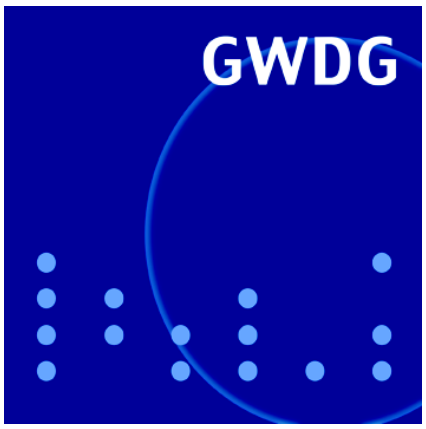


Sophos-Update-Service für Linux und Mac OS X

Zertifizierungsrichtlinien der GWDG-CA

Web-Schnittstelle zum Drucker-Server

GWDG Nachrichten

8 / 2004

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Inhaltsverzeichnis

1. Sophos-Update-Service unterstützt nun auch Linux und Mac OS 3
2. Sophos Anti-Virus für Mac OS X 4
3. Zertifizierungsrichtlinien der GWDG-CA 5
4. Die Web-Schnittstelle zum zentralen Drucker-Server der GWDG 8
5. Kurse des Rechenzentrums 12
6. Betriebsstatistik Juli 2004. 17
7. Autoren dieser Ausgabe 18

GWDG-Nachrichten für die Benutzer des Rechenzentrums

ISSN 0940-4686

27. Jahrgang, Ausgabe 8 / 2004

http://www.gwdg.de/GWDG-Nachrichten

Herausgeber: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg, 37077 Göttingen-Nikolausberg

Redaktion: Dr. Th. Otto Tel.: 0551 201-1828, E-Mail: Thomas.Otto@gwdg.de
Herstellung: S. Greber Tel.: 0551 201-1518, E-Mail: Sigrun.Greber@gwdg.de

1. Sophos-Update-Service unterstützt nun auch Linux und Mac OS

Der Sophos-Update-Service der GWDG, über den seit etwa fast einem Jahr den Mitarbeitern und Studierenden der niedersächsischen Hochschulen wie auch den Mitarbeitern der Institute der Max-Planck-Gesellschaft die komfortable Installation und Aktualisierung des Virenscanners **Sophos Anti-Virus** auf den Windows-Derivaten ermöglicht wird (s. auch die GWDG-Nachrichten 10/2003), dehnt ab sofort seine Dienste zusätzlich auch auf die Betriebssysteme Linux und Mac OS X aus. Möglich wurde das durch ein Upgrade des Sophos-Enterprise-Managers auf die neue EM-Library 1.1. Diese holt, wie schon ihre Vorgängerin, zeitnah die aktuellen Updates für die Antiviren-Software von der zentralen Sophos- Datenbank ab und stellt diese Dateien über das **Remote Update** komfortabel der Nutzerschaft zur Verfügung. Voraussetzung für den Zugang zu diesem unkomplizierten Verfahren ist dann nur noch eine Verbindung ins Internet und schon hat man für einen umfassenden Virenschutz gesorgt. Die für den Nutzer sicherlich augenscheinlichste Neuerung dieser neuen EM-Library dürfte das Angebot von Updates auch für die Nicht-Windows-Plattformen **Mac OS** und **Linux** sein und zwar genauer für die folgenden Versionen:

- Mac OS X ab der Version 10.2 (*Jaguar*)
- Alle Linux-Distributionen, die auf der glibc-Version 2.2 aufsetzen.

Vielleicht mag sich hier der Leser fragen, warum für diese beiden Plattformen überhaupt ein Virenschutz nötig sein soll, zielten doch die meisten Schädlinge in der Vergangenheit fast ausschließlich auf die Windows-Systeme. Einerseits werden unter Mac OS oftmals die gleichen Office-Anwendungen betrieben wie unter Windows, so dass hier zumindest die zahlreichen Makroviren einen geeigneten Nährboden finden könnten. Andererseits ist zudem gewissermaßen systembedingt nicht selten ein reger Datenaustausch zwischen Mac- und Windows-Systemen erforderlich, wobei natürlich dann auch die Viren und Würmer mit transportiert werden. Da macht es durchaus Sinn, diese Schädlinge gleich auch auf dem Mac-Rechner zu eliminieren und sie nicht erst von dort aus auf die diversen Windows-Systeme zu verteilen.

Leuchtet somit ein Virenschutz auf dem Mac-Rechner also noch ein, zeigten sich gerade auch die Linux-Systeme gegenüber den Viren- und Wurmattacken in der Vergangenheit gänzlich immun. Warum also dort überhaupt einen Virenscanner installieren? Ein Grund liegt in der Tatsache, dass Linux-Systeme zunehmend Einsatz als Server finden, sei es als Mailserver oder als Datei-Server. In beiden Fällen beherbergen sie kurz- oder auch längerfristig Daten für Windows-Systeme, die durchaus auch den einen oder anderen Schädling enthalten könnten. Ein auf dem Linux-Server regelmäßig durchgeführter Virencheck auf Basis einer stets aktuell gehaltenen Datenbank hilft, die Verbreitung der Viren und Würmer ganz erheblich zu minimieren. Und schließlich resultiert die große Zahl von Schädlingen für die Windows-Systeme aus der starken Verbreitung dieses Betriebssystems. Sollte sich in Zukunft die Anzahl der Mac-OS- und Linux-Installationen drastisch erhöhen, werden auch diese beiden Plattformen für die Virenschreiber sicher sehr schnell an Attraktivität gewinnen.

Wer an dem Update-Service teilhaben möchte, findet die Anleitungen zur Installation und Konfiguration auch für die neu unterstützten Betriebssysteme auf dem folgenden Server:

`http://antivir.gwdg.de`

Das für die Installation erforderliche Zugangskennwort hat sich übrigens nicht geändert und kann bei der GWDG erfragt werden. Eine ausführlichere Installationsanleitung für die Mac-Plattform findet sich übrigens auch im nachfolgenden Artikel.

Auch wenn mit dem Virenscanner Sophos Anti-Virus sicherlich ein umfassender und komfortabel zu konfigurierender Schutz gegen die Mehrzahl der im Internet vertretenen Schädlinge zur Verfügung steht, so sollte man dennoch immer dabei berücksichtigen, dass zwischen dem Erkennen eines neuen Virus, der Erstellung einer passenden Virensignatur durch den Hersteller der Antiviren-Software und der anschließenden Verteilung dieser Signaturen auf den Rechner des einzelnen Nutzers durchaus einige Stunden bis zu einem Tag verstreichen können. In diesem Zeitraum ist man zwangsläufig ungeschützt und ist somit stets gut beraten, die aus dem Internet bezogenen Daten immer mit einer gesunden Skepsis zu betrachten. Die hohe Verbreitungsgeschwindigkeit einiger in den vergangenen Monaten aufgetauchten Würmer hat das leider nur allzu deutlich gemacht.

Reimann

2. Sophos Anti-Virus für Mac OS X

Für die Plattform Apple Macintosh existieren immer noch recht wenige Antivirenprogramme. Die Hersteller versuchen, das dadurch zu begründen, dass es auf dem Mac kaum Virenplagen gibt, was so nicht ganz korrekt ist, wenn man zumindest die Word-Makroviren betrachtet. Somit ist der Einsatz einer Antivirensoftware durchaus zu empfehlen, damit man nicht unbeabsichtigt zum Wirt und Verbreiter diverser PC- oder Makroviren macht.

Sophos Anti-Virus ist (mittlerweile) ein Produkt unter den Antivirenprogrammen, das mit einer guten Erkennungsleistung, unproblematischer Installation und einfacher Bedienbarkeit aufwartet.

2.1 Installation

Die Installation ist, wie typisch für Mac OS X, sehr einfach und unkompliziert: Disk-Image herunterladen, aktivieren und das Installationsprogramm starten.

Das (jeweils monatsaktuelle) Programm kann man vom Server

`http://www.mac.gwdg.de`

herunterladen. Dazu ist im Browser-Fenster

`ftp://sophoslice@www.mac.gwdg.de`

einzutragen und das Passwort unter

`machelp@gwdg.de`

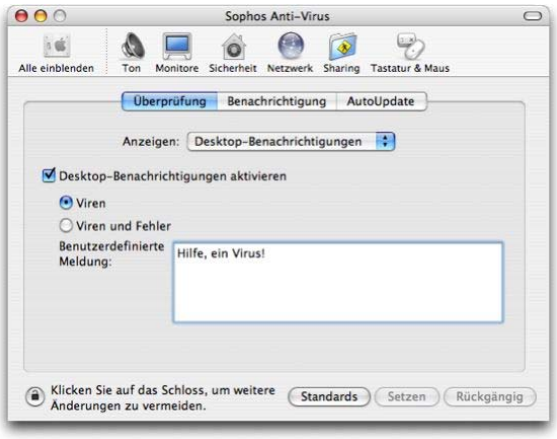
zu erfragen.

Der Pfad lautet *Software -> Utilities -> Virenschutz -> Sophos*. Der Installer führt durch die notwendigen Schritte, wobei man auswählen kann, welche Bestandteile von Sophos installiert werden sollen: z. B. nur der On-Access-Scanner oder die Aktualisierung des Programms. Nach erfolgreicher Installation, die in „/Programme“ den On-Demand-Scanner und den Systemeinstellungen ein weiteres Kontrollfeld hinzufügt, ist ein Neustart des Computers nötig.

In „/Library/Application Support/Sophos Anti-Virus“ werden für den On-Demand-Scanner und den On-Access-Scanner die benötigten IDE-Dateien und weitere Bestandteile abgelegt. Außerdem befindet sich dort ein Un-Installer, um bei Bedarf Sophos ohne viel Aufwand zu deinstallieren.

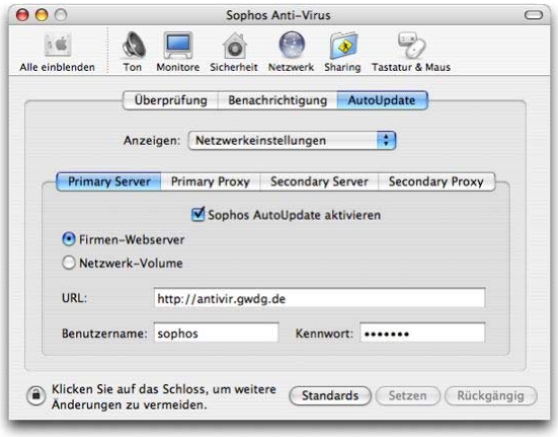
2.2 Konfigurieren des On-Access-Scanners

Sophos liefert zwei verschiedene Virenscanner mit: zum einen den sog. On-Demand-Scanner, der erst vom Benutzer aufgerufen werden muss, um das System nach infizierten Dateien zu durchsuchen. Zum anderen den On-Access-Scanner, der hingegen als Daemon (ein Hintergrundprozess) läuft und für automatische Aktualisierungen der Virensignaturen und der Scan-Engine sorgt. Konfiguriert wird dieser Dienst über die Systemeinstellungen.



Neben Start/Stopp des Scanners finden sich unter dem Reiter „Überprüfung“ auch Voreinstellungen zum Speichern von Log-Dateien, Warnmeldungen und die Möglichkeit, nach Windows-Viren zu suchen.

Über den Reiter „AutoUpdate“ hat man die Möglichkeit, direkt über den Sophos-Update-Service der GWDG den Virenscanner auf dem aktuellsten Stand zu halten.



Um den AutoUpdate-Service nutzen zu können, müssen die folgenden Einträge in den Netzwerkeinstellungen gemacht werden: „Sophos AutoUpdate aktivieren“ anklicken und als Server „Firmen-Webserver“ auswählen.

In das Feld „URL“ muss nun die Adresse des Updateservers eingetragen werden:

URL: **`http://antivir.gwdg.de`**

Benutzername: sophos

Kennwort: kann bei der GWDG erfragt werden

Im Aufklappmenü finden sich weitere Optionen, z. B. die Angabe des Aktualisierungs-Zeitplans und des Speicherorts von Log-Dateien. Sind alle Einstellungen korrekt vorgenommen, verbindet sich Sophos mit dem Updateserver und aktualisiert die Virenbeschreibungen sowie die Scan-Engine.

2.3 Fazit

Mit Sophos hat man eine umfassende und komfortable Möglichkeit, seinen Mac-Rechner vor Viren zu schützen. Durch die Option des Erkennens von Windows-Viren hilft man gleichzeitig den PC-Nutzern, indem der Mac-Nutzer keine Viren weitergeben kann. Leider entspricht der On-Demand-Scanner nicht ganz den grafischen Gepflogenheiten von Mac OS X, der On-Access-Scanner ist hingegen gelungen in die Systemeinstellungen integriert und reicht durch die beständige Überwachung des Systems im Hintergrund als Standarddienst auch völlig aus. Da die Bedrohung einer Viren- und Wurminfektion beim Mac-Rechner derzeit ohnehin nicht sehr hoch ist, hat man durch den Einsatz von Sophos Anti-Virus auch dieses Restrisiko gut unter Kontrolle.

Bartels, Goy

---

3. Zertifizierungsrichtlinien der GWDG-CA

3.1 Einleitung

In den GWDG-Nachrichten 5/2004 wurde bereits über den Aufbau einer Public-Key-Infrastruktur (PKI) in Göttingen berichtet. Eine PKI ermöglicht es u. a., reale Personen und ihre Identität auf digitale Identitäten eindeutig abzubilden und dabei die Authentizität zu gewährleisten. Die digitale Identität der Personen wird hierbei in Form eines Zertifikats verwaltet. Obwohl Zertifikate, einmal ausgestellt, bei ausreichender Schlüssellänge als fälschungssicher angesehen werden können, kann durch ein Zertifikat alleine noch nicht garantiert werden, dass für eine vermeintliche digitale Identität auch wirklich

ein korrektes Pendant in der Realität existiert. So kann z. B. theoretisch ein Zertifikat für eine fiktive Person ausgestellt werden.

Ein zusätzliches Problem ist die eindeutige Identifizierung des Zertifikatnehmers, nachdem für diesen ein korrektes Zertifikat ausgestellt wurde. Zertifikate beinhalten den öffentlichen Schlüssel eines asymmetrischen Schlüsselpaares einer Identität bzw. einer Person. Signiert diese nun eine Information mit ihrem privaten Schlüssel, so kann die Authentizität der Informationen sowie der Person später anhand dieses öffentlichen Schlüssels eindeutig überprüft werden. Das Vertrauen in die Signatur setzt jedoch voraus, dass der private Schlüssel tatsächlich „privat“ verwendet wird bzw. geheim ist und sich nicht im Besitz eines unbekannten Dritten befindet.

Diese Probleme zeigen u. a., dass eine PKI von der technischen Seite her allein nicht ausreichend ist, um Sicherheit und Authentizität in der digitalen Welt der IT zu garantieren. Es sind in jedem Fall zusätzlich organisatorische Vorgaben erforderlich.

Die GWDG begründet ihre PKI daher, gemäß dem X.509-Standard, auf ein Regelwerk für die Zertifizierung (auch Zertifizierungsrichtlinien, Policy oder Certificate Practice Statement, kurz CPS, genannt). Dieses Regelwerk bzw. Dokument umfasst Vorgaben, an die sich sowohl die GWDG als Aussteller von Zertifikaten als auch die Zertifikatsnehmer halten müssen, um u. a. die eingangs geschilderten Probleme zu unterbinden.

Während der Beantragung eines Zertifikats werden diese Zertifizierungsrichtlinien vor dem Ausstellen des Zertifikats durch den neuen Teilnehmer anerkannt. Die Policy der GWDG-CA (CA = Certification Authority / Zertifizierungsstelle) kann unter

`https://ca.gwdg.de/policy`

nachgelesen werden. Unter

`http://ca.gwdg.de/request`

kann außerdem ein eigenes Zertifikat beantragt und damit der beschriebene Ablauf nachvollzogen werden.

Ausgestellte Zertifikate beinhalten einen Verweis auf die ihnen zugeordnete Policy. Mit OpenSSL kann dieser Verweis durch

```
openssl x509 -in zertifikat-name.pem
-text
```

(siehe **`X509v3 Certificate Policies:`**)

angezeigt werden. Unter Windows verweist der Dialog für die Anzeige eines Zertifikats auf die zugehörigen Zertifizierungsrichtlinien (Ausstellererklärung).

In beiden Fällen wird der Benutzer, der die Gültigkeit des Zertifikats und dessen Qualität bewerten möchte, auf die Web-Seite der GWDG-CA mit der zugehörigen Policy weitergeleitet:

`https://ca.gwdg.de/policy`

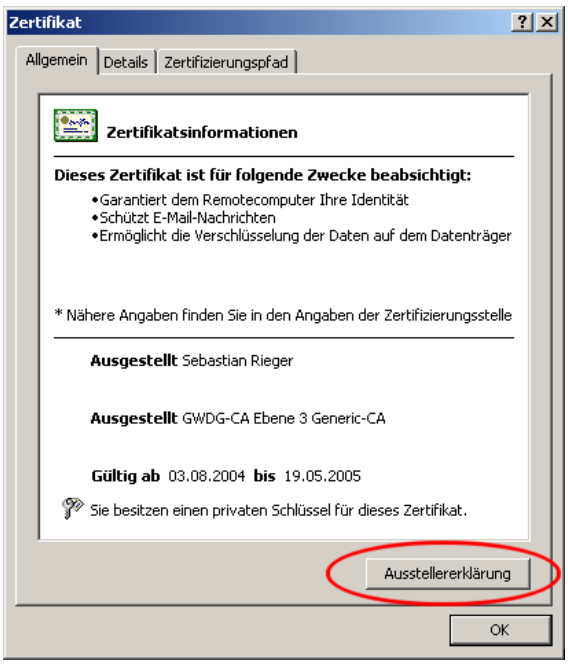


Abb. 1: Anzeige der Zertifizierungsrichtlinien eines Zertifikats unter Windows

Die Policy der GWDG-CA basiert auf den Vorgaben der DFN-PCA als höchste Zertifizierungsinstanz des Vereins zur Förderung eines Deutschen Forschungsnetzes e. V. in der Version 1.4. Sie erweitert diese Policy zusätzlich um für die GWDG relevante Details. Die Policy der GWDG-CA ist sowohl für den Betrieb der GWDG-CA selbst als auch für alle untergeordneten Zertifizierungsstellen bindend.

Die folgenden Abschnitte nennen einige wesentliche Vorgaben der Zertifizierungsrichtlinien der GWDG-CA und beschreiben ihre Anwendung.

3.2 Zertifizierungsregeln und Identifizierung

Während der Zertifizierung wird von der GWDG-CA ein eindeutiger Name für die dem Zertifikat zugewiesene Identität vergeben. Die Namensgebung erfolgt dabei anhand des aus X.500 und heutigen LDAP-Stukturen bekannten „Distinguished Name“. So würde ein Zertifikat für Max Mustermann beispielsweise den eindeutigen Namen (distinguished name) **`CN=Max Mustermann,O=Gesellschaft fuer wissenschaftliche Datenverarbeitung,L=Goettingen,C=DE`** erhalten. Max Mustermann würde hiermit der Organisation (**`O`**) „Gesellschaft für wissenschaftliche Datenverarbeitung“ in (**`L`** für Locality) Göttingen in (**`C`** für Country) Deutschland zugeordnet.

Durch diese eindeutige Bezeichnung können Identitäten anhand ihrer Zertifikate einheitlich nachvollzogen werden. Die wichtigste Funktion nimmt hierbei das Attribut **CN** (für Common Name) als gebräuchlicher Name ein. Dieses Attribut wird später bei der Verwendung des Zertifikats angezeigt und nennt den Besitzer des Zertifikats.

Jedem Zertifikat wird außerdem eine Seriennummer zugewiesen, die von der Zertifizierungsstelle einmalig vergeben wird. Die Zertifizierungsstelle begrenzt ebenfalls die Lebensdauer des Zertifikats, indem ein Ablaufdatum für dieses definiert wird.

Die beschriebenen Maßnahmen sorgen somit dafür, dass der Besitzer eines Zertifikats eindeutig erkennbar ist, sein Zertifikat genau einmal bei der Zertifizierungsstelle vorliegt und damit überprüfbar ist sowie seine Lebensdauer begrenzt wird. Trotzdem kann die Zuweisung dieser digitalen Identität z. B. zu einer realen Person noch nicht eindeutig nachgewiesen werden. Das fiktive Zertifikat für Herrn Max Mustermann könnte ordnungsgemäß nach diesen Vorgaben erstellt werden, ohne dass Herr Mustermann real existiert.

Aus diesem Grund beinhalten die Zertifizierungsrichtlinien der GWDG den Vorgang der Identitätsprüfung. Derzeit wird hierbei vom DFN-Verein eine persönliche Identifizierung vorausgesetzt. Ein Zertifikatnehmer muss sich während der Stellung eines Zertifizierungsantrags persönlich mittels Lichtbildausweis (bzw. amtlichem Dokument) identifizieren. Die digitale Identität einer Person wird dadurch eindeutig ihrer realen Identität zugeordnet. Zu diesem Zweck wird von dem elektronisch eingereichten Zertifizierungsantrag ein digitaler Fingerabdruck angefertigt, den der Antragsteller während der Zertifizierung bestätigt.

In der nahen Zukunft wird der DFN zusätzlich auch die Identifizierung von Benutzern über alternative Verfahren wie z. B. per E-Mail zulassen. Nach diesem Verfahren ausgestellte Zertifikate weisen jedoch ein wesentlich geringeres Sicherheitsniveau auf und werden daher z. B. nur für die E-Mail-Kommunikation zugelassen.

3.3 Sicherheitsanforderungen

Im vorherigen Abschnitt wurde die persönliche Identifizierung der Zertifikatnehmer während der Antragstellung als Voraussetzung für die erfolgreiche Zertifizierung beschrieben. Diese Identitätsprüfung findet nur einmalig während der Zertifizierung statt. Anhand des Zertifikats soll allerdings auch bzw. insbesondere nach der Antragstellung eine Identitätsprüfung ermöglicht werden.

Damit hierbei die digitale Identität nicht von einem Dritten genutzt werden kann, muss der private Schlüssel, der zum im Zertifikat enthaltenen öffentlichen Schlüssel gehört, sicher verwahrt und verwendet werden. Dies gilt sowohl für den Zertifikatnehmer als auch für die Zertifizierungsstelle. Käme beispielsweise der private Schlüssel einer Zertifizierungsstelle der GWDG-CA in die Hände eines Dritten, so könnte dieser nicht nur die Identität dieser Zertifizierungsstelle vortäuschen, sondern zusätzlich eigene Zertifikate mit beliebigem Inhalt unter falschem Namen ausstellen und veröffentlichen.

Die Policy der GWDG-CA definiert daher Sicherheitsanforderungen für die GWDG-CA, untergeordnete Zertifizierungs- und Registrierungsstellen sowie zertifizierte Benutzer und Endgeräte.

Für Zertifizierungsstellen der GWDG-CA wird hierbei beispielsweise vorgeschrieben, dass das Schlüsselpaar bzw. der private Schlüssel geeignet vor Missbrauch zu schützen ist. Der Zugriff auf den privaten Schlüssel muss zusätzlich durch ein mindestens acht Zeichen langes, nicht triviales Passwort kontrolliert werden. Die kleinste mögliche Schlüssellänge innerhalb der GWDG-CA ist zusätzlich auf 1024 Bit (für RSA, sonst für äquivalente Sicherheit) begrenzt. Dadurch wird vermieden, dass Dritte durch geeignete Fälschungsverfahren gewissermaßen einen „Zweitschlüssel“ zum Zertifikat anfertigen können.

Um den Missbrauch des privaten Schlüssels zu verhindern, bietet sich zusätzlich die Verwendung einer Smart Card oder eines USB-Tokens an. Der private Schlüssel wird dabei im Idealfall direkt auf der Smart Card oder dem Token erzeugt und kann von diesem nicht ausgelesen oder kopiert werden. Nach außen können über die Karte oder das Token lediglich Operationen wie die Entschlüsselung oder Signatur von Daten genutzt werden, die intern den privaten Schlüssel verwenden.

Auch für Smart Cards und Tokens ist dabei die Verwendung einer mindestens acht Zeichen langen, nicht-trivialen Zeichenfolge als PIN in der Policy der GWDG-CA vorgeschrieben. Um den privaten Schlüssel zum Zertifikat zu verwenden, ist somit der Zugriff auf das Token bzw. die Karte sowie die Kenntnis der PIN erforderlich.

Generell sollten private Schlüssel und der Zugriff auf sie im Betriebssystem geeignet geschützt werden. Dieser Schutz sollte neben dem Schutz vor Missbrauch auch eine Sicherung des privaten Schlüssels einschließen. Werden mit dem Schlüssel unwiederbringliche Daten ver- bzw. entschlüsselt, so hat ein Verlust des Schlüssels fatale Folgen.

Die GWDG wird hierfür in naher Zukunft Schlüsselarchivierungsmechanismen anbieten, die ausschließlich von den Benutzern verwendet werden können. Hierfür trifft der DFN-Verein derzeit notwendige Vorgaben innerhalb seiner PKI.

3.4 Teilnehmererklärung

Um die Einhaltung der Zertifizierungsrichtlinien und insbesondere der im vorherigen Abschnitt genannten Sicherheitsanforderungen durch die Benutzer zu garantieren, müssen alle Antragsteller von neuen Zertifikaten (Benutzer, Administratoren und Betreiber von Endgeräten etc.) eine Teilnehmererklärung unterzeichnen, in der sie sich verpflichten, den Missbrauch ihres Zertifikats bzw. ihres privaten Schlüssels zu verhindern und eine eventuelle Kompromittierung umgehend der GWDG-CA zu melden. In diesem Fall wird das Zertifikat von der GWDG-CA öffentlich gesperrt. Die GWDG-CA bietet hierfür öffentliche Sperrlisten an, auf die Programme, die eine PKI nutzen, über das World Wide Web sowie weitere Verzeichnisdienste direkt zugreifen können.

Der Antragsteller versichert in seiner Teilnehmererklärung zusätzlich, den Schlüssel persönlich erstellt zu haben, und eventuelle Änderungen der im Zertifikat enthaltenen Informationen (z. B. die Änderung des Nachnamens, E-Mail Adresse o. ä.) der GWDG-CA mitzuteilen. Die GWDG-CA verpflichtet sich ihrerseits, das Zertifikat des Benutzers (inkl. dem öffentlichen Schlüssel) zu veröffentlichen und damit eine Überprüfung des öffentlichen Schlüssels durch Dritte zu ermöglichen, sofern der Antragsteller nicht explizit einer Veröffentlichung widerspricht.

Um die unterzeichnete Teilnehmererklärung eindeutig der digitalen Identität des Antragstellers und damit dem beantragten Zertifikat zuzuordnen, wird von dem elektronisch übermittelten Zertifizierungsantrag ein digitaler Fingerabdruck erzeugt, den der Antragsteller durch seine Unterschrift bestätigt.

Erst die Anerkennung der Policy und die Einhaltung der in ihr enthaltenen Vorgaben bildet somit die sichere Vertrauensbasis einer Public-Key-Infrastruktur. Basierend darauf kann nicht zuletzt durch Verschlüsselungs- und Signaturtechniken die Sicherheit im IT-Umfeld deutlich gesteigert werden.

Literaturverweise und weitere Informationen

Understanding PKI, Addison-Wesley Professional, 2002

DFN Policy-based Certification Authority (PCA), World Wide Web Policy

`http://www.dfn-pca.de/certification/policies/x509policy.html`

ITU-T Recommendation X.509 (1997 E): Information Technologie – Open Systems Interconnection – The Directory: Authentication Framework

Informationen zur Zertifizierungstelle der GWDG (Policy, Zertifikate, Sperrlisten usw.) unter:

`https://ca.gwdg.de`

Rieger

---

4. Die Web-Schnittstelle zum zentralen Drucker-Server der GWDG

4.1 Einleitung

Für alle von der GWDG betriebenen Monochrom- und Farbdrucker werden die von den Nutzern eingestellten Druckaufträge auf einem zentralen Server verwaltet. Zurzeit handelt es sich um ein Pentium-Xeon-Doppelprozessorsystem mit 2,4-GHz-Prozessoren, 2 GB Hauptspeicher und 290 GB Plattenkapazität, das unter dem UNIX-Derivat FreeBSD betrieben wird.

Seit einigen Jahren steht auf dem Drucker-Server eine Web-Schnittstelle zur Verfügung, deren Funktionen schrittweise ausgebaut wurden. Benutzer können hiermit beispielsweise den Status der Warteschlangen ermitteln, eine Druckvorschau für PostScript-Dateien anfordern und seit kurzer Zeit auch Druckaufträge absetzen.

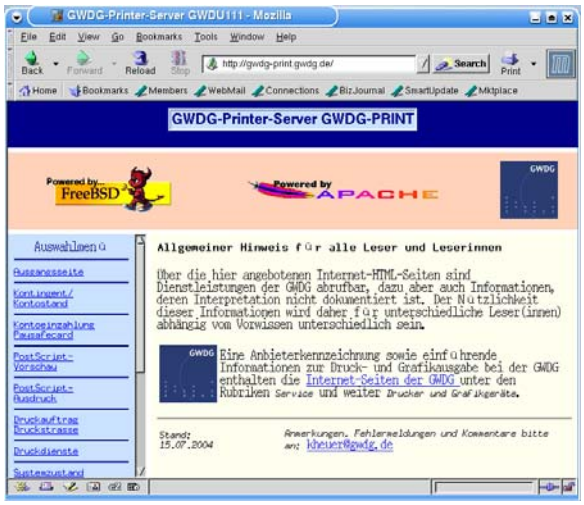


Abb. 1

Die Web-Schnittstelle ist über die Adresse

`http://gwdg-print.gwdg.de`

aufrufbar und soll im Folgenden in ihren wichtigtsten Bestandteilen beschrieben werden.

Nach dem Aufruf zeigt sich dem Nutzer eine Startseite mit einem Auswahlmenü im linken Teil des Browser-Fensters (hier und nachfolgend wird Mozilla als Browser verwendet); die Startseite enthält einige allgemeine Hinweise. Das Auswahlmenü bietet eine Reihe von Möglichkeiten an, die nachfolgend teilweise kurz und teilweise ausführlicher dargestellt werden.

4.2 Ausgangsseite

Dieser Menüpunkt führt bei Bedarf zur Startseite zurück.

4.3 Kontingent/Kontostand

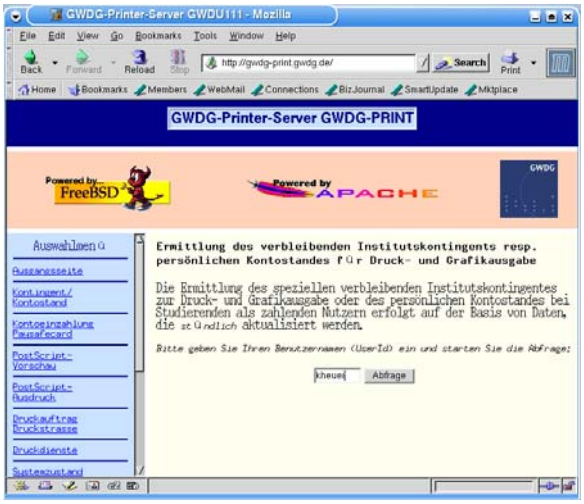


Abb. 2

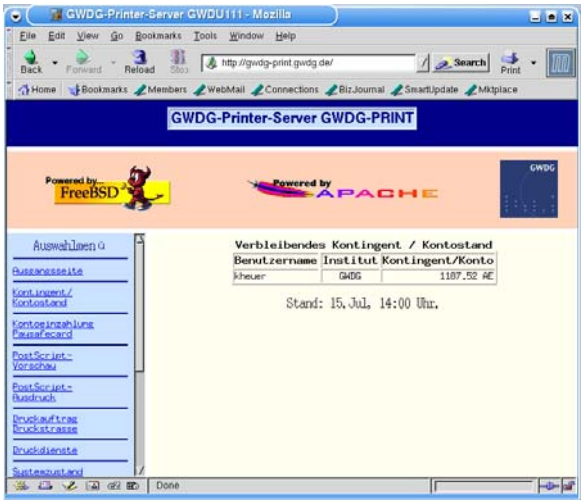


Abb. 3

GWDG-Nutzer erhalten hier Auskunft über den Stand des Druckkontingents ihres Institutes, studentische Nutzer über ihr persönliches Druckkonto. Nach Eingabe des Benutzernamens (s. Abb. 2) wird in einer kleinen Tabelle (s. Abb. 3) das Resultat angezeigt. Die zugrunde liegende Informationsquelle über die Kontenstände wird stündlich aktualisiert.

4.4 Kontoeinzahlung Paysafecard

Studierende, die eine „Paysafecard“ besitzen, können über diese Funktion Geld auf ihr persönliches Druckkonto einzahlen.

4.5 PostScript-Vorschau

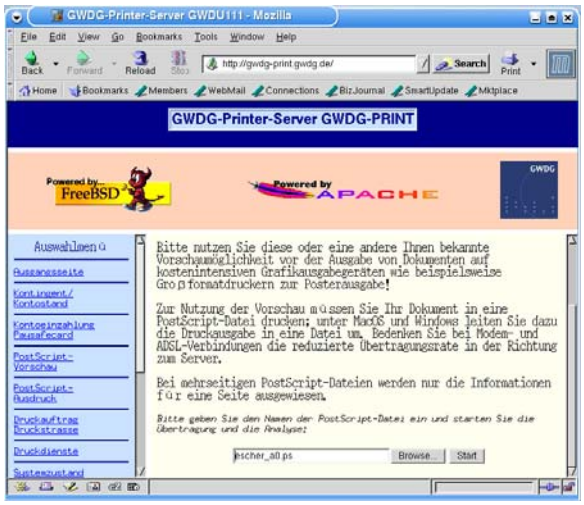


Abb. 4

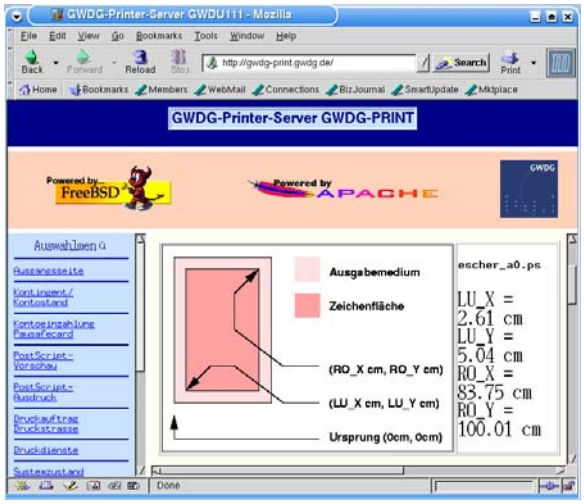


Abb. 5

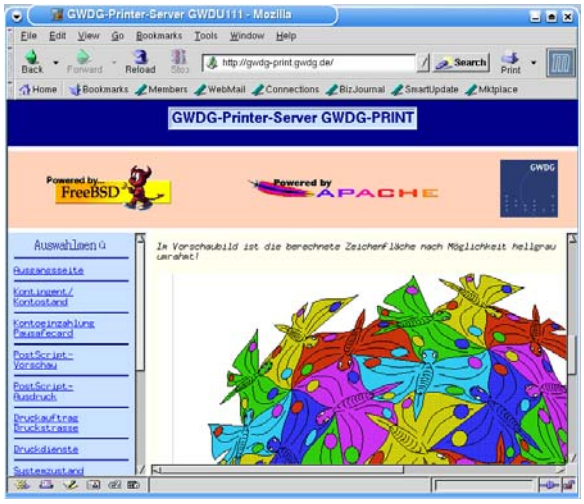


Abb. 6

Über diesen Menüpunkt kann eine PostScript-Datei vom Arbeitsplatzrechner des Benutzers auf den Drucker-Server übertragen werden. Mittels des Programms Ghostscript werden dort die maximalen Abmessungen des Ausdrucks und ein Vorschaubild der ersten (oder einzigen) Seite berechnet. Abb. 4 zeigt das Eingabefeld für den Dateinamen (über eine Schaltfläche kann auch eine Datei per Maus ausgewählt werden). In Abb. 5 sind die ermittelten Druckabmessungen der Beispieldatei erkennbar (hier für einen Großformatdruck), und in Abb. 6 ist ein Teil des Vorschaubildes dargestellt. Insbesondere vor der Nutzung teurer Ausgabegeräte, z. B. eines Großformatdruckers, lohnen sich oft die Berechnung der Abmessungen und das Kontrollieren des Vorschaubildes, um Fehldrucke zu vermeiden.

4.6 PostScript-Ausdruck

Die Möglichkeit, PostScript-Dateien aus dem Browser vom Arbeitsplatzrechner zum Drucker-Server zu übertragen und anschließend zu drucken, ist neu. Bei Anwahl dieses Menüpunktes wird die Verbindung zwischen beiden Rechnern auf eine verschlüsselte Verbindung umgeleitet, da eine Benutzeranmeldung erforderlich ist (s. Abb. 8).

In Abb. 7 ist der Erläuterungstext dargestellt, der über Hypertext-Verbindungen die Möglichkeit eröffnet, ein Einrichtungsprogramm mit Druckerbeschreibungsdatei auf den Arbeitsplatzrechner zu kopieren, um auf Microsoft-Windows-Systemen einen PostScript-Druckertreiber einzurichten und PostScript-Dateien erzeugen zu können.

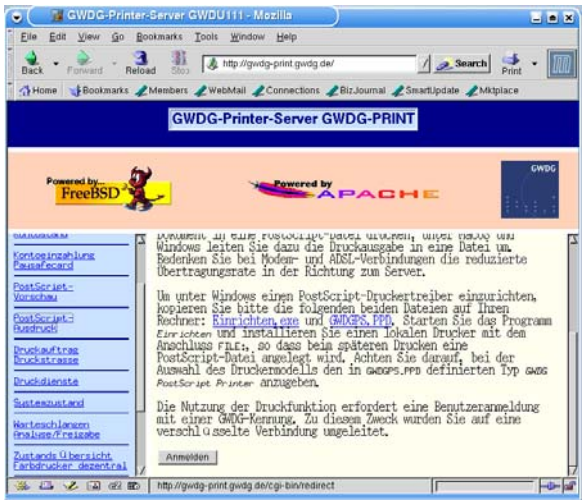


Abb. 7

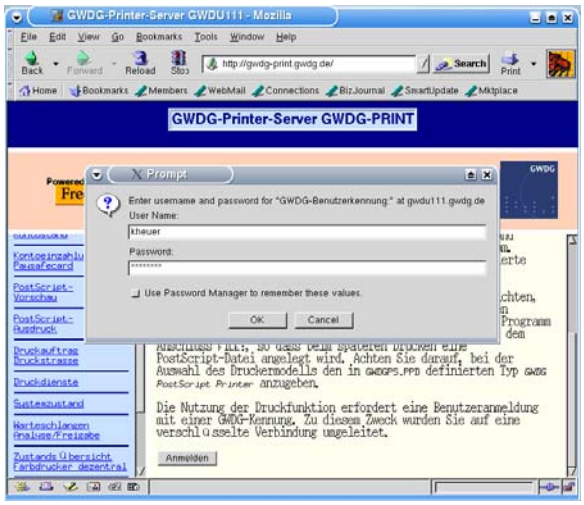


Abb. 8

Nach der Benutzeranmeldung können ein Warteschlangenname und eine zu druckende PostScript-Datei ausgewählt werden, wie in Abb. 9 zu erkennen ist.

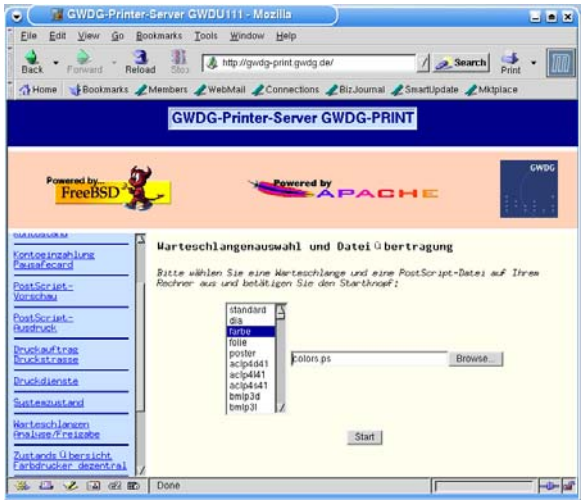


Abb. 9

Die Betätigung der Schaltfläche „Start“ bewirkt die Dateiübertragung und den anschließenden Druckbefehl, der im Browser angezeigt wird (hier nicht dargestellt).

4.7 Druckauftrag Druckstraße

Diese Funktion steht aus technischen Gründen leider zurzeit nicht zur Verfügung. Sie bietet die Möglichkeit, einen Broschüren-Druckauftrag per E-Mail und Dateiübertragung an die GWDG zu übermitteln.

4.8 Druckdienste

Der Drucker-Server bietet Druckdienste über verschiedene Netzwerkprotokolle an. Hier kann sich der Nutzer schnell einen Überblick verschaffen (s. Abb. 10), ob die Dienste auf dem Drucker-Server verfügbar sind oder ob eine Betriebsstörung auf dem Server selbst vorliegt.

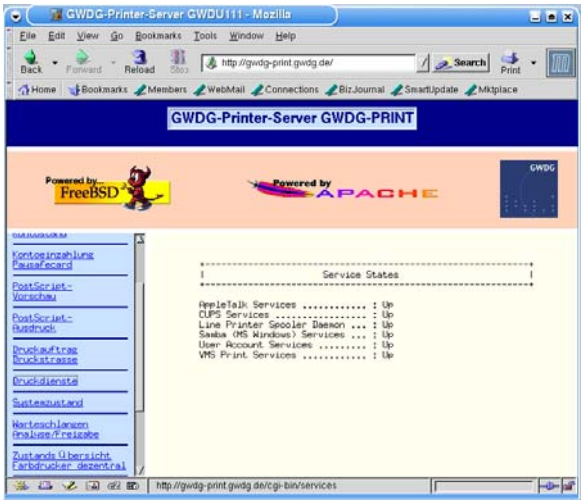


Abb. 10

4.9 Systemzustand

Die aktuelle Systembelastung des Drucker-Servers ist über diesen Punkt abrufbar.

4.10 Warteschlangen Analyse/Freigabe

Jedem Nutzer ist es möglich, nach Auswahl einer Warteschlange deren Status oder Füllung abzufragen oder die zugehörige Protokolldatei einzusehen. Von bestimmten, privilegierten Rechnern aus kann das Bedienpersonal auch Druckaufträge entfernen oder die Ausgänge geschlossener Warteschlangen öffnen. Das Einsehen der Protokolldateien ist aufgrund der eingetragenen Fehlermeldungen bei der Fehleranalyse hilfreich, wenn Ausdruckversuche fehlgeschlagen sind.

4.11 Zustandsübersichten zu den zentralen und dezentralen Farb- und S/W-Druckern

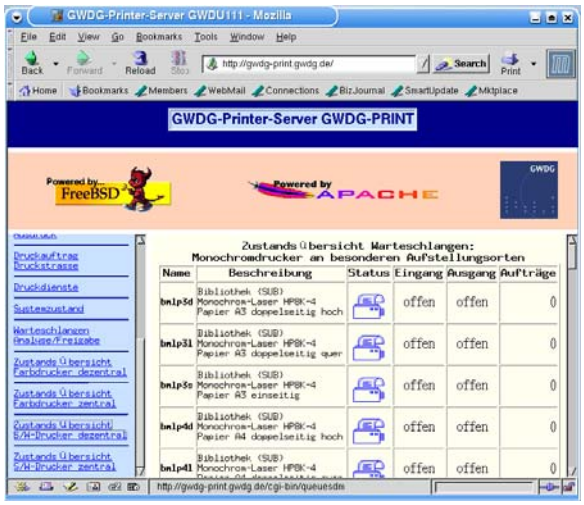


Abb. 11

Die insgesamt über 130 Druckerwarteschlangen der GWDG sind, nach Gerätetyp und Aufstellungsort gegliedert, über diesen Menüpunkt schnell kontrollierbar. Abb. 11 zeigt als Beispiel einige Warteschlangen für einen dezentral aufgestellten Monochromdrucker. Neben Namen und ausführlicher Beschreibung der Warteschlangen sind die Zustände von Ein- und Ausgängen und die Zahl der vorliegenden Druckaufträge dargestellt. Die Farbe der Druckersymbole charakterisiert den Zustand: blau bedeutet inaktiv, grün aktiv und rot kennzeichnet einen geschlossenen Ein- oder Ausgang. Bei geschlossenen Eingängen sind keine Druckaufträge einreihbar, bei geschlossenen Ausgängen werden keine Aufträge abgearbeitet.

4.12 Anmerkung zum Zugriffsschutz und zur Implementation

Bei vielen Seiten von

`http://gwdg-print.gwdg.de`

besteht eine Zugriffsbeschränkung auf Rechner mit Internet-Adressen im GÖNET-Bereich. Ausgenommen ist u. a. die Funktion zum Drucken von PostScript-Dateien, da hier eine Benutzeranmeldung den Zugang kontrolliert. Da Browser sich i. d. R. eine erfolgreiche Benutzeranmeldung „merken“, ist der Anmeldevorgang (nebenbei bemerkt) nach jedem Start des Browsers nur einmal vorzunehmen.

Die meisten der auf dem Drucker-Server angebotenen Web-Seiten werden dynamisch durch CGI-Skripte erzeugt. Als Web-Server wird Apache eingesetzt, die Benutzeranmeldung erfolgt mittels des Moduls *mod_auth_ldap* gegen den OpenLDAP-Server der GWDG.

Heuer

---

5. Kurse des Rechenzentrums

5.1 Allgemeine Informationen zum Kursangebot der GWDG

5.1.1 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.

5.1.2 Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 21119 an die

GWDG
Kursanmeldung
Postfach 2841
37018 Göttingen

oder per E-Mail an die Adresse auftrag@gwdg.de mit der Subject-Angabe „Kursanmeldung“ erfolgen. Für die schriftliche Anmeldung steht unter

`http://www.gwdg.de/service/nutzung/antragsformulare/kursanmeldung.pdf`

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 authorisierte Person - oder Geschäftsführenden Direktor des Instituts vorgenommen werden. Die Anmeldefrist endet jeweils 7 Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit dem Dispatcher (Tel.: 0551 201-1523, E-Mail: auftrag@gwdg.de) möglich. Eine Anmeldebestätigung wird nur an auswärtige Insti-

tute oder auf besonderen Wunsch zugesendet. Falls eine Anmeldung wegen Überbelegung des Kurses nicht berücksichtigt werden kann, erfolgt eine Benachrichtigung.

5.1.3 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.

5.1.4 Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu 8 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.

5.1.5 Kursorte

Die meisten Kurse finden in Räumen der GWDG oder des Max-Planck-Instituts für biophysikalische Chemie statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Fassberg, 37077 Göttingen, der Große Seminarraum im Allgemeinen Institutsgebäude dieses Instituts. 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/gwdg/standort/lageplan`

zu finden. Der gemeinsame Schulungsraum von GWDG und SUB befindet sich im Untergeschoss der Niedersächsischen Staats- und Universitätsbibliothek, Platz der Göttinger Sieben 1, 37073 Göttingen.

5.1.6 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/service/kurse`

zu finden. Anfragen zu den Kursen können an den Dispatcher per Telefon unter der Nummer 0551 201-1524 oder per E-Mail an die Adresse auftrag@gwdg.de gerichtet werden. Zweimal jährlich wird ein Katalog mit dem aktuellen GWDG-Kursprogramm versendet. Interessenten, die in den Verteiler aufgenommen werden möchten, können dies per E-Mail an die Adresse gwdg@gwdg.de mitteilen.

5.2 Kurse von September bis Dezember 2004 in thematischer Übersicht

EDV-Grundlagen und Sonstiges

Kurse	Termine	Vortragende
Einführung in die Nutzung des Leistungsangebots der GWDG	• 15.09.2004 • 08.12.2004	Dr. Grieger Dr. Grieger
Einführung in Aufbau und Funktionsweise von PCs	• 13.09.2004	Eyßell
Führung durch das Rechnermuseum	• 17.09.2004 • 08.10.2004 • 12.11.2004 • 10.12.2004	Eyßell Eyßell Eyßell Eyßell

EDV-Grundlagen und Sonstiges

Kurse	Termine	Vortragende
Einführung in die Bedienung von Windows-Oberflächen	• 14.09.2004	Eyßell

Betriebssysteme

Kurse	Termine	Vortragende
Grundkurs UNIX/Linux mit Übungen	• 31.08.2004 - 02.09.2004 • 07.12.2004 - 09.12.2004	Hattenbach Hattenbach
Schnellkurs UNIX für Windows-Benutzer mit Übungen	• 29.11.2004 - 30.11.2004	Dr. Bohrer
Installation und Administration von UNIX-Systemen	• 14.12.2004 - 17.12.2004	Dr. Heuer, Dr. Sippel
UNIX für Fortgeschrittene	• 22.11.2004 - 24.11.2004	Dr. Sippel
Die Windows-Active-Directory-Domäne	• 06.10.2004 - 08.10.2004	Quentin
Windows XP für Systembetreuer	• 04.10.2004 - 05.10.2004	Quentin

Netze / Internet

Kurse	Termine	Vortragende
Das Internet als Werkzeug für die Biowissenschaften	• 15.10.2004	Dr. Liesegang
Sicherheit im Internet für Anwender	• 02.12.2004	Reimann
Web Publishing I	• 28.10.2004 - 29.10.2004	Reimann
XML	• 29.09.2004 - 01.10.2004	Reimann, Koch

Grafische Datenverarbeitung

Kurse	Termine	Vortragende
Arbeiten mit CAD, Grundlagen	• 06.09.2004 - 10.09.2004	Witt
CorelDRAW - Grundlagen	• 19.10.2004 - 20.10.2004	Wagenführ

Sonstige Anwendungssoftware

Kurse	Termine	Vortragende
Datenbanksystem MS Access, Einführung mit Übungen	• 22.11.2004 - 26.11.2004	Dr. Kneser
Anwendungen in Lotus Notes	• 26.10.2004 - 27.10.2004	Greber, Dr. Grieger

Sonstige Anwendungssoftware

Kurse	Termine	Vortragende
PowerPoint	• 21.12.2004 - 22.12.2004	Reimann
SAS - Grundlagen	• 09.11.2004 - 11.11.2004	Wagenführ
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN	• 11.10.2004 - 14.10.2004	Dr. Bohrer, Dr. Liesegang
Mit StarOffice zum Schwarzen Loch	• 12.11.2004	Dr. Grieger

Programmiersprachen

Kurse	Termine	Vortragende
Einführung in die Programmiersprache Fortran 90/95	• 27.09.2004 - 28.09.2004	Dr. Schwardmann
Programmierung von Parallelrechnern	• 02.11.2004 - 04.11.2004	Prof. Haan, Dr. Schwardmann

5.3 Kurse von September bis Dezember 2004 in chronologischer Übersicht

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Grundkurs UNIX/Linux mit Übungen	Hattenbach	31.08.2004 - 02.09.2004 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	24.08.2004	12
Arbeiten mit CAD, Grundlagen	Witt	06.09.2004 - 10.09.2004 09.00 - 16.00 Uhr, (am 06.09. ab 10.00 Uhr; am 10.09. bis 13.00 Uhr)	30.08.2004	20
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	13.09.2004 09.15 - 12.30 Uhr	06.09.2004	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	14.09.2004 09.15 - 12.30 Uhr und 13.30 - 16.00 Uhr	07.09.2004	4
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	15.09.2004 17.15 - 20.00 Uhr	08.09.2004	0
Führung durch das Rechner-museum	Eyßell	17.09.2004 10.00 - 12.00 Uhr	10.09.2004	0
Einführung in die Programmier-sprache Fortran 90/95	Dr. Schwardmann	27.09.2004 - 28.09.2004 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr	20.09.2004	8
XML	Reimann, Koch	29.09.2004 - 01.10.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	22.09.2004	12

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Windows XP für Systembetreuer	Quentin	04.10.2004 - 05.10.2004 09.15 - 15.30 Uhr	27.09.2004	8
Die Windows-Active-Directory-Domäne	Quentin	06.10.2004 - 08.10.2004 09.15 - 15.30 Uhr	29.09.2004	12
Führung durch das Rechner-museum	Eyßell	08.10.2004 10.00 - 12.00 Uhr	01.10.2004	0
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN	Dr. Bohrer, Dr. Liesegang	11.10.2004 - 14.10.2004 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	04.10.2004	16
Das Internet als Werkzeug für die Biowissenschaften	Dr. Liesegang	15.10.2004 09.30 - 12.30 Uhr und 13.30 - 16.00 Uhr	08.10.2004	4
CorelDRAW - Grundlagen	Wagenführ	19.10.2004 - 20.10.2004 09.15 - 12.00 Uhr und 13.30 - 16.30 Uhr	12.10.2004	8
Anwendungen in Lotus Notes	Greber, Dr. Grieger	26.10.2004 - 27.10.2004 09.15 - 16.30 Uhr	19.10.2004	8
Web Publishing I	Reimann	28.10.2004 - 29.10.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	21.10.2004	8
Programmierung von Parallel-rechnern	Prof. Dr. Haan, Dr. Schwardmann	02.11.2004 - 04.11.2004 09.15 - 12.15 Uhr und 14.00 - 17.00 Uhr	26.10.2004	12
SAS - Grundlagen	Wagenführ	09.11.2004 - 11.11.2004 09.15 - 12.00 Uhr und 13.30 - 16.30 Uhr	02.11.2004	12
Führung durch das Rechner-museum	Eyßell	12.11.2004 10.00 - 12.00 Uhr	05.11.2004	0
Mit StarOffice zum Schwarzen Loch	Dr. Grieger	12.11.2004 09.15 - 12.00 Uhr	05.11.2004	2
Datenbanksystem MS Access, Einführung mit Übungen	Dr. Kneser	22.11.2004 - 26.11.2004 09.00 - 12.00 Uhr	15.11.2004	10
UNIX für Fortgeschrittene	Dr. Sippel	22.11.2004 - 24.11.2004 09.15 - 12.00 Uhr und 13.15 - 15.30 Uhr	15.11.2004	12
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	29.11.2004 - 30.11.2004 13.30 - 16.30 Uhr	22.11.2004	4
Sicherheit im Internet für Anwender	Reimann	02.12.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	25.11.2004	4
Grundkurs UNIX/Linux mit Übungen	Hattenbach	07.12.2004 - 09.12.2004 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	30.11.2004	12

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	08.12.2004 17.15 - 20.00 Uhr	01.12.2004	0
Führung durch das Rechner-museum	Eyßell	10.12.2004 10.00 - 12.00 Uhr	03.12.2004	0
Installation und Administration von UNIX-Systemen	Dr. Heuer, Dr. Sippel	14.12.2004 - 17.12.2004 09.30 - 12.00 Uhr und 13.30 - 16.30 Uhr	07.12.2004	16
PowerPoint	Reimann	21.12.2004 - 22.12.2004 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	14.12.2004	8

6. Betriebsstatistik Juli 2004

6.1 Nutzung der Rechenanlagen

Rechner	Zahl der Prozessoren	CPU-Stunden
DECalpha	12	1.818,34
IBM RS/6000 SP	224	97.126,20
IBM Regatta	96	36.521,28
Linux Parallel	198	128.563,57

6.2 Betriebsunterbrechungen

Rechner/PC-Netz	Störungen		System-pflege	
	Anzahl	Stunden	Anzahl	Stunden
UNIX-Cluster	1	1,60	0	
IBM SP/Regatta	1	41,50	0	
Linux Parallel	1	19,50	0	
PC-Netz	1	1,60	0	
Nameserver	0		0	
Mailer	2	2,10	2	0,60

7. Autoren dieser Ausgabe

Name	Artikel	E-Mail-Adresse / Telefon-Nr.
Holger Bartels	• Sophos Anti-Virus für Mac OS X	hbartel2@gwdg.de 0551 201-1830
Nicole Goy	• Sophos Anti-Virus für Mac OS X	ngoy@gwdg.de 0551 201-1557
Dr. Konrad Heuer	• Die Web-Schnittstelle zum zentralen Drukker-Server der GWDG	kheuer@gwdg.de 0551 201-1540
Michael Reimann	• Sophos-Update-Service unterstützt nun auch Linux und Max OS	mreiman1@gwdg.de 0551 201-1826
Sebastian Rieger	• Zertifizierungsrichtlinien der GWDG-CA	srieger1@gwdg.de 0551 201-1878