

inforum

Zentrum für Informationsverarbeitung der Universität Münster

Jahrgang 27, Nr. 2 – Juni 2003

ISSN 0931-4008

Inhalt

Editorial	2
ZIV-Aktuell	3
Das IKM-Konzept der Universität	3
Soforthilfe gegen Spam	5
Linux-Parallelrechner in Betrieb	8
20.000 TP-Anschlüsse – und kein Ende?	9
Langzeit-Ausleihe von Funk-LAN-Karten	11
Preisliste für LAN-Anschlüsse	13
Ein neuer Posterdrucker im ZIV	13
wwuzugang – Ein Terminal zum Netz der WWU	14
CHAP nicht von PAPpe	15
i in MIAMI	16
Regelmäßige Überprüfung der redundanten Internet/G-WiN-Anbindung	17
McAfee VirusScan Enterprise	18
SPSS für Windows Version 11.5	19
ZIV-Lehre	20
Veranstaltungen in der vorlesungsfreien Zeit (August – Oktober 2003)	20
Veranstaltungen in der Vorlesungszeit (Wintersemester 2003/2004)	21
Kommentare zu den Lehrveranstaltungen	22
ZIV-Regularia	26
Fingerprints	26



Impressum



ISSN 0931-4008

Westfälische Wilhelms-Universität
Zentrum für Informationsverarbeitung (Universitätsrechenzentrum)
Röntgenstr. 9 – 13
48149 Münster

E-Mail: ziv@uni-muenster.de
WWW: <http://www.uni-muenster.de/ZIV/>

Redaktion: H. Pudlatz (G 83-31672, [☎ pudlatz@uni-muenster.de](mailto:pudlatz@uni-muenster.de))
E. Sturm (G 83-31679, [☎ sturm@uni-muenster.de](mailto:sturm@uni-muenster.de))

Satzsystem: Corel WordPerfect 8.0 für Windows 98/NT

Druck: Drucktechnische Zentralstelle der WWU
(Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1500

Editorial



H. Pudlatz

E-Mail war in den Anfängen der elektronischen Kommunikation ein Nebenprodukt der Nutzung dieses Mediums. Wichtiger war der Dateitransfer und der entfernte Zugang zu Rechnern. Heutzutage ist aus diesem Nebenprodukt anscheinend die Hauptsache geworden, man schaue nur einmal in die Rechner-Pools und nach den dort hauptsächlich betriebenen Aktivitäten. Man läßt sich ja auch keine Nutzerkennung mehr einrichten, sondern eine E-Mail-Adresse. So ist es denn auch kein Wunder, wenn diese eigentlich sinnvolle Nutzungsmöglichkeit – wie bei so manchem technischen Fortschritt – immer mehr zu missbräuchlicher Nutzung verleitet.

E-Mail ist schon lange zum Vehikel für eCommerce geworden, eine durchaus erwünschte moderne Entwicklung im Wirtschaftsleben, aber leider auch zur Spielwiese dubioser Geschäftemacher, die jeden – ob Mann oder Frau – mit den seltsamsten Angeboten bombardieren, SPAM eben, genannt nach „Spiced Pork and hAM“, dem Produkt eines amerikanischen Dosenfleischherstellers, der erstmals das „Zumüllen“ mit Massenwerbung praktizierte.

Wir wurden oft gefragt, ob wir nicht zentral etwas gegen die Werbeflut unternehmen können, was sich jedoch schwieriger gestaltete als bei der der Einführung des zentralen Virenfilters vor einem Jahr. Konnte man dort noch mit der Notwendigkeit der Abwehr böswilliger Attacken auf die Netznutzergemeinde argumentieren, so ließ sich diese Begründung für Spam nicht so einfach geben. Die Grenze zwischen „guter“ und „schlechter“ Post muss jeder für sich selbst ziehen. Was nämlich für den einen lästige Werbung ist, ist gerade bei einem anderen als Informationsquelle erwünscht.

Aufgrund der explosionsartigen Zunahme von Spam wird aber die Beurteilung der eingegangenen E-Mail ohne einen unterstützenden Automatismus immer mehr zu einem ärgerlichen und zeitraubenden Unterfangen. Hier hilft nun die automatische Inhaltsanalyse, wie sie schon in dem Artikel „Spam verrät sich durch ihren Inhalt“ von E. Sturm im letzten i beschrieben wurde. Er stellt nun in diesem Heft das Verfahren in Gestalt des Programms Deleatur unseren Lesern zur Verfügung, bei dem jeder selbst definieren kann, was er unter Spam verstanden wissen will. Der Vorteil besteht aber auch darin, dass ein derartiger „Spamfilter“ nach einer kurzen Lernphase, bei der Sie das Programm unterstützen, selbsttätig Spam direkt auf dem POP-Server löscht.

Der Einsatz einer darüber hinausgehenden zentralen Spam-Abwehr wird derzeit im ZIV untersucht. Der Erfolg gegenüber individueller Einstellung der Filterfunktion wird dabei aber vermutlich nicht erreicht werden können.

ZIV-Aktuell

Das IKM-Konzept der Universität

W. Held

Für unsere Universität wurde ein Konzept entwickelt, das die notwendigen Dienste für Information, Kommunikation und Medien (kurz: IKM) für die Zwecke von Forschung und Lehre koordiniert und als Kompetenzzentrum Dienstleistungen für Information, Kommunikation und Medien anbietet. Nachfrager sind die Fachbereiche und Studierenden der Universität.

Partner des IKM-Service sind die Universitäts- und Landesbibliothek (ULB), das Zentrum für Informationsverarbeitung (ZIV) sowie die Universitätsverwaltung (UniV). Der IKM-Service bündelt die in diesen Organisationseinheiten vorhandenen Kompetenzen für den Bereich IKM in einer festen Organisationsstruktur mit kooperativer Leitung.

Für den IKM-Service sollte keine neue Einrichtung geschaffen werden. Vielmehr sollen die beteiligten Einrichtungen (ULB, ZIV und UniV) flexibel auf neue Aufgaben, die regelmäßig im Detail festzulegen sind, reagieren, Mitarbeiter/innen ihrer Bereiche dem Bedarf entsprechend zusammenziehen und am Ende wieder zurücknehmen. Die Kooperation ist auf Dauer angelegt. Der Themenkatalog wird dem Bedarf folgend auf wechselnde Schwerpunkte in der sich schnell wandelnden IV ausgerichtet werden.

Zum Spektrum dieser Dienste gehören: Technische Infrastruktur, Vermittlung von Medien- und Informationskompetenz, Bereitstellung von Inhalten, Nutzungsverwaltung, Service-Punkte und Marketing der Dienstleistungen und Produkte sowie Entwicklung und Etablierung von Controlling und Evaluierungsinstrumenten.

An der Universität Münster wird bereits ein breites Spektrum an IKM-Diensten angeboten; für die notwendigen Anwendungen und den Aufbau der Strukturen sind hochentwickelte Techniken vorhanden, die jedoch mit hochschulspezifischen Standards nachhaltig eingeführt werden müssen, wobei eine umfassende und hohe Qualität sichergestellt werden muss. Die dezentrale Organisationsform der Dienste erweist sich als leistungsfähig, da auf diese Weise die an der Universität verfügbaren Kernkompetenzen ausgeschöpft werden können.

Zur nachfrageorientierten Koordination im Arbeitsfeld Medien (M) wurde eine Anwendergruppe zur Weiterentwicklung der computergestützten Hochschullehre eingerichtet (cHL-Anwendergruppe). Diese Anwendergruppe bildet die Verbindung zwischen IKM-Service und den Fachbereichen und damit die Verknüpfung zwischen der Erstellung der Inhalte auf der einen und der unterstützenden Infrastruktur auf der anderen Seite (s. Abb. 2). Die Leitung der Gruppe soll von einem Hochschullehrer übernommen werden, ihr sollen auch zwei studentische Mitglieder angehören. Jeder Fachbereich sollte einen Medienbeauftragten in diese cHL-Anwendergruppe entsenden. Die Fachbereiche sind aufgefordert, auch auf ihrer Ebene die IKM-Aktivitäten unter Einbeziehung der IVVen und bereits bestehender Einrichtungen oder Arbeitsgruppen mit Zuständigkeiten im Bereich IKM zu bündeln und ihr Expertenwissen in den IKM-Service einzubringen. Die IV-Versorgungseinheiten (IVVen) übernehmen analog zu der bisherigen Arbeitsteilung zwischen ZIV und IVVen die Aufgaben aus dem IKM-Service mit Schwerpunkten in der Endanwender-Betreuung.

Da die bisherigen Aufgaben der beteiligten Einrichtungen nicht erkennbar abnehmen, überprüfen sie regelmäßig, ob ihre bisherigen Kernaufgaben, an denen sich ihre Rollen im IKM ausrichten, zur Vermeidung von Doppelarbeiten anders zugeordnet oder gemeinsam durchgeführt werden können. Das betrifft u. a. die IV-Anwendungen, die Beschaffung von Hard- und Software, Themen der Aus- und Weiterbildung, die Unterbringung und den Betrieb von Servern und Rechnerpools, die Personal- und Nutzerverwaltung, das Rechnungs- und Haushaltswesen sowie die Konvergenz der Telefon- und Rechnernetze. Gleichartige Aufgaben sollen zusammengefasst und konzentriert ausgeführt werden. Die eine oder andere Aufgabe wird dadurch wegfallen können oder rationeller gelöst werden. Auf diese Weise freigesetzte Synergien sollen einige Freiräume für die Übernahme neuer Aufgaben schaffen. Die Zuständigkeiten sollen klar geregelt werden. Aufgaben sollen dort erledigt werden, wo dies besonders effizient erscheint.

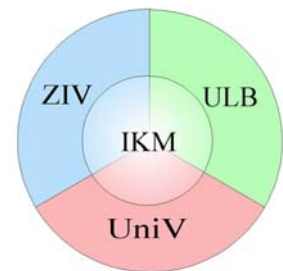


Abb. 1: Am IKM-Service beteiligte Einrichtungen

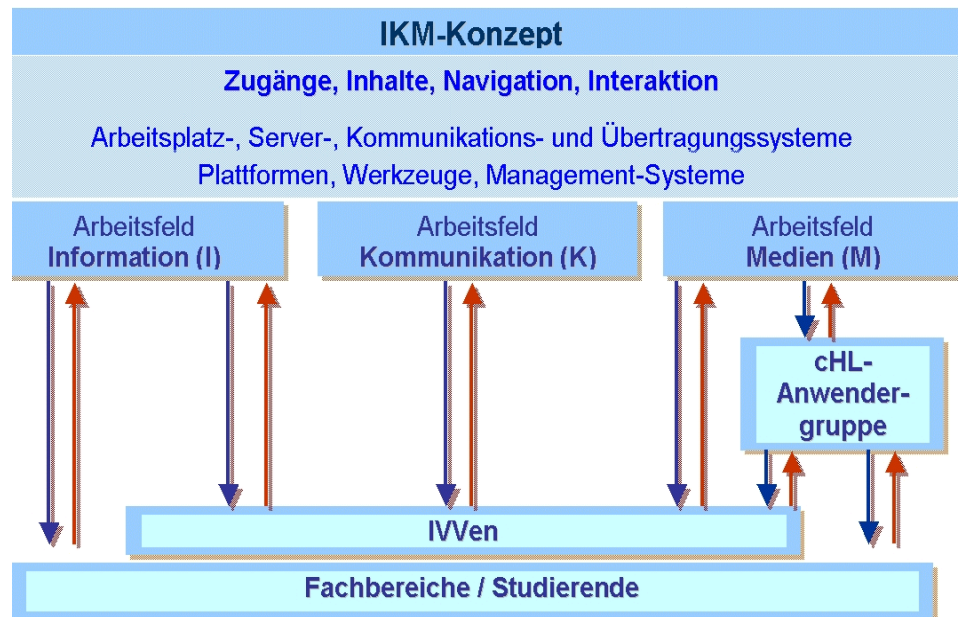


Abb. 2: Struktur des IKM-Verbunds

Ein erster Maßnahmenkatalog umfasst u. a. folgende Themen:

Technische Infrastruktur

Die digitale Bibliothek MIAMI soll mit einem Video-Server verbunden werden, damit die Video-Recherche komfortabler wird. Die vorhandene TeX-Shell soll mit entsprechenden UB-Dienstleistungen zum wissenschaftlichen Publizieren verknüpft werden. Der Einsatz mobiler Rechner soll gefördert werden. Im ZIV sollen in der Einsteinstraße ein Multimedia-Raum und in der ULB ein Multimedia-Hörsaal jeweils mit Servicepunkt eingerichtet werden. In den am ITM beteiligten Einrichtungen sollen das im ZIV eingeführte Systemmanagement (Tivoli, Microsoft) sowie die Konzepte für den Betrieb von CIP-Pools und Server-Hosting erprobt werden. Neben OpenUSS sollen das Content Management System und das LDAP-Directory-System sowie Videokonferenzen und digitale Übertragungen aus Hörsälen gefördert werden.

Vermittlung von Medien- und Informationskompetenz

Das Schulungsangebot zur Informationskompetenz und das Schulungsprogramm LOTSE sollen systematisiert bzw. ausgebaut werden. Ein Lehr- und Beratungsangebot für Medienkompetenz soll entwickelt werden.

Bereitstellung von Inhalten

Elektronische Dokumente der Universität sollen vermehrt in MIAMI eingebunden werden; Dazu sollen Metadaten durch einen entsprechenden Service (Beratung zur Nutzung) weiter erschlossen werden. Zur Langzeit-Archivierung neuer Medien sollen Konzepte und Richtlinien erstellt werden. Für einen digitalen Universitätsverlag sollen Richtlinien und ein Geschäftsmodell erarbeitet sowie rechtliche Grundlagen geklärt werden. Die Drucktechnischen Zentralstelle soll eingebunden werden. Für die Medien-Erstellung sollen geeignete Autorenwerkzeuge zusammengestellt werden.

Nutzungsverwaltung

Die dringend notwendige Einführung digitaler Ausweis- und Signierkarten soll gefördert werden. Die Nutzerverwaltung soll in der Universität weiter vereinheitlicht werden.

Service-Punkte und Marketing

Eine IKM-Website sollen eingerichtet und die Öffentlichkeitsarbeit gemeinsam betrieben werden.

Soforthilfe gegen Spam

E. Sturm

Das im letzten i vorgestellte Antispam-Programm ist jetzt frei verfügbar – unter dem Namen „Deleatur“. Auch AIX- und Linux-Benutzer bleiben nicht im Regen stehen.

An sich war das im letzten i (Nr. 1/2003) vorgestellte Antispam-Programm nur zum Erfahrungssammeln gedacht gewesen. Unter dem allgemeinen Leidensdruck habe ich mich jetzt aber doch überreden lassen, es unter dem Namen „Deleatur“ (lat. „es möge gelöscht werden“) frei zur Verfügung zu stellen. Die ersten Absätze des erwähnten Artikels möchte ich hier zunächst zur Verdeutlichung wiederholen:

Spam-Filter alter Art

Wer irgendwo im Internet seine E-Mail-Adresse hinterlassen hat, sei es auf einer Webseite oder in einer Zuschrift an ein Diskussionsforum, hat wohl inzwischen Ärger mit unverlangt zugeschickter Reklame-E-Mail, gemeinhin Spam genannt.

Bei vielen Mail-Programmen kann man Filter einstellen, die bei bestimmten Absendern, verdächtigen Wörtern und nach anderen Kriterien neue E-Mail aussondern. Wer das versucht hat, hat wohl bemerkt, dass er so mehr Arbeit hat, als wenn er Reklame-Mail selbst gelöscht hätte.

Spam-Filter neuer Art

Die neue Erkenntnis ist nun, dass eine Spam-Mail sich vor allem durch ihren Inhalt verrät. Ein Antispam-Programm braucht also nur ein Wortverzeichnis aufzubauen und für jedes Wort mitzuzählen, wie oft es in einer ordentlichen und wie oft in einer Spam-Mail vorkommt, um dann bei einer neu ankommenden Mail eine Voraussage treffen zu können.

Genau diesen Ansatz verfolgt das Deleatur-Programm. Vorteilhaft ist seine unkomplizierte und von einem Mailprogramm unabhängige Anwendbarkeit. Unkompliziert deswegen, weil keinerlei Konfigurierung nötig ist – unabhängig, weil Deleatur nur auf den Mails des POP-Servers arbeitet und ggf. schon dort Spam löscht. Näheres über die Funktionsweise lesen Sie bitte im letzten i nach.

Üblicherweise wird man mit Deleatur nach Mail schauen und nur dann, wenn ordentliche Mail übriggeblieben ist, sein normales Mailprogramm nach neuer Mail suchen lassen.

„Installation“

Interessenten gehen bitte folgendermaßen vor:

1. Man hole sich mit Hilfe von ZIVsoft (siehe ZIV-Webseite) die gezippten Dateien `deleatur.zip` (Programm) und, wenn man will, `spam.zip` (Wortbasis mit Wahrscheinlichkeiten) und entpacke sie in einem Ordner.

Einen zweiten Punkt gibt es nicht – eine eigentliche Installation findet nämlich nicht statt. Bei der ersten Benutzung wird man gefragt, welchen POP3-Server man benutzt und wie Kennung und Passwort lauten. Diese Daten merkt sich das Programm bis zum nächsten Aufruf in der Parameterdatei `deleatur.prm`, wobei das Passwort verschlüsselt wird.

Handhabung

Der Start erfolgt per Doppelklick auf die Datei `deleatur.exe`. Sinnvollerweise erstellt man sich eine Verknüpfung auf dem Desktop, dem Startmenü oder (besonders empfehlenswert) der Schnellstartleiste – ein Symbol wird mitgeliefert. Alles spielt sich in einem Konsolenfenster ab:

Hat man sich die angebotene Wortbasis nicht heruntergeladen, so fragt das Programm bei

```

deleatur.exe
DELEATUR 1.7 - Copyright 2003 Eberhard Sturm (sturm@uni-muenster.de)
Zentrum für Informationsverarbeitung - Westf. Wilhelms-Universität Münster

Es gibt folgende Reaktionen auf Anfragen des Programms:
+: Mail soll akzeptiert werden.
-: Mail soll als SPAM gelten.
=: Status gleich lassen, Mail ignorieren.
?: Mail soll angezeigt werden (erste 50 Zeilen).
Die leere Eingabe entspricht dem Vorschlag. Am Ende
erfolgt immer noch die Frage, ob tatsächlich gelöscht
werden soll.

Aktuelle Werte:
- Größe der Wortbasis: 1530 KB
- Untergrenze Wortbasis: 1400 KB
- Obergrenze Wortbasis: 2000 KB
- Löschgrenze: 75 %
- Akzeptanzgrenze: 15 %

Starten POP3-Sitzung mit "pop.uni-muenster.de" ...
Startzeit: 0 s.
Anmelden Nutzer "pudlatz" ...
Nutzer angemeldet.
Anmeldezeit: 1 s.
6 Mails auf dem Server:
1 =====
<<<<<: "invite" <returns-tukvcuzchubjkcc@opt.inbargains4u.com>
>>>>>: "friend" <pudlatz@uni-muenster.de>
=====: join our group friend
0.8? ----- Mail ist SPAM!

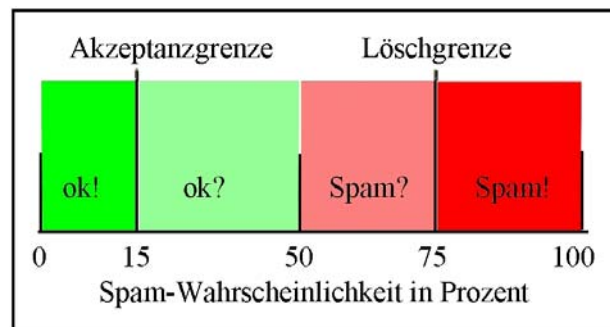
```

jeder Mail, ob sie Spam ist und merkt sich für jedes Wort der ersten 50 Zeilen, wie häufig es in einer Spam- und wie häufig in einer ordentlichen Mail vorkommt. Am Ende wird gefragt, ob die als Spam bewerteten Mitteilungen auf dem POP-Server tatsächlich gelöscht werden sollen.

Benutzt man die herunterladbare Wortbasis, so ist der größte Teil der Arbeit schon getan: Ein erheblicher Teil der Mail wird automatisch gelöscht und ein weiterer Teil sofort als ordentlich gewertet. Nur beim Rest fragt das Programm nach, ob die vorgeschlagene Bewertung (an roter bzw. grüner Schrift erkennbar) korrekt ist. Im Normalfall wird man nur ein paar Mal die Eingabetaste drücken müssen.

Mit wachsender Wortbasis wächst die Grenze für automatische Akzeptanz und fällt die Grenze für automatisches Löschen. Ist die Wortbasis größer als 1,5 MB, so hat sich das Programm auf folgende Maximalgrenzen eingestellt:

Unter 15 % und bei mehr als 75 % Spam-Wahrscheinlichkeit wird nicht mehr nachgefragt, bei Werten dazwischen wird ein entsprechender Vorschlag gemacht, je nachdem ob sie



unter oder über 0.5 liegt.

Hatte ein Spammer eine neue „Geschäftsidee“, so wird man bei den ersten Spam-Mails zu diesem Thema korrigierend eingreifen müssen. Dazu drückt man einfach die „-“-Taste (gefolgt von der Eingabetaste).

Andererseits: Hatte ein (ansonsten gutwilliger) Absender die Idee, eine HTML-Mail zu schicken, so kann es auch vorkommen, dass diese Mail als Spam gewertet wird. Hier hilft das „+“-Zeichen, um sie dennoch als „ordentlich“ zu bewerten. Probleme gibt es auch schon mal, wenn jemand glaubt, seiner Mail ein Gedicht befügen zu müssen: „Life is only a dream!“ enthält schon zwei verdächtige Wörter!

Ist man sich nicht sicher (pro Mail wird Absender, Empfänger und Betreff ausgegeben), so kann man sich per Fragezeichen die in die Bewertung eingegangenen ersten 50 Zeilen

anschauen.

In der folgenden Abbildung sieht man die mehr und weniger intensiv hervorgehobenen Bewertungen:

AIX und Linux

Benutzer aus der Paläontologie schrieben mir, dass sie noch Pine auf AIX benutzten, um

```

deleatur.exe
2 =====
<<<<<: " " <111@111.com>
>>>>>: "new020913-300000-400000" <111@111.com>
=====: 010-82561122 021-64477506
0.05 ----- Mail ist SPAM!

3 =====
<<<<<: "dieter frieler" <frieler@uni-muenster.de>
>>>>>: <ziv-all@uni-muenster.de>
=====: betriebsausflug
0.17 ++++++++ Vorschlag: Mail sei akzeptiert! (?/=/-)

4 =====
<<<<<: gqtkeriann <dxkiara@yahoo.com>
>>>>>: pudlatz@uni-muenster.de
=====: your application was accepted. dynqd
0.06 ----- Mail ist SPAM!

5 =====
<<<<<: system administrator <root@printfix.uni-muenster.de>
>>>>>: pudlatz@ganzfix.uni-muenster.de
=====:
0.48 ++++++++ Vorschlag: Mail sei akzeptiert! (?/=/-)

6 =====
<<<<<: "ben kwong" <benkwong@mail.com>
>>>>>: "senior@info.com" <pudlatz@uni-muenster.de>
=====: go north and save big
0.00 ----- Mail ist SPAM!

Mail automatisch gestrichen: 4
Mail korrekt als Spam bewertet: 0
Mail fälschlich als Spam bewertet: 0
Mail automatisch akzeptiert: 0
Mail korrekt akzeptiert: 2
Mail fälschlich akzeptiert: 0
Mail nicht bewertet: 0

4 Mails zu löschen.
Was soll geschehen?
- werten, ggf. löschen, beenden => Eingabetaste
- werten, nicht löschen, beenden => w
- nicht werten, nicht löschen, beenden => n
- nicht werten, einzeln noch einmal => e

Mail 6 gelöscht.
Mail 4 gelöscht.
Mail 2 gelöscht.
Mail 1 gelöscht.
Abmelden Nutzer "pudlatz" ...
Stoppen POP3-Sitzung mit "pop.uni-muenster.de" ...
Sitzung beendet.
Fenster schließen?_

```

nach Mail zu schauen, und ob ich Deleatur nicht auch nach AIX portieren könne. Tatsächlich ist es mir innerhalb eines Tages gelungen (nach Schlachten mit Codepage 850, "littleendian"-Bytefolge, ANSI-Farben, LF statt CRLF), das Programm Deleatur auf AIX zum Laufen zu bringen. Sogar die Wortbasis ist identisch mit der von Windows, was für den Compiler spricht, da die Bytefolge von Zahlen bei Windows an sich umgekehrt ist. In der Programmiersprache PL/I reicht da ein Schlüsselwort, um anzugeben, welche Bytefolge man gerne verwenden möchte. Leider sind die Hintergrundfarben nicht ganz so knallig wie bei Windows.

Wie benutze ich Deleatur also unter AIX? Ich lege z. B. einen Ordner namens Deleatur an, gehe mit `cd` in diesen Ordner und gebe dann einfach ein:

```
deleatur
```

Vorher kann ich, wenn ich möchte, noch die Windows-Wortbasis `spam.basis` (klein geschrieben!) in diesen Ordner packen. Man sollte sich aber klarmachen, dass zwar die Spam-Wörter bei allen Nutzern ähnlich sein werden, die „guten“ aber bei jedem anders, vor allem, wenn man auch fremdsprachliche Korrespondenz führt.

Die AIX-Version eröffnet auch Linux-Benutzern einen Weg, Deleatur zu verwenden. Zwar gibt es noch keinen PL/I-Compiler für Linux, aber ein Universitätsangehöriger hat ja Zugriff auf AIX, kann also z. B. mit SSH eine Terminalsitzung starten und so die AIX-Version von Deleatur vor seinem Linux-Mailprogramm aufrufen.

Sollte es noch OS/2-Anwender geben: Für dieses Betriebssystem ist Deleatur auch direkt erhältlich – es gibt ja schließlich nur einen PL/I-Sourcecode!

Spezialwünsche

In der mitgelieferten Datei `liesmich.txt` werden Einstellmöglichkeiten vorgestellt für diejenigen, die meinen, noch an etwas „drehen“ zu müssen. Erwähnenswert sind zwei Dinge, die durch Angaben in der Parameterdatei `deleatur.prm` eingestellt werden können:

Zum einen kann man mehrere Verknüpfungen mit unterschiedlichen Parameterdateien verwenden, um bei mehreren Diensteanbietern nach Mail schauen zu können. Man könnte z. B. in einer Windows-Kommandodatei namens `deleatur.cmd` schreiben:

```
deleatur anbieter1.prm
deleatur anbieter2.prm
```

Wenn man dann zwei leere Dateien `anbieter1.prm` und `anbieter2.prm` erstellt, so erfragt Deleatur beim Start alle notwendigen Angaben und speichert sie in die jeweilige Datei. Wenn man nur einen Ordner für alles verwendet, wird auch für beide Anbieter dieselbe Wortbasis benutzt und aktualisiert.

Zum anderen kann man die Programmdateien auf einen Fileserver legen, so dass Benutzer immer auf die aktuelle Version zugreifen können, dabei auf dem eigenen Rechner aber nur Platz für die modifizierbaren Dateien benötigen.

Linux-Parallelrechner in Betrieb

St. Ost

Nach einer längeren Test- und Aufbauphase und der Lösung betrieblicher Probleme steht der Linux-Parallelrechner `zivcluster` nun allgemein zur Verfügung.

Der Rechner besteht aus 94 Rechnerknoten und 2 so genannten Kopfstationen, die das Gesamtsystem steuern und verwalten. Jeder Rechnerknoten besitzt einen mit 2,2 GHz getakteten Xeon-Prozessor, der breitbandig auf 1 GB Hauptspeicher zugreifen kann. Zur Speicherung temporärer Daten stehen auf jedem Knoten 40 GB Plattenplatz zur Verfügung. Rechnerknoten und Kopfstationen sind zweifach vernetzt: Über das *Myrinet* können die rechnenden Programme untereinander besonders schnell kommunizieren. Die zusätzlich installierte FastEthernet-Infrastruktur dient der Installation, Wartung und Pflege der Rechnerknoten.

Gesteuert wird der Rechner von den Kopfstationen aus. Diese dienen gleichzeitig als Portal für die Rechnernutzer, denen 700 GB zur Speicherung von nicht-temporären Daten zur Verfügung stehen. Die Daten werden auf schnellen Fibre-Channel-Platten gespeichert und von beiden Kopfstationen parallel den Rechnerknoten über das *Myrinet* zur Verfügung gestellt. Die Zuteilung von Rechnerknoten zu Rechenaufträgen (Jobs) übernimmt das *Portable Batch System* (PBS). Betrieben werden Rechnerknoten und Kopfstationen unter RedHat-Linux.

Benutzt werden kann der Cluster von Institutsangehörigen und Nutzern des Rechnerverbundes NRW. Nähere Informationen zur Nutzung des Parallelrechners finden Sie unter der URL <http://zivcluster.uni-muenster.de>. Anfang Oktober 2003 findet eine „Einführung in die Benutzung des Parallelrechners“ statt. Nähere Informationen zu dieser Lehrveranstaltung finden Sie unter der URL http://www.uni-muenster.de/ZIV/Lehre/2003_Wintersemester/www11.html.

20.000 TP-Anschlüsse – und kein Ende?

N. Gietz

Die zeitgemäße LAN-Versorgung von Universität und UKM hat einen Meilenstein erreicht – der Weg führt weiter.

Kaum ein Gerät der Informationselektronik wird heute noch ohne Datenkommunikationsanschluss hergestellt und betrieben. Nicht nur die PCs als quasi die klassischen Rechner, auch Notebooks, PDAs, Telefone, Analyse- und Messgeräte sowie Geräte der Gebäudeleittechnik werden heute vernetzt. Selbst der Fernseher zuhause wird mit wenig Mehrausstattung zum Internet-Terminal.

Diese „ubiquitäre“ Verbreitung von netzwerkfähigen Geräten macht in Gebäuden eine flächendeckende Versorgung mit leistungsfähiger LAN-Technologie (LAN: Local Area Network, z. B. Ethernet) erforderlich. Um den erkennbar wachsenden Anforderungen gerecht zu werden und um eine flexible, zukunftssichere Infrastruktur aufbauen zu können, wurde bereits Mitte der neunziger Jahre eine Norm zur so genannten strukturierten Verkabelung verabschiedet, die im Rahmen einer einheitlichen Kabel-Infrastruktur die Versorgung einer Vielfalt von IT-Systemen ermöglichen sollte. Diese Norm sieht die systematische Verlegung von eigenen Kommunikationskabeln zu jedem einzelnen Gerät vor. Im letzten Jahr wurde diese Norm überarbeitet und den neuesten Entwicklungen angepasst, so dass vom Telefon über das digitale Video-Übertragungssystem bis zum Server mit Gigabit-Ethernet-Anschluss praktisch alle modernen digitalen Systeme der Informationsübertragung und -verarbeitung einheitlich verkabelungstechnisch versorgt werden können. Insbesondere wurden in diese überarbeitete Norm auch neue anspruchsvollere Kategorien für übertragungstechnische Eigenschaften der Kabel festgelegt, so dass auch die neueren LAN-Technologien wie Gigabit-Ethernet sicher auf solchen Verkabelungen eingesetzt werden können.

Zur Zeit haben Jubiläen der Informationstechnologie Hochkonjunktur:

- Die Erfindung des Ethernets hat sich gerade zum 30. Mal gejäht – unglaublich aber wahr, zumal Ethernet in all seinen Varianten heute die zeitgemäße LAN-Technologie schlechthin ist,
- der IBM-PC ist bereits im vergangenen Jahr 20 Jahre Maßstab für den PC an sich gewesen,
- 2004 werden wir auf 20 Jahre LAN an der Universität zurückblicken können,
- der oben genannte Standard für strukturierte Verkabelung existiert seit 10 Jahren.

Da trifft es sich auch gut, dass das ZIV im April 2003 den 20.000. TP-Anschluss für die Universität und das Universitätsklinikum (UKM) in Betrieb nehmen konnte; TP-Anschluss steht hier für den standardisierten (d. h. also normgerechten strukturierten) Anschluss auf der Basis einer Verkabelung mit vier Paaren verseilter Kupferadern (Twisted Pairs). Hier wurde ein Meilenstein erreicht, der durchaus eines kurzen Blickes zurück auf die vielfältigen Weichenstellungen und Anstrengungen wert sein sollte, wovon viele den Endnutzern am Rechner bisher kaum aufgefallen sein dürften.

Bereits bei den ersten TP-Installationen der Universität Mitte der neunziger Jahre wurde soweit als möglich – und nicht ganz standardkonform – auf Verteiler in den Gebäudeetagen verzichtet und die Verkabelung auf möglichst nur einen Gebäudeverteiler konzentriert. Hierdurch konnten mehrere hundert Verteiler eingespart und die eingesetzte Elektronik („Hubs“, Repeater und Switches) konnte deutlich effektiver ausgenutzt werden, zusätzlich reduzierte sich dadurch die Anzahl der Verbindungen an den Kernnetzbereich (Backbone). Interessanterweise sieht die neueste Version des Standard genau solch eine Verkabelungsstruktur optional nun auch vor, so dass unsere Vorgehensweise im Nachhinein als „legitimiert“ gelten kann.

Beim Kabelmaterial wurde vom ZIV bereits 1995 ein nur geringfügig teurerer, aber hochwertiger Typ ausgewählt, der auch heute noch bei Neuinstallationen verwendet wird und der den Anforderungen der erst 2002 definierten Kategorie 6 (z. B. für Gigabit-Ethernet) entspricht und Reserven für zukünftige Technologien bietet. In der gesamten TP-Verkabelung der Universität und des UKM können heute also alle verfügbaren LAN-Technologien einschließlich Gigabit Ethernet eingesetzt werden.

Anfänglich musste noch erhebliche Überzeugungsarbeit für die strukturierte Verkabelung geleistet werden; der bis dahin verwendete koaxiale Bus des Ethernets war zum Einen weniger aufwendig in der Installation und konnte leicht erweitert werden und zum Anderen schien die separat betriebene Verkabelung für die Telefonie ausreichend, aber schließlich überzeugten die besseren Betriebseigenschaften (insbesondere die Managementfähigkeit), die höhere Zuverlässigkeit, die Abhörsicherheit und die Flexibilität in der Nutzung durch unterschiedliche Medien (Konvergenz der Medien). Diesen Weg einzuschlagen war schließlich unumgänglich, da die etwas später eingeführten und nun Markt beherrschenden Technologien wie Dedicated Ethernet, Fast Ethernet, schließlich Gigabit-Ethernet und zukünftig IEEE 802.1x (Authentifizierung gegenüber dem Netz) eine Verkabelung nach der genannten Norm (EN 50173) ohnehin zwingend erforderlich machen. Allein aus Gründen der Sicherheit in der Informationsverarbeitung müsste man heute diese Technologie einführen – nur diese Technologie erlaubt es uns heute mit wirtschaftlich vertretbarem Aufwand Nutzergruppen in so genannten virtuellen LANs (VLANs) so zusammenzuführen, dass diese mit netztechnischen Mitteln (Firewalls) vor unerwünschten Zugriffen gemäß ihrem spezifischen Bedarf individuell geschützt werden können. Schließlich muss man den Schritt zur strukturierten Verkabelung auch vor dem Hintergrund sehen, dass die LAN-Technologie an der Universität zum damaligen Zeitpunkt gerade vor etwas mehr als 10 Jahren (Ende 1984) als Innovation mit anfänglich astronomisch hoch erscheinenden Übertragungsraten eingeführt worden war (unvorstellbare 10.000.000 Bit pro Sekunde gegenüber maximal 19.600 Bit pro Sekunde auf einzelnen gesonderten Punkt-zu-Punkt-Verbindungen!), und die Gesamtversorgung der Universität war ja selbst nach damaligen Vorstellungen bei weitem nicht erreicht. Ja, man hatte sogar anfänglich die vage Hoffnung, dass die Koaxialverkabelung der IV-Versorgung über mehrere Dekaden gerecht werden würde.

Da diese alten Netze den Anforderungen nicht mehr gewachsen sind und auch Ersatzteile kaum noch beschafft werden können, wird die Universität die Unterstützung für die koaxialen Bussysteme zum Ende dieses Jahres einstellen. Aufgrund eines entsprechenden Beschlusses des Rektorates haben viele Fachbereiche bereits in erheblichem Umfang in die Umwandlung der alten AUI-Anschlüsse investiert, entsprechend sind auch zentrale Mittel der Universität (bzw. des ZIV) und HBMG-Mittel in entsprechenden Baumaßnahmen umgesetzt worden. Wenn also Ende dieses Jahres dieser Prozess abgeschlossen sein sollte – hier sind durchaus noch weitere Anstrengungen bis dahin notwendig –, ist letztlich nur ein vorläufiger Schlussstrich gemacht, der nur den Technologiewandel der vernetzten Datenverarbeitung im engeren Sinne beschreibt.

Ohne Frage kann auch mit 20.000 TP-Anschlüssen von einer vollständigen Versorgung der bekannten IV-Strukturen an Universität und UKM noch keine Rede sein – mancher Angehöriger von Universität oder UKM ohne vernetzten Arbeitsplatz wird dies bestätigen können. Darüber hinaus wird aber die unabwendbar erscheinende Konvergenz der heute noch weitgehend nebeneinander betriebenen Netze (Telefonie bzw. Voice over IP – VoIP, Video, Gebäudeleittechnik, Sicherheitstechnik usw.) in den nächsten Jahren den Anschlussbedarf weiter verstärken. Und letztlich werden Techniken wie das neue Internet-Protokoll IPv6, das bereits in den Startlöchern steht und das im Rahmen internationaler Projekte, an denen sich auch das ZIV beteiligt, bereits pilotartig eingeführt wird (z. B. im europäischen Forschungsnetz GEANT), dafür sorgen, dass auch Geräte wie selbstverständlich vernetzt und über das Internet global erreichbar gemacht werden, an die bisher meist nur Technologiespezialisten denken: elektrische Steckdosen, Klimaanlage, Beamer, Stromzähler, ... Bei diesen Beispielen handelt es sich keineswegs nur um Visionen, sondern um verfügbare und sinnvoll einsetzbare Produkte! Bei Betrachtung dieser Perspektiven muss das in der Überschrift gesetzte Fragezeichen sicherlich in ein Ausrufezeichen geändert werden: 20.000 Anschlüsse – und kein Ende!

Langzeit-Ausleihe von Funk-LAN-Karten

G. Richter

Die Universität fördert den Einsatz des *Mobile Computing* durch Ausleihe von Funk-LAN-Karten.

Allgemeines

An Standorten mit universitätsöffentlichen Funk-LAN-Zellen können Studierende mit mobilen Rechnern Zugang zum Rechnernetz der Universität und seinen angeschlossenen Diensten, damit auch zu weiteren Netzen, insbesondere zum Internet erhalten. Mindestvoraussetzung der mobilen Rechner ist eine WLAN-Ausstattung. Für Notebooks mit sogenanntem PCMCIA-Slot können entsprechende Funk-LAN-Karten (WLAN-Karten) verwendet werden.

Die Universität Münster fördert den Einsatz des mobilen Computing für seine Angehörigen, insbesondere natürlich auch seine Studierenden. Die Universität wird deshalb weitere Funk-LAN-Zellen einrichten und leiht deshalb WLAN-Karten auch längerfristig aus. Für die eigene Beschaffung von Karten durch Studierende gibt das ZIV Hinweise und ggf. Unterstützung.

Unter <http://www.uni-muenster.de/ZIV/Rechnernetz/wlan/kurzausleihe.html> erfahren Sie, wie Sie Funk-LAN-Karten kurzfristig für einen kürzeren Zeitraum ausleihen.

Ausleihe

Die im Folgenden dargestellten Regelungen gelten ab Mai 2003 und lösen ältere Regelungen bei Neuausleihen ab. Für die bisherigen Ausleihen gelten die alten Regelungen weiter. Die Fassungen früherer Ausleiheregulungen finden Sie unter <http://www.uni-muenster.de/ZIV/Rechnernetz/wlan/Ausleihe/Archiv/>.

Funk-LAN-Karten werden gegen 60 € Kautionsausleihe ausgeliehen. Die Ausleihdauer beträgt maximal ein halbes Jahr; Dauerausleihe ist möglich. Es ist folgende Verfahrensweise für die Ausleihe von Funk-LAN-Karten festgelegt worden:

- Interessierte beantragen eine Funk-LAN-Karte einfach per E-Mail an das Netz-Informationen-Center (NIC); bitte geben Sie unbedingt an
 - Ihren vollständigen Vor- und Nachnamen,
 - Ihre Nutzerkennung im ZIV (diese ist Voraussetzung für die Nutzung der Funk-LANs an der WWU, Anträge können am Service-Schalter des ZIV gestellt werden),
 - die von Ihnen regelmäßig genutzte E-Mail-Adresse; falls noch keine E-Mail-Adresse vorhanden ist, erhalten Sie ohnehin eine solche mit der unbedingt notwendigen Beantragung einer Nutzerkennung im ZIV (s. o.): <userid>@uni-muenster.de, dabei ist <userid> durch die Ihnen zugeordnete Kennung zu ersetzen,
 - Ihre vollständige Adresse am Hauptwohnsitz und Ihre Telefonnummer,
 - Ihre vollständige Adresse am Studienort und Ihre Telefonnummer, soweit zutreffend (soweit Studierende/r),
 - Ihre Matrikelnummer (soweit Studierende/r), sonst die Bezeichnung Ihrer Einrichtung der Universität,
 - Ihre Bankverbindung (Bezeichnung des Bankinstituts, Bankleitzahl und Kontonummer, ggf. Name des Kontoinhabers, falls nicht identisch) für die Rücküberweisung der Kautionsausleihe,
 - den Typ Ihres Laptops und das Betriebssystem.
- Allen Antragstellern wird per E-Mail mitgeteilt, ob und wann sie eine Funk-LAN-Karte gegen Kautionsausleihe erhalten können. Wenn Sie eine positive Benachrichtigung erhalten, müssen Sie innerhalb von 14 Tagen bei der Universitätskasse, Schlossplatz 2 (im „Schloss“) 60 € als Kautionsausleihe einbezahlen; geben Sie dort bitte als Stichwort an

ZIV - Funk-LAN - <xxx>

Dabei ist <xxx> eine Bezugsnummer, die wir Ihnen im Fall einer positiven Nachricht

in gleicher E-Mail mitteilen.

- Unter Vorlage der von der Universitätskasse erhaltenen Quittung kann dann die Funk-LAN-Karte am Service-Schalter des ZIV (Einsteinstraße 60) abgeholt werden; auf der Quittung wird ein Vermerk über den Erhalt der Karte angebracht, auf einem Lieferschein (Empfangsbestätigung) bestätigen Sie den Erhalt der Karte, von dem Lieferschein erhalten Sie eine Kopie. Die Vergabe der Funk-LAN-Karten wird laufend durchgeführt, das zur Verfügung stehende Kontingent ist leider immer wieder schnell ausgeschöpft. Trotzdem sollten Interessenten auch dann Funk-LAN-Karten per E-Mail beantragen, wenn bekannt ist, dass gerade das Kontingent erschöpft ist. Für die Vergabe der Karten gibt das Eingangsdatum der E-Mail den Ausschlag, zunächst nicht berücksichtigte Interessenten kommen auf eine Warteliste.

Mit dem Empfang der Leihgabe verpflichtet sich der Empfänger

- zur Rückgabe innerhalb eines halben Jahres
- oder aber zu automatischem Verzicht auf Rückerstattung der Kautions bei gleichzeitiger Übernahme der Karte als **Dauerleihgabe**, wenn die Rückgabe nicht termingerecht erfolgt.
- Die Rückgabe der Karten erfolgt unter Vorlage der genannten Empfangsbestätigung am Service-Schalter im ZIV. Sie erhalten über die Kartenrückgabe natürlich eine Quittung und erhalten die gezahlte Kautions per Banküberweisung zurückerstattet.

Beschaffung eigener Karten durch Angehörige der Universität

Das ZIV unterstützt bisher ausschließlich folgende Funk-LAN-Karten im Einsatz in Notebooks mit neueren Microsoft-Windows-Betriebssystemen:

- Orinoco PC Card Turbo 11 MB Silver PC Card – Zulassung entsprechend ETS EUROPE (ohne Frankreich),
- dto. als Gold-Version (heutige Standardversion),
- alle baugleichen Karten mit identischer Software [Karten des Herstellers Proxim (ehemals Lucent, dann Agere), nach Aussagen des OEM-Herstellers Avaya sind dessen Karten auch baugleich und mit Original-Hersteller-Software betreibbar; in der Ausleihe sind Karten von Lucent und Avaya].

Voraussetzung ist ein Steckkartenplatz des Typs PCMCIA Type II Extended. Das Orinoco-Produkt ist bereits in höherer Stückzahl im Einsatz.

Für Rechner mit PCI-Slots, USB-Anschluss oder in Apple-Technologie existieren in der Orinoco-Produktreihe entsprechende Adapter bzw. gesonderte Funk-LAN-Karten.

Im Grundsatz sollten alle Rechner-Funk-LAN-Ausrüstungen kompatibel sein mit der Installation an der Universität Münster, wenn diese dem Standard **IEEE 802.11b (DSSS HR)** mit europäischer Frequenznutzung und den Qualitätsmerkmalen **WEP** und **WiFi** entsprechen. Dementsprechend wird vom ZIV keine besondere Kartenempfehlung herausgegeben. Erfahrungen mit anderen Technologien, z. B. Modemtechnologie, haben in der Vergangenheit jedoch gezeigt, dass trotz Standardisierung deutlich weniger Interoperabilitätsprobleme und Nutzerfragen auftreten, wenn Technologie ein und desselben Herstellers auf beiden Seiten (hier: im Rechner und in der Funk-LAN-Infrastruktur) verwendet wird. Vor einem Kauf einer Funk-LAN-Karte sollte man sich deshalb zumindest überzeugen, dass diese Orinoco-kompatibel ist bzw. dass man ein Rückgaberecht erhält.

Das ZIV plant baldmöglichst den neuen 54 MBit/s-Standard **IEEE 802.11g** verfügbar zu machen und auch bisher vorhandene Funk-LAN-Zellen abwärtskompatibel aufzurüsten. Es soll also in Funk-LAN-Zellen in Zukunft sowohl IEEE 802.11b als auch IEEE 802.11g nutzbar sein. Da aber keine endgültigen Regelungen bisher getroffen werden konnten, können auch keine weitergehenden Kaufempfehlungen gegeben werden.

Ein Verkauf von Funk-LAN-Karten über die Universität oder eine Verkaufsvermittlung wird zzt. nicht ausreichend nachgefragt und ist derzeit nicht geplant.

Preisliste für LAN-Anschlüsse

G. Richter

Die Preise für die Umwandlung von TP-LAN-Anschlüssen mit Repeater wurden halbiert.

Ab 5.6.2003 gilt bis auf Widerruf für alle Einrichtungen der Westfälischen Wilhelms-Universität eine neue Preisliste für LAN-Anschlüsse. Sie löst damit frühere Preisinformationen ab. Für das Universitätsklinikum Münster (UKM) gelten eigene Regelungen; Anforderungen sind dort stets an die Verwaltung des UKM zu richten.

Bei den Preisen handelt es sich um grundsätzlich geregelte Pauschalpreise aufgrund des Beschlusses des IV-Lenkungsausschusses (IVL) und des Rektorats vom Dezember 2001 und Anpassungen der Server-Anschlussaufpreise im Dezember 2002. Weiter wurden die Pauschalpreise für Umwandlungen von Twisted-Pair-Anschlüssen mit Repeater-Technologie durch Beschluss des IVL am 5.6.2003 weiter reduziert (halbiert). Im Durchschnitt decken diese Pauschalpreise bei weitem nicht die tatsächlich entstehenden Kosten. Sollten die tatsächlichen Kosten im Einzelfall unter den Pauschalpreisen liegen, so begründet dies keinen Anspruch auf Berechnung der geringeren Kosten.

Bestellungen für Bau- und Lieferleistungen sind stets in schriftlicher Form an das Zentrum für Informationsverarbeitung (ZIV) zu richten: Für LAN-Anschlüsse sind besondere Formulare zu verwenden, für Materiallieferungen sind die üblichen Bestellscheine der Universität zu verwenden. Materialien müssen in der Regel beim ZIV abgeholt werden.

Bitte beachten Sie auch die Informationen zur Außerbetriebnahme von AUI-Anschlüssen bis Ende 2003!

Einzelheiten entnehmen Sie bitte der Tabelle in

http://www.uni-muenster.de/ZIV/Rechnernetz/LAN/preisliste/2003_06_06.html

Die Akkumulation von Anschlüssen zur Erzielung der dort genannten Pauschalpreise ($n > 1$) kann nur jeweils für ein Gebäude und nur innerhalb einer Baumaßnahme vorgenommen werden; pro Maßnahme kann in der Regel nur eine einzige Belastung zu Lasten des Titels einer Einrichtung erfolgen. Bitte wenden Sie sich an Ihre IV-Versorgungseinheit mit der Bitte um Koordination, wenn verschiedene Einrichtungen innerhalb eines Gebäudes Anschlüsse gesammelt beantragen wollen. In den Fällen, in welchen gleichzeitig Neuanschlüsse und Anschlussumwandlungen beantragt werden, wird eine „Bestabrechnung“ zugunsten der antragstellenden Einrichtung durchgeführt; d. h. zunächst werden die Umwandlungskosten und danach die Neuanschlusskosten in die Rechnung einbezogen.

Ein neuer Posterdrucker im ZIV

J. Hölters

Zur Verbesserung der Qualität der Ausdrücke im Großformat hat das ZIV einen Drucker vom Typ HP Designjet 5500 PS angeschafft. Dieser Drucker ist völlig software-kompatibel zu den bisher eingesetzten Druckern vom Typ HP Designjet 2500 CP.

Der neue HP-Drucker ist schon seit einigen Wochen mit Erfolg in Betrieb und übernimmt zur Zeit die Druckaufträge in Fotoqualität. Da er außerdem die Druckzeit pro Druckauftrag mehr als halbiert und das bei besserer Ausgabequalität, ist eine deutliche Entspannung bei den Warteschlangen der Großformatdrucker zu beobachten.

Die Qualitätssteigerung ist im Wesentlichen im Bereich von hellen Farbtönen, die bisher als Streumuster auf dem Papier sichtbar waren, erkennbar. Möglich wird dies durch zwei zusätzliche Pastelltinten bei diesem Drucker.

Die Kosten für Ausgaben auf diesem Gerät ändern sich gegenüber den bisherigen Drucksystemen nicht.

wwuzugang – Ein Terminal zum Netz der WWU

M. Kamp

Ein Terminal-Server ermöglicht den Zugang aus Fremdnetzen zu geschützten Informationsangeboten im Universitätsnetz.

Häufig stellt sich Nutzern des Rechnernetzes der Universität das Problem, dass verschiedene Informationsangebote im Web oder andere Netz-Dienste, die von Einrichtungen der Universität angeboten werden, nur von Rechnern im Netz der Uni erreicht werden können, der Zugriff aus fremden Netzen aber verboten wird. In den meisten Fällen kann VPN als elegante Lösung betrachtet werden, um den Zugang von außerhalb dennoch zu ermöglichen (siehe i 2/2001 „Virtuelle Private Netze an der WWU im Test“). In besonderen Fällen reicht dies jedoch nicht aus, weil eine Datenbank z. B. aus Lizenzgründen nur von festen Internet-Adressen genutzt werden darf¹ oder weil der Nutzer auf dem gerade verwendeten Gerät keinen VPN-Client zur Verfügung hat.

Eine andere Möglichkeit ist die Nutzung eines Microsoft-Terminal-Servers. Dies ist ein spezieller Windows-Server, den man genau so wie jedes übliche Windows-System nutzen kann. Die Bildschirmausgabe des Nutzers wird dabei über das Datennetz auf den eigenen Rechner des Nutzers umgeleitet und dort dargestellt, der Server wird sozusagen über das Netz fernbedient. Wenn der Terminal-Server im Netz der Universität betrieben wird, hat er Zugriff auf die gewünschten universitätsinternen Angebote, stellt das Ergebnis aber auf dem lokalen Rechner dar, der innerhalb eines anderen Netzes betrieben werden kann. Das ZIV hat einen Microsoft-Terminalserver mit dem Namen `wwuzugang.uni-muenster.de` eingerichtet, der von allen Universitätsangehörigen genutzt werden kann. Es muss lediglich vor der ersten Nutzung die Windows-Nutzerkennung aktiviert worden sein. Dies kann unter <https://www.uni-muenster.de/exec/passwd> erledigt werden.

Zugang zu einem Terminal-Server erhält man über einen Microsoft-TerminalserverClient. Seit Windows XP ist dieser in Microsoft-Betriebs-Systemen bereits vorhanden (unter Start -> Programme -> Zubehör -> Kommunikation -> Remote Desktop Verbindung). Auf älteren Windows-Systemen muss ein Client erst installiert werden. Erhältlich ist dieser z. B. von Microsoft unter <http://www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp>. Ein Macintosh-Client wird ebenfalls von Microsoft unter <http://www.microsoft.com/mac/DOWNLOAD/MISC/RDC.asp> angeboten. Für Linux-Nutzer bietet sich als Alternative z.B. der Client „HOBLink JWT“ der Firma HOBLink an (kostenlose Testversion unter <http://www.hob.de>).

Auf `wwuzugang` sind nur wenige Applikationen zur Nutzung bereitgestellt: Internet Explorer, Secure-Shell, Acrobat Reader. Es handelt sich also im Wesentlichen um Anwendungen, die man beim Zugang zu universitätsinternen Diensten benötigt. Bei Bedarf kann die Liste der Applikationen für spezielle Netzdienste unter Umständen erweitert werden. Im Gegensatz zu den schon vorhandenen universitätsöffentlichen Terminal-Servern des ZIV stellt dieser Server also keine besondere Anwendungssoftware zur Verfügung und ist aus dem gesamten Internet erreichbar.

Da es sich hier nur um eine besondere Art des Netzzugangs handeln soll, ist der verfügbare Plattenplatz für jeden Nutzer auf 100Mbyte beschränkt. Die Nutzer-Daten können jederzeit gelöscht werden, ohne die Daten zu archivieren. Es sollten also keine Daten auf dem Server gesammelt werden!

In einer Sitzung gesammelte Daten können mit Hilfe von PerMail (<https://permail.uni-muenster.de>) als Anhang einer E-Mail verschickt werden. Falls es sich um eine größere Anzahl von Dateien handelt, können diese vorher mit dem installierten Tool „Power Archiver 2000“ in eine Archiv-Datei eingepackt werden, die später auf dem eigenen Rechner wieder ausgepackt werden kann.

Wer einen aktuellen Terminalserver-Client von Microsoft verwendet, kann vor der Anmeldung am Terminal-Server einstellen, dass seine lokalen Laufwerke (Diskette, Festplatte) vom Server aus mitgenutzt werden können.

Zur Sicherheit ist dieser Server durch einen Virensch scanner geschützt.

¹ Bei VPN werden die IP-Adressen dynamisch vergeben.

CHAP nicht von PAPpe

Passwortverschlüsselung für Einwahl und VPN

M. Kamp / M. Speer

Mit CHAP wird der authentifizierte Zugang zum Rechnernetz sicherer.

Das ZIV betreibt eine Vielzahl von Netzzugangssystemen. Analog- und ISDN-Einwahlsysteme werden seit langem betrieben, Funk-LANs gibt es seit 2001 und die VPNZugänge befinden sich im Aufbau. All diese Technologien haben eines gemeinsam – die Authentifizierung des Benutzers beim Zugang zum Rechnernetz der Universität.

Eine inzwischen längst etablierte Technik zur Authentifizierung ist das so genannte *Remote Access Dialin User Service* Protokoll (RADIUS). Hierbei sendet der Nutzer seine Nutzerkennung mit seinem Passwort an das jeweilige Zugangssystem, dieses übermittelt die Information dann zur Überprüfung an einen so genannten RADIUS-Server und stellt bei Gültigkeit eine Datenverbindung zwischen dem Rechner des Nutzers und dem Rechnernetz der Universität her.

Die RADIUS-Server des ZIV nutzen bisher zur Authentifizierung der Nutzerkennung das Unix-DCE-System. Hierzu müssen dem RADIUS-Server Kennung und Passwort mitgeteilt werden. Dabei wurde bisher das *Password Authentication Protocol* (PAP) verwendet, bei dem das Passwort unverschlüsselt vom Nutzer zum Zugangssystem gesendet wird. Unter ungünstigen Umständen könnte es auf dem Übertragungsweg abgehört werden. Bei der Modem- oder ISDN-Einwahl mag dies nicht so gravierend sein, da das Passwort nur auf der Telefonleitung vom Nutzer zum ZIV übertragen wird, das Abhören durch Dritte ist dort nicht ohne besonderen Aufwand möglich. Anders verhält es sich aber bei Funknetzen, in denen alle Teilnehmer einer Funkzelle auch die Datenpakete der anderen Teilnehmer mithören können. Inzwischen kursieren bereits einschlägige Werkzeuge im Internet, die den Datenverkehr in Funknetzen abhören und nach Passwörtern durchsuchen, obwohl so etwas natürlich auch gesetzlich untersagt ist.

Ein sicheres Verfahren zur Authentifizierung ist das so genannte *Challenge Handshake Authentication Protocol* (CHAP). In einem Abfrage-Antwort-Mechanismus wird dem Klienten, der sich anmelden möchte, vom RADIUS-Server ein zufälliger Wert übermittelt, den dieser mit seinem Passwort verschlüsseln und zurücksenden muss. Auf der Gegenseite kann anschließend geprüft werden, ob der Zufallswert korrekt verschlüsselt wurde, das verwendete Passwort also korrekt ist. Das Problem dieses Verfahrens ist allerdings, dass das Passwort des Nutzers dazu auf dem RADIUS-Server im Klartext bekannt sein muss! Dies ist bisher nicht der Fall. Im DCE wird nur ein aus dem Passwort generierter Schlüssel gespeichert, das eigentliche Passwort ist daraus nicht zu berechnen. Deshalb konnte CHAP bisher nicht angeboten werden.

Das ZIV hat sich wegen der großen Bedeutung der IV-Sicherheit entschlossen, ein zusätzliches Passwort speziell für den authentifizierten Zugang zum Datennetz einzuführen und dieses in einer Datenbank zu speichern und auf den Radius-Servern vorzuhalten. Dieses Passwort soll im Folgenden als **Netzzugangspasswort** bezeichnet werden, da es für alle Formen des authentisierten Netzzugangs benutzt werden soll. Nutzer, die für ihre Kennung ein Netzzugangspasswort festgelegt haben, können sich bei der Einwahl anschließend nur noch mit diesem Passwort für den Netzzugang authentifizieren, auch wenn sie in manchen Fällen weiterhin das weniger sichere PAP als Zugangsprotokoll verwenden möchten.

Für Nutzer ohne Netzzugangspasswort wird das ZIV bis auf Widerruf weiterhin eine Authentifizierung über PAP anbieten, die mit dem zentralen Standard-Passwort genutzt werden kann. Langfristig soll PAP aber vollständig durch sichere Verfahren wie CHAP und zertifikatbasierte Verfahren, z. B. mit Smart-Cards abgelöst werden; Nutzer von authentifizierten Netzzugängen sollten also baldmöglichst ein zusätzliches Netzzugangspasswort festlegen.

Das Netzzugangspasswort kann über die WWW-Seite <https://www.nic.uni-muenster.de/Netzzugangspasswort> erstmalig festgelegt und danach auch geändert werden und muss sich vom zentralen Standard-Passwort unterscheiden.

Dieses Verfahren befindet sich derzeit in einer Testphase und wird in Kürze in den Pilotbetrieb übergehen. Anleitungen zur Konfiguration eines Endsystems zur Nutzung von

CHAP sind in Produktion und werden alle bisherigen Anleitungen zu den Netzzugängen ersetzen.

Unterstützt werden sämtliche im Regelbetrieb betriebenen Netzzugänge, also auch Uni@home, Uni@home plus, Teleport, Uni-interne Einwahl sowie alle VPN-Dienste (siehe auch <http://www.uni-muenster.de/ZIV/Rechnernetz/Zugaenge/uebersicht.html>).

Wer die Möglichkeit der CHAP-Authentifizierung bereits jetzt teilweise nutzen möchte, sollte folgendes beachten:

- Setzen eines „sicheren“ Netzzugangspasswort unter:
<https://www.nic.uni-muenster.de/Netzzugangspasswort>
Das Passwort kann nach spätestens 30 Minuten genutzt werden.
- Konfiguration des Authentifizierungsprotokolls auf dem Client-Rechner:
 - Bei Windows-Systemen im DFÜ-Netzwerk; verschlüsselte Passwort-Übertragung (CHAP) aktivieren, unverschlüsselte Passwort-Übertragung (PAP) darf dann nicht aktiviert sein. Die Varianten MS-CHAP oder MS-CHAPv2 werden nicht unterstützt.
 - Bei Linux-Systemen in der jeweiligen PPP-Konfiguration nur CHAP konfigurieren.

i in MIAMI

H. Pudlatz

Hier geht es leider nicht um einen Ausflug der i-Redaktion in das Surf-Paradies. Hinter dem groß geschriebenen Wort verbirgt sich natürlich ein Akronym.

MIAMI steht für das „Münstersche Informations- und Archivierungssystem Multimedialer Inhalte“ und ist eine kooperative Dienstleistung der Universitäts- und Landesbibliothek (ULB) und des Zentrums für Informationsverarbeitung (ZIV) der Universität Münster. Sie wurde ins Leben gerufen, um

- innovative Ansätze im Bereich Multimedia zu unterstützen,
- digitale Publikationsmöglichkeiten an der Universität auszubauen,
- Langzeit-Archivierung digitaler und multimedialer Dokumente sicherzustellen und
- einen möglichst freien Zugang zu Dokumenten für Forschung und Lehre zu bieten.

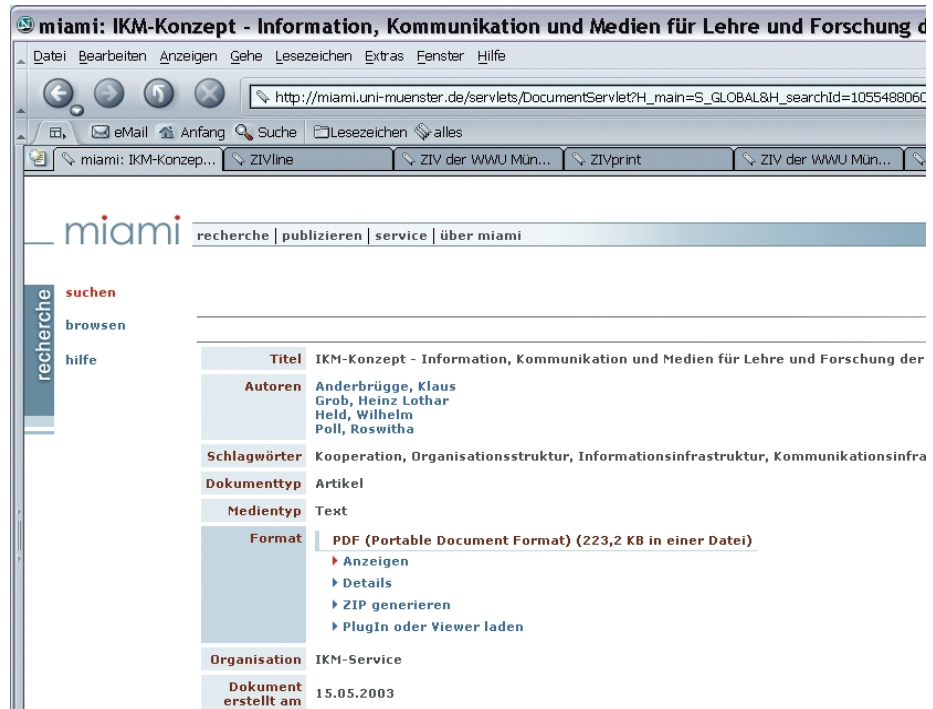
Das Konzept von MIAMI basiert auf dem Open Source Projekt MyCoRe, einem Archivierungsstandard für digitale Bibliotheken, an dem mehrere Universitäten zusammenarbeiten (In „MyCoRe“ stand „My“ früher für „MILESS Community“, dem digitalen Bibliotheksprojekt der Universität Essen, heute steht es für die lokale Anpassbarkeit eines allgemeinen „Content Repository“, das auf dem IBM Content Manager und der Datenbank DB2 desselben Herstellers basiert und ein umfangreiches Software-Projekt unter Verwendung von Java-Klassenbibliotheken und XML-Techniken darstellt).

Die organisatorische Betreuung von MIAMI hat die ULB übernommen, die Bereitstellung des MIAMI-Servers obliegt dem ZIV. MIAMI ist damit eine der ersten Realisierungen des IKM-Konzepts der Universität, das in diesem i vorgestellt wird.

Noch sind erst wenige digitale und multimediale Publikationen in MIAMI enthalten. Beim i sind es die auch schon vorher im Web bereitgestellten Jahrgänge ab 1993. Die Nachlieferung der Jahrgänge 1977–1992 in grafischer Form ist angedacht.

Wir ermuntern zum Aufsuchen der in MIAMI gespeicherten Informationen auf dem Server miami.uni-muenster.de. Man gelangt zu den zunächst nur als PDF-Versionen vorliegenden i-Heften über die Kommandos „recherche“ – „browsen“, findet das Zentrum für Informationsverarbeitung und klickt auf „inforum“ und „details“. Man erhält eine Liste der bisher gespeicherten 32 i-Ausgaben. Eine detaillierte Suche nach bestimmten Artikeln oder Schlagwörtern ist allerdings zzt. noch nicht möglich.

Auch das IKM-Konzept der Universität finden Sie in MIAMI außerhalb von i ausführlich dargestellt:



Regelmäßige Überprüfung der redundanten Internet/G-WiN-Anbindung

M. Speer

Eine dauerhafte, störungs-freie Internet-Anbindung ist für Hochschulen unverzichtbar. Ob die zur Erhöhung der Verfügbarkeit der Internet-Anbindung vorgenommenen Maßnahmen im Störfall auch wirklich funktionieren, muss regelmäßig überprüft werden.

Die gemeinsam von der Universität Münster, der Fachhochschule Münster und dem DFN-Verein seit Juni 2001 betriebene sog. Internet/G-WiN-Backup-Konfiguration realisiert bis zu einem gewissen Grad eine erhöhte Verfügbarkeit der Internet-Anbindung beider Hochschulen (vgl. einen entsprechenden Artikel im i Nr. 2/2001). Die Konfiguration wurde in der letzten Zeit mehrfach auf ihre Funktionalität überprüft. Diese Überprüfungen haben zu einigen sehr kurzen aber unvermeidbaren, in den Hot News angekündigten Unterbrechungen der Anbindung in den frühen Morgenstunden geführt und werden auch in Zukunft immer wieder durchgeführt werden.

Ob die Backup-Funktion tatsächlich noch gegeben ist, muss nämlich regelmäßig überprüft werden, da diese Funktion im Normalbetrieb nicht zum Tragen kommt, und daher ein Nicht-Funktionieren (aus welchen Gründen auch immer) der Backup-Konfiguration nicht unmittelbar erkennbar ist; gerade beim letzten Test im Mai zeigte sich, dass unerwarteter Weise auf Seiten des G-WiN neue Konfigurationsfehler entstanden waren. Bei einer solchen Überprüfung werden verschiedene Fehlersituationen simuliert: z. B. Ausfall des G-WiN-Anschlusses oder der Ausfall des G-WiN-Routers. Ein Hauptgrund für Probleme mit der G-WiN-Backup-Konfiguration sind – wie sich in der Vergangenheit gezeigt hat – Konfigurationsänderungen an einem der beteiligten Einzelsysteme, bei denen die speziellen Erfordernisse der Backup-Konfiguration übersehen wurden. Das Gesamtsystem besteht, wenn man sich auf die reinen Internet-Protokollfunktionen beschränkt, aus Komponenten (Routern) von derzeit drei beteiligten Einrichtungen: Universität, Fachhochschule und DFN-Verein. Dazu kommen noch die Systeme des Leitungsbetreibers (Deutsche Telekom).

An dieser Stelle wird klar, dass für die Realisierung von Redundanzfunktionen möglichst einfache Konfigurationen anzustreben sind. Auch aus diesem Grund wird derzeit im ZIV ein Projekt durchgeführt, bei dem neue Netzstrukturen realisiert werden, welche die Anbindung des Universitätsnetzes an Fremdnetze erheblich vereinfachen.

Auch der aktuelle Brand in einem Universitätsrechenzentrum in NRW mit längerem Totalverlust der Internet-Konnektivität zeigt, neben dem fast schon sprichwörtlichen Geschehen an der Universität Enschede im vergangenen Jahr, dass Redundanz in unseren modernen Datennetzen, die nun über etwa 20 Jahre gewachsen sind, ein Hauptanliegen zur Sicherung der Funktion und Dienstqualität sein muss.

McAfee VirusScan Enterprise

S. Zörkendörfer

Inbesondere auf Windows-Rechnern mit Anschluss ans Internet sollten Virenschutzprogramme mit aktuellen Virendefinitionen betrieben werden.

Die WWU hat einen Lizenzvertrag (s. <http://www.uni-muenster.de/ZIV/Organisation/SoftwareVerteilungMcAfeeVirusScan.html>) zu McAfee-Virenschutzprogrammen abgeschlossen. In diesem Artikel sind angesprochen erstmalige Nutzer (am dienstlichen Arbeitsplatz wie am häuslichen PC) sowie Nutzer von VirusScan Version 4.5.1 unter Windows NT, 2000 und XP und Systemadministratoren von Windows-Servern mit NetShield. (Für NetShield besteht bereits „End of Support“, für VirusScan 4.5 unter Win95/98/ME wird „End of Life“ zum 30.6.2004 angekündigt.) Zur Vermeidung von Verwechslungen sei darauf hingewiesen, dass diese Bezeichnungen und Versionsangaben unsere Lizenz für „Geschäftskunden“ betreffen und nicht die McAfee-Produkte der „Home Edition“.

Am 9. April wurde von McAfee eine Produktversion **VirusScan Enterprise Version 7.0.0** freigegeben. Wir haben dies u. a. in den ZIV-News (<http://www.uni-muenster.de/News/120.html>) angekündigt und die Installationsmaterialien Berechtigten bereitgestellt (z.B. <https://winkiosk.uni-muenster.de/VirScan/VirusScan/Windows/Enterprise/VSE700DE.zip>). In diesem Artikel sollen nun Einzelheiten zum Umstieg auf dieses Produkt genannt sein. Diese Empfehlungen sind immer noch nur vorläufig – sie betreffen ausschließlich eine Einzelinstallation auf einem Windows-PC. Bezüglich der Vorgehensweise zur Aktualisierung der Virendefinitionsdateien und Scan-Module mögen im Laufe der Zeit noch Änderungen erwogen werden.

Das Protokoll einer Musterinstallation habe ich auf einer Webseite im Winkiosk bereitgestellt. Beachten Sie insbesondere die Hinweise zum „AutoUpdate“, so etwa zum Importieren und Bearbeiten einer „AutoUpdate-Repository-Liste“. Bezüglich der Erneuerung des Scan-Moduls haben sich die Empfehlungen (zugunsten geringerer Datenübertragungskapazitäten) wesentlich geändert. Die bei uns gespiegelten Aktualisierungen pflegen wir mit den **McAfee AutoUpdate Architect**; zu diesen Vereinbarungen mögen sich im Zusammenhang mit ferngewarteten Systemen Änderungen ergeben. Eingerichtet ist diesbezüglich derzeit eine „Internet-Verbindung“ zu unserem Server WinKiosk.

Ferner sei darauf hingewiesen, dass die „VirusScan Command Line Scanner“ nun in einer Version 4.24 vorliegen. Für Macintosh-Systeme finde ich derzeit widersprüchliche Angaben zu Virex, wir halten im Winkiosk (außer Version 6.1) Virex7.0 sowie ein Hotfix nach Virex7.0Version1.0H1 und Virex Version 7.2.1 zum Kopieren bereit, können aber diesbezüglich keinerlei Beratung leisten.

SPSS für Windows Version 11.5

S. Zörkendörfer

Zum Statistik-Paket SPSS besteht für Windows-Arbeitsplatzrechner eine Mehrfachlizenz als Wartungsvertrag. Die Auslieferung einer neuen Version wird hiermit angekündigt.

Zunächst eine allgemeine Mitteilung zum SPSS: Lizenziert sind die SPSS-Produkte in einer Hochschullandeslizenz, vergleichbar mit einem Jahresabonnement. Das Lizenzjahr beginnt jeweils am 1. Dezember. Wir werden ab Ende Mai keine zusätzlichen Exemplare für das laufende Lizenzjahr weitergeben können. Die bei der Bestellung erhobenen Gebühren sind Gebühren für die Lizenz, nicht für Dokumentation oder Datenträger. Lizenznehmer können im laufenden Lizenzjahr auf eine andere Version umsteigen.

Nun zur Ankündigung der Auslieferung einer neuen Version: Auf der Windows-Plattform ist uns die Version 11.5 ausgeliefert worden, und zwar sowohl die deutschsprachige wie die englische Version. Die Installationsmaterialien sind jeweils auf einer CD zusammengestellt. Wir haben diese Dateien in Verzeichnisse eingespielt, zu dem die Informationsverarbeitungsversorgungseinheiten (IVVen) Lesezugriff haben bzw. beantragen können. Vereinbarungsgemäß können Berechtigte Kopien solcher Datenträger von ihrer IVV erstellen lassen. Zur Installation wird ein Installationscode benötigt, beim Umstieg von Version 11.0.1 nach Version 11.5 (in der jeweiligen Sprachvariante) sollte der bereits mitgeteilte Code weiterhin gelten (und bei Überinstallation gar nicht neu eingegeben werden müssen). Sprechen Sie mich an, wenn Sie Version 11.5 nutzen wollen und Schwierigkeiten bei der Beschaffung der Installationsmaterialien oder mit dem Lizenzcode haben.

Diese Ankündigung ist (noch) keine Empfehlung zum Umstieg, in den ZIV-Pools unseres Hauses werden wir im laufendem Semester weiterhin die deutsche Version 11.0.1 vorhalten. Zum SPSS-Ferienkurs im Herbst 2003 mag diese neue Version 11.5 bereitgestellt werden.

Um erste Eindrücke von den Neuerungen zu gewinnen, nenne ich folgende menüorientierte Aktionen (mit den Bezeichnungen der deutschen Version 11.5 auf einem deutschsprachigen WinXP):

- **Hilfe – Themen:** Neben den Syntax Reference Guides ist hier nun in großem Umfang Informationsmaterial in deutscher Sprache mitgeliefert.
- **Hilfe – Lernprogramm:** Gelang mir in meiner Installation mit einem Internet Explorer, aber nicht unter Netscape. Gleiches gilt für den Aufruf des Ergebnis-Assistenten aus einem Objekt des Ausgabefensters heraus.
- **Bearbeiten – Optionen – Allgemein – Sprache** zum Wechseln der/vieler Bezeichnungen der Ausgabe (auch innerhalb einer laufenden Sitzung)
- Neue Menüpunkte im Daten-Editor: **Daten – Variableneigenschaften definieren ...** und **Daten – Dateneigenschaften kopieren ...**
- **Analysieren – Tabellen – Benutzerdefinierte Tabellen ...** mit neuer Benutzeroberfläche zum Komponieren von Tabellen
- und schließlich **Analysieren – Klassifizieren – Two-Step-Clusteranalyse...**

ZIV-Lehre

Veranstaltungen in der vorlesungsfreien Zeit (August – Oktober 2003)

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12, G 83-31561	Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse http://www.uni-muenster.de/ZIV/Content-Lehre.html unter „Anmelden zu den Veranstaltungen“ erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind möglich ab 1. Juli 2003.	
260018	Betriebssystem Linux/Unix: Einführung und Grundlagen vom 04.08. bis 15.08.2003, Mo-Fr 10-16 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60	Grote, M.
260022	Sichere Kommunikation im Internet vom 22.09. bis 26.09.2003, Mo-Fr 10-17 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60	Perske, R.
260037	Programmieren in Fortran vom 15.09. bis 26.09.2003, Mo-Fr 9-11 Uhr Hörsaal: ZIV-Pool 2, Einsteinstr. 60	Reichel, K.
260041	Java-Server-am Beispiel von Windows 98 oder XPProgrammierung vom 15.09. bis 26.09.2003, Mo-Fr 9-11 Uhr Hörsaal: M4, Einsteinstr. 64	Süselbeck, B.
260056	Statistische Datenanalyse mit dem Programmsystem SPSS vom 04.08. bis 15.08.2003, Mo-Fr 9-11 Uhr, nachmittags n.V. Hörsaal: ZIV-Pool 2, Einsteinstr. 60	Zörkendörfer, S.
260060	Multimedia-Praktikum: Bildgewinnung und -präsentation vom 15.09. bis 19.09.2003, Mo-Fr 9-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13	Kisker, H.-W.
260075	Einführung in die Benutzung des Parallelrechners vom 06.10. bis 10.10.2003, Mo-Fr 9-11 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13	Leweling, M.
260080	Administration eines Windows-Systems vom 08.09. bis 12.09.2003, Mo-Fr 9-17 Uhr Hörsaal: M4, Einsteinstr. 64 und ZIV-Pool 3, Einsteinstr. 60	Kämmerer, M.
260094	Systemadministration für Linux-Systeme vom 06.10. bis 10.10.2003, Mo-Fr 9-16 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60	Hölters, J.

Veranstaltungen in der Vorlesungszeit (Wintersemester 2003/2004)

Beratung zum Lehrangebot durch Herrn W. Bosse
jeweils Di, Do 11-12,
G 83-31561

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse <http://www.uni-muenster.de/ZIV/Content-Lehre.html> unter „Anmelden zu den Veranstaltungen“ erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind möglich ab 1. September 2003.

260109	cms@uni – Werkzeuge für den Webauftritt Mittwoch 15-17 Uhr Hörsaal: M4, Einsteinstr. 64	Neukäter, B.
260113	Programmieren in C++ Mittwoch 13-15 Uhr Hörsaal: M4, Einsteinstr. 64	Mersch, R.
260128	Programmieren in Java Dienstag 13-15 Uhr Hörsaal: M4, Einsteinstr. 64	Pudlatz, H.
260132	Statistische Datenanalyse mit dem Programmsystem SPSS Mittwoch 11-13 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60	Nienhaus, R.
260147	Windows-Betriebssysteme: Einführung und Grundlagen Mittwoch 9-11 Uhr Hörsaal: M4, Einsteinstr. 64	Sturm, E.
260151	Windows-Systemadministration: Ausgewählte Themen Mittwoch 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13	Lange, W./ Winkelmann, O.
260166	Rechnernetze und Internet: Technische Grundlagen Donnerstag 10-12 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13	Richter, G./ Forsmann, A./ Kamp, M./ Speer, M./ Wessendorf, G.
260170	Kolloquium des Zentrums für Informationsverarbeitung Freitag 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13	Held, W.

Kommentare zu den Lehrveranstaltungen

260018 Betriebssystem Linux/Unix: Einführung und Grundlagen

Linux ist ein leistungsstarkes Unix-System für viele Hardware-Architekturen. Als preiswerte Windows-Alternative ist es augenblicklich in aller Munde. Die Vorlesung will in die Linux-Benutzung einführen. Sie besteht aus zwei Teilen. Zuerst erfolgt eine an üblichen Unix-Einführungen orientierte Beschreibung des Unix-Datei-Systems und der wesentlichen Unix-Befehle. Anschließend wird die grafische Oberfläche KDE behandelt, die für viele ein Linux-System erst attraktiv macht.

260022 Sichere Kommunikation im Internet

Das Internet ist eine mächtige und leistungsfähige Kommunikations-Infrastruktur, birgt aber auch erhebliche Gefahren, welche für einen unbedarften Nutzer nur schwer zu erkennen sind.

In der Veranstaltung wird gezeigt, welche Gefahren bestehen und wie man sich ohne große Mühe vor den meisten dieser Gefahren schützen kann. Praktisch geübt werden kurz das Absichern des eigenen Rechners am Beispiel von Windows 98 oder XP sowie ausführlich das Einrichten und die Benutzung entsprechender Software zur sicheren Kommunikation:

- Sichere E-Mail mit Pretty Good Privacy und mit Secure MIME
- Sichere Dialog- und Datenverbindungen mit Secure Shell
- Sichere Interaktion im WWW mit SSL/TLS (HTTPS)

Den Teilnehmerinnen und Teilnehmern wird dabei deutlich, dass Verschlüsselung, elektronische Unterschriften und Zertifikate viel einfacher zu benutzen sind als man sich gemeinhin vorstellt.

Vorausgesetzt werden Erfahrungen im Umgang mit den Internetanwendungen E-Mail, WWW, Telnet und FTP sowie Grundkenntnisse der Funktionsweise (wozu braucht man IP-Adressen? Portnummern? Nameserver? Router?).

260037 Programmieren in Fortran

Fortran ist eine weit verbreitete Programmiersprache, die insbesondere für die Programmierung naturwissenschaftlicher und technischer Anwendungen eingesetzt wird. In dieser Vorlesung sollen die Hörerinnen und Hörer lernen, wie Programme systematisch konstruiert werden. Gleichzeitig wird ihnen zunächst der Fortran-77-Standard, anschließend darauf aufbauend der Fortran-90-Standard vermittelt. Es werden keine Programmierkenntnisse vorausgesetzt. Praktische Übungen sind Teil der Veranstaltung.

BRAUER: *Programmieren in Fortran 77*, Müthig

MICHEL: *Fortran 90*, BI-Wiss.-Verlag

BRAINARD/GOLDBERG/ADAMS: *Fortran 90*, Oldenbourg

HEISTERKAMP: *Fortran 90*, BI Wiss.-Verlag University Press

260041 Java-Server-Programmierung

Die Erstellung Web-basierter Dienste und Anwendungen ist inzwischen eine der wichtigsten Aufgaben der Softwareentwicklung. Die Lehrveranstaltung bietet eine Einführung in Java-Techniken zur Entwicklung und Bereitstellung von Web-Services und Web-Applikationen. Themen sind u. a.: Netzwerkprogrammierung in Java, Servlets, Java und XML, Java Server Pages, Java und Datenbanken.

Kenntnisse in der Programmiersprache Java werden vorausgesetzt.

260056, 260132 Statistische Datenanalyse mit dem Programmsystem SPSS

Das statistische Programmsystem SPSS (Statistical Package for the Social Sciences) wird in dieser Veranstaltung in der neuesten deutschsprachigen Version unter Windows vorgestellt und erprobt. Mit diesem System stehen bequem aufzurufende Programme zu den gebräuchlichen univariaten und multivariaten statistischen Verfahren sowie zur Datenaufbereitung zur Verfügung. SPSS wird z. B. zur Auswertung von Fragebögen eingesetzt.

In dieser Veranstaltung wird das programmtechnische Rüstzeug zur Durchführung derartiger Auswertungen vermittelt. Solide Grundkenntnisse bezüglich der anzusprechenden statistischen Verfahren sowie Kenntnisse der Anwendungsmöglichkeiten dieser Verfahren im jeweiligen Fachgebiet sind erwünscht und bei den praktischen Übungen von großem Nutzen.

260060 Multimedia-Praktikum: Bildgewinnung und -präsentation

Das Praktikum führt in die elementaren Techniken der Bildgewinnung und deren Präsentation ein. Die Hörerinnen und Hörer sollen Erfahrung im Umgang mit Flachbett-Scannern, Dia-Scannern, digitalen Kameras, Videokameras und Webcams gewinnen. Gleichzeitig wird auch die Präsentation des gewonnenen Bildmaterials als Druckausgabe, Foto-CD, Video-CD und Live-Internet-Übertragung trainiert.

Das Praktikum besteht aus zwei Teilen. Der erste Teil ist als Web-Vorlesung organisiert. Hier wird zum einen in die theoretischen Grundlagen der verschiedenen Techniken eingeführt, und zum anderen werden die Experimente und Aufgaben aus Teil 2 beschrieben. Dieser Teil kann und soll von den Studierenden selbstständig als Vorbereitung auf Teil 2 durchgearbeitet werden. Er wird ab Anfang September im Web zur Verfügung stehen. Der zweite Teil stellt das eigentliche Praktikum dar. Dabei wird der in Teil 1 erarbeitete Stoff vorausgesetzt. Gruppen von bis zu drei Personen beschäftigen sich jeweils mit einem Experiment. Jeder Gruppe wird jeden Tag der Woche ein neues Experiment zugeteilt.

Im Einzelnen sind folgende Experimente vorgesehen:

1. Gewinnung von gerasterten Bildern (d. h. von Druckvorlagen); Gerät: Flachbett-scanner; Präsentation: Druck
2. Gewinnung von Bildern mit kontinuierlicher Farbverteilung (d. h. Fotos); Gerät: Dia-Scanner; Präsentation: Druck
3. Bildgewinnung mit einer digitalen Kamera; Gerät: Digitale Kamera; Präsentation: Still-Video-CD
4. Bildgewinnung mit Video-Kamera (d. h. Filmerstellung); Gerät: Video-Kamera; Präsentation: Video-CD
5. Bildgewinnung und Präsentation in Echtzeit (d. h. Video-Konferenz); Gerät: Webcam; Präsentation: Bildschirm

Die Experimente werden jeweils morgens unter Aufsicht in den für das Praktikum reservierten Räumen durchgeführt. Auch an den Nachmittagen stehen alle Geräte für selbständige Auswertungen und Nacharbeiten zur Verfügung. Insbesondere an den Tagen vor den Experimenten 3 und 4 sind auch die Nachmittage mit Arbeit belegt. Den entsprechenden Gruppen werden digitale Kameras bzw. Video-Kameras ausgeliehen. Sie müssen dann selbständig die für den folgenden Tag benötigten Bilder bzw. Videos erstellen.

260075 Einführung in die Benutzung des Parallelrechners

Das Zentrum für Informationsverarbeitung bietet seit Beginn des Sommersemesters 2003 zentrale Rechenkapazität auf dem Linux-Cluster ZIVCLUSTER. Dieser Cluster eignet sich insbesondere für die Ausführung parallelisierter Programme. In dieser Veranstaltung werden die Grundlagen zur Benutzung dieses Parallelrechners vermittelt. Das *Portable Batch System* sowie die zur Verfügung stehenden Compiler und Programmbibliotheken (z. B. MPI, MKL) werden vorgestellt. Im weiteren Verlauf wird anhand von Beispielen die parallele Programmierung in Fortran erläutert.

Die Hörer sollten grundlegende Kenntnisse der Programmiersprache Fortran besitzen.

260080 Administration eines Windows-Systems

Für Hörer mit Windows-Vorkenntnissen werden Arbeiten zum Aufbau und Betrieb eines Windows-Servers vorgestellt und gemeinsam erprobt.

Die folgenden Themen werden u. a. behandelt:

- Installation und Konfiguration des Servers,
- Benutzer- und Gruppenverwaltung, lokale Administration,
- Druck-, Datei-, Logon- und allgemeine Programm-Services,
- Zugriffsrechte und Netz-Freigaben,
- Diagnose- und Überwachungsfunktionen,
- Internet, LAN, Netz-Protokolle,
- Absicherung des Servers gegen Angriffe von außen.

Die speziellen Dienste E-Mail-, Datenbank-, Web- und Media-Server können im Rahmen dieser Veranstaltung nicht bearbeitet werden. Die Einbindung des Servers in eine Windows-Active-Directory-Domäne wird nur am Rande erwähnt werden. Wir verweisen auf die Semester-Veranstaltung Windows-Systemadministration (260151).

260094 Systemadministration für Linux-Systeme

Die Vorlesung richtet sich an fortgeschrittene Linux-Anwender, die Unterstützung bei der Installation und System-Integration von Linux-Systemen benötigen. Voraussetzung sind grundlegende Kenntnisse der Unix-Kommandos und der Shell-Script-Sprache. Die Teilnehmer werden in der Veranstaltung ein Linux-System selbst installieren und in die Netzwerk- und Systeminfrastruktur der Universität einbinden. Ferner wird demonstriert, wie man einen speziell auf die Hardware-Ausstattung des Rechners optimierten Kernel generiert.

260109 cms@uni – Werkzeuge für den Webauftritt

Das Internet wird neben den traditionellen Medien in immer stärkerem Umfang zur Öffentlichkeitsarbeit genutzt. Zur Realisierung der Dokumente im Web dient die Hypertext Markup Language (HTML). Um den Publizierenden auch ohne Kenntnisse der HTML den Zugang zum Web zu ermöglichen, werden Content-Management-Systeme (CMS) eingesetzt.

Die Teilnehmer dieser Veranstaltung sollen die Methoden der Inhaltsverwaltung im Web und den Aufbau eines CMS kennen lernen. Für sie wird ein Zugang zu dem an der Universität verwendeten System Imperia eingerichtet, an dem die erworbenen Kenntnisse in die Praxis umgesetzt werden können.

Kenntnisse im Umgang mit dem PC und dem World Wide Web (WWW) werden vorausgesetzt.

260113 Programmieren in C++

C++ erweitert die Programmiersprache C mit ihren durch Assembler-ähnliche Sprach-elemente einerseits und Elemente moderner blockstrukturierter Sprachen andererseits sehr vielseitigen Einsatzmöglichkeiten um objektorientierte Konzepte. Diese Verbindung einer sehr erfolgreichen Programmiersprache mit einem seit einigen Jahren boomenden Programmier-Paradigma macht C++ zu einer der am meisten benutzten Programmiersprachen. In der Lehrveranstaltung wird C++ gemäß dem 1998 erschienenen ISO/ANSI-Standard von Grund auf vorgestellt. Kenntnisse einer anderen Programmiersprache wären hilfreich, werden aber nicht vorausgesetzt.

STROUSTRUP: *Die C++ Programmiersprache, dritte Auflage*, Addison-Wesley

260128 Programmieren in Java

Java ist eine objektorientierte Programmiersprache, die inzwischen weltweit große Verbreitung gefunden hat und sich weiterhin dynamisch entwickelt. Sie basiert auf dem Konzept einer virtuellen Maschine, die es ermöglicht, Anwendungen für unterschiedliche Plattformen ohne Neuübersetzung zu entwickeln, und verfügt über eine sehr umfangreiche Klassenbibliothek, die ständig erweitert wird. Grundkenntnisse in Java sind für die Softwareentwicklung in vielen Bereichen unbedingt erforderlich. Die Vorlesung bietet eine Einführung in die objektorientierte Programmierung anhand von Java. Sie ist auch für Hörer ohne Vorkenntnisse im Programmieren geeignet.

260147 Windows-Betriebssysteme: Einführung und Grundlagen

In dieser Veranstaltung wird sowohl der Einsatz von Windows XP als auch die Betriebssystemarchitektur vorgestellt. Dabei soll u. a. auf Installation, Konfiguration, Bedienoberfläche und Kommunikation in Internet und lokalem Netz eingegangen werden. Hinzu kommen Sicherheitsmaßnahmen und die Benutzung frei verfügbarer Programme wie GhostScript und PGP.

Die Hörer sollten praktische Erfahrung mit PCs besitzen.

260151 Windows-Systemadministration: Ausgewählte Themen

Die Veranstaltung richtet sich an fortgeschrittene Windows-Benutzer, die ihre Kenntnisse mit Blick auf die Anforderungen in einem großen Rechnernetz erweitern möchten. Als Schwerpunkte sind u. a. das „Client-Management“ (Installation und Konfiguration von Win2000/XP-Workstations) sowie Aufbau und Betrieb von Servern im Netzwerk (Windows 2000/2003) vorgesehen.

Themenauswahl:

- Installation und Konfiguration;
- Benutzerverwaltung: lokal/im Netz (ADS);
- Sicherheit u. a.: Dateisystem, Registry, Netzwerk, Sicherheitsrichtlinien;
- Server im Active Directory: Gesamtstrukturen, Domänenstrukturen, Domänen, Organisationseinheiten (OU), Vertrauensstellungen, Standorte, Replikation, Gruppenrichtlinien;
- Softwareverteilung und Systemüberwachung.

260166 Rechnernetze und Internet: Technische Grundlagen

Diese Veranstaltung gibt einen Einblick in die technischen Grundlagen der Rechnernetze unter besonderer Berücksichtigung des Internets.

Folgende Themen werden behandelt:

- Architekturmodell für Rechnernetze (OSI-Modell), Kommunikationsprotokolle,
- Techniken für lokale Rechnernetze (LANs): Ethernet, Fast Ethernet, Gigabit Ethernet,
- Kopplung/Strukturierung von Rechnernetzen: Routing, Bridging und Switching,
- Grundlegende Internet-Protokolle: IP, TCP, UDP, ICMP, ARP, DNS, DHCP, WINS,
- TCP/IP-Software: Konfiguration und Diagnose,
- spezielle TCP/IP-Funktionen unter Windows,
- Funk-LANs,
- Struktur und Funktionen des Rechnernetzes der Universität Münster.

260170 Kolloquium des Zentrums für Informationsverarbeitung

Im Rahmen des Kolloquiums werden Vorträge über aktuelle Themen der Informationsverarbeitung gehalten. Vortragstermine werden im WWW und durch Aushang bekanntgegeben.

ZIV-Regularia

Fingerprints

R. Perske

Unter dieser Rubrik erscheinen regelmäßig die aktuellen kryptographischen Prüfsummen der öffentlichen Schlüssel, die von der WWUCA und vom ZIV verwendet werden.

Anhand dieser Zusammenstellung können Sie die Echtheit aller Schlüssel der Zertifizierungsstellen der Universität Münster und des DFN überprüfen, vgl. <http://www.uni-muenster.de/WWUCA/>, <http://www.dfn-pca.de> und die Übersichtsartikel in früheren i -Ausgaben.

PGP-Schlüsseldaten der WWUCA

WWUCA-Zertifizierungsschlüssel für 2002-2003:
Zertifizierungsstelle Universitaet Muenster 2002-2003
KeyID: BC811EB1, Schlüssellänge 2048 Bits, Erstellungsdatum: 2001/11/14
Key fingerprint = 28 64 01 BC F0 EF D5 BA D9 A0 86 6C 43 79 4C 1D

WWUCA-Zertifizierungsschlüssel für 2000-2001:
Zertifizierungsstelle Universitaet Muenster 2000-2001
KeyID: 313C02F5, Schlüssellänge 2048 Bits, Erstellungsdatum: 2000/03/24
Key fingerprint = 37 62 F5 E0 C2 78 76 97 53 0F 2D F2 F3 B3 27 F5

Alter Zertifizierungsschlüssel (nur durch DFN-User-CA zertifiziert):
Rainer Perske +49(251)83-31582 Certification Key
KeyID: EF750F1D, Schlüssellänge 2048 Bits, Erstellungsdatum: 1997/10/14
Key fingerprint = 2F 38 6E F8 DC 2E D8 5E 5B 35 DB 49 8A E4 52 AF

PGP-Kommunikationsschlüssel für verschlüsselte E-Mails an die WWUCA:

Zertifizierungsstelle Universitaet Muenster (E-Mail) <ca@uni-muenster.de>
KeyID: 4CB7658D, Schlüssellänge 2048 Bits, Erstellungsdatum: 2000/07/06
Key fingerprint = 38 3D 0F 16 CE FC 1F 9E B7 C3 04 B1 20 20 FC E6

PGP-Schlüsseldaten der DFN-PCA

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

DFN-PCA-Wurzelschlüssel für 2001:
DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2001) <not-for-mail>
KeyID: 63EB5391, Schlüssellänge 2048 Bits, Erstellungsdatum: 2000/12/28
Key fingerprint = CF AF 6C 29 4E 57 4E 0E E8 1C BD B4 54 FD 2A AB

DFN-PCA-Wurzelschlüssel für 1999-2000:
DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1999-2000) <not-for-mail>
KeyID: F7E87B9D, Schlüssellänge 2048 Bits, Erstellungsdatum: 1998/12/29
Key fingerprint = 65 70 72 74 B5 E0 3F F0 EA 7C AB E4 46 5F B8 B2

DFN-PCA-Wurzelschlüssel für 1997-1998:
DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1997-1998) <not-for-mail>
KeyID: 35DBF565, Schlüssellänge 2048 Bits, Erstellungsdatum: 1997/04/16
Key fingerprint = 09 7C 09 19 D3 C3 86 DC 7A 30 15 11 12 95 8D E3

PGP-Kommunikationsschlüssel für verschlüsselte E-Mails an die DFN-PCA:

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

Alle Angaben zur DFN-PCA ohne Gewähr.

X.509-Zertifikatdaten der WWUCA

WWUCA-Zertifikat für 2002-2003 plus 2 Jahre:

Serial Number: 1774668 (0x1b144c)
 Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH,
 OU=DFN-PCA,
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
 Validity
 Not Before: Jan 1 00:00:00 2002 GMT
 Not After : Dec 31 23:59:59 2005 GMT
 Subject: C=DE, O=Universitaet Muenster,
 CN=Zertifizierungsstelle 2002-2003/Email=ca@uni-muenster.de
 Fingerprints:
 MD5: a4:31:ad:41:d8:f2:18:56:4e:31:cc:69:71:e6:17:4f
 SHA1: 69:45:20:ca:1a:fe:5c:fa:6c:37:52:eb:b7:72:b0:54:90:ec:d9:79

WWUCA-Zertifikat für 2000-2001:

Serial Number: 16 (0x10)
 Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA,
 CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
 Validity
 Not Before: Jun 5 15:35:24 2000 GMT
 Not After : Jun 5 15:35:24 2002 GMT
 Subject: C=DE, O=Universitaet Muenster,
 CN=Zertifizierungsstelle 2000-2001/Email=ca@uni-muenster.de
 Fingerprints:
 MD5: da:e3:e2:5d:bc:93:ef:03:37:96:4e:25:c1:ab:2b:d1
 SHA1: a7:64:55:75:e0:ad:9a:2c:0c:b4:c8:ed:be:e0:bf:d4:72:6c:5c:b2

X.509-Zertifikatdaten der DFN-PCA

DFN-PCA-Wurzelzertifikat für 2002-2005 plus 4 Jahre:

Serial Number: 1429501 (0x15cffd)
 Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH,
 OU=DFN-PCA,
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
 Validity
 Not Before: Dec 1 12:11:16 2001 GMT
 Not After : Jan 31 12:11:16 2010 GMT
 Subject: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH,
 OU=DFN-PCA,
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
 Fingerprints:
 MD5: 3e:1f:9e:e6:4c:6e:f0:22:08:25:da:91:23:08:05:03
 SHA1: 8e:24:22:c6:7e:6c:86:c8:90:dd:f6:9d:f5:a1:dd:11:c4:c5:ea:81

DFN-PCA-Wurzelzertifikat für 1998-2001:

Serial Number: 1 (0x1)
 Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA,
 CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
 Validity
 Not Before: Oct 29 18:03:10 1998 GMT
 Not After : Dec 31 18:03:10 2001 GMT
 Subject: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA,
 CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
 Fingerprints:
 MD5: 45:bb:9b:c8:8a:a4:84:8b:2d:a0:08:8f:9e:b6:b8:10
 SHA1: df:a5:6f:b5:fc:41:e3:a8:92:1f:77:ad:16:22:ee:fd:91:52:a5:ad

Alle Angaben zur DFN-PCA ohne Gewähr.

Liebe Leserin, lieber Leser,

wenn Sie i regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von i nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.

Bitte haben Sie Verständnis dafür, dass ein Versand außerhalb der Universität nur in begründeten Einzelfällen erfolgen kann.

Vielen Dank!

Redaktion i



-
- ~ Ich bitte um Aufnahme in den Verteiler.
 - ~ Bitte streichen Sie mich/den nachfolgenden Bezieher aus dem Verteiler.
 - ~ Mir reicht ein Hinweis per E-Mail nach dem Erscheinen einer neuen WWW-Ausgabe.
Meine E-Mail-Adresse:

-
- ~ Meine Anschrift hat sich geändert.
Alte Anschrift:

An die
Redaktion i
Zentrum für Informationsverarbeitung
Röntgenstr. 9-13
48149 Münster

Absender:

Name: _____

FB: _____ Institut: _____

Straße: _____

Außerhalb der Universität:

(Bitte deutlich lesbar in Druckschrift ausfüllen!)

Ich bin damit einverstanden, dass diese Angaben in der i

-Leserdatei gespeichert werden (§ 4 DSGVO).

Ort, Datum

Unterschrift