GWDG Nachrichten

für die Benutzerinnen und Benutzer des Rechenzentrums

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Ausgabe 10/2011

Inhalt

IMPRESSUM

GWDG-Nachrichten für die Benutzerinnen und Benutzer des Rechenzentrums
ISSN 0940-4686
34. Jahrgang, Ausgabe 10/2011 **Erscheinungsweise: monatlich**
www.gwdg.de/gwdg-nr **Auflage: 500**

Titelfoto: Ausschnitts des Plakats zum Tag der offenen Tür am 5. November 2011

Herausgeber:	**Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen**		
	Am Faßberg 11		
	37077 Göttingen	**Tel.: 0551 201-1510**	**Fax: 0551 201-2150**
Redaktion:	**Dr. Thomas Otto**	**Tel.: 0551 201-1828**	**E-Mail: Thomas.Otto@gwdg.de**
Herstellung:	**Maria Geraci**	**Tel.: 0551 201-1804**	**E-Mail: Maria.Geraci@gwdg.de**
Druck:	**GWDG / AG H**	**Tel.: 0551 201-1523**	**E-Mail: printservice@gwdg.de**

Wechsel in der Geschäftsführung

Bei der GWDG hat es einen Wechsel in der Geschäftsführung gegeben. Seit dem 1. Oktober 2011 ist Prof. Dr. Ramin Yahyapour neuer Geschäftsführer. Er löst damit den bisherigen wissenschaftlichen Geschäftsführer, Prof. Dr. Oswald Haan, und Dr. Paul Suren, den bisherigen administrativen Geschäftsführer, ab. Beide hatten nach dem Weggang von Prof. Dr. Bernhard Neumair am 01.07.2010 gemeinsam die Geschäftsführung übernommen. Prof. Haan geht nach 18-jähriger Tätigkeit bei der GWDG in den Ruhestand, Dr. Suren wird weiterhin, wie vorher auch, als Prokurist und Verwaltungsleiter bei der GWDG tätig sein.

Prof. Haan war seit 1993 bei der GWDG tätig. Vor seiner Berufung zum wissenschaftlichen Geschäftsführer im letzten Jahr war er langjähriger Leiter der Arbeitsgruppe „Anwendungs- und Informationssysteme“, zu deren Tätigkeitsbereich insbesondere die Hochleistungs-Rechencluster und das Grid Computing gehören, sowie seit dem 1. April 2007 zudem stellvertretender Leiter des Rechenzentrums.

Prof. Dr. Oswald Haan

Die 15-monatige Amtszeit von Prof. Haan war von einigen bedeutenden Ereignissen und Projekten geprägt. Zu nennen sind hier vor allem die erfolgreiche IT-Begutachtung am Wissenschaftsstandort Göttingen im Juli 2010, das Festkolloquium zum 40-jährigen Bestehen der GWDG am 28.10.2010, der Gewinn des Förderpreises des Bundeswirtschaftsministeriums auf der CeBIT Anfang März 2011 für das Cloud-Computing-Projekt „Cloud4E“, die erfolgreiche Einwerbung von Drittmitteln für weitere Forschungsprojekte zur Etablierung von eScience-Strukturen für Speicherung, Nachnutzung und Management von Forschungsdaten, die Inbetriebnahme eines neuen Hochleistungs-Rechenclusters ebenfalls Anfang März 2011, der die Gesamtrechenleistung aller Parallelrechnersysteme bei der GWDG verdoppelt hat, sowie der Aufbau der sog. Niedersachsen-Storage-Cloud als wichtigen Schritt in Richtung einer landesweiten, konsolidierten IT-Speicherstruktur.

Dr. Paul Suren

Der neue Geschäftsführer, Prof. Yahyapour, Jahrgang 1972, war bis zum 30.09.2011 Leiter des IT & Medien Centrums (ITMC) der TU Dortmund und gleichzeitig deren Chief Information Officer (CIO). An der dortigen Fakultät für Informatik hatte er eine Professur im Fach Angewandte Informatik und Informationstechnologien.

Prof. Dr. Ramin Yahyapour

Seine Forschungsinteressen, die sich auch in zahlreichen Projekten, Veröffentlichungen und der Mitgliedschaft in mehreren internationalen Grid-Computing-Netzwerken widerspiegeln, liegen auf den Gebieten Grid Computing, Job Scheduling, serviceorientierte Architekturen und Visualisierung.

Diese Forschungsgebiete will Prof. Yahyapour auch in seiner

Professur für das Fach Praktische Informatik am Institut für Informatik der Georg-August-Universität Göttingen weiter vertreten und vertiefen, die er gleichzeitig mit der GWDG-Geschäftsführerstelle übernimmt. Prof. Yahyapour sieht in dieser Konstellation großes Potenzial, dass die wissenschaftliche Tätigkeit verstärkt unmittelbar in die Arbeit des Rechenzentrums einfließen kann, damit dann frühzeitig innovative, für die Wissenschaft wichtige Dienste bereitgestellt werden. Der Ausbau zukunftsorientierter wissenschaftsnaher IT-Services sowie die sichere und effiziente Bereitstellung von IT-Basisdiensten für die Max-Planck-Gesellschaft und die Universität Göttingen, die beiden Gesellschafter der GWDG, gehören zu Prof. Yahyapours weiteren zukünftigen Aufgabenschwerpunkten.

Göttingen soll als leistungsfähiger und etablierter Grid-Standort weiter ausgebaut und damit auch der Göttingen Research Campus als mittlerweile etabliertes Netzwerk Göttinger Forschungseinrichtungen gestärkt werden. Die langjährige bewährte Kooperation zwischen den wissenschaftlichen IT-Dienstleistern am Göttingen Research Campus soll hierfür noch weiter intensiviert werden, denn nur durch eine konsequente Nutzung von Synergieeffekten kann die für das sog. eScience, das mittlerweile alle Wissenschaftsbereiche erfasst hat, notwendige leistungsfähige IT-Infrastruktur auch bereitgestellt werden.

Otto

Kontakt:
Dr. Thomas Otto
Thomas.Otto@gwdg.de
0551 201-1828

Liebe Kunden und Freunde der GWDG,

ich darf mich mit dieser Ausgabe der GWDG-Nachrichten als neuer Geschäftsführer und wissenschaftlicher Leiter der GWDG vorstellen. Mit dem 1. Oktober wurden mir die Geschäftsführung und damit die Verantwortung für eines der überregional anerkannten wissenschaftlichen Rechenzentren übertragen, das auf eine beeindruckende Historie zurückblicken kann. Mit 41 Jahren ist die GWDG im besten Alter. Dabei war die Struktur bereits 1970 ihrer Zeit voraus und ist mit jeweils hälftiger Beteiligung der Max-Planck-Gesellschaft und der Universität Göttingen ein echtes und vor allem erfolgreiches Kooperationsmodell. Damit wurden die jeweiligen Anforderungen an ein Rechenzentrum mit einem IT-Kompetenzzentrum für die Wissenschaft sinnvoll verbunden, das nicht nur den Standort Göttingen, sondern auch die überregionalen Max-Planck-Institute bei ihrer Arbeit unterstützt.

Es gilt mehr denn je, dass exzellente Forschung eine ausgezeichnete IT-Infrastruktur erfordert, die sich an internationalen Maßstäben nicht nur messen lässt, sondern diese möglichst auch übertrifft. Mein Ziel ist es, die Kundenorientierung der GWDG künftig noch weiter zu stärken und das Dienstleistungsspektrum weiter an den aktuellen Erfordernissen der Nutzer auszurichten. Dies betrifft zum einen die wichtigen Basis-IT-Dienste, die jederzeit verlässlich und wirtschaftlich funktionieren müssen, damitSie wissenschaftlich produktiv arbeiten können. Zum anderen besteht ein stetig wachsender Bedarf an forschungsnaher Unterstützung für erfolgreiches e-Science. So kann heute kaum noch eine Wissenschaftsdisziplin ohne den Zugriff auf eine leistungsfähige IT-Infrastruktur für daten- oder rechenintensive Anwendungen auskommen. Fragen der Langzeitarchivierung von Forschungsdaten z. B. sind ebenso aktuelle Themen wie der Umgang mit großen Datenmengen. Um diesen Anforderungen gerecht zu werden, wird die GWDG ihre Anstrengungen verstärken, um durch eigene Forschung an Forschungsinfrastrukturen mit Ihnen zusammen neue Methoden und Dienste frühzeitig entwickeln und für Sie produktionsreif anbieten zu können.

Ich werde meine bisherigen Erfahrungen aus der Leitung des Rechenzentrums in Dortmund nutzen, um die Rolle der GWDG als innovativer IT-Dienstleistungspartner mit hoher Beratungskompetenz zu stärken. Neben meinen bisherigen Forschungsschwerpunkten im Bereich Grid und Cloud Computing wird das Management von großen Datenmengen ein weiterer Schwerpunkt für e-Science-Infrastrukturen sein. Mein besonderes Interesse besteht in Forschungs-

kooperationen mit Partnern aus der Max-Planck-Gesellschaft und der Universität Göttingen, um gemeinsam innovative Lösungen vorantreiben können.

Ich freue mich auf die künftige Zusammenarbeit mit Ihnen und bedanke mich bereits jetzt für Ihr Vertrauen. Bitte zögern Sie nicht, mich bei Anregungen oder Kritik zu kontaktieren.

Prof. Dr. Ramin Yahyapour
ramin.yahyapour@gwdg.de

Feierstunde zum Geschäftsführungswechsel am 14. Oktober 2011

Anlässlich des Wechsels in der Geschäftsführung der GWDG fand am 14.10.2011 eine Feierstunde statt, in der der ehemalige wissenschaftliche Geschäftsführer und langjährige stellvertretende Leiter des Rechenzentrums, Prof. Dr. Oswald Haan, verabschiedet und der neue Geschäftsführer, Prof. Dr. Ramin Yahyapour, begrüßt wurden.

Begrüßung

Die Feierstunde begann um 13:00 Uhr mit der Begrüßung durch den **Prokuristen und Verwaltungsleiter der GWDG, Dr. Paul Suren,** im Manfred-Eigen-Saal des Max-Planck-Instituts für biophysikalische Chemie.

Er hieß die gut 100 Gäste herzlich willkommen und stellte kurz das Programm der 1,5-stündigen Veranstaltung vor.

Verabschiedung von Prof. Haan

Bevor **Markus Hoppe, hauptberuflicher Vizepräsident der Universität Göttingen und zugleich auch stellvertretender Aufsichtsratsvorsitzender der GWDG,** ausführlicher auf die fast 18-jährige Tätigkeit von Prof. Haan bei der der GWDG einging, bedankte er sich zunächst kurz beim neuen Geschäftsführer, Prof. Yahyapour, für die gute Zusammenarbeit bei den Verhandlungen in den letzten Monaten, insbesondere das Vertrauen zu den handelnden Personen in den zuständigen Gremien. Es war zeitweise eine komplizierte Konstellation, aber am Ende war Göttingen erfolgreich.

Vizepräsident Hoppe gab einen kurzen Rückblick auf die berufliche und wissenschaftliche Laufbahn von Prof. Haan: 1964 bis 1969 Studium der Physik in München, Mainz und Heidelberg, 1969 Diplom, 1971 Promotion, anschließend einige Jahre wissenschaftlicher Assistent an den Universitäten Heidelberg und Wuppertal, 1978 Habilitation an der Universität Wuppertal und dort dann auch Professor, 1986 bis 1990 Fachreferent für wissenschaftliche Anwendungen auf Höchstleistungsrechnern bei Siemens. Am 01.12.1993 ist er dann schließlich als Leiter der damaligen Arbeitsgruppe „Numerische Anwendungssoftware“ in die GWDG eingetreten. Er hatte im Laufe der Jahre mehrere Lehraufträge an der Universität Göttingen und wurde schließlich auch zum außerplanmäßigen (apl.) Professor berufen. 2007 wurde er stellvertretender Leiter des Rechenzentrums und am 01.07.2010 schließlich wissenschaftlicher Geschäftsführer der GWDG, als er nach dem Weggang von Prof. Neumair ohne Zögern in der „Notsituation“ eingesprungen ist und als verlässlicher Partner die GWDG in den vergangenen 15 Monaten „auf Kurs gehalten hat“.

Die im Zusammenhang mit der jetzt abgeschlossenen Neubesetzung der GWDG-Leitung im Sommer letzten Jahres erfolgte IT-Begutachtung am Wissenschaftsstandort Göttingen hat sich für alle Beteiligten gelohnt. Der GWDG wurde ein gutes Zeugnis ausgestellt und genaue Hinweise für ihre Weiterentwicklung gegeben, die z. T. schon umgesetzt sind. Die Geschäftsführung der GWDG war bei dieser externen Begutachtung ein bedeutender Erfolgsgarant. Die Zusammenarbeit mit Prof. Haan

war immer sehr angenehm. Er hat sich stets in die „Pflicht nehmen lassen", zeigte ein hohes Maß an Gelassenheit gepaart mit Loyalität und Herzlichkeit, so Vizepräsident Hoppe. Für all seinen Einsatz dankte er zum Schluss im Namen der Universität, der Universitätsmedizin, des Aufsichtrates sowie der Gesellschafterversammlung der GWDG, verbunden mit den besten Wünschen für seinen nun begonnenen Ruhestand.

Uwe Gerdes, Betriebsratsvorsitzender der GWDG, ging in seinen Abschiedsworten zunächst auf die verschiedenen Aufgabenbereiche ein, für die Prof. Haan während seiner fast 18 Jahre bei der GWDG tätig war. Lag zunächst der Tätigkeitsschwerpunkt im Bereich „Parallelrechnen", kam dann in den Folgejahren der Bereich „Multimedia" mit der Realisierung des Druck- und Grafikbetriebs sowie netzbasierten Multimediaanwendungen wie Videoverteilung und Videokonferenzen hinzu.

Sowohl bei der Auswahl und Bereitstellung von Parallelrechnersystemen als auch bei der Unterstützung und Beratung der Anwender bei ihren Fragen zur Parallelverarbeitung war der enge Kontakt mit den Nutzern für Prof. Haan von großer Bedeutung. Die Einführung von Grid-Technologien wurde von Prof. Haans Arbeitsgruppe engagiert vorangetrieben und durch zahlreiche Forschungsprojekte begleitet, zu denen aktuell OptiNum-Grid, DGSI und Cloud4E gehören. Auch im Windows-Bereich hat Prof. Haan als Gruppenleiter die Arbeit koordiniert und die Voraussetzungen für zentrale Dienstleistungen in diesem Bereich geschaffen. Damit wurden auch die Grundlagen für das heutige Active Directory von ihm mit gelegt.

Die erfolgreiche Arbeit Prof. Haans basierte neben seinen fachlichen Qualitäten auch auf den persönlichen Eigenschaften: in seiner ruhigen Art immer ausgleichend und vermittelnd sowie mit dem notwendigen Interesse für die Belange aller Mitarbeiter, um Vorgänge zu verstehen und jederzeit als Gesprächspartner zur Verfügung stehen zu können. Die Zusammenarbeit mit dem Betriebsrat, nicht nur in den letzten Monaten als wissenschaftlicher Geschäftsführer, war immer fair und konstruktiv. Bevor Herr Gerdes Herrn Haan mit den besten Wünschen für seinen Ruhestand verabschiedete, hieß er im Namen aller Mitarbeiterinnen und Mitarbeiter der GWDG Prof. Yahyapour herzlich bei der GWDG willkommen, verbunden mit der Freude auf die künftige Zusammenarbeit.

Für den **IT-Sprecherkreis der Max-Planck-Institute** sprach C**hrista Hausmann-Jamin** ihr Bedauern aus, dass die die kurze, überaus angenehme und erfolgreiche Zusammenarbeit mit Prof. Haan als wissenschaftlicher Geschäftsführer leider schon beendet ist. Die Einführung der Institutsbetreuer für die Max-Planck-Institute sowie der neuen Nutzervertretung sind aus Sicht der Max-Planck-Institute wichtige Meilensteine aus dieser Zeit, an denen Prof. Haan großen Anteil hat. Mit Spannung wird die weitere Zusammenarbeit erwartet. Die Messlatte liegt hoch, so Frau Hausmann-Jamin abschließend.

Bevor **Prof. Haan** einen Rückblick auf seine lange Zeit bei der GWDG gab, bedankte er sich zunächst bei allen drei Rednern für die herzlichen Abschiedsworte. Als er 1993 bei der GWDG anfing, hatte gerade auch die Ära der Parallelrechner begonnen. Der Einsatz des Computers und insbesondere des Parallelrechners erschloss der Forschung neue, bis dahin nicht gekannte Möglichkeiten. Die Rechengeschwindigkeit spielte dabei eine große Rolle. Deren Entwicklung bei der GWDG im Parallelrechnerbereich verdeutlicht dies in beeindruckender Weise: Der erste Parallelrechner KSR1 leistete mit 32 Prozessoreinheiten 1,2 Millionen Rechenoperationen pro Sekunde, alle derzeitigen Parallelrechnercluster bei der GWDG leisten aktuell mit 5.700 Prozessoreinheiten 58 Billionen Rechenoperationen pro Sekunde – also der Faktor 50.000 bei der Parallelrechnerleistung.

An den Schnittstellen zwischen den Forschungsthemen und den IT-Werkzeugen zu ihrer Bearbeitung gab es im Laufe der Jahre viele spannende und interessan-

te Nutzerprojekte, die immer von guter Zusammenarbeit geprägt waren. Das Werkzeug Parallelrechner zu verstehen und laufend zu verbessern, war sein zentrales Forschungsthema über all die Jahre, so Prof. Haan, und das zeigte sich auch in vielen seiner Vorlesungen und Veröffentlichungen. Wichtig war ihm dabei auch die Organisation eines leistungsfähigen Parallelrechnerbetriebes. Dabei konnte er sich stets auf die Unterstützung seiner Mitarbeiter verlassen. Die Zusammenarbeit mit ihnen war angenehm und produktiv.

Die IT ist mittlerweile in alle Bereiche der Wissenschaft vorgedrungen, was auch zu einer gewissen Abhängigkeit der Wissenschaftler von den IT-Diensten geführt hat. Die GWDG hat bei der Bereitstellung solcher Dienste oftmals eine Vorreiterrolle eingenommen und sich schon sehr früh vom reinen Rechenzentrum zu einem leistungsfähigen IT-Kompetenzzentrum mit einem umfangreichen Leistungsspektrum entwickelt.

Die letzten 15 Monate als wissenschaftlicher Geschäftsführer waren aus Prof. Haans Sicht schöne Monate, die ihm noch Mal einen neuen Blickwinkel auf die GWDG ermöglicht haben. Er dankte allen Mitarbeiterinnen und Mitarbeitern für ihren großen Einsatz, insbesondere Dr. Suren für seine Unterstützung als administrativer Geschäftsführer, und dem Aufsichtsrat und der Gesellschafterversammlung für das ihm entgegengebrachte Vertrauen in der Geschäftsführerfunktion. Prof. Haan schloss seine Abschiedsworte mit den besten Wünschen für seinen Nachfolger Prof. Yahyapour. Die Übergabe und der Start sind gelungen und eine gute Basis für die positive Weiterentwicklung der GWDG.

Wissenschaftlicher Vortrag

Prof. Dr. Arnulf Quadt, Direktor des II. Physikalischen Instituts der Universität Göttingen, gab in seinem 30-minütigen Vortrag einen interessanten Überblick in den Stand und die weitere Entwicklung des Grid Computing in der Teilchenphysik. Zuvor bedankte er sich bei Prof. Haan, dass er vieles in diesem Bereich am Wissenschaftsstandort Göttingen unterstützt und möglich gemacht hat und auch er sehr von ihm profitiert hat. In der Teilchenphysik geht es darum, die Grundbausteine der Natur zu verstehen, u. a. die Fragen, wie diese zusammenhalten. Vieles ist schon verstanden, aber es sind noch viel mehr Fragen offen (z. B. die Rolle der Neutrinos).

Zur Untersuchung der Fragestellungen werden Teilchenbeschleuniger eingesetzt, in denen es zu Proton-Proton-Kollisionen kommt. Am CERN, dem europäischen Zentrum für Teilchenphysik in Genf, werden 40 Millionen solcher Kollisionen pro Sekunde im sog. Large Hadron Collider (LHC) erzeugt. In verschiedenen Experimenten untersucht eine Vielzahl von Physikern in internationalen Kollaborationen die unterschiedlichsten Fragestellungen. Dabei kommt dem Grid Computing eine zentrale Rolle zu. Ohne dieses Instrument wäre es nicht möglich, die riesigen anfallenden Datenmengen auszuwerten.

Auch Göttingen ist wichtiger Standort im World Wide Grid und sog. Tier-2- und Tier-3-Zentrum beim LHC-Projekt. Die Rechen- und Speicherressourcen dafür sind im GoeGrid zusammengefasst, das 2008 mit tatkräftiger Unterstützung von Prof. Haan gegründet wurde und bei der GWDG angesiedelt ist. Es beinhaltet auch die Rechen- und Speicherressourcen der anderen Grid-Communities am Wissenschaftsstandort Göttingen und es ein wichtiger Bestandteil der leistungsfähigen Göttinger eScience-Infrastruktur in Forschung und Lehre.

Begrüßung von Prof. Yahyapour

Prof. Dr. Christian Griesinger, Direktor am Max-Planck-Institut für biophysikalische Chemie in Göttingen und zugleich Aufsichtsratsvorsitzender der GWDG, stellte Prof. Yahyapour vor, indem er zunächst einen kurzen Überblick über dessen Lebenslauf mit seinen bisherigen beeindru-

ckenden beruflichen und wissenschaftlichen Stationen gab: 1991 bis 1996 Studium der Elektrotechnik an der Universität Dortmund, 1996 Diplom, 2002 Promotion zum Dr.-Ing., 1996 bis 2007 wissenschaftlicher Mitarbeiter an der Universität Dortmund, 2007 bis 2009 kommissarischer Leiter des IT und Medien Centrums (ITMC) der TU Dortmund und Übernahme der Vertretungsprofessur für „IT und Medien", 2009 Ernennung zum Chief Information Officer (CIO) der TU Dortmund, 2009 Berufung als Professor und Leiter des ITMC der TU Dortmund mit angeschlossenem Lehrstuhl in „Angewandter Informatik und Informationstechnik" und Kooptation in der Fakultät Informatik. Seit 2009 ist Prof. Yahyapour Koordinator des BMBF-Projektes „SLA4D-Grid" im Rahmen der D-Grid-Initiative und wissenschaftlicher Koordinator im Projekt „SLA@SOI" im 7. Rahmenprogramm der EU. Eine äußerst beachtliche Zahl von Veröffentlichungen dokumentiert die intensive wissenschaftliche Arbeit von Prof. Yahyapour.

Auf der Grundlage des positiven Ergebnisses und der Empfehlungen der IT-Begutachtung im Sommer 2010 wurde mit Prof. Yahyapour eine wissenschaftlich ausgewiesene Führungspersönlichkeit gefunden, die auch über die notwendigen Erfahrungen im Management eines wissenschaftlichen Rechenzentrums verfügt. In Verbindung mit der gleichzeitigen Professur für das Fach Informatik am Institut für Informatik der Universität Göttingen ergibt sich ein großes wissenschaftliches Potenzial. Die derzeit laufende Neuordnung der IT-Governance-Struktur am Wissenschaftsstandort Göttingen führt zudem zu einer noch besseren Wahrnehmung und Vertretung der Interessen aller Nutzer der GWDG. Erfreulich ist, dass zusammen mit Prof. Yahyapour auch acht Wissenschaftler aus seinen Dortmunder Projekten mit nach Göttingen gewechselt sind und damit drei feste Stellen für die Forschung geschaffen werden konnten.

Der Aufsichtsrat freut sich, so Prof. Griesinger abschließend, auf die künftige Zusammenarbeit mit Prof. Yahyapour und ist sehr zuversichtlich, dass es ihm gelingen wird, die erfolgreiche Arbeit der GWDG fortzusetzen und die für das eScience in allen Wissenschaftsbereichen notwendige IT-Infrastruktur bereitzustellen und weiterzuentwickeln.

Prof. Yahyapour dankte zu Beginn seiner Rede allen Vorrednern für die guten Wünsche zu seinem Start in Göttingen. Dieser wurde ihm durch die angenehme Zusammenarbeit mit seinem Vorgänger, Prof. Haan, sehr erleichtert: Der Wechsel war vorbildlich vorbereitet und das gut geführte Schiff wurde in gutem Zustand übergeben. Für seinen Wechsel nach Göttingen führte Prof. Yahyapour vier entscheidende Gründe an. Erstens: Der exzellente Ruf der GWDG in der Community der Rechenzentren als gut aufgestellter IT-Dienstleister für die Wissenschaft. Zweitens: Das erfolgreiche Konstrukt der GWDG als Gemeinschaftsunternehmen mit je hälftiger Beteiligung der Max-Planck-Gesellschaft und der Universität Göttingen. Solche Kooperationen sind aktueller denn je und bei der GWDG schon seit 40 Jahren erfolgreich gelebte Realität – ein Modell mit Vorbildcharakter.

Drittens: Das breite Spektrum an IT-Themen bzw. -Fragen und -Dienstleistungen. Dazu gehören zum einen die Bereitstellung von IT-Basisdiensten und zum anderen die Unterstützung exzellenter Forschung durch eine entsprechende eScience-Infrastruktur. Für ein Rechenzentrum wie die GWDG stellt es eine große Herausforderung dar, beim Aufbau neuester und modernster Technologien möglichst eine Vorreiterrolle einzunehmen und zu versuchen, besser als andere zu sein. Und schließlich viertens: Der Standort Göttingen selbst mit seinem einzigartigen Umfeld des Göttingen Research Campus als etabliertes Netzwerk unterschiedlicher Göttinger Forschungseinrichtungen, universitärer wie außeruniversitärer, der alle Wissenschaftsbereiche umfasst. Ein wichtiger Aufgabenbereich dabei ist der weitere Ausbau Göttingens als leistungsfähiger Grid-Standort. All diesen Herausforderungen stellt er sich gerne, so Prof. Yahyapour, und er freut sich auf die Zusammenarbeit mit allen Beteiligten.

Empfang

Die Feierstunde klang mit einem Empfang im Foyer aus. Zahlreiche Gäste nutzen dabei die Gelegenheit, sich persönlich von Prof. Haan zu verabschieden und Prof. Yahyapour zu begrüßen.

Beim Smalltalk mit ihm entwickelten sich schon erste Ideen für neue Projekte und IT-Leistungen.

Otto

Kontakt:
Dr. Thomas Otto
Thomas.Otto@gwdg.de
0551 201-1828

Neuer Großformatscanner „Contex HD4230“

Seit Kurzem verfügt die GWDG über einen neuen Großformatscanner zum Scannen von Vorlagen bis zu 106 cm (42``) Breite.

CCD-Kameras und hochwertigen Linsen ausgestattet, die laut Herstellerangebe die beste Bildqualität im gesamten Großformatscanner-Bereich liefern.

1 *Der neue Großformatscanner Contex HD4230*

Merkmal	Beschreibung
Optische Auflösung	600 dpi
Maximale Auflösung	1.200 dpi
Maximale Scanbreite	1.067 mm
Maximale Medienbreite	1.118 mm
Maximale Medienstärke	15 mm
Scangenauigkeit	0,1 % +/- 1 Pixel
Farbtiefe der Scans (Farbe / SW)	48 bit / 16 bit
Farbraum	sRGB
Scannscoftware	NextImage

2 *Technische Daten des Contex HD4230*

Die GWDG freut sich, ihren Benutzern diesen Scanner als ersehnten Ersatz für den defekten und nicht mehr reparierbaren Scanner Graphtec CS600 präsentieren zu können. Die Scanbreite von 106 cm ist darauf ausgelegt, die Reproduktion oder das Archivieren einer Vielzahl von Dokumenten wie z. B. Landkarten, Poster, technische Zeichnungen oder Gebäudegrundrisse in hoher Auflösung und maximaler Detailtreue zu ermöglichen. Der Contex HD4230 ist mit vier

Da es sich bei diesem Scanner um ein teures und hochempfindliches Gerät handelt, ist eine Nutzung nur nach Einweisung durch das GWDG-Bedienpersonal möglich.

Nolte

Kontakt:
Uwe Nolte
unolte@gwdg.de
0551 201-1547

Tag der offenen Tür am 5. November 2011

Forschung hautnah – von der lebenden Zelle bis zum Roboter: Der neue Max-Planck-Campus stellt sich am Samstag, 5. November 2011, mit einem Tag der offenen Tür vor.

Von gewaltigen Luftverwirbelungen bis zu winzigen Zellbausteinen, von riesigen Mengen Bits und Bytes in der Datenwolke bis zu den Vorgängen, die das Leben steuern. Die Forschungsthemen des Max-Planck-Instituts für biophysikalische Chemie (MPIbpc), des Max-Planck-Instituts für Dynamik und Selbstorganisation (MPIDS) und der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) am neuen Max-Planck-Campus auf dem Faßberg 11-17 könnten vielfältiger nicht sein. Ein ebenso abwechslungsreiches Programm bieten die drei dort ansässigen Forschungseinrichtungen beim Tag der offenen Tür am Samstag, 5. November. Unter dem Motto „Forschung hautnah – von der lebenden Zelle bis zum Roboter" geben die Mitarbeiter an diesem Tag von 10 bis 16 Uhr detaillierte Einblicke in ihre Arbeit, öffnen Labore, Rechnerräume und Werkstätten und verraten, was sie an der Forschung fasziniert.

Auf dem Faßberg ganz in der Nähe des Nordcampus der Universität Göttingen hat sich in den vergangenen Monaten einiges getan: Mit dem Umzug des MPIDS aus der Stadtmitte an den Faßberg ist der Forschungscampus um ein weiteres Institut gewachsen – und bietet nun noch mehr spannende Forschungsschwerpunkte. Was genau sich hinter den drei Forschungseinrichtungen verbirgt, erfahren Interessierte am Tag der offenen Tür.

Einen Überblick können die Besucher am Tag der offenen Tür im Info-Foyer gewinnen. Dort präsentieren fast 40 Forschungsgruppen und Einrichtungen ihre Projekte in Kürze. Wie gelingt es den Nervenzellen im Gehirn, Informationen schnell und fehlerfrei zu übertragen? Wie funktioniert ein Elektronenmikroskop? Was ist eigentlich Chaos und wie arbeitet ein Parallelrechner? Antworten erhalten die Gäste bei mehr als 20 verschiedenen Führungen, die sie direkt an die Orte des Geschehens bringen: in die biologischen Labore und Rechnerräume, zum riesigen Turbulenz-Windkanal oder an meterhohe Elektronenmikroskope. Während sich die einen im Magnetresonanztomografen beim Sprechen und Denken zuschauen lassen, können sich die anderen auf die Spuren der ersten

Rechenmaschinen begeben oder beobachten, wie sich Schwärme künstlicher Käfer selbst organisieren.

Parallel dazu berichten Forscher des Max-Planck-Campus in allgemeinverständlichen Vorträgen von ihrer Arbeit und ihren neuesten Ergebnissen. Ganz wie im Kino können sich Besucher zudem Filme rund um wissenschaftliche Themen und die Max-Planck-Gesellschaft sowie die GWDG anschauen. Im Mitmach-Labor können schließlich alle Besucher selbst experimentieren.

Schülerinnen und Schüler dürfen sich auf ein eigenes Programm freuen: Bei der Campus-Rallye werden sie selbst zu Forschern. An knapp 30 verschiedenen Stationen wagen sie den Röntgenblick ins Überraschungsei, bringen Zellen zum Leuchten oder erforschen das Innenleben eines Computers. Schritt für Schritt erkunden die Nachwuchsforscher so den gesamten Campus und sammeln Stempel für ihren Forscherpass. Natürlich wird so viel Neugier und Einsatz zum Schluss mit einer Urkunde belohnt. Darüber hinaus steht eine Vortragsreihe speziell für Kinder auf dem Programm: Hier berichten Wissenschaftler, wie das Herz funktioniert, was Sandburgen im Innersten zusammenhält und wie klug Roboter sind – zum Zuhören, Mitmachen und Anfassen. Im Anschluss an die Vorträge werden die Gewinner des Grundschul-Malwettbewerbs „Was macht ein Forscher?“ gekürt. Mehr als 160 Schüler haben sich an der Aktion mit bunten Bildern beteiligt, die die Besucher den ganzen Tag in einer Ausstellung anschauen können.

Für eine Stärkung zwischendurch stehen ein warmer Imbiss, Getränke, Kaffee und Kuchen in der Kantine und Espressobar bereit. Kinder von drei bis sechs Jahren werden in der Kindertagesstätte auf dem Campus professionell betreut. Und die Anreise? Kein Problem. Auf dem Campus sind Parkplätze in begrenzter Anzahl verfügbar. Weitere Parkplätze mit kostenloser Shuttle-Bus-Anbindung befinden sich am Nordcampus der Universität sowie an der Fakultät für Forstwissenschaften und Waldökologie. Der Shuttle-Bus bringt die Besucher ab 9:30 Uhr viertelstündlich vom Bahnhof (Bussteig D) über die Haltestellen Auditorium, Tammannstraße (Uni-Nord) und Burckhardtweg (Fakultät Forstwissenschaften) zum Campus und zurück.

Weitere Informationen sind unter dem URL *http://www.gwdg.de/index.php?id=2429* zu finden.

Krummheuer, Otto, Rotte

Kontakt:
Dr. Thomas Otto
Thomas.Otto@gwdg.de
0551 201-1828

FÜHRUNGEN

Allgemeine Führungen	Anmeldung	Dauer
Betriebstechnik MPI für biopysikalische Chemie	Stand 9,	ca. 1 Stunde
Elektronenmikroskopie von der Zelle bis zur molekularen Maschine	Stand 29,	ca. 1 Stunde
Entwicklungsbiologie	Stand 20,	ca. 1 Stunde
Magnetresonanztomografie	Stand 26,	ca. 2 Stunden
Musterbildung in Organismen	Stand 34,	ca. 1/4 Stunde
NanoBiophotonik	Stand 3,	ca. 1/2 Stunde
Nanomaschinen bei der Arbeit. Wie Proteine mit Computersimulationen beobachtet werden können	Stand 17,	ca. 1 Stunde
Neurobiologie auf molekularer Ebene	Stand 19,	ca. 1 1/2 Stunden
NMR-basierte Strukturbiologie	Stand 25,	ca. 1 1/2 Stunden
Plastizität der synaptischen Übertragung	Stand 18,	ca. 1 Stunde
Rasterelektronenmikroskopie	Infostand,	ca. 1/2 Stunde
Rechenzentrum	Stand 31,	ca. 1 Stunde
Rechnermuseum	Stand 31,	ca. 1 1/2 Stunden
Röntgentomograph	Stand 34,	ca. 1/2 Stunde
Struktur und Dynamik von Mitochondrien	Stand 4,	ca. 1/2 Stunde
Struktur und Regulation des Chromatins	Stand 16,	ca. 1 Stunde
Superschnell und superempfindlich – biophysikalische Methoden zur Erforschung von Nanomaschinen	Stand 30,	ca. 1 1/2 Stunde
Wie Gene die Entwicklung kontrollieren und steuern	Stand 23,	ca. 1 Stunde
Windkanal	Stand 34,	ca. 1/2 Stunde
Zelluläre Biochemie	Stand 21,	ca. 1 Stunde
Zelluläre Logistik	Infostand,	ca. 1/2 Stunde

10:30 11:30 12:30 13:30 14:30 15:30
11:00 12:00 13:00 14:00 15:00

Führungen für Kinder und Jugendliche

Wie breiten sich Infektionskrankheiten aus?	Stand 34,	ca. 1/2 Stunde
Röntgenblick ins Überraschungsei	Stand 34,	ca. 1/2 Stunde
Die Chaos-Forscher	Stand 34,	ca. 1/2 Stunde

10:30 11:30 12:30 13:30 14:30 15:30
11:00 12:00 13:00 14:00 15:00

Tag der offenen Tür

Forschung hautnah –

von der lebenden Zelle bis zum Roboter

Windows Phone 7

Neben den beiden derzeit am weitesten verbreiteten beiden Smartphone-Betriebssystemen, Apples iOS (iPhone und iPad) und Googles Android, hat Microsoft im Oktober 2010 mit „Windows Phone 7" einen weiteren Konkurrenten ins Rennen geschickt. Er kann ebenfalls dank Multi-Touch über Fingergesten bedient werden und wurde im Wesentlichen als Nachfolger des bereits damals nicht mehr ganz zeitgemäßen „Windows Mobile" positioniert.

Erscheinungsbild

Die Bedienung von Windows Phone 7 ist konsequent auf Mehrfingergesten und Multitouch-Oberflächen ausgelegt. Auffällig ist die Möglichkeit zur benutzerspezifischen Anpassung des Startbildschirms (Homescreen). Werden Anwendungen (Apps) neu installiert, dann landen sie nicht dort, sondern alphabetisch sortiert in einem separaten Fenster (Screen), von dem aus sie dann auf Wunsch auf den Homescreen gebracht werden können. Dort erscheinen sie, wie die bereits standardmäßig mitgelieferten Funktionen und Apps, als quadratische oder rechteckige Programmsymbole, die kachelförmig angeordnet sind. Manche dieser Kacheln – „Live Tiles" oder auch Live-Kacheln genannt – ermöglichen bereits die Anzeige von wichtigen Informationen und Statusmeldungen, ohne dazu die dazugehörigen Anwendungen öffnen zu müssen. Ein weiteres neues Konzept stellen die „Hubs" dar, die bestimmte Themenbereiche vereinigen und fest im Betriebssystem verankert sind. So gibt es beispielsweise einen „Kontakte-Hub", der alle Kontakte aus Exchange, Windows Life, Facebook, Twitter etc. zusammenfasst und so gewissermaßen als Kommunikationszentrale die daraus entstehenden Informationen übersichtlich aufbereitet. Der „Bilder-Hub" erlaubt den Überblick auf alle Fotos, ob sie lokal auf dem Mobilgerät oder im Internet gespeichert vorliegen. In gleicher Weise bietet der „Office-Hub"-Zugriff auf die Office-Anwendungen Word, Excel, PowerPoint und OneNote, egal ob die Dokumente lokal oder auf Servern im Internet (Office 365, SkyDrive oder SharePoint-Server) liegen.

Das System als Ganzes lässt sich flüssig bedienen, was nicht zuletzt auch an den Hardware-Vorgaben liegen mag, die Microsoft von den Herstellern fordert. Viele Anwendungen kommen ganz ohne Grafiken aus, und die Auswahl der Funktionen wird dann über Textmenüs in gut lesbarer, großer Schrift realisiert. Diese auf den ersten Blick vielleicht ungewohnte Darstellung verhilft ebenfalls zu höherer Geschwindigkeit und guter Übersicht.

Online-Speicher

Über die „Windows Live Id", die Windows Phone 7 im Zuge der Einrichtung abfragt bzw. bei deren Fehlen auch neu einrichtet, werden cloud-basierte Dienste kostenlos zur Verfügung gestellt. So bietet beispielsweise der 25 GByte große Online-Speicherplatz „SkyDrive" Ablagemöglichkeiten für Bilder und Office-Dokumente, die dann ohne Zutun des Anwenders mit dem Mobilgerät abgeglichen werden. Es wird aber auch die Synchronisation mit Exchange-Servern und institutsinternen SharePoint-Servern ermöglicht.

Windows Marketplace

Wie iOS und Android lässt sich auch Windows Phone 7 durch zusätzliche Anwendungen – den sog. Apps – erweitern. Sie bezieht der Anwender über einen zentralen Softwareshop, dem „Windows Marketplace", sobald er sich dort mit seiner Windows-Live-Id anmeldet. Im Unterschied zu den Softwareshops der Konkurrenz unterstützt der „Windows Marketplace" die Möglichkeit zum Testkauf.

Zune-Software

Windows Phone 7 bietet im Gegensatz zu seinem Vorgänger keinen USB-Laufwerksmodus mehr, um so zwecks Übertragung von Daten direkt auf den integrierten Flash-Speicher des Mobilgeräts zugreifen zu können. Beim erstmaligen Verbinden wird daher neben der üblichen Treiberinstallation unter Windows auch gleich der Download der Zune-Software vom folgenden Ort angeboten: *http://www.zune.net/*. Diese ermöglicht die Übertragung von Videos, Musik und Fotos per USB-Verbindung. Für Mac OS X gibt es alternativ den „Windows Phone 7

Connector for Mac“ *http://www.microsoft.com/windowsphone/de-de/apps/mac-connector.aspx*, der sich nahtlos in die iTunes-Library einklinkt, um auf diese Weise die Multimedia-Dateien zu übertragen.

Updates und Versionen

Der ursprünglich von Windows Phone 7 gebotene Funktionsumfang konnte mit den Mitbewerbern wie iOS oder Android nicht konkurrieren. Aber bereits damals wurde auf zwei größere Updates verwiesen, die allen Geräten kostenlos in Aussicht gestellt wurden.

So reichte das im März 2011 erschienene Update mit dem Codenamen „NoDo“ neben der Verbesserung der Geschwindigkeit im Wesentlichen die bislang fehlende „Copy&Paste“-Funktion nach. Aber erst das Update 7.5 mit dem Codenamen „Mango“ liefert nun alle die Funktionen nach, die Windows Phone 7 erst konkurrenzfähig machen. Es wird ab Oktober 2011 nach und nach allen Anwendern zur Verfügung gestellt und bietet laut Microsoft mehr als 500 neue Funktionen, worunter die folgenden sicherlich die wichtigsten sind:

- **Multitasking:** Mehrere Anwendungen können jetzt gleichzeitig ablaufen, und durch einen längeren Druck auf die „Zurück-Taste“ wird eine Übersicht über und der Zugriff auf die aktuell laufenden Applikationen geboten.

- **Ein verbesserter Browser:** Statt des arg veralteten, ursprünglich mitgelieferten Internet Explorer kommt nun dessen aktuelle Version 9 mit der Unterstützung von HTML5 und einer hardwarebeschleunigten grafischen Darstellung zum Einsatz. Damit bietet sich nun auch die Möglichkeit, YouTube-Videos zu betrachten. Auf die Darstellung von Flash-Inhalten verzichtet übrigens Microsoft ebenso wie Apple.

- **Soziale Netzwerke:** Twitter, LinkedIn und Facebook können jetzt im Kontakte-Hub integriert werden.

- **Eine erweiterte Nachrichten-App:** unterstützt neben SMS auch Facebook- und MSN-Chat.

- **Die Gruppierungsfunktion im Adressbuch:** Kontakte können einfach in Gruppen sortiert und auf die Startseite gebracht werden; über Live-Kacheln lassen sich so verpasste Anrufe, Nachrichten oder Status-Updates sofort erkennen.

- **Mail:** Mehrere E-Mail-Konten können in einem Posteingang zusammengeführt werden, und auch die bei der Konkurrenz so beliebte Konversationsansicht, bei der zusammengehörige Mails zusammenfasst werden, ist nun möglich.

- Der **Exchange-Server** gleicht jetzt auch die Aufgabenplanung mit ab.

- **Verbesserte Bedienung dank dynamischer Live-Kacheln:** Die bisherigen Live-Kacheln („Live Tiles“) werden dynamischer und liefern nun noch mehr Informationen.

- **Windows Phone Web Marketplace:** Zeitgleich mit dem „Mango“-Update startet auch der neue „Windows Phone Web Marketplace“, über den der Anwender nun auch über den Browser Einkäufe tätigen und dort seine Apps verwalten kann

- **Bing für Windows Phone:** Microsofts Suchmaschine „Bing“ bietet neben einer Musiksuche auch die Suche nach Produkten, indem diese über die eingebaute Kamera erfasst werden.

Das „Mango“-Update wird übrigens über die Zune-Software oder auf dem Mac über den „Windows Phone 7 Connector“ eingespielt.

Anwendungen

Der Erfolg eines mobilen Betriebssystems hängt heutzutage auch ganz entscheidend von den verfügbaren Anwendungen (Apps) ab. Selbst wenn die Anzahl der für Windows Phone 7 derzeit erhältlichen Programme längst nicht mit der von Android oder iOS konkurrieren kann, so findet der Nutzer unter den inzwischen etwa 50.000 Programmen durchaus das Wichtigste für seine tägliche Arbeit. Im Folgenden soll eine kleine Auswahl aufgelistet werden (wobei hier die Interessenlage des Autors nicht ganz ohne Folgen blieb):

- **Office:** Im Gegensatz zur Konkurrenz liefert Microsoft wie schon bei dem Vorgänger „Windows Mobile“ die komplette Office-Suite mit:

Word, Excel, PowerPoint und OneNote, jeweils mit der Abgleichmöglichkeit zu Office 365, SkyDrive oder einem SharePoint-Server.

- **APPA Mundi Tasks:** Wem der Aufgabenabgleich in „Mango“ noch zu spartanisch ist, findet in „APPA Mundi Tasks“ einen leistungsfähigen Task-Manager, der sich mit der Aufgabenverwaltung des Exchange-Servers synchronisiert.

- **Soziale Netze:** Wem die Unterstützung in „Mango“ noch nicht weitreichend genug ist, der findet im Marketplace native Apps beispielsweise für Twitter (von „Twitter, Inc.“) und für Facebook.

- **Evernote:** Die beliebte leistungsfähige Online-Notizenerfassung und -verwaltung bietet inzwischen auch eine native App für Windows Phone 7 und deckt damit nun fast alle verfügbaren Betriebssysteme ab.

- **NextGen:** Wer gerne Neuigkeiten über sogenannte RSS-Feeds verfolgt und diese im Google Reader sammeln lässt, findet in NextGen einen konfortablen und leistungsfähigen RSS-Reader.

- **Navigon Select Telekom Edition:** Wie schon für Besitzer des iPhones oder eines Android-Gerätes gibt es auch für die Nutzer des Windows Phone 7 die beliebte Turn-by-Turn-Navigationslösung „Navigon Select Telekom Edition“ kostenlos, sofern er Telekom-Kunde ist. Die Software kann über den Windows Marketplace heruntergeladen werden. Bei der Aktivierung sollte wie immer darauf geachtet werden, dass man sich im Mobilfunknetz befindet (WLAN deaktivieren).

- **Adobe Reader:** Da Windows Phone 7 PDF-Dokumente nicht anzuzeigen in der Lage ist, braucht man hierfür den Adobe Reader, der ebenfalls kostenlos im Windows Marketplace bereitsteht.

Fazit

Zusammenfassend betrachtet erweist sich Windows Phone 7 besonders nach dem „Mango“-Update als eine interessante Alternative zu Android und iOS und zeigt durchaus Potenzial. Ob man sich letztlich dazu entscheidet, hängt natürlich immer auch von der Hardware, also dem jeweiligen Mobiltelefon ab. Da aber aus der Kooperation von Microsoft und Nokia bald interessante Smart-Phones zu erwarten sind, dürfte das die Vielfalt für die Zukunft entscheidend verbessern. Immerhin prognostizieren die Analysen von Gartner und IDC Windows Phone 7 für 2015 einen Marktanteil von 20 % und sehen es damit sogar noch vor iOS an zweiter Stelle.

Ob diese Entwicklung wirklich auch so oder vielleicht anders eintrifft, die GWDG bietet bereits heute ihren Kunden Support für dieses mobile Betriebssystem von Microsoft. So finden sich beispielsweise Konfigurationsanleitungen für Exchange-Server und Eduroam unter der Adresse *http://www.gwdg.de/index.php?id=2432* und auch in der Mailingliste GWDG-MOBIL wird Windows Phone 7 immer mehr zum Gegenstand der Betrachtung. Auf diese kann sich übrigens jeder Interessierte über die Webseite *https://listserv.gwdg.de/mailman/listinfo/gwdg-mobil* anmelden. Die Beiträge aus dieser Mailingliste können auch auf den Seiten *http://www.gwdg.mobi* oder auch über Twitter (gwdgmobil) verfolgt werden.

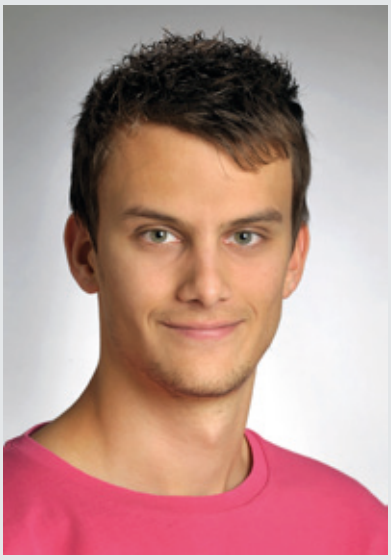
Reimann

Kontakt:
Michael Reimann
Michael.Reimann@gwdg.de
0551 201-1826

Personalia

Neuer Mitarbeiter in der AG O

Seit Anfang Oktober verstärkt Herr **Philipp Kreis** die Netzwerkgruppe innerhalb der Arbeitsgruppe „Basisdienste und Organisation“ (AG O).



Herr Kreis ist von der Universität Göttingen angestellt und zur GWDG abgeordnet worden. Sein Aufgabengebiet liegt demzufolge hauptsächlich in der Betreuung des gesamten Göttinger Datenübertragungsnetzes GÖNET.

Herr Kreis ist in Duderstadt zur Schule gegangen und hat bei der SerNet Service Network GmbH in Göttingen seine Berufsausbildung zum Fachinformatiker Fachrichtung Systemintegration in diesem Jahr erfolgreich abgeschlossen. Während seiner Ausbildung hat Herr Kreis bereits an mehreren Großkundenprojekten im Netzwerkbereich in ganz Deutschland mitgewirkt, sodass er seine fundierten Erfahrungen auch bei der GWDG erfolgreich einsetzen kann.

Herr Kreis ist telefonisch unter der Nummer 0551 39-172356 und per E-Mail unter *pkreis@gwdg.de* erreichbar.

Grieger

Acht neue Mitarbeiter

Seit dem 1. Oktober 2011 sind acht neue Mitarbeiter bei der GWDG tätig. Sie sind zusammen mit dem neuen Geschäftsführer Prof. Yahyapour von der TU Dortmund nach Göttingen gewechselt.

Herr **Peter Chronz** hat Elektrotechnik an der TU Dortmund und an der University of Leeds studiert. Von 2009 bis 2011 war er wissenschaftlicher Angestellter am Lehrstuhl für Service Computing an der TU Dortmund.

Seine Aufgaben lagen in der Forschung und Entwicklung im Bereich Service Level Management für das EU-Projekt SLA@SOI, wo er zuletzt auch mit der Leitung eines Arbeitspakets betraut war. Weiterhin studiert Herr Chronz Informatik als Zweitstudium und forscht an der Automatisierung von IT-Diensten mit dem Ziel einer Promotion. Bei der GWDG wird Herr Chronz zudem im Bereich Cloud Computing tätig sein.

Herr Chronz ist telefonisch unter der Nummer 0551 39-20364 und per Mail unter *peter.chronz@gwdg.de* erreichbar.

Herr **Ali Imran Jehangiri** hat an der Bergischen Universität Wuppertal studiert und hält einen Master im Fach Computer Simulation in Science. Der Titel seiner Masterarbeit ist „Performance Analysis of Monitoring Software for User Jobs in a World Wide Distributed Grid“.

Herr Jehangiri, dessen gegenwärtige Forschungstätigkeit vom DAAD und dem pakistanischen Bildungsministerium gefördert wird, beschäftigt sich mit dem Monitoring von Service Level Agreements in virtualisierten Infrastrukturen. Seine Doktorarbeit, welche er am Lehrstuhl für Service Computing der TU Dortmund begonnen hat, wird er im Rahmen an der GWDG fortsetzen.

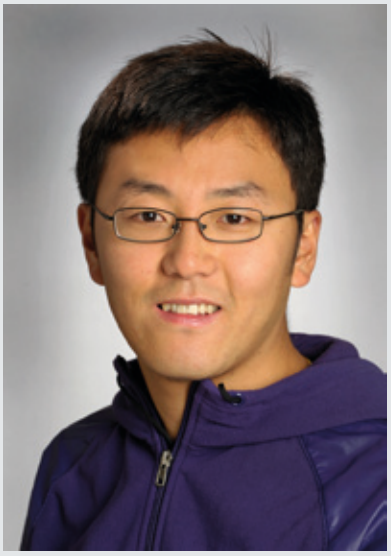
Herr Jehangiri ist telefonisch unter der Nummer 0551 39-20363 und per E-Mail unter *ali.jehangiri@gwdg.de* erreichbar.

Herr **Piotr Kasprzak** hat an der TU Dortmund Kerninformatik studiert und anschließend am IT & Medien Centrum der TU Dortmund an verschiedenen Projekten in den Bereichen Enterprise Application Integration, Portalentwicklung und Business Process Management mitgewirkt. Zuletzt kümmerte er sich um die Administration der Grid-Ressourcen sowie die Entwicklung von Konzepten zur effizienten Nutzung von Storage im Kontext von Virtualisierung.

Bei der GWDG wird Herr Kasprzak in den Themenfeldern Cloud- und Grid-Computing tätig sein, wo er auch eine Promotion anstrebt.

Herr Kasprzak ist telefonisch unter der Nummer 0551 201-1579 und per E-Mail unter *piotr.kasprzak@gwdg.de* erreichbar.

Herr **Kuan Lu** hält einen Master der Universität Duisburg-Essen im Fach Computer Engineering. Er arbeitete am Lehrstuhl für Service Computing der TU Dortmund für das EU-Projekt SLA@SOI und erforschte dort den Einsatz formal spezifizierter Service Level Agreements für dienstorientierte Infrastrukturen.



Herr Lu arbeitet gegenwärtig in den Bereichen Service- und Cloud-Computing sowie der Planung und Optimierung automatisierter Verhandlungen von Service Level Agreements. Bei der GWDG wird Herr Lu in Projekten tätig sein und seine Promotion vorantreiben.

Herr Lu ist telefonisch unter der Nummer 0551 39-20370 und per E-Mail unter *kuan.lu@gwdg.de* erreichbar.

Herr **Christof Pohl** war vor seinem Wechsel an die GWDG am IT & Medien Centrum der TU Dortmund als kommissarischer Leiter und Projektkoordinator der Abteilung Anwendungsentwicklung tätig. Zuletzt wurden dort verschiedene Projekte aus den Bereichen Identity Management, SmartCards, integriertes Informationsmanagement, BPM/Prozessautomatisierung sowie Online-Dienste-Portale durchgeführt. Bei der GWDG wird Herr Pohl zunächst an dem Aufbau eines zentralen Online-Dienste-Portals und der Bereitstellung einer föderierten AAI für die Max-Planck-Institute mitwirken.

Herr Pohl ist telefonisch unter der Nummer 0551 201-1878 und per E-Mail unter *christof.pohl@gwdg.de* erreichbar.

Herr **Dr. Thomas Röblitz** hat an der Humboldt-Universität zu Berlin (HUB) Informatik und Geographie studiert. Nach seinem Studium arbeitete er am Zuse-Institut Berlin in mehreren Forschungsprojekten mit dem Schwerpunkt Ressourcen-Management im Grid und promovierte 2008 mit dem Thema „Co-Reservation of Resources in the Grid“ an der HUB.

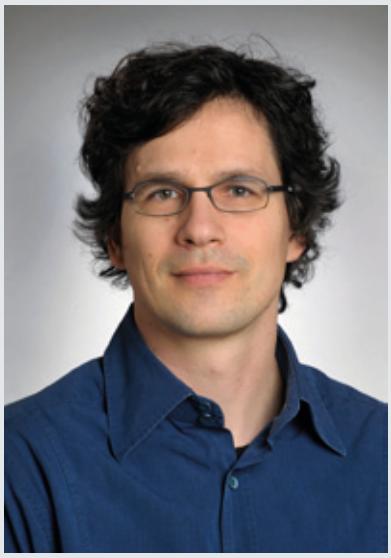
Im Juni 2009 wechselte er an die TU Dortmund und begann dort mit seiner Habilitation. Sein aktuelles Forschungsgebiet, in dem er auch bei der GWDG aktiv sein wird, sind verteilte Infrastrukturen für das Verwalten von wissenschaftlichen Daten und

deren Analyse sowie das Ressourcen-Management in Cloud-Umgebungen.

Herr Dr. Röblitz ist telefonisch unter der Nummer 0551 39-20366 und per Mail unter *thomas.roeblitz@gwdg.de* zu erreichen.

Herr **Philipp Wieder** hat sich nach seinem Studium der Elektrotechnik an der RWTH Aachen mit den Themenbereichen massivparallele Systeme, verteilte Systeme, Service Level Management und Scheduling, insbesondere im Rahmen von EU Projekten, befasst.

Nach mehreren Jahren Tätigkeit am Forschungszentrum Jülich und der TU Dortmund wird Herr Wieder an der GWDG seine Erfahrungen in diesen Bereichen einbringen und die Koordination von e-Science-Projekten unterstützen.



Herr Wieder ist telefonisch unter der Nummer 0551 201-1576 und per E-Mail unter *philipp.wieder@gwdg.de* erreichbar.

Herr **Edwin Yaqub** hält einen Master der RWTH Aachen im Fach Computer Science. Er arbeitete am Lehrstuhl für Service Computing der TU Dortmund für das EU-Projekt SLA@SOI im Bereich automatisierte Verhandlungen von Service Level Agreements.

Sein gegenwärtiger Themenschwerpunkt liegt bei der Erarbeitung von effizienten Methoden zur Verhandlung komplexer Dienststrukturen für verteilte Infrastrukturen. Herr Yaqub wird in diesem Bereich in Projekten an der GWDG tätig sein und an seiner Promotion weiterarbeiten.

Herr Yaqub ist telefonisch unter der Nummer 0551 39-20365 und per Mail unter *edwin.yaqub@gwdg.de* erreichbar.

Wieder

Sicherheit und Vertraulichkeit: Authentifizierung und Verschlüsselung im Internet

Damit in einem System vernetzter Rechner und im Internet Informationen wie Passwörter, Dokumente und elektronische Poste sicher und vertraulich übertragen werden können, werden Verfahren der Kryptologie eingesetzt. In zwei Artikeln der GWDG-Nachrichten soll dem Leser das Thema Verschlüsselung vertraut gemacht werden. Nachdem in der letzten Ausgabe der GWDG-Nachrichten eine allgemeine Einführung in Verschlüsselungstechniken gegeben wurde, soll nun der vorliegende Artikel eine praktische Anleitung zur Nutzung von Zertifikaten für eine digitale Signatur und zur Verschlüsselung von E-Mails geben. Für weitergehende Informationen sei auf die Beschreibungen auf den entsprechenden Webseiten der GWDG verwiesen.

Zertifikate

Das Versenden von Nachrichten in elektronischer Form (E-Mail) über das prinzipiell nicht vertrauenswürdige, unsichere Übertragungsmedium „Internet" bietet Eindringlingen Möglichkeiten, vertrauliche Daten zu lesen, zu verfälschen oder sich als jemand anderes auszugeben. Durch Anwendung kryptografischer Methoden kann jedoch für Datenschutz und Datenintegrität gesorgt werden. Mit Hilfe von digitalen Signaturen und Zertifikaten können die Herkunft und die Unverfälschtheit von Nachrichten geprüft und sichergestellt werden. Bei der heute üblichen Anwendung asymmetrischer Verschlüsselungsverfahren können die Verschlüsselungsalgorithmen, die Schlüsselgrößen und die Dateiformate öffentlich gemacht werden, während der Kryptografieschlüssel geheim und unter Verschluss gehalten wird – von demjenigen, der das Schlüsselpaar (öffentlicher und privater Schlüssel) für sich erzeugt hat.

Das im vorigen Artikel (s. GWDG-Nachrichten 9/2011) beschriebene asymmetrische Verschlüsselungsverfahren RSA, das 1978 von den Mathematikern Ronald L. Riverst, Adi Shamir und Leonard Adleman entwickelt wurde, ist inzwischen für vielerlei Dienste üblich und selbstverständlich geworden. Es wird nicht nur in der Verschlüsselung von Texten, die per E-Mail versendet werden, genutzt, sondern auch, um sich gegenüber anderen im Internet auszuweisen, wenn man z. B. einen Kaufvertrag abschließt, indem man die auf diesem Verschlüsselungsverfahren basierende elektronische Unterschrift nutzt. Ebenfalls nutzt man dieses Verschlüsselungsverfahren zur Sicherstellung, dass ein Anbieter, dessen Internet-Seite man aufruft, tatsächlich der gewünschte Dienst ist oder dass ein Server, an dem man sich anmeldet, um darauf zu arbeiten oder um Daten zu übertragen, tatsächlich der richtige ist. In all diesen Fällen wird die Sicherheit durch die Speicherung bzw. den Austausch von Zertifikaten gewährleistet.

Die meisten E-Mail Programme bieten inzwischen die Möglichkeit der digitalen Signatur, mit der die Identität des Autors/Versenders sichergestellt wird und eventuelle Veränderungen des Mail-Inhalts während der Übertragung zum Empfänger aufgedeckt werden können. Zudem ist es möglich, den ganzen Brieftext zu verschlüsseln, womit eine dritte Person daran gehindert wird, den Text zu lesen.

Frau Weiß und Herr Schwarz aus dem vorangegangenen Artikel müssen sich nicht mehr selbst Schlüsselzahlen erzeugen und sich darum kümmern, dass sie ihren Korrespondenzpartnern einen öffentlichen Schüssel zusenden. Auch für die sichere Verwahrung der privaten Schlüssel ist gesorgt.

Diese Möglichkeiten beruhen auf dem RSA-Verfahren. Das Verschlüsselungsverfahren ist in das E-Mail-Programm eingebaut und die drei Schlüsselzahlen N, D und E erhält man in Form eines Zertifikats bei einer Zertifizierungsstelle (einer sog. CA = Certification Authority). Um Verschlüsselungen und eine digitale Signatur durchführen zu können, muss man zunächst bei einer Zertifizierungsstelle ein Zertifikat (eine digitale ID) beantragen und in das eigene E-Mail-Programm einfügen. Die digitale ID enthält einen privaten Schlüssel, der auf dem Computer des Absenders gespeichert bleibt, und ein Zertifikat (mit einem öffentlichen Schlüssel). Dieses „Public-Key"-Zertifikat wird zusammen mit digital signierten Nachrichten versendet. Die Empfänger speichern das Zertifikat und können den öffentlichen Schlüssel zum Verifizieren empfangener E-Mails und auch zum Verschlüsseln von Nachrichten an den Absender verwenden.

Zertifikate können neben der Verschlüsselung von E-Mails oder für die Überprüfung einer digital signierten E-Mail auch für andere Zwecke als Beweis der Identität verwendet werden. Authentizität und Integrität werden durch kryptografische Verfahren geprüft. Ein Zertifikat ist im elektronischen Datenverkehr der Nachweis, dass der öffentliche Schlüssel eines asymmetrischen Verschlüsselungsverfahrens zu der vorgeblichen Person oder Institution gehört, weil es von einer staatlich überwachten Behörde ausgestellt und verwaltet wird. Es ist vergleichbar mit einem Personalausweis. Das Wort „Zertifikat" wurde aus den lateinischen Wörtern certus = sicher und facere = machen gebildet.

Die Generierung eines Schlüsselpaares ist jedem Anwender mit Hilfe eines Internet-Browsers möglich. Dieses wird mit einem Zertifikat verbunden, wenn der ganze Vorgang in Zusammenarbeit mit einer Zertifizierungsstelle abläuft.

Ein Zertifikat ist also mehr als die drei Schlüsselzahlen, die wir aus dem RSA-Verfahren (s. den Artikel in den GWDG-Nachrichten 9/2011) kennen. Es beinhaltet Angaben zur Identität des Zertifikatsinhabers, auch die Benennung der Stelle, die das Zertifikat ausgestellt hat, und wiederum deren Zertifikat (Zertifikatkette). Weiterhin besitzt das Zertifikat eine Gültigkeitsdaue. Es enthält die öffentlichen Schlüssel N und E und gibt Auskunft über die Verschlüsselungsverfahren, mit denen es verwendet werden will.

Zum Zertifikat gehört auch der private Schlüssel des Zertifikatinhabers, der allerdings im „Public-Key"-Zertifikat nicht enthalten ist. Er wird passwortgeschützt auf dem Rechner des Zertifikatinhabers verwahrt.

In den meisten Ländern existiert eine „Public Key Infrastructure" (PKI), in der hierarchisch geordnet vertrauenswürdige Institutionen die Zertifikate vergeben und verwalten. In Deutschland hat die Bundesnetzagentur (http://www.bundesnetzagentur.de) die oberste Aufsicht über diese Hierarchie von Zertifizierungsstellen. In einer PKI gibt es eine baumförmig angelegte Hierarchie von Verwaltungsstellen, die sich gegenseitig vertrauen und für die Vergabe und Aufbewahrung der Zertifikate zuständig sind. Für die wissenschaftlichen und Forschungseinrichtungen in Deutschland ist der DFN-Verein (DFN = Deutsches Forschungsnetz), der das deutsche Forschungsnetz betreibt, aktiv geworden (seit dem Jahr 2006) und betreut unter sich eine große Anzahl von Zertifizierungsstellen. Die Zertifizierungsstelle des DFN-Vereins selbst wurde von der Deutschen Telekom zertifiziert; diese nimmt die Spitze der Hierarchie ein und wird von der Bundesnetzagentur überwacht.

In dem nachfolgend besprochenen Beispiel steht an oberster Stelle das „Deutsche Telekom Trust Center" mit der Bezeichnung „Deutsche Telekom Root CA 2", in der Ebene darunter der „DFN-Verein" mit der Bezeichnung „DFN-Verein PCA Global - G01" und als unterste Instanz die „Gesellschaft für wissenschaftliche Datenverarbeitung" mit der Bezeichnung „GWDG-CA". Unter der GWDG gibt es weitere Stellen, sogenannte Registrierungsstellen (RA = Registration Authority), die Zertifikatanträge entgegennehmen können, aber nicht selbst Zertifikate ausstellen dürfen: so der gemeinsame Bibliotheksverbund (GBV RA) und das Deutsche Primatenzentrum (DPZ). Die Max-Planck-Institute und die Universität Göttingen verfügen über eigene Zertifizierungsstellen MPG-CA und Uni-Goettingen-CA).

Mit diesen drei Institutionen ergibt sich eine Zertifikatkette, die auch in jedem Zertifikat aufgeführt ist, damit man erkennen kann, welche Institutionen die Echtheit des Zertifikats garantieren.

Das Zertifikat der obersten Instanz, für die GWDG, das Zertifikat der Telekom, das „Deutsche Telekom Root CA2", bezeichnet man als Wurzel-Zertifikat (Root-Certificate). Für die sichere Verbindung mit Servern im Internet braucht man dieses Zertifikat normalerweise nicht mehr selbst installieren (in den Webbrowser importieren), denn es ist in den Servern der meisten Institutionen, die „zertifiziert" sind, vorhanden, und es ist auf den Anwenderrechnern in vielen Anwendungen und Betriebssystemen bereits integriert.

Verwendungszweck des Zertifikats

- Public-Key-Zertifikate werden verwendet zur digitalen Signatur, mit der die Identität des Autors/Versenders einer E-Mail sichergestellt wird und eventuelle Veränderungen des Mail-Inhalts aufgedeckt werden können (Protokoll S/MIME = Secure Multipurpose Internet Mail Extensions),

- zur Verschlüsselung des gesamten Brieftextes, womit einer dritten Person unmöglich gemacht wird, den Text zu lesen (Protokoll S/MIME),

- zur sicheren Kommunikation mit Webseiten über HTTPS (= HyperText Transfer Protocol Secure) und SSL/TLS (Verschlüsselungsprotokoll-Implementierung: SSL = Secure Sockets Layer; TLS = Transport Layer Security),
- zur Sicherheit in Netzwerkprotokollen zur Datenübertragung (z. B. IPsec, SSL, SSH (= Secure Shell)),
- zur Sicherheit in Virtual Private Networks (VPN) über IPsec,
- um Programmcode zu signieren, damit er vom Betriebssystem ohne Warnung installiert wird, und
- zur Authentisierung bei Chipkarten.

Inhalt des Zertifikats

Ein Public-Key-Zertifikat enthält folgende Informationen:

- den Anwendungszweck des Zertifikats,
- den Namen des Eigentümers des Zertifikats (engl. subject),
- die Bezeichnung des Ausstellers des Zertifikats (engl. issuer),
- die Gültigkeitsdauer des Zertifikats,
- eine Versionsbezeichnung,
- die Seriennummer,
- Informationen zu den Regeln und Verfahren, unter denen das Zertifikat ausgegeben wurde,
- den öffentlichen Schlüssel,
- die E-Mail-Adresse des Eigentümers des Zertifikats,
- den Fingerabdruck (Fingerprint) und den Fingerabdruckalgorithmus,
- Angaben zum zulässigen Anwendungs- und Geltungsbereich des öffentlichen Schlüssels und
- das Zertifikat des Ausstellers und der in der Zertifizierungskette darüber angeordneten Stellen mit allen Detailinformationen.

Standards von Zertifikaten

Das Zertifikat wird auch als „digitale ID" oder kurz als S/MIME-ID bezeichnet. Die Spezifikation „S/MIME" für digitale Zertifikate verwendet das aktuelle Zertifikatformat – Standard der internationalen Fernmeldeunion – X.509v3 (Version 3) sowie unterschiedliche Verschlüsselungsalgorithmen wie RSA für die asynchrone Verschlüsselung, 3DES (= Triple Data Encryption Standard) für die symmetrische Verschlüsselung und SHA1 für die Erstellung des Fingerabdrucks (Hash-Wert).

Anbieter von Zertifikaten

Will man kryptografische Verfahren zur Absicherung der E-Mail-Verkehrs verwenden, muss man sich zunächst bei einer Zertifizierungsstelle ein Zertifikat besorgen. Dies ist normalerweise kostenpflichtig.

In Deutschland akkreditierte Anbieter von qualifizierten Zertifikaten gemäß deutschem Signaturgesetz sind z. B.

- AuthentiDate International AG,
- verschiedene Bundesnotarkammern,
- DGN Service GmbH,
- D-TRUST (Bundesdruckerei-Gruppe),
- DATEV,
- Deutsche Post AG,
- medisign GmbH,
- S-TRUST (Deutscher Sparkassenverlag),
- TC TrustCenter und
- T-Systems.

Beantragung eines Zertifikats

Ein Zertifikat beantragt man normalerweise auf elektronischem Weg, also auf der Webseite oder per E-Mail bei der nächstgelegenen unteren Verwaltungsstelle, der Registrierungsstelle (RA). Diese überprüft die

Identität und übermittelt die notwendigen Daten an eine Zertifizierungsstelle (CA), die die technischen Systeme betreibt, das Zertifikat erzeugt und es dem Antragssteller entweder direkt oder über die Registrierungsstelle zukommen lässt.

In der Zertifizierungsstelle gibt es Mitarbeiter mit speziellem technischen Know-how, spezielle Rechnersysteme und einen gesicherten Raum und speziell gesicherte Rechner ohne Netzzugang. Die hier erzeugten Zertifikate sind dort sicher vor missbräuchlichem Zugriff.

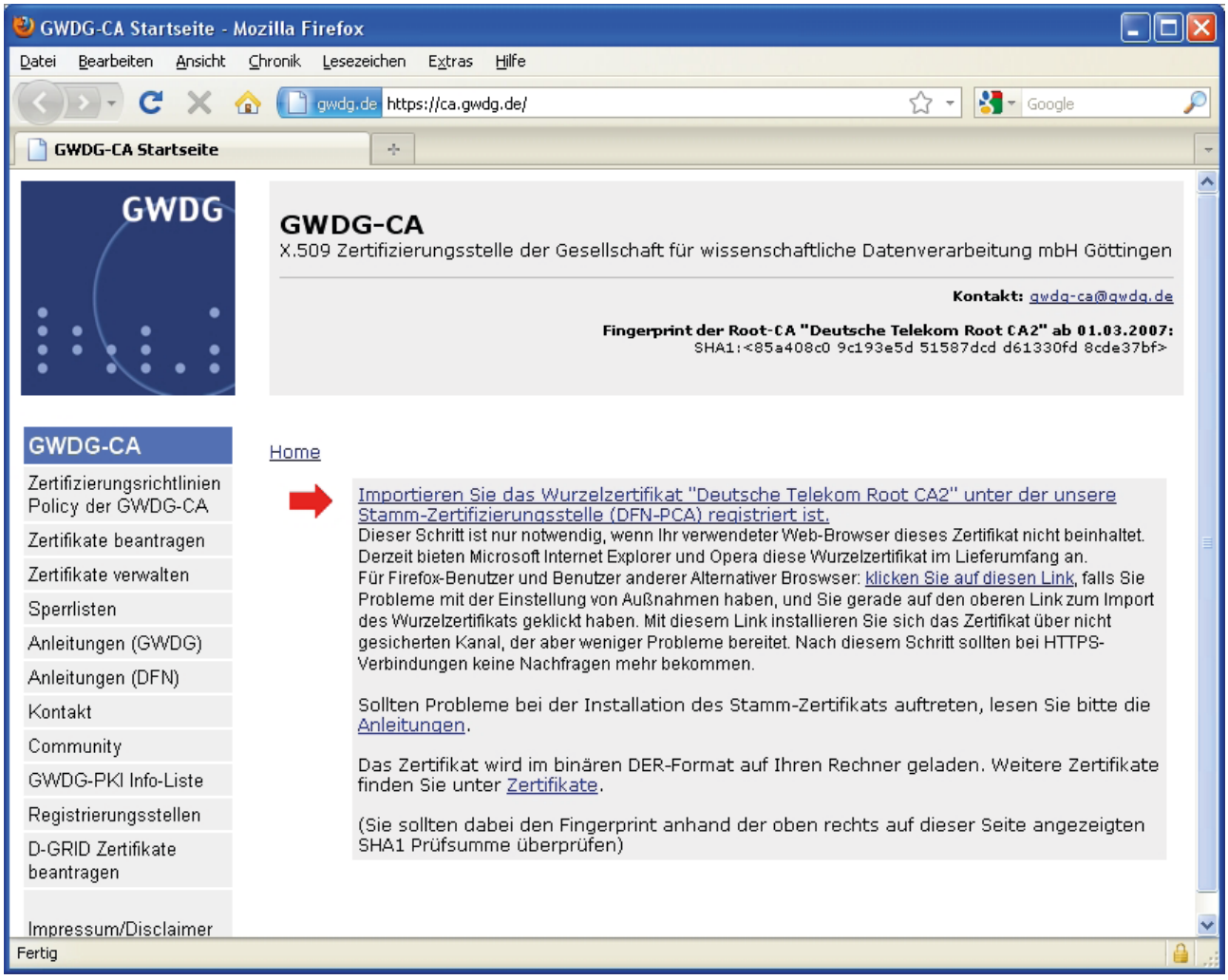
Man unterscheidet persönliche Zertifikate (Nutzerzertifikate) und Serverzertifikate:

- Bei Nutzerzertifikaten werden die Schlüsselpaare (öffentlicher und privater Schlüssel) im Browser (z. B. MS Internet Explorer oder Mozilla Firefox) erzeugt. Nutzerzertifikate sind drei Jahre gültig und können dann erneuert werden.
- Serverzertifikate werden z. B. auf Internet-Servern oder Terminal-Servern installiert. Sie laufen nach fünf Jahren ab und können dann erneuert werden.

Moderne E-Mail-Programme bieten heutzutage die Möglichkeit, E-Mails digital zu signieren und zu verschlüsseln. Dazu ist es notwendig, dass man im Besitz eines persönlichen Zertifikats ist. Um eines zu erhalten, kann man im Internet-Browser eine Stelle wählen, die Zertifikate vergibt. Im folgenden Beispiel wird dies im Umfeld des Rechenzentrums der Universität Göttingen durchgespielt. Während Zertifikate generell kostenpflichtig sind, können Mitarbeiter der wissenschaftlichen Einrichtungen Göttingens kostenlos ein Zertifikat bei den entsprechenden Zertifizierungsstellen GWDG-CA, MPG-CA oder Uni-Goettingen-CA erhalten.

Beantragung des Zertifikats bei der GWDG-CA

Man begibt sich zunächst an seinen Computer, startet den Internet-Browser seiner Wahl und wählt die



1 *Startseite der Zertifizierungsstelle der GWDG im WWW*

2 *Homepage der Zertifizierungsstelle „GWDG-CA“*

Webseite (URL) einer Zertifizierungsstelle (CA) oder Registrierungsstelle (RA). Im Falle der GWDG ist dies *https://ca.gwdg.de* (Abb. 1).

Die folgenden Schritte bis zum Erhalt des Zertifikats müssen auf demselben Rechner mit wiederum demselben Internet-Browser durchgeführt werden. Im Beispiel geschieht dies mit dem „Mozilla Firefox“.

Auf der Startseite der GWDG-CA kann man sich im Menü am linken Rand über alle Aspekte der Zertifizierung informieren. Nachdem man sich dort kundig gemacht hat, beginnt man die Beantragung des Zertifikats mit dem Menüpunkt „Zertifikate beantragen“. Man gelangt auf die entsprechende Webseite (Abb. 2).

Die Seite enthält zwei Angebote (blaue Schrift mit Unterstreichung). Die (obere) Möglichkeit der Beantragung per Web-Browser wird gewählt, da ein persönliches Zertifikat (Benutzerzertifikat) gewünscht wird.

Das System legt einem nun ein Antragsformular vor (Abb. 3). Notwendige Einträge sind die E-Mail-Adresse, Vor- und Nachnamen und eine PIN (= Persönliche Identifikationsnummer). Natürlich muss man der Zertifizierungsrichtlinie zustimmen; die Veröffentlichung des Zertifikats – also des öffentlichen Schlüssels – ist sinnvoll.

3 *Formular zur Beantragung eines Zertifikats*

Von: gwdg-ca@gwdg.de Gesendet: Do 23.06.2011 12:01
An: Eyssell, Manfred
Cc: gwdg-ca@gwdg.de
Betreff: GWDG CA Zertifikatinformation
Anlagen: cert-304254067.pem (2 KB)

Sehr geehrte Nutzerin, sehr geehrter Nutzer,

die Bearbeitung Ihres Zertifizierungsantrags ist nun abgeschlossen.

Ihr Zertifikat mit der Seriennummer 304254067 ist auf den Namen CN=Manfred Eyssell,O=Gesellschaft fuer wissenschaftliche Datenverarbeitung,C=DE erstellt worden und im Anhang dieser Mail beigelegt.

Sie benötigen die Seriennummer, um Ihr Zertifikat gegebenenfalls sperren zu können.

Um Ihr Zertifikat nutzen zu können, müssen Sie alle folgenden Zertifikate in Ihren Browser importieren. Achten Sie darauf, dass Sie die Zertifikate auf dem Rechner importieren, von dem aus Sie den Antrag gestellt haben, weil sich dort der zugehörige Schlüssel befindet.

1. Für die CA-Zertifikate wählen Sie bitte die Seite

https://pki.pca.dfn.de:443/gwdg-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2

und folgen den Anweisungen.

2. Ihr eigenes Zertifikat erhalten Sie direkt über folgenden Link:

https://pki.pca.dfn.de:443/gwdg-ca/cgi-bin/pub/pki?cmd=getcert&key=304254067&type=CERTIFICATE

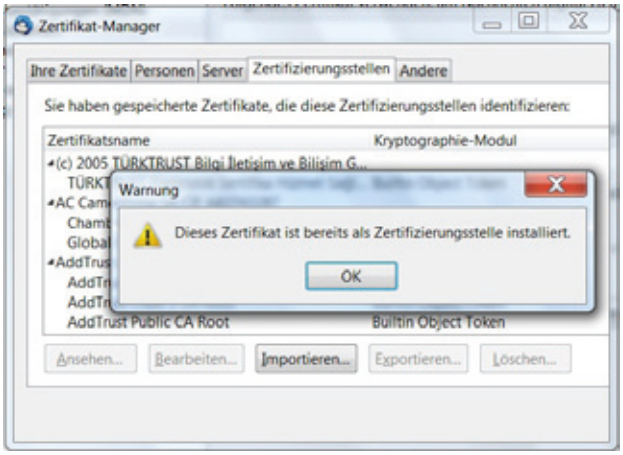
Mit freundlichen Grüßen

Ihr PKI-Team der Gesellschaft fuer wissenschaftliche Datenverarbeitung

4 *Bestätigungsnachricht der Zertifizierungsstelle*

Wenn das Formular ausgefüllt und die Taste „Weiter" betätigt ist, erfolgt zur Kontrolle eine Zusammenfassung der eingegebenen Daten. Werden diese bestätigt, erzeugt der Web-Browser das persönliche Zertifikat mit privatem und öffentlichem Schlüssel. Das System speichert es am eigenen Computer versteckt ab. Anschließend wird ein Antragsformular im PDF-Format angezeigt, das man sich ausdrucken muss.

In dieses Formular trägt man seine persönlichen Daten einschließlich seiner Personalausweisnummer ein und legt es dem zuständigen Mitarbeiter der Zertifizierungsstelle – einem Mitarbeiter der GWDG in der Information – persönlich vor. Dieser prüft die Angaben und die Identität des Antragstellers. Er nimmt das Formular entgegen, um es an den Mitarbeiter weiterzuleiten, der schließlich dafür sorgt, dass der Antragsteller eine E-Mail mit der Bestätigung der Registrierung des Zertifikats erhält (Abb. 4).

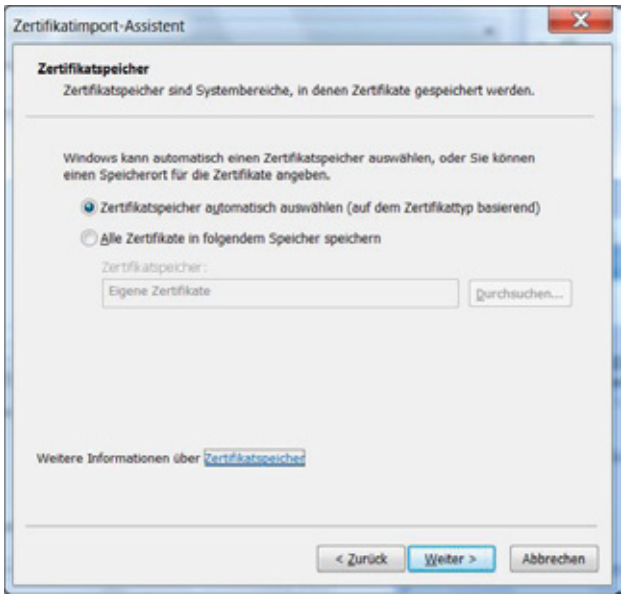


5 *Die Zertifikate der Zertifizierungsstellen sind meist schon vorhanden.*

Auf seinem Rechner richtet man sich nun einen Speicherplatz ein, in den man das Zertifikat aus der Anlage der Benachrichtigungs-E-Mail speichert (hier im Beispiel die Datei mit dem Namen „cert-304254067.pem"). Die Nummer im Dateinamen ist die Seriennummer des Zertifikats. Weiterhin speichert man die

6 *An dieser Stelle wird das persönliche Zertifikat in das eigene System eingefügt.*

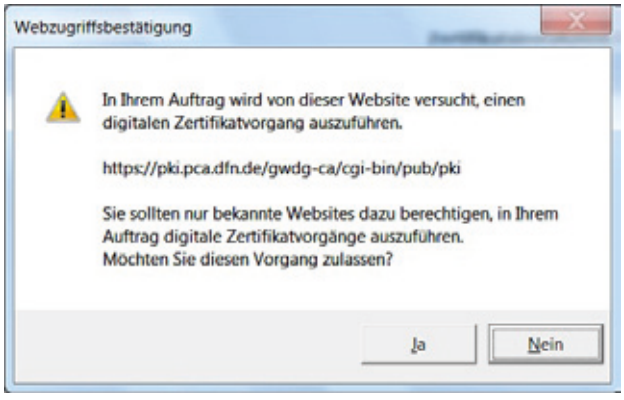
öffentlichen Schlüssel der in der PKI-Kette beteiligten Zertifizierungsstellen auf seinen Rechner. Sie können von der unter „1." genannten Webseite heruntergeladen werden. Meist sind diese auf dem PC bereits vorhanden und man bekommt eine entsprechende Meldung (Abb. 5).



7 *Das System soll seinen Zertifikatspeicher automatisch wählen.*

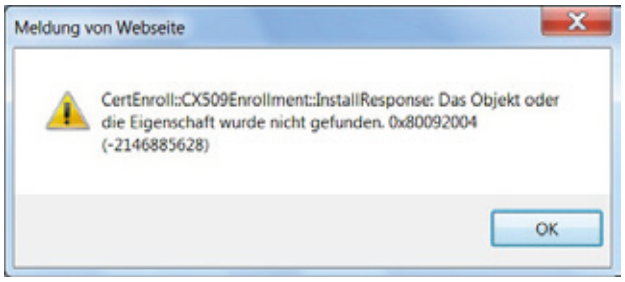
Von der unter „2." genannten Webseite kann man nun das eigene Zertifikat in seinen Web-Browser importieren. Das funktioniert jedoch nur, wenn derselbe Browser auf demselben Rechner zur Beantragung und Erzeugung des Zertifikats verwendet wurde. Es erscheint eine Webseite, auf der man auf der Karteikarte „Zertifikate" die Befehlstaste „Zertifikat importieren" anklickt (Abb. 6).

Man sollte das Zertifikat in den dafür vom System vorgesehenen Bereich abspeichern (Abb. 7).



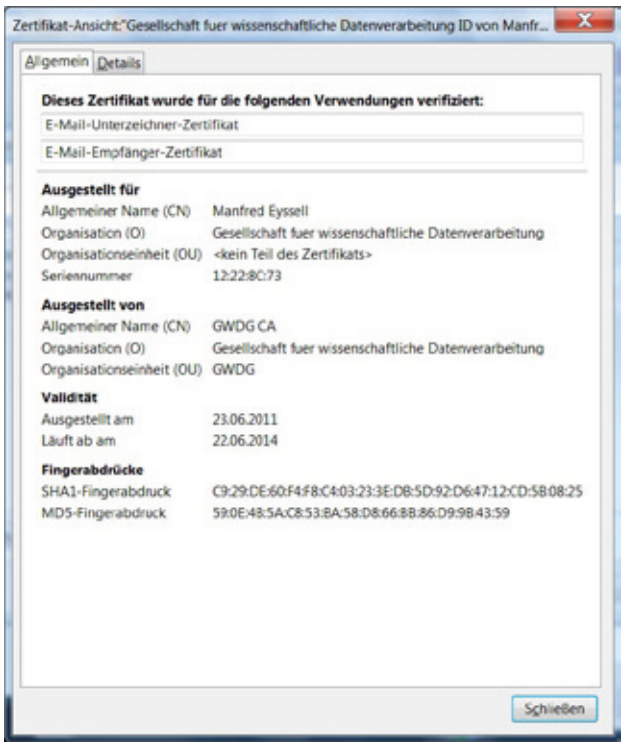
8 *Die Sicherheitsanfrage ist mit „Ja" zu beantworten*

Nochmal der Hinweis: Es ist notwendig, für diesen Vorgang denselben Browser zu verwenden, auf dem man den Antrag gestellt hat. Benutzt man einen anderen Browser als den, mit dem man das Zertifikat beantragt hat, bekommt man eine entsprechende Fehlermeldung (Abb. 9).



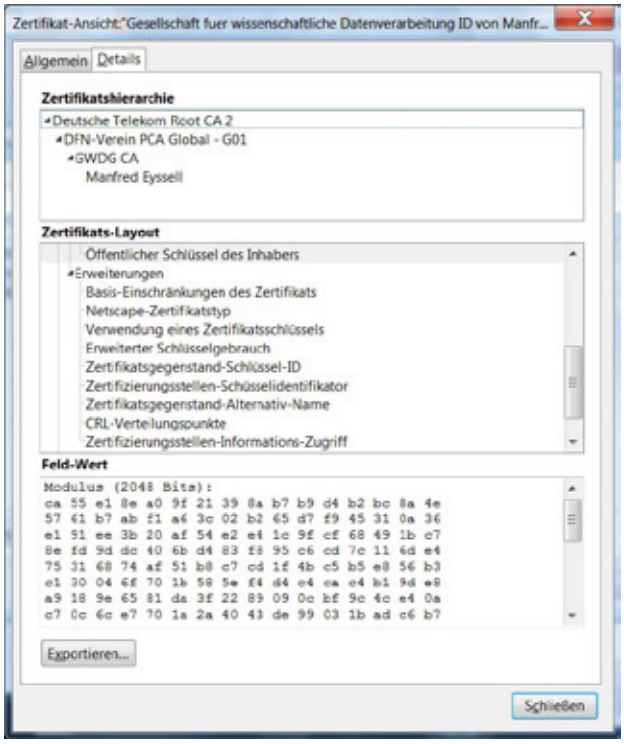
9 *Es wurde nicht wieder derselbe Browser genommen*

Sobald man das Zertifikat importiert hat, kann man es sich ansehen. Auf der ersten Karteikarte sind allgemeine Daten des Zertifikats vermerkt (Abb. 10).



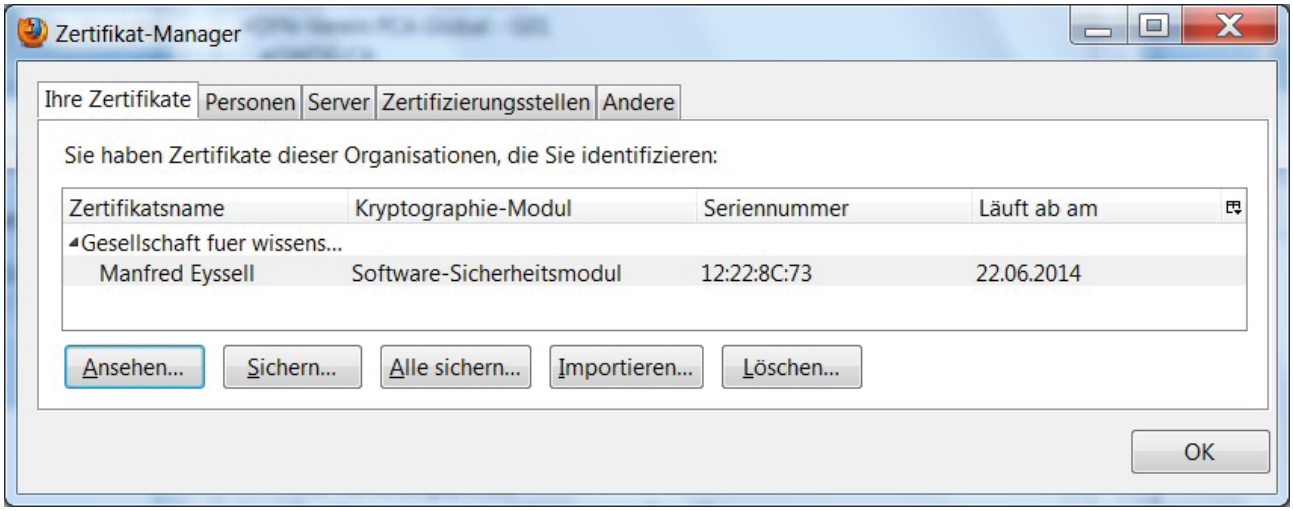
10 *Allgemeine Informationen zum persönlichen Zertifikat*

Auf der zweiten Karteikarte „Details“ (Abb. 11) hat man Zugang zu den Inhalten des Zertifikats. Im Bild ist der Beginn des öffentlichen Schlüssels in hexadezimaler Darstellung zu sehen.

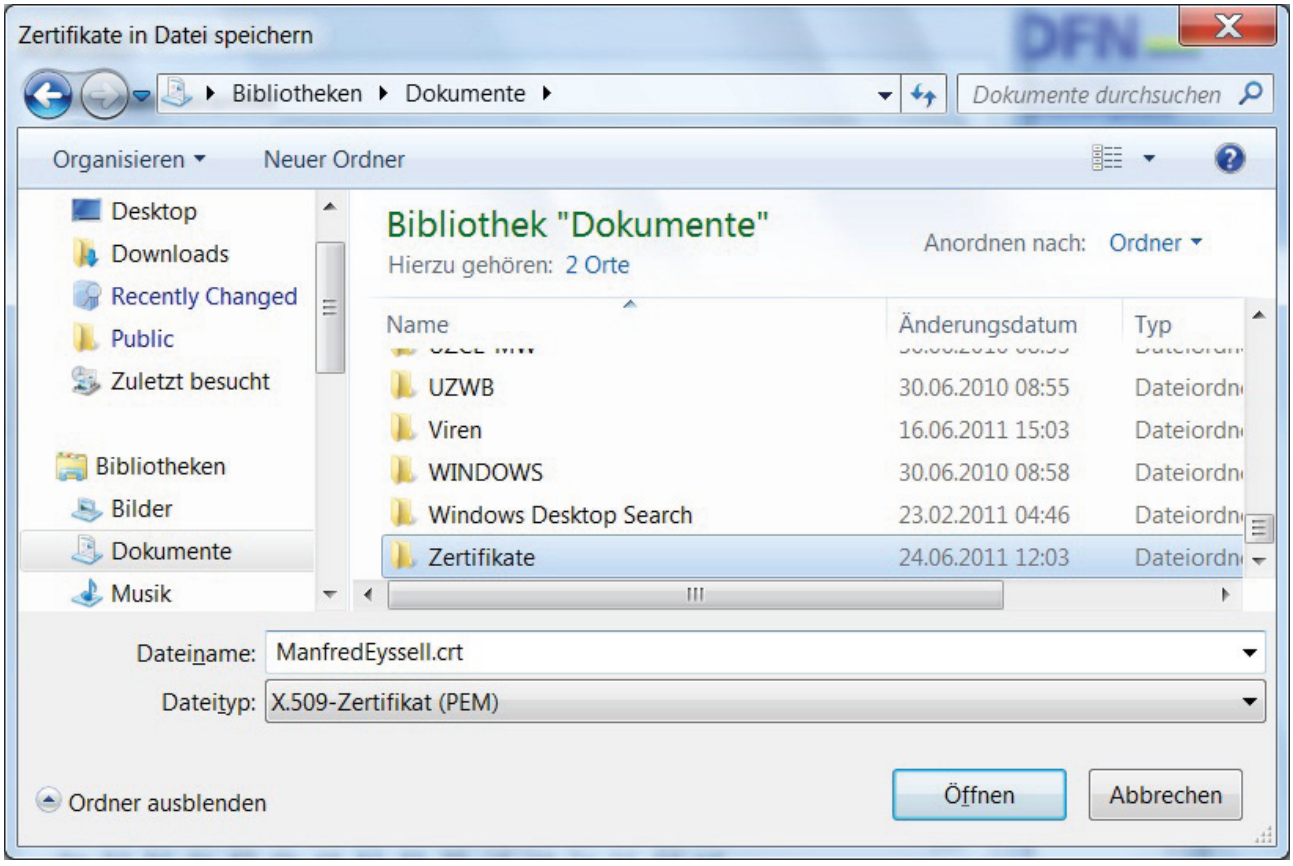


11 *Auf der Karteikarte „Details“ wird zuoberst der Zertifizierungspfad angezeigt, darunter kann man sich den Inhalt des Zertifikats Punkt für Punkt anzeigen lassen.*

Der Zertifikat-Manager des Browsers zeigt an, dass ein Zertifikat abgespeichert ist. Die Seriennummer 304254067 ist hier in hexadezimaler Darstellung angegeben (Abb. 12).



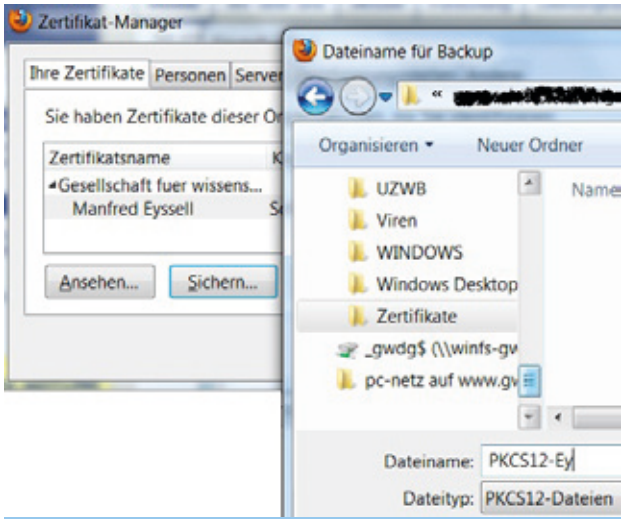
12 *Im Browser „Mozilla Firefox“ ist der Zertifikat-Manager die zentrale Stelle, um Zertifikate zu importieren, anzusehen, zu sichern oder zu löschen.*



13 *Das eigene Zertifikat mit den öffentlichen Schlüsseln speichert man sich in einen Ordner „Zertifikate“.*

Mit dem Befehl „Importieren“ kann man das Zertifikat mit den öffentlichen Schlüsseln (public certificate) in eine Datei speichern. Sie bekommt den Dateityp „.crt“. Als Speicherort richtet man sich einen Ordner „Zertifikate“ ein (Abb. 13).

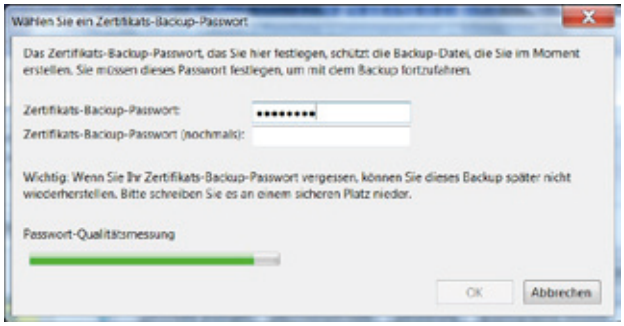
Sichern des privaten Schlüssels



14 *Sichern des geheimen Schlüssels in die Datei „PKCS12-Ey.p12“*

Im Zertifikat-Manager sollte man nun eine Sicherheitskopie des eigenen Zertifikats (mit dem geheimen persönlichen Schlüssel) anlegen. Diese dient auch dazu, das Zertifikat in andere Browser und ins E-Mail-Programm (z. B. Mozilla Thunderbird oder MS Outlook) zu importieren. Auf der Karteikarte, die das persönliche Zertifikat (mit dem geheimen Schlüssel) verwaltet, klickt man auf „Sichern…“ (Abb. 14).

Diese Sicherheitskopie ist die einzige Datei, in der auch der private Schlüssel abgelegt ist. Sie muss mit einem Passwort abgesichert werden (Abb. 15).



15 *Notwendige Absicherung der Datei mit dem privaten Schlüssel durch ein Passwort*

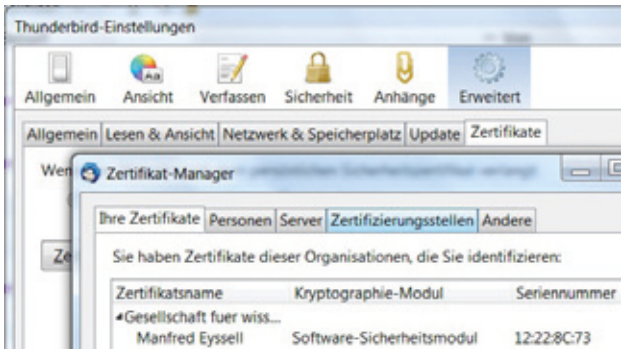
Diese Datei dient auch dazu, den persönlichen Schlüssel in anderen E-Mail-Programmen – auch auf anderen Computern – zu installieren. Dabei ist dann

jeweils auch das eben verwendete Passwort einzugeben.

Einbau des privaten Schlüssels in andere Programme

Zertifikat in Mozilla Thunderbird importieren

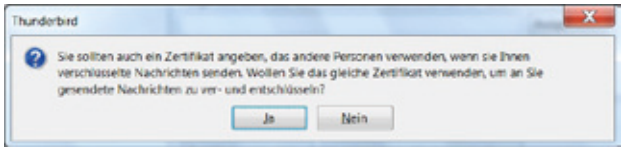
Bei den „Thunderbird-Einstellungen“ geht man im Bereich „Erweitert“ auf die Karteikarte „Zertifikate“. Hier kann man über die Befehlstaste „Importieren...“ seinen geheimen Schlüssel in das E-Mail-Programm einfügen. Im Beispiel ist dies die Datei „PKCS12-Ey.p12“. Es funktioniert natürlich nur, wenn man das zugehörige Passwort kennt (Abb. 16).



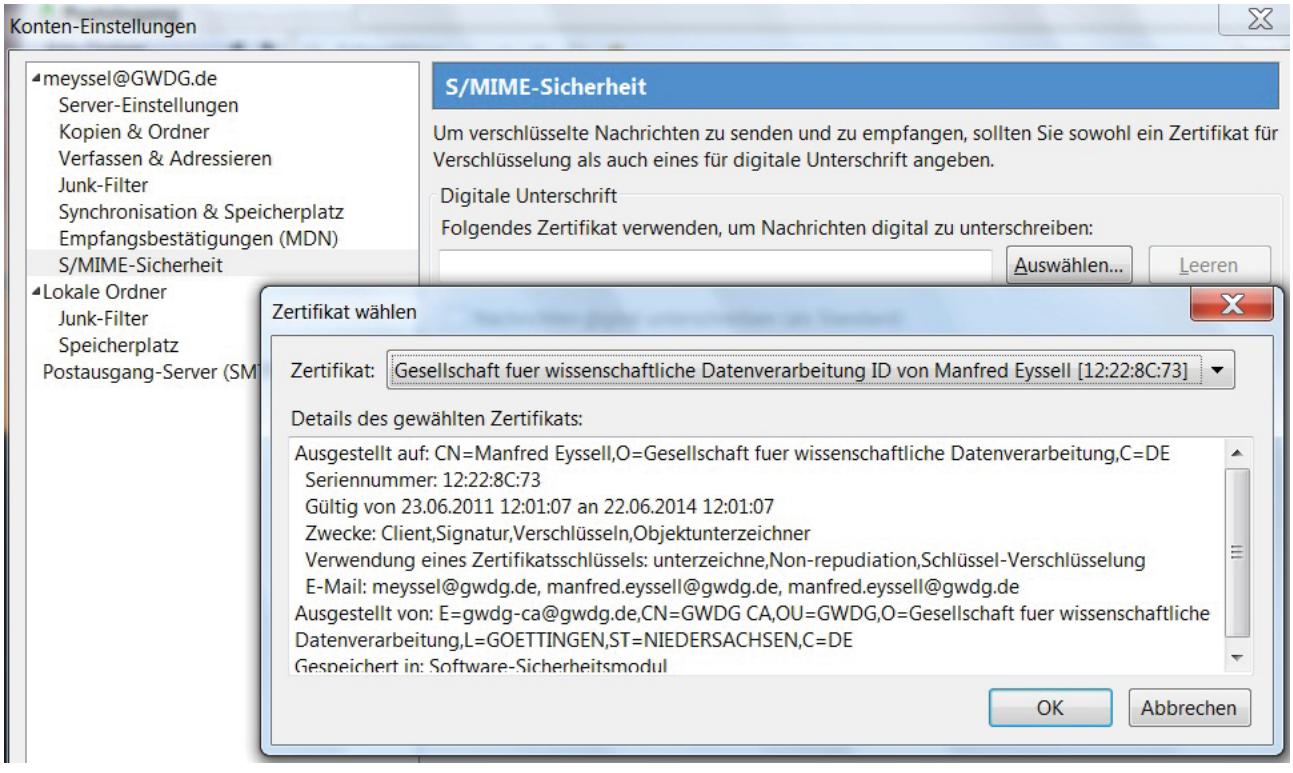
16 *Der persönliche Schlüssel ist in Mozilla Thunderbird integriert.*

Nachdem man diese Datei in Mozilla Thunderbird importiert hat, ist man nun auch in der Lage, mit diesem Programm seine E-Mails zu signieren und zu verschlüsseln. Vorher muss man noch in seinem Thunderbird-Konto eintragen, dass man dieses Zertifikat zum digitalen Signieren und/oder zum Verschlüsseln verwenden will. Dies geschieht in der Abteilung „S/MIME-Sicherheit“ (Abb. 17).

Welches Zertifikat (von eventuell mehreren) in das aktuelle Thunderbird-Konto eingebaut werden soll, bestimmt man im Textfeld unter der Überschrift „Digitale Unterschrift“ (Abb. 17). Man klickt auf die Befehlstaste „Auswählen…“ und kann im Fenster „Zertifikat wählen“ die Auswahl treffen. Im Feld darunter wählt man auf gleiche Weise das fürs Verschlüsseln zu verwendende Zertifikat. Darauf macht allerdings das Programm selbst aufmerksam. Es fragt, ob man das gleiche Zertifikat auch zum Verschlüsseln verwenden will (Abb. 18).

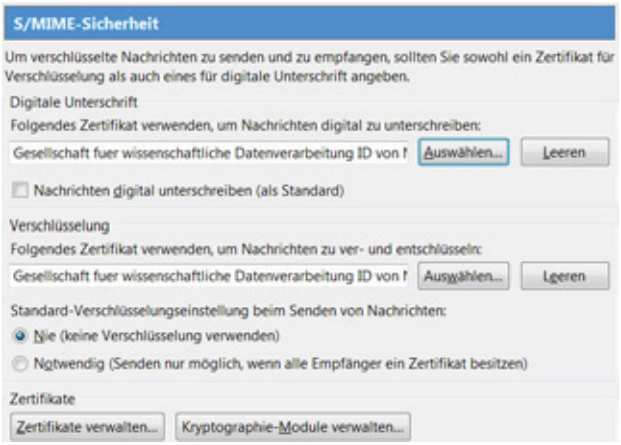


18 *Anfrage, ob für die Verschlüsselung das gleiche Zertifikat verwendet werden soll*



17 *Auswahl des Zertifikats für ein Thunderbird-Konto unter „S/MIME-Sicherheit“*

Antwortet man mit „Ja“, wird auch dies eingetragen – unter der Überschrift „Verschlüsselung“ (Abb. 19).



19 *Sowohl für die digitale Unterschrift als auch für die Verschlüsselung ist ein Zertifikat benannt.*

Unter „Standard-Verschlüsselungseinstellung beim Senden von Nachrichten” kann man den Auswahlpunkt vor „Notwendig“ setzen (Abb. 19). Man entscheidet dann beim Absenden jeder einzelnen E-Mail, ob man sie verschlüsseln will. Das funktioniert allerdings nur dann, wenn man das Zertifikat (die öffentlichen Schlüssel) des Adressaten gespeichert hat.

Verwendung des Zertifikats in MS Outlook

20 *Importieren des persönlichen Schlüssels in Outlook aus der Datei „PKCS12-Ey.p12 (hier im Beispiel)*

Im Outlook-Pull-Down-Menü „Extras“ besteht unter dem Punkt „Optionen“ die Möglichkeit, ein persönliches Zertifikat zu importieren. Im Bereich „Digitale IDs (Zertifikate)“ klickt man auf die Schaltfläche „Importieren/Exportieren…“ und kommt zum Fenster „Digitale ID importieren/exportieren“ (Abb. 20). Man gibt den Dateinamen an, unter dem man das Zertifikat gesichert hat, das zugehörige Passwort und den Namen der digitalen ID (das ist der zusammengeschriebene Vor- und Nachname).

Standardmäßig ist die mittlere Sicherheitsstufe eingestellt (Abb. 21).

21 *Wahl der Sicherheitsstufe in Outlook*

Mit Einstellung der hohen Sicherheitsstufe erreicht man, dass bei jedem Absenden einer digital signierten E-Mail das Kennwort eingegeben werden muss. Um die hohe Sicherheitsstufe einzustellen, ist das Kennwort hier einzugeben (Abb. 22).

22 *Wahl der Sicherheitsstufe in Outlook mit ggf. Kennworteingabe*

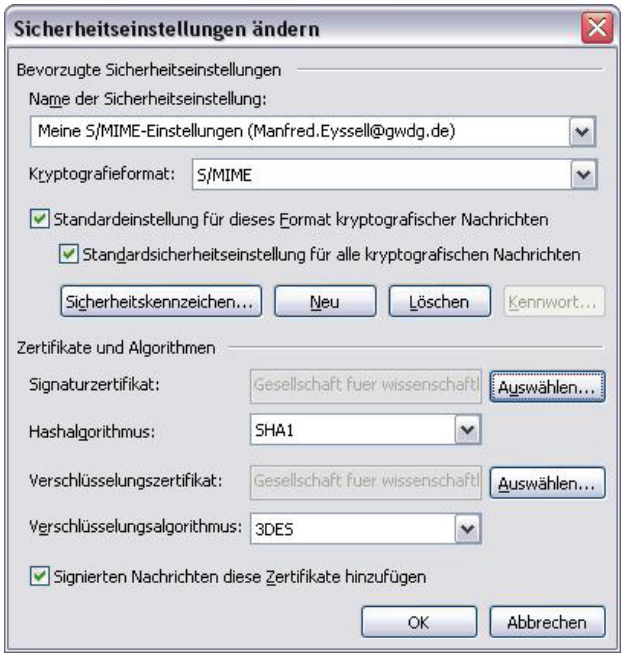
23 *Die Sicherheitsstufe ist auf „hoch" eingestellt.*

In den Outlook-Optionen sollte man nun einstellen, ob man Nachrichten verschlüsseln will und/oder eine digitale Signatur anfügen will.

24 *Auf der Karteikarte „Sicherheit" wird angehakt, ob man digital signieren und/oder verschlüsseln will.*

Von der Karteikarte „Sicherheit" (Abb. 24) kommt man über die Befehlstaste „Einstellungen" zu einem Fenster (Abb. 25), in dem man sieht, dass das Zertifikat geladen ist – genauer wird es angezeigt, wenn man auf die Schaltfläche „Auswählen…" neben dem Feld „Signaturzertifikat:" oder „Verschlüsselungszertifikat:" klickt.

Zurück auf der Karteikarte „Sicherheit" von Optionen (Abb. 24) setzt man nun im oberen Drittel („Verschlüsselte Nachrichten") Häkchen, je nachdem, ob man



25 *Unter „Zertifikate und Algorithmen" kann man bestimmen, welches Zertifikat für Signatur und welches für Verschlüsselung verwendet werden soll. Die Auswahl für den Algorithmus ist bereits passend gewählt.*

- Nachrichten und deren Anlagen verschlüsseln können will,
- Nachrichten digital signieren möchte,
- signierte Nachrichten als Klartext senden und
- eine Bestätigung erhalten möchte, dass die signierte E-Mail gesendet wurde.

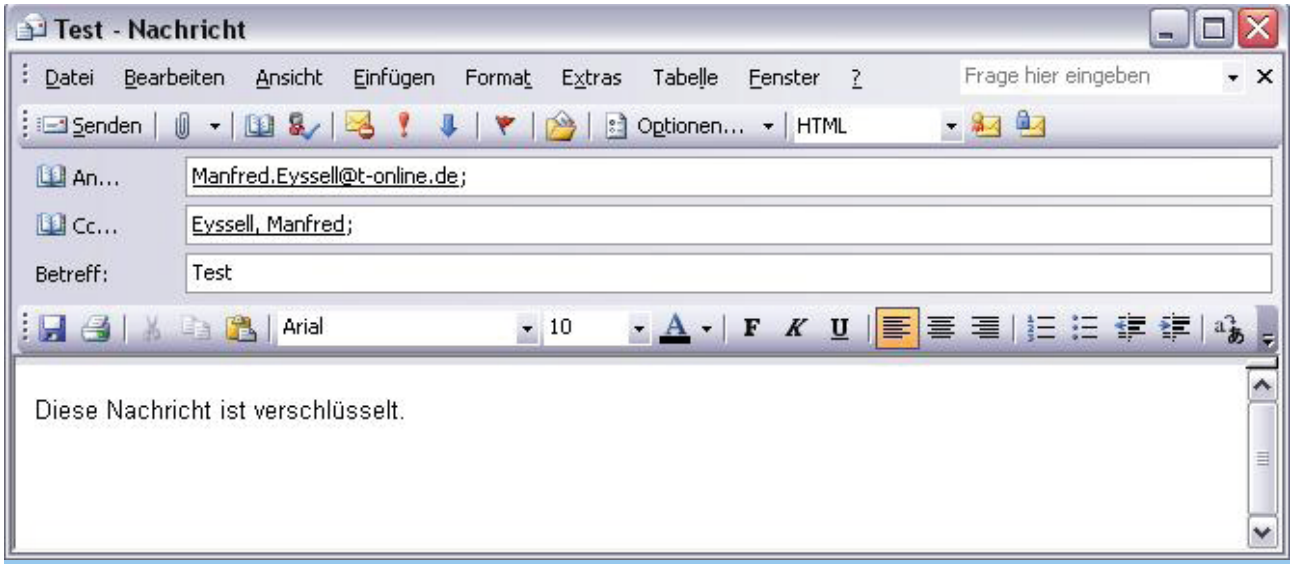
Die ersten drei Punkte sollten angehakt werden.

Beim Erstellen einer zu sendenden Nachricht findet man nun rechts oben in der Symbolleiste die Schaltflächen für das Signieren der Nachricht (gelber Brief mit rotem Personen-Symbol; Abb. 26) und für das Verschlüsseln der Nachricht (gelber Brief mit blauem Schloss; Abb. 27). Die Befehlstaste erscheint nach dem Klicken als markiert, d. h. sie rastet ein.

26 *Die Befehlstaste zur Auswahl von „Nachricht digital signieren" (mit Hilfstext)*

27 *Die Befehlstaste zur Auswahl von „Nachrichten und Anlagen verschlüsseln" (mit Hilfstext)*

Digitales Signieren einer Nachricht



28 *Für diese E-Mail wurde nur die Taste „Digital unterzeichnen" mit dem roten Symbol am gelben Briefumschlag gedrückt.*

Beim digitalen Signieren werden das Zertifikat des Absenders (öffentlicher Schlüssel) und ein mit dem geheimen Schlüssel des Absenders verschlüsselter Hash-Wert (Fingerprint) mitgesendet.

Der öffentlicher Schlüssel ist der Schlüssel, den ein Empfänger vom Absender erhält, so dass der Empfänger die Signatur des Absenders überprüfen und gewiss sein kann, dass die Nachricht nicht von einem Dritten verändert wurde. (Ein Empfänger kann den öffentlichen Schlüssel des Absenders darüber hinaus auch zum Verschlüsseln von E-Mail-Nachrichten an den Absender verwenden.)

Öffnet man in MS Outlook das Fenster zum Erstellen einer E-Mail, findet man rechts oben in der Symbolleiste die Symbole, mit denen man durch Anklicken festlegen kann, ob die E-Mail signiert (digital unterzeichnet) oder/und verschlüsselt werden soll (Abb. 26 bis 28).

In Abb. 28 fällt auf, dass die Nachricht an eine Adresse bei T-Online geschickt wurde. Da der öffentliche Schlüssel als Anhang mitgeschickt wird (Dateiname „smime.p7s") kann das Zertifikat beim Empfänger geprüft werden. Die meisten Provider (T-Online, MS Hotmail, Yahoo, Webmail, Googlemail usw.) bieten leider noch nicht den Umgang mit Zertifikaten. Mit Outlook Web Access (OWA) ist es möglich, E-Mails digital zu signieren oder zu verschlüsseln. Diese Option kann unter „Optionen" aktiviert werden.

Im E-Mail-Programm Mozilla Thunderbird findet man die Auswahlbefehle, ob digital signiert oder verschlüsselt werden soll, im neu hinzugekommenen Pull-down-Menü „S/MIME" (Abb. 29).

29 *Befehle zum Signieren/Verschlüsseln im Menü „S/MIME"*

Empfang einer signierten oder verschlüsselten Nachricht

Empfang einer signierten Nachricht in MS Outlook

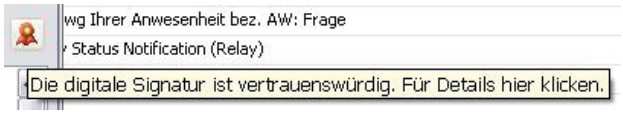
Dass die empfangene Nachricht digital signiert oder verschlüsselt ist, wird dem Empfänger erst in der „Inbox" und dann im Nachrichtenkopf angezeigt (Abb. 30).

30 *Anzeige einer digital signierten Nachricht im Posteingang*

Links oben im Kopf der E-Mail wird angezeigt, dass es sich um eine digital signierte E-Mail handelt. Rechts über dem Textfeld zeigt dies ein rotes Symbol an (Abb. 31). Klickt man auf dieses Symbol oder sieht sich

31 *Im Anzeigefenster der empfangenen E-Mail findet man links die Information, dass es sich um eine digital signierte Nachricht handelt, rechts wird dies mit einem Symbol angezeigt.*

die Eigenschaften der empfangenen E-Mail an (unter „Sicherheit"), bekommt man genauere Informationen zur Signatur (Abb. 32).



32 *Mit dem Mauszeiger auf das Symbol gehen...*

Klickt man auf das Symbol, wird die Anzeige etwas ausführlicher (Abb. 33).

33 *Outlook hat die digitale Signatur überprüft und als vertrauenswürdig eingestuft.*

Nun kann man sich noch Details zur Signatur anzeigen lassen (Abb. 34).

Im Beschreibungsfeld werden jeweils die Details der markierten Sicherheitsschicht angezeigt (Abb. 35).

Die Schaltfläche „Vertrauen..." führt zu den Fenstern mit den Zertifikateigenschaften (Abb. 36 und 37). Die

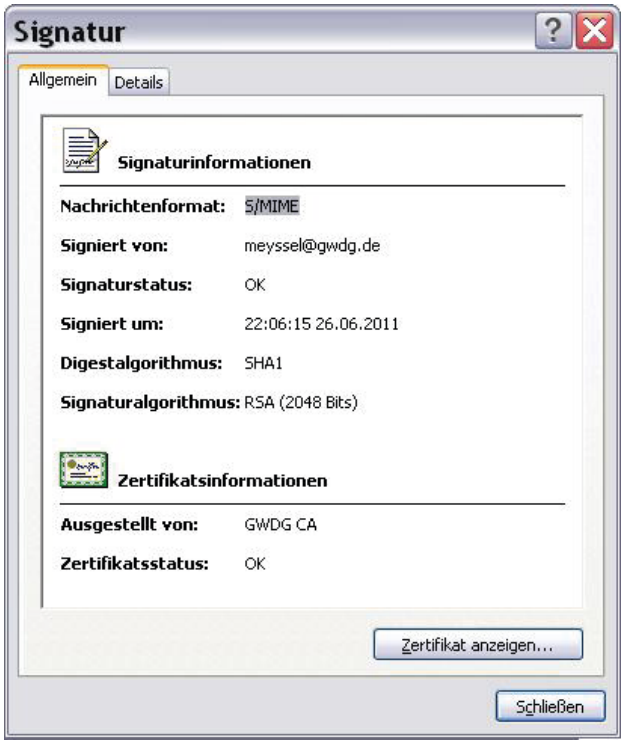
34 *Eigenschaften der E-Mail mit dem Betreff „signierte Nachricht"*

Schaltfläche „Details anzeigen..." (in Abb. 35) lässt alle Details der Signatur erkennen.

Die Karteikarte „Allgemein" gibt eine Übersicht (Abb. 36), unter „Details" findet man genauere Informationen (Abb. 37).

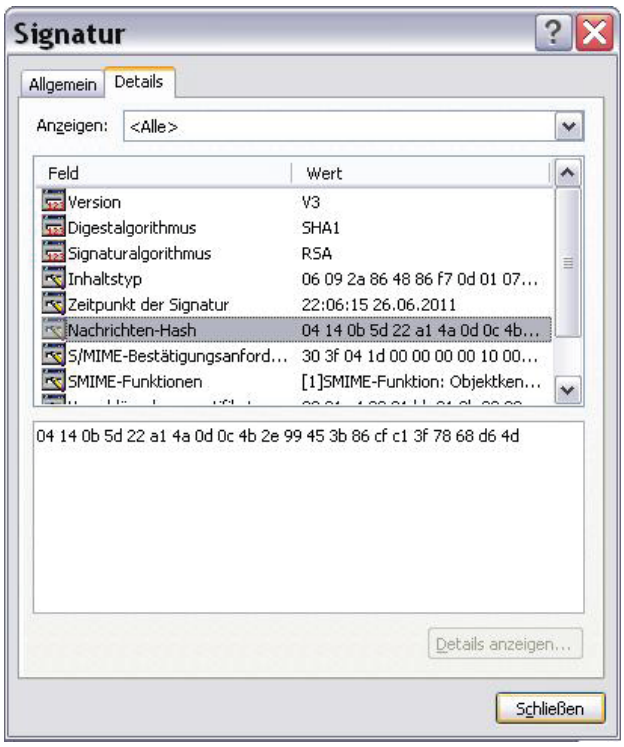
Auf der Karteikarte „Allgemein" findet man die Befehlstaste „Zertifikat anzeigen…", die man betätigt, wenn man das Zertifikat ansehen und/oder abspeichern will (Abb. 38).

35 *Information zum Signierer der E-Mail*

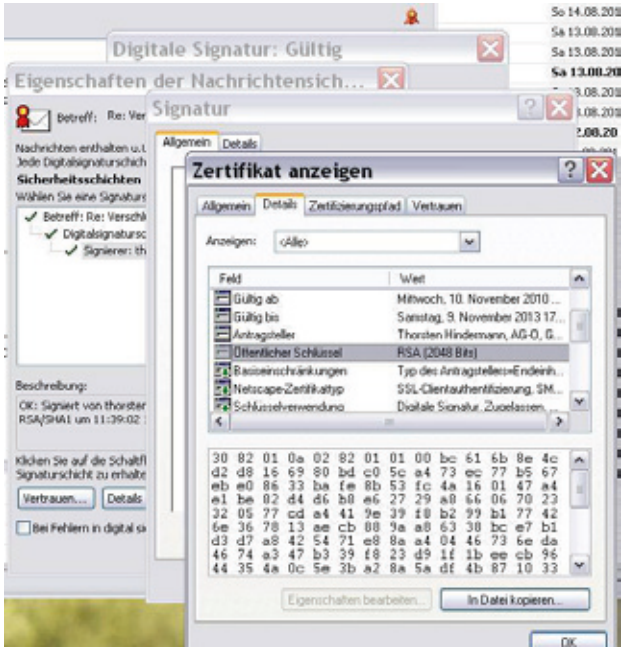


36 *Informationen zur Signatur und zum Zertifikat*

Erhält man von einem Korrespondenzpartner eine digital signierte E-Mail, so enthält diese dessen öffentlichen Schlüssel. Man kann ihn z. B. in seiner Outlook-Adressliste „Kontakte“ abspeichern, so dass signierte Nachrichten von diesem Absender immer sicher identifiziert werden.



37 *In der Detailansicht wird hier der Hash-Wert (Fingerprint) der E-Mail angezeigt.*

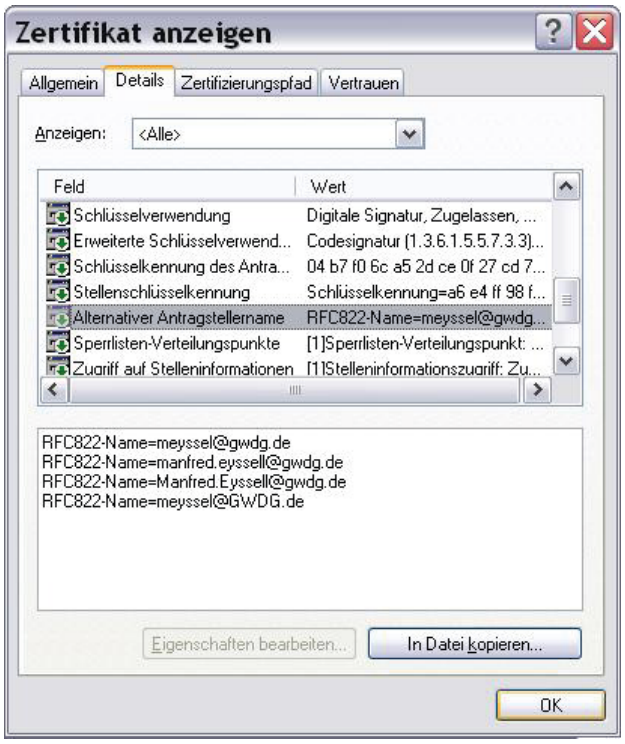


38 *Anzeige des öffentlichen Schlüssels*

Dazu muss man das Zertifikat anzeigen lassen und in eine Datei kopieren (Befehlstaste „In Datei kopieren…“, s. Abb. 38 und 40). Dann öffnet man den Outlook-Kontakt dieses Korrespondenzpartners und wählt auf der Karteikarte „Zertifikate“ die Befehlstaste „Importieren…“.

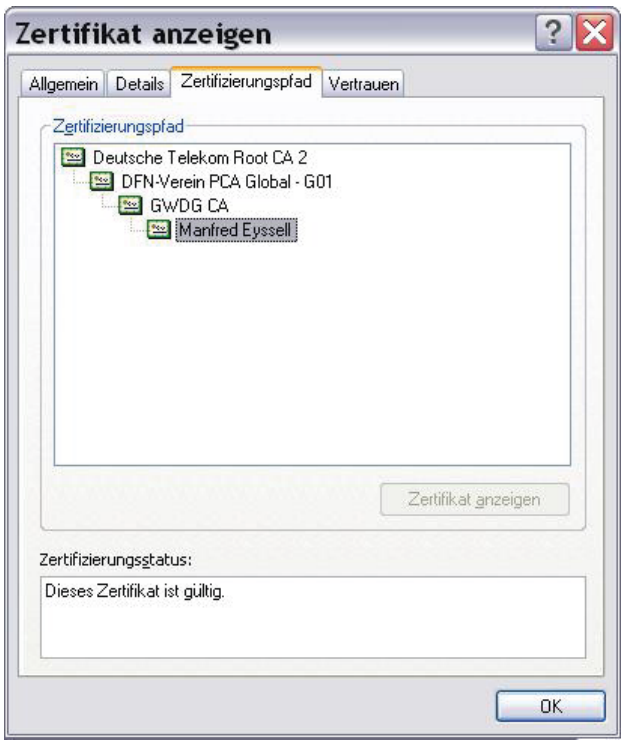
39 *Übersicht über das Zertifikat*

Die Karteikarte „Details“ enthält die einzelnen Inhalte des Zertifikats (Abb. 40).



40 *Die verschiedenen Felder mit den Eigenschaften des Zertifikats werden im unteren Bereich detailliert angezeigt.*

Auf der Karteikarte „Zertifizierungspfad“ kann man auch die Zertifikate der Zertifizierungsstellen prüfen. (Abb. 41).



41 *Der Zertifizierungspfad ermöglicht es, die Zertifikate der Zertifizierungsstellen zu prüfen.*

Will man dem Zertifikat vertrauen, kann man das im Fenster entsprechend ausfüllen (Abb. 42).

42 *Das Zertifikat kann als vertrauenswürdig übernommen oder abgewiesen werden.*

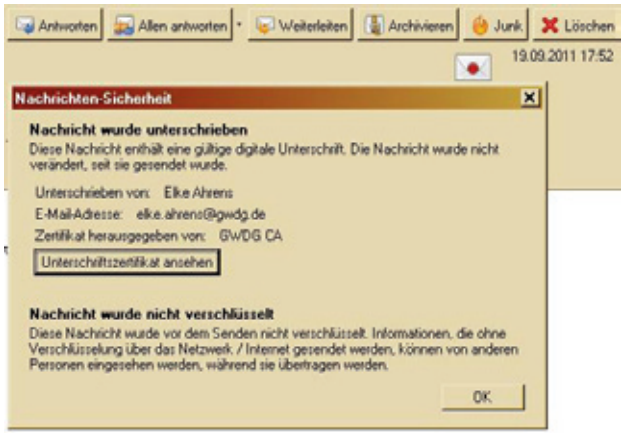
Das Zertifikat kann als vertrauenswürdig übernommen oder abgewiesen werden.

Anschließend bietet das Anzeigefenster von „Outlook-Kontakte“ die Möglichkeit, das Zertifikat zu importieren, zu exportieren (in eine Datei abspeichern) oder zu entfernen.

Empfang einer digital signierten Nachricht in Mozilla Thunderbird

Die digital signierte Nachricht wird mit einem versiegelten Briefumschlag kenntlich gemacht (Abb. 43).

43 *Der versiegelte Briefumschlag zeigt in Thunderbird an, dass eine E-Mail digital signiert ist.*



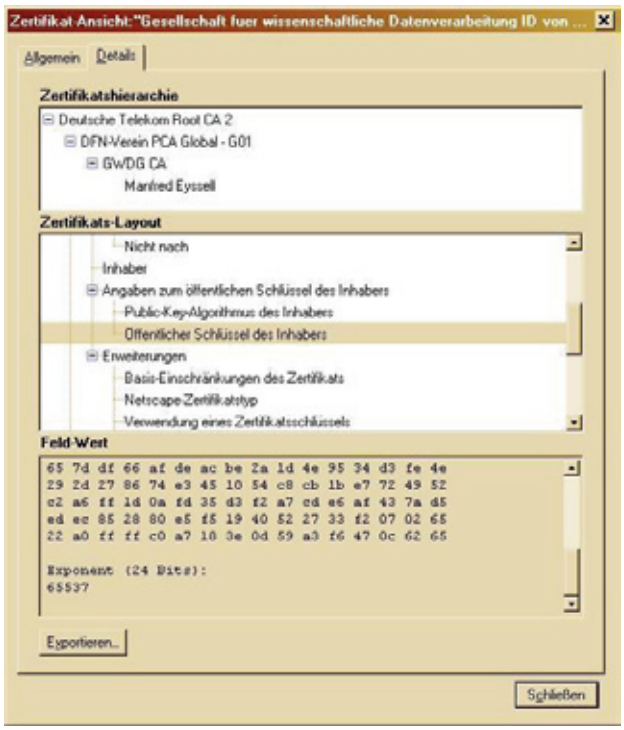
44 *Klickt man auf das Symbol, erhält man bei Thunderbird auch die Information: „Die Nachricht wurde nicht verändert, seit sie gesendet wurde.“*

Beim Ansehen des Zertifikats (Befehlstaste „Unterschriftzertifikat ansehen“) stößt man auf die Besonderheit, dass die beiden öffentlichen Schlüssel getrennt angezeigt werden (Abb. 45), und zwar wird der Schlüssel „E“ als Dezimalzahl angezeigt („Exponent“)

Verschlüsselung einer Nachricht

Senden einer verschlüsselten Nachricht

Hat man die Befehlstaste für die Verschlüsselung einer zu sendenden Nachricht gedrückt und sendet die Nachricht ab, so funktioniert das nur, wenn ein Zertifikat, d. h. der öffentliche Schlüssel des Empfängers in Outlook (oder Thunderbird) verfügbar ist. Dann wird die verschlüsselte Nachricht abgesendet und der Empfänger bekommt sie entschlüsselt angezeigt



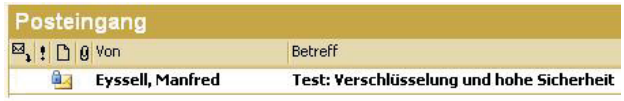
45 *Vom öffentlichen Schlüssel werden die Schlüsselzahlen N (2.048 Bits) und E (24 Bits) getrennt angezeigt.*

(wenn er seinen privaten Schlüssel installiert hat), wobei ihm mitgeteilt wird, dass die Nachricht verschlüsselt übertragen wurde. Ist kein Zertifikat des Adressaten verfügbar, so kann die E-Mail nicht in verschlüsselter Form abgesendet werden, man bekommt eine Fehlermeldung (Abb. 46).

46 *Fehlermeldung, wenn eine E-Mail nicht verschlüsselt werden kann, weil der öffentliche Schlüssel des Absenders nicht vorliegt*

Empfang einer verschlüsselten Nachricht

Dass die empfangene Nachricht digital signiert oder verschlüsselt ist, wird dem Empfänger erst in der „Inbox“ und dann im Nachrichtenkopf angezeigt (Abb. 47).



47 *Anzeige einer verschlüsselten Nachricht im Posteingang mit einem blauen Schloss am Briefsymbol*

Außer dieser Anzeige erfährt man nichts davon, dass die Nachricht verschlüsselt übertragen wurde, denn der Absender konnte sie nur dann verschlüsseln, wenn er im Besitz des öffentlichen Schlüssels (Zertifikats) des Empfängers war. Das Entschlüsseln geschieht ohne weiteres Zutun, denn der private Schlüssel des Empfängers ist ja in das E-Mail-Programm eingebaut.

In Mozilla Thunderbird wird die empfangene verschlüsselte E-Mail mit einem Schloss rechts oben über dem Text der E-Mail angezeigt (Abb. 48).

48 *Symbol für eine verschlüsselt empfangene Nachricht in Mozilla Thunderbird*

Sicherheit im Web und bei der Servereinwahl

Da beim Informationsaustausch zwischen einem Webanbieter (Webserver) und dem Nutzer vielfach eine gesicherte Übertragung – es soll niemand die Informationen mitlesen dürfen – gewünscht wird, wird neben dem normalen Übertragungsprotokoll im World Wide Web (http = HyperText Transfer Protocol) auch eine Version mit Verschlüsselung und Authentifizierung der Kommunikation zwischen Webserver und Browser angeboten: „https" (= HyperText Transfer Protocol Secure = sicheres Hypertext-Übertragungsprotokoll). Man kann diese Protokollbezeichnung der gewünschten URL (z. B. *https://www.xyz.com*) voranstellen; normalerweise schaltet aber ein angewählter Server, der verschlüsselte Übertragung bietet, automatisch auf diese Protokollvariante um.

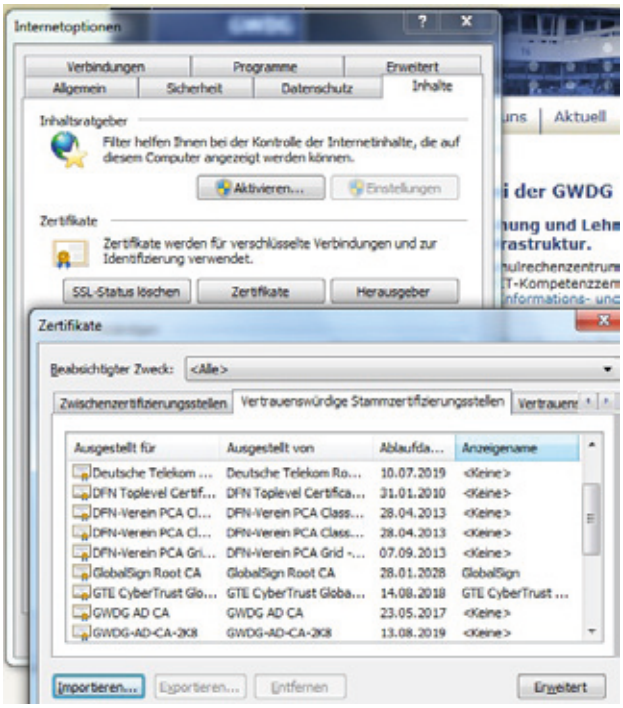
Enorm wichtig ist diese Möglichkeit der Verschlüsselung der Nachrichtenübertragung in Funknetzen, da diese auf sehr einfache Weise abgehört werden können. Durch die Authentifizierung kann sich jede Seite der Identität des Verbindungspartners vergewissern.

Die Verschlüsselung erfolgt mit dem Verfahren SSL/TLS. SSL sorgt für die geschützte Identifikation und Authentifizierung der Kommunikationspartner und für die Verschlüsselung eines weiteren Schlüssels mit dem asymmetrischen Verschlüsselungsverfahren RSA. Da asymmetrische Verschlüsselungsverfahren wegen ihres hohen mathematischen Aufwands viel Prozessorlast verursachen, wird anschließend dieser weitere Schlüssel für eine symmetrische Verschlüsselung der Datenübertragung mit dem Verfahren 3DES verwendet.

Das Wurzel-Zertifikat der Telekom, das „Deutsche Telekom Root CA2", ist in vielen Anwendungen und Betriebssystemen bereits integriert und braucht daher nicht mehr in Ihren Web-Browser importiert werden.

Bankgeschäfte

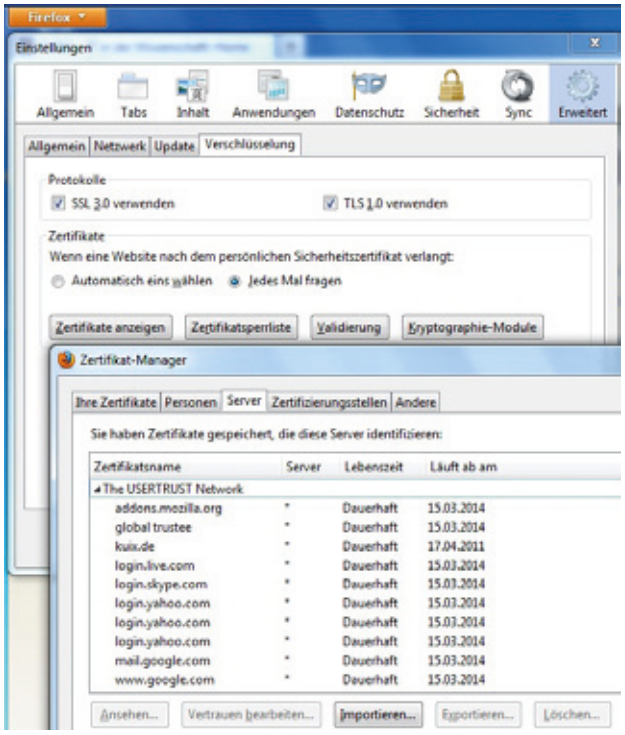
Beim Aufruf einer Webseite erwartet man, dass die mit einem URL angesteuerte Seite auch wirklich ein Portal der Institution ist, mit der man Informationen austauschen will. Hat man z. B. vor, mit dem Internet-Auftritt seiner Bank Kontakt aufzunehmen und anschließend Überweisungen von seinem Konto zu tätigen (sog. Homebanking), möchte man nicht auf die täuschend ähnlich aussehende gefälschte Webseite eines Internet-Hackers kommen, der kurzzeitig die URL der Bank auf seinem Server eingestellt hat und außerdem Name-Server-Informationen manipuliert hat. Es würde dann dazu kommen, dass man in die falsche Webseite seine persönlichen Daten, seine Kontonummer und dazu Passwörter eingibt. Mit diesen Informationen könnte der betrügerische Besitzer der „gefaketen" Webseite dann über das Konto verfügen.



49 *In den Internet Explorer eingebaute Zertifikate*

Gebraucht wird also ein Mechanismus, der sicherstellt, dass die mit meinem Browser verbundene Webseite wirklich der Bank gehört, die mein Kon-

to verwaltet. Hier kommen die Zertifikate ins Spiel. Die Webseite der Bank bietet ihr „Server-Zertifikat“ zur Ansicht, zur Prüfung und zum Herunterladen auf meinen Computer an. Wenn mein Browser über eine Liste von Zertifikaten verfügt, unter denen auch das meiner Bank ist, kann dieser durch Vergleich der Zertifikate sicher feststellen, ob die aufgerufene und dargestellte Webseite wirklich meiner Bank gehört. Diese Liste von Zertifikaten besteht aus solchen, die vom Browser-Hersteller bereits mitgeliefert wurden (Abb. 49 und 50), und solchen, die ich selbst hinzugefügt habe, jeweils nach sorgfältigster Prüfung der Echtheit des Zertifikats.

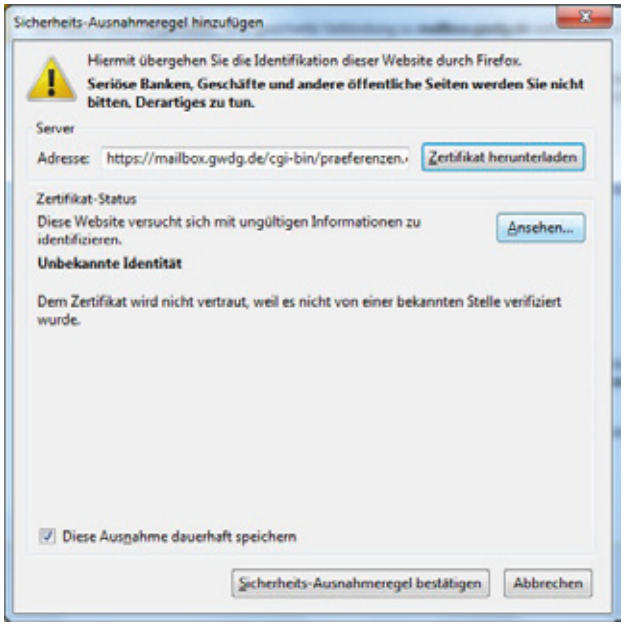


50 *In den Mozilla Firefox eingebaute Zertifikate*

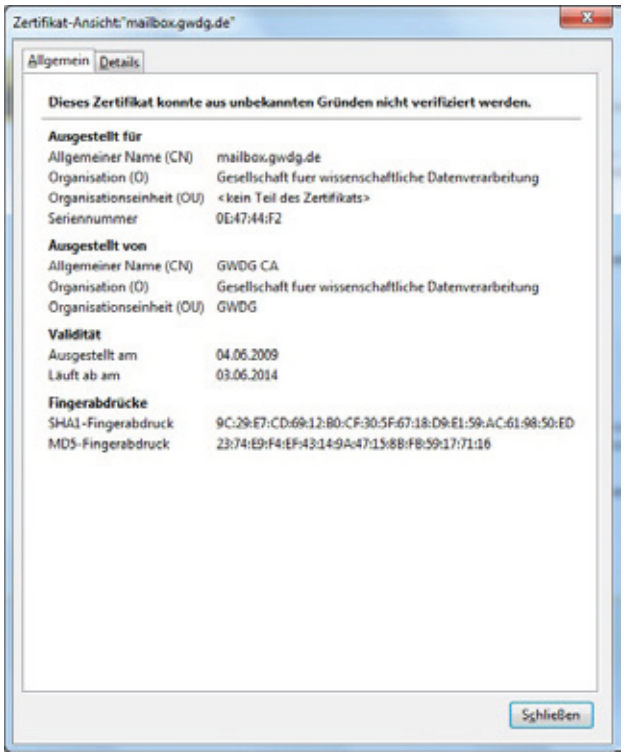
Wählt man einen Server oder eine Webseite, deren Zertifikat nicht im eigenen Browser bekannt ist, fragt dieser an, ob man dem Zertifikat vertrauen will und es in seinen Browser einfügen will (Abb. 51).

Hakt man „Diese Ausnahme dauerhaft speichern“ an, läuft man Gefahr, in Zukunft einer Webseite zu vertrauen, die nicht vertrauenswürdig ist. Man sollte dies nur tun, wenn man sich das Zertifikat angesehen hat (Taste „Ansehen...“) und es als vertrauenswürdig erkannt hat.

- Certificate name: Name des Zertifikat-Inhabers
- Issuer: Zertifizierungsstelle, die die Authentizität bestätigt
- Details: Gültigkeitsdauer und andere Daten; digitale Signatur des Zertifikats durch die Zertifizierungsstelle (Issuer)
- Public Key: der öffentliche Schlüssel



51 *Warnung vor unbekanntem Zertifikat*



52 *Anzeige eines noch unbekannten Zertifikats. Die Detailansicht gibt genaueren Aufschluss.*

Ist man nach Prüfung des Zertifikats davon überzeugt, dass es glaubwürdig ist, lädt man es auf seinen Computer und fügt es in seinen Internet-Browser ein.

Von da an weiß der Browser, dass die Seite mit dem Zertifikat, das nun auch in seiner Liste vorhanden ist, echt ist und ein Datenaustausch mit dieser Seite ist möglich: Ein verschlüsselter Datenaustausch (mit dem SSL-Protokoll, das sich dem Benutzer als „https:" statt „http:" mitteilt) kann vorgenommen werden.

Die Methode funktioniert, denn nur der Server, der seinen öffentlichen Schüssel bekanntgegeben hat, kann (mit seinem privaten Schlüssel) die Daten entschlüsseln, die der Klient mit diesem Schlüssel ihm zusendet.

Nicht passieren darf, dass man einem angebotenen Zertifikat leichtsinnigerweise – ohne Prüfung – vertraut. Dann könnte ein von einem Betrüger betriebener Server mit gefälschter „Homepage" vorgeben, die Hausbank zu sein: Der Web-Browser zeigt zwar beim ersten Besuch dieser Webseite an, dass er das Zertifikat des Betrügers nicht kennt. Wenn nun der Benutzer des Web-Browsers aus Bequemlichkeit ohne Prüfung auf „Zertifikat annehmen" klickt, kommunizieren fortan Web-Browser und der Server des Betrügers über eine sichere Verbindung.

Diese nun falsche Gewissheit, mit dem richtigen Partner zu kommunizieren, kann wegen der leichtsinnigen Annahme des unbekannten Zertifikats dazu führen, dass nicht nur folgende Besuche des Betrüger-Servers als sicher eingestuft werden, sondern auch weitere Zertifikate, die der Betrüger-Server signiert hat.

Eyßell

Kontakt:
Manfred Eyßell
meyssel@gwdg.de
0551 201-1539

Offener Testbetrieb für den neuen Dienst „PowerFolder" – eine Alternative zu „Dropbox"

Mit der Ankündigung am 07.10.2011 hat die GWDG mit einem neuen Dienst für Dateisynchronisation den offenen Testbetrieb gestartet. Mit diesem Dienst ist es möglich, mit auf PCs und Laptops installierten Client-Programmen Verzeichnisse auf dem gleichen Stand zu halten. Zusätzlich ist es möglich, den Zugriff auf einzelne Verzeichnisse auch anderen Nutzern zu gestatten. Das Arbeiten an den überwachten Dateien ist dabei ebenfalls offline möglich, Änderungen werden dann bei der nächsten Online-Verbindung übertragen und empfangen. Die Arbeitsweise ist mit ein paar Einschränkungen aber auch neuen Möglichkeiten vergleichbar zu dem bekannten „Dropbox".

Für unseren Dienst kommt die Software „PowerFolder" der gleichnamigen Firma zum Einsatz. Der Client steht für Windows, Mac OS X und Linux zur Verfügung. Nähere Informationen zum Dienst und „Erste Schritte" finden sich während des Testbetriebs im öffentlichen Wiki der GWDG (*http://wiki.gwdg.de/index.php/PowerFolder*).

Mit dem aktuellen Testbetrieb möchte die GWDG Erfahrungen mit dem Client auf unterschiedlichen Plattformen und bei unterschiedlichen Benutzern und Nutzungsszenarien sammeln, die Administrierbarkeit, Zuverlässigkeit und Leistungsfähigkeit des Serverdienstes kennenlernen und die Integration in die Infrastruktur der GWDG prüfen. Wir sind dabei auf die Mithilfe unserer Benutzer aus der Max-Planck-Gesellschaft und der Universität Göttingen angewiesen und würden uns über rege Teilnahme und einen intensiven Testbetrieb freuen. Um einen Test mit breiter Benutzerbasis zu ermöglichen, streben wir schon während unseres Testbetriebs die Leistung und Zuverlässigkeit des späteren Regelbetriebs an. Dazu gehört auch das Backup der Benutzerdaten für 90 Tage. Der Server wird von der GWDG betrieben und im Rechenzentrum gehostet. Der Speicherplatz für Server- und Benutzerdaten befindet sich ebenfalls bei der GWDG. Der Dienst steht allen Benutzern der Max-Planck-Gesellschaft, der Universität Göttingen, der GWDG sowie den Studierenden der Universität Göttingen offen.

Wegmann

Kontakt:
Bendedikt Wegmann
Benedikt.Wegmann@gwdg.de
0551 201-1870

Kurse von November bis Dezember 2011

Allgemeine Informationen zum Kursangebot der GWDG

Teilnehmerkreis

Das Kursangebot der GWDG richtet sich an die Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus anderen wissenschaftlichen Einrichtungen, die zum erweiterten Benutzerkreis der GWDG gehören. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die GWDG, Kursanmeldung, Postfach 2841, 37018 Göttingen oder per E-Mail an die Adresse *support@gwdg.de* mit dem Betreff „Kursanmeldung" erfolgen. Für die schriftliche Anmeldung steht unter *http://www.gwdg.de/index.php?id=799* ein Formular zur Verfügung. Telefonische Anmeldungen können wegen der Einbeziehung der Kurse in die interne Kosten- und Leistungsrechnung der GWDG nicht angenommen werden. Aus diesem Grund können Anmeldungen auch nur durch den Gruppenmanager – eine der GWDG vom zugehörigen Institut bekannt gegebene und dazu autorisierte Person – oder Geschäftsführenden Direktor des Instituts vorgenommen werden. Die Anmeldefrist endet jeweils sieben Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit der Service-Hotline bzw. Information (Tel.: 0551 201-1523, E-Mail: *support@gwdg.de*) möglich.

Kosten bzw. Gebühren

Die Kurse sind – wie die meisten anderen Leistungen der GWDG – in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die bei den Kursen angegebenen Arbeitseinheiten (AE) werden vom jeweiligen Institutskontingent abgezogen. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu acht Tagen vor Kursbeginn erfolgen. Bei späteren Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht. Sollte ein Kurs aus irgendwelchen Gründen, zu denen auch die Unterschreitung der Mindestteilnehmerzahl bei Anmeldeschluss sowie die kurzfristige Erkrankung des Kurshalters gehören, abgesagt werden müssen, so werden wir versuchen, dies den betroffenen Personen rechtzeitig mitzuteilen. Daher sollte bei der Anmeldung auf möglichst vollständige Adressangaben inkl. Telefonnummer und E-Mail-Adresse geachtet werden. Die Berechnung der Arbeitseinheiten entfällt in diesen Fällen selbstverständlich. Weitergehende Ansprüche können jedoch nicht anerkannt werden.

Kursorte

Alle Kurse finden in Räumen der GWDG statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 5 bzw. 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Faßberg 11, 37077 Göttingen. Die Wegbeschreibung zur GWDG bzw. zum Max-Planck-Institut für biophysikalische Chemie sowie der Lageplan sind im WWW unter dem URL *http://www.gwdg.de/index.php?id=13* zu finden.

Ausführliche und aktuelle Informationen

Ausführliche Informationen zu den Kursen, insbesondere zu den Kursinhalten und Räumen, sowie aktuelle kurzfristige Informationen zum Status der Kurse sind im WWW unter dem URL *http://www.gwdg.de/index.php?id=57* zu finden. Anfragen zu den Kursen können an die Service-Hotline bzw. Information per Telefon unter der Nummer 0551 201-1523 oder per E-Mail an die Adresse *support@gwdg.de* gerichtet werden.

Kurs	Vortragende/r	Termin	Anmeldeschluss	AE
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	01.11.2011 - 02.11.2011, 09.11.2011 - 10.11.2011 13:00 - 16:30 Uhr	25.10.2011	8
Einführung in die Statistische Datenanlyse mit SPSS	Cordes	03.11.2011 - 04.11.2011 09:00 - 12:00 Uhr und 13:00 - 15:30 Uhr	27.10.2011	8
Programmierung von Parallelrechnern	Dr. Boehme, Dr. Schwardmann	15.11.2011 - 17.11.2011 09:15 - 12:15 Uhr und 13:30 - 16:30 Uhr	08.11.2011	12
Einführung in die Programme zur Sequenzanalyse	Dr. Bohrer	22.11.2011 - 23.11.2011, 29.11.2011 - 30.11.2011 13:00 - 16:30 Uhr	15.11.2011	8
Angewandte Statistik mit SPSS für Nutzer mit Vorkenntnissen	Cordes	01.12.2011 - 02.12.2011 09:00 - 12:00 Uhr und 13:00 - 15:30 Uhr	24.11.2011	8
UNIX/Linux-Arbeitsplatzrechner – Installation und Administration	Dr. Heuer, Dr. Sippel	05.12.2011 - 06.12.2011 09:15 - 12:00 Uhr und 13:30 - 16:00 Uhr	28.11.2011	8
UNIX/Linux-Server – Grundlagen der Administration	Dr. Heuer, Dr. Sippel	07.12.2011 - 08.12.2011 09:15 - 12:00 Uhr und 13:30 - 16:00 Uhr	30.11.2011	8
UNIX/Linux-Systemsicherheit für Administratoren	Dr. Heuer, Dr. Sippel	09.12.2011 09:15 - 12:00 Uhr und 13:30 - 15:00 Uhr	02.12.2011	4