

# inforum

---

Zentrum für Informationsverarbeitung der Universität Münster  
Jahrgang 23, Nr. 3                      Dezember 1999                      ISSN 0931-4008

---

## Inhalt

Editorial .....	2
RUM-Aktuell .....	3
Guter Rat ist nicht teuer .....	3
Videokonferenzen im Internet .....	4
Terminal-Server .....	5
Weitere Sicherungsmaßnahmen für die Informationsverarbeitung .....	6
Neue Rechner zum Rechnen .....	7
Zugang für Studierende zu den Rechnern der Fachbereiche .....	7
Übergroße E-Mails .....	9
Referenzzentrum für das neue Internet .....	10
Neues über Software .....	12
CITYKOM-Zugang zum Rechnernetz der WWU .....	14
MeDiDa-Prix 2000 .....	14
Betriebsreports des Universitätsrechnernetzes .....	15
X11-Server-Emulation mit Exceed im Universitätsrechnernetz .....	15
DFN-Verein vervierfacht Netzrate in die USA .....	16
Neue TUSTEP-Version 2000 .....	16
Fingerabdrücke .....	17
Änderungen beim plot-Kommando .....	19
RUM-Tutorial .....	21
Einsatz von Smart-Karten in Betrieben, Hochschulen und Ämtern (1) .....	21
RUM-Lehre .....	28
Lehrveranstaltungen im 1. Halbjahr 2000 .....	28



## Impressum

**informum**

ISSN 0931-4008

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

E-Mail: [ziv@uni-muenster.de](mailto:ziv@uni-muenster.de)  
WWW: <http://www.uni-muenster.de/ZIV/>

Redaktion: W. Bosse (☎ 83-31561, ✉ [bosse@uni-muenster.de](mailto:bosse@uni-muenster.de))  
R. Perske (☎ 83-31582, ✉ [perske@uni-muenster.de](mailto:perske@uni-muenster.de))  
H. Pudlatz (☎ 83-31672, ✉ [pudlatz@uni-muenster.de](mailto:pudlatz@uni-muenster.de))  
E. Sturm (☎ 83-31679, ✉ [sturm@uni-muenster.de](mailto:sturm@uni-muenster.de))

Satzsystem: Corel WordPerfect 8.0 für Windows 95/NT

Druck: Zentrum für Informationsverarbeitung  
(Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1500

## Editorial

*E. Sturm*



Haben Sie auch schon Vorräte gesammelt und die Badewanne gefüllt? Wer weiß, ob die Strom- und Wasserversorgung beim Jahrtausendwechsel nicht automatisch abgeschaltet wird? Benutzen Sie also nicht die Tiefkühltruhe für die Vorräte! Auch etwas Bargeld könnte nicht schaden. Sollten die Bargeldautomaten im Jahr 2000 etwa auf Euro umschalten, weil die Programmierer da etwas verwechselt haben, so bekommen Sie immer nur die Hälfte ausgezahlt.

Keine außergewöhnlichen Probleme werden Windows-Benutzer haben: Ob der Rechner nun einmal mehr oder weniger abstürzt, fällt nicht ins Gewicht. Der Windows-Benutzer ist abgehärtet. Eine falsche Sortierreihenfolge in irgendwelchen Tabellen ist ja auch nicht weiter schlimm. Schwerer wiegt da schon, dass die deutschen Atomkraftwerke nicht mit Windows gesteuert werden, die armen Ingenieure wissen bei einem Absturz womöglich nicht, wo der Knopf für „Booten“ ist.

Diese Ausgabe des **informum** hat sich unter anderem aus dem Grunde etwas verspätet, dass auch für den Rechenbetrieb an der Universität noch abschließende Regelungen zum Jahrtausendwechsel getroffen werden mussten. Lesen Sie bitte hierzu den Artikel „Guter Rat ist nicht teuer“.

Ansonsten möchte ich keinen weiteren Artikel herausgreifen, auffallend ist allerdings, dass in diesem **informum** 50 Mal das Wort „Server“ vorkommt. (Hat unsere Textverarbeitung herausgefunden!)

## RUM-Aktuell

### Guter Rat ist nicht teuer

H. Pudlatz

**Das ZIV hilft, wo es kann: ZIVline und NOC helfen bei Problemen im Umgang mit den IV-Ressourcen. Beim Jahr-2000-Problem müssen Sie allerdings selbst aktiv werden.**

So mancher fiebert in diesen Tagen dem bevorstehenden Jahrtausendwechsel entgegen, manch einer naiv-euphorisch, ein anderer besorgt um die Funktionsfähigkeit der computergesteuerten Technik auch im neuen Jahr. Was das **Jahr-2000-Problem** betrifft, haben wir frühzeitig Hinweise zur Vermeidung von Schwierigkeiten gegeben. Wir erinnern an einen Beitrag im **inforum** Nr. 1/1999 und an unsere Web-Seite

<http://www.uni-muenster.de/ZIV/Hinweise/Y2K.html>

Das dort als erste Instanz genannte Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt außer Hinweisen über die Jahr-2000-Festigkeit einzelner Programme auch aktuelle Last-Minute-Tips und versichert, dass nach sorgfältiger Erledigung der Prüf- und Umstellungsarbeiten, wie sie z. B. von den Banken und den großen Versorgungsunternehmen mit großem personellen und finanziellen Aufwand geleistet wurden, mit keinen größeren Störungen zu rechnen sei.

Falls beim Einzelnen noch nicht geschehen, empfehlen wir die von uns gegebenen Hinweise auf die Funktionstests für Hard- und Software durchzuführen. Jeder ist für die Überprüfung seiner persönlichen Arbeitsumgebung selbst verantwortlich! Hilfestellung bei der Überprüfung jedes der über 5000 PCs und der mehreren 100 Workstations im Universitätsbereich kann von uns personell leider nicht geleistet werden.

Wie schon im genannten **inforum**-Artikel betont, ist es ebenso falsch, die Augen vor dem Problem zu verschließen – nach dem Motto „Es wird schon schiefgehen“ – wie in Torchlusspanik bei einem freundlichen „Helfer“ viel Geld für die Lösung des Jahr-2000-Problems auszugeben. Wir warnen noch einmal davor: schlechter Rat kann teuer werden! Sehen Sie sich – falls noch nicht geschehen – lieber die Grundfunktionen Ihres Rechners an und vergewissern Sie sich, dass die wenigen täglich benötigten Programme den Jahrtausendwechsel überstehen!

Wir weisen darauf hin, dass unsere seit November 1998 im Testbetrieb laufende **Zentrale Servicestelle** („ZIVline“) zur festen Einrichtung geworden ist, die montags bis freitags von 7:30 bis 17:30 Uhr unter der Rufnummer (0251) 83-3 16 00 erreichbar ist, um allen Universitätsangehörigen bei IV-Problemen Hilfestellung zu geben. Außerhalb der angegebenen Zeiten ist ein Anrufbeantworter auf diese Nummer geschaltet, der auch Anfragen entgegennimmt. Diese werden zu den üblichen Dienstzeiten der ZIVline beantwortet. Darüber hinaus ist die Servicestelle auch über die Fax-Nr. (0251) 83-3 15 55 und über die zentrale E-Mail-Adresse des ZIV unter [ziv@uni-muenster.de](mailto:ziv@uni-muenster.de) erreichbar.

Bei Störungen im Universitäts-LAN hilft das **Netz-Operating-Center (NOC)** unter der Rufnummer (0251) 83-3 15 99 ebenfalls montags bis freitags von 7:30 bis 17:30 Uhr. Dies betrifft sowohl Probleme im LAN der Universität als auch bei serverseitigen Problemen der Einwählzugänge für häusliche Arbeitsplätze. In extrem dringenden Fällen und nach Ausschöpfung aller Maßnahmen zur Selbsthilfe kann ein Rufbereitschaftsdienst des NOC **außerhalb** der genannten Zeiten (also insbesondere des Nachts und an Wochenenden) über die Rufnummer (0251) 83-4 59 07 der Leitwarte der Universität erreicht werden.

Bei unvorhergesehenen Problemen, die im Universitäts-LAN und auf den vom Zentrum für Informationsverarbeitung betreuten Servern im Zusammenhang mit dem erwähnten Jahr-2000-Problem zum **Jahreswechsel** auftreten können, werden wir in angemessenem Umfang und frühzeitig reagieren. Sie können davon ausgehen, dass wir versuchen werden, aufgetretene Störungen noch im Laufe des Neujahrstages zu beheben.

## Videokonferenzen im Internet

W. Held / G. Richter

**Noch reicht die Netzgeschwindigkeit nicht ganz, um das Gefühl einer echten Kommunikation mit den Konferenzteilnehmern auf dem Bildschirm zu vermitteln, aber komfortabler als eine lange Reisen zum Konferenzort ist eine Videokonferenz allemal.**

Die Leiter der Hochschulrechenzentren in NRW sowie einzelne Arbeitsgruppen der Hochschulrechenzentren nutzen seit längerer Zeit regelmäßig ihre lokalen Rechnernetze (LANs) und das Wissenschaftsnetz (BWiN) für Videokonferenzen. Man kann zwar noch nicht von einem umfassenden Regeldienst sprechen, der hier genutzt wird, die Qualität hat sich aber doch so weit verbessert, dass die Konferenzen sogar in der Regel mit bis zu 12 Teilnehmern über 1–2 Stunden stattfinden. 12 Kamerabilder der Teilnehmer sind auf dem Bildschirm natürlich nur in Miniaturform unterzubringen, aber wenn man sich kennt, genügt in vielen Fällen auch allein die sprachliche Kommunikation, so dass man von einer Telefonkonferenz sprechen kann.

Derartige Konferenzen werden, wenn die grundsätzlichen Maßnahmen einmal durchgeführt worden sind, in wenigen Minuten ohne die Mitwirkung Dritter initiiert. Sie sparen Zeit und Reisekosten.

An die Rechnerausstattung werden nicht sehr hohe Anforderungen gestellt. Man benötigt Standard- oder Public-Domain-Software, Kopfhörer und Mikrofon (Headset) sowie eine Soundkarte und – wenn man auch gesehen werden will – eine einfache Kamera und eine geeignete Videokarte zur Digitalisierung (entsprechende Komplett-Sets sind bereits für wenige hundert D-Mark erhältlich!).

Als technische Basis dient sogenanntes IP-Multicast-Routing, d. h. eine Weiterleitungstechnik (Routing) in Internet-basierenden Rechnernetzen (IP – Internet-Protokoll), die gleichzeitig alle Informationen an eine Gruppe von Rechnern aussendet (Multicast). Entsprechend müssen die Rechnernetz-Infrastrukturen mit besonderen Routing-Funktionen ausgerüstet sein, um ein effizientes und leistungsfähiges IP-Multicasting zu erlauben.

Als *Mbone* (so viel wie *Multicast-Backbone*) wird der globale Verbund von IP-Netzen bezeichnet, die diese Fähigkeiten unterstützen. Das Deutsche Breitband-Wissenschaftsnetz BWiN unterstützt diese Funktionalität seit längerem auf mehr oder weniger experimenteller Basis, jedoch soll *Mbone* im Zusammenhang mit dem ab März 2000 entstehenden Gigabit-Wissenschaftsnetz (GWiN) als Regeldienst aufgebaut werden.

Auch in den beteiligten lokalen Rechnernetzen (LANs) müssen IP-Multicasting-Funktionen geeignet unterstützt werden. In LANs mit älterer Ausrüstung ist dies oft nur sehr beschränkt der Fall und IP-Multicasting kann dann nur mit Hilfskonstruktionen angeboten werden, wobei unter Umständen die Betriebssicherheit durch zu hohe Netzlasten gefährdet werden kann.

Das LAN der WWU ist in Teilbereichen wegen des Alters der Ausrüstung (zum Teil älter als 7 Jahre) auch nur sehr beschränkt *Mbone*-fähig, jedoch zeigen unsere schon seit längerem laufenden Testnutzungen, dass ein begrenzter IP-Multicasting-Betrieb durchaus machbar ist. In einer Anfangsphase werden wir deshalb Ende Februar oder Anfang März 2000 die *Mbone*-Möglichkeiten der Kommunikation für einige interessierte Wissenschaftler/innen einrichten, die bereit sind, in einem begrenzten Umfang auch in Tests einzutreten.

Dazu wird das ZIV zur weiteren Vorbereitung Ende Februar eine entsprechende Einführungsveranstaltung anbieten.

## Terminal-Server

M. Kamp / W. Lange

**Durch Einführung einer im PC-Bereich neuen, aber eigentlich sehr alten Organisationsform kann die Unzulänglichkeit des eigenen PCs durch Zugriff auf die Fähigkeiten eines starken Rechners gemildert werden.**

Im ZIV sind einige Terminal-Server in Betrieb, die von den Mitgliedern der WWU genutzt werden können. Diese Server können über das LAN oder (per Telefoneinwahl) auch von zu Hause aus erreicht werden. Die Programme des Nutzens werden dabei auf dem Terminal-Server ausgeführt. Der eigene Rechner dient nur noch als grafisches Terminal<sup>1</sup>, das auf ein Windows-NT-System zugreift. Allerdings kann man jederzeit zwischen selbstständigem PC-Betrieb und Terminal-Server-Betrieb umschalten. Auf diese Weise kann man z. B. Software-Produkte nutzen, die auf dem eigenen Rechner nicht zur Verfügung stehen. Die eigene PC-Hardware muss nicht auf dem neuesten Stand sein, trotzdem stehen neueste Funktionen zur Verfügung. Ein Teil der vielfachen Pflegearbeiten für die einzelnen PCs wird auf die Pflege weniger Server reduziert.

Mindestvoraussetzungen am Arbeitsplatz sind:

Ein PC mit 486-Prozessor (oder besser) und ein Microsoft-Windows-Betriebssystem mit TCP/IP als Netzwerkprotokoll. Zusätzlich sollten die Microsoft-Netzwerkdienste (Arbeitsstations- und Serverdienst) installiert sein. Das entspricht der Standardkonfiguration, wie sie auch sonst für den Betrieb der Rechner im Netz der WWU erforderlich ist.

Für andere Rechner, z. B. Unix-Workstations oder Apple-Rechner, gibt es Möglichkeiten, diese ebenfalls als Zugangsgerät zum Terminal-Server zu nutzen. Diese Varianten sind aber im ZIV nur für Linux in ersten Ansätzen erprobt.

Grundsätzlich ist die Nutzung der Terminal-Server unproblematisch, wenn auf den Zugriff auf lokale Ressourcen (Verzeichnisse und am eigenen PC angeschlossene Drucker) verzichtet werden kann – was aber häufig nicht möglich oder nicht zumutbar ist. Der Zugang zu den lokalen Ressourcen ist mit einigen Einschränkungen möglich, gestaltet sich aber je nach Windows-Version und -Konfiguration unterschiedlich schwierig. Insbesondere die Nutzung eigener Drucker an Win9x- und Win3.x-PCs hat sich als ausgesprochen problematisch erwiesen. Der angekündigte Win2000-Terminal-Server lässt in dieser Hinsicht einige Verbesserungen erwarten.

Die Registrierung zur Nutzung der Terminal-Server des ZIV muss derzeit noch von einem Mitarbeiter der PC-Gruppe im ZIV vorgenommen werden. Vorgesehen ist ein WWW-Formular zur Selbstanmeldung, das aber noch erstellt werden muss.

Die Arbeit auf dem Terminal-Server bietet sich an, wenn man übliche Büro- und Internet-Anwendungen nutzen will, für die die Software auf dem Terminal-Server eingerichtet ist. Nicht sinnvoll ist die Nutzung der Terminal-Server bei rechenintensiven oder grafischen Arbeiten. Nicht möglich sind Anwendungen, die die Multimediaausstattung am eigenen PC nutzen (Video und Audio). In diesen Fällen muss man auf den lokalen PC-Betrieb umschalten.

Weitere Einzelheiten zur Nutzung der Terminal-Server werden auf den Web-Seiten des ZIV bekanntgegeben werden.

---

<sup>1</sup> Terminal = Gerät lediglich zur *Ein- und Ausgabe* von Informationen über Tastatur, Bildschirm und Maus, nicht aber zur Informationsverarbeitung selbst. Der Begriff *Terminal* war früher im Zusammenhang mit Großrechnern sehr geläufig.

## Weitere Sicherungsmaßnahmen für die Informationsverarbeitung

W. Held / G. Richter

**Was wir für die sichere Datenübertragung und die Absicherung von Rechnern gegen unberechtigte Benutzung tun ...**

Leider gibt es kein umfassendes Konzept zur Sicherung der Informationsverarbeitung. Man kann nur schrittweise vorgehen. Drei dieser Schritte werden hier angesprochen:

### 1. E-Mail-Server

Zur Erhöhung der Sicherheit der Informationsverarbeitung hatte die IV-Kommission der WWU den Betrieb von E-Mail-Servern eingeschränkt. Vom 10. Januar 2000 an können nur noch die Server ihre E-Mail-Dienste anbieten, die den IVV-Leitern bekannt gegeben und vom ZIV freigeschaltet worden sind. Wir verweisen auf einen entsprechenden Artikel im *infoRUM* Nr. 2/1999 und die WWW-Seite

<http://www.uni-muenster.de/ZIV/Content--Regelungen.html>

### 2. Technisch Verantwortliche der Institute für die Rechner im LAN

Immer wieder haben wir es mit Missbrauchsversuchen (Hacker, ...) im LAN der WWU zu tun. In letzter Zeit wurden z. B. Rechner aus drei Bereichen zweckentfremdet, um in anderen Standorten Einbruchsmöglichkeiten auszuspähen oder Störungen zu verursachen. Zur schnellen Abwendung derartiger „Störungen“ sind wir vielfach auf die schnelle Mitwirkung der für die Rechner technisch Verantwortlichen angewiesen. Diese Verantwortung muss ernsthaft wahrgenommen werden. Die Mitarbeiterinnen und Mitarbeiter müssen sich z. B. über CERT-Listen einen aktuellen Informationsstand besorgen, um „Löcher in ihren Systemen“ schnell zu stopfen. Bitte betrachten Sie deshalb bei der Anmeldung der Rechner für das Rechnernetz der WWU die Angabe „Technisch Verantwortlicher“ nicht einfach als formalen Akt.

Vielmehr sollte jede Einrichtung sich darum bemühen, dass die technische Betreuung der Rechner möglichst effizient erfolgt und dass dabei auch ein möglichst hoher Grad an IV-Sicherheit erzeugt wird. Eine Einsetzung von studentischen Hilfskräften für einzelne Rechner mag zwar im Einzelfall eine vorübergehend sogar durchaus qualitativ befriedigende Situation ergeben, aber eine dauerhaft angemessene Betreuung auch unter Sicherheitsaspekten in der Breite ist davon i. Allg. nicht zu erwarten. Allein daraus ist zu folgern, dass diese Aufgaben mehr und mehr in die Verantwortung der IVVen verlagert werden müssen, wo die Informationen zur IV-Sicherheit vorliegen und auch gesichert umgesetzt werden können.

### 3. Absicherung von Rechnern

Rechner können durch bestimmte Maßnahmen so abgesichert werden, dass unbefugte Zugänge durch Dritte (z. B. über an sich nicht benötigte Anwendungen oder Kommunikationsprotokolle) unterbunden werden. Hier gibt es Möglichkeiten, dies im Rechner selbst zu tun. Im Frühjahr 2000 werden wir darüber ausführlicher informieren. Die Systemabteilungen im ZIV können in Einzelfällen auch heute schon Hinweise an die IVVen geben, welche rechnerseitigen Maßnahmen genutzt werden sollten, die IV-Sicherheit zu verbessern. Auch netzseitig sind Maßnahmen möglich. Jedoch gibt es für das Rechnernetz der WWU bisher kein generelles Angebot für sogenannte „Firewall“-Funktionen, da dies erhebliche organisatorische und technische Voraussetzungen bedingt. Dennoch kann die Sicherheit durch netzseitige Maßnahmen für besonders gefährdete Systeme zum Teil auch heute schon mit einfachen Mitteln erheblich verbessert werden, wenn bestimmte Voraussetzung erfüllt sind. Interessierte sollten sich über ihre IVV an das ZIV wenden.

## Neue Rechner zum Rechnen

St. Ost

**Nach langer Zeit tut sich im Zentrum für Informationsverarbeitung wieder etwas für das numerisch intensive Rechnen.**

Im Rahmen des zweiten Teils einer HFBG-Beschaffung (vgl. [info<sup>rum</sup>](#) Nr. 1/1999) wird die Kapazität des ZIV im Bereich des numerisch intensiven Rechnens (Batchverarbeitung) drastisch erhöht. Beschafft werden sieben baugleiche Rechner des Typs IBM RS/6000 Modell 260:

- 64bit-Doppelprozessor-Systeme (200 MHz POWER3 Chip),
- 1 GB Hauptspeicher,
- 18 GB lokaler Plattenplatz.

Ein Prozessor dieses Doppelprozessor-Systems ist im Integer-Bereich viermal und im Gleitkomma-Bereich dreimal so schnell wie die bislang benutzten Rechner des Typs IBM RS/6000 Modell 590. Oder anders ausgedrückt: Im Integer-Bereich ist ein Prozessor eines neuen Rechners etwa so schnell wie die gesamte bislang im ZIV installierte Rechnerleistung für numerische Anwendungen! Bei sieben Doppelprozessoren vervierzehnfacht sich demnach die verfügbare Integer-Leistung.

Mit der Inbetriebnahme der Rechner werden wir auf den WWW-Seiten des ZIV Informationen zu deren Benutzung veröffentlichen.

Erfreulicherweise können wir die Kapazität des ZIV auch in anderen Bereichen ausbauen:

- 1 weiterer DFS-File-Server mit 180 GB Raid5-Plattenplatz,
- 1 weiteres Magnetbandlaufwerk für den Band-Roboter,
- Verdopplung der Speicher-Kapazität des Band-Roboters,
- 3 Server für den Netzwerkbereich.

Der zusätzliche Plattenplatz soll ausschließlich für Nutzer-Dateien verwendet werden. Wir denken an eine generelle Erhöhung der Platz-Quote für jeden.

## Zugang für Studierende zu den Rechnern der Fachbereiche

K.-B. Mertz

**Einige Fachbereiche, deren Rechner-Systeme an die Benutzerdatenbank des ZIV angeschlossen sind, erlauben nicht nur ihren Mitarbeitern, sondern auch Studierenden Zugang zu ihren Rechnern.**

### Rechner der Fachbereiche, Gemeinsamkeiten und Unterschiede

Der Anschluss an die Benutzerdatenbank bedeutet, dass die *Benutzerkennungen* (also die Namen, die man im Computer hat) in all diesen Systeme *dieselben* sind wie in den Rechnern des ZIV und dass die Dauer der Zugangsberechtigung beim ZIV registriert ist und von dort überwacht wird.

Die eigentlichen *Zugangskontrollsysteme* und die *Dateisysteme* sind jedoch voneinander und von denen der Rechner im ZIV (wo es zur Zeit auch noch zwei (fast) unabhängige Systeme, UNIX/DCE und Windows NT, gibt) *unabhängig*. Daher müssen die *Passwörter* in jedem dieser Systeme getrennt voneinander geändert werden und können folglich *unterschiedlich* sein. Außerdem haben Benutzer mit Zugang zu mehreren der beteiligten Systeme in jedem von ihnen (mit Ausnahme der Windows-Systeme) eine *eigene Mailbox*, so dass es sich empfiehlt, durch automatische Weiterleitung ankommender E-Mail diese in einer von ihnen zu sammeln. Die dafür notwendigen Schritte hängen von dem System ab, in dem die Weiterleitung eingetragen werden soll.

### DV-Projekte für Studierende

Jede Benutzerkennung ist in der Benutzerdatenbank mindestens einem DV-Projekt zugeordnet, das beschreibt, auf welchen Rechner-Systemen diese Kennung gültig ist und welche Rechte sie dort jeweils hat. Ein DV-Projekt kann also verstanden werden als Menge von Benutzerkennungen mit gleichartigen Rechten. Eine Kennung mit Zuordnung zu mehreren Projekten hat alle entsprechenden Rechte.

Studierende der WWU dürfen **für Zwecke des Studiums** die *UNIX- und NT-Rechner im ZIV*, ihre dort angelegte *Mailbox*, die *Einwählmöglichkeiten* sowie zum Drucken von Dateien den *Laser-Schnelldrucker (p3800)* benutzen; die Kennung wird beim Einrichten dem Projekt `u0dawin` zugeordnet, das diese Rechte beinhaltet.

Die *Zugangserlaubnis zu den Rechnern der angeschlossenen Fachbereiche* wird durch die Zuordnung zu einem entsprechenden DV-Projekt dokumentiert. Diese Zuordnung wird auf Antrag registriert, sofern man einen Studiengang in diesem Fachbereich belegt hat, und kann durch Ankreuzen des Punktes „im Rahmen des Projektes“ und Angabe des Projektnamens (s. u.) auf dem Standard-Formular B beantragt werden. Die Kontrolle über die Berechtigung geschieht zum Teil durch Beauftragte des Fachbereichs, die diese auf der Rückseite des Formulars bestätigen, für andere Fachbereiche an Hand einer Liste der Matrikelnummern, die beim Eintragen in die Datenbank durch das ZIV durchsucht wird.

Die Bezeichnungen und Bedingungen für die einzelnen Fachbereiche entnehmen Sie bitte der folgenden Projekt-Tabelle, wobei zu beachten ist, dass die Zuordnung zu `u0dawin` Voraussetzung für die übrigen Projekte ist.

Bereich	Projekt	Email-Adresse (Rechner-Teil)	Wo Antrag abgeben/ Kennung abholen ?	Unterschrift erforderlich?
ZIV	<code>u0dawin</code>	uni-muenster.de	ZIV, Einsteinstr. 60 <sup>3</sup>	nein
FB Psychologie / Sportwissenschaft	<code>h0stud</code> <sup>1</sup>	psy.uni-muenster.de	IVV, Fliegerstr. 21	ja
FB Mathematik / Informatik	<code>o0stud</code> <sup>1</sup>	math.uni-muenster.de	IVV, Einsteinstr. 62, 6. OG	ja
FB Physik	<code>p0stud</code> <sup>2</sup>	nwz.uni-muenster.de	ZIV, Einsteinstr. 60 <sup>3</sup>	nein
FB Chemie / Pharmazie	<code>q0stud</code> <sup>2</sup>	nwz.uni-muenster.de	ZIV, Einsteinstr. 60 <sup>3</sup>	nein
FB Biologie	<code>r0stud</code> <sup>2</sup>	nwz.uni-muenster.de	ZIV, Einsteinstr. 60 <sup>3</sup>	nein

Bei Fragen zum Rechner-Zugang wenden Sie sich bitte per E-Mail an `admuser@uni-muenster.de`.

<sup>1</sup> Erfolgt die Zuordnung zu diesem Projekt *am Tage der Zuordnung zu u0dawin*, so wird automatisch eine Weiterleitung der E-Mail an die Mailbox im Rechner-System des Fachbereichs eingerichtet.

<sup>2</sup> Jeder kann nur einem der 3 Projekte `p0stud`, `q0stud` und `r0stud` angehören; das Passwort im NWZ-Cluster (VMS) wird beim normalen LOGIN automatisch an das im NWZLAN (Windows NT) angeglichen.

<sup>3</sup> Zu Beginn eines Semesters kann die Kennung über ein WWW-Formular beantragt werden.

# Übergroße E-Mails

R. Perske

**Ein neuer Mechanismus erlaubt die Weitergabe auch solcher Dateien, die wegen Ihrer Größe nicht mehr als E-Mail-Anhang versendet werden können.**

Im Oktober 1995, also vor gerade einmal vier Jahren, wurden durch die Internet-Gemeinschaft Leitlinien für die Höflichkeitsregeln im Internet in Form des informellen Standards RFC 1855 festgelegt. Diese *Netiquette Guidelines* besagen unter anderem, dass man im Internet keine Dateien per E-Mail versenden soll, die größer als 50 Kilobyte sind.

Da eine Datei während des Transports per E-Mail aus technischen Gründen ein Drittel mehr Platz benötigen kann, müssen die E-Mail-Transportsysteme im Internet also in der Lage sein, E-Mails von etwa 70 Kilobyte Größe zu transportieren.

In anderen Netzen gelten sogar noch weit rigidere Vorschriften: Größenbeschränkungen auf höchstens 16 Kilobyte insgesamt für E-Mails sind durchaus noch in einigen Netzen üblich; angesichts der Tatsache, dass in solchen Netzen der Datentransport über Modem und Telefonfernverbindungen erfolgt, hat diese Beschränkung durchaus ihren Sinn.

Zwar tolerieren unsere eigenen E-Mail-Server schon seit längerer Zeit eine Maximalgröße von 2000 Kilobyte pro E-Mail, also dem 30-fachen der in den *Netiquette Guidelines* gesetzten Grenze; jedoch reicht vielen Nutzern auch dieser Freiraum angesichts der bei heutiger Software häufig üblichen Ressourcenverschwendung nicht mehr aus. Größere E-Mails können wir jedoch noch nicht akzeptieren, um nicht den Betrieb aller unserer E-Mail-Server zu gefährden; immerhin besagt die Grenze von 2000 Kilobyte bereits, dass der gesamte Inhalt einer 3½"-Diskette und dazu noch einige Begleitzeilen in einer einzigen E-Mail verschickt werden können. Einige andere Einrichtungen im Wissenschaftsnetz haben ähnliche Grenzen, es gibt Bestrebungen, diese zu vereinheitlichen.

## Die Alternative: Bigmail

Im Zeitalter des World Wide Web haben wir jetzt eine Alternative entwickelt, um große Dateien zu versenden, ohne sie an E-Mails anhängen zu müssen.

Das Prinzip ist einfach: Sie benutzen ein WWW-Programm, um die Dateien auf einem zentralen WWW-Server abzulegen. Der Empfänger erhält per E-Mail eine kurze Nachricht, von wo er die Datei herunterladen kann. Dazu hat er etwa eine Woche Zeit; danach wird die Datei automatisch wieder vom WWW-Server gelöscht.

Sie finden die entsprechende WWW-Seite unter dem Stichwort **Übergroße E-Mails** auf der Titelseite des Zentrums für Informationsverarbeitung oder direkt unter der Adresse

<http://user.uni-muenster.de/exec/bigmail>

Dieses Formular kann sowohl von angemeldeten Nutzern verwendet werden, um Dateien an beliebige Adressaten zu versenden, als auch von beliebigen Außenstehenden; letztere können Dateien jedoch nur an angemeldete Nutzer versenden. Angemeldete Nutzer sind alle Inhaber einer E-Mail-Adresse der Form `kennung@uni-muenster.de`.

## Referenzzentrum für das neue Internet

### - Das JOIN-Projekt im ZIV wird weitergeführt -

C. Müller-Böhm

**Im Auftrag des DFN wird seit dem 1. Oktober das JOIN-Projekt mit zwei neuen Mitarbeitern im Zentrum für Informationsverarbeitung (ZIV) weitergeführt.**

JOIN (*Join Open InterNetworks*) soll die Einführung des neuen Internet-Protokolls IPv6 vorantreiben und Mitgliedsorganisationen des Deutschen Forschungsnetzes (DFN) mit Rat und Tat zur Seite stehen. Wie bisher wird das JOIN-Projekt-Team unter der Adresse <http://www.join.uni-muenster.de> aktuelle Informationen über IPv6 anbieten. Ein weiterer Schwerpunkt liegt in der Mitarbeit im weltweiten IPv6-Testnetz *6bone*, in dem JOIN einer der größten Provider ist.

### IPv6 – das neue Internet-Protokoll

IPv6 (Internet-Protokoll Version 6) ist der Nachfolger von IPv4, auf dem das Internet zur Zeit basiert. Ein neues Internet-Protokoll wurde durch die zunehmende Verknappung der Internetadressen im weltweiten Netz nötig. Noch reicht der Adressraum zwar aus und lässt sich durch technische Tricks besser ausnutzen, es ist aber abzusehen, dass die Grenzen in den nächsten Jahren erreicht werden. So denken Unternehmen im Bereich der Telekommunikation bereits darüber nach, ihre zukünftigen Handy-Produkte mit IP-Adressen zu versehen, auch Handheld-PC sollen ihre eigenen IP-Adressen bekommen. Dazu kommt, dass die intensive Nutzung des Internets bisher hauptsächlich auf die Industrienationen beschränkt ist. Weltweit muss also weiterhin mit einem immensen Wachstum des Internets gerechnet werden. Mit dem heutigen Adressraum von 32 Bit ist es nicht mehr möglich, vernünftige hierarchische Adressstrukturen im Internet aufzubauen, wodurch die Tabellen in den Routern für das Weiterleiten (*Routen*) von IP-Paketen sehr komplex werden und die Kapazitätsgrenzen der Router erreicht werden.

Nach langer Entwicklungszeit für ein neues Internet-Protokoll entschied sich die IETF (*Internet Engineering Task Force*) aus einer Reihe von Vorschlägen für IPv6 als neues Protokoll. Wichtige Standards wurden Ende 1998 verabschiedet, so dass nun für Hard- und Softwarehersteller die Grundlagen bestehen, IPv6-fähige Produkte auf den Markt zu bringen. Fast alle namhaften Hersteller entwickeln IPv6-fähige Produkte oder bieten bereits solche an. So ist z. B. IPv6 im Unix-Betriebssystem AIX von IBM der Version 4.3 schon integriert. Auch für Windows NT gibt es einfach zu installierende Software für IPv6, hier allerdings noch als Testversion. Ebenso gibt es für die Unix-Derivate Linux und BSD IPv6-fähige Softwarepakete.

Das neue Protokoll erhöht den Adressraum von 32 auf 128 Bit und stellt damit praktisch unbegrenzt viele Adressen zur Verfügung. Durch den deutlich erweiterten Adressraum wird gewährleistet, dass hierarchische Routing-Strukturen im Internet aufgebaut werden können, so dass das Weiterleiten der IP-Pakete durch kleinere Routing-Tabellen erleichtert wird. Auch werden strenge Kriterien an Provider gestellt, um eine effiziente Verteilung der neuen Internet-Adressen zu gewährleisten.

Einen weiteren Vorteil bietet IPv6 durch die Bedingung, dass jede vollständige IPv6-Implementierung auch die IP Security Architecture (IPSec) beinhalten muss. Mit IPSec werden dann auf jedem IPv6-System Verfahren zur geschützten Datenübertragung und zur Signierung vorhanden sein. Dadurch werden Sicherheitsmechanismen im Internet zur Verfügung stehen, die unabhängig vom Betriebssystem der einzelnen Rechner sind.

Um einen allmählichen Übergang von IPv4 zu IPv6 zu gewährleisten, wurde ein Migrationsszenario entwickelt, das die Koexistenz von IPv6 und IPv4 ermöglicht. Grundprinzip ist hier das *Dual-IP-Stack*-Verfahren. IPv4-Hosts und -Router werden nach und nach um IPv6-fähige Software erweitert und können dann beide Protokolle verarbeiten. Um IPv6-Pakete durch das heutige auf IPv4 basierende Internet zu senden, werden die IPv6-Pakete in IPv4-Pakete eingepackt und auf speziell dafür konfigurierten Wegen durch das Internet geroutet (IPv4-Tunnel). Solche Tunnel werden für das internationale IPv6-Testnetz *6bone* benutzt, um IPv6-Verbindungen im heutigen IPv4-Internet herzu-

stellen. Für eine lange Zeit wird es IPv4 und IPv6 parallel geben, so dass Umstellungen auf IPv6 dann gemacht werden können, wenn Geräte planmäßig ersetzt werden oder wenn neue Softwareversionen eingespielt werden.

### **JOIN im internationalen IPv6-Verbund**

JOIN gehört mit 19 internationalen Verbindungen zu einem der großen Provider im 6bone-Testnetz. JOIN stellt für interessierte Einrichtungen IPv6-Adressen und IPv4-Tunnel zur Verfügung, um die Teilnahme am 6bone zu ermöglichen. Zur Zeit sind 44 Einrichtungen über JOIN an das 6bone angeschlossen, 14 weitere sind in Vorbereitung. Das JOIN-Projekt-Team hilft den IPv6-Interessierten bei der Einrichtung ihrer Geräte und kann im eigenen IPv6-Labor im Problemfall Szenarien nachstellen, um gezielte Fehlersuche zu betreiben.

Als nächstes wird sich JOIN am *Quantum IPv6 Test Program* (QTPv6) beteiligen. Im QTPv6 wird auf internationaler Ebene ein „echtes“ IPv6-Testnetzwerk aufgebaut. Initiiert wurde das Programm von DANTE (*Delivery of Advanced Network Technology to Europe Limited*), dem Betreiber des europäischen Forschungsnetzes TEN-155, und von TERENA (*Trans-European Research and Education Networking Association*), der europäischen Vereinigung nationaler Forschungsnetzbetreiber. Zur Teilnahme am QTPv6 hat JOIN eine 1 Mbit/s Leitung vom JOIN-Labor im ZIV nach Amsterdam schalten lassen. Durch die direkte Verbindung kann ein reines IPv6-Netzwerk aufgebaut werden, in dem IPv6-Pakete direkt geroutet werden – ohne Umwege über IPv4-Tunnel gehen zu müssen. In diesem reinen IPv6-Netzwerk sollen verschiedene Tests durchgeführt werden, z. B. in wie weit Router von verschiedenen Herstellern fehlerfrei zusammenarbeiten. Durch Übergänge zum 6bone und zum „normalen“ IPv4-Internet können hier auch die Migrationsszenarien getestet werden.

### **Was JOIN sonst noch so bietet ...**

Auf den JOIN-Web-Seiten (<http://www.join.uni-muenster.de>) findet man ein ständig aktualisiertes Angebot von Informationen und Dokumenten zu IPv6. Auch Hinweise zu IPv6-Implementationen von verschiedenen Herstellern und Tipps zur Installation von IPv6-Software werden dort gesammelt. Noch im Aufbau befindet sich ein Pressearchiv, in dem auch allgemeinverständliche Artikel zum Thema IPv6 angeboten werden. JOIN bietet eine Mailingliste, einen Ftp-Server mit IPv6-Software und hat natürlich viele wichtige Links zum Thema IPv6 zusammengetragen. Wer sich näher für IPv6 interessiert oder am 6bone teilnehmen möchte, kann sich gerne direkt an das JOIN-Projekt-Team per E-Mail an [join@uni-muenster.de](mailto:join@uni-muenster.de) wenden.

## Neues über Software

B. Süselbeck / S. Zörkendörfer

**Hier erwartet Sie aktuelle Information zu den bekannten Statistik-Programmen SAS und SPSS, den Programmen SYSTAT und Statistica und zur Vertragslage bezüglich der Nutzung von Virenschutz-Software.**

### SPSS und Axum

Am 1. Dezember 1999 begann ein neues Lizenzjahr zum SPSS am PC. Auch für dies neue Lizenzjahr hat das ZIV (URZ) im Voraus eine angemessene Kopienzahl geordert, evtl. notwendige Nachbestellungen werden wir wieder bis etwa April/Mai 2000 nachmelden können, danach läuft nichts mehr. In der Vergangenheit erreichten uns im Sommer und Herbst regelmäßige Nachfragen zu weiteren Kopien – wir antworteten leider mit „Vergriffen/Ausverkauft“. Dieser Hinweis gilt deshalb insbesondere denjenigen, die noch nicht wissen, dass sie im Laufe des Lizenzjahres das SPSS auf einem dienstlichen oder häuslichen PC nutzen wollen! Innerhalb der Universität kann das SPSS weiterhin auf vielen öffentlich zugänglichen Rechnern genutzt werden, so z. B. auch im CIP-Pool des ZIV.

Als Standardversion wird die deutsche Version 9 des SPSS zur Verteilung gelangen, dabei sind folgende Optionen eingeschlossen: *Base, Regression Models, Advanced Models, Tables, Trends, Categories, Exact Tests, Missing Value Analysis, Conjoint*. Bereits im Herbst konnte ich die deutsche Version 9 erfolgreich in einer Lehrveranstaltung in unserem CIP-Pool erproben. Bezüglich der Neuerungen des SPSS möchte ich insbesondere auf die Nachbearbeitung der OLAP-Würfel im Ausgabefenster, auf ROC-Kurven und auf zusätzliche Variationsmöglichkeiten bei der interaktiven Grafik hinweisen. Solange der Vorrat reicht, werden wir zu den Lizenzen als Datenträger CDs ausliefern. Den Bonner Kollegen sei an dieser Stelle Dank ausgesprochen für die Pflege unseres Hochschullandeslizenzvertrags sowie den Kölner Kollegen für die Aufbereitung der CD.

Eine SPSS-Lizenz umfasst zusätzlich die Nutzungsberechtigung der Produkte *SPSS Data Entry Builder* (und nicht *SPSS Data Entry Network Server*), *Amos* (in Nachfolge vom *Lisrel*), *Axum6* (in Nachfolge von *Axum5*) und *CHAID* (bis 31.12.1999, danach *AnswerTree 2.0*). Zur Nutzung von *Neuronal Connection* fragen Sie bitte bei mir nach, ebenso bezüglich eines Datenträgers zu *AnswerTree*. Die Produkte des *SPSS Science* (*SYSTAT, SigmaPlot, ...*) sind nicht Gegenstand dieses Lizenzvertrages.

Mit Beginn des neuen Lizenzjahres sollten Sie – falls nicht bereits erfolgt – von älteren Versionen auf die Version 9 umsteigen. Ältere Versionen sind nicht Jahr-2000-zertifiziert, zu Versionen 7 und 8 werden wir keine Lizenzcodes erhalten. Mit der bereitgestellten CD sind Installationsmaterialien für die deutsche Version 9 und die englische Version 9 aufbereitet, ferner veraltete 6er Versionen für Windows 3.1, WfW3.11, Mac und Power-Mac. Die CD enthält die *Syntax-Reference-Guides* im PDF-Format. Ein deutschsprachiges Benutzerhandbuch der Version 9 ist im Buchhandel erhältlich, bei Anfrage nenne ich gerne Bezugshinweis und Rabattvereinbarung. Ausführliche Informationen zum Bestellvorgang des SPSS sehen Sie auf einem Aushang im ZIV und auf der WWW-Seite

<http://www.uni-muenster.de/ZIV/Organisation/SoftwareVerteilungSPSS.html>.

SPSS-Fans werden sich an den Anfang der 80er Jahre erinnern: Nach SPSS Release 9 wurden sehnlichst die Neuerungen des SPSS<sup>X</sup> (X wie römisch 10 oder X wie eXtended?) erwartet. Zeitgemäß ist das jetzt wesentlich anwendungsfreundlicher geworden: Auf Version 9 folgt Version 10; die englische Version 10 wird uns evtl. noch im Jahr 1999 angeliefert werden.

Zum 30.9.1999 haben wir die Bereitstellung des SPSS unter Unix eingestellt. Diese Plattform diente seinerzeit insbesondere für die Migration von unseren IBM-Großrechnern – heute kommen wir in der Regel mit der Leistungsfähigkeit eines PC aus! Aber nicht ausschließlich Kapazitätsfragen waren für die Abmietung maßgebend – auch unter AIX und Solaris wurde nur eine veraltete Version 6 bereitgestellt. Das derzeit angekündigte *SPSS 10.0 Server* ist nicht Produkt unseres PC-Vertrags.

## SAS

Bezüglich des Hochschullandeslizenzvertrages zum SAS am PC sind Neuigkeiten zu vermelden. Auch hier wird wegen des Jahr-2000-Problems ein Produkt aus dem Vertrag genommen: SAS 6.04 unter MS-DOS wird nicht mehr angeboten, als Ersatz wird die Macintosh-Version (mit dem Optionen-Umfang der DOS-Version, nämlich *BASE, STAT, GRAPH, ETS, FSP, AF, OR, IML, QC, ASSIST*) angeboten. Für die Windows-Version SAS 6.12 ist ein Upgrade TS060 angekündigt, auf Zuruf werde ich Kopien der Datenträger weitergeben. Die Version 7 des SAS wird in Europa nicht zur Auslieferung gelangen.

## Statistica und SYSTAT

Der Campusvertrag Statistica zur Nutzung auf dienstlichen Rechnern ist bis zum 30.11.2000 verlängert worden. Im Rahmen dieses Vertrages sind noch Lizenzen für die Windows-Plattformen erhältlich. Die Kosten für eine Einzellizenz betragen DM 208,80. Eine solche Lizenz kann bis zu dem oben genannten Datum genutzt werden.

Der Lizenzvertrag SYSTAT 9.0 wurde bis zum 30.11.2000 verlängert. Im Rahmen dieses Vertrages sind noch Lizenzen für die Windows-Plattformen erhältlich. Die Kosten für eine Einzellizenz betragen DM 200,00. Eine solche Lizenz kann zur Nutzung auf dienstlichen Rechnern bis zu dem oben genannten Datum eingesetzt werden.

Rückfragen und Bestellungen zu beiden Produkten richten Sie bitte an Dr. B. Süselbeck, ☎ 3 16 86, ✉ [suselbe@uni-muenster.de](mailto:suselbe@uni-muenster.de)

## Virenschutz

Es gab und gibt Schwierigkeiten bezüglich der Versorgung mit Datenträgern aktuellen Inhalts zu den vom Universitätsrechenzentrum geschlossenen Verträgen zum Virenschutz. Eine vollständige Beschreibung der Situation ist an dieser Stelle schon deshalb nicht möglich, weil diese Verträge eine Vielzahl von Produkten auf vielen Plattformen beinhalten. Der Einfachheit wegen sei hier also nur die Situation beschrieben für den Virenschutz auf einer Windows-NT-Workstation – dies die bei uns am häufigsten nachgefragte Systemumgebung.

Der Lizenzvertrag wurde – unter Einschaltung eines Handelspartners – geschlossen zwischen der (damaligen) Firma Dr. Solomon's Software GmbH und der WWU, er umfasst u. a. **Dr. Solomon's AntiVirusToolkit AVT** für Windows NT, und zwar sowohl die stückzahlbegrenzte Nutzungsberechtigung wie die zusätzlich in Rechnung gestellte Versorgung mit monatlichen Aktualisierungen auf Datenträgern. Bezüglich dieser monatlichen Zusendung kam und kommt es nach Übernahme der Firma Dr. Solomon's durch Network Associates (NAI) zu Lücken. Dies lässt sich in Notfällen dadurch entschärfen, dass Updates übers Netz bei Dr. Solomon's oder NAI gezogen werden können. Es zeigte sich aber auch, dass eine nur monatliche Versorgung nicht mehr zeitgemäß ist.

Nun soll aber auch eine gute Seite dieser Vereinbarung genannt sein. Nach Firmenübernahme bietet uns NAI zusätzlich zum AVT die Nutzung der **Virus Scan Security Suite (McAfee)** an – diese beinhaltet u. a. das *VirusScan for Windows NT (Intel) Version 4*. Hier hat sich nun eine durchaus zufriedenstellende Versorgung eingestellt – wir ziehen regelmäßig Updates (oder bekommen sie übers Netz zugeschickt, wenn wir Schreibzugriff auf einem System einräumen), die Wartung ist wesentlich einfacher geworden, indem z. B. ein wöchentlicher automatischer Update von einem Verzeichnis eines Netzwerklaufrwerks konfiguriert wird. Auch die Migration von AVT zu VirusScan gelang auf den NT-Workstations problemlos – Erfahrungsberichte vieler Nutzer bestätigen diese Einschätzung.

Nutzern des AVT (Dr. Solomon's) empfehlen wir dringend und baldigst den Umstieg zum VirusScan (McAfee).

Da das ZIV einerseits nicht über Finanzierungsmittel zu einer umfassenden Lizenz verfügte, andererseits aber auch nicht Ummengen von Einzelrechnungen mit kleinen Beträgen verwalten kann – zum ursprünglichen Vertragstext wäre auch noch die monatliche Versorgung mit Datenträgern in Rechnung zu stellen – werden Lizenzen vom ZIV (URZ) direkt nur an IVVen weitergegeben; Nutzer wenden sich also an ihre IVV. Der ursprünglich geschlossene Vertrag läuft im Frühjahr 2000 aus, wir werden uns um einen Nachfolgevertrag bemühen und streben diesbezüglich einen Campus-Vertrag (mit Einbeziehung der häuslichen Nutzung für Mitarbeiter und Studierende) für die gesamte Universität an.

## CITYKOM-Zugang zum Rechnernetz der WWU

W. Held / G. Richter

**Neben den bisherigen Einwählzugängen der Telekom gibt es jetzt auch Zugänge des münsterschen Netzproviders CITYKOM.**

Das Zentrum für Informationsverarbeitung bietet 120 Einwählzugänge an, die über das Telefonnetz der *CITYKOM Münster GmbH Telekommunikationsservice* erreichbar sind. Diese Zugänge ermöglichen den Zugang zum gesamten Rechnernetz der WWU und den damit verbundenen Netzen Dritter, insbesondere dem Internet. Die CITYKOM ist bekanntlich eine lokale Telekommunikationsgesellschaft in Münster, die u. a. verschiedene Dienste im Bereich der Telefonie und der Standard-Festverbindungen anbietet. Die Einwähldienste der WWU können von Studierenden und Mitarbeiter/innen der WWU in Anspruch genommen werden. Das Einwählen ist über Modem- und ISDN-Verbindungen möglich. Die Nutzer benötigen eine Kennung und ein Passwort der WWU, die sie im ZIV bekommen können. Die Rufnummer der CITYKOM-Einwählzugänge lautet einheitlich: (0251) 987 26 60

Einzelheiten (z. B. Tarife für CITYKOM-Kunden und andere Nutzer) werden von der Fa. CITYKOM selbst bekannt gegeben. Technische Einzelheiten und den aktuellen Status aller Einwählsysteme im ZIV sowie weitere wichtige Hinweise erfahren Sie unter

<http://www.uni-muenster.de/ZIV/Content--NetzEinwahl.html>

## MeDiDa-Prix 2000

**Auf Initiative der Gesellschaft für Medien in der Wissenschaft e. V. (GMW) wird im kommenden Jahr erstmals der mediendidaktische Preis MeDiDa-Prix 2000 vergeben.**

Zweck der Preisvergabe ist die Förderung der Qualität in der mediengestützten Lehre, wobei es nicht so sehr auf technische, sondern auf didaktische Innovationen ankommt. Der Preis wird vom österreichischen Ministerium für Wissenschaft und Verkehr vergeben und ist mit

ATS 1.000.000,- (ca. DM 140.000,-)

dotiert. Er wird im Rahmen der internationalen Fachtagung der GMW in Innsbruck (19.–21.09.2000) verliehen. Der Schlusstermin für die Online-Registrierung ist der 6. Januar 2000. Detaillierte Informationen und Ausschreibungsunterlagen im WWW:

<http://www.medidaprix.org>

Weitere Auskünfte und gedrucktes Material erhalten Sie auf Anfrage per E-Mail bei [medidaprix@uibk.ac.at](mailto:medidaprix@uibk.ac.at).

## Betriebsreports des Universitätsrechnernetzes

M. Speer

**Auf den Web-Seiten des ZIV werden seit einiger Zeit schon Betriebsreports des Universitätsrechnernetzes bereitgestellt. In diesen Betriebsreports wird die Nutzung ausgewählter Netzkomponenten zusammenfassend dargestellt.**

In folgenden Arbeitsbereichen des Netzbetriebs sind derartige Reports von besonderer Bedeutung:

- Dienstgüteüberwachung,
- Kapazitätsplanungen (frühzeitige Erkennung von Engpässen),
- Fehlererkennung, -analyse.

In einem ersten Schritt werden Reports zur Nutzung des Anschlusses des Universitätsnetzes an das Internet (BWiN-Anschluss) und zur Auslastung der Einwählzugänge bereitgestellt. Es ist geplant, zukünftig weitere Betriebsreports hinzuzufügen. Dabei kommen Reports nicht nur für das Datennetz im engeren Sinne in Frage, sondern auch solche, die z. B. die Auslastung von wichtigen Servern in den IV-Versorgungsbereichen darstellen. Bei Bedarf wenden Sie sich bitte an das ZIV.

Die Betriebsreports sind unter folgender Adresse zu finden:

<http://www.uni-muenster.de/ZIV/Content--NetzBetriebReports.html>

## X11-Server-Emulation mit Exceed im Universitätsrechnernetz

M. Speer

**Im Rechnernetz der Universität steht das Produkt Exceed der Firma Hummingbird nun in der Version 6.1 zur Nutzung bereit**

Exceed beinhaltet u. a. die Emulation eines Servers des X-Window-Systems (kurz X11-Server). Das bedeutet, dass Sie Ihren Windows-PC zu einem grafischen Terminal für Mehrbenutzersysteme (i. Allg. Unix-Systeme) im Rechnernetz der Universität machen können. Grafische Programme (sog. X11-Anwendungen) und Benutzeroberflächen, die auf anderen Systemen im Netz ablaufen, werden auf dem Bildschirm Ihres PCs dargestellt. Darüber hinaus umfasst das Produkt eine Reihe weiterer gängiger Internet-Anwendungen (z. B. FTP und TELNET mit hochwertiger Terminal-Emulation).

Das ZIV hat in ausreichender Anzahl Lizenzen für den Einsatz des Produktes im Universitätsrechnernetz erworben. Um Exceed auf einem Rechner im Netz nutzen zu können, benötigen Sie eine Benutzerkennung auf den zentralen Systemen des ZIV. Diese Benutzerkennung muss auch in der Windows-NT-Domäne WWU bekannt sein. Eine Nutzung von Exceed ohne eine geeignete Benutzerkennung (z. B. eine lokale Installation der Software) ist nicht vorgesehen. Hinweise zur Einrichtung einer Kennung in der Windows-NT-Domäne WWU und zur Installation und Nutzung der Software finden Sie auf dem zentralen Web-Server der Universität:

<http://www.uni-muenster.de/ZIV/Hinweise/exceed/install-6.1/>

## DFN-Verein vervierfacht Netzrate in die USA

**Der DFN-Verein erweitert die USA-Kapazität im Deutschen Forschungsnetz und strukturiert die internationale Anbindung neu.**

Der DFN-Verein wurde 1984 als Gemeinschaftseinrichtung deutscher Hochschulen und außeruniversitärer Forschungseinrichtungen sowie forschungsnaher Wirtschaftsunternehmen zur Förderung des Deutschen Forschungsnetzes (DFN) gegründet. Als kritische Größe für die Leistungsfähigkeit des DFN wurde stets die Geschwindigkeit der Datenübertragung von und in die USA angesehen. Die Kapazität der USA-Leitungen konnte im Oktober 1999 von 155 Mbit/s auf insgesamt 610 Mbit/s, also auf nahezu das Vierfache erhöht werden. Gleichzeitig wurde die Verteilstruktur innerhalb des Breitband-Wissenschaftsnetzes (BWiN) neu organisiert, um die internationale Kapazität effektiver nutzen zu können.

Darüber hinaus hat der DFN-Verein in seinem Standort New York gemeinsam mit der europäischen Netzorganisation DANTE Ltd., Cambridge, eine direkte Verbindung zu „Abilene“, dem Netz der Internet2-Initiative der US-amerikanischen Wissenschaftsorganisation UCAID (The University Corporation for Advanced Internet Development) geschaltet. Durch diese Anbindung wird die Kooperation zwischen den europäischen Wissenschaftsnetzen und UCAID zum Aufbau der nächsten Internet-Generation, dem Internet2, gewährleistet. Über das BWiN wird der transatlantische Datenverkehr an derzeit vier Knoten geleitet: Hannover, Köln, Leipzig und München.

Das BWiN wird von ca. 700 Einrichtungen genutzt. Das im BWiN übertragene Datenvolumen lag im Sommer 1999 bereits bei mehr als 120 TeraBytes pro Monat. Der DFN-Verein rechnet damit, dass in fünf Jahren das übertragene Datenvolumen im GWiN nicht mehr in TeraBytes, sondern in PetaBytes (1.000 TeraBytes = 1 PetaByte) pro Monat gemessen werden wird. Um diesen Anstieg des Datenvolumens im nationalen Wissenschaftsnetz aufzufangen und neue Formen der Netznutzung zu ermöglichen, stellt der DFN-Verein ab Frühjahr 2000 das Gigabit-Wissenschaftsnetz GWiN zur Verfügung. Dieses Wissenschaftsnetz wird in der Anfangsphase Anschlusskapazitäten in den nutzenden Einrichtungen von Wissenschaft und Forschung in Deutschland bis zu 2,5 Gbit/s ermöglichen.

## Neue TUSTEP-Version 2000

*W. Kaspar*

**Ab sofort steht bei uns die neue TUSTEP-Version 2000 für die Betriebssysteme Solaris, AIX, Linux und Windows 95/98/NT zur Verfügung.**

Die Autoren schreiben hierzu auf Ihren WWW-Seiten unter

`<http://www.uni-tuebingen.de/zdv/tustep/index.html>`

„Da in der Version 1999 noch Y2K-Probleme entdeckt wurden, raten wir dazu, die neue Version noch vor der Jahreswende zu installieren. Im Übrigen wurde für die Version 2000 viel Aufwand in die Abrundung und Konsolidierung der Erweiterungen der Vorgängerversionen (Kommandomakros; CGI-Schnittstelle; XML-Unterstützung im Satz) gesteckt. Darüber hinaus wurde der Tatsache Rechnung getragen, dass TUSTEP in immer größerem Umfang als Datenbanksystem, auch für den Zugriff über das WWW, eingesetzt wird. Dies erfordert u. a. Möglichkeiten zur Koordination von konkurrierenden (lesenden und schreibenden) Zugriffen auf Datenbestände. Schließlich wurden die Schnittstellen für den Datenaustausch den internationalen Entwicklungen angepasst.“

Die Unix-Varianten befinden sich wie üblich auf unserem zentralen Server und können von dort direkt aufgerufen werden. Die Windows-Variante ist wie auch die Linux-Variante auf CD (oder auch Disketten) erhältlich. Außerdem steht auch noch für MS-DOS die etwas ältere Version 10/95 zur Verfügung.

Die TUSTEP-Disketten können nach Absprache direkt über mich (W. Kaspar, [kaspar@uni-muenster.de](mailto:kaspar@uni-muenster.de), © 3 16 73) bezogen werden.

# Fingerabdrücke

R. Perske

**Dieser Beitrag enthält die aktuellen kryptografischen Prüfsummen der öffentlichen Schlüssel, die vom Zentrum für Informationsverarbeitung verwendet werden.**

Die PGP-Schlüssel der Mitarbeiter des ZIV finden Sie im WWW zusammen mit den PGP-Schlüsseln verschiedener Zertifizierungsinstanzen unter der Adresse

<http://www.uni-muenster.de/ZIV/Mitarbeiter/urzring.asc>.

Die Prüfsumme des öffentlichen PGP-Schlüssels der Zertifizierungsstelle im ZIV lautet:

```
2048/EF750F1D 1997/10/14 Rainer Perske +49(251)83-31582 Certification Key
Key fingerprint = 2F 38 6E F8 DC 2E D8 5E 5B 35 DB 49 8A E4 52 AF
```

Die Prüfsummen der öffentlichen PGP-Schlüssel der Mitarbeiter des Zentrums für Informationsverarbeitung lauten:

```
2048/CB300279 1999/12/13 Hermann Kamp <kamp@uni-muenster.de>
Key fingerprint = 52 E3 72 08 31 FE 8D 8C A4 22 47 F4 50 4E 39 8D
2048/B8DEA0FB 1999/12/03 Holger Schwering <puersh@uni-muenster.de>
Key fingerprint = 82 09 CC 44 4E 7D 60 94 0F 33 49 1B 41 81 12 D5
1024/E63AEF1F 1999/11/10 Peter Drube <drube@uni-muenster.de>
Key fingerprint = 58 B0 41 5E 29 9A 9F A8 8A 0C 76 81 98 AE 10 0E
2048/BEC48A5D 1999/11/15 Rita Sieber <sieberr@uni-muenster.de>
Key fingerprint = A6 92 0D 1A 4B A9 90 CE 48 E0 5B 76 AC BC C9 5E
2048/6CDC0153 1999/11/15 Norbert Gietz <gietz@uni-muenster.de>
Key fingerprint = 42 6B 42 8B 34 0A 42 E1 91 49 FA B8 BA 07 B9 28
2048/4985B561 1999/11/15 Marco Angerstein <marcoa@uni-muenster.de>
Key fingerprint = 8F 5B 6D F6 FD D3 D1 BE 6D 2B 1E 66 69 DC 96 09
1024/E12EFB01 1999/11/15 Dieter Schulze <schulze@uni-muenster.de>
Key fingerprint = E2 14 0D 1F 7C D3 40 52 6D 8E B5 AC 79 A7 2C C1
2048/C81E1ED7 1999/11/15 Dany Born <born@uni-muenster.de>
Key fingerprint = 84 9D 92 D8 5D 5D B4 50 4E 2F B8 5F 3A 68 B0 56
2048/A6615C71 1999/11/15 Christian Döring <chrischd@uni-muenster.de>
Key fingerprint = B5 61 C3 BF 09 28 E4 BB 60 5B 29 67 A6 AB 24 30
2048/D574E271 1999/11/12 Stefan Focke <focke@uni-muenster.de>
Key fingerprint = CD 08 85 3F 4B 66 96 7E 73 45 E4 DC 2D 38 93 4F
2048/E583CC4B 1999/11/12 Martin Ketteler-Eising <mke@uni-muenster.de>
Key fingerprint = 11 EA 7D 89 B8 47 50 1A 35 6E C2 FE 22 23 F6 4F
2048/1EDC8B37 1999/11/12 Herbert Mohr <mohr@uni-muenster.de>
Key fingerprint = 82 02 04 53 7A 4C 15 C7 EF FF 6A A3 20 95 D4 1A
2048/9EF30A7D 1999/11/12 Cornelia Ossendorf <ossendo@uni-muenster.de>
Key fingerprint = 4E CB 19 E1 11 AF C5 98 E0 54 D9 B1 FF 52 61 03
2048/C03D79CF 1999/11/11 Frank Borß <borss@uni-muenster.de>
Key fingerprint = F5 5E DC 29 6B A5 8B D8 37 6D 0D 7A FC A9 6C EC
2048/3BFABFD5 1999/11/09 Dieter Frieler <frieled@uni-muenster.de>
Key fingerprint = 0A 5B 4C 66 FF B2 F8 0B F1 90 E9 27 05 B0 D4 AC
2048/B2ACA3B7 1999/10/26 Christian Mueller-Boehm <bohmc@uni-muenster.de>
Key fingerprint = 3F AA 2D CB E6 AA 08 1D C5 7A E1 65 A8 81 C6 D6
2048/361F825D 1999/09/02 Dr. Wilhelm Lange <lange@uni-muenster.de>
Key fingerprint = FA 4C 9D 40 CF C4 FB 7A 21 9D 45 F5 4E C1 18 84
2048/284F8FBB 1999/08/13 Michael Kamp <kampm@uni-muenster.de>
Key fingerprint = 78 F4 72 1B CD 36 D0 BE 77 97 1E 0D 3D FB CB FE
2048/5B50E4E7 1999/07/16 Dr. Wilhelm Held <held@uni-muenster.de>
Key fingerprint = 0E 82 2F 90 42 A2 E8 5B E9 C5 2A 0E EE 43 71 60
1536/7870F29D 1999/05/21 Martin Schlütz <schlutz@uni-muenster.de>
Key fingerprint = E8 F4 DB FA F0 40 D1 0B 58 43 9F 43 13 7B 14 9D
2048/DE00243F 1999/05/05 Wolfgang Kaspar <kaspar@uni-muenster.de>
Key fingerprint = E2 38 F0 5C 58 94 C5 6F F9 D7 06 AD 17 9E A9 59
2048/456CC783 1999/03/19 Karin Giermann <giermann@uni-muenster.de>
Key fingerprint = C2 19 72 89 36 36 76 6F 4C 4E 1F 5B 2B 12 05 03
2048/8D598B97 1999/03/17 Walter Bosse <bosse@uni-muenster.de>
Key fingerprint = 15 32 90 0C 3E 91 00 9A 8F 5A 82 2C D4 62 56 A3
2048/7231BCE7 1999/03/17 Dr. Hilmar Pudlatz <pudlatz@uni-muenster.de>
Key fingerprint = 7B F7 C6 06 95 99 53 3A 90 7B BF FB 7D 78 03 2E
1024/D3560AA5 1998/11/30 Guido Wessendorf <wessend@uni-muenster.de>
Key fingerprint = 46 F8 4E C0 3E 85 0D 05 10 E1 44 6E AF F1 0D 47
2048/131B72ED 1998/08/18 Rainer Altvater <altvate@uni-muenster.de>
Key fingerprint = FF 89 81 67 37 45 2B 1C 57 F5 BB DD 4A D5 04 60
2048/8D1993F9 1998/02/27 DaWIN-Team <dawin@uni-muenster.de>
Key fingerprint = 4D 3F C7 49 F6 75 E1 AF 36 A3 F8 2C 04 86 F8 0F
1536/E307C0B9 1997/10/14 Rainer Perske <perske@uni-muenster.de>
Key fingerprint = F3 99 93 1F AC 06 0D 17 ED 93 35 19 F6 2D A3 22
1024/525140B9 1997/09/01 JOIN Project Team <join@uni-muenster.de>
Key fingerprint = 8C A9 DF 11 F5 21 89 DA 44 73 F1 FA 86 3A 1A 71
768/D782E369 1997/07/18 Klaus Reichel <reichel@uni-muenster.de>
Key fingerprint = 6C 35 15 A9 E3 9E 83 4E 2E 95 4A F1 47 FC 7F 58
```

```

1024/9C6463F9 1997/07/14 Christian Schild <schild@uni-muenster.de>
  Key fingerprint = D7 D9 15 53 2C BB 5D 70 FD C1 E1 C5 EF 05 95 EE
1024/3D37C6E1 1997/06/19 Dr. Klaus-Bolko Mertz <mertz@uni-muenster.de>
  Key fingerprint = CA 6F 8D 5C EB 67 EA 18 38 79 64 3D 64 4C 4A 8C
1024/29A14DD1 1997/06/18 Reinhard Mersch <mersch@uni-muenster.de>
  Key fingerprint = F0 AF 2B F1 FE 55 7A 3A E6 0D C7 27 29 50 22 26
1024/51F8EA05 1997/06/18 Mathias Grote <grote@uni-muenster.de>
  Key fingerprint = 0F 13 5B 2D 1D A5 9D 65 DF EA 41 6B CE E5 88 C2
1024/BD7873F5 1997/06/17 Jürgen Hölterers <holterers@uni-muenster.de>
  Key fingerprint = EA CB 47 AF 3A 79 96 B5 D3 46 C8 98 53 72 3F 2B
1024/3EBBF595 1997/02/24 "Eberhard Sturm" <sturm@uni-muenster.de>
  Key fingerprint = 6C 9D B3 38 C0 8C 3C BB AF 55 2A 7B 6A C4 66 B6
1024/44C661C5 1996/12/06 Stefan Ost <ost@uni-muenster.de>
  Key fingerprint = 6F DB 21 B4 67 EA C2 E0 E8 3D 78 28 7C 66 09 38

```

Folgende Schlüssel sind widerrufen und nicht mehr gültig; bitte markieren Sie diese Schlüssel in Ihrem Schlüsselring als ungültig (bei PGP 2 mit `pgp -kd 0x8A2097A5` usw., bei PGP 5 und 6 mit dem Kontextmenüpunkt *Disable*):

```

1024/8A2097A5 1997/06/13 Rainer Perske <perske@uni-muenster.de>
1024/17817C39 1997/09/01 Manfred Sand <sand@uni-muenster.de>
1024/D726DB95 1998/03/11 Guido Wessendorf <wessend@uni-muenster.de>
2048/914AD795 1999/03/17 Dr. Wilhelm Held <held@uni-muenster.de>
2048/4F643FF5 1999/05/26 Rita Sieber <siebert@uni-muenster.de>
2048/5F108685 1999/05/26 Dany Born <born@uni-muenster.de>

```

Die Prüfsummen der SSL-Zertifikate der zentralen WWW-Server lauten:

```

www.uni-muenster.de:
  Zentrum für Informationsverarbeitung
  Nr. 54 (0x36), gültig bis Sep 5 07:47:56 2001 GMT
  Fingerprint=59:91:5A:A4:30:81:FA:12:56:4A:8E:10:01:C1:D5:DB
user.uni-muenster.de:
  Universitätsrechenzentrum
  Nr. 16 (0x10), gültig bis Dec 17 15:48:16 2002 GMT
  Fingerprint=4F:D7:42:05:05:AA:EE:80:FF:35:C7:B4:53:09:6C:1F

```

Auf Anfrage zertifiziere ich auch WWW-Server und andere SSL-Server. Als Herausgeber wird dabei eingetragen: Rainer Perske, perske@uni-muenster.de, Universitätsrechenzentrum, Westfälische Wilhelms-Universität, Münster, Germany, DE.

Anders als bei PGP-Schlüsseln, die ich nur gegen Vorlage eines Ausweises zertifiziere, führe ich bei SSL-Servern jedoch nur eine minimale Plausibilitätskontrolle durch und halte mich an keine vorgegebene Policy. Die Ausstellung des Zertifikats hat den einzigen Zweck, den Betreibern der WWW-Server verschlüsselte Datenübertragung zu ermöglichen, ohne dass sie gleich viel Geld an irgendwelche Firmen überweisen müssen.

Wenn ein Server hier genannt wird, bedeutet dies nur, dass ich ein noch gültiges Zertifikat für den Server ausgestellt haben, jedoch nicht, dass der Server läuft oder für andere als interne Zwecke des jeweiligen Instituts verwendet wird.

```

mail.uni-muenster.de:
  Universitätsrechenzentrum
  Nr. 14 (0xe), gültig bis Dec 17 14:03:35 2002 GMT
  Fingerprint=91:73:A4:91:77:A0:CD:5A:BF:22:AD:C0:FE:5A:3D:67
user.uni-muenster.de:
  Zentrum für Informationsverarbeitung
  Nr. 24 (0x18), gültig bis Oct 3 15:37:01 2001 GMT
  Fingerprint=7D:31:D4:5A:38:10:6F:9E:4C:32:AE:42:D3:23:92:09
wwwunix.uni-muenster.de:
  Zentrum für Informationsverarbeitung
  Nr. 29 (0x1d), gültig bis Apr 29 15:02:13 2000 GMT
  Fingerprint=52:0D:67:00:1D:F7:FB:BE:1E:C5:2F:DA:B0:85:AA:2E
winkiosk.uni-muenster.de:
  Zentrum fuer Informationsverarbeitung (Rechenzentrum)
  Nr. 31 (0x1f), gültig bis May 24 13:59:23 2000 GMT
  Fingerprint=0C:6E:A3:94:F5:71:60:2F:45:B3:20:D4:04:23:C0:1B
www.wi.uni-muenster.de:
  Institut für Wirtschaftsinformatik
  Nr. 33 (0x21), gültig bis Jun 17 10:58:29 2000 GMT
  Fingerprint=0B:C8:0D:1F:24:6C:51:A3:9E:74:28:3E:2B:DB:D9:FD
pcwi003.uni-muenster.de:
  Systemadministration WI

```

Nr. 46 (0x2e), gültig bis Jun 17 11:02:22 2000 GMT  
 Fingerprint=04:75:54:CD:E8:C5:F1:8B:8F:3E:D7:16:BA:41:51:76  
 wwwzuv.uni-muenster.de:  
 ZUV - Datenverarbeitung  
 Nr. 47 (0x2f), gültig bis Jun 24 08:12:58 2000 GMT  
 Fingerprint=76:C0:0B:DA:6F:33:3F:AE:51:14:41:A3:1C:59:5C:29  
 news.uni-muenster.de:  
 Zentrum für Informationsverarbeitung  
 Nr. 48 (0x30), gültig bis Jul 1 16:04:56 2000 GMT  
 Fingerprint=CF:96:CA:3E:AE:21:C4:C4:21:FD:2D:4F:FD:FF:9A:C5  
 redenix.uni-muenster.de:  
 Zentrum für Informationsverarbeitung  
 Nr. 49 (0x31), gültig bis Jul 5 14:34:01 2000 GMT  
 Fingerprint=BA:A9:E5:C4:B7:ED:27:98:06:89:94:20:2D:EE:E8:20  
 ec.uni-muenster.de:  
 Westfaelische Wilhelms-Universitaet  
 Nr. 50 (0x32), gültig bis Aug 3 16:17:44 2000 GMT  
 Fingerprint=55:BA:5C:F6:94:BC:EE:7B:8D:89:F8:5C:CB:AC:1A:01  
 aberfix.uni-muenster.de:  
 Universitäts- und Landesbibliothek  
 Nr. 51 (0x33), gültig bis Aug 29 15:56:00 2000 GMT  
 Fingerprint=CF:17:2A:53:D9:99:08:1C:18:2C:06:95:7F:D6:E3:81  
 wwweb01.uni-muenster.de:  
 Zentrum fuer Informationsverarbeitung (Rechenzentrum)  
 Nr. 52 (0x34), gültig bis Aug 30 14:46:18 2000 GMT  
 Fingerprint=FB:52:97:3A:9F:59:5C:72:29:27:98:ED:49:0E:55:52  
 sisis-i.uni-muenster.de:  
 Universitäts- und Landesbibliothek  
 Nr. 53 (0x35), gültig bis Aug 30 15:49:34 2000 GMT  
 Fingerprint=02:2E:4F:A0:75:38:81:E9:1D:A4:E8:77:EB:67:39:FB  
 wi-2b.uni-muenster.de:  
 Institut fuer Wirtschaftsinformatik  
 Nr. 55 (0x37), gültig bis Sep 20 14:57:56 2000 GMT  
 Fingerprint=57:88:5C:B0:03:AF:05:54:41:E4:8B:6C:BE:CC:B7:47

Eine vollwertige Zertifizierungsstelle sowohl für PGP-Schlüssel als auch für SSL-Schlüssel im Rahmen der DFN-Zertifizierungshierarchie befindet sich im Aufbau.

## Änderungen beim plot-Kommando

*E. Sturm*

### Das plot-Kommando wurde vereinfacht.

Wir hatten es uns so schön gedacht: Ganz egal, ob ein Bild hochkant oder quer daher kommt, das plot-Kommando sollte es so drehen, dass es optimal aufs Papier passt. Leider ist die Welt nicht so schön, und Windows-Druckertreiber machen Fehler. Die Entwicklung gipfelte schließlich darin, dass sogar ein Parameter zur Korrektur der Treiberfehler eingeführt wurde.

Da so die Praktikabilität aber nicht gerade verbessert wurde, ist das plot-Kommando in dieser Hinsicht vereinfacht worden. Die Orientierung des Bildes wird jetzt immer als intern hochkant angenommen. Dies ist auch für Landschaftsbilder nicht abwegig: Ein Druckertreiber dreht üblicherweise von sich aus ein Bild, das auf dem Bildschirm im Querformat erscheint, intern auf hochkant, da er „weiß“, dass ein A4-Drucker immer A4 hochkant meint.

Sollte sich diese Annahme als falsch erweisen, so kann man als Orientierung "rotiert" angeben, implizit gilt „original“. Es reicht hier natürlich wieder, den Anfangsbuchstaben anzugeben. Wer die eigenständige Kommandoingabe bevorzugt, schreibt „-o r“. Die alten Angaben „-o n“ und „-b“ entfallen also.

Eine weitere Neuerung ist, dass die Angabe eines so genannten DIN-Faktors jetzt auch auf dem Xerox-Farblaserdrucker möglich ist. Als Anwendung ist z. B. denkbar, ein Bild,

das an sich das Format DIN A4 besitzt, mit dem DIN-Faktor 2 auf A3 hoch zu skalieren. Der entsprechende Kommando-Parameter lautet dann „-d 2“, also Verdoppelung.

Ein Hinweis noch, wenn Sie alles selbst in ein Kommando packen wollen: Haben Sie für die Bilddatei einen Namen vergeben, der Leerzeichen enthält, so müssen Sie diesen in Apostrophe einschließen. Bedenken Sie aber, dass der Dateiname am Ende stehen muss. Wenn Sie sich lieber in einen Dialog verwickeln lassen, erledigt das `plot`-Kommando solche Kleinigkeiten für Sie.

Eine weitere Fehlerquelle ist jetzt auch umgangen. Benutzen Sie einen HP-Druckertreiber, so erzeugt dieser standardmäßig keine gültige PostScript-Datei, sondern zusätzlich noch einen Vorspann, der einen echten HP-Drucker in den PostScript-Modus umschaltet. Man musste bisher durch Angabe von „Auftragssteuerungscode erzeugen: <Nein>“ den Vorspann abstellen. Dies braucht man jetzt nicht mehr, da die neue Version des `plot`-Kommandos den Vorspann toleriert, allerdings auf Kosten eines nunmehr nichts sagenden Dateinamens, wenn Sie die Warteschlange abfragen. Bei

```
qchk -P plot
```

für die Warteschlange des Farblaserdruckers und

```
qchk -P hp650
```

für den Posterdrucker erscheint bei einer Bilddatei mit HP-Vorspann nur ein Standardname, nicht mehr der von Ihnen verwendete.

Erläuterungen zum aktuellen `plot`-Kommando erhalten Sie bei Eingabe von

```
plot -?
```

Noch ein Hinweis: Den Farblaser- und die beiden Posterdrucker dürfen nur diejenigen benutzen, die die Rechnerlaubnis über ein Institut bekommen haben.

Zum Schluss noch eine Bemerkung zur Zukunft. Im Test ist bereits ein Programm, das es erlaubt, mit Hilfe eines WWW-Browsers (etwa Netscape) ein Bild, das auf dem eigenen Rechner vorliegt, zu betrachten und ggf. zu einem der zentralen Drucker zu schicken.

# RUM-Tutorial

## Einsatz von Smart-Karten in Betrieben, Hochschulen und Ämtern (1)

W. Bosse, W. Held, H.-W. Kisker

**Smart-Karten oder Chip-Karten sind die in Europa entwickelten und sich nun auch in den USA verbreitenden Plastikkarten, die anstelle des bisherigen Magnetstreifens einen Mikrocomputer (Chip) enthalten. Wir bringen in diesem info.rum den ersten Teil eines Übersichtsartikels.**

### Einführung

Smart-Karten sind z. B. als EC-Karten oder Telefonkarten im Einsatz. Ihre Möglichkeiten reichen aber sehr viel weiter. Der Mikrocomputer ist wie alle Computer programmierbar, Daten können abgelegt oder abgerufen werden. Verschiedene Zugriffsarten bis hin zur Sperre von Daten für Dritte können festgelegt werden. Die Verbindung zu anderen Computern wird über ein Schreib/Lesegerät (kurz: Kartenleser) hergestellt. Dabei können die Daten über Kontakte (Einschub in Leser) oder kontaktlos (Funk) fließen; Hybridkarten vereinen beide Eigenschaften in sich.

Die Smart-Karte kann außerhalb des Chips bedruckt oder mit Folien beklebt werden. Spezielle Beschichtungen (Hologramm, IUV-Belichtung) können die bedruckte Information fälschungssicherer machen. Es gibt auch Oberflächen, die gelöscht und wieder beschrieben werden können.

### Anwendungsmöglichkeiten

#### Benutzer-Identifikation beim Computerzugang (Login)

Identitätskontrollen beim Computer-Zugang finden an verschiedenen Stellen statt, dazu gehören z. B. Windows-Login, Unix-Login, Einwähl-Server-Login. Die Smart-Karte liefert für das Login eine „starke“ Authentifizierung im Gegensatz zum herkömmlichen Passwort, dessen Authentifizierung als „schwach“ zu bezeichnen ist, da das Passwort nun mittels Karte viel länger und weniger leicht zu erraten oder zu errechnen sein wird. Die Smart-Karte kann die Sicherheit der Informationsverarbeitung (IV) entscheidend erhöhen, was angesichts der zahlreichen Missbrauchsfälle und des teilweise sehr hohen Schutzbedarfs personenbezogener und medizinischer Daten und des häufig noch nicht besonders ernst genommenen Schutzbedarfs wissenschaftlicher Daten dringend notwendig ist. Diese Erhöhung der Sicherheit ist unverzichtbare Voraussetzung, wenn Betriebe sich mehr und mehr dem elektronischen Handel zuwenden, insbesondere wenn dabei die Zahl der entsprechenden Arbeitsplätze steigt und ihre Nutzung damit unübersichtlicher wird.

Dieses Login mittels Smart-Karte soll in absehbarer Zeit auf allen Rechnern – auch den häuslichen Arbeitsplätzen – der Studierenden und Bediensteten der Westfälischen Wilhelms-Universität Münster (WWU) angewendet und erzwungen werden. Zur Zeit sind das bereits etwa 32.000 Nutzer, die allein im Zentrum für Informationsverarbeitung (ZIV, früher Universitätsrechenzentrum) eine Nutzererkennung haben. Vorübergehend wird ein Parallelbetrieb des alten Login und der Passworteingabe aus dem Gedächtnis mit dem neuen Login und der Passworteingabe in verschlüsselter Form über die Smart-Karte möglich sein. Die Sicherheit der Rechnernutzung und der elektronischen Kommunikation soll damit auf ein neues Niveau gehoben werden. Die Kartenleser werden voraussichtlich in den nächsten 2 Jahren zur Standardausstattung eines jeden neuen Computers gehören.

Die Smart-Karte ist ein ganz wichtiger Teil bei der Erhöhung der IV-Sicherheit. Sie ist das erste Glied in einer langen Kette von Sicherheitsmaßnahmen, die in einer weiteren Zusammenstellung des ZIV unter dem Titel „Absicherung der IV in heterogenen Umgebungen“ beschrieben sind.

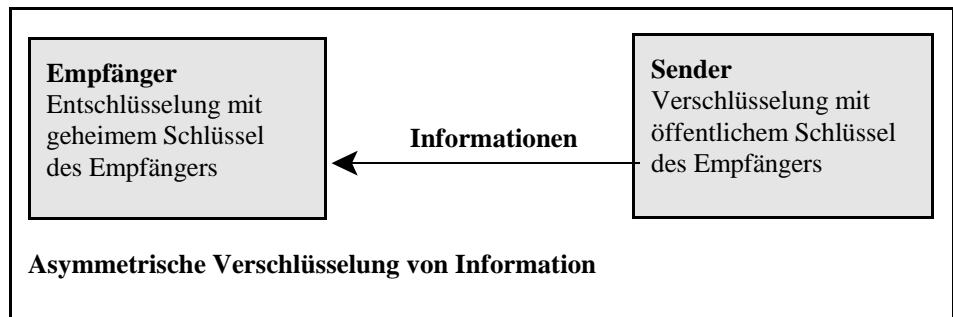
## Personalisierung, Kryptographie und Zertifizierung

### Asymmetrische Kryptographie für Daten, digitale Unterschriften und Zeitstempel

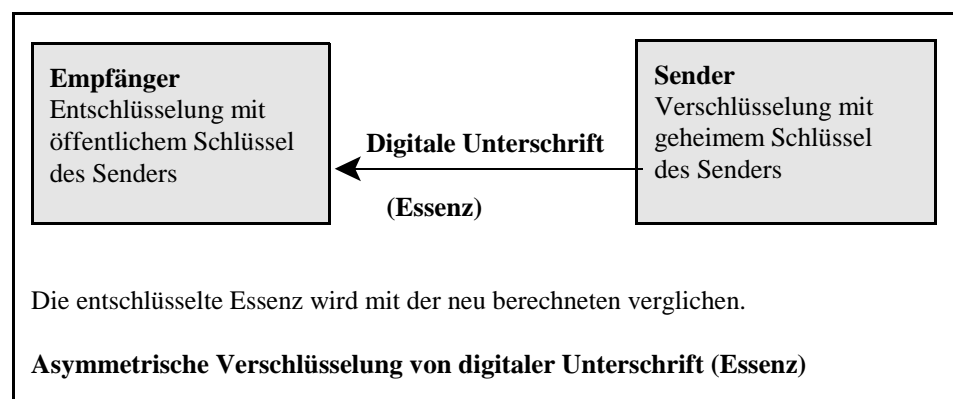
Die Verschlüsselung und Entschlüsselung von E-Mail und anderen Informationen ist ein weiteres wichtiges Mittel zur Erhöhung der IV-Sicherheit. Sie ist ebenfalls über eine Smart-Karte auslösbar. Eine besondere Rolle spielen dabei der Standard X.509 und S/MIME (und bis auf weiteres sicher auch PGP). Das X.509-Schlüsselpaar, bestehend aus privatem (geheimem) und öffentlichem Schlüssel, wird zusammen mit dem Verschlüsselungsalgorithmus auf der Smart-Karte erzeugt und abgelegt. Der private (geheime) Schlüssel verlässt die Karte nicht und ist für Dritte unerreichbar. Der öffentliche Schlüssel muss allen Interessierten verfügbar gemacht werden.

Das asymmetrische Verschlüsselungsverfahren ist u. a. aufgrund der verwendeten Algorithmen und der längeren Schlüssel sehr rechenaufwendig.

Der geheime Schlüssel des Empfängers dient in der Regel der Entschlüsselung empfangener Informationen. Der öffentliche (veröffentlichte) Schlüssel des Empfängers wird vom Absender einer Nachricht zum Verschlüsseln genutzt (nachstehende Abbildung).



Bei digitalen Unterschriften geht man etwas anders vor. Beim Erstellen einer digitalen Unterschrift spielt die Essenz (digitaler Fingerabdruck) eines Dokumentes eine wichtige Rolle. Diese wird mit sogenannten Hashfunktionen berechnet. Die Hashfunktion verdichtet den Inhalt eines Dokuments auf einen eindeutigen Wert von fester Länge. Der Algorithmus ist Sender und Empfänger bekannt. Die Berechnung ist begrenzt vergleichbar mit der Berechnung eines Parity-Bits. Entscheidend ist dabei, dass zwei verschiedene Dokumente nicht die gleiche Essenz (Hashwert) ergeben.



Aus der Essenz lässt sich der ursprüngliche Inhalt nicht rekonstruieren. Die Essenz wird mit dem geheimen Schlüssel des Senders verschlüsselt. Diese Signatur wird der Nachricht angefügt und mit ihr verschickt. Der Empfänger entschlüsselt die digitale Signatur mit dem öffentlichen Schlüssel des Inhabers, gleichzeitig berechnet er die Essenz der erhaltenen

nen Nachricht neu. Sind beide identisch, beweist dies die Echtheit des Absenders. Es wird auch garantiert, dass die Nachricht unterwegs nicht verändert wurde (vorstehende Abbildung).

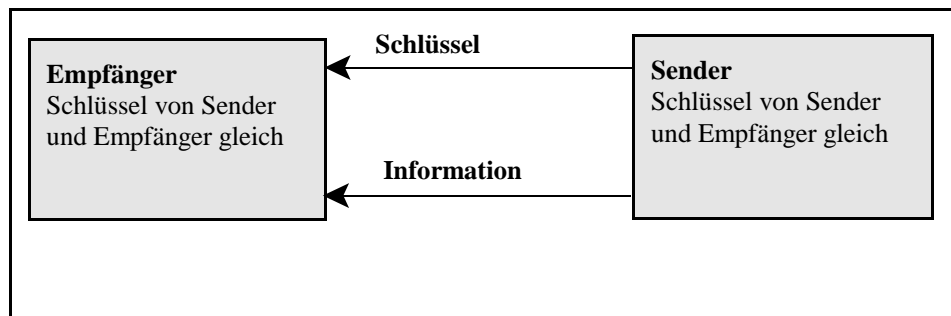
Die Sicherheit vieler Vorgänge lässt sich mit der digitalen Signatur entscheidend verbessern, sie ist der Handunterschrift deutlich überlegen. Kommt man bei digitalen Unterschriften mit etwas geringeren Randbedingungen aus, als sie im Signaturgesetz festgelegt sind, so wäre die WWU schon heute in der Lage, diese einzuführen.

Zeitangaben in einem Dokument können natürlich ohne besondere Vorkehrungen sowohl vom Absender als auch vom Empfänger nachträglich verfälscht werden, selbst wenn die Übertragung verschlüsselt erfolgte. Abhilfe schaffen zentrale, vertrauenswürdige Zeitstempeldienste, die elektronisch realisiert sind. Mit ihrer Hilfe kann man beweisen, dass ein Dokument zu einer gegebenen Zeit existiert hat. Dazu schickt man dem Zeitstempeldienst die Essenz des Dokuments, diese wird vom Zeitstempeldienst zusammen mit dem aktuellen Datum und der Uhrzeit digital unterschrieben und an den Absender zurückgeschickt, diesen Dienst können Absender und Empfänger unabhängig voneinander initiieren. Wenn alle dem Zeitstempeldienst und seinen Angaben vertrauen können, lässt sich so beweisen, dass das Dokument zu dem angegebenen Zeitpunkt existiert haben muss.

Die besondere Zertifizierung der Smart-Karte zur Nutzung der digitalen Signatur gemäß Signaturgesetz und der Zeitstempeldienste (elektronische Notariatsdienste) werden z. Z. nur von der Telekom als Zusatzdienst angeboten. Weitere Anbieter sind bald zu erwarten. Zeitstempeldienste allein werden bereits von anderen angeboten (z. B. Informatik Kooperation GmbH, das Rechenzentrum westfälisch-lippischer und hessischer Sparkassen in Münster und Offenbach).

### Symmetrische Kryptographie

Zur Verschlüsselung größerer Datenmengen benutzt man auch symmetrische Verfahren, bei denen beide Kommunikationspartner denselben Schlüssel benutzen (nachstehende Abbildung). Die Algorithmen sind einfacher. Beide Partner müssen den Schlüssel geheim halten. Problematisch ist die geheime Schlüsselabsprache.

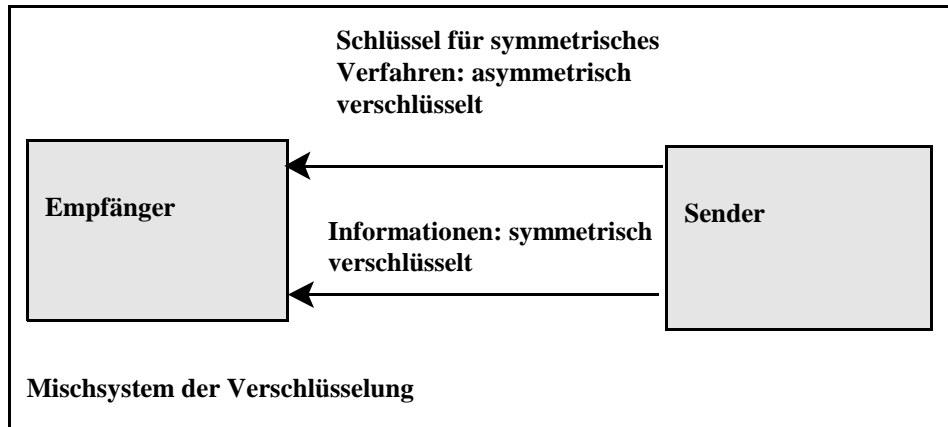


### Kryptographie als Mischform

Da das symmetrische Verfahren sehr viel schneller abläuft als das asymmetrische (z. B. ist der Faktor 1.000 ohne weiteres erreichbar), nutzt man das symmetrische Verfahren für die Verschlüsselung der Informationen, nachdem man zuvor lediglich die Schlüssel dazu mit dem asymmetrischen Verfahren ausgetauscht hat (nachstehende Abbildung).

**Variante 1:** Mit Smart-Karten lassen sich kryptographische Verfahren in der IV sehr weit treiben und dennoch sehr einfach handhaben. Sie können vielfältige kryptographische Verfahren direkt auslösen, wenn man die dazu erforderlichen Algorithmen schon auf der Smart-Karte selbst vorsieht. Dies wird in Form von Zusatzprodukten am Markt angeboten.

Dabei ist darauf zu achten, dass diese Verfahren auch beim Einsatz von Sonderprodukten über den eigenen Bereich hinaus anwendbar und nicht firmenspezifisch angelegt sind, da man sich sonst mit Externen, die diese Verfahren nicht einsetzen, schwerlich austauschen kann. Diese Verfahren erfordern in der Regel zusätzliche Investitionen, die man vermeiden kann, wenn man die in den gängigen Softwareprodukten enthaltenen Möglichkeiten, wie in Variante 2 beschrieben, ausschöpft.



**Variante 2:** Für die Verschlüsselung von E-Mails, Dateien (einschließlich Verzeichnissen) sowie WWW-Zugriffe und Telnet-Anwendungen und die Übergänge vom Arbeitsplatzrechner zu Servern und zwischen Servern bieten sich andere Sicherheitsmaßnahmen an, die in der o. a. Broschüre mit dem Titel „Absicherung der IV in heterogenen Umgebungen“ beschrieben sind. Mit der Smart-Karte wird lediglich das Login zum Arbeitsplatzrechner durchgeführt. Mit der PIN (persönliche Identifikationsnummer) des Inhabers der Smart-Karte kann dieser Vorgang zusätzlich gesichert werden.

Die Smart-Karte liefert darüber hinaus das Zertifikat (s. u.) mit dem öffentlichen Schlüssel des Inhabers und den personenbezogenen Informationen. Diese Daten können dann für die Kryptographie unter Einsatz der typischen Standardprodukte (Netscape usw.) und für den Zugang zu Anwendungen genutzt werden.

## Personalisierung und Zertifizierung

Auf der Smart-Karte sind der private Schlüssel und die PIN des Inhabers verriegelt und für Dritte nicht erreichbar. Zur Smart-Karte gehören darüber hinaus einige wenige persönliche Daten des Karteninhabers und sein öffentlicher Schlüssel. Diese Daten bilden die Personalisierungsdaten.

Die Personalisierungsstellen legen die Personalisierungsdaten fest und sie stellen die Verbindung zur zugehörigen Datenbank der Kartenverwaltung her. Als Ausstattung für Personalisierung und Zertifizierung sind notwendig, wenn man entsprechende Dienste selbst wahrnimmt: Personalisierungssysteme, Kartenverwaltungssysteme und ein Zertifizierungssystem. Diese Geräte/Software sind nicht immer im Lieferprogramm der Firmen, insbesondere dann nicht, wenn diese Firmen entsprechende Dienste, die damit möglich werden, selbst verkaufen wollen.

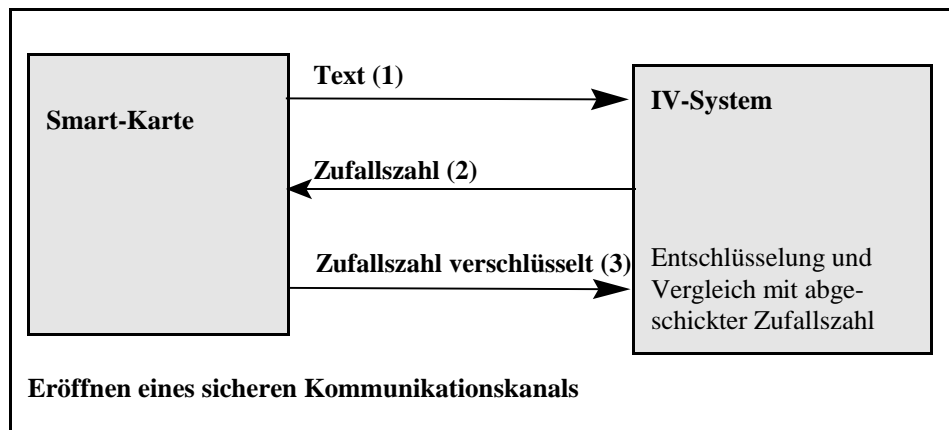
Die Personalisierungssysteme benötigt man, um die persönlichen Daten des Karteninhabers in der Smart-Karte zu speichern. Sie dienen auch dazu, alle oder einige der äußerlichen Informationen auf die Smart-Karten aufzubringen. Es werden so viele Personalisierungssysteme benötigt, dass die Personalisierungsvorgänge nicht zu Warteschlangen führen.

Kartenverwaltungssysteme stellen die Verbindung zu den Personalisierungsdaten auf der Smart-Karte und zum Karteninhaber her. Sie sind notwendig zum Erstellen, Sperren und Aktualisieren von Smart-Karten, um den Fehlbedienungszähler der Karten zurückzusetzen oder den Status aller Karten festzuhalten usw. Hier ist zu klären, was man selbst macht (z. B. die WWU) und was man als Service einkaufen will. Das sofortige Sperren der Karten kann – abhängig von den Anwendungen – u. U. bis zu 24 Stunden täglich erforderlich werden und damit einen hohen Personalaufwand erfordern, wenn dieser Dienst nicht noch von ohnehin Tätigen übernommen werden kann.

Das Zertifizierungssystem wird benötigt, um die von den Personalisierungssystemen eingeschriebenen persönlichen Daten zusammen mit dem auf der Karte erzeugten öffentlichen Schlüssel (für die Kryptographie) des Karteninhabers zu zertifizieren. Dazu werden die Personalisierungsdaten zusammen mit dem automatisch in der Smart-Karte generierten öffentlichen Schlüssel des Karteninhabers der Zertifizierungsstelle vorgelegt, welche die Daten nach festgelegten und garantiert einzuhaltenden Sicherheitsregeln zertifiziert. Wenn die Personalisierungsstellen dabei in Kooperation mit der Zertifizierungsstelle arbeiten, kann der Vorgang weitgehend automatisiert werden.

Eine derartige Zertifizierung, und das soll zur Diskussion gestellt werden, gehört aus verschiedenen Gründen in eine staatliche und vertrauenswürdige Stelle, die z. B. für Zwecke der WWU anfangs in der WWU vorgenommen werden sollte. Diese zu zertifizierenden Informationen erreichen nämlich mehr und mehr die Qualität eines Personalausweises.

Die Zertifizierungsstelle verwendet bei ihren Arbeiten ebenfalls eine asynchrone Verschlüsselung mit öffentlichem und geheimem Schlüssel.



Der öffentliche Schlüssel der Zertifizierungsstelle könnte/sollte auf allen Smart-Karten verbreitet werden, weil dies ein einfacher und störungsfreier Weg wäre. Er könnte genau so gut in der Tageszeitung verbreitet werden, wäre dann aber mühsamer zu überprüfen.

Aufgrund seiner zentralen Bedeutung muss der geheime Schlüssel der Zertifizierungsstelle besonders gesichert werden. Seine Unterbringung in einem Panzerschrank ist dabei mindestens notwendig. Eine weitere Vorsorge kann getroffen werden, wenn man dem Schlüsselpaar der Zertifizierungsstelle eine zeitlich befristete Gültigkeit gibt. In der Universität könnte z. B. mit jeder Rückmeldung ein neues Schlüsselpaar verteilt und das alte für ungültig erklärt werden.

Wenn der geheime Schlüssel der Zertifizierungsstelle trotz der Sicherungsmaßnahmen vorzeitig bekannt würde, wären aufwändige Rückrufaktionen für die ausgegebenen Smart-Karten notwendig, denn das Schlüsselpaar ist dann unverzüglich zu ersetzen und die Zertifizierung der Smart-Karten zu erneuern.

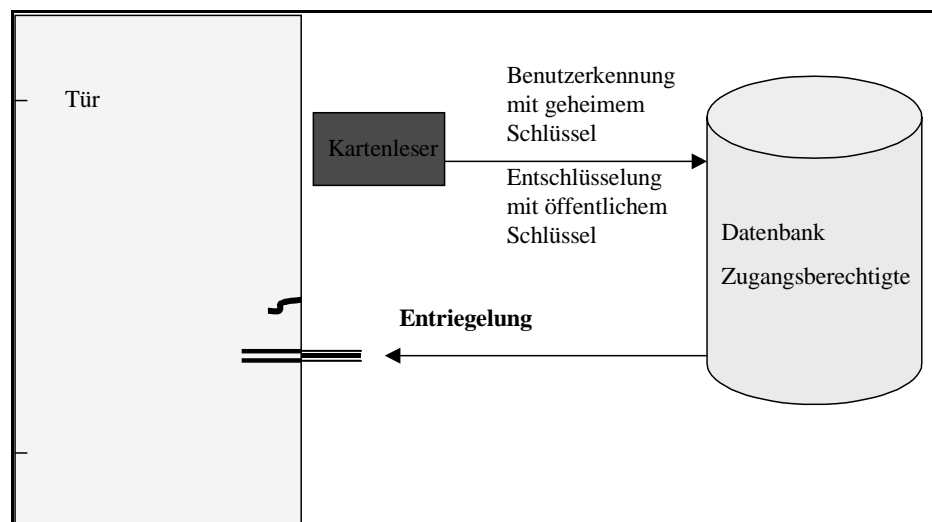
Zur Absicherung der Personalisierungs- und Kartenverwaltungssysteme wird dabei zur Absicherung i. Allg. auch ein Firewall eingesetzt. Der Firewall, in der Regel genügt schon ein Packet-Filter im LAN-Router oder -Switch, dient dem Schutz vor unerwünschten Zugriffen auf die Sicherheitsserver.

## Zugangskontrolle zu schutzbedürftigen Räumen

Der Zugang zu schutzbedürftigen Räumen oder zu Parkplätzen lässt sich mit der Smart-Karte organisieren. Der Sicherheitsstandard kann so hoch gehalten werden, dass selbst nachts oder an Wochenenden etwa der Zugang für Studierende zu Rechner-Pools auch ohne Aufsicht ermöglicht werden kann.

Für Türen und Rechner in sicherheitsrelevanten Bereichen (Universitätsverwaltung, Medizin, Systemadministration) sind weitreichende Schutzmechanismen zwingend. Die verschiedenen Schließsysteme, wenn sie mit Kartenlesern für Smart-Karten ausgestattet wären, würde man über eine Verbindung mit einer Datenbank zur Definition der Zugangsrechte zusammenführen. Die Änderung von Berechtigungen und die Kosten für die Ausgabe neuer Schlüssel (z. B. bei Verlust eines Schlüssels) wären auf leichte Weise zu verbessern. Eine generelle Ausstattung aller Räume mit einem derartigen Schließsystem scheidet aus Kostengründen allerdings aus.

Die Vorgehensweise könnte wie folgt aussehen:



## Standards und Sonstiges

Der Chip der Smart-Karte enthält einen vollständigen Rechner mit CPU, Haupt- und Hintergrundspeicher. Ein ROM<sup>1</sup> enthält das Betriebssystem und andere Tools zur Programmausführung. Ein RAM<sup>2</sup> dient als schneller Arbeitsspeicher. Und der Hintergrundspeicher ist z. B. als nicht flüchtiger EEPROM<sup>3</sup> realisiert. Er hält also die Informationen auch ohne Spannung und ist wieder zu beschreiben. Die Daten des Hintergrundspeichers sind oftmals als hierarchisches Filesystem mit vielfältigen Zugriffsrechten organisiert. In diesen Dateien werden die ausführbaren Programme und die Daten abgelegt. Programmstarts auf dem Chip erfolgen in der Regel nur nach Anstoß von außen. Dasselbe gilt für jeglichen Datentransport zwischen Chip und Rechner, auch dieser muss grundsätzlich

<sup>1</sup> ROM = Read Only Memory

<sup>2</sup> RAM = Random Access Memory

<sup>3</sup> EEPROM = Electrically Erasable Programmable Read Only Memory

vom Rechner angestoßen werden. Üblich ist dazu das als ISO/IEC-Standard 7816-3 festgelegte Kommunikationsprotokoll T=1. Der Smart-Karten-Standard ISO 7816 (genauer 7816-1,-2,-3 für physische und elektrische Eigenschaften) ist Grundvoraussetzung für den Einsatz der Smart-Karten.

Die PersonalComputer/SmartCard-Arbeitsgruppe (PC/SC) hat Standardschnittstellen zur Smart-Karte zum Zwecke der Interoperabilität zwischen Produkten verschiedener Hersteller festgelegt. Ihr gehören an: IBM, SUN, MS, Schlumberger, Bull,... . Diese Gruppe hat auch dafür gesorgt, dass die proprietären Standards EMV (Europay, MC, Visa) und GSM (Mobil-Telefonie) nutzbar sind. Es sind auch die Karten der Sparkassen-Organisation (Space Manager) und der privaten Banken (Cash Group) lesbar. PC/SC ist ursprünglich für PCs entwickelt worden. Es gibt Anzeichen dafür, dass diese Festlegungen auf Unix-Systeme ausgedehnt werden. Neben PC/SC ist auch noch mit ähnlichen Aufgaben CT-API verbreitet. Es gibt auch Software, welche die Schnittstellen PC/CS und CT-API gegenseitig abbildet, so dass sich die Wahl erst einmal nicht zwingend stellt.

Es gibt außerdem Gerätetreiber und weitergehende Bibliotheken für Anwendungsunterstützungen, wobei gesicherte und andere Operationen unterschieden werden. Microsoft unterscheidet z. B. sicherheitsrelevante APIs, andere APIs und COMs. Erste Realisierungen für Linux sind bereits verfügbar. Letztere werden auf komfortablerer Ebene zur Anwendungsprogrammierung eingesetzt und sind über C, C++, Java und VisualBasic nutzbar. Andere (z. B. Telekom) bieten entsprechende Software auf Basis von PKCS 11 (s. u.). Die Informatik Kooperation GmbH könnte die Krypto-API (C-Schnittstelle) einbringen.

Lieferanten/Hersteller der Karte liefern die File-Struktur und auf Wunsch die Inhalte auf der Smart-Karte. Die betrieblichen oder universitären Inhalte können aber auch vom Betrieb oder der WWU aufgebracht werden (vermutlich mit Ausnahme der Zahlfunktion).

Während Passwörter mit einer Länge von 40 Bits in wenigen Minuten geknackt werden können, ist das für symmetrische Schlüssel mit 128 Bits praktisch nicht möglich. PCs (i. Allg. nur Windows) lassen sogar lange asymmetrisch verschlüsselte Kennungen bis zu 2.048 Bits zu. Die entsprechende Schnittstelle für Smart-Karten ist gemäß PKCS 11 festgelegt. PKCS 11 ist der Public Key Kryptographie-Standard, oft auch als Cryptoki (Cryptographic Token Interface) bezeichnet.

Die Krypto-API in Windows 95/98/NT/2000 soll nachgewiesenermaßen Hintertüren besitzen. Daher wird von ihrer Verwendung sowie von der Nutzung digital signierter Objekte unter diesen Systemen grundsätzlich abgeraten, da die Public Keys einer bekanntermaßen mit Wirtschaftsspionage befassten US-Organisation bereits mit dem System als „vertrauenswürdig“ ausgeliefert werden.

Manche Hersteller bieten für ihre Karten Software-Updates, um nachträglich hinzukommende Funktionen leichter ergänzen zu können.

Die PIN könnte später durch ein biometrisches „Passwort“ ersetzt werden, z. B. den physischen Fingerabdruck oder Kamera-Aufnahmen der Iris.

(Fortsetzung im nächsten **inforum**)

# RUM-Lehre

## Lehrveranstaltungen im 1. Halbjahr 2000

**Lehrveranstaltungen und Kurse aus dem Bereich der Informationsverarbeitung für Hörer aller Fachbereiche.**

**Beratung zum Lehrangebot jeweils Di, Do 11-12 durch Herrn W. Bosse,  
☎ 315 61**

Nähere Angaben über den Inhalt und die Voraussetzungen der genannten Veranstaltungen werden vor Semesterbeginn vom Zentrum für Informationsverarbeitung (ZIV) bekanntgegeben

- im Internet auf den WWW-Seiten des ZIV (unter Lehre und Ausbildung),
- in der Informationsschrift **infoRUM**,
- durch Aushang in den Gebäuden Einsteinstraße 60 und Röntgenstraße 9-13.

### Veranstaltungen in der vorlesungsfreien Zeit

<b>260015</b>	Computerunterstütztes Publizieren mit LaTeX vom 14.2. bis 25.2.2000, ganztägig Hörsaal: M4, Beginn: 14.2.2000, 10 Uhr	<i>Kaspar, W.</i>
<b>260020</b>	Statistische Datenanalyse mit dem Programmsystem SPSS vom 14.2. bis 25.2.2000, vormittags Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 14.2.2000, 9 Uhr	<i>Nienhaus, R.</i>
<b>260034</b>	Kommunikation und Information im Internet vom 28.2. bis 10.3.2000, ganztägig Hörsaal: M4, Beginn: 28.2.2000, 10 Uhr	<i>Perske, R.</i>
<b>260049</b>	Publizieren im Internet mit HTML und XML vom 28.2. bis 10.3.2000, ganztägig Hörsaal: M4, Beginn: 28.2.2000, 15 Uhr	<i>Neukäter, B.</i>
<b>260053</b>	Programmieren in Java vom 13.3. bis 24.3.2000, vormittags Hörsaal: SR B Wirtschaftsinformatik, Steinfurter Str. 107 Beginn: 13.3.2000, 10 Uhr	<i>Süselbeck, B.</i>
<b>260068</b>	Betriebssystem Windows NT vom 13.3. bis 17.3.2000, ganztägig Hörsaal: M4, Beginn: 13.3.2000, 10 Uhr	<i>Kämmerer, M.</i>
<b>260072</b>	System-Administration einer Domäne in Windows NT (für Fortgeschrittene) vom 20.3. bis 24.3.2000, ganztägig Hörsaal: M4, Beginn: 20.3.2000, 10 Uhr	<i>Kämmerer, M.</i>

Für *alle* vorgenannten Veranstaltungen ist eine frühzeitige Anmeldung am Service-Schalter des Zentrums für Informationsverarbeitung im Gebäude Einsteinstraße 60 erforderlich. Die entsprechenden Listen liegen *ab 10.1.2000* aus.

## Kommentare zu den Lehrveranstaltungen

### 260015 Computerunterstütztes Publizieren mit LaTeX

LaTeX, basierend auf dem Satzsystem TeX, ist eine Sprache zur Beschreibung von Dokumenten, mit der relativ einfach wissenschaftliche Publikationen in professioneller Qualität erstellt werden können. Dem Autor werden fertige Layouts für Bücher, Reports, Artikel und anderes zur Verfügung gestellt, die er selbst in gewissen Grenzen seinen eigenen Vorstellungen leicht anpassen kann. LaTeX steht praktisch auf jedem Rechner-System zur Verfügung.

In dieser Veranstaltung wird der Einsatz von LaTeX im Publikationsprozess vorgestellt. Es wird gezeigt, wie Texte für LaTeX erfasst, mit TeX formatiert, zur Kontrolle am Bildschirm angezeigt und auf unterschiedlichen Druckern ausgegeben werden können.

Die Hörer sollten Grundkenntnisse im Umgang mit PCs besitzen.

LAMPORF: *Das LaTeX-Handbuch*, Addison-Wesley

GOOSSEN, MITTELBACH, SAMARIN: *Der LaTeX Begleiter*, Addison-Wesley

ABDELHAMID: *Das Vieweg LaTeX2e-Buch*, Vieweg

GÜNTHER: *Einführung in LaTeX2e*, dpunkt

KOPKA: *LaTeX – Band 1: Einführung*, Addison Wesley

KOPKA: *LaTeX – Band 2: Ergänzungen – mit einer Einführung in METAFONT*, Addison Wesley

PARTL/SCHLEGEL/HYNA: *LaTeX Kurzbeschreibung*

SOWA: *TeX/LaTeX und Graphik*, Springer

WONNEBERGER: *Kompaktführer LaTeX*, Addison Wesley

### 260020 Statistische Datenanalyse mit dem Programmsystem SPSS

Das statistische Programmsystem SPSS (*Statistical Package for the Social Sciences*) wird in einer aktuellen Windows-Version 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.

### 260034 Kommunikation und Information im Internet

In den letzten Jahren haben sich die internationalen Datenkommunikationsnetze – eines der wichtigsten ist das Internet – in rasantem Tempo ausgebreitet. Sie sind durch ihre Möglichkeiten zur Informationsgewinnung und zur Kommunikation ein unverzichtbares Hilfsmittel – nicht nur für Wissenschaftler.

Den Teilnehmern der Veranstaltung wird in praktischen Übungen gezeigt, wie man sich in dieser komplexen Welt zurechtfinden und sie sich zunutze machen kann. Die Teilnehmer sollten bereits wissen, wie man mit der Windows-Fensteroberfläche umgeht und welchem Zweck die DOS-Befehle `dir`, `cd`, `mkdir`, `rmdir` usw. dienen.

**260049 Publizieren im Internet mit HTML und XML**

Neben den traditionellen Medien Buch, Zeitschrift, Presse, Rundfunk und Fernsehen wird das Internet zunehmend zur Veröffentlichung wissenschaftlicher Erkenntnisse in Wort, Bild und Ton genutzt. Eine wichtige Grundlage für Veröffentlichungen im Internet ist die Hypertext Markup Language (HTML), mit deren Hilfe ein Geflecht von Texten, Bildern und anderen multimedialen Elementen im World Wide Web (WWW) dargestellt werden kann.

Die HTML steht im Mittelpunkt dieser Lehrveranstaltung, in der gezeigt werden soll, dass es keiner besonderen Rechner- oder Informatikkenntnisse bedarf, um Web-Seiten für das Internet zu gestalten. Voraussetzung für diese Veranstaltung sind lediglich Kenntnisse, wie sie etwa in der Vorlesung „Kommunikation und Information im Internet“ vermittelt werden. Hilfreich sind auch Kenntnisse der rechnergestützten Textverarbeitung, die als Hilfsmittel zur Erzeugung von HTML-Dokumenten eingesetzt werden kann.

Im zweiten Teil der Veranstaltung sollen neben der HTML weitere Auszeichnungssprachen behandelt werden. Dazu zählen MathML für mathematische Texte und XML, eine Teilmenge des ISO-Standards SGML. XML ist flexibler als HTML und deckt eine größere Klasse von Anwendungen ab.

**260053 Programmieren in Java**

Java ist eine Programmiersprache, die von SUN Microsystems direkt für das Internet entwickelt wurde. Sie erlaubt es, Anwendungen zu schreiben, die vom Benutzer über das Internet angefordert und auf seiner Maschine ausgeführt werden können, ohne dass der Entwickler die lokale Umgebung des Anwenders, wie Hardware und Betriebssystem, kennen muss.

Als objektorientierte Sprache ähnelt Java der Sprache C++, ist jedoch konzeptionell einfacher und enthält spezielle Sicherheitsfunktionen. In Java geschriebene Programme, so genannte Applets, lassen sich insbesondere zur Gestaltung von WWW-Seiten verwenden, die dynamische Elemente, also z. B. bewegte Bilder, enthalten.

Java hat sich seit einigen Jahren auf dem Markt etabliert, und es ist zu erwarten, dass es sich weiterhin dynamisch entwickelt.

**260068 Betriebssystem Windows NT**

Diese Vorlesung bietet eine Einführung in Windows-NT-Prinzipien:

- das Dateisystem NTFS,
- lokale Zugriffsrechte,
- die Benutzerverwaltung,
- Systemrichtlinien und Registry,
- Drucker- und Platten-Freigaben,
- die Netzwerkumgebung,
- Arbeitsgruppen (Win NT, Win 9x).

Windows Vorkenntnisse sind unbedingt erforderlich. Der Zugang zur Vorlesung ist frei, Übungsplätze am Nachmittag stehen nur begrenzt zur Verfügung. Für die Teilnahme an den Übungen ist eine Anmeldung erforderlich. Diese sollte per E-Mail unmittelbar beim Dozenten erfolgen: [kammere@uni-muenster.de](mailto:kammere@uni-muenster.de)

**260072 System-Administration einer Domäne in Windows NT**

Für Hörer mit Windows- und Netzwerk-Vorkenntnissen werden Arbeiten zum Aufbau einer NT-Domäne dargestellt und mit den Teilnehmern erprobt.

Die folgenden Themen werden u. a. behandelt:

- Absicherung von NT-Systemen,
- Protokolle und Netz-Konfigurationen,
- Einbindung von Win9x-Rechnern,
- effektive Userverwaltung und zentrale Konfiguration,
- Programm- und Datenablage im Netz,
- Print- und File-Service (auch in Kombination mit Unix-Systemen).

Eine Teilnahme an dieser Veranstaltung wird besonders empfohlen für Mitarbeiter in IV-Versorgungseinheiten der WWU, die mit der Administration von NT-Systemen betraut sind.

Eine Anmeldung ist erforderlich und sollte per E-Mail unmittelbar beim Dozenten erfolgen: [kammere@uni-muenster.de](mailto:kammere@uni-muenster.de)

Liebe Leserin, lieber Leser,

wenn Sie **infoforum** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von **infoforum** 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 **infoforum**



- .....
- 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:

┌  
An die  
Redaktion **infoforum**  
Zentrum für Informationsverarbeitung  
Röntgenstr. 9-13  
48149 Münster  
└

- \_\_\_\_\_
- Meine Anschrift hat sich geändert.  
Alte Anschrift:
- \_\_\_\_\_
- \_\_\_\_\_

Absender:

Name: \_\_\_\_\_

FB: \_\_\_\_\_ Institut: \_\_\_\_\_

Straße: \_\_\_\_\_

Außerhalb der Universität:

\_\_\_\_\_

*(Bitte deutlich lesbar in Druckschrift ausfüllen!)*

Ich bin damit einverstanden, dass diese Angaben in der **infoforum**-Leserdatei gespeichert werden (§ 4 DSGVO).

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift