schlüssel ermöglicht es jedermann, Daten für den Schlüsselinhaber zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Im Gegensatz zu einem symmetrischen Kryptosystem müssen die kommunizierenden Parteien keinen gemeinsamen geheimen Schlüssel kennen.

Der Durchbruch bei der Entwicklung eines asymmetrischen Algorithmus gelang in den 1970er Jahren dem New Yorker Mathematiker Ronald L. Rivest, dem israelischen Kryptologen Adi Shamir und kalifornischen Computerwissenschaftler Leonard M. Adleman, die 1977 gemeinsam das nach den Anfangsbuchstaben ihrer Nachnamen benannte RSA-Verfahren veröffentlichten. Es gilt bis heute als sicheres Verfahren und hat außerdem den großen Vorteil, sowohl zu Ver-/Entschlüsseln als auch zum Signieren/Verifizieren eingesetzt werden zu können, und durch die Vergrößerung der Schlüssellänge die Sicherheit skalieren zu können (Modul n = das Produkt zweier ca. gleich großer Primzahlen hat heute sinnvolle Längen von 768, 1024 oder 2048 Bit).

Das RSA-Kryptosystem ist in CrypTool in allen Einzelheiten und für verschiedene Codierungen dargestellt. Der RSA-Schlüssel wird ausgehend von den beiden selbst erzeugten Primzahlen generiert. Schlüsselerzeugung sowie die Ver- und Entschlüsselung kann in allen Einzelschritten sowohl für kleine als auch für sehr große Zahlen nachvollzogen werden.

Die Faktorisierung von Zahlen ist auch für die Kryptographie eine wichtige Anwendung. Mit den in CrypTool vorgestellten Faktorisierungsalgorithmen lassen sich einfache RSA-Kryptosysteme leicht knacken. Damit erhalten Anwender eine Idee für die Mindestschlüssellänge sicherer Verfahren.

Mit der Dialogbox „Das RSA-Kryptosystem" können Sie auch Varianten des RSA-Verfahrens durchspielen (unterschiedliche Schlüssellänge, verschiedene Alphabete, verschiedene Blocklänge).

Interaktive Demonstrationen / Visualisierungen

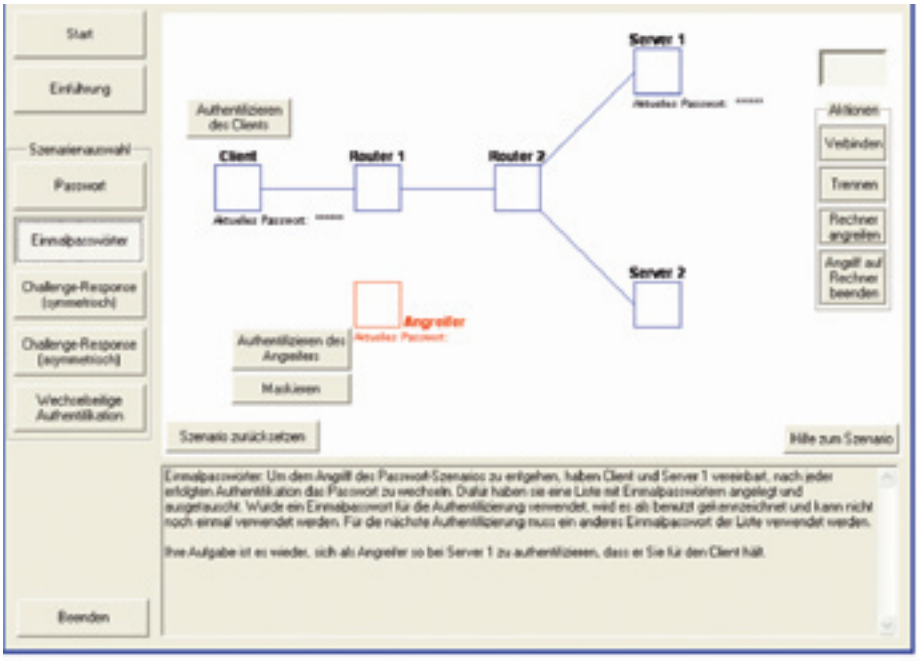
CrypTool bietet außerdem eine umfangreiche Bibliothek interaktiver visueller Demonstrationen, die zu einem tieferen Verständnis für eine Vielzahl von Problemstellungen verhelfen.

Von der Erzeugung einer elektronischen Signatur, der Hybridverschlüsselung über Hashverfahren bis zu Schlüsselaustauschverfahren oder Seitenkanalangriffen werden unterschiedliche Anwendungs- und Sicherheitsfälle simuliert und visualisiert.

Von UID/PW und One-Time-Password über (einseitige) Challenge-Response (symmetrisch + asymmetrisch) bis zu asymmetrischer gegenseitiger Authentisierung.

Der Benutzer kann interaktiv steuern, wie der Angreifer vorgeht (Rechner übernehmen, Verbindungen aufbauen oder trennen, lauschen).

Demo zu Authentisierungsmöglichkeiten im Netz: Von UID/PW und One-Time-Password über (einseitige) Challenge-Response (symmetrisch + asymmetrisch) bis zu asymmetrischer gegenseitiger Authentisierung. Der Benutzer kann interaktiv steuern, wie der Angreifer vorgeht (Rechner übernehmen, Verbindungen aufbauen oder trennen, lauschen).



Bernhard Esslinger

Dozent Uni Siegen
Institut für Wirtschaftsinformatik
bernhard.esslinger@db.com

Kai Hoelzner

DFN-Verein
hoelzner@d**fn.de**

Ausblick

Seit Juli 2007 ist CrypTool in seiner jüngsten Release-Version 1.4.10 verfügbar. Neuerungen sind unter anderem ein Lernprogramm für die Grundlagen der Zahlentheorie, Flash-Animationen zum AES-Verfahren und zur Enigma-Chiffriermaschine sowie eine Demonstration der Addition auf reellen und diskreten Elliptischen Kurven.

Das CrypTool-Projekt wurde vor kurzem für die Veranstaltungsreihe „Deutschland – Land der Ideen" in der Kategorie „Wissenschaft und Technik" ausgewählt: Diese vom Bundespräsidenten im Jahr der Fußball-Weltmeisterschaft eingeführte Standortinitiative prämiert „Orte", die zukunftsorientierte Ideen entwickeln und aktiv umsetzen. Das CrypTool-Projekt wird damit insbesondere am 22.07.2008 in Siegen präsentiert.

Für 2008 sind etliche weitere Neuerungen geplant: Das größte Projekt für die Zukunft ist die vollständige Neuentwicklung der Software mit Eclipse/Java (zusammen mit der Universität Darmstadt), mit der CrypTool plattformunabhängig auf allen Betriebssystemen läuft und Linux- und Mac-Nutzern lästige Windowsemulationen erspart. Daneben wird der direkte Nachfolger CrypTool 2 in .NET mit C# auf einem schlanken Architekturdesign erstellt (zusammen mit der Universität Duisburg-Essen).

Außerdem wird an der auf der GI-Konferenz INFOS2007 geborenen Idee gearbeitet, ein Portal zu erstellen, das Lehrern eine zentrale Anlaufstelle zum Austausch von Unterrichtseinheiten zum Thema Kryptologie bietet.

Eine Demo für einen Seitenkanalangriff gegen ein typisches Hybridverschlüsselungsprotokoll: Bei einer nicht optimalen Implementierung, wie sie in der Realität vorkam, kann der Angreifer den Sessionkey durch Protokoll-gerechte Anfragen an den Server hoch effizient berechnen.

Rollout von Zertifikaten leichter gemacht

SOAP-Schnittstelle erweitert die Möglichkeiten in der DFN-PKI

Die Beantragung, Genehmigung und Ausstellung von Zertifikaten in der DFN-PKI funktioniert für einzelne Nutzer mit Hilfe eines Webbrowsers einfach und bequem. Doch was ist zu tun, wenn es gilt, mehrere hundert oder gar tausend Anträge für Nutzer- oder Serverzertifikate zu bearbeiten? Wie können Zertifikate der DFN-PKI auf USB-Kryptotoken oder SmartCards gebracht werden, die bereits im Einsatz sind? Für diese Fragen gibt es jetzt eine Antwort: Eine SOAP-Schnittstelle, die eine maschinelle Kommunikation mit den Servern der ausgelagerten Zertifizierungsstellen in der DFN-PKI ermöglicht.

Neue Schnittstelle

Im bisherigen Ablauf einer Zertifizierung in der DFN-PKI stellt der Zertifikatnehmer einen Antrag, der danach durch die Registrierungsstelle genehmigt wird. Beide Vorgänge werden in einem Webbrowser auf einer für Menschen konzipierten Benutzeroberfläche durchgeführt. Jeder Antrag muss einzeln gestellt und von der Registrierungsstelle einzeln digital signiert und genehmigt werden. Eine Möglichkeit, über diese Webschnittstellen auch eine größere Anzahl von Nutzerzertifikaten zu bearbeiten, ist das sogenannte Self-Service Verfahren. Dabei werden policy-konform geprüfte Nutzerdaten von der Registrierungsstelle in einer Datei an die Zertifizierungsstelle übermittelt und der Nutzer kann sich sein Zertifikat über die Webschnittstelle „abholen". Aber auch bei diesem Verfahren ist menschliche Interaktion notwendig.

Die SOAP-Schnittstelle der DFN-PKI ermöglicht jetzt eine Kommunikation nicht mehr nur zwischen Mensch und Maschine, sondern auch zwischen Maschine und Maschine. Die in der Webschnittstelle wählbaren Aktionen wie „Zertifikat beantragen", „Antrag bearbeiten", „Antrag genehmigen" oder „Antragsdatei hochladen" wer-

den in der SOAP-Schnittstelle als ein entfernter Prozeduraufruf durchgeführt. Eine lokal entwickelte Software kann mit Hilfe dieser Prozeduraufrufe alle notwendigen Schritte für eine Zertifizierung durchführen und dabei sowohl die Rolle des Zertifikatnehmers als auch die der Registrierungsstelle einnehmen. Die SOAP-Schnittstelle bietet damit alle Möglichkeiten, die auch in der Webschnittstelle zur Verfügung stehen. Darüber hinaus kann der Zertifizierungsprozess durch den Einsatz lokaler Software individuell an die jeweiligen Anforderungen angepasst werden *(Abbildung 1)*.

Die neuen Möglichkeiten in der DFN-PKI

- Einbindung existierender Prozesse
- Verwendung lokaler Datenquellen
- Automatisierte Ausstellung von sehr vielen Zertifikaten
- Lokale Initialisierung kryptographischer Geräte
- Erzeugung eines lokalen Schlüssel-Backup
- Diverse Abfragen für Statistiken

Abb. 1: Erweiterungen der DFN-PKI

Anwendungen

Durch die Bereitstellung der SOAP-Schnittstelle besteht nun die Möglichkeit, bereits vorhandene lokale Strukturen und Prozesse in die DFN-PKI einzubinden. Die Erzeugung der Schlüssel und der Zertifikatanträge sowie deren Genehmigung können jetzt durch eine selbst entwickelte Software durchgeführt werden. Da diese Software lokal - und nicht auf den vom DFN betriebenen Servern der ausgelagerten Zertifizierungsstelle - läuft, kann auch bei der Beschaffung der Zertifikatdaten (Name, E-Mail Adresse etc.) direkt auf lokale Quellen wie z.B. einen Verzeichnisdienst oder eine Datenbank zugegriffen werden. Entscheidend ist, dass die Eingabe dieser Daten entsprechend der Policy der DFN-PKI vorgenommen wurde, das heißt insbesondere, dass eine persönliche Identifizierung durch Vorlage eines Ausweispapiers durchgeführt wurde. Wenn eine persönliche Identifizierung bereits in den lokalen Prozessen - z.B. Ausweisvorlage bei der Immatrikulation - verankert ist, genügen die Daten den Anforderungen der DFN-PKI Policy. An der Fachhochschule Landshut wurde die Integration der lokalen Infrastruktur in die DFN-PKI bereits erfolgreich durchgeführt. Einen Erfahrungsbericht dazu gibt der Artikel von Herrn Hartmann in diesem Heft.

Mit dem Zugriff auf lokale Datenquellen, die die notwendigen Zertifikatinformationen enthalten und der Möglichkeit, ohne weitere Interaktionen von Nutzern, Administratoren oder Mitarbeitern der Registrierungsstelle Zertifikatanträge zu stellen bzw. zu genehmigen, ist nun die schnelle Verarbeitung einer großen Anzahl von Zertifikatanträgen ohne weiteres möglich. Die Realisierung an der FH Landshut hat gezeigt, dass über die SOAP-Schnittstelle mehrere hundert Zertifikate innerhalb von wenigen Minuten problemlos ausgestellt und übermittelt werden können.

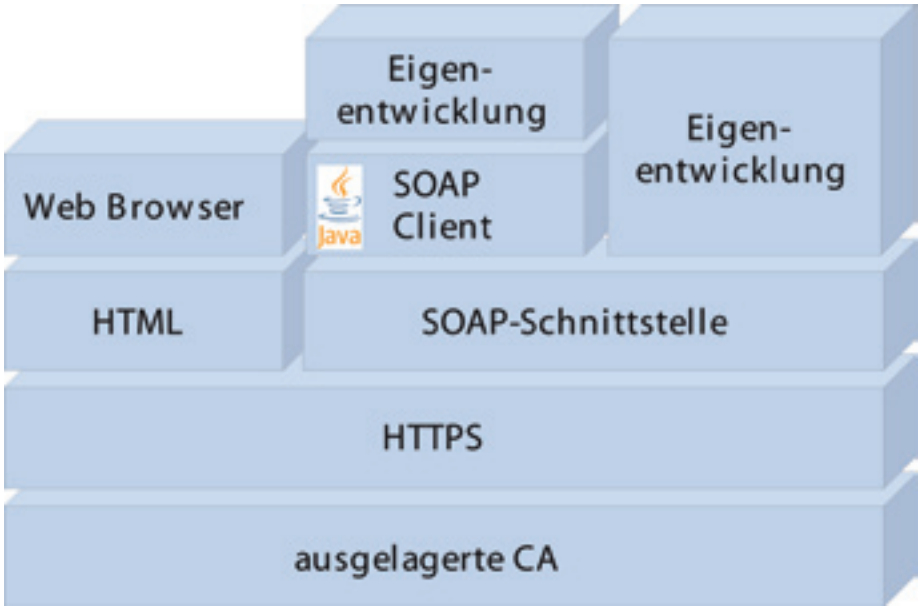
Eine weitere Anwendung der SOAP-Schnittstelle ist die Bestückung von USB-Kryptotoken oder SmartCards mit Zertifikaten der DFN-PKI. Eine lokale Software kann einen Zertifikatantrag erstellen, genehmigen, an die Zertifizierungsstelle übermitteln, das ausgestellte Zertifikat empfangen und auf das kryptographische Gerät schreiben. Interessant ist bei dieser Vorgehensweise die Möglichkeit, zuvor eine lokale Kopie des generierten privaten Schlüssels zu erzeugen und diese in verschlüsselter Form zu speichern. Dies ist unabdingbar, wenn die Zertifikate zur Verschlüsselung eingesetzt werden sollen, da ohne eine Sicherheitskopie des privaten Schlüssels bei einem Defekt oder Verlust des kryptographischen Gerätes die verschlüsselten Daten nicht mehr wiederhergestellt werden können.

Die SOAP-Schnittstelle bietet außerdem die Funktionalität, Listen von Anträgen und Zertifikaten zu erstellen. Durch Auswertung dieser Listen mit einer geeigneten Software können dann für ausgelagerte Zertifizierungsstellen Statistiken in beliebiger Form erstellt werden. Denkbar sind hier einfache Übersichten wie z.B. eine Liste der Gesamtanzahl von Zertifikaten einer Zertifizierungsstelle bis hin zur Anzeige von allen bereits mit einem Zertifikat versehenen Servern der Einrichtung. Eine entsprechende Software könnte die Informationen z.B. auch nutzen, um bald ablaufende Zertifikate zu ermitteln und eine Verlängerung dieser Zertifikate automatisch durchzuführen.

Konzeptionelle Einordnung

Die SOAP-Schnittstelle ist als Ergänzung zu der bestehenden Webschnittstelle zu sehen und kann parallel zu dieser betrieben werden *(Abbildung 2)*. So können Anträge in der Webschnittstelle gestellt und in der SOAP-Schnittstelle genehmigt werden und umgekehrt. Die SOAP-Schnittstelle kann entweder durch eine SOAP-Implementierung für die jeweilige Programmiersprache oder durch einen eigens für die DFN-PKI entwickelten SOAP-Client angesprochen werden. Dieser SOAP-Client wird vom DFN-Verein zur Verfügung gestellt und beinhaltet bereits viele häufig gebrauchte kryptographische Funktionen wie z.B. das digitale Signieren. Damit wird die Kommunikation mit den Servern der ausgelagerten Zertifizierungsstelle deutlich vereinfacht.

Abb. 2: Schnittstellen in der DFN-PKI



Gerti Foest

DFN-Verein
foest@dfn.de

Jan Mönnich

DFN-PCA
moennich@dfn-cert.de

Technik

Mit der SOAP-Schnittstelle wurde ein Webservice implementiert, der auf dem SOAP-Protokoll basiert. Dabei handelt es sich um ein Protokoll, mit dem auf Basis von XML Nachrichten ausgetauscht werden können. Bei diesen Nachrichten kann es sich entweder um generelle Dokumente oder, wie in diesem Fall, um entfernte Prozeduraufrufe (Kommunikationsstil rpc/encoded) handeln. Die Übertragung des Protokolls ist nicht festgelegt, erfolgt jedoch in den meisten Fällen über HTTP(S) und TCP, was auch auf die SOAP-Schnittstelle der DFN-PKI zutrifft.

Die SOAP-Schnittstelle ist analog zu der Webschnittstelle aufgebaut: Die Beantragung von Zertifikaten kann ohne eine Authentifizierung mit entsprechenden SOAP-Aufrufen über eine URL erfolgen. Der Zugang zu einer weiteren URL, über die SOAP-Aufrufe zur Bearbeitung und Genehmigung von Zertifikatanträgen abgesetzt werden können, ist nur mit einer SSL-Client-Authentifizierung mit einem Zertifikat der Registrierungsstelle möglich.

Die Aufrufe in der SOAP-Schnittstelle sind den Aktionen in den bestehenden Webschnittstellen nachempfunden. Einige Beispiele für den Zusammenhang zwischen einer Aktion in einer der Webschnittstellen und dem entsprechenden SOAP-Aufruf sind in *Abbildung 3* dargestellt.

Die SOAP-Schnittstelle ist durch WSDL (Web Service Description Language) für Maschinen beschrieben. Viele SOAP-Implementierungen können auf Basis dieser standardisierten Beschreibung Quellcode für die jeweilige Programmiersprache erzeugen, so dass die Prozeduren direkt als Befehle ausgeführt werden können.

Fazit

Die SOAP-Schnittstelle der DFN-PKI ermöglicht eine maschinelle Kommunikation mit den Servern der ausgelagerten Zertifizierungsstellen in der DFN-PKI und damit die Einbindung eigener Programmentwicklungen in den Zertifizierungsprozess. So kann eine Anpassung des Zertifizierungsvorgangs an verschiedenste lokale Anforderungen erreicht werden. Insbesondere können bereits vorhandene Prozesse jetzt in die DFN-PKI integriert werden. Die Kompatibilität zwischen der gewohnten Webschnittstelle und der neuen SOAP-Schnittstelle ist gegeben, so dass diese miteinander kombiniert werden können. Die Programmierung einer eigenen Anwendung ist aufgrund der Dokumentation der Schnittstelle in WSDL und des sofort verwendbaren SOAP-Clients einfach und schnell umzusetzen.

Bei Interesse an den neuen Möglichkeiten wenden Sie sich bitte an pki@dfn.de, eine ausführliche Dokumentation der Schnittstelle inklusive Beispiel-Quelltexten für mehrere Programmiersprachen senden wir Ihnen dann gerne zu.

Abbildung 3: Zusammenhang Aktion Webschnittstelle / SOAP-Aufruf

Webschnittstelle	SOAP-Aufruf
Nutzer stellt Antrag	**newRequest**
Nutzer druckt Antrag aus	**getRequestPrintout**
RA ruft Antrag auf	**getRawRequest**
RA genehmigt Antrag	**approveRequest**
Nutzer erhält Zertifikat	**getCertificateByRequestSerial**

Umzug des DFN-CERT

Anfang Dezember 2007 ist das DFN-CERT in Hamburg umgezogen. Die neue Adresse lautet:

DFN-CERT Services GmbH
Sachsenstraße 5
20097 Hamburg

Alle bekannten E-Mail-Adressen und Telefonnummern bleiben unverändert.

15. DFN-Workshop „Sicherheit in vernetzten Systemen“

Am 13. und 14. Februar 2008 findet im CCH Hamburg bereits zum fünfzehnten Mal der DFN-Workshop „Sicherheit in vernetzten Systemen“ statt. Der Kanadier Dick Hardt von Sxip Identity wird die Veranstaltung mit einem sehr speziellen Vortrag zum Thema „Identity Management“ eröffnen. Natürlich erwartet die Teilnehmer außerdem eine Reihe vielfältiger interessanter Beiträge: Die aktuell heiß diskutierten Themenbereiche „Online-Durchsuchungen“ und „Botnetze“ bilden zwei Schwerpunkte des Programms.

Im Anschluss an den Workshop findet ein Tutorium zum Thema „Praktische Rechtsfragen“ statt.

Das komplette Programm sowie Informationen zur Anmeldung finden Sie auf den Seiten des DFN-CERT unter https://www.dfn-cert.de/events/ws/2008/

Feuerprobe für DFN-PKI

Die Zertifizierungsstelle der FH Landshut in der DFN-PKI – Ein Erfahrungbericht

Seit dem Wintersemester 2006 müssen sich die Studierenden der FH Landshut für die Nutzung der Onlinedienste der Hochschule mit einem Zertifikat authentifizieren. Für das Wintersemester 2007 sollten diese Zertifikate erstmalig im Sicherheitsniveau Global der DFN-PKI ausgestellt werden. Eine Feuerprobe für die Integration einer gut etablierten lokalen Infrastruktur in die DFN-PKI mit Hilfe der vom DFN-Verein neu entwickelten SOAP-Schnittstelle (siehe Artikel „Rollout von Zertifikaten leichter gemacht" in diesem Heft). Am 18. September 2007 begann der „Belastungstest" mit der Übermittlung von mehr als 450 Zertifikatanträgen an die ausgelagerte Zertifizierungsstelle der FH Landshut. Die Zertifikate wurden innerhalb kürzester Zeit von der Zertifizierungsstelle erzeugt, der lokalen Infrastruktur zugestellt und konnten dann in gewohnter Prozedur von den Studierenden „abgeholt" werden.

Abbildung 1: Startseite der FH Landshut CA

Bis Mitte November 2007 wurden mit diesem Verfahren über 1500 Zertifikate erstellt – die Feuerprobe ist bestanden. Der Artikel beschreibt den Weg vom Aufbau der lokalen Zertifizierungsinfrastruktur bis zu deren Integration in die DFN-PKI über die neue SOAP-Schnittstelle.

Der Anfang – ein Studienprojekt

Im Jahr 2001 entwickelten fünf Studierende des Fachbereichs Informatik die erste Zertifizierungsstelle (CA – Certification Authority) an der FH Landshut – eigentlich eine prototypische Implementierung im Rahmen eines Studienprojekts. Um die Nutzung der Projektergebnisse interessant zu machen, wurde in einem parallelen Projekt die elektronische Noteneinsicht als Schlüsselanwendung für den Einsatz von Zertifikaten implementiert. Die Studierenden sollten mit Hilfe ihres Zertifikats durch eine SSL-Client-Authentifizierung die aktuellen Prüfungsnoten über das Internet abfragen können.

Eine wertvolle Hilfe bei der Realisierung der FH Landshut CA war der Ergebnisbericht eines DFN-Projektes zum Thema PKI, der im März 2000 veröffentlicht worden war: „Aufbau und Betrieb einer Zertifizierungsstelle". Wie dort vorgeschlagen, wurde die Zertifizierungsstelle auf Basis von OpenSSL realisiert. Sie wurde auf einem Notebook implementiert, das keinen

Netzanschluss hatte und das außerhalb der Öffnungszeiten der Zertifizierungsstelle in einem Tresor eingeschlossen wurde.

Neben der technischen Ausführung waren etliche administrative Aufgaben zu lösen. Die größten Probleme in diesem Zusammenhang stellten die Authentifizierung der Nutzer und die eindeutige Namensvergabe dar. Zur Namensvergabe wurde eine etablierte Methodik des Rechenzentrums genutzt, das schon lange eindeutige Accountnamen aus den Benutzernamen erzeugt und dabei auch konsistent mit dem dritten „Michael Maier" umgehen kann. Daher wurde als Voraussetzung für die Erstellung eines Zertifikats die Existenz eines gültigen Benutzeraccounts am Rechenzentrum der FH gefordert. Der Accountname ist Bestandteil des eindeutigen Namens im Zertifikat. Weiter musste sich jeder Studierende bei der Antragstellung mit seinem gültigen Studentenausweis mit Lichtbild ausweisen.

Die ersten Zertifikate und ihre Nutzung

Im Januar 2002 war es geschafft: Die ersten Zertifikate wurden ausgestellt, gleichzeitig wurde ein SSL-Server zur Notenabfrage in Betrieb genommen. An zwei Nachmittagen in der Woche hatte die Zertifizierungsstelle geöffnet. Die Daten der Studierenden wurden manuell über eine Weboberfläche in ein Notebook eingegeben, die lokal erzeugten Zertifikate auf Diskette geschrieben und den Antragstellern mitgegeben. Sehr bald bildeten sich lange Schlangen vor der Registrierungsstelle. Die Bearbeitung eines Antrags dauerte mehrere Minuten und der Anreiz der elektronischen Noteneinsicht führte schon sehr schnell zu mehreren hundert Nutzern.

Insbesondere während der Prüfungszeiten blieben die Warteschlangen bei der Registrierung bestehen. Zum einen betrug die Laufzeit der Zertifikate nur ein Jahr, danach musste ein neuer Antrag gestellt werden. Zum anderen sprach sich die Nützlichkeit der Zertifikate schnell herum und die Nutzerzahl nahm stetig zu. Dabei waren die Nutzer über alle Fachbereiche relativ gleichmäßig verteilt, es waren keineswegs nur die Studierenden der technischen Fachbereiche, die Zertifikate beantragten.

Von Anfang an hat sich die Zertifizierungsstelle der FH Landshut in die Hierarchie der DFN-PKI gestellt. Der erste CA-Schlüssel der FH Landshut wurde am 25. Januar 2002 vom DFN nach der World Wide Web Policy 1.2 zertifiziert.

Der nächste Schritt

Im Sommersemester 2004 wurde ein neues Studienprojekt zum Thema Zertifizierungsstelle gestartet, das die Zertifikaterstellung und -verteilung schneller und einfacher gestalten sollte. OpenSSL, MySQL und der Apache Webserver bildeten die Grundlage.

Zunächst wurde dabei die Zertifizierung von der Registrierung getrennt. Bei der Registrierungsstelle (RA – Registration Authority) mussten die Antragsteller nur noch ihren Studentenausweis vorlegen. Mit Hilfe der Matrikelnummer konnten die Studentendaten aus dem LDAP-Server der Fachhochschule abgefragt werden, damit wurde gleichzeitig bestätigt, dass der Antragsteller registrierter Studierender der Fachhochschule war. Auch Mitarbeiter der Fachhochschule konnten Zertifikate beantragen, die Mitarbeiterdaten wurden ebenfalls aus dem LDAP-Server entnommen.

Nach erfolgreicher Antragstellung wurden bei der RA das Schlüsselpaar und der Zertifikatantrag (CSR – Certificate Signing Request) erzeugt. Der Antragsteller erhielt auf einer schriftlichen Bestätigung ein Zertifikatpasswort, das zum Schutz seines privaten Schlüssels diente. Die Zertifizierungsstelle wurde auf einem PC mit herausnehmbarer Festplatte realisiert. Diese Festplatte wurde nur zur Zertifizierung, in der Regel zweimal in der Woche, aus dem Tresor genommen, um die Requests herunter zu laden, zu signieren und die Zertifikate wieder auf die RA herauf zu laden. Die RA erzeugte dann die fertigen Nutzerzertifikate, indem sie den passwortgeschützten privaten Schlüssel mit dem Zertifikat zu einer Datei nach dem PKCS#12-Standard zusammenpackte. Anschließend wurden die Zertifikate auf dem CA-Webserver zum Download bereitgestellt. Der Nutzer erhielt gleichzeitig eine E-Mail-Benachrichtigung und konnte sich dann nach einer Authentifizierung mit seinem FH-Account und mit Hilfe seines Zertifikatpassworts sein Zertifikat auf seinen PC herunterladen und installieren.

Als weitere wesentliche Neuerung wurde die Möglichkeit einer Online-Zertifikatverlängerung eingeführt. Solange ein Zertifikat noch nicht abgelaufen ist, kann nach einer SSL-Client-Authentifizierung am CA-Webserver ein neues Zertifikat beantragt werden. Dabei wird während der Beantragung im LDAP-Server überprüft, ob der Antragsteller noch immatrikulierter Studierender der FH ist. Falls ja, erhält er das Zertifikatpasswort, mit dem er später sein Zertifikat abholen kann, sofort am Webbrowser angezeigt.

Prof. Peter Hartmann
Fachhochschule Landshut
peter.hartmann@fh-landshut.de

„Zertifikatpflicht" für alle Studierenden

Die neue Zertifizierungsstelle wurde im Frühjahr 2005 erfolgreich in Betrieb genommen. Die deutliche Verbesserung des Ablaufs bei der Zertifikatausstellung ermutigte die Hochschulleitung dazu, die Nutzung der Zertifikate für Onlinedienste der Fachhochschule auszuweiten. Dabei wurde zum Wintersemester 2006 erstmals die Verwendung von Zertifikaten für alle Studierenden der Fachhochschule (etwa 2500) verpflichtend. Die Hochschule richtete ein SB-Portal für Studierende ein, auf das nur mit einem Nutzerzertifikat zugegriffen werden kann und in dem die Studierenden Aktionen wie Prüfungsanmeldung, Rückmeldung oder Ausdruck von Studentenausweisen durchführen können (Abbildung 2). Als weitere freiwillige Anwendungen der Zertifikate können Studierende beispielsweise ihre Notebooks für das WLAN der FH registrieren lassen oder einen VPN-Tunnel von zu Hause in das Hochschulrechenzentrum aufbauen.

Die Einrichtung des SB-Portals bedeutete einen Quantensprung in der Zertifikatnutzung. Dabei war weniger die Anzahl der Antragsteller das Problem, sondern die Tatsache, dass jetzt auch viele Studierende Zertifikate beantragen mussten, die wenig oder keinen Bezug zur Datenverarbeitung hatten, geschweige denn zu dem Konzept des digitalen Ausweises „Zertifikat". Der Supportaufwand für Studierende, die nicht wussten, wie sie Zertifikate downloaden, installieren, nutzen oder auf andere Rechner transportieren können, wuchs explosionsartig an. Geradezu unglaubliche Mengen von abgestürzten PCs, versehentlich formatierten Festplatten, gelöschten Dateien und verlorenen Passworten wurden dem Rechenzentrum gemeldet. Dies stell-

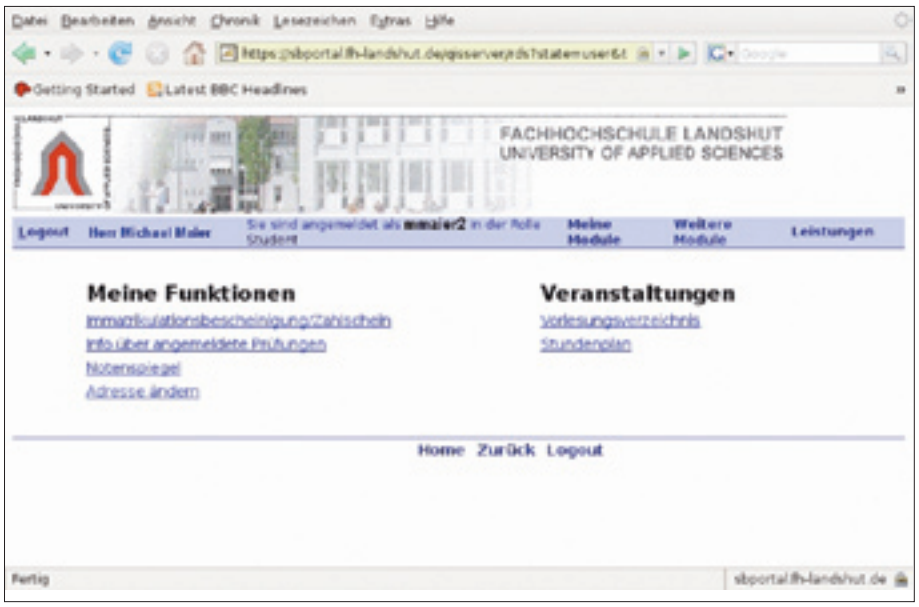


Abbildung 2: SB-Portal der FH Landshut

te zeitweise ein massives Problem dar, da nach der Fertigstellung des Studienprojektes die Zertifizierungsstelle im Rechenzentrum im Wesentlichen nur von – allerdings sehr qualifizierten – studentischen Hilfskräften betreut werden konnte.

Das CA Zertifikat der FH Landshut muss erneuert werden – was nun?

Das inzwischen verwendete zweite Zertifikat der FH Landshut CA hatte eine Laufzeit bis zum 15. Juli 2008. Das bedeutete, dass Studentenzertifikate mit einer Gültigkeitsdauer von einem Jahr nur noch bis zum Sommer 2007 ausgestellt werden konnten. Ende 2006 musste daher eine Rezertifizierung der FH Landshut CA beim DFN beantragt werden. Dies war wider Erwarten nicht mehr so ohne weiteres möglich. Die WWW-Policy wird in der neuen DFN-PKI nicht mehr unterstützt. Eine Anpassung an die neue Policy hätte zu erheblichen organisatorischen Problemen geführt und eine Integration der an der FH eingespielten und bewährten Prozesse wie zum Beispiel der Online-Beantragung einer Zertifkatverlängerung wären nicht möglich gewesen.

Als Alternative wurde vom DFN angeboten, die Zertifizierungsstelle im Auftrag der FH Landshut zu betreiben und die Registrierung über eine Webschnittstelle abzuwickeln. Aber auch die Webschnittstelle passte nicht zu den Prozessen der FH Landshut. Sie skaliert schlecht für große Nutzerzahlen und setzt auf das Konzept der dezentralen Schlüsselerzeugung (Abbildung 3). Es gab jedoch zwei gute Gründe, die zentrale Schlüsselerzeugung beizubehalten:

- Bei Versuchen mit Mitarbeitern wurde festgestellt, dass die eigenverantwortliche Schlüsselerzeugung in einem Browser und die anschließende Integration des Zertifikats in genau diesen Browser ohne Hilfe von Mitarbeitern des Rechenzentrums praktisch nicht möglich war. Es handelt sich um einen relativ komplexen Prozess, der nur sehr selten durchzuführen ist, daher auch nicht eingeübt wird und meistens Support erfordern wird. Dieses Verfahren bei allen Studenten der Fachhochschule anzuwenden, erschien undurchführbar.

- Das Konzept des „digitalen Ausweises", der geschützt aufbewahrt werden muss, ist noch nicht in den Köpfen aller Nutzer verankert. Ständig gab es eine große Menge von Problemen mit nicht importierbaren, verloren gegangenen oder aus anderen Gründen unbrauchbaren Zertifikaten. Die FH Landshut CA führt zwar keine Schlüsselwiederherstellung durch, jedoch werden die mit dem Zertifikatpasswort geschützten PKCS#12-Dateien aufgehoben. Die Zertifikatpasswörter werden nicht gespeichert. Sofern ein Nutzer das Zertifikatpasswort aufgehoben hat, kann er sein Zertifikat wiederbekommen. Dies erleichtert den Support des Rechenzentrums erheblich.

Zu diesem Zeitpunkt schienen die Nachteile des Betriebs einer CA in der DFN-Hierarchie die Vorteile deutlich zu überwiegen. Die FH Landshut stand kurz davor, ihre Zertifizierungsstelle aus dem DFN Verband herauszulösen.

Abbildung 3: Möglichkeiten der Schlüsselerzeugung

Schlüsselerzeugung – zentral oder dezentral?

Bei der Erzeugung des Schlüsselpaares für einen Zertifikatnehmer sind zwei Verfahren verbreitet. Beide Verfahren haben sinnvolle Einsatzbereiche und Vor- und Nachteile.

1. Die dezentrale Erzeugung

Der Zertifikatnehmer erzeugt das Schlüsselpaar selbst und übergibt nur den öffentlichen Schlüssel an die CA zur Signatur.
Vorteilhaft ist sicherlich, dass nur der Zertifikatnehmer den privaten Schlüssel kennt. Er muss nicht darauf vertrauen, dass die CA seinen privaten Schlüssel zuverlässig vernichtet. Andererseits braucht der Zertifikatnehmer eine gewisse IT-Kompetenz, um die Schlüssel zu generieren, den Zertifikatantrag zu erzeugen und das von der CA erhaltene Zertifikat dem privaten Schlüssel wieder zuzuordnen.

2. Die zentrale Erzeugung

Die CA erzeugt das Schlüsselpaar für den Zertifikatnehmer, unterschreibt den öffentlichen Schlüssel und stellt das Zertifikat sowie den zugehörigen privaten Schlüssel dem Zertifikatnehmer zur Verfügung. Der private Schlüssel darf nicht bei der CA gespeichert werden.
In diesem Fall muss der Zertifikatnehmer der Kompetenz und Rechtschaffenheit der CA vertrauen. Auf der anderen Seite kann er einen Komplettservice erhalten: Die CA übergibt ihm nach der Antragstellung das Zertifikat mit privatem Schlüssel in einer geeignet geschützten Form, zum Beispiel auf einer Chipkarte oder in einer PKCS#12-Datei.

Neue Entwicklungen beim DFN ab dem Jahresende 2006 haben die Fachhochschule aber davon abgehalten. Im Dezember 2006 erfolgte die Zertifizierung des Wurzelzertifikats DFN-Verein PCA Global durch die T-Systems und damit die Verankerung in MS Windows Browsern und E-Mailsystemen. Allerdings kann eine Zertifizierungsstelle im Sicherheitsniveau "Global" der DFN-PKI nur als ausgelagerte CA, also beim DFN im Auftrag des Anwenders, betrieben werden, was wiederum die Verwendung der Webschnittstelle erforderlich macht. Die Planung der FH Landshut sah daraufhin zunächst vor, eine CA im Sicherheitsniveau "Global" nur für Serverzertifikate und Mitarbeiterzertifikate über die Webschnittstelle zu betreiben. Für die Studentenzertifikate sollte weiter eine eigene Zertifizierungsstelle eingerichtet werden.

Einsatz der SOAP-Schnittstelle

In dieser Zeit gab es immer wieder Kontakt zwischen den Mitarbeitern der FH Landshut und dem DFN-PKI Team. Die Probleme mit der Skalierbarkeit der Webschnittstelle und der mangelnden Integrationsmöglichkeit der lokalen Prozesse waren daher dem DFN bekannt und sie wurden auch als solche ernst genommen. Im April 2007 haben sich Mitarbeiter des Rechenzentrums der FH Landshut und der DFN-PKI zusammengesetzt und gemeinsam nach Lösungsmöglichkeiten gesucht. Dabei wurde vom DFN angeboten, eine SOAP-Schnittstelle zu einer beim DFN betriebenen CA bereit zu stellen, in die die an der FH Landshut bestehenden lokalen Prozesse integriert werden könnten. Zwei hochengagierte studentische Kräfte des Rechenzentrums der FH Landshut haben diesen Ball aufgegriffen und es wurde daraufhin beschlossen, bis zum September 2007 an der FH Landshut eine Registrierungsstelle mit SOAP-Zugang zu einer beim DFN betriebenen Global-CA zu implementieren. Dabei sollten Antragstellung, Schlüsselerzeugung, Zertifikatverteilung und Onlineverlängerung in Landshut ähnlich weiterbetrieben werden wie bisher (Abbildung 4).

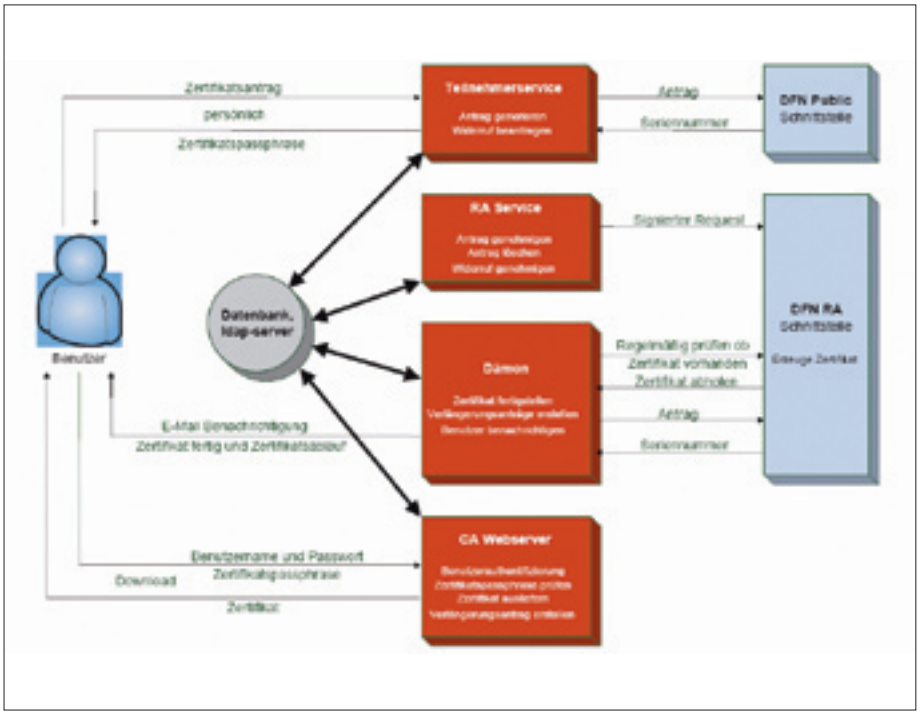


Abbildung 4: Workflow an der FH Landshut

Dies war ein sehr ehrgeiziger Plan: In Landshut wurde die Registrierungsstelle vollständig neu entwickelt. Diese wurde jetzt auf Basis von Java realisiert; sie umfasst einen Teilnehmerserviceclient, einen Registrierungsclient, einen Dämon sowie den CA-Webserver. Der Teilnehmerserviceclient ist für die Entgegennahme der Anträge und die Ausgabe der Zertifikatpasswörter zuständig. Er reicht die Anträge über SOAP an den DFN weiter, wo sie auf Korrektheit überprüft und genehmigt werden. Im Registrierungsclient werden die Anträge in Landshut zur Zertifizierung freigegeben und in einer sicheren Verbindung, wieder über SOAP, zur CA beim DFN zur Signierung geschickt. Der Dämon fragt in regelmäßigen Abständen bei der CA nach, ob fertige Zertifikate zum Download bereitstehen, holt diese ab, packt sie mit dem passenden (passwortgeschützten) privaten Schlüssel zu PKCS#12-Dateien zusammen und stellt sie zum Download für den Nutzer bereit. Vom CA-Webserver können unter anderem die Zertifikate heruntergeladen oder über diesen Verlängerungen beantragt werden.

Fazit

Die Entwicklung der SOAP-Schnittstelle für die DFN-PKI kam für die FH Landshut genau zum richtigen Zeitpunkt. Durch die frühe Zusammenarbeit zwischen der Hochschule und dem DFN-Verein konnten die aus der Praxis entstandenen Anforderungen bei den Entwicklungsarbeiten mit berücksichtigt und die SOAP-Schnittstelle entsprechend realisiert und getestet werden.

Die neue Zertifizierungsstelle im Sicherheitsniveau Global der DFN-PKI konnte pünktlich zur Neuimmatrikulation für das Wintersemester 2007 in Betrieb genommen werden. Die etablierten Workflows konnten beibehalten werden und die Registrierungsstelle kann auf Grund der SOAP-Schnittstelle weiter wie gewohnt arbeiten.

An der FH Landshut ist das „Experiment" gelungen, eine bestehende Zertifizierungsinfrastruktur in die DFN-PKI zu integrieren. Vielleicht macht das auch anderen Einrichtungen Mut, diesen Schritt zu gehen.

Speicherung von IP-Adressen auf Webseiten verboten?

Gericht lehnt auch Speicherung zur Störungsermittlung ab.

Das temporäre Einlagern von Datum und Uhrzeit, der übertragenen Datenmenge sowie der dynamischen Internetprotokolladresse (IP-Adresse) gehört bei vielen Internetauftritten zum Standard. Soweit die IP-Kennung aber einen Personenbezug erlaubt, ist die Speicherung laut einer Entscheidung des Amtsgerichts (AG) Berlin-Mitte rechtswidrig, wenn das Web-Angebot kostenlos in Anspruch genommen werden kann.[1] In derartigen Fällen ist die Speicherung auch nicht zur Ermittlung von Störungen zulässig. Das Urteil des Amtsgerichts wurde durch das Landgericht (LG) als Berufungsinstanz im Wesentlichen bestätigt.[2] Nach den Entscheidungen dürfen IP-Adressen von Contentprovidern auch nicht kurzfristig gespeichert werden. Für Provider, die lediglich den Zugang zum Web offerieren (Accessprovider), sieht die Rechtslage neuerdings hingegen anders aus.

Beklagte der Berliner Verfahren war pikanterweise die Bundesrepublik Deutschland, weil das Bundesministerium der Justiz auf seiner Homepage www.bmj.bund.de bis zum 16.12.2006 bei jedem Zugriff personenbezogene Daten des jeweiligen Nutzers gespeichert hatte, wozu insbesondere auch dynamische IP-Adressen gehörten. Die Angaben speicherte das Haus von Ministerin Brigitte Zypries 14 Tage lang. Gegen die Speicherung ihm zugeordneter IP-Kennungen wehrte sich ein Bürger mit dem Argument, das Ministerium missachte sein Recht auf informationelle Selbstbestimmung. Zu Recht, wie sowohl Amtsgericht als auch Landgericht entschieden.

IP-Adresse identifiziert Nutzer

Ausgangspunkt für die rechtliche Beurteilung war das seit dem 1. März diesen Jahres geltende Telemediengesetz (TMG). Nach dessen Paragraf 15 Absatz 1 dürfen Web-Anbieter personenbezogene Daten nur dann erheben, wenn dies für die Inanspruchnahme des jeweiligen Angebotes erforderlich ist. Nach Auffassung der Richter gehören dynamische IP-Adressen ebenfalls zu den personenbezogenen Daten, wobei es keinen Unterschied mache, ob der Zugriff und die Speicherung durch einen Accessprovider oder einen Contentprovider in Gestalt von Internetportalen erfolge. Maßgeblich für die Klassifizierung einer Angabe als personenbezogenes Datum sei die Bestimmbarkeit einer Person. Laut Begründung des AG sei „es durch die Zusammenführung der personenbezogenen Daten mit Hilfe Dritter bereits jetzt ohne großen Aufwand in den meisten Fällen möglich, Internetbenutzer aufgrund ihrer IP-Adresse zu identifizieren". Dies stelle einen Eingriff in das nach dem Grundgesetz geschützte Recht auf informationelle Selbstbestimmung dar, wonach jedermann grundsätzlich die Befugnis besitzt, selbst entscheiden zu dürfen, wer wann um welches ihn betreffende Datum Kenntnis wissen darf. Das genannte Grundrecht wird dem Bürger jedoch nicht schrankenlos gewährt, sondern tritt dann zurück, wenn der Betroffene in die Erhebung seiner personenbezogenen Daten eingewilligt hat oder ein Gesetz es erlaubt. Gestattet ist die Erhebung von personenbezogenen Daten und somit auch von dynamischen IP-Kennungen nach dem Telemediengesetz, wenn die Daten zu Abrechnungszwecken benötigt werden. Dies stellt Paragraf 15 Absatz 4 TMG eindeutig klar.[3] Keine Einwände gegen die Erhebung und Aufbewahrung bestehen ferner dann, wenn der begründete Verdacht besteht, dass ein kostenpflichtiges Angebot illegal genutzt wird (Paragraf 15 Absatz 8 TMG). Diese als Erlaubnisnormen bezeichneten Zulässigkeitsgründe lagen im Falle des Bundesministeriums der Justiz indes nicht vor, da der Abruf sämtlicher Inhalte von der Homepage kostenlos war und eine Einwilligung des

„Datensicherheit" kein zulässiges Argument

Als weiteres Argument für die Speicherung insbesondere der IP-Kennungen führte das Bundesministerium der Justiz die Datensicherheit an, die in Paragraf 9 Bundesdatenschutzgesetz (BDSG) verankert ist.[4] Danach ist eine datenverarbeitende Stelle zum Ergreifen von Maßnahmen verpflichtet, um einen unzulässigen „Umgang mit personenbezogenen Daten zu verhindern und die Integrität sowie Verfügbarkeit der Daten und die zu deren Verarbeitung eingesetzten technischen Einrichtungen zu erhalten".[5] Dem schenkten die Berliner Gerichte jedoch keine Beachtung und erklärten das BDSG für nicht anwendbar, da die Speicherung von personenbezogenen Daten abschließend im Telemediengesetz geregelt sei und sich dort eben keine Norm finde, wonach die Speicherung personenbezogener Daten in Form von dynamischen IP-Adressen im konkreten Fall erlaubt sei.

Berlin ist nicht Darmstadt

Die beiden Berliner Entscheidungen sind klar zu trennen vom Urteil des Landgerichts Darmstadt, das Ende 2005 für viel Aufmerksamkeit gesorgt hat. Der dortige Sachverhalt betraf nicht das Telemediengesetz, sondern das Telekommunikationsgesetz (TKG). Dem Darmstädter Fall lag die Klage eines Bürgers gegen den Zugangsprovider T-Online zugrunde, der trotz bestehender Flatrate die dem Kunden zugewiesenen dynamischen IP-Adressen protokolliert und über einen Zeitraum von 80 Tagen gespeichert hatte. Auch das hessische Gericht stufte dynamische IP-Kennungen als personenbezogene Daten ein.[6] Anders als in den Hauptstadtfällen zog das LG Darmstadt aber das TKG als Rechtsrahmen heran, da es sich bei der Dienstleistung von T-Online um die Bereitstellung des Internetanschlusses und nicht um das Vorhalten eigener Inhalte auf einer Homepage gehandelt habe und T-Online somit als reiner Zugangsprovider nach den Buchstaben des TKG einzuordnen sei. Da der Vertragsgegenstand einer Flatrate einen volumenunabhängigen Dienst zu einem Festpreis darstelle, sei die Erhebung und Speicherung von dynamischen IP-Adressen nicht für Abrechnungszwecke erforderlich. Folge: Laut Paragraf 96 Absatz 2 TKG seien die IP-Adressen sofort nach jeder Session zu löschen. Das Speichern und Vorhalten von dynamischen IP-Adressen ist Zugangsprovidern aber nach Paragraf 100 TKG in zwei Fällen gestattet: Zum Ersten, soweit die Speicherung „zum Erkennen, Eingrenzen und Beseitigen von Störungen und Fehlern an Telekommunikationsanlagen" erforderlich ist und zum Zweiten, um die Erschleichung von Leistungen oder sonstigen Missbrauch aufdecken und unterbinden zu können. Laut Richterspruch des LG Darmstadt rechtfertige dies aber keine pauschale Speicherung von IP-Kennungen. Es müsse vielmehr konkret der Verdacht von Störungen oder Missbrauch vorliegen, was im Falle von T-Online nicht gegeben gewesen sei.[7]

Kehrtwende – Aufbewahrungsrecht für Zugangsprovider

Im Hinblick auf die sofortige Löschungspflicht von dynamischen IP-Adressen für Zugangsprovider vertritt der Bundesdatenschutzbeauftragte, Peter Schaar, jedoch eine andere Auffassung. Er hält es für zulässig, dass die IP-Kennungen sieben Tage lang gespeichert werden dürfen.[8] Für seinen Standpunkt zieht der oberste Datenschützer des Bundes den „Störungs- und Missbrauchsverhinderungs-Paragraf" 100 TKG heran. In einem offenen Brief begründet Schaar das siebentätige Speicherungsrecht mit dem Schutz der Netzinfrastruktur einerseits und dem Schutz der Nutzer „vor Schadsoftware und betrügerischer Inanspruchnahme ihrer Zugangsberechtigung" andererseits.[9] So sei beispielsweise eine Identifizierung von gekaperten Computern, die „ohne Wissen des rechtmäßigen Nutzers unter dessen Berechtigungskennung Spams und/oder Viren an andere Nutzer versenden oder die DOS-Attacke durchführen, nur mittels gespeicherter dynamischer IP-Adressen möglich".[10] Das Landgericht Darmstadt hat jüngst seine einstige Rechtsprechung zur sofortigen Löschungspflicht aufgegeben. Im Einklang mit der Meinung des Bundesdatenschutz-

beauftragten gewährt nunmehr auch das hessische Landgericht Zugangsprovidern eine Speicherungsdauer von sieben Tagen.[11] Ebenso sieht es das Amtsgericht Bonn.[12] Beide Gerichte lassen auch dann eine Speicherung dynamischer IP-Adressen für sieben Tage zu, wenn es an konkreten Anhaltspunkten für eine Störung oder einen Missbrauch mangelt. Auch die juristische Literatur teilt den Ansatz, dass eine Erlaubnis zu einer vorsorglichen Störungs- und Fehlerbekämpfung besteht,[13] die aber nur gelingen kann, wenn die dafür relevanten personenbezogenen Daten erhoben und für ein eng abgestecktes Zeitfenster gespeichert werden dürfen.

Anmerkung

In nicht wenigen Pressepublikationen werden die Entscheidungen der Berliner Gerichte zum Speicherungsverbot von dynamischen IP-Adressen durch Contentprovider als Grundsatzurteile betitelt. Dies ist aber nicht der Fall. Es ist festzuhalten, dass sich das Landgericht Berlin mit der grundsätzlichen Problematik der Speicherung von IP-Adressen durch Homepage-Betreiber nur am Rande befasst hat, da es sich vielmehr mit prozessualen Feinheiten beschäftigen musste. In der Argumentation selbst liegt folglich für die Contentprovider nur ein amtsgerichtliches Urteil vor. Bei der Speicherung von dynamischen IP-Kennungen durch Homepage-Betreiber ist – anders als bei Zugangsprovidern - bereits stark anzuzweifeln, ob es sich bei diesen überhaupt um ein personenbezogenes Datum handelt. Laut Paragraf 3 Bundesdatenschutzgesetz (BDSG) liegt zwar auch dann ein personenbezogenes Datum vor, wenn mittels einer Einzelangabe eine natürliche Person bestimmbar ist. Verlangt ist aber, dass die Stelle, die im Besitz der Daten ist, mit „den ihr normalerweise zur Verfügung stehenden Mitteln und ohne unverhältnismäßigen Aufwand" in der Lage ist, die betreffende Person zu ermitteln.[14] Davon wird man bei einem Contentprovider nur schwerlich sprechen können. Er verfügt gerade nicht über Name und Anschrift der Person, der eine dynamische IP-Adresse zuordnet ist. Will der Contentprovider die Identität ermitteln, bleibt ihm nichts anderes übrig als die Staatsanwaltschaft einzuschalten, die dann ihrerseits an den Zugangsprovider herantreten muss.[15]

Literatur

1 Urteil des Amtsgerichts Berlin-Mitte vom 27.3.2007, Az. 5 C 314/06, http://www.daten-speicherung.de/?p=197#ag.

2 Urteil des Landgerichts Berlin vom 6.9.2007, Az. 23 S 3/07, http://www.daten-speicherung.de/?p=197#lg.

3 Paragraf 15 TMG im Volltext unter http://www.gesetze-im-internet.de/tmg/__15.html.

4 Paragraf 9 BDSG im Volltext unter http://www.gesetze-im-internet.de/bdsg_1990/__9.html.

5 Ernestus in: Simitis, Bundesdatenschutzgesetz – Kommentar, 6. Aufl., 2006, § 9, Rdnr. 2.

6 Urteil des LG Darmstadt vom 7.12.2005, Az. 25 S 118/05, Datenschutz und Datensicherheit (DuD) 2006, S. 178 ff.

7 Urteil des LG Darmstadt vom 7.12.2005, Az. 25 S 118/05, Datenschutz und Datensicherheit (DuD) 2006, S. 178 ff.

8 Bundesdatenschutzbeauftragter hält Speicherung der IP-Adresse für sieben Tage für zulässig, www.heise.de/newsticker/meldung/86914.

9 Offener Brief des Bundesdatenschutz beauftragten zur Rechtfertigung des siebentägigen Speicherungsrechts, http://www.bfdi.bund.de/cln_029/nn_530308/DE/Themen/KommunikationsdiensteMedien/Telekommunikation/Artikel/VorratsdatenspeicherungLG-Darmstadt.html.

10 http://www.bfdi.bund.de/cln_029/nn_530308/DE/Themen/KommunikationsdiensteMedien/Telekommunikation/Artikel/VorratsdatenspeicherungLG-Darmstadt.html.

11 Urteil des Landgerichts Darmstadt vom 6.6.2007, Az. 10 O 562/03, Computer und Recht (CR) 2007, Heft 9, S. 574 ff.

12 Urteil des Amtsgerichts Bonn vom 5.7.2007, Az. 9 C 177/07, CR 2007, Heft 10, S. 640.

13 Klesczewski in: Säcker, Berliner Kommentar zum Telekommunikationsgesetz, 2005, § 100, Rndr. 8.

14 Gola/Klug in: Gola/Klug, BDSG – Kommentar, 2005, 8. Aufl., § 3, Rndr. 9.

15 So auch Köcher voraussichtlich dem nächst in: MMR 2007, Heft 12.

Noogie C. Kaufmann

Rechtsanwalt, Master of Arts
Forschungsstelle Recht im DFN

E-Mail: recht@dfn.de

GEZ und die Gebühren

Auf der Suche nach einem neuen Image über das Ziel hinaus geschossen?

Die Gebühreneinzugszentrale (GEZ) ist im Kampf gegen ihr schlechtes Image[1] wohl über das Ziel hinaus geschossen und hat eher Schaden angerichtet, als in der breiten Öffentlichkeit zu punkten – und das ausgerechnet pünktlich zum Beginn einer neuen, groß angelegten GEZ-Imagekampagne.[2]

Auslöser der Diskussion in den Medien war der folgende Fall: Die GEZ hatte dem deutschen Bildungsportal akademie.de eine 29-seitige Abmahnung zukommen lassen. Bei der Berliner Website handelt es sich um ein Informationsportal, welches praxisnahe Informationen, die vor allem an Kleinunternehmer gerichtet sind, aus unterschiedlichsten Gebieten anbietet. Unter anderem befindet sich auf dem Portal ein ca. 80 Seiten umfassender Ratgeber zu dem Thema GEZ-Gebühren. Hierdurch hatte sich die GEZ offensichtlich in ihren Rechten verletzt gefühlt. Neben der Beanstandung bestimmter, auf der Seite getätigter Tatsachenbehauptungen, sah die Abmahnung in zwei der insgesamt 32 Punkte eine „Korrektur" der verwendeten Begriffe vor: die GEZ wollte damit die Verwendung offizieller, korrekter Bezeichnungen rund um das Thema GEZ mittels des juristischen Druckmittels der Abmahnung erzwingen.

Im Einzelnen sollten nach Wunsch der GEZ die Begriffe „Gebührenjäger" und „Fangprämie" von dem Benutzungsverbot umfasst sein und durch die offiziellen Begriffe „Beauftragtendienst der öffentlich-rechtlichen Rundfunkanstalten" oder „Rundfunkgebührenbeauftragter" sowie „Provision des Beauftragtendienstes der öffentlich-rechtlichen Rundfunkanstalten oder Rundfunkgebührenbeauftragten" ersetzt werden. Bizarr wird die Beanstandung spätestens dort, wo sich auch die Begriffe „GEZ-Gebühren", „PC-Gebühr" und „GEZ-Brief" auf der Liste falscher und damit verbotener Bezeichnungen wiederfinden. Für letztere sieht die GEZ beispielsweise die impraktikable Bezeichnung „Informationsschreiben der GEZ" und/oder „Schreiben, mit dessen Hilfe der gesetzliche Auskunftsanspruch des § 4 Abs. 5 Rundfunkgebührenstaatsvertrag (RGebStV) geltend gemacht wird" vor.

Angesichts eines solchen Amtsdeutschs stellt sich die Frage, was die GEZ hiermit erreichen wollte.

Aus juristischer Sicht sollte sich akademie.de im Rahmen einer sogenannten strafbewehrten Unterlassungserklärung verpflichten, in Zukunft die auf dem Index stehenden Bezeichnungen nicht mehr zu verwenden. Die Unterzeichnung der Erklärung hätte dazu geführt, dass sich akademie.de bei einer Zuwiderhandlung in Form jedweder weiteren öffentlichen Verwendung eines Verbotswortes verpflichtet, 5100 Euro pro Bezeichnung an die GEZ zu zahlen.

Die GEZ verteidigte dieses Vorgehen damit, dass solche „nicht existenten Begriffe"[3] letztlich nur dazu dienen, ein negatives Image der GEZ hervorzurufen. Kann man jedoch von nicht existenten Begriffen sprechen, wenn beispielsweise allein die

Eingabe des Begriffs „GEZ-Gebühren“ bei der Suchmaschine Google zu ca. 219.000 Treffern führt und insbesondere auch auf der Webseite ZDF.de 36 mal zu finden ist.

Dies scheint nun auch den Verantwortlichen selbst einzuleuchten. Jedenfalls hat der Südwestrundfunk (SWR) stellvertretend für die übrigen öffentlich-rechtlichen Rundfunkanstalten nun eine modifizierte Unterlassungserklärung von akademia.de akzeptiert, in der die Verantwortlichen der Website zwar erklären, bestimmte falsche Tatsachenbehauptungen zukünftig zu unterlassen, jedoch keine Unterlassungserklärung bezüglich der Nutzung der oben genannten Begriffe abgeben.

Dennoch gibt es noch offen gebliebene Streitpunkte. Hierzu zählt insbesondere die Interpretation des § 5 Abs. 3 RGebStV. Dieser sieht eine Gebührenbefreiung für im „nicht ausschließlich privaten Bereich genutzte neuartige Rundfunkempfänger“ vor, soweit „die Geräte ein- und demselben Grundstück oder zusammenhängenden Grundstücken zuzuordnen sind und andere Rundfunkempfangsgeräte dort zum Empfang bereitgehalten werden“.[4] Akademie.de folgerte hieraus, dass aufgrund der Tatsache, dass nicht auf dieselbe Person, sondern dasselbe Grundstück abgestellt wird, nur „in seltenen Fällen“ tatsächlich eine Zahlungspflicht bestehe - in der Regel reiche für ein Eintreten des Befreiungstatbestandes aus, dass der Hausmeister auf dem Grundstück ein Radio angemeldet habe.

Das Bildungsportal will sogar eine negative Feststellungsklage gegen den SWR erheben, durch die klargestellt werden soll, dass die GEZ eben gerade keinen Anspruch auf Unterlassung der Veröffentlichung dieser Rechtsmeinung habe.[5] Bleibt abzuwarten, wie die GEZ hierauf reagiert.

Aus juristischer Sicht kann grundsätzlich festgehalten werden, dass ein Anspruch der GEZ auf Unterlassung dieser Aussage ohnehin nur besteht, wenn es sich um eine falsche Tatsachenbehauptung handelt, und nicht um eine von Art. 5 Abs. 1 GG geschützte Meinungsäußerung.[6] Bei der hier konkret getroffenen Äußerung mag es sein, dass es sich um eine umstrittene und für die GEZ auch nicht wünschenswerte Rechtsauffassung handelt. Jedoch stellt die Vorschrift laut Gesetzesbegründung eindeutig auf den räumlichen Zusammenhang ab und nicht auf die wirtschaftliche Verbindung.[7] Somit fällt es schwer, die Aussage als falsche Tatsachenbehauptung zu deklarieren. Darüber hinaus darf nicht außer Acht gelassen werden, dass es lediglich um eine auf die neuen Rundfunkempfangsgeräte (internetfähiger PC) bezogene Befreiung geht. Dies bedeutet, dass ein Unternehmen, welches neben herkömmlichen auch neuartige Rundfunkgeräte auf ein- und demselben Grundstück bereithält, trotzdem für jedes einzelne Rundfunkempfangsgerät an die GEZ zahlt – die Zahlungspflicht entfällt lediglich für die neuartigen Rundfunkempfangsgeräte, § 5 Abs. 3, 1. Unterabsatz RGebStV.

Für die Hochschulen lässt sich daraus schließen, dass nach derzeitiger Rechtslage die gesetzliche Gebühr für neuartige Rundfunkgeräte gem. § 5 Abs. 3 RGebStV nur dann zu entrichten ist, wenn nicht auf demselben (räumlich zusammenhängenden) Grundstück bereits ein herkömmliches Gerät (Fernseher oder Radio) angemeldet ist. Und auch dann fällt für die Gesamtheit aller sich dort befindenden neuartigen Empfangsgeräte pro Grundstück nur eine Gebühr i.H.v. EUR 5,52 an. Zu beachten ist für die Hochschulen allerdings, dass räumlich getrennte – d.h. auf unterschiedlichen Grundstücken befindliche – Institute auch einzeln zahlungspflichtig sind.

Festzuhalten bleibt im Ergebnis jedenfalls, dass die GEZ mit dem Verlangen nach einer strafbewehrten Unterlassungserklärung für viel Wirbel gesorgt hat, der ihr schlechtes Image allenfalls bestätigt und nicht verbessert. Zwar übten die verantwortlichen Sender öffentlich keine Kritik am Vorgehen der GEZ; zu erwarten ist aber, dass intern nach der Verantwortlichkeit für diese ganz eigene Image-Kampagne der GEZ gefragt werden wird. Im Übrigen ist bis dahin Vorsicht geboten bei der Verwendung von Begriffen rund um das Thema GEZ.

Eva Schröder

Wissenschaftliche Mitarbeiterin
Forschungsstelle Recht im DFN
recht@dfn.de

Literatur

1 http://www.heise.de/newsticker/meldung/82511

2 http://www.natuerlich-zahl-ich.de

3 Spiegel-Online, abrufbar unter www.spiegel-online.de/netzwelt/web/0,1518,501730,00.html; siehe Abmahnschreiben unter: http://www.akademie.de/private-finanzen/sparen-altersvorsorgevermoegens-bildung/tipps/sparen-vermoegen-altersvorsorge/gez-abmahnung/index.html

4 Schreier, MMR 2005, S. 572; Kitz, NJW 2006, 408

5 www.heise.de/newsticker/meldung/96025

6 Vgl. Köcher, Harter Tobak in Meinungsforen, DFN-Infobrief, Juni 2006, S. 9ff

7 Schreier, MMR 2005, S. 572

Übersicht über die Mitgliedseinrichtungen und Organe des DFN-Vereins

(Stand 12/2007)

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 Prof. Dr. Gerhard Peter, FH Heilbronn.

Verwaltungsrat
Der Verwaltungsrat beschließt über alle wesentlichen Aktivitäten des Vereins, insbesondere über die technisch-wissenschaftlichen Arbeiten, und berät den Jahreswirtschaftsplan. Für die 8. Wahlperiode bis Ende 2008 sind Mitglieder des Verwaltungsrates:

- Prof. Dr. Claudia Eckert, Fraunhofer-Institut für Sichere Telekooperation, Darmstadt
- Vis. Prof. Geerd-Rüdiger Hoffmann, Deutscher Wetterdienst
- Prof. Dr. Wilfried Juling, Universität Karlsruhe
- Dr. Klaus-Peter Kossakowski, PRESECURE Consulting GmbH, Telgte
- Prof. Dr. Reinhard Maschuw, Forschungszentrum Karlsruhe
- Prof. Dr. Wolfgang E. Nagel, TU Dresden
- Prof. Dr. Bernhard Neumair, GWDG Göttingen
- Dr. Frank Nolden, Universität Leipzig (Kanzler)
- Dr.-Ing. Christa Radloff, Universität Rostock
- Prof. Dr. Gerhard Schneider, Universität Freiburg
- Manfred Seedig, Universität Kassel
- Günter Springer, TU Ilmenau
- Prof. Dipl.-Ing. Herbert Wiese, FH Esslingen

Vorstand
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. Wilfried Juling, Vorsitz, sowie Prof. Dr. Bernhard Neumair und Dr. Frank Nolden.

Der Vorstand wird beraten von einem Technologie-Ausschuss (TA), einem Betriebsausschuss (BA), und einem Ausschuss für Recht und Sicherheit (ARuS), der zugleich auch als Jugendschutzbeauftragter für das DFN fungiert.

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 und Jochem Pattloch bestellt.

Der DFN-Verein hat derzeit folgende Mitglieder:

Aachen	Fachhochschule Aachen
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Albstadt	Hochschule 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 Synchrotronstrahlung mbH (BESSY)
	BBB Management GmbH
	Bundesanstalt für Materialforschung und -prüfung (BAM)
	Bundesinstitut für Risikobewertung
	Bundesministerium für Verkehr, Bau- und Stadtentwicklung
	CDU Bundesgeschäftsstelle
	Deutsche Telekom AG
	Deutsches Herzzentrum
	Deutsches Historisches Museum (DHM) GmbH
	Deutsches Institut für Normung e.V. (DIN)
	Deutsches Institut für Wirtschaftsforschung (DIW)
	Alice-Salomon-Fachhochschule für Sozialarbeit und Sozialpädagogik Berlin
	Fachhochschule für Technik und Wirtschaft
	Fachhochschule für Wirtschaft
	Fachinformationszentrum Chemie GmbH (FIZ Chemie)
	Institut für Nachrichtentechnik
	Forschungsverbund Berlin e.V.
	Freie Universität Berlin (FUB)
	Hahn-Meitner-Institut Berlin GmbH (HMI)
	Humboldt-Universität Berlin (HUB)
	IT-Dienstleistungszentrum
	Konrad-Zuse-Zentrum für Informationstechnik Berlin (ZIB)
	Landesbetrieb für Informationstechnik (LIT)
	Robert-Koch-Institut
	Stiftung Preußischer Kulturbesitz
	Stanford-Universität in Berlin
	Technische Fachhochschule Berlin (TFH)
	Technische Universität Berlin (TUB)
	Umweltbundesamt
	Universität der Künste
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum für Sozialforschung gGmbH (WZB)
	T-Systems Enterprise Services GmbH
Biberach	Fachhochschule Biberach, HS für Bauwesen und Wirtschaft
Bielefeld	Fachhochschule Bielefeld
	Universität Bielefeld
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische FH Rheinland-Westfalen-Lippe
	Fachhochschule Bochum, Technische FH Georg Agricola für Rohstoffe, Energie und Umwelt
	Ruhr-Universität Bochum
Böblingen	Staatliche Akademie für Datenverarbeitung
Bonn	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
	Deutsche Forschungsgemeinschaft
	Deutscher Akademischer Austauschdienst e.V. (DAAD)
	Deutsches Zentrum für Luft und Raumfahrt
	Universität Bonn
Bonn	IZ Sozialwissenschaften
	Zentrum für Informationsverarbeitung und Informationstechnik
	Bundesministerium des Innern
Borstel	FZB, Leibniz-Zentrum für Medizin und Biowissenschaften
Brandenburg	Fachhochschule Brandenburg
Braunschweig	Biologische Bundesanstalt für Land- und Forstwirtschaft
	Bundesforschungsanstalt für Landwirtschaft (FAL)
	Helmholtz-Zentrum für Infektionsforschung
	Hochschule für Bildende Künste
	Physikalisch-Technische Bundesanstalt (PTB)
	Technische Universität Braunschweig
Bremen	Hochschule Bremen
	Jacobs University Bremen gGmbH
	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)
	Hochschule Darmstadt
	Gesellschaft für Schwerionenforschung mbH (GSI)
	Merck KGaA
	Technische Universität Darmstadt
	T-Systems Enterprise Services GmbH
Deggendorf	Fachhochschule Deggendorf
Detmold	Lippische Landesbibliothek
Diepholz	Private Fachhochschule für Wirtschaft und Technik
Dortmund	Fachhochschule Dortmund
	Technische Universität Dortmund
Dreieich	PanDacom Networking AG
Dresden	Forschungszentrum Dresden Rossendorf e.V.
	Hannah-Arendt-Institut für Totalitarismusforschung e.V.
	Hochschule für Bildende Künste
	Hochschule für Technik und Wirtschaft (FH)
	Leibniz-Institut für Festkörper- und Werkstofforschung e.V.
	Leibniz-Institut für Polymerforschung Dresden e.V.
	Sächsische Landesbibliothek
	Technische Universität Dresden
Düsseldorf	Fachhochschule Düsseldorf
	Landesamt für Datenverarbeitung und Statistik des Landes NRW
	Heinrich-Heine-Universität Düsseldorf
Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Joh. A. Lasco Bibliothek - Große Kirche Emden
Erfurt	Fachhochschule Erfurt
	Universität Erfurt
Erlangen	Universität Erlangen-Nürnberg
Essen	Rheinisch-Westfälisches Institut für Wirtschaftsforschung
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen, Hochschule für Technik
Flensburg	Fachhochschule Flensburg
Frankfurt/M.	Bundesamt für Kartographie und Geodäsie
	Die Deutsche Nationalbibliothek Frankfurt

Frankfurt/M.	Deutsches Institut für Internationale Pädagogische
.	Forschung
	Fachhochschule Frankfurt am Main
	Fachinformationszentrum Technik e. V. (FIZ Technik)
	Juniper Networks GmbH
	KPN EuroRings B.V.
	Phil.-Theol. Hochschule St. Georgen e. V.
	Universität Frankfurt am Main
Frankfurt/O.	Europa-Universität Viadrina Frankfurt/Oder
	IHP GmbH, Institut für innovative Mikroelektronik
Freiberg	TU/Bergakademie Freiberg
Freiburg	Universität Freiburg
Fulda	Hochschule Fulda
Furtwangen	Hochschule Furtwangen
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften
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 gGmbH
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes
Greifswald	Universität Greifswald
Hagen	FernUniversität in Hagen
	Fachhochschule Südwestfalen, Fachhochschule für Technik und Wirtschaft
Halle/Saale	Martin-Luther-Universität Halle-Wittenberg
	Institut für Wirtschaftsforschung Halle
Hamburg	Bundesamt für Seeschiffahrt und Hydrographie (BSH)
	Deutsches Elektronen Synchrotron (DESY)
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	Hochschule für angewandte Wissenschaften Hamburg
	Heinrich-Pette-Institut für Experimentelle Virologie und Immunologie
	Hewlett Packard GmbH
	Hochschule für Bildende Künste
	Hochschule für Musik und Theater Hamburg
	Technische Universität Hamburg-Harburg
	Helmut-Schmidt-Universität, Universität der Bundeswehr
	Universität Hamburg
Hannover	Bundesanstalt für Geowissenschaften und Rohstoffe (BGR)
	Evangelische Fachhochschule Hannover
	Hochschule für Musik und Theater Hannover
	Hochschul-Informations-System-GmbH
	Medizinische Hochschule Hannover
	Landesamt für Bergbau, Energie und Geologie
	Gottfried Wilhelm Leibniz Bibliothek - Niedersächsische Landesbibliothek
	Tierärztliche Hochschule Hannover
	Universität Hannover
	Technische Universitätsbibliothek Hannover und Technische Informationsbibliothek (TIB)
Heide	FH Westküste
Heidelberg	Network Laboratories, NEC Europe Ltd.
	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	Universität Heidelberg
Heilbronn	Hochschule Heilbronn
Heyrothsberge	(Institut der Feuerwehr Sachsen-Anhalt)
Hildesheim	Fachhochschule Hildesheim/Holzminden/Göttingen
	Hochschule für angewandte Wissenschaft und Kunst
	Universität Hildesheim
Hof	Fachhochschule Hof
Ilmenau	Technische Universität Ilmenau
Ingolstadt	Fachhochschule Ingolstadt
	DIZ - Zentrum für Hochschuldidaktik der bayerischen Fachhochschulen
Jena	Fachhochschule Jena
	Friedrich-Schiller-Universität Jena
	Leibniz-Institut für Altersforschung e.V. (FLI)
	Institut für Photonische Technolgien e.V.
Jülich	Forschungszentrum Jülich GmbH
Kaiserlautern	Fachhochschule Kaiserslautern
	Technische Universität Kaiserslautern
Karlsruhe	Bundesanstalt für Wasserbau
	Hochschule Karlsruhe
	Fachinformationszentrum (FIZ Karlsruhe)
	Forschungszentrum Informatik
	Forschungszentrum Karlsruhe GmbH
	Technische Universität Karlsruhe
	Universität Karlsruhe
	Zentrum für Kunst und Medientechnologie
Kassel	Universität Kassel
Kempten	Fachhochschule Kempten
Kiel	Fachhochschule Kiel
	Leibniz-Institut für Meereswissenschaften
	Universität Kiel
Koblenz	Fachhochschule Koblenz
	Universität Koblenz-Landau
	Landesbibliothekszentrum Rheinland-Pfalz
Köln	Deutsche Sporthochschule Köln
	Fachhochschule Köln
	Hochschulbibliothekszentrum des Landes NRW
	Kunsthochschule für Medien Köln
	Rheinische Fachhochschule Köln e.V.
	Universität zu Köln
Köthen	Hochschule Anhalt (FH)
Konstanz	Universität Konstanz
Krefeld	Hochschule Niederrhein
Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e.V.
Landshut	Fachhochschule Landshut
Leipzig	Deutsche Telekom, Hochschule für Telekommunikation Leipzig (FH)
	Hochschule für Grafik und Buchkunst
	Hochschule für Technik, Wirtschaft und Kultur Leipzig (FH)
	Hochschule für Musik und Theater
	Institut für Troposphärenforschung e.V.
	Mitteldeutscher Rundfunk
	Helmholtz-Zentrum für Umweltforschung
	Universität Leipzig
Lemgo	Fachhochschule Lippe und Höxter
Ludwigshafen	Fachhochschule Ludwigshafen, HS für Wirtschaft
Lübeck	Fachhochschule Lübeck
	Universität zu Lübeck
Lüneburg	Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal (FH)
	Institut für Neurobiologie
	Otto-von-Guericke-Universität Magdeburg
Mainz	Fachhochschule Mainz
	Universität Koblenz-Landau
	Universität Mainz
Mannheim	Hochschule Mannheim
	TÜV Süd Energie- und Systemtechnik GmbH
	Universität Mannheim

Mannheim	Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW)
Marbach a. N.	Deutsches Literaturarchiv
Marburg	Universität Marburg
Merseburg	Hochschule Merseburg (FH)
Mittweida	Hochschule Mittweida
Mosbach	Berufsakademie Mosbach, Staatl. Studienakademie
München	Bayerische Staatsbibliothek Bibliotheksverbund Bayern
	DECUS München e.V.
	Fachhochschule München
	Fraunhofer-Gesellschaft (FhG) e. V.
	GSF-Forschungszentrum für Umwelt und Gesundheit GmbH
	IFO-Institut für Wirtschaftsforschung e.V.
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft e.V., (MPG)
	SIEMENS AG
	Technische Universität München
	Universität der Bundeswehr München
Müncheberg	Leibniz-Zentrum für Agrarlandschafts- und Landnutzungsforschung (ZALF) e.V.
Münster	Fachhochschule Münster
	Universität Münster
Neu Ulm	Fachhochschule Neu Ulm
Neubrandenburg	Hochschule Neubrandenburg
Nordhausen	Fachhochschule Nordhausen
Nürnberg	Fachhochschule Nürnberg
	Kommunikationsnetz Franken e.V.
Nürtingen	Hochschule für Wirtschaft und Umwelt
Oberursel	Dimension Data Germany AG & Co. KG
Oberwolfach	Mathematisches Forschungsinstitut gGmbH
Offenbach/Main	Deutscher Wetterdienst Offenbach
Offenburg	Hochschule Offenburg (FH)
Oldenburg	Landesbibliothek Oldenburg
	Universität Oldenburg
Osnabrück	Fachhochschule Osnabrück
	Universität Osnabrück
Paderborn	HNF Heinz Nixdorf MuseumsForum GmbH
	Universität Paderborn
Passau	Universität Passau
Peine	Deutsche Gesellschaft zum Bau und Betrieb von Endlagern für Abfallstoffe mbH
Potsdam	Deutsches Institut für Ernährungsforschung Nuthetal
	Fachhochschule Potsdam
	GeoForschungsZentrum Potsdam
	Hochschule für Film und Fernsehen „Konrad Wolf“
	Potsdam Institut für Klimafolgenforschung e.V. (PIK)
	Universität Potsdam
Regensburg	Fachhochschule Regensburg
	Universität Regensburg
Rosenheim	Fachhochschule Rosenheim
Rostock	Institut für Ostseeforschung
	Universität Rostock
Saarbrücken	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Fachhochschule Bonn Rhein-Sieg
Schmalkalden	Fachhochschule Schmalkalden
Schwäbisch-Gmünd	Pädagogische Hochschule
Schwerin	Landesbibliothek Mecklenburg-Vorpommern
Senftenberg	Fachhochschule Lausitz
Siegen	Universität Siegen
Speyer	Deutsche Hochschule für Verwaltungswissenschaften
	Landesbibliothekszentrum Rheinland-Pfalz
Stralsund	Fachhochschule Stralsund
Straelen	GasLINE
Stuttgart	Cisco Systems GmbH
Stuttgart	DaimlerChrysler AG
	Hochschule der Medien
	Hochschule für Technik
	NextiraOne Deutschland GmbH
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte
Trier	Fachhochschule Trier
	Universität Trier
Tübingen	Friedrich-Loeffler-Institut Bundesforschungsinstitut für Tiergesundheit
	Universität Tübingen
Ulm	Fachhochschule Ulm, Hochschule für Technik
	Universität Ulm
Vechta	Hochschule Vechta
Wachtberg	Forschungsgesellschaft für angewandte Naturwissenschaften e.V.
Weidenbach	Fachhochschule Weihenstephan
Weimar	Bauhaus-Universität Weimar
Weingarten	Hochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten
Wernigerode	Hochschule Harz (FH)
Wiesbaden	Fachhochschule Wiesbaden
	Statistisches Bundesamt
Wessling	T-Systems Solutions for Research GmbH
Wildau	Technische Fachhochschule Wildau
Wilhelmshaven	Fachhochschule Oldenburg/Ostfriesland/Wilhelmshaven
Wismar	Hochschule Wismar
Witten	Universität Witten/Herdecke GmbH
Wolfenbüttel	Herzog-August-Bibliothek
	Fachhochschule Braunschweig/Wolfenbüttel
Worms	Fachhochschule Worms
Würzburg	Fachhochschule Würzburg-Schweinfurt
	Universität Würzburg
Wuppertal	Bergische Universität Wuppertal
Zittau	Hochschule Zittau/Görlitz (FH)
	Internationales Hochschulinstitut
Zwickau	Westsächsische Hochschule Zwickau (FH)

Termine

15.01.2008
Einweihung Cross-Border-Fibre RENATER/DFN
Strasbourg, Universität

13.02. - 14.02.2008
15. DFN Workshop „Sicherheit in vernetzten Systemen"
Congress Centrum Hamburg

26.02. - 27.02.2008
48. DFN-Betriebstagung
Berlin

28.05. - 29.05.2008
1. DFN-Forum Kommunikationstechnologien
Kaiserslautern, Universität

21.10. - 22.10.2008
49. DFN-Betriebstagung
Berlin