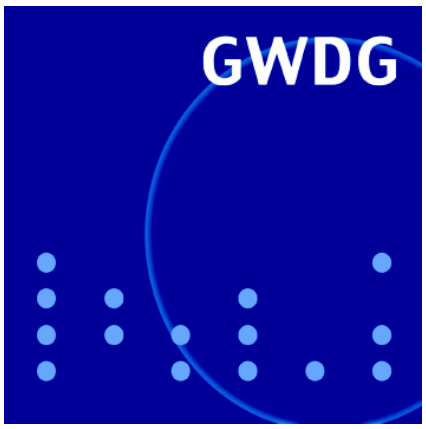

OpenLDAP-Server

Mac OS X 10.4 Tiger

RDP über SSL bei Windows Server 2003

allegro V25

GWDG Nachrichten

7 / 2005

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Inhaltsverzeichnis

GWDG-Nachrichten für die Benutzer des Rechenzentrums

ISSN 0940-4686

28. Jahrgang, Ausgabe 7 / 2005

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

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

Redaktion und Herstellung: Dr. Thomas Otto Tel.: 0551 201-1828, E-Mail: Thomas.Otto@gwdg.de

1. Der OpenLDAP-Server der GWDG – Teil II

1.1 Einleitung

Der erste Teil dieses Beitrags, welcher in der letzten Ausgabe der GWDG-Nachrichten enthalten war, gab eine allgemeine Einführung in die Begriffe Verzeichnisdienst, LDAP und OpenLDAP.

Dieser zweite Teil beschreibt die OpenLDAP-Server der GWDG und die Daten, welche dort verzeichnet sind.

1.2 OpenLDAP-Server

OpenLDAP ist auf unterschiedlichen UNIX-Varianten sowie Linux einsetzbar. Die GWDG betreibt OpenLDAP-Server unter FreeBSD und Linux.

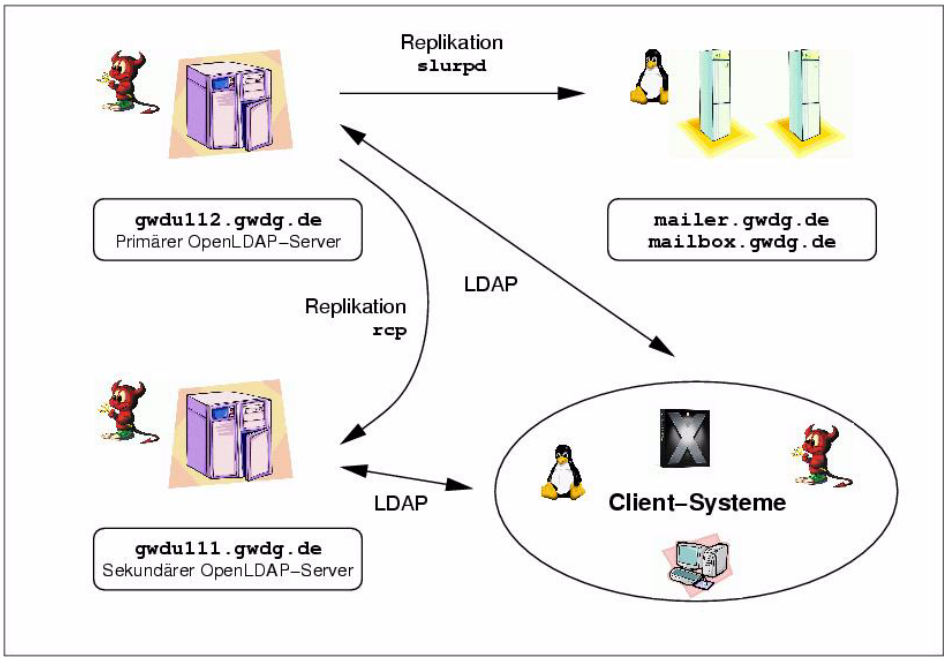

Abb. 1: OpenLDAP-Server der GWDG

Abb. 1 zeigt die Zusammenhänge zwischen den von der GWDG betriebenen OpenLDAP-Servern und -Klienten, wobei das jeweilige Betriebssystem durch Symbole angedeutet wird (Daemon – FreeBSD, Pinguin – Linux, X – Mac OS X).

Der primäre Server **gwdu112** ist die Quelle aller Verzeichnisdaten; der Abgleich mit der traditionellen UNIX-Benutzerdatenbank der GWDG erfolgt zurzeit mit Hilfe kleiner Programme.

Zur Erhöhung der Ausfallsicherheit und zur Verteilung der Last werden zusätzliche OpenLDAP-Server verwendet, welche die Verzeichnisdaten per Replikation übermittelt bekommen.

OpenLDAP bietet zwei Mechanismen zur Replikation an: Zum einen kann der primäre Server über ein als UNIX-Daemon laufendes Programm **slurpd** alle Änderungen zeitnah an sekundäre Server weitergeben, oder diese holen periodisch Änderungen beim primären Server ab (sog. *sync replication*). Das zweite Verfahren ist relativ neu und gilt als noch nicht stabil genug.

Die **slurpd**-Replikation wird verwendet, um die OpenLDAP-Server auf den Linux-Mail-Systemen der GWDG zu aktualisieren. Die Mailserver sind selbst OpenLDAP-Klienten mit einem hohen Lastpotenzial und wenden sich an ihre eigenen exklusiven Replikationsserver, um die Last nicht anderen Servern aufzubürden und auch bei Ausfall der anderen OpenLDAP-Server oder der Netzwerkkommunikation dorthin autonom weiterarbeiten zu können.

Da auch die **slurpd**-Replikation in seltenen Fällen zu Inkonsistenzen führen kann, kopiert der sekundäre OpenLDAP-Server **gwdu111** periodisch die kompletten Datenbanken, auf die sich OpenLDAP stützt, per **rcp**-Befehl von dem Rechner **gwdu112**. Beide Rechner sind u. a. zu diesem Zweck unmittelbar über separate Netzwerkadapter und ein gekreuztes Netzwerkkabel verbunden.

Abgesehen von den Linux-Mail-Systemen wenden sich alle OpenLDAP-Klienten an die Server **gwdu112** und **gwdu111**.

Der Zugang zu den Verzeichnisdaten ist bis auf einzelne Ausnahmen auf Rechner im IP-Adressbereich des GÖNET beschränkt.

1.3 OpenLDAP-Klienten

Insbesondere viele der bei der GWDG im Einsatz befindlichen Linux-Systeme, an erster Stelle zu nennen die Knoten der als Parallelrechner betriebenen Compute-Cluster, verwenden OpenLDAP zur Benutzeranmeldung und -verwaltung. Hinzu kommen einige Spezialdienste wie Lotus- oder Apache-Web-Server.

In Abb. 2 ist dargestellt, dass der Server **`gwdu112`** an einem typischen Wochentag zurzeit durchschnittlich etwa 50 gleichzeitige Zugriffe von Klienten auf das Verzeichnis bewätigen muss, es aber durchaus auch Spitzenwerte mit bis zu 300 gleichzeitigen Zugriffen gibt.

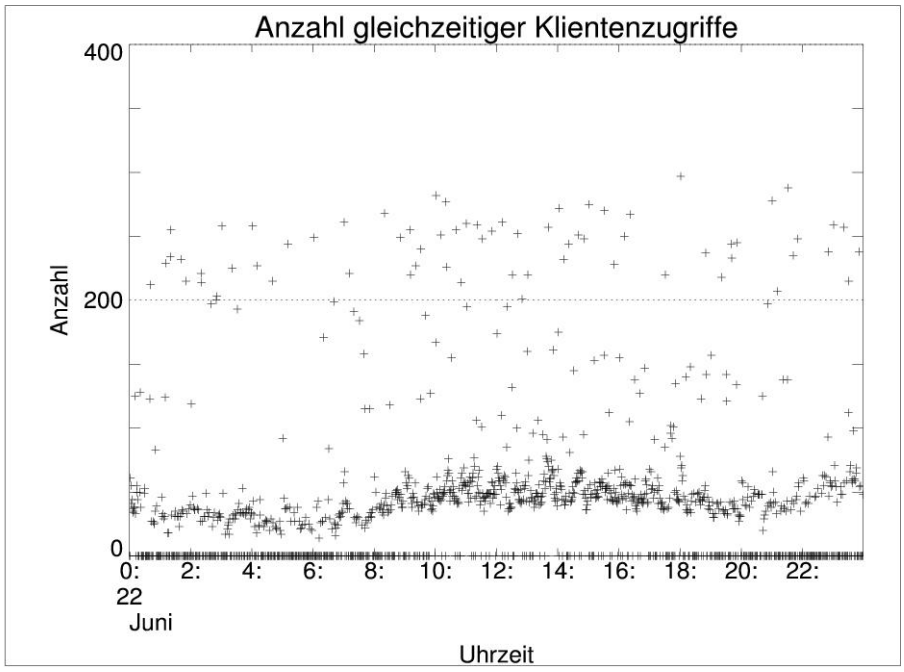

Abb. 2: Anzahl gleichzeitiger Klientenzugriffe auf den OpenLDAP-Server gwdu112 am 22.06.2005

1.4 Verzeichnisdaten

In Abb. 3 ist ein Beispieleintrag für eine GWDG-Kursbenutzerkennung dargestellt. Bislang beinhaltet das von OpenLDAP verwaltete Verzeichnis hauptsächlich Daten, die für eine Benutzeranmel-

dung unter UNIX (z. Z. nur FreeBSD oder Mac OS X) oder Linux benötigt werden.

```
dn: cn=4kurst00,ou=GKRS,ou=gwdgadm,dc=gwdg,dc=de
objectClass: inetOrgPerson
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetLocalMailRecipient
objectClass: GWDGuser
objectClass: top
cn: 4kurst00
cn: 4kurst00 Kursleiter(in)
gidNumber: 5050
ou: GKRS
gecos: 4kurst00 Kursleiter(in) ,,,
givenName: 4kurst00
mail: 4kurst00@gwdg.de
mailHost: -
mailPrefs: -
homeDirectory: /usr/users/4kurst00
loginShell: /bin/ksh
sn: Kursleiter(in)
uid: 4kurst00
uidNumber: 5265
userPassword:{crypt}4lq/F9j/UbOWg
```

Abb. 3: Beispiel für einen Verzeichniseintrag

Zu erkennen ist, dass ein Nutzer durch mehrere Objektklassen beschrieben wird, beispielsweise durch **posixAccount** und **shadowAccount**. Diese Objektklassen beinhalten ihrerseits Attribute wie **homeDirectory** und **loginShell**, die notwendig sind, damit OpenLDAP die Benutzerverwaltung für UNIX-Systeme übernehmen kann.

Ein großer Sicherheitsvorteil gegenüber der Benutzerverwaltung per NIS (Network Information System von SUN, früher *yellow pages* genannt) ist, dass das verschlüsselte Benutzerkennwort nur bei einer autorisierten Anmeldung am OpenLDAP-Server durch den Nutzer selbst oder einen besonders privilegierten Administrator sichtbar wird.

Interessierte Leser können das ausprobieren, indem sie auf einem Dialog-Server wie der **gwdu05**, der **gwdu60** oder der **gwdu101** folgenden Befehl eingeben:

```
ldapsearch -x uid=4kurst00
```

Anstelle von **4kurst00** kann auch der eigene Benutzername angegeben werden. Bei diesem Befehl erfolgt eine vollkommen unprivilegierte Gastanmeldung, so dass das verschlüsselte Kennwort nicht ausgeliefert wird.

Soll eine Anmeldung mit Benutzerrechten erfolgen, so wird der **ldapsearch**-Befehl recht länglich. Interessierte können einfacher auf der **gwdu60** das menügesteuerte Programm

```
ldapquery
```

aufrufen oder sich alternativ per Befehl

```
man ldapsearch
```

die Dokumentation von **ldapsearch** genauer anschauen.

Alle Nutzer der existierenden NIS-Datenbasis sind automatisch in das Verzeichnis übernommen worden, und die Einträge werden kontinuierlich gepflegt.

Noch für die nächsten Monate ist geplant, das OpenLDAP-Verzeichnis als primäre Datenquelle für die GWDG-Benutzerverwaltung einzusetzen und auch einen gewissen Abgleich mit dem *Active Directory* der Windows-Welt vorzunehmen. Dazu ist die Einführung einer ganzen Reihe weiterer Attribute erforderlich, die in Abb. 3 noch nicht zu erkennen sind. Sie sind in einem GWDG-eigenen sog. Schema definiert und der Objektklasse **GWDGuser** zugeordnet.

Ein weiterer Vorteil von OpenLDAP gegenüber NIS ist die Möglichkeit der hierarchischen Strukturierung der Benutzereinträge. Abb. 3 zeigt dies anhand des *distinguished name* (**dn**-Zeile ganz oben): Jedes Institut ist im Verzeichnis eine eigene Organisationseinheit (*organizational unit* – **ou,** im Beispiel **GKRS**), wodurch sich bei Bedarf Verantwortung für die jeweiligen Benutzereinträge leichter delegieren lässt. Auch kann der Zugriff von Klienten so auf ein einzelnes Institut begrenzt werden.

Bei der bereits erwähnten und in Kürze zu erwartenden Neustrukturierung des OpenLDAP-Verzeichnisses im Zuge der Übernahme der primären Benutzerdatenbankfunktion wird es sogar möglich sein, unterhalb der Institutsebene Abteilungen als zusätzliche Organisationseinheiten einzuführen, was für große Institute wie z. B. das Max-Planck-Institut für biophysikalische Chemie in Göttingen wichtig sein kann. Die gemeinsame Mitgliedschaft in einer UNIX-Gruppe (hier dann **MBPC**) bleibt davon unberührt.

Neben der übergeordneten Organisationseinheit **gwdgadm** für die GWDG-Benutzerverwaltung (ebenfalls in Abb. 3 zu erkennen) existieren andere Organisationseinheiten wie **gwdgovid** für die OVID-Benutzer der Max-Planck-Gesellschaft oder auch schon institutsspezifische Organisationseinheiten, die Instituten eine Absicherungsmöglichkeit für selbstbetriebene OpenLDAP-Server bieten können.

1.5 Ausblick

In Teil III dieses Beitrags, geplant für die August-Ausgabe der GWDG-Nachrichten, soll die Anbindung von Klientensystemen an die OpenLDAP-Server der GWDG beschrieben werden.

Heuer

2. Mac OS X 10.4 Tiger

2.1 Einleitung

Puma, Jaguar, Panther und jetzt also Tiger: Das Betriebssystem Mac OS X, das ausschließlich auf den Mac-Computern von Apple eingesetzt werden kann, ist jetzt in der Version 10.4 auf dem Markt.

Mac OS X 10.4 läuft auf allen Macs, die mindestens einen G3-Prozessor haben und über 256 MByte Arbeitsspeicher und mehr verfügen. Auf der Festplatte müssen mindestens noch 3 GByte Platz sein.

Was das neue Mac OS von anderen Systemen unterscheidet, sind die liebevollen Details. Im Finder von Mac OS X 10.4 kann man z. B. einen Brenn-Ordner über „Ablage > Neuer Brennordner“ oder das Kontextmenü der Maus anlegen. Dateien, die in dem Ordner liegen, lassen sich mit einem Klick auf einen Button rechts oben im geöffneten Fenster auf CD und DVD brennen.

Der Finder kann „intelligente Ordner“ anlegen, die sich als Ergebnisliste in der linken Spalte eines Finder-Fensters speichern lassen. Statt der Spaltenansicht zeigt der Ordner Miniaturen der Dateien als Vorschau auf den Inhalt an. Über Pfeilsymbole lassen sich Namen, Ordner, Vorschauen und Dokumenttypen ein- und ausblenden. Ein Klick auf den Dokumenttyp blendet in der Fußzeile in einer Reihe den Speicherort ein. Wer im Finder die gewohnte Tastenkombination Befehltaste-F drückt, kommt in die gleiche Maske wie zum Anlegen intelligenter Ordner; die Ergebnisliste lässt sich entsprechend in der linken Navigationsspalte speichern.

Über 200 neue Funktionen listet Apple auf. Am wichtigsten ist vermutlich die weiter verbesserte Zusammenarbeit mit Windows-Netzen und -PCs.

Einige der Highlights unter den Neuerungen werden im Folgenden näher erläutert.

2.2 Spotlight

Zu den Hauptattraktionen des Systems zählt die interne automatische Meta-Suche *Spotlight*. Nach der Installation von Mac OS X sieht man direkt in der rechten oberen Ecke des Bildschirms ein blaues Icon mit einer Lupe. Klickt man auf das Symbol, dann öffnet sich ein Eingabefeld für den Suchbegriff. Spotlight durchforstet die Datenbestände automatisch und sortiert die Informationen. Die Ergebnisse werden teilweise noch beim Eintippen des Wortes angezeigt.

Hier hat Apple eindeutig die Nase vorn, denn Windows will eine solche Desktop-Suche erst mit dem für 2006 erwarteten Systemupdate Longhorn anbieten.

Vor dem richtigen Einsatz muss das Dateisystem indiziert werden. Als Suchsyntaxe funktionieren nur die englischen Konjunktionen AND und OR. Die Suche in Anführungszeichen funktioniert hingegen anscheinend nur bei Dateinamen, nicht bei Volltextsuchen. Die systemweite Suchfunktion lässt sich nicht nur durch das Lupensymbol in der Menüleiste, sondern auch von anderen Stellen des Systems aus aufrufen: z. B. über ein Suchfeld in den Systemeinstellungen. Spotlight sucht nicht nur nach Dateinamen, sondern auch nach Metadaten und Dateiinhalten. Standardmäßig sucht Spotlight in 14 Kategorien: Programme, Systemeinstellungen, Dokumente, Ordner, E-Mails, Kontakte, Ereignisse und Aufgaben, Bilder, PDF-Dokumente, Lesezeichen, Musik, Filme, Schriften sowie Präsentationen. Verschiedene Kriterien wie Datum, Speicherort oder Art schränken die Ergebnisliste ein.

Eine sehr nützliche Funktion von Spotlight ist das Verwalten von intelligenten Ordnern. Durch diese intelligenten Ordner kann man häufig genutzte Dokumente physisch an einem Ort belassen, aber diese tauchen in mehreren intelligenten Ordnern auf. So kann man zum Beispiel alles, was mit einem Oberbegriff zu tun hat, in solche intelligente Ordner abgelegt werden, ohne dass man physisch einen Ordner auf der Festplatte anlegt. Die Dateien können verstreut auf der Festplatte liegen, aber werden dank Spotlight immer schnell wieder gefunden.

Manchmal möchte man aber auch Ordner haben, die nicht durchsucht werden sollten. Dafür hat Spotlight auch eine Funktion, die sich *Privatsphäre* nennt. Die unter Privatsphäre eingetragenen Ordner werden dann von Spotlight beim Suchen nicht beachtet.

2.3 Dashboard

Auf dem *Dashboard* (Armaturenbrett) werden kleine Helferprogramme abgelegt. Ähnlich wie bei *Exposé* gewöhnt man sich schnell an Dashboard, das sich per Voreinstellung über die F12-Taste aufrufen lässt. Neue *Widgets*, das sind die kleinen Icons, die die Informationen oder andere Dinge anzeigen, blendet das Armaturenbrett über das Plus-Symbol unten links ein und springt auf eine eigene Webseite bei Apple, wenn man unten rechts auf „Weitere Widgets“ klickt. Um den kostenpflichtigen .mac-Account zu bewerben, kündigt Apple Widgets an, die exklusiv .mac-Abonnenten zur Verfügung stehen sollen.

Apple liefert 14 Widgets schon mit, aber man kann sich noch diverse weitere Widgets von der Apple-Webseite herunterladen.

Wer selbst einmal versuchen will, ein Widget zu erstellen, der findet auf der Apple-Developer-Webseite eine ausführliche Anleitung zum Erstellen von Widgets.

2.4 Automator

Bislang war *AppleScript* mehr etwas für die Programmierer oder die, die sich tiefer in die Apple-Materie eingearbeitet hatten. Für normale Apple-Nutzer gibt es nun *Automator.*

Automator ist so einfach, dass man sich eigentlich nur noch die Skripte, die man erstellen will, „erklickt“. Mac OS X 10.4 kommt schon mit einer Reihe von vorgefertigten Aktionen daher. So hat Apple zum Beispiel Abläufe zum Suchen von Dateien und Umbenennen in Spotlight mitgeliefert, und auch Adressen aus dem Adressbuch können automatisch in Serienbriefen eingebaut werden.

Hauptsinn und -zweck von Automator ist es, die täglichen Arbeitsabläufe von immer wiederkehrenden Aufgaben zu übernehmen und dem Benutzer das Leben einfacher zu gestalten.

2.5 Mail

Dass sich in *Mail 2* mehr geändert hat als nur die Oberfläche, zeigt sich schon bei der Installation des Systems: Mit dem Migrations-Assistenten lassen sich bestehende Accounts und Mailboxen vom Betriebssystem oder anderen Volumes importieren. Wer das am Anfang nicht tut, kann es beim ersten Programmstart von Mail nachholen. E-Mails werden jetzt nicht mehr gemeinsam in mbox-Datenbanken gespeichert, sondern als einzelne elmx-Dateien, um sie mit Spotlight zu finden. Selbst bei großen Mailarchiven ist das aber kein Problem. Ganz im Gegenteil: Den Bug, der Mailinhalte bei großen Archiven nicht richtig angezeigt hat, hat Apple behoben.

Ansonsten versteht sich Mail 2 nun auch mit Microsofts Exchange Server. Damit erweitert Apple die Unterstützung von IMAP und POP3 jetzt auch um den Exchange Server. Das hat natürlich den Vorteil, dass man mit Mac OS X 10.4 nun auch über den Exchange Server seine E-Mails abrufen kann.

Goy

---

3. RDP über SSL (TLS 1.0) – neues Feature bei Windows Server 2003 SP 1

3.1 Einleitung

Das Remote-Desktop-Protokoll (RDP), welches im Wesentlichen von Microsoft entwickelt wurde, wird immer mehr zum de-facto-Standard für die zentrale Bereitstellung von Anwendungen sowie den administrativen Fernzugriff (Remote Access) auf Windows-Server. RDP ist eine Entwicklung, die einen Fernzugriff auf Rechner erlaubt, bei dem der Bildschirminhalt vom Server zum Client übertragen wird. Überdies werden Tastatur- und Mausaktivitäten über RDP an den Rechner übermittelt. Weil mitunter sensitive Daten übertragen werden, ist eine Verschlüsselung der Daten in vielen Fällen erforderlich oder zumindest angebracht. RDP ist in der Lage, mit ausreichend sicherer Verschlüsselung die Daten zu übertragen. Es bietet eine Datenverschlüsselung an, jedoch keine Authentifizierung, mit deren Hilfe ein Terminalserver authentifiziert werden kann. Das Service Pack 1 (SP 1) für Windows Server 2003 bringt in dieser Hinsicht eine bedeutende Veränderung und Funktionserweiterung für die Terminal Services mit sich: die Fähigkeit des RDP-Clients, sich mit dem Terminalserver komplett über SSL zu verbinden und zu authentifizieren.

Nach der Installation des SP 1 und Erfüllung einiger Voraussetzungen kann die Sicherheitsstufe der Terminalserver-Verbindung auf Secure Socket Layer (SSL) umgeschaltet werden. Ab diesem Zeitpunkt werden die Terminalserver-Client-Verbindungen über Transport-Layer-Security-Protokoll (TLS, eine sehr sichere Version des SSL 3.0) authentifiziert und verschlüsselt. Das Ganze findet nach wie vor über den TCP-Port 3389 statt (s. Abb. 1).

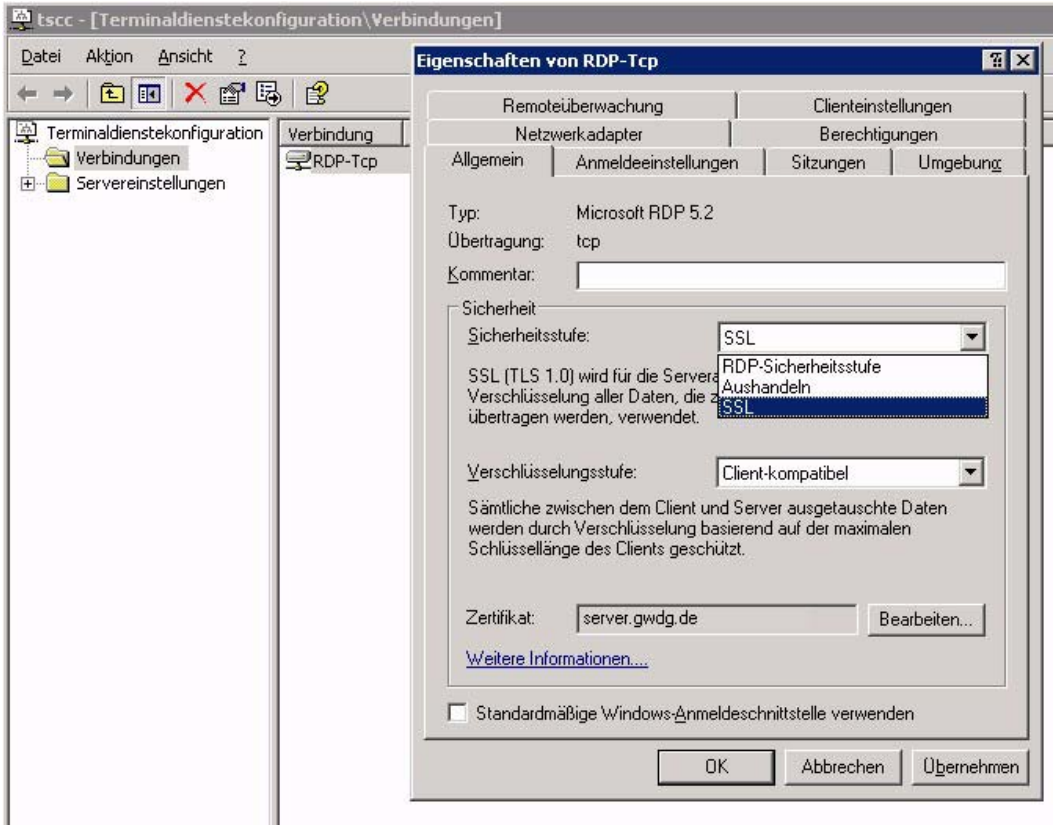

Abb. 1

3.2 TLS-Authentifizierung

TLS 1.0 ist eine geringfügig weiterentwickelte Version des SSL-3.0-Protokolls und hat sich bereits als Industriestandard etabliert. Unterschiede zu SSL 3.0 sind zum einen die Benutzung des Prüfsummenalgorithmus: TLS 1.0 benutzt einen eigenen HMAC(keyed Hashing for Message Authenti-Cation)-Algorithmus, während SSL noch einen „normalen“ MAC(Message Authentication Code)-Algorithmus benutzt. Die Hash-Funktion des HMAC-Algorithmus stellt mit einer Quersumme sicher, dass an den Daten nichts manipuliert wurde. Zum anderen unterscheidet sich TLS 1.0 von SSL 3.0 in der getrennten Spezifikation des Handshake- und Record-Protokolls.

3.3 Grundvoraussetzungen für die Konfiguration von RDP über SSL (TLS 1.0)

Um RDP über SSL realisieren zu können, sind sowohl server- als auch clientseitig einige Voraussetzungen zu erfüllen:

3.3.1 Server-Voraussetzungen

Damit die TLS-Authentifizierung ordnungsgemäß funktioniert, muss der Terminalserver folgende Voraussetzungen erfüllen:

- Auf dem Terminalserver muss Windows Server 2003 SP 1 installiert sein.
- Für den Terminalserver muss ein Server-Zertifikat vorhanden sein.

Das Server-Zertifikat muss folgende Bedingungen erfüllen:

- Das Zertifikat muss ein Computerzertifikat sein.
- Der beabsichtigte Zweck des Zertifikats muss sich auf Server-Authentifizierung beziehen.
- Das Zertifikat muss einen entsprechenden privaten Schlüssel aufweisen.
- Das Zertifikat muss in dem Computerkonto-Zertifikatspeicher auf dem Terminalserver gespeichert sein (s. Abb. 2).

Abb. 2

3.3.2 Client-Voraussetzungen

Der Client-Computer muss die folgenden Voraussetzungen erfüllen:

- Auf dem Client-Computer muss Microsoft Windows 2000 oder Microsoft Windows XP sowie das Terminalserver-Client-Programm *RDP Version 5.2* (Build 3790) installiert sein. Das Terminalserver-Client-Programm **`msrdpcli.msi`** befindet sich i. d. R. im Verzeichnis **`%SYSTEMROOT%\System32\Clients\Tsclient\Win32`** auf Windows-2003-Terminalservern und wird nach der Installation des SP 1 auf dem Terminalserver auf Version 5.2 (Build 3790) upgegraded.
- Der Client-Computer muss der Stamm-Zertifizierungsstelle des Zertifikats des Terminalservers vertrauen. Daher muss das Zertifikat bzw. die gesamte Zertifikatkette der Zertifizierungsstelle in dem Verzeichnis „Zertifikate der vertrauenswürdigen Stammzertifizierungsstellen“ (Trusted Root Certificate Certification Authorities) des Client-Computers enthalten sein. Mit Hilfe von Zertifikat-Snap-Ins können Sie sich diesen Ordner anzeigen lassen (s. Abb. 3).

Abb. 3

3.4 Konfiguration

3.4.1 Konfigurieren des Servers

Die SSL- bzw. TLS-Authentifizierungs-Option kann folgendermaßen konfiguriert werden:

Schritt 1: Anfordern und Installieren eines Computerzertifikats

Wenn Sie nicht bereits über ein Server-Zertifikat verfügen, das die oben genannten Anforderungen erfüllt, haben Sie die Möglichkeit ein Zertifikat anzufordern. Für die Anforderung eines Client-Zertifikats benötigen Sie eine **Zertifizierungsstelle** (**CA**)**.** Eine Zertifizierungsstelle ist eine Einheit, die zur Ausstellung von Zertifikaten an Personen, Computer oder Organisationen berechtigt ist. Es bestehen grundsätzlich die Möglichkeiten, entweder eine eigenständige **Zertifizierungsstelle** bzw. eine **Organisationszertifizierungsstelle** einzurichten, die dann für den Zielserver ein Zertifikat ausstellt, oder ein Zertifikat von einer **fremden Zertifizierungsstelle** anzufordern bzw. zu erwerben.

Für den Terminalserver wie auch für Webserver empfiehlt es sich, ein Zertifikat einer offiziell bekannten und vertrauten Zertifizierungsstelle zu erwerben, was natürlich immer mit Kosten verbunden ist.

Seit ca. einem Jahr verfügt die GWDG über eine **Zertifizierungsstelle**, die durch die **Stammzertifizierungsstelle** des Deutschen Forschungsnetzes (DFN) zertifiziert wurde. Die GWDG-CA bietet Zertifizierungsdienste für die Max-Planck-Gesellschaft, die Georg-August-Universität Göttingen und weitere angebundene Einrichtungen an. Unter

`http://ca.gwdg.de`

erhalten Sie alle benötigten Informationen und Unterlagen zur Beantragung eines Server-Zertifikats.

Nach dem Vorliegen des Server-Zertifikats muss dies im Computerkonto-Zertifikatspeicher auf dem Terminalserver installiert bzw. gespeichert werden (s. Abb. 2).

Schritt 2: Konfigurieren der TLS-Authentifizierung und Verschlüsselung

Nach der Installation des Server-Zertifikats kann die TLS-Authentifizierung und Verschlüsselung sowohl unter Verwendung von „Gruppenrichtlinien“ als auch unter „Terminaldienstekonfiguration“ konfiguriert werden. Hier wird die Konfiguration der Authentifizierung und Verschlüsselung über die Terminaldienstekonfiguration beschrieben (weitere Informationen am Ende dieses Artikels unter „Relevante Links“):

1. Starten des Terminaldienstekonfigurations-Programms:
   Klicken Sie auf „Start“, zeigen Sie auf „Verwaltung“ und klicken Sie anschließend auf „Terminaldienstekonfiguration“!
2. Klicken Sie auf „Verbindung“ im linken Ausschnitt!
3. Klicken Sie mit der rechten Maustaste auf die Verbindung in dem rechten Fenster und klicken Sie dann auf „Eigenschaft“!
4. Klicken Sie auf „Bearbeiten“ neben „Zertifikat“ in der Registerkarte „Allgemein“!
5. In dem Zertifikats-Auswahl-Dialogfeld auf das Zertifikat klicken, das Sie verwenden möchten (s. Abb. 4)!

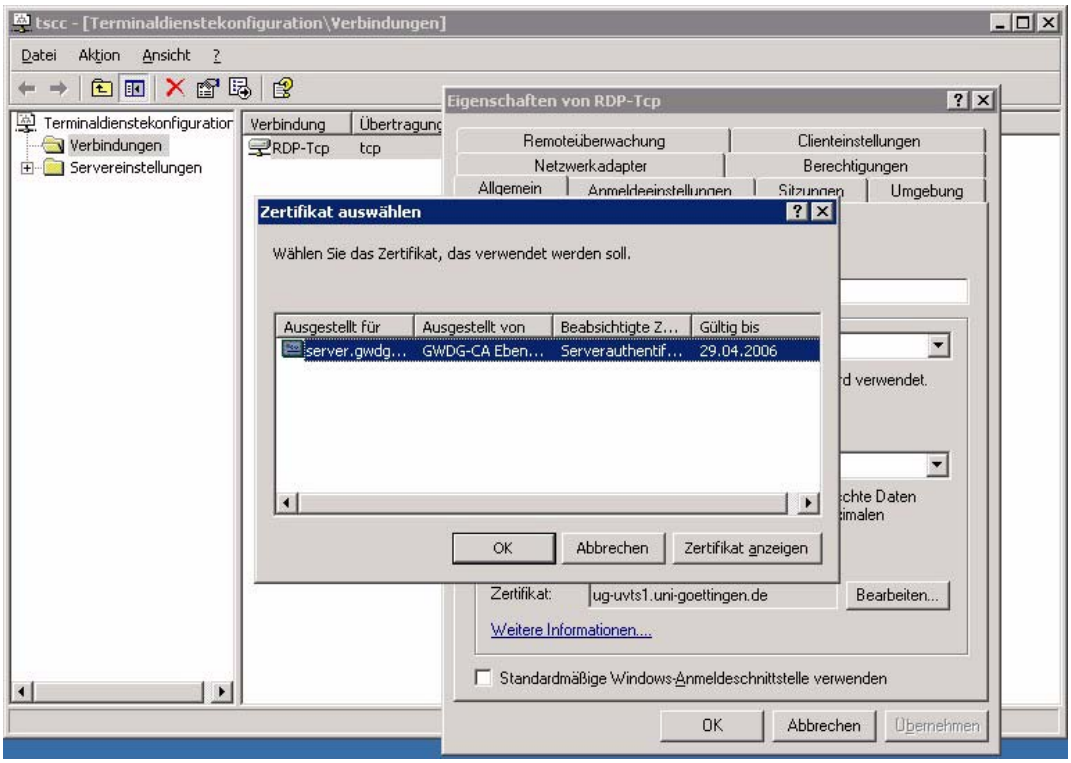

Abb. 4

Anmerkung: Um zu überprüfen, ob es sich bei dem Zertifikat um ein geeignetes Zertifikat handelt, klicken Sie auf „Zertifikat anzeigen“! Der folgende Text sollte unter den Zertifikatinformationen angezeigt werden: „*Sie besitzen einen privaten Schlüssel für dieses Zertifikat.*“

6. Schließen Sie das Zertifikats-Auswahl-Dialogfeld durch Klicken der OK-Taste!

7. Klicken Sie im Sicherheitsstufe-Dropdownmenü auf eine der folgenden Optionen (s. Abb. 5)!

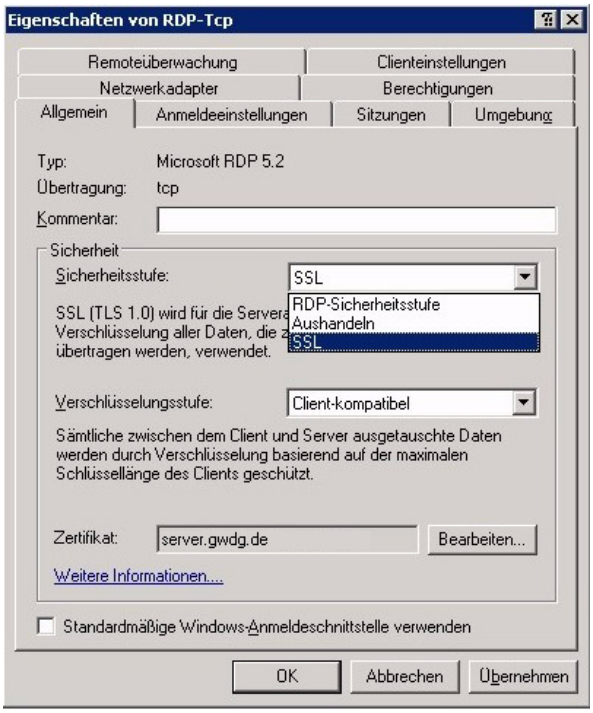

Abb. 5

- **RDP-Sicherheitsstufe** - Diese Sicherheitsmethode verwendet die RDP-Verschlüsselung für die Kommunikation zwischen Server und Client. Bei dieser Option wird der Server nicht authentifiziert.
- **Aushandeln** - Diese Sicherheitsmethode verwendet TLS 1.0, um den Server zu authentifizieren, falls dies clientseitig unterstützt wird. Wenn TLS clientseitig nicht unterstützt wird (z. B. wenn die Terminalserver-Clientsoftware-Version älter ist als RDP 5.2 (Build 3790), wird der Server nicht authentifiziert.
- **SSL** (nur verfügbar, wenn ein gültiges Zertifikat installiert/ausgewählt ist) - Diese Sicherheitsmethode erfordert TLS 1.0, um den Server zu authentifizieren. Wenn TLS clientseitig nicht unterstützt wird (z. B. wenn die Terminalserver-Clientsoftware-Version älter ist als RDP 5.2 des Windows Server 2003 SP 1), kann keine Verbindung zum Terminalserver hergestellt werden.

8. Klicken Sie im Verschlüsselungsstufe-Dropdownmenü auf eine der folgenden Optionen (s. Abb. 6)!

- **FIPS-Konform** - Mit dieser Einstellung werden alle Daten mit Hilfe von Methoden verschlüsselt, die anhand des Federal Information Processing Standard (FIPS) 140-1 validiert wurden.
- **Hoch** - Diese Einstellung bietet bidirektionale Sicherheit mit Hilfe einer 128-Bit-Verschlüsselung.
- **Client-Kompatibel** - Unter dieser Verschlüsselungsstufe werden die Daten mit der maximalen Verschlüsselungsstufe, die vom Client-Computer unterstützt wird, verschlüsselt.
- **Niedrig** (diese Option ist unter der Sicherheitsstufen-Option „SSL“ nicht verfügbar) - Diese Einstellung verwendet eine 56-Bit-Verschlüsselung.

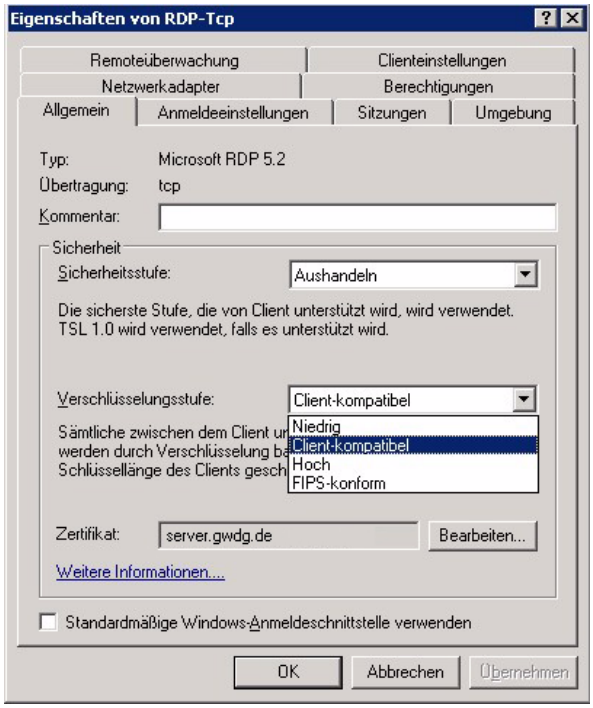

Abb. 6

Alle Stufen verwenden die Standard-RSA-RC4-Verschlüsselung.

9. Klicken Sie auf „OK“!

3.4.2 Konfigurieren des Client-Computers

Der Client-Computer kann folgendermaßen für TLS-Authentifizierung konfiguriert werden:

Anmerkung: Wie schon oben erwähnt, muss auf dem Client-Computer RDP Version 5.2 installiert sein, um die TLS-Authentifizierung konfigurieren zu können. Die RDP-Software (`msrdpcli.msi`) steht i. d. R. auf allen Windows-2003-Terminalservern im Verzeichnis `%systemroot%\system32\clients\tsclient\win32` zur Verfügung und wird mit dem Windows Server 2003 SP 1 auf Version 5.2 (Build 3790) upgegraded.

Schritt 1: Installieren Sie auf dem Client-Computer das Zertifikat der Stammzertifizierungsstelle, damit der Client-Computer allen Zertifikaten (auch denen

der untergeordneten Zertifizierungsstellen) vertrauen kann. Wenn Sie auf Ihrem Zielserver ein GWDG-Server-Zertifikat installiert haben, können Sie unter

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

das Zertifikat der Stammzertifizierungsstelle bzw. die gesamte Zertifikatkette auf dem Client-Computer installieren.

Schritt 2: Jetzt kann die Authentifizierung auf dem Client-Computer folgendermaßen konfiguriert werden:

1. Starten Sie „Remotedesktopverbindung“ (zum Öffnen der Remotedesktopverbindung klicken Sie im Startmenü auf „Programme“ oder auf „Alle Programme“, zeigen Sie auf „Zubehör“ und dann auf „Kommunikation“, und klicken Sie dann auf „Remotedesktopverbindung“)!
2. Klicken Sie auf „Optionen“ und dann auf die Registerkarte „Sicherheit“!

   Anmerkung: Die Registerkarte „Sicherheit“ wird nur mit RDP 5.2 (Build 3790) angezeigt.

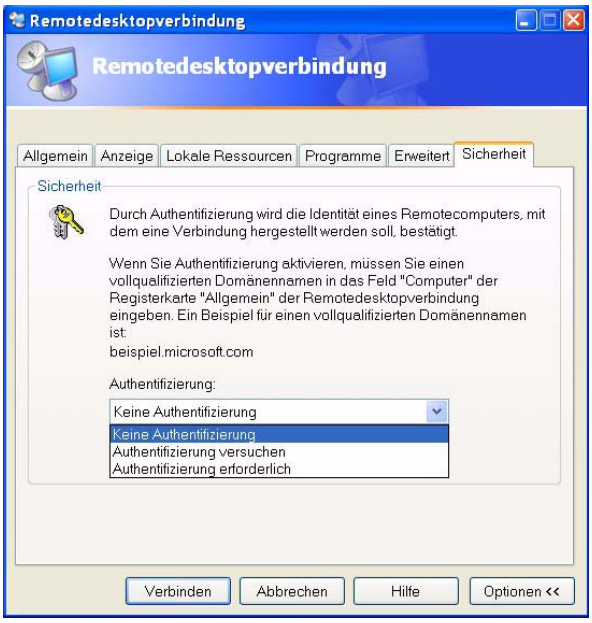

Abb. 7

3. Klicken Sie in der Liste „Authentifizierung“ auf eine der folgenden Optionen:

- **Keine Authentifizierung** ist die Standardoption. Wenn Sie diese Option auswählen, wird der Terminalserver nicht authentifiziert.
- **Authentifizierung versuchen** - Unter dieser Option wird TLS 1.0 verwendet, wenn der Terminalserver TLS-Authentifizierung unterstützt bzw. diese korrekt auf dem Terminalserver konfiguriert ist.
- **Authentifizierung erforderlich** - Wenn Sie diese Option wählen, ist TLS zum Authentifizieren des Terminalservers erforderlich. Der Verbindungsversuch wird abgebrochen, wenn auf dem Terminalserver TLS nicht unterstützt wird bzw. nicht korrekt konfiguriert ist. Diese Option ist nur verfügbar für Client-Computer, die eine Verbindung zu Terminalservern herstellen, auf denen Windows Server 2003 SP 1 ausgeführt wird.

Abb. 8

Nach dem erfolgreichen Aufbau einer Remotedesktopverbindung über SSL (TLS 1.0) erscheint auf der Leiste am oberen Bildschirmrand das typische Schloss-Symbol der SSL-Verbindung (s. Abb. 8).

3.5 Relevante Links

SSL/TLS in Windows Server 2003:

`http://go.microsoft.com/fwlink/?LinkId=19646`

Configure Authentication and Encryption:

`http://go.microsoft.com/fwlink/?LinkId=45407`

Public Key Infrastructure Windows Server 2003:

`http://go.microsoft.com/fwlink/?LinkId=45371`

GWDG Public Key Infrastructure:

`http://ca.gwdg.de`

Sheikhikhou

4. *allegro* V25 verfügbar

Die aktuelle Version 25 der an der TU Braunschweig entwickelten Bibliothekssoftware *allegro* kann von den Instituten der Universität Göttingen und den Göttinger Max-Planck-Instituten im Rahmen einer Campuslizenz kostenlos über die GWDG bezogen werden.

Ansprechpartnerin ist Frau Anke Bruns (Tel.: 0551 201-1519, E-Mail: anke.bruns@gwdg.de).

Nähere Informationen zu allegro sind unter dem URL

`http://www.allegro-c.de`

zu finden.

Bruns

---

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 201-2150 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 Institute 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 August bis Dezember 2005 in thematischer Übersicht

EDV-Grundlagen und Sonstiges

Kurse	Termine	Vortragende
Einführung in die Nutzung des Leistungsangebots der GWDG	• 31.08.2005 • 07.12.2005	Dr. Grieger Dr. Grieger
Einführung in Aufbau und Funktionsweise von PCs	• 13.09.2005	Eyßell
Einführung in die Bedienung von Windows-Oberflächen	• 14.09.2005	Eyßell
Führung durch das Rechnermuseum	• 02.09.2005 • 30.09.2005 • 04.11.2005 • 09.12.2005	Eyßell Eyßell Eyßell Eyßell

Betriebssysteme

Kurse	Termine	Vortragende
Grundkurs UNIX/Linux mit Übungen	• 08.11.2005 - 10.11.2005	Hattenbach
Schnellkurs UNIX für Windows-Benutzer mit Übungen	• 11.09.2005 - 12.09.2005 • 28.11.2005 - 29.11.2005	Dr. Bohrer Dr. Bohrer
Installation und Administration von UNIX-Systemen	• 13.12.2005 - 16.12.2005	Dr. Heuer, Dr. Sippel
UNIX für Fortgeschrittene	• 05.12.2005 - 07.12.2005	Dr. Sippel
Windows 2000/XP/2003 in kleinen Netzwerken	• 10.10.2005 - 11.10.2005	Quentin
Die Windows-Active-Directory-Domäne	• 12.10.2005 - 14.10.2005	Quentin

Netze / Internet

Kurse	Termine	Vortragende
Sicherheit im Internet für Anwender	• 16.09.2005 • 16.12.2005	Reimann Reimann
Web Publishing I	• 31.08.2005 - 01.09.2005	Reimann
Web Publishing III - PHP	• 01.11.2005 - 03.11.2005	Koch, Reimann

Grafische Datenverarbeitung

Kurse	Termine	Vortragende
Arbeiten mit CAD, Grundlagen	• 05.09.2005 - 09.09.2005	Witt
CorelDRAW - Grundlagen	• 18.10.2005 - 19.10.2005	Wagenführ
Grundlagen der Bildbearbeitung mit Photoshop	• 25.08.2005 - 26.08.2005	Töpfer
Photoshop für Fortgeschrittene	• 04.10.2005 - 05.10.2005	Töpfer

Sonstige Anwendungssoftware

Kurse	Termine	Vortragende
Datenbanksystem MS Access, Einführung mit Übungen	• 08.12.2005 - 09.12.2005	Reimann
PowerPoint	• 22.11.2005 - 23.11.2005	Reimann
Projektplanung mit MS Project	• 06.10.2005	Reimann
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN	• 26.09.2005 - 29.09.2005	Dr. Bohrer, Dr. Liesegang
Nutzung fortschrittlicher Datenbanken zur Charakterisierung von Proteinen	• 30.09.2005	Dr. Liesegang
Mit StarOffice zum Schwarzen Loch	• 11.11.2005	Dr. Grieger

Programmiersprachen

Kurse	Termine	Vortragende
Einführung in die Programmiersprache Fortran 90/95	• 29.08.2005 - 30.08.2005	Dr. Schwardmann
Programmierung von Parallelrechnern	• 29.11.2005 - 01.12.2005	Prof. Haan, Dr. Boehme, Dr. Schwardmann

5.3 Kurse von August bis Dezember 2005 in chronologischer Übersicht

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Grundlagen der Bildbearbeitung mit Photoshop	Töpfer	25.08.2005 - 26.08.2005 09.30 - 16.00 Uhr	18.08.2005	8
Einführung in die Programmier-sprache Fortran 90/95	Dr. Schwardmann	29.08.2005 - 30.08.2005 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr	22.08.2005	8
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	31.08.2005 17.00 - 20.00 Uhr	24.08.2005	0
Web Publishing I	Reimann	31.08.2005 - 01.09.2005 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	24.08.2005	8
Führung durch das Rechner-museum	Eyßell	02.09.2005 10.00 -12.00 Uhr	26.08.2005	0
Arbeiten mit CAD, Grundlagen	Witt	05.09.2005 - 09.09.2005 09.00 - 16.00 Uhr (am 05.09. ab 10.00 Uhr; am 09.09. bis 13.00 Uhr)	29.08.2005	18
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	12.09.2005 - 13.09.2005 13.00 - 16.00 Uhr	05.09.2005	4
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	13.09.2005 09.15 - 12.30 Uhr	06.09.2005	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	14.09.2005 09.15 - 12.30 Uhr und 13.30 - 16.00 Uhr	07.09.2005	4
Sicherheit im Internet für Anwender	Reimann	16.09.2005 09.15 - 12.00 Uhr	09.09.2005	2
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, STADEN	Dr. Bohrer, Dr. Liesegang	26.09.2005 - 29.09.2005 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	19.09.2005	16
Nutzung fortschrittlicher Datenban-ken zur Charakterisierung von Pro-teinen	Dr. Liesegang	30.09.2005 09.30 - 12.30 Uhr und 13.30 - 16.00 Uhr	23.09.2005	4
Führung durch das Rechner-museum	Eyßell	30.09.2005 10.00 - 12.00 Uhr	23.09.2005	0
Photoshop für Fortgeschrittene	Töpfer	04.10.2005 - 05.10.2005 09.30 - 16.00 Uhr	27.09.2005	8
Projektplanung mit MS Project	Reimann	06.10.2005 09.15 - 12.00 Uhr und 13.00 -15.00 Uhr	29.09.2005	4
Windows 2000/XP/2003 in kleinen Netzwerken	Quentin	10.10.2005 - 11.10.2005 09.00 - 15.00 Uhr	03.10.2005	8

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Die Windows-Active-Directory-Domäne	Quentin	12.10.2005 - 14.10.2005 (am 14.10. bis 13.00 Uhr)	05.10.2005	10
CorelDRAW - Grundlagen	Wagenführ	18.10.2005 - 19.10.2005 09.15 - 12.00 Uhr und 13.30 - 16.30 Uhr	11.10.2005	8
Web Publishing III - PHP	Koch, Reimann	01.11.2005 - 03.11.2005 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	25.10.2005	12
Führung durch das Rechner-museum	Eyßell	04.11.2005 10.00 - 12.00 Uhr	28.10.2005	0
Grundkurs UNIX/Linux mit Übungen	Hattenbach	08.11.2005 - 10.11.2005 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	01.11.2005	12
Mit StarOffice zum Schwarzen Loch	Dr. Grieger	11.11.2005 09.00 - 12.00 Uhr	04.11.2005	2
PowerPoint	Reimann	22.11.2005 - 23.11.2005 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	15.11.2005	8
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	28.11.2005 - 29.11.2005 13.00 - 16.00 Uhr	21.11.2005	4
Programmierung von Parallel-rechnern	Prof. Dr. Haan, Dr. Boehme, Dr. Schwardmann	29.11.2005 - 01.12.2005 09.15 - 12.15 Uhr und 13.30 - 16.30 Uhr	22.11.2005	12
Datenbanksystem MS Access, Einführung mit Übungen	Reimann	**Neuer Termin!!!** 08.12.2005 - 09.12.2005 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	01.12.2005	8
UNIX für Fortgeschrittene	Dr. Sippel	05.12.2005 - 07.12.2005 09.15 - 12.00 Uhr und 13.15 - 15.30 Uhr	28.11.2005	12
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	07.12.2005 17.00 - 20.00 Uhr	30.11.2005	0
Führung durch das Rechner-museum	Eyßell	09.12.2005 10.00 - 12.00 Uhr	02.12.2005	0
Installation und Administration von UNIX-Systemen	Dr. Heuer, Dr. Sippel	13.12.2005 - 16.12.2005 09.30 - 12.00 Uhr und 13.30 - 16.30 Uhr	06.12.2005	16
Sicherheit im Internet für Anwender	Reimann	16.12.2005 09.15 - 12.00 Uhr	06.12.2005	2

6. Betriebsstatistik Juni 2005

6.1 Nutzung der Rechenanlagen

Rechner	Zahl der Prozessoren	CPU-Stunden
DECalpha	8	420,16
IBM RS/6000 SP	224	51.177,85
IBM Regatta	124	49.065,85
Linux Parallel	252	161.479,45
Linux Opteron	96	47.091,49

6.2 Betriebsunterbrechungen

Rechner/PC-Netz	Störungen		System-pflege	
	Anzahl	Stunden	Anzahl	Stunden
UNIX-Cluster	0		0	
IBM SP/Regatta	0		0	
Linux Parallel	0		0	
Linux Opteron	0		0	
PC-Netz	0		0	
Nameserver	0		0	
Mailer	0		0	

7. Autoren dieser Ausgabe

Name	Artikel	E-Mail-Adresse / Telefon-Nr.
Anke Bruns	• *allegro* V25 verfügbar	anke.bruns@gwdg.de 0551 201-1519
Nicole Goy	• Mac OS X 10.4 Tiger	ngoy@gwdg.de 0551 201-1557
Dr. Konrad Heuer	• Der OpenLDAP-Server der GWDG – Teil II	kheuer@gwdg.de 0551 201-1540
Hossein Sheikhikhou	• RDP über SSL (TLS 1.0) – neues Feature bei Windows Server 2003 SP 1	hsheikh@gwdg.de 0551 201-1841