

# inforum

---

Zentrum für Informationsverarbeitung der Universität Münster

Jahrgang 28, Nr. 1 – Februar 2004

ISSN 0931-4008

---

## Inhalt

Editorial .....	2
<b>ZIV-Aktuell</b> .....	<b>3</b>
Abschied von HP .....	3
Sicherheit in der Informationsverarbeitung .....	4
Spam-Filtern markierter E-Mails .....	4
Deleatur und SpamAssassin .....	7
Das Content Management System Imperia an der WWU .....	8
Active Directory und Linux .....	9
„uni@home plus“: Verfügbarkeit in den Region-50-Bereichen erweitert .....	10
Neues vom ZIVCLUSTER .....	11
Neue Drucker im ZIV .....	12
Alternativer Netzzugang zu den zentralen Druckern im ZIV .....	12
<b>ZIV-Tutorial</b> .....	<b>13</b>
Die Überwachung der Multimedia-Rechner im ZIV mit WMI .....	13
<b>ZIV-Lehre</b> .....	<b>21</b>
Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2004) .....	21
Veranstaltungen in der Vorlesungszeit (Sommersemester 2004) .....	22
Kommentare zu den Lehrveranstaltungen .....	22
<b>ZIV-Regularia</b> .....	<b>26</b>
Fingerprints .....	26



## Impressum

i  
ISSN 0931-4008

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

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

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

Satz: K. Hovestadt (☎ 83-31562, ✉ hovestad@uni-muenster.de)

Satzsystem: Corel WordPerfect 11 für Windows XP

Druck: Zentrum für Informationsverarbeitung  
(Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1500

## Editorial

H. Pudlatz



Spam scheint ein Dauerbrenner im i zu sein. Zwei Artikel dieser Ausgabe beschäftigen sich mit diesem ärgerlichen Thema, nachdem wir ihm schon in den letzten vier Ausgaben jeweils einen Artikel haben widmen müssen – zunächst noch zurückhaltend-abwehrend mit dem Hinweis auf das Postgeheimnis, inzwischen, nachdem viele von uns über 90 % ihrer Mail ungesehen wegwerfen dürfen, schon sehr viel ärgerlicher.

Hieß noch ein von uns empfohlenes Programm „Deleatur“ („es möge gelöscht werden“), so kommt in dieser Ausgabe ein zentraler Spamfilter zum Zuge mit dem Namen SpamAssassin, nicht einfach SpamKiller, was ja nur „Vernichter“, bestenfalls „Mörder“ bedeutet, so ist das aus dem Französischen entliehene Wort Assassin zeitgemäß als „Attentäter“ oder „Meuchelmörder“ einzudeutschen.

Wenn man jetzt aber die ganz große Feuerpatsche gegen Spam erwartet hatte, ist man zunächst etwas enttäuscht, denn hier werden Mails nur als Spam *markiert*, der Meuchelmord wird dem einzelnen Nutzer überlassen. Auch gehen noch viele Mails bei SpamAssassin durch, selbst wenn im Betreff das Wort Viagra vorkommt – Abhilfe ist jedoch versprochen.

Dennoch ist das Programm eine Hilfe: man braucht nur noch seinem Mail-Programm – soweit es dazu in der Lage ist, Outlook Express kann es nicht – eine Wegsortierregel für die als Spam markierte Mail hinzuzufügen und entledigt sich des Problems weitgehend automatisch.

Wird Deleatur – unser eigenes Programm zur Spamabwehr – dadurch überflüssig? Nein! Deleatur arbeitet sogar mit SpamAssassin zusammen. Ich benutze Delatur zusätzlich, weil es mir das Löschen von Spam schon auf dem POP-Server erlaubt und ich darüber hinaus individuelle Präferenzen angeben kann.

Schließlich benutze ich auch noch die Mail-Komponente von Netscape 7.1 (Mozilla 1.4) als dritten Spamfilter nach SpamAssassin und Deleatur. Alle bis hierher durchgelassenen Spam-Mails werden von diesem Mail-Client nach eigenen Regeln markiert und können durch einen einzigen Mausklick gelöscht werden.

Abschließend ein persönliches Wort: Seit der Nr. 2/1980 war ich Mitglied der i -Redaktion. Übermorgen ist mein letzter Arbeitstag und damit das Ende meiner Mitarbeit am i wegen Erreichens der Altersgrenze gekommen. Die Mitarbeit am i hat mir viel Freude gemacht.

Ich wünsche den Lesern von i weiterhin alles Gute.

## ZIV-Aktuell

### Abschied von HP

W. Bosse

**Wer beim Lesen des Titels zunächst an Computer und periphere Geräte denkt, der übersieht, dass auch ein Rechenzentrum in der Hauptsache von den Menschen geprägt wird, die hier arbeiten.**

Von den Anfängen des Zentrums für Informationsverarbeitung an, das damals „Rechenzentrum“ hieß, hat unser Kollege Dr. Hilmar Pudlatz das Gesicht dieser zentralen Einrichtung der Universität mit geprägt. Doch nun holt ihn, obwohl er sich weder durch Angebote zum Wechsel noch durch die „Verlockung“ auf Altersteilzeit hat beirren lassen, seine Pensionierung ein. Nach 39 Jahren verlässt er uns als jetzt dienstältester Mitarbeiter – somit ein Anlass, zurück zu schauen sowie Dank und Anerkennung auszusprechen.

Als Hilmar Pudlatz (HP) im Frühjahr 1965 seine Tätigkeit als wissenschaftlicher Mitarbeiter im Rechenzentrum aufnahm, war der Rechner Zuse Z23 in Betrieb – in Konkurrenz mit mechanischen und elektromechanischen Tischrechnern. Die in jenen Jahren noch sehr ungewöhnliche und umständliche Datenfernverarbeitung durch den Betrieb eines Terminals in Verbindung mit dem Deutschen Rechenzentrum in Darmstadt über eine Wählleitung der Post bedeutete da bereits einen Fortschritt. Im April 1967 war das heutige Dienstgebäude in der Einsteinstraße 60 fertiggestellt und der Rechner IBM /360-50 wurde dort installiert. Auf diesem sollte fortan auch die Lohn- und Gehaltsabrechnung der Universität ablaufen. Aber wie? In Zusammenarbeit mit dem Personaldezernat der Universitätsverwaltung entwarf und programmierte Herr Pudlatz diese umfangreiche und wichtige Anwendung in Rekordzeit (was selbst bei der damals festgelegten Wochenarbeitszeit von 44 Stunden auch Nacharbeit erforderte).

Schon früh wurde ihm in Arbeitsgruppen jeweils eine leitende Funktion übertragen und seit nunmehr über 18 Jahren war Herr Pudlatz Leiter der Abteilung Anwendungssysteme im ZIV. Er nahm jeweils mit großem Interesse und Engagement immer wieder aktuelle Entwicklungen auf, arbeitete sich in neue Tätigkeitsfelder ein und vergaß auch niemals unsere Nutzer, die er stets freundlich und hilfsbereit unterstützte. Im Fokus seines Interesses standen dabei die Anwendungen der Datenverarbeitung. Hier war das Rechenzentrum schon früh ein Vorreiter bei nichtnumerischen Arbeiten; auch die Zusammenarbeit mit den Fächern wurde gepflegt. Die anwendungsorientierte und auf enge Zusammenarbeit mit den Nutzern bedachte Arbeitsausrichtung von Herrn Pudlatz lässt sich besonders an Fragestellungen der grafischen Datenverarbeitung verdeutlichen, da gute Verbindungen zum Fach Geographie bestanden und er schon früh spezielle Lehrveranstaltungen wie „Fortran-Programmierung mit Plotteranwendungen für Geographen“ und „Kartographische Projektionen für Geographen“ durchführte. Sein Fachwissen war auch im Rahmen von Lehraufträgen an der Universität Gießen zu „EDV-Anwendungen in der Geographie“ gefragt. Folgerichtig widmete er sich später dann den neuen vielfältigen Multimedia-Anwendungen. Außerdem lag ihm immer die Betreuung des Blindenarbeitsplatzes der Universität am Herzen.

In der Lehre behandelte Herr Pudlatz eine Vielzahl an Themen der Informationsverarbeitung und Angewandten Informatik, wobei die Programmierung in allen gängigen Programmiersprachen einen wesentlichen Anteil hatte. Daraus entstanden auch Lehrbücher zur Einführung in das Programmieren mit PL/I (zusammen mit H. Kamp) und Modula. Der Entwicklung seines Fachgebietes entsprechend bearbeitete er die Themen praktisch von „A bis Z“ (z. B. Programmierkonzepte von Algorithmus bis Zeigerstrukturen) „und zurück“ (so benutzte er ganz unterschiedliche Rechnersysteme von Zuse bis Apple).

Über all die Jahre haben wir Herrn Pudlatz als einen fachlich kompetenten, stets freundlich und auf Ausgleich bedachten Kollegen geschätzt und auch die i -Redaktion, der er seit dem Frühjahr 1980 angehörte, lebte von seinem gewissenhaften Engagement, das auch noch (um 24 Jahre voll zu machen!) für die aktuelle Ausgabe ungebremst war.

Unseren herzlichen Dank für die geleistete Arbeit und die langjährige gute Zusammenarbeit verbinden wir mit den besten Wünschen für seinen nun beginnenden neuen Lebensabschnitt.

## Sicherheit in der Informationsverarbeitung

W. Held

Im letzten i vom Dezember 2003 hatten wir über die heftige Zunahme der Angriffe gegen die IV-Sicherheit berichtet. Insbesondere sollen deshalb nach Beschlüssen der zuständigen Gremien und des Rektorats vor allem auch für die persönlichen Arbeitsplatzcomputer Maßnahmen vorgeschlagen werden, die mögliche Schäden deutlich eindämmen.

Dazu wird an alle IV-Nutzer, die von dienstlichen, aber auch von häuslichen Arbeitsplätzen aus den Zugang zum Rechnernetz der Universität und darüber zu Servern oder zum Wissenschaftsnetz/Internet suchen, appelliert, die Maßnahmen, die derzeit erarbeitet werden, auch umzusetzen, sobald sie bekannt gegeben werden.

Die Handlungsbasis für die „Eingriffe in die Arbeitsplatzsysteme“ wird in Kürze in den Amtlichen Bekanntmachungen der Universität in „Regelungen zur IV-Sicherheit in der Universität Münster“ und in der „Benutzungsordnung des ZIV und aller IV-Versorgungseinheiten der WWU“ veröffentlicht. Die Arbeitsgruppen aus Mitgliedern der IVVen und des ZIV haben unter Mitwirkung des Sicherheitsteams der Universität ihre Arbeit aufgenommen bzw. werden dies kurzfristig tun.

Zur Vorbereitung der notwendigen Schritte werden vereinzelt auch Auskünfte von den Betreibern der Arbeitsplatzsysteme eingeholt werden müssen. Wir bitten dazu im Interesse einer zu verbessernden Sicherheit um Unterstützung.

## Spam-Filtern markierter E-Mails

R. Perske

**Aufgrund der dramatisch steigenden Anzahl unerwünschter Werbe-E-Mails, auch als Spam bezeichnet, haben wir uns nach gründlichen Tests dafür entschieden, auf allen E-Mail-Transport-Servern die Software *SpamAssassin* zu installieren.**

### Worum geht es?

Diese Software untersucht jede ankommende E-Mail auf technisch erkennbare Merkmale, die darauf hinweisen, dass es sich um eine unerwünschte Werbe-E-Mail handelt, und markiert alle auffällig gewordenen E-Mails.

**Die Markierung erfolgt ausschließlich durch Hinzufügen von Kopfzeilen (Header lines) in die E-Mail. Es werden von uns keine E-Mails gelöscht oder anders als durch Hinzufügen dieser Kopfzeilen verändert!**

Dieses reine Markieren von E-Mails ist die einzige legale Vorgehensweise, mit der wir Ihnen ermöglichen können, Spam-E-Mails sofort zu erkennen, und bei der gleichzeitig garantiert bleibt, dass keine erwünschte E-Mail verloren geht.

Mit vielen E-Mail-Programmen kann man die auf diese Weise markierten E-Mails automatisch filtern, d. h. sie in einem speziellen Ordner ablegen oder löschen. Solange Sie keine Änderungen an der Konfiguration Ihres E-Mail-Programms vornehmen, werden alle E-Mails genauso wie bisher bei Ihnen ankommen.

**Anleitungen zum Einrichten der Filter für verschiedene gängige E-Mail-Programme folgen weiter unten.**

Sofern Sie Ihre E-Mails über unseren POP3-Server `pop.uni-muenster.de` abholen, hat dieses Verfahren den kleinen Nachteil, dass Sie alle Spam-E-Mails erst herunterladen müssen, bevor Ihr Program sie filtern kann. Da Spam-Mails jedoch nur durch Ihre große Zahl, nicht jedoch durch ihr großes Datenvolumen belästigen, fällt dieser Nachteil nicht sonderlich ins Gewicht.

Falls Sie sich trotzdem dadurch gestört fühlen, haben Sie die Möglichkeit, noch vor dem Herunterladen die markierten E-Mails mit unserem Webmail-Programm `perMail` (s. u.) oder mit unserer Anti-Spam-Software `Deleatur` aus Ihrem Postfach auszusortieren und die E-Mails erst dann abzurufen.

## Wer hat uns das erlaubt?

Unsere Vorgehensweise bei Spam-Mails entspricht den Beschlüssen der IV-Kommission vom 16.06.2003 und des IV-Lenkungsausschusses vom 24.07.2003 und wurde mit der Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen abgestimmt. (Diese Abstimmung bezieht sich auch auf die Behandlung virusverseuchter E-Mails.)

## Wie sehen die Markierungen aus?

SpamAssassin bewertet jede E-Mail, verteilt dabei Spam-Punkte und fügt jeder auffälligen E-Mail zwei bis drei Kopfzeilen hinzu. Diese tragen die Feldnamen *X-Spam-Status*, *X-Spam-Level* und *X-Spam-Flag* und sehen etwa so aus wie in folgenden Beispielzeilen:

```
X-Spam-Status: Yes, hits=15.4 tagged above=3.0 required=6.3
tests=DATE_IN_FUTURE_03_06, FORGED_MUA_AOL,
FORGED_YAHOO_RCVD, FROM_NUM_AT_WEBMAIL, MISSING_MIMEOLE,
MISSING_OUTLOOK_NAME, ONLINE_PHARMACY
X-Spam-Level: *****
X-Spam-Flag: YES
```

Die obere Zeile *X-Spam-Status* wird bei allen auffälligen E-Mails eingefügt und beschreibt das genaue Untersuchungsergebnis. Die E-Mail, der dieses Beispiel entnommen wurde, wurde nach Meinung von SpamAssassin sicher als Spam erkannt (deshalb das Yes), da 15.4 Spam-Punkte erreicht wurden. Um auffällig zu werden, reichen 3.0 Spam-Punkte aus; um sicher als Spam erkannt zu werden, 6.3 Punkte. Es folgt die Liste der von SpamAssassin überprüften Spam-Kriterien, die bei dieser E-Mail zutreffen.

Die mittlere Zeile *X-Spam-Level* wird ebenfalls bei allen auffälligen E-Mails eingefügt; die Anzahl der Sternchen entspricht der gerundeten Anzahl der Spam-Punkte.

Die untere Zeile *X-Spam-Flag: YES* wird nur dann eingefügt, wenn es sich nach Meinung von SpamAssassin um eine sicher als Spam erkannte E-Mail handelt.

Eigentlich wären die beiden unteren Zeilen überflüssig, da alle Informationen bereits in der oberen Zeile enthalten sind. Jedoch vereinfachen diese Zeilen das Erstellen automatischer Filterregeln: Man lässt einfach nachschauen, ob es eine Zeile *X-Spam-Flag: YES* gibt oder ob die Zeile *X-Spam-Level* mindestens eine bestimmte Anzahl Sternchen enthält.

## Wie zuverlässig ist die Bewertung?

Gründliche Tests aller im Zeitraum vom 01.10.2003 0 Uhr bis 23.12.2003 11 Uhr beim Test-Opfer eingehenden E-Mails haben folgende Resultate geliefert. In dieser Zeit hat das Test-Opfer 18.125 Spam-E-Mails und ein- bis zweitausend normale E-Mails erhalten.

Filterkriterium	erwischte Spam-E-Mails	fälschlich erwischte echte E-Mails
X-Spam-Flag: YES	14.230 = 78,5 %	keine
X-Spam-Level: *****	14.836 = 81,9 %	1 *)
X-Spam-Level: *****	15.682 = 86,5 %	7 *)
X-Spam-Level: *****	16.411 = 90,5 %	14 *)
X-Spam-Level: ***	16.761 = 92,7 %	zu viele

\*) Die eine mit sechs Sternchen markierte Nicht-Spam-Mail enthielt als Anlage eine Spam-Mail. Alle mit fünf Sternchen markierten Nicht-Spam-Mails und die allermeisten mit vier Sternchen wurden mit Outlook 2003 verschickt, als unser SpamAssassin die von diesem Programm erzeugten Kopfzeilen noch für gefälschte Outlook-Express-Kopfzeilen hielt. Diese Ungereimtheit wurde inzwischen beseitigt.

**Natürlich besteht immer die Gefahr, dass auch eine „echte“ E-Mail eine größere Anzahl Spam-Punkte sammelt.**

Es scheint jedoch eine vernünftige Einstellung zu sein, alle E-Mails mit *X-Spam-Flag: YES* sofort wegzuworfen und alle E-Mails mit *X-Spam-Level: \*\*\*\*\** (fünf oder mehr Stern-

chen) in einen Spamverdacht-Ordner auszusortieren, dessen Inhalt man wöchentlich überfliegt und dann wegwirft.

**Natürlich kann solch ein zentraler Einheitsfilter niemals so gute Filterergebnisse erzielen wie ein individuell „trainierter“ Filter.**

Wer bereit ist, die notwendige Zeit in das Training eines individuell angepassten Filters zu investieren, der sollte sich unser *Deleatur* und/oder die trainierbaren Filter in den E-Mail-Programmen Mozilla und Eudora (Vollversion) anschauen oder auch die Programme, auf die in [email.about.com](mailto:email.about.com) verwiesen wird.

#### **Wie Sorge ich dafür, dass mein E-Mail-Programm die Spam-Mails filtert?**

Unter <http://www.uni-muenster.de/ZIV/Hinweise/SPAM/> finden Sie Hinweise, wie Sie bei verschiedenen gängigen E-Mail-Programmen die Filterung einstellen können, und zwar zzt. für:

- Unser Web-Mail-Programm perMail
- Mozilla 1.4 und Netscape Communicator 7.1
- Netscape Messenger 4.7x
- Eudora 6 (Light)
- Pegasus v4.12a
- KMail 1.5 (Linux)
- Pine 4.58
- Microsoft Outlook 2003
- Microsoft Outlook 2000 (und XP)
- Microsoft Outlook Express für Macintosh

Und was ist mit Outlook Express für Windows? Microsoft Outlook Express für Windows unterstützt keine Filter basierend auf zusätzlichen E-Mail-Kopfzeilen.

Auch auf Grund der vielen Sicherheitsprobleme und sonstigen Fehler in Microsoft Outlook Express für Windows raten wir von der Nutzung ab und empfehlen statt dessen perMail oder Mozilla zu verwenden.

## Deleatur und SpamAssassin

E. Sturm

### Deleatur und der zentrale Spammarker SpamAssassin können zusammenarbeiten.

Seit kurzem setzt das ZIV den zentralen Spammarker *SpamAssassin* ein, um spamverdächtige Mail zu kennzeichnen. Da zentrale Spammarker und persönliche Spamfilter beide Ihre Meriten haben, kann es durchaus sinnvoll sein, auch beide zu verwenden.

Ob das auch für Sie zutrifft, können Sie ausprobieren. Der vom ZIV bereitgestellte persönliche Spamfilter Deleatur kann (wie schon im [i](#) beschrieben) von ZIVsoft (<http://www.uni-muenster.de/ZIV/zivsoft>) heruntergeladen werden.

Gibt man Deleatur in der Parameterdatei `deleatur.prm` die Zeile `x=spamassassin` mit, so berücksichtigt Deleatur bei der eigenen Bewertung die Bewertung von SpamAssassin in der Weise, dass keine Mail automatisch gelöscht oder akzeptiert wird, wenn SpamAssassin gegenteiliger Auffassung ist. Deutlich wird dies an der Kennzeichnung in eckigen Klammern in der Bewertungszeile. Stehen `[]` ohne Zahlen, so ist SpamAssassin der Auffassung, dass die Mail in Ordnung ist. Anderenfalls liest man z. B. `[9.1 / 6.3]`, was zu interpretieren ist als: Diese Mail hat 9.1 Spampunkte bekommen, wobei oberhalb von 6.3 die Mail zentral als Spam definiert wurde.

Wer noch feiner granuliert auf die Sternchenwertungen von SpamAssassin reagieren möchte, kann eine entsprechende Zeile in seine Deleatur-Malus-Datei eintragen. Die Zeile

```
x-spam-level:*****
```

in der Datei `deleatur.mal` würde bewirken, dass Mail schon ab einer SpamAssassin-Bewertung von 5,0 nicht mehr automatisch von Deleatur akzeptiert würde.

```
deleatur.exe
1 =====
<<<<<: "Hiram Hedrick" <pldpolpeu@yahoo.com>
>>>>>: strohsa@uni-muenster.de
=====: She'll never stop thinking about that night with YOU
0.97 [6.7 / 6.3] ----- Mail ist SPAM!
2 =====
<<<<<: Armanda <Piperdd@personal.ro>
>>>>>: <sturm@uni-muenster.de>
=====: You have the skills and knowledge...show it
0.97 [] ----- Uorschlag: Mail sei SPAM! (?/=+)
3 =====
<<<<<: "Inger Graham" <glamating@baseball-email.com>
>>>>>: "Web GurU" <hochgar@uni-muenster.de>, "Our Friend" <floreant@uni-muen...
=====: TO: Grant Money For You glamating@baseball-email.com glamating
0.96 [3.7 / 6.3] ----- Uorschlag: Mail sei SPAM! (?/=+)
4 =====
<<<<<: Durden <durden@freechal.com>
>>>>>: Sturm <sturm@uni-muenster.de>
=====: RE[u] please, confirm jifNU
0.92 [11.1 / 6.3] ----- Mail ist SPAM!
5 =====
<<<<<: "Rebekah Goodwin" <teline@uncivilised.com>
>>>>>: studkol@uni-muenster.de
=====: what I did yesterday night
0.97 [8.9 / 6.3] ----- Mail ist SPAM!
```

## Das Content Management System Imperia an der WWU

B. Neukäter, W. Kaspar

**Nach erfolgreichem Abschluss von Pilotprojekten mit Imperia können seit Beginn dieses Jahres auf dem universitätsweiten Imperia-Hauptsystem die ersten Benutzer ihre Arbeit aufnehmen.**

Ausgehend von einer Evaluation des Institut für Wirtschaftsinformatik waren mehrere *Content Management Systeme (CMS)* von den IV-Versorgungseinheiten, dem Zentrum für Informationsverarbeitung und weiteren Universitäten aus NRW begutachtet worden. Als Ergebnis dieses Prozesses wurde das CMS Imperia von der Universität beschafft.

Dieses System kann alle Anbieter von Inhalten im World Wide Web (WWW) bei der Erfassung, Strukturierung, Darstellung und Verwaltung dieser Inhalte unterstützen. Mitarbeiter können diese Arbeiten auch ohne HTML-Kenntnisse durchführen. Außerdem besteht für alle Einrichtungen der Universität die Möglichkeit, ohne großen Entwicklungsaufwand ihre Internetseiten einem universitätsweiten Layout anzupassen.

In einem Pilotprojekt wurden zunächst die neuen Internetseiten vom „Haus der Niederlande“ online geschaltet. Inzwischen wird ein großer Teil dieses Webangebots mit Imperia gepflegt. Im Herbst 2003 veröffentlichte die Universitäts- und Landesbibliothek ihre Seiten mit Imperia im neuen Layout der Universität.

Ein Ziel dieser Projekte war unter anderem, Erfahrungen für die Einführung eines universitätsweiten, zentral gepflegten Content Management Systems zu sammeln, das nun allen Einrichtungen der Universität zur Verfügung steht, ohne dass diese sich um die Pflege, Wartung und Bereitstellung eines solchen Systems kümmern müssen.

Da auf Grund der heterogenen Organisationsstruktur und der vielfältigen Anforderungen aus allen Bereichen der Universität nicht unerhebliche Entwicklungsarbeiten für ein solches Content Management System notwendig waren, wurden diese Arbeiten parallel zu den Pilotprojekten in Zusammenarbeit mit verschiedenen Einrichtungen der Universität begonnen. Beteiligt waren unter anderem das Institut für Wirtschaftsinformatik, die Presse- und Informationsstelle der WWU und die Universitäts- und Landesbibliothek.

Zunächst musste eine flexible Gestaltung der Webseiten im Rahmen des vorgegebenen universitätsweiten Layouts ermöglicht werden. Dafür wurde ein System von Parametern eingeführt, das auch den Vorgang der Publikation steuert und den Schutz gegen unbeabsichtigte Überschreibung gewährleistet. Ebenfalls mit Hilfe dieses Systems definiert der Anwender in einfacher Weise einzelne Seitenbestandteile, die in der gleichen Form an vorgegebenen Stellen auf allen gewünschten Webseiten automatisch eingefügt werden.

Weitere Programme sorgen für automatisch erzeugte Navigationselemente auf jeder Webseite. Über leicht zu bedienende Eingabeseiten wird ihre Reihenfolge festgelegt und verändert.

Um die Eingabe der Webseiteninhalte möglichst weit den üblichen Textverarbeitungssystemen anzugleichen, wurde ein mit den Pilotanbietern abgestimmter Satz von Modulen bereitgestellt.

Da die einzelnen Informationsanbieter ihr Webangebot selbstständig verwalten sollen, mussten spezielle Mechanismen und Organisationsstrukturen geschaffen werden, die dem einzelnen Anbieter einen möglichst umfassenden Zugriff auf die „Imperia-Werkzeuge“ und seine Webseiten gestatten, ihn aber gleichzeitig vor fehlerhaften Eingaben anderer Anbieter schützen.

Darüber hinaus ermöglicht es diese Organisationsstruktur, dass ein Anbieter die Verantwortlichkeit für die Struktur seines Webangebots, für das Verfassen der Webseiten und für deren endgültige Veröffentlichung bei Bedarf verschiedenen Mitarbeitern übertragen kann. Auch die administrativen und redaktionellen Arbeiten können zwischen mehreren Personen aufgeteilt werden.

Nicht zuletzt waren, um die Benutzerverwaltung von Imperia mit der Benutzerdatenbank der WWU zu koppeln, spezielle Anpassungen in beiden Systemen notwendig. Der Zugang zu Imperia kann somit über die üblichen Formulare des ZIV für Nutzer und Nutzergruppen beantragt werden.

Auf der Grundlage dieser Erweiterungsarbeiten konnte Ende 2003 die Phase der praktischen Umsetzung beginnen. Erste Anwender sind dafür die Presse- und Informationsstelle der WWU und die IVV 1 (Geisteswissenschaften) sowie der Lehrstuhl für Wirtschaftsinformatik und Informationsmanagement und der Lehrstuhl für BWL, insbesondere Organisation, Personal und Innovation.

Ab März diesen Jahres können weitere Einrichtungen mit Imperia starten. Für die Mitarbeiter dieser Einrichtungen werden dann auch Schulungen angeboten werden, deren genaue Termine noch bekannt gegeben werden.

Bei dem Umfang einer solchen universitätsweiten Einführung von Imperia stehen wir sicherlich erst am Anfang einer längeren Entwicklungsperiode, in deren Verlauf auch weitere CMS-Funktionalitäten insbesondere für spezielle universitäre Belange bereitgestellt werden müssen.

Eine wichtige Voraussetzung für das Gelingen dieser Entwicklung ist weiterhin eine enge Zusammenarbeit mit den Informationsanbietern – vor allem mit denjenigen, die schon über größere Erfahrungen mit vergleichbaren Systemen verfügen.

## Active Directory und Linux

*O. Winkelmann*

**Seit Anfang Januar besteht die Möglichkeit eine sichere Benutzer-Authentifizierung für Linux-Systeme am Active Directory der Windows-Domäne uni-muenster.de einzurichten.**

In einer heterogenen IT-Infrastruktur stellt sich immer wieder das Problem einer gemeinsamen Nutzerdatenbank, an der sich Benutzer mit unterschiedlichen Betriebssystemen sicher authentifizieren können. Eine Schlüsselrolle zur Lösung dieses Problems nehmen immer mehr Verzeichnisdienste ein, die das Lightweight Directory Access Protokoll (LDAP) unterstützen. Schwierigkeiten aufgrund proprietärer Protokolle gehören damit der Vergangenheit an.

Mit der ULB ist ein Pilotprojekt gestartet worden, um die Benutzer-Authentifizierung an Linux-Systemen mit der vom ZIV betriebenen Windows-2003-Domäne uni-muenster.de zu koppeln. Seit Windows 2000 bietet Microsoft mit dem Verzeichnisdienst Active Directory eine LDAP-fähige Plattform an. Mittels Schemaerweiterungen können dem Active Directory weitere Klassen und Eigenschaften hinzugefügt werden, die u. a. Benutzeranmeldungen an Linux- und Unix-Maschinen ermöglichen. Unix-spezifische Attribute wie UID, GID etc. werden jetzt im Active Directory gespeichert und entsprechend konfigurierten Linux-Maschinen zur Verfügung gestellt. Auf den Linux-Systemen sorgen Open-Source-Module für die Benutzer-Authentifizierung (pam\_ldap [1] oder pam\_krb5) und das Mapping der Unix-Attribute aus dem Active Directory (nss\_ldap [1]). Die Überprüfung des Benutzerpassworts geschieht wahlweise über verschlüsseltes LDAP (LDAP over SSL: SLDAP) oder Kerberos, das Attribut-Mapping über SLDAP. Der Vorteil dieses Verfahrens liegt auf der Hand. Es findet nicht nur eine Überprüfung des Passwortes des Benutzers statt, sondern der Benutzer erhält nach dem Anmeldeprozess eine Umgebung, in der seine Rechte aufgrund seiner Gruppenmitgliedschaften bekannt sind. Einen Schönheitsfehler hat das System allerdings (noch): Zurzeit wird nur die Information über die Hauptgruppe des Benutzers an das Linux-System weitergegeben. Alle weiteren Gruppenzugehörigkeiten stehen quasi nicht zur Verfügung.

Hier besteht die Möglichkeit im Bedarfsfall spezielle Windows-Gruppen einzurichten, die komplett auf dem Linux-System sichtbar sind, allerdings nur ca. 800 Benutzerkennungen enthalten können. Diese Beschränkung beruht auf einer Speicherlimitierung eines Datenfeldes im Active Directory.

Die unter Linux verfügbaren Windows-Kennungen und Gruppen in der Domäne uni-muenster.de findet man in zwei Organisationseinheiten. Die LDAP-Pfade für die verfügbaren Kennungen (und Gruppen) mit dem nss\_ldap-Modul lauten:

```
ou=Projekt-Benutzer,dc=uni-muenster,dc=de
ou=Projekt-Gruppen,dc=uni-muenster,dc=de
```

Mehrmals am Tag findet eine Synchronisation der dort gespeicherten Daten mit der zentralen Nutzerdatenbank des ZIV statt. Für weitere Informationen wenden Sie sich bitte an Oliver Winkelmann, © 31618.

Literatur:

[1] <http://www.padl.com/Contents/OpenSourceSoftware.html>  
<http://www.padl.com/Contents/Documentation.html>

## „uni@home plus“: Verfügbarkeit in den Region-50-Bereichen erweitert

M. Speer

**Die Zahl der Region-50-Bereiche, in denen der Internet-Einwahldienst „uni@home plus“ verfügbar ist, wurde deutlich erweitert.**

Im Januar 2004 wurde die Zahl der Ortsnetzbereiche der Deutschen Telekom, in denen der Internet-Einwahldienst „uni@home plus“ genutzt werden kann, erheblich erweitert. Es wurden 27 zusätzliche Region-50-Bereiche freigeschaltet. Insgesamt ist „uni@home plus“ nun im gesamten Tarifbereich Münster City für 0,91 Cent/Min. und 33 Region-50-Bereichen für 1,54 Cent/Min. rund um die Uhr verfügbar. Die folgende Tabelle listet die nun abgedeckten Region 50-Bereiche auf:

- |                                |                        |
|--------------------------------|------------------------|
| ● 2303 Unna                    | ● 2572 Emsdetten       |
| ● 2306 Lünen                   | ● 2581 Warendorf       |
| ● 2361 Recklinghausen          | ● 2584 Warendorf-Milte |
| ● 2364 Haltern                 | ● 2591 Lüdinghausen    |
| ● 2381 Hamm                    | ● 2592 Selm            |
| ● 2389 Werne                   | ● 2594 Dülmen          |
| ● 2521 Beckum                  | ● 541 Osnabrück        |
| ● 2543 Billerbeck Westf.       | ● 5451 Ibbenbüren      |
| ● 2546 Coesfeld-Lette          | ● 5459 Hörstel         |
| ● 2551 Steinfurt-Burgsteinfurt | ● 5481 Lengerich       |
| ● 2552 Steinfurt-Borghorst     | ● 5482 Tecklenburg     |
| ● 2553 Ochtrup                 | ● 5923 Schüttorf       |
| ● 2554 Laer                    | ● 5971 Rheine          |
| ● 2555 Schöppingen             | ● 5973 Neuenkirchen    |
| ● 2556 Metelen                 | ● 5975 Rheine-Mesum    |
| ● 2558 Horstmar                | ● 5976 Salzbergen      |
| ● 2562 Gronau                  |                        |

Tabelle 1: Von „uni@home plus“ abgedeckte Region-50-Bereiche

Der Vollständigkeit halber sind in der folgenden Tabelle noch einmal sämtliche Ortsnetzbereiche des von „uni@home plus“ komplett abgedeckten Tarifbereichs Münster City aufgelistet:

- |                            |                                |
|----------------------------|--------------------------------|
| ● 251 Münster              | ● 2534 Münster-Roxel           |
| ● 2501 Münster-Hiltrup     | ● 2535 Sendenhorst-Albersloh   |
| ● 2502 Nottuln             | ● 2536 Münster-Albachten       |
| ● 2504 Telgte              | ● 2538 Drensteinfurt-Rinkerode |
| ● 2505 Altenberge Westf.   | ● 2571 Greven Westf.           |
| ● 2506 Münster-Wolbeck     | ● 2573 Nordwalde               |
| ● 2507 Havixbeck           | ● 2575 Greven-Reckenfeld       |
| ● 2508 Drensteinfurt       | ● 2582 Everswinkel             |
| ● 2509 Nottuln-Appelhülsen | ● 2593 Ascheberg Westf.        |
| ● 2526 Sendenhorst         | ● 2597 Senden Westf.           |
| ● 2532 Ostbevern           | ● 2598 Senden-Ottmarsbocholt   |
| ● 2533 Münster-Nienberge   |                                |

Tabelle 2: Von „uni@home plus“ komplett abgedeckter Tarifbereich Münster City

Weitere ausführliche Informationen findet man auf der „uni@home plus“-Homepage [www.uni-muenster.de/ZIV/unihomeplus](http://www.uni-muenster.de/ZIV/unihomeplus).

## Neues vom ZIVCLUSTER

M. Leweling

### Geänderte Konfiguration der Warteschlangen auf dem Linux-Parallelrechner

Wer schon einmal versucht hat, auf dem Linux-Parallelrechner eine größere Anzahl von Rechnerknoten anzufordern, wird bemerkt haben, dass bisher meistens unzumutbare Wartezeiten auftraten – falls der Rechenjob überhaupt jemals an die Reihe kam. Seit dem 28. Januar sorgt nun eine Batch-Queue mit reservierbarer Rechenzeit auf dem ZIVCLUSTER dafür, dass jeder Rechenjob mit einer endlichen und zumutbaren Wartezeit abgearbeitet werden kann. Zu diesem Zweck wurde eine Queue `dedicatedq` eingeführt mit folgenden Eigenschaften:

- Die Anzahl der insgesamt zur Verfügung gestellten Knoten beträgt 92 (`resources_available.ncpus = 92`).
- Die Anzahl der Knoten, die pro Job angefordert werden können, beträgt 92 (`resources_max.ncpus = 92`).
- Die maximale Rechenzeit pro Job beträgt 30 Minuten (`walltime = 0:30:00`).

Der Clou dieser Warteschlange besteht darin, dass sie vom Benutzer selbst aktiviert werden kann. Sobald der erste Benutzer einen Rechenjob in diese Queue abschickt, wird die angeforderte Rechenzeit für eine Woche später reserviert. Beispiel: Benutzer A schickt am 5.2. den ersten Job mit der Angabe `walltime=0:20:00` in die `dedicatedq`-Warteschlange, dann werden ihm unter zusätzlicher Berücksichtigung von 20 Prozent Reserve 24 Minuten Rechenzeit am 12.2. eingeräumt. Die reservierte Zeit wird nach einigen Minuten (die Überprüfung der Warteschlangen findet alle 10 Minuten statt) auf der Status-Webseite <http://zivcluster.uni-muenster.de/cgi-bin/qview> angezeigt.

Eine wichtige Eigenschaft der `dedicatedq`-Queue besteht in der Bündelung von reservierten Rechenzeiten. Liegt der Startzeitpunkt einer Reservierung einmal fest, werden alle bis zu diesem Zeitpunkt eingehenden Jobs in der Queue zusammengefasst und der reservierte Zeitraum entsprechend verlängert, bis zu einer Maximaldauer von 8 Stunden. Für unser genanntes Beispiel bedeutet das:

Benutzer B schickt am 7.2. einen weiteren Job mit `walltime=0:10:00` in die Warteschlange, dann wird der reservierte Zeitraum am 12.2. von 24 auf 36 Minuten erweitert. Selbst Rechenjobs, die noch während des reservierten Zeitraums abgeschickt werden, finden hierbei Berücksichtigung. Sobald allerdings dieser Zeitraum einmal abgelaufen ist, muss man wieder eine Woche auf die nächste Reservierung warten.

Durch die Bündelung der Zeitreservierung wird gewährleistet, dass weiterhin Langzeit-Queues auf dem Cluster abgearbeitet werden können und dass kein Batch-Job vorzeitig abgebrochen werden muss. Da die `dedicatedq` exklusiv läuft, kann nämlich kein Job einer anderen Queue in die Zeitreservierung hineinlaufen. Als Benutzer der Langzeit-Queues erfordert das natürlich etwas mehr Flexibilität: Will man unbedingt noch vor der nächsten Zeitreservierung rechnen, muss man unter Umständen die `walltime`-Anforderung des eigenen Jobs mit `qalter` herunterschrauben.

Ein praktischer Nebeneffekt dieser exklusiven Nutzung liegt darin, dass jeweils vor Beginn und nach Ende der Zeitreservierung alle Rechnerknoten frei werden, also spätestens nach dem Ablauf der Zeitreservierung automatisch die ältesten Rechenjobs an die Reihe kommen, selbst wenn sie bisher aufgrund hoher Ressourcen-Anforderungen kein Zeitfenster zur Ausführung fanden. Folglich kann nun für jeden Batch-Job eine endliche Wartezeit garantiert werden.

Natürlich funktioniert die automatische Reservierung mit einwöchiger Wartezeit nur, wenn die längste Queue in das Zeitfenster zwischen zwei Reservierungen passt. Daher wurde die maximale Rechenzeit der bisherigen Langzeit-Queue (`bigq`) von 14 Tagen auf 160 Stunden verkürzt, also etwas weniger als 7 Tage.

Zum Schluss noch ein Tipp für die Praxis: in der Regel wird der Cluster ab etwa einen Tag vor der Zeitreservierung allmählich entleert, so dass Kurzzeit-Nutzer schon hier eine gute Gelegenheit erhalten, eine größere Anzahl von Rechnerknoten zu bekommen. Man muss also meistens nicht bis zum Beginn der `dedicated time` warten, um Kurzzeit-Jobs auf vielen Knoten zu rechnen, und sollte diese Gelegenheit im Hinblick auf eine möglichst hohe Auslastung des Clusters auch nutzen.

## Neue Drucker im ZIV

J. Hölters

**Das Jahr 2003 hat eine Reihe von Neuerungen im Druckbereich gebracht. Die Verbesserungen und Veränderungen werden hier dargestellt.**

Im Bereich Farblaserdrucker wurde der Drucker vom Typ HP Color LaserJet 8550 GN durch zwei leistungsfähigere Drucker vom Typ HP Color LaserJet 9500 HDN ersetzt. Zum einen gibt es jetzt Redundanz, so dass bei Störung eines Druckers immer noch Ausgaben möglich sind, wenn auch mit verminderter Kapazität, zum anderen vermag jeder der neuen Drucker bis zu 24 Seiten pro Minute vollfarbig zu drucken und bietet damit die bis zu 4-fache Leistung. Die Namen der Druckerwarteschlangen haben sich nicht geändert, jedoch sind auf dem Windows-Server `zivprint.wwu.uni-muenster.de` die Treiber an die neuen Drucker angepasst.

Im Bereich Großformatdruck ist ein neuer Drucker vom Typ Epson Stylus Pro 10000CF hinzugekommen, der auch Fotoqualität-Ausdrucke im Format A0 und knapp darüber ermöglicht. Für Nutzer des Windows-Server `zivprint.wwu.uni-muenster.de` steht dieser Drucker durch die Warteschlange `ep10000` zur Verfügung. Für Nutzer des Web-Dienstes ZIVprint ist der Drucker noch nicht nutzbar, da die nativen Druckauftragsdaten für diesen Drucker im Bereich 1 GByte pro Seite liegen. Ein *Software RIP* für PostScript wird gerade erprobt, um das Datenvolumen in handhabbaren Größen zu halten. Als Druckmaterial steht zur Zeit „Premium Glossy Photo Paper“ in einer Breite von 36 Zoll zur Verfügung. Im Gegensatz zu den Ausdrucken auf den bisherigen HP Großformatdruckern sind die Drucke des Epsondruckers lichtbeständiger.

Ein Ausfall eines alten Druck-Servers hat im Dezember 2003 für einen abrupten Umstieg auf die neuen Druck-Server gesorgt, der dann leider etwas holperig ausgefallen ist, so dass einzelne Druckerwarteschlangen auf dem neuen Druck-Server nicht eingesehen werden können und daher der Verbleib von Druckaufträgen manchmal etwas unübersichtlich ist. Hier wird es allerdings in Kürze Besserung geben, so dass über den Web-Dienst ZIVprint wieder alle Daten verfügbar sind.

## Alternativer Netzzugang zu den zentralen Druckern im ZIV

W. Lange

**Als Alternative zum manchmal schwer handhabbaren LAN-Zugang stehen die Windows-Warteschlangen für die zentral bereitgestellten Drucker auf dem Server `zivprint.uni-muenster.de` (ZIVPRINT) jetzt – zunächst im Testbetrieb – auch per IPP zur Verfügung.**

IPP (*Internet Printing Protocol*) ermöglicht das Versenden von Druckaufträgen per HTTP. Damit entfällt die Notwendigkeit, einen „Clienten für Microsoft-Netzwerke“ zu installieren. Das spart Ressourcen und trägt zur Verbesserung der Sicherheit bei. Vor allem für Benutzer von Rechnern, die nicht in einer Windows-Domäne betrieben werden (z. B. per DFÜ-Verbindung angebundene häusliche Arbeitsplatzrechner), vereinfacht sich der Netzwerkdruckerzugang ganz erheblich.

Auf Windows-XP-Rechnern wird Internet-Printing über den „Druckerinstallations-Assistenten“ über die Option „Verbindung mit einem Drucker im Internet oder Heim-/Firmennetzwerk herstellen“ unterstützt. Anders als in dem dort angezeigten Beispiel **muss** für den Zugang zum Server ZIVPRINT **https** anstelle von **http** verwendet werden. Damit wird eine verschlüsselte Datenübertragung bewirkt und vor allem das Versenden von Klartext-Passwörtern vermieden.

Die anzugebene URL hat die Form `https://zivprint.uni-muenster.de/printers/<name_des_druckers>/printer`. Dabei ist anstelle von `<name_des_druckers>` die gewünschte Druckerwarteschlange (z. B. `ein-ps`) anzugeben. Die Liste der verfügbaren Druckerwarteschlangen kann mit jedem Internet-Browser über die URL `https://zivprint.uni-muenster.de/printers` eingesehen werden.

Nach Angabe der URL wird zur Eingabe einer gültigen Benutzerkennung mit Passwort aufgefordert. Dies sind Kennungen der Windows-Domäne `uni-muenster.de`. Sie werden automatisch „freigeschaltet“, wenn entsprechend den Empfehlungen des ZIV eine „Änderung des zentralen Standardpassworts“ durchgeführt wird. Bei Bedarf ist dazu die Webseite `http://user.uni-muenster.de/index.html#passwoorte` aufzurufen.

Weitere Einzelheiten werden bekannt gemacht, sobald genügend Erfahrungen mit einem größeren Nutzerkreis vorliegen. Erfahrungsberichte sind daher ausdrücklich willkommen

(Dr. W. Lange, ✉ `lange@uni-muenster.de`, © (83) 31655).

## ZIV-Tutorial

### Die Überwachung der Multimedia-Rechner im ZIV mit WMI oder: Was Sie schon immer über Ihren PC wissen wollten ...

H.-W. Kisker

Das ZIV bereitet zurzeit die Bereitstellung von so genannten Multimedia-Rechnern vor. Über diese Rechner steht allen Universitätsangehörigen bei Bedarf eine Reihe hochwertiger Geräte für Multimedia-Anwendungen zur Verfügung. Da die Rechner und Geräte unbeaufsichtigt genutzt werden können, wird ein Überwachungssystem erforderlich, das die Vollständigkeit der Geräte überwacht. Zu diesem Zweck wurde im ZIV eine softwarebasierende Überwachungslösung auf Basis von WMI entwickelt.

Der *Windows Management Instrumentation Service (WMI)* ist ein Windows-Betriebssystemdienst, der den Zugriff auf umfangreiche Informationen über die Ablaufumgebung eines Rechners bietet und deren Manipulation gestattet. Ein WMI verwendender Benutzer oder Administrator befindet sich bezüglich seiner Informationsbasis (fast) auf gleicher Augenhöhe mit dem Betriebssystem. Das ist die gute Nachricht. Die schlechte ist, dass WMI, gepaart mit leichtfertigem Umgang, ein **erhebliches Gefährdungspotenzial** beinhaltet.

Dieser Artikel beschreibt das am ZIV eingeführte System zur Überwachung der Multimedia-Rechner. Dabei skizziert er die Nutzung von WMI und geht auf die damit verbundenen Probleme ein.

#### Die Problemstellung

Im ZIV wird zurzeit eine neue Multimedia-Infrastruktur aufgebaut. Ziel ist es, den Angehörigen der Universität eine Reihe von hochwertigen Geräten wie z. B. Flachbett-Scanner mit Mehrfacheinzug oder Dia-Scanner für handelsübliche Magazine usw. bereitzustellen. Die Geräte sind in besonderen Räumen untergebracht, die auch eine angemessene Arbeitsumgebung bieten. Zu diesen kann jeder Universitätsangehörige bei Bedarf Zugang erhalten, um diese Geräte zu nutzen. Da die Tätigkeit in den Räumen nicht überwacht werden kann und soll, ist nach Abschluss der Arbeiten eine Überprüfung der vorhandenen Geräte auf Vollständigkeit durch einen Mitarbeiter des ZIV vorgesehen. Eine Inaugenscheinnahme des Raums erscheint dabei nur bedingt wirkungsvoll, da zum einen manche Unstimmigkeiten nicht direkt ins Auge fallen und zum anderen nicht jeder Mitarbeiter über die genaue Ausstattung der Geräte informiert ist. Deshalb haben wir ein Hilfsmittel entwickelt, das die Vollständigkeit der Geräteausstattung über das Netz zuverlässig überprüft und in einer leicht zu überblickenden Form anzeigt. Der Betriebssystemdienst WMI des Windows-Betriebssystems stellt einen vollständigen Satz von Informationen über die Ablaufumgebung eines Rechners zur Verfügung. So war es naheliegend, hier eine auf WMI basierende Lösung zu realisieren. Der Artikel beginnt mit einer Skizze des WMI-Dienstes und konkretisiert im zweiten Teil den Nutzen von WMI durch die Vorstellung der Überwachungslösung am ZIV. Derjenige, der weniger an Systemkomponenten interessiert ist, sei ermuntert, beim Lesen mit dem zweiten Teil zu beginnen.

Anmerkung: Die Multimedia-Räume werden im Laufe des Monats März nacheinander in Betrieb genommen. Die Einzelheiten werden im Web bekannt gegeben.

#### Der Betriebssystemdienst WMI

Die Windows-Betriebssysteme erhalten Informationen über ihre Ablaufumgebung durch einen auf jedem Rechner vorhandenen Betriebssystemdienst mit Namen: *Windows Management Instrumentation Service (WMI)*. Die darüber erreichbare Datensammlung enthält den vollständigen Satz von Informationen über jede vorhandene Hardware-Komponente und über jede installierte Software-Komponente. Anders ausgedrückt: Geräte oder Software-Produkte, die hier nicht eingetragen sind, existieren für das Betriebssystem nicht.

WMI wurde mit dem Service Pack 4 von Windows NT freigegeben und ist heute für alle Betriebssysteme ab Windows 95 verfügbar. Die aktuellen Betriebssystemversionen enthalten es standardgemäß. Alle folgenden Ausführungen und Beispiele beziehen sich ausschließlich auf Windows XP Professional.

Die Schnittstellen zu dem Dienst sind offen gelegt und stehen Anwendungsprogrammen und Benutzern zur Verfügung. Auch der externe Zugriff über das Netz ist implementiert. Insgesamt ist WMI ein mächtiges Werkzeug, dessen Nutzung verblüffend simpel ist, das aber bei leichtfertigem Umgang ein **beängstigendes Gefahrenpotential** in sich birgt.

#### Der Zugang zum WMI-Dienst

Üblicherweise wird der Zugang zu WMI über einen von drei Wegen realisiert:

- über das Kommando-Interface (Aufruf des Kommandozeilenprogramms WMIC.EXE),

- über ein VisualBasic-Skript oder
- über das Programm-Interface (Namensraum **SYSTEM.MANAGEMENT**).

Typisch ist dabei der Zugang über ein Skript. Die Einschätzung, dass WMI so ein Skript-Kram für Administratoren sei, ist weit verbreitet. Dieser Artikel enthält jedoch vor allen Beispiele für das Kommando-Interface.

Um die gewaltige Datenflut zu kanalisieren, kapselt WMI alle Informationen zu den von ihm verwalteten Komponenten in einer Klasse. Alle möglichen Klassen sind auf jedem Rechner in einer Datenbank (WMI Repository) abgelegt. Es gibt Prozessor-Klassen, Monitor-Klassen, Maus-Klassen, Drucker-Klassen usw. usw. Mit Hilfe dieser Klassen werden für den konkreten Rechner Objekte erzeugt (Instanzierung), die jeweils eine reale Komponente beschreiben. Das größte Problem, das sich mit WMI aus meiner Sicht ergibt, ist es, einen Überblick zu gewinnen. Der Zugriff und auch die Programmierung sind sehr unkompliziert, arten aber leicht in Fleißarbeit aus. Als kleine Hilfestellung ist am Ende des Artikels eine kurze Literatur- und Download-Liste angefügt.

Wie jede ordentliche Klasse verfügen auch die WMI-Klassen über Eigenschaften, Methoden und Ereignisse. Die Eigenschaften beschreiben die Informationen, die über WMI abgefragt werden können (z. B. Taktfrequenz des Prozessors), die Methoden sind Programmstücke, die die zugehörige Komponente manipulieren (z. B. Setzen der Lüfterumdrehung), und Ereignisse gestatten es, Aktionen in Abhängigkeit von bestimmten Vorkommnissen anzustoßen (z. B. Senden einer Mail bei Start eines bestimmten Programms).

Wie bereits angedeutet, ist die Nutzung von WMI verblüffend einfach. Sie möchten alles über den in Ihrem Rechner werkenden Prozessor wissen? Windows XP bietet hierfür das kommandoorientierte Programm WMIC.EXE an. Starten Sie über **START** → **RUN** → **WMIC** dieses Programm und geben Sie die Anweisung **CPU GET /VALUE** ein. Auf meinem Dienst-Notebook erhalte ich dadurch folgendes hier aus Platzgründen zweispaltig wiedergegebenes Ergebnis:

wmic:root\cli>CPU get /VALUE	LoadPercentage=0
AddressWidth=32	Manufacturer=GenuineIntel
Architecture=0	MaxClockSpeed=1000
Availability=3	Name=Intel(R) Pentium(R) M processor 1000MHz
Caption=x86 Family 6 Model 9 Stepping 5	OtherFamilyDescription=
ConfigManagerErrorCode=	PNPDeviceID=
ConfigManagerUserConfig=	PowerManagementSupported=FALSE
CpuStatus=1	ProcessorId=A7E9F9BF00000695
CreationClassName=Win32_Processor	ProcessorType=3
CurrentClockSpeed=1000	Revision=2309
CurrentVoltage=33	Role=CPU
DataWidth=32	SocketDesignation=U1
Description=x86 Family 6 Model 9 Stepping 5	Status=OK
DeviceID=CPU0	StatusInfo=3
ErrorCleared=	Stepping=5
ErrorDescription=	SystemCreationClassName=Win32_ComputerSystem
ExtClock=	SystemName=HWKONTOUR
Family=2	UniqueId=
InstallDate=	UpgradeMethod=8
L2CacheSize=1024	Version=Modell 9, Stepping 5
L2CacheSpeed=	VoltageCaps=2
LastErrorCode=	
Level=6	

(Auf eine Erläuterung der einzelnen Angaben sei hier verzichtet. Eine gut nutzbare Erläuterung ist z. B. in [1] enthalten.)

In der benutzten Anweisung **CPU GET /VALUE** steht **CPU** für die zu untersuchende Klasse, **GET** bezeichnet die gewünschte Aufgabe und der Term **/VALUE** bestimmt das Format der Ausgabe. Neben **GET** zur Informationsgewinnung gibt es auch noch **SET** zur Wertveränderung und **CALL** zum Aufruf von Methoden.

Der wirkliche Name der oben verwendeten Prozessorklasse ist **Win32\_Processor**. Der Name **CPU** ist ein nur innerhalb von **WMIC** gültiger Alias für diese Klasse. Welche Alias-Namen insgesamt in **WMIC** definiert sind, erhält man durch den Befehl **/?**. Leider gibt es längst nicht für alle Klassen Alias-Namen in **WMIC**. Insbesondere fehlen auch

einige durchaus interessante Klassen, wie z.B. **Win32\_PnPEntity**, über die man Zugriff auf die Fülle der Plug-and-Play-Komponenten erhält.

Möchte man solche Klassen mit WMIC abfragen, so ist dem Klassennamen der Term **PATH** voranzustellen. Die Anweisung **PATH Win32\_PnPEntity get /Value** liefert also Informationen über alle verfügbaren PnP-Komponenten. Diese Abfrage grenzt aber bereits an eine Art Informations-Overkill. Auf meinem Arbeits-PC wird hierdurch ein Report von 5525 Zeilen generiert.

Möchten Sie dennoch noch mehr sehen? Dann probieren Sie doch die Klassen (kleine Auswahl, mehr in [1]):

**BIOS, DesktopMonitor, DiskDrive, LogicalDisk, MemPhysical, NIC, NICConfig, OnboardDevice, OS, Process, Registry, Service, SystemSlot, Temperature, Voltage.**

Das Ergebnis einer Anweisung kann auch über eine **FORMAT**-Option als HTML-Report in besser lesbarer Form ausgegeben werden. Natürlich sollte die HTML-Seite dann zwischengespeichert werden. Die Anweisung

```
/OUTPUT:"C:\wmi.htm" CSProduct get /format:hform
```

erzeugt die unten angezeigte HTML-Seite **wmi.htm**.

<b>Knoten: HWKonTour TravelMate C110.</b>	
Eigenschaftename	Wert
Caption	Computersystemprodukt.
Description	Computersystemprodukt.
IdentifyingNumber	LXT270E067341010A6M000 .
Name	TravelMate C110.
SKUNumber	.
UUID	401478E4-D0FE-D711-A6FE-A2E34BB155A1.
Vendor	Acer .
Version	-1 .

Als Anmerkung sei angefügt, dass die im obigen Report dargestellte Klasse **CSProduct** für Zwecke der Rechner-Inventarisierung gedacht ist.

Die Informationen, die eine Anweisung an WMI liefert, können, wie wir bei den PnP-Komponenten gesehen haben, von einem schwer handhabbaren Umfang sein. Schon ein Abfragen aller laufenden Prozesse oder aller Betriebssystemdienste ergibt eine unübersichtlich lange Liste. Völlig unerträglich wird der Umgang eines Administrators mit allen Instanzen der Benutzerklasse. In der Active-Directory-Domäne `uni-muenster.de` müssen hier immerhin 20.000 Benutzer behandelt werden. Hier ist es unbedingt erforderlich, Abfragen auf die Benutzer zu beschränken, die in dem gerade anliegenden Problem eine Rolle spielen. Hierzu bietet WMI eine Abfragemöglichkeit, die an SQL angelehnt ist. Mit der Anweisung

```
UserAccount WHERE status!="Ok" GET Name
```

werden z. B. alle gesperrten Konten aufgelistet.

Alle diese Informationen können auch extern über das Netz abgefragt werden. Programmsysteme wie SMS oder MOM nutzen genau diese Möglichkeit. Ein Ausspionieren meines Notebooks von meinem Arbeitsplatzrechner aus ist mit dem Befehl

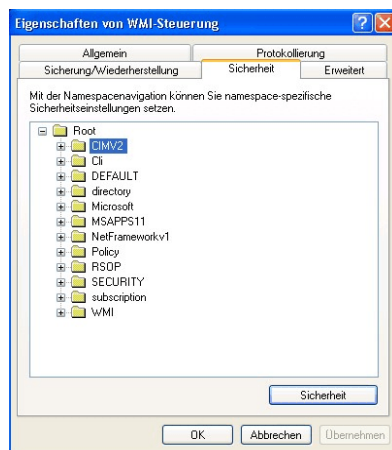
```
/NODE:HWKonTour Process get /value
```

möglich. Er liefert eine lange Liste aller gerade laufenden Prozesse und gibt bedenklicher-

weise damit auch Auskunft über meine aktuellen Aktivitäten. Wenn man noch bedenkt, dass so auch Methoden über das Netz ausgeführt werden können, wobei ein Shutdown noch als harmlos einzustufen ist, so bekommt die Bemerkung, dass der leichtfertige Umgang mit WMI ein beängstigendes Gefahrenpotenzial in sich birgt, schärfere Konturen. Um dieses Gefahrenpotenzial handhaben zu können, gibt es natürlich Absicherungsmöglichkeiten.

## Sicherheit

Die innerhalb von WMI definierten Klassen sind baumförmig organisiert. Dieser Baum wird als Eigenschaften der WMI-Steuerung in der Computerverwaltung unter *Sicherheit* angezeigt. Wie Sie sehen, hat der WMI-Baum mehrere Zweige. Auch ist es möglich, den Baum zu erweitern, insbesondere im Zuge von Treiberinstallationen können weitere gerätespezifische Klassen hinzugefügt werden. Auch die Installation des *Internet Information Servers* bringt eigene Klassen mit. Alle Klassen, die in diesem Artikel bisher genutzt wurden, sind im Zweig **ROOT\CIMV2** zu finden. Für jeden dieser Zweige können die Zugriffsrechte der Benutzer getrennt festgelegt werden. Die Standardeinstellungen sind so, dass der normale Benutzer zwar lokalen Zugriff auf WMI hat, dass jedweder externe Zugriff aber gesperrt ist. Benutzer der Gruppe Administratoren haben Vollzugriff. In vielen Fällen wird es sinnvoll sein, den Zugriff auf WMI nur bestimmten Benutzern und nicht jedem zu gestatten.



Zusätzlich kann der externe Zugriff auf WMI noch durch die Installation eines Firewalls (z. B. ICF = *Internet Connection Firewall*) blockiert werden. Der externe Zugriff auf WMI erfolgt über die RPC-Schnittstelle (*Remote Procedure Call*). Dies ist eine allgemeine Schnittstelle, die für die unterschiedlichsten Kommunikationsaufgaben genutzt werden kann. Der Start einer RPC-Verbindung erfolgt stets über Port 135 und hat die Vereinbarung weiterer Ports für die eigentliche Kommunikation zur Folge. Der ICF verhindert den Aufbau einer RPC-Verbindung zuverlässig. Will man trotz des Firewalls extern auf WMI zugreifen, muss der Port 135 und ein weiterer selbst festlegbarer Bereich freigegeben werden. Das Loch, das damit in den Firewall gebohrt wird, ist also schon ziemlich groß.

**Zusammenfassend ist beim Einsatz von WMI die Installation eines Firewalls und die Einschränkung der Benutzerzugriffe dringend anzuraten.**

## Das System zur Überwachung der Multimedia-Rechner im ZIV

### Konzeptionelle Überlegungen

Grundvoraussetzung für eine softwarebasierende Lösung zur Sicherung der Rechner war natürlich die Lösung eines unvermeidlichen technischen Sekundärproblems im Vorfeld. Die Rechner und Peripheriegeräte dürfen nicht ausgeschaltet werden, da sonst natürlich keine softwarebasierende Überprüfung möglich ist. Alle Geräte sind also entsprechend manipuliert. Sie hängen an einem Stromversorgungsweig, der nur von dazu autorisierten ZIV-Mitarbeitern z. B. abends mit einem über das Netz bedienbaren elektronischen Schalter abgeschaltet werden kann.

Von der Aufgabenstellung her ist keine dauernde Überwachung der Multimedia-Rechner gefordert, sondern nur eine Überprüfung der Vollständigkeit der Ausstattung am Ende der Arbeiten des jeweiligen Benutzers. Bei der Realisierung sollten folgende Punkte beachtet werden:

1. Die Sicherheit der Multimediarechner darf nicht beeinträchtigt werden.
2. Um unnötige Wege der mit der Überprüfung betrauten Mitarbeiter zu vermeiden, muss die Überprüfung über das Netz möglich sein.
3. Jeder Arbeitsplatzrechner der Mitarbeiter soll für die Überprüfung genutzt werden können.
4. Der Installationsaufwand soll insbesondere bei den zur Überwachung genutzten Arbeitsplätzen gering sein.

5. Die Mitarbeiter müssen die Überprüfung durchführen können, auch wenn sie über die Ausstattung der Multimedia-Rechner nicht unterrichtet sind.
6. Das Ergebnis der Überprüfung, also die Vollständigkeit der Geräteausstattung, muss mit einem Blick zweifelsfrei erkennbar sein.

Die nahe liegende Lösung, WMIC auf dem Mitarbeiterrechner zu nutzen, um zu sehen, welche Komponenten auf dem Multimedia-Rechner noch vorhanden sind, wurde von vorne herein ausgeschlossen. Die Punkte 5 und 6 waren hiermit nicht zu erfüllen.

Generell suchten wir auch nach einer Lösung, die ohne die Öffnung des Firewalls für RPC-Verbindungen auskommt. Nun gibt es zumindest in der Windows-Welt eine Tendenz, Firewall-Einschränkungen zu umgehen, indem Dienste über Port 80 (HTTP) abgewickelt werden. Natürlich bringt diese Vorgehensweise neue Sicherheitsprobleme mit sich und rückt Filter für den Port-80-Datenverkehr ins Blickfeld. Auch wir haben uns aber für diesen Weg entschieden, da der Datenverkehr über Port 80, wenn er streng reglementiert und stark eingeschränkt wird, zuverlässig zu überwachen ist.

Für jeden zu überwachenden Rechner muss festgelegt werden, welche Komponenten für ihn überprüft werden sollen. Dies läuft auf einen rechner-spezifischen Satz von WMI-Abfragen hinaus, deren positive oder negative Beantwortung über das Ergebnis der Überprüfung entscheidet. Dieser Satz von Abfragen wird von den die Multimedia-Rechner konzipierenden Mitarbeitern festgelegt und als ein so genanntes Profil auf dem jeweiligen Rechner abgelegt. Hierfür müssen handhabbare Hilfsmittel bereitstehen.

Insgesamt erfüllt das im Folgenden beschriebene Überwachungssystem alle obigen Forderungen.

## Die Struktur des Überwachungssystems

### 1. Der zu überprüfende Rechner

Auf jedem zu überprüfenden Rechner wird ein stark eingeschränkter Web-Server installiert. Er verfügt nur über eine durch eine Web-Anwendung realisierte dynamisch gebildete Standardseite. Sie gibt zu jedem Zeitpunkt das Ergebnis einer Überprüfung wieder. Egal mit welcher URL der Rechner angesprochen wird, es wird immer diese eine Seite zurückgegeben. Auf dem Rechner ist neben der Standardseite auch das Überwachungsprofil abgelegt. Gemäß dem Inhalt dieses Profils wird die Rückgabeseite gebildet.

Zurzeit kann diese Überprüfung von jedem angefordert werden. Die in der HTML-Seite enthaltenen Daten sind in keiner Weise schützenswert. Bei Bedarf kann der Zugriff natürlich in der üblichen Weise abgesichert werden.

### 2. Der zur Überprüfung genutzte Rechner

An den zur Überprüfung genutzten Rechner des Mitarbeiters werden keine weiteren Anforderungen gestellt.

### 3. Das Überwachungsprofil

Das Überwachungsprofil enthält eine Liste von WMI-Abfragen für jede zu überwachende Komponente. Jede dieser Abfragen erzeugt bei Vorhandensein der Komponente eine typische Zeilenfolge. Alle Antworten zu einer Komponente werden zu einer Soll-Zeichenkette zusammengefügt und ebenfalls im Profil abgelegt. Das Profil für mein Notebook enthält etwa für den Prozessor folgenden Sollwert:

CPU (1 processor; x86 Family 6 Model 9 Stepping 5; speed: 1000 MHz)

### 4. Die Überprüfung

Bei der Überprüfung werden alle im Profil enthaltenen WMI-Anfragen dem System noch einmal gestellt und deren Antworten hintereinander gefügt. Die so entstandene Zeichenkette wird mit dem Sollwert aus dem Profil verglichen. Bei Übereinstimmung wird in die Web-Seite eine Zeile mit positiver Markierung aufgenommen. Gibt es eine Unstimmigkeit, wird die entsprechende Zeile deutlich mit einer Fehlermarkierung versehen. Die Überschrift der Seite enthält eine Zusammenfassung aller Überprüfungen.

### Die Überprüfung im Web-Browser

Um einen Rechner zu überprüfen, wird von ihm eine beliebige HTML-Seite angefordert, z.B. durch

<http://HWKonTour.laer.de/Beliebige Seite.htm> (mein Notebook).

Der zu überprüfende Rechner benötigt einige Zeit zum Aufbereiten der Seite. Danach erscheint die Seite:

The screenshot shows the HWKONTOUR interface with the following components listed:

- Alle Komponenten sind vorhanden!** (All components are available!)
- CPU (1 processor; x86 Family 6 Model 9 Stepping 5; speed: 1000 MHz)
- Speicher (512 MB)
- Platte (IC25N040ATMR04-0; 37GByte)
- Netzwerkkarte (Intel(R) PRO/100 VE Network Connection; 00:0A:E4:03:32:CB)
- Device (Digital-Flachbildschirm (1024x768))
- Device (Acer Tablet PC Keyboard Buttons (101/102 Key))
- Device (Microsoft USB Wheel Mouse Optical)

© 2003 Hans-Werner Kisker - Zentrum für Informationsverarbeitung

Die grüne Überschrift zeigt an, dass der Rechner vollständig ist. Wenn man die Maus abzieht und den Rechner noch einmal überprüft, erhält man die Seite:

The screenshot shows the HWKONTOUR interface with the following components listed:

- 1 Komponente fehlt!** (1 component missing!)
- CPU (1 processor; x86 Family 6 Model 9 Stepping 5; speed: 1000 MHz)
- Speicher (512 MB)
- Platte (IC25N040ATMR04-0; 37GByte)
- Netzwerkkarte (Intel(R) PRO/100 VE Network Connection; 00:0A:E4:03:32:CB)
- Device (Digital-Flachbildschirm (1024x768))
- Device (Acer Tablet PC Keyboard Buttons (101/102 Key))
- Device (Microsoft USB Wheel Mouse Optical)  
(Sollwert: ---- nicht vorhanden ----)

© 2003 Hans-Werner Kisker - Zentrum für Informationsverarbeitung

Die rote Überschrift warnt vor einer unvollständigen Ausstattung. Das rote STOP-Schild zeigt an, welche Komponente fehlt.

## Die Zusammenstellung eines Profils

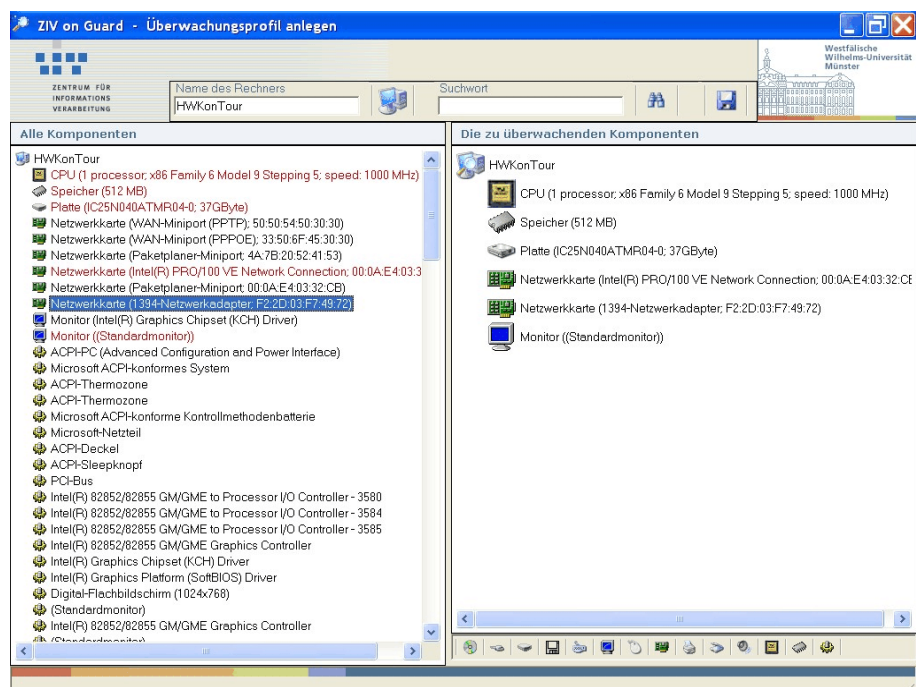
Zur Zusammenstellung eines Profils dient das am ZIV entwickelte Programm ZoGprofil.exe (ZoG = ZIV on Guard). Es ist ein dotnet-Programm, das ausschließlich Komponenten des dotnet-Frameworks benutzt. Das dotnet-Framework ist so etwas wie die aktuelle Version des Betriebssysteminterfaces und ersetzt das gute alte Win32-Interface. Dotnet-Programme sind auf alle Rechner, auf denen das dotnet-Framework installiert ist, durch kopieren zu „installieren“. Dies wird als *xcopy deployment* bezeichnet und ist keineswegs neu, sondern ein ganz alter Hut aus Vor-Windows-Zeiten.

Das Programm erzeugt die angezeigten Informationen zu jeder Komponente durch entsprechende Unterprogramme. Das folgende Fragment zeigt beispielhaft das Unterprogramm für die Prozessor-Klasse:

(Fehlerbehandlung wurde entfernt!)

```
Imports System
Imports System.Management
. . .
Public Function CPU(ByVal v As String) As String
    Dim mClass As New ManagementClass("Win32_processor")
    Dim mCollection As System.Management.ManagementObjectCollection
    Dim CurrentCpu As ManagementObjectCollection.ManagementObjectEnumerator
    Dim mObject As ManagementObject
    Dim Solltext As String = ""
    mCollection = mClass.GetInstances()
    CurrentCPU = mCollection.GetEnumerator()
    CurrentCPU.MoveNext()
    mObject = CType(CurrentCPU.Current, ManagementObject)
    Solltext = "CPU ("
    If mCollection.Count > 1 Then
        Solltext = Solltext & mCollection.Count & " processors; "
    Else
        Solltext = Solltext & "1 processor; "
    End If
    Solltext = Solltext & mObject("Description").ToString & "; "
    Solltext = Solltext & "speed:" & mObject("MaxClockSpeed").ToString & " MHz)"
    CPU = Solltext
End Function
. . .
```

Ruft man das Programm auf und trägt einen Rechnernamen ein (hier HWKonTour), so erhält man die folgende Ansicht:



Links sind alle auf dem Rechner überwachbaren Komponenten aufgezählt. Hieraus kann man Komponenten zur Überwachung auswählen. Diese werden links rot markiert und rechts in die Liste eingetragen. Mit dem Knopf rechts oben in der Ecke werden alle für die Überprüfung erforderlichen Informationen in einer Textdatei mit dem Standardnamen `<Rechnername>-Profile.txt` abgelegt. Diese Datei kann von der Web-Anwendung direkt für die Überprüfung genutzt werden.

## Grenzen und Ausblick

Nicht alle Komponenten sind ohne weiteres auf Vorhandensein mit WMI überprüfbar. Z. B. ist an dem Rechner für die Video-Bearbeitung über eine SVHS-Schnittstelle ein Video-Recorder angeschlossen. Dessen Vorhandensein kann nur dann überprüft werden, wenn die Treiber zu der Video-Grabber-Karte entsprechende WMI-Informationen liefern.

Der Gedanke liegt nahe, WMI auch für eine dauernde Diebstahlsicherung einzusetzen. Immerhin bietet selbst WMIC die Möglichkeit, einen Wert dauernd abzufragen. Z. B. gibt die Anweisung

```
temperature get /EVERY:2
```

alle 2 Sekunden den Temperaturwert des Prozessors aus. Außerdem könnte und müsste so ein System natürlich durch von WMI erzeugte Ereignisse gesteuert werden. Das große Problem, das aber zu lösen ist, ist der Neustart eines Rechners. Stromabschalten, Diebstahl und Neustart sind nicht zu unterscheiden. Sollte dieser Zustand handhabbar werden, so wäre eine auf WMI basierende Diebstahlsicherung eine elegante und kostengünstige Lösung.

## Referenzen

- [1] Tobias Werter, Windows-Verwaltung mit WMI, Microsoft Press, 2003, ISBN 3-86063-598-0
- [2] Dirk Primes, Schweizer Taschenmesser für Entwickler, DOTNET PRO, Heft 11/2003
- [3] WMI Dokumentation,  
[http://msdn.microsoft.com/library/en-us/wmisdk/wmi\\_start.asp](http://msdn.microsoft.com/library/en-us/wmisdk/wmi_start.asp)
- [4] Download: Aktuelle Skript-Version; <http://www.microsoft.com/scripting>
- [5] Download: WMI Tools, Dokumente, SDK,  
<http://msdn.microsoft.com/downloads/list/wmi.asp>

# ZIV-Lehre

## Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2004) für Hörer aller Fachbereiche

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

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse <http://www.uni-muenster.de/ZIV/Content-Lehre.html> unter „Anmelden zu den Veranstaltungen“ erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldeöglichkeit zu den Veranstaltungen besteht seit dem 5. Januar 2004.

<b>260016</b>	Publizieren im Internet mit XML Blockveranstaltung vom 22.3. bis 2.4.2004 Mo-Fr 10-12, 14-16 Hörsaal: ZIV-Pool 3, Einsteinstr. 60	Neukäter, B.
<b>260020</b>	Publizieren mit LaTeX Blockveranstaltung vom 1.3. bis 12.3.2004 Mo-Fr 9-11, 15-17 Hörsaal: M4, Einsteinstr. 64 (vormittags), ZIV-Pool 3, Einsteinstr. 60 (nachmittags)	Kaspar, W.
<b>260150</b>	Programmieren in Fortran Blockveranstaltung vom 15.3. bis 26.3.2004 Mo-Fr 8-10 Hörsaal: ZIV-Pool 2, Einsteinstr. 60	Reichel, K.
<b>260035</b>	Programmieren in Java Blockveranstaltung vom 15.3. bis 26.3.2004 Mo-Fr 9-11 Hörsaal: M4, Einsteinstr. 64	Süselbeck, B.
<b>260040</b>	Statistische Datenanalyse mit dem Programmsystem SPSS Blockveranstaltung vom 9.2. bis 20.2.2004 Mo-Fr 9-11 Hörsaal: ZIV-Pool 3, Einsteinstr. 60	Zörkendörfer, S.
<b>260054</b>	Betriebssystem Linux/Unix: Einführung und Grundlagen Blockveranstaltung vom 24.2. bis 5.3.2004 Mo-Fr 10-16 (Beginn dienstags!) Hörsaal: ZIV-Pool 3, Einsteinstr. 60	Grote, M.
<b>260069</b>	Einführung in die Benutzung des Parallelrechners Blockveranstaltung vom 13.4. bis 16.4.2004 Di-Fr 9-12 Hörsaal: Raum 206, Röntgenstr. 9-13	Leweling, M.
<b>260073</b>	Systemadministration für Linux-Systeme Blockveranstaltung vom 15.3. bis 19.3.2004 Mo-Fr 9-16 Hörsaal: ZIV-Pool 3, Einsteinstr. 60	Hölters, J.
<b>260088</b>	Systemadministration für Windows-Systeme Blockveranstaltung vom 22.3. bis 26.3.2004 Mo-Fr 9-16 Hörsaal: Raum 206, Röntgenstr. 9-13	Lange, W. Winkelmann, O.

## Veranstaltungen in der Vorlesungszeit (Sommersemester 2004) für Hörer aller Fachbereiche

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

Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse <http://www.uni-muenster.de/ZIV/Content-Lehre.html> unter „Anmelden zu den Veranstaltungen“ erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind ab 15. März 2004 möglich.

<b>260092</b>	Erstellen dynamischer Webseiten mit PHP Mittwoch 9-11 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 28.04.2004	Sturm, E.
<b>260107</b>	Objektorientiertes Programmieren in C++ Mittwoch 15-17 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 28.04.2004	Mersch, R.
<b>260111</b>	Statistische Datenanalyse mit dem Programmsystem SPSS Donnerstag 11-13 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 29.04.2004	Nienhaus, R.
<b>260126</b>	Windows-Betriebssysteme: Einführung und Grundlagen Mittwoch 14-18 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 28.04.2004	Kämmerer, M.
<b>260130</b>	Rechnernetze und Internet: Fortgeschrittene Themen Donnerstag 10-12 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13, Beginn: 29.04.2004	Richter, G./ Forsmann, A./ Kamp, M./ Speer, M./ Wessendorf, G.
<b>260164</b>	Sicherheit in der Informationsverarbeitung (vorrangig für Systemadministratoren und Technisch Verantwortliche) Mittwoch 10-12 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13, Beginn: 28.04.2004	Richter, G./ Ost, St./ Müller-Böhm, Ch./ N. N.
<b>260145</b>	Kolloquium des Zentrums für Informationsverarbeitung Freitag 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13	Held, W.

## Kommentare zu den Lehrveranstaltungen

### **260016 Publizieren im Internet mit XML**

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

Voraussetzung für diese Veranstaltung sind grundlegende Kenntnisse der Kommunikation und Information im Internet.

### **260020 Publizieren mit LaTeX**

LaTeX ist ein mächtiges und flexibles Satzsystem, das sich besonders für wissenschaftliche und technische Publikationen eignet. Autoren können aus einer Vielzahl von fertigen Layouts auswählen und diese eigenen Vorstellungen anpassen. Mit speziellen Komponenten, z. B. zur Erzeugung von PDF-Dateien, können LaTeX-Publikationen für die Veröffentlichung auf CD-ROM oder im Internet vorbereitet werden. Das komplette Satzsystem ist frei erhältlich und steht praktisch auf allen verbreiteten Betriebssystemen zur Verfügung.

In dieser Veranstaltung werden die Grundkonzepte und wichtigsten Erweiterungen von LaTeX vorgestellt, u. a.

- die Komponenten des Satzsystems,
- allgemeine Dokument- und Textstrukturen,
- Formeln, Tabellen, Grafiken und
- die Erzeugung von PDF-Dokumenten,

und wie hiermit ordentlich strukturierte und typografisch ansprechende Dokumente erstellt werden können.

Voraussetzung für diese Veranstaltung sind Grundkenntnisse im Umgang mit PCs.

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

ABDELHAMID: *Das Vieweg LaTeX2e-Buch*, Vieweg

DETIG: *Der LaTeX Wegweiser*, Thomson

NIEDERMAIR: *LaTeX – Das Praxisbuch*, Franzis

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

KLÖCKL: *LaTeX2e: Tips und Tricks*, dpunkt

### 260150 Programmieren in Fortran

Fortran ist eine weit verbreitete Programmiersprache, die insbesondere für die Programmierung naturwissenschaftlicher und technischer Anwendungen eingesetzt wird.

In dieser Vorlesung sollen die Hörer lernen, wie Programme systematisch konstruiert werden. Gleichzeitig wird ihnen zunächst der Fortran-77-Standard, anschließend darauf aufbauend der Fortran-90-Standard vermittelt. Es werden keine Programmierkenntnisse vorausgesetzt. Praktische Übungen sind Teil der Veranstaltung.

BRAUER: *Programmieren in Fortran 77*, Müthig

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

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

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

### 260035 Programmieren in Java

Java ist eine objektorientierte Programmiersprache, die inzwischen weltweit große Verbreitung gefunden hat und sich weiterhin dynamisch entwickelt.

Sie basiert auf dem Konzept einer virtuellen Maschine, die es ermöglicht, Anwendungen für unterschiedliche Plattformen ohne Neuübersetzung zu entwickeln, und verfügt über eine sehr umfangreiche Klassenbibliothek, die ständig erweitert wird. Grundkenntnisse in Java sind für die Softwareentwicklung in vielen Bereichen unbedingt erforderlich.

Die Vorlesung bietet eine Einführung in die objektorientierte Programmierung anhand von Java. Sie ist auch für Hörer ohne Vorkenntnisse im Programmieren geeignet.

### 260040, 260111 Statistische Datenanalyse mit dem Programmsystem SPSS

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

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

### 260054 Betriebssystem Linux/Unix: Einführung und Grundlagen

Linux ist ein leistungsstarkes Unix-System für viele Hardware-Architekturen. Als preiswerte Windows-Alternative ist es augenblicklich in aller Munde.

Die Vorlesung will in die Linux-Benutzung einführen. Sie besteht aus zwei Teilen. Zuerst erfolgt eine an üblichen Unix-Einführungen orientierte Beschreibung des Unix-Dateisystems und der wesentlichen Unix-Befehle. Anschließend wird die grafische Oberfläche KDE behandelt, die für viele ein Linux-System erst attraktiv macht.

**260069 Einführung in die Benutzung des Parallelrechners**

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

Die Hörer sollten grundlegende Kenntnisse der Programmiersprache Fortran besitzen.

**260073 Systemadministration für Linux-Systeme**

Die Vorlesung richtet sich an fortgeschrittene Linux-Anwender, die Unterstützung bei der Installation und System-Integration von Linux-Systemen benötigen. Voraussetzung sind grundlegende Kenntnisse der Unix-Kommandos und der Shell-Script-Sprache.

Die Teilnehmer werden in der Veranstaltung ein Linux-System selbst installieren und in die Netzwerk- und Systeminfrastruktur der Universität einbinden. Ferner wird demonstriert, wie man einen speziell auf die Hardware-Ausstattung des Rechners optimierten Kernel generiert.

**260088 Systemadministration für Windows-Server**

Die Veranstaltung richtet sich an fortgeschrittene Windows-Benutzer, die ihre Kenntnisse mit Blick auf die Anforderungen in einem großen Rechnernetz erweitern möchten. Als Schwerpunkte sind u. a. der Aufbau und Betrieb von Servern im Windows-Netzwerk (Active Directory) vorgesehen.

Themenauswahl:

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

Im Rahmen der Veranstaltung wird auch Gelegenheit zu praktischen Übungen gegeben.

**260092 Erstellen dynamischer Webseiten mit PHP**

Viele Internet-Provider bieten ihren Kunden inzwischen an, eigene Webseiten mit Hilfe von PHP dynamisch zu gestalten.

PHP ist eine Programmiersprache, deren Befehle in HTML-Seiten eingebettet werden und die darüber hinaus eine Vielzahl von Unterprogramm-bibliotheken mitbringt, etwa für Datenbankzugriffe, E-Mail-Verschicken und vieles mehr.

Beispiel für eine PHP-Anwendung ist ZIVprint, das Programm, mit dem man Druckdateien vorher anschauen und dann zu einem der zentralen Drucker des Zentrums für Informationsverarbeitung (ZIV) leiten kann.

In dieser Veranstaltung sollen sowohl die Elemente der Sprache als auch konkrete Projekte wie ZIVprint und ZIVlehre vorgestellt werden. Dabei wird als Datenbank MySQL näher betrachtet. Programmierkenntnisse (die Sprache ist egal) sollten vorhanden sein.

**260107 Objektorientiertes Programmieren in C++**

Objektorientierte Programmierung wird einerseits als wichtiger Schritt in Richtung ingenieurmäßige Software-Erstellung gesehen, andererseits ist sie das „natürliche“ Programmier-Paradigma für einige Klassen von Anwendungen, wie z. B. grafische Oberflächen und Simulationen.

In dieser Lehrveranstaltung werden die Prinzipien der objektorientierten Programmierung vorgestellt und mit Hilfe der Programmiersprache C++ demonstriert. C++, eine Erweiterung der Programmiersprache C um objektorientierte Elemente, wurde Ende 1997 von ANSI und ISO standardisiert. Implementierungen der Sprache gibt es praktisch für alle Betriebssysteme und Rechnertypen.

In der Lehrveranstaltung werden die Programmiersprache und Teile der Standardbibliothek gemäß ISO/ANSI-Standard vorgestellt. Sie ist als weiterführende Veranstaltung konzipiert; Grundkenntnisse in C oder C++ werden vorausgesetzt.

### **260126 Windows-Betriebssysteme: Einführung und Grundlagen**

Folgende Themen sollen behandelt werden:

1. Die Bedienoberfläche von Windows: Look and Feel, Standardprogramme
2. Betriebssystemarchitektur: Dateisystem, Registry, Systemsteuerung, Dienste, Benutzerverwaltung, Zugriffsrechte, Kryptographie, Objekte
3. Kommunikationsdienste: Internet, LAN, TCP/IP, NetBios, Browser, Telnet, X, Terminal-Server-Client, Netzwerkverbindungen
4. Installation und Konfiguration: Betriebssysteme, Anwendungsprogramme, Netzkonfiguration (Ethernet, ISDN, Modem)
5. Sicherheit: Viren, Netzangriffe, Absicherung des PCs, McAfee, Personal FireWall
6. PC-Hardware: Bus-System, Plattentechnologien, Speicher, Peripherie
7. Rückblick und Ausblick: DOS, WfW, Windows 95/98/ME, Windows NT/2000, Architekturunterschiede, Stärken und Schwächen der aktuellen Versionen

### **260130 Rechnernetze und Internet: Fortgeschrittene Themen**

Folgende Themen sollen behandelt werden:

1. IP-Routing-Protokolle
2. IP-Multicast
3. virtuelle Netzstrukturen: VLANs, ELANs, VPN
4. Zugangstechnologien: Modem, ISDN, ADSL
5. Sicherheit in Rechnernetzen
6. Netzwerk-Policies
7. Multimediaanwendungen in Datennetzen
8. Netzwerkmanagement
9. Ethernet-Troubleshooting
10. ATM: Asynchronous Transfer Mode

An anderer Stelle finden Sie vorlesungsbegleitende Materialien im WWW.

### **260164 Sicherheit in der Informationsverarbeitung (vorrangig für Systemadministratoren und Technisch Verantwortliche)**

Ziel der Veranstaltung ist es, Verantwortlichen für die Informationsverarbeitung (IV) – und hier insbesondere den in der IV aktiv Tätigen, d. h. Technisch Verantwortliche, (Domänen-)Administratoren – Grundlagen, Elemente und Konzepte der Sicherheit in der Informationsverarbeitung im Grundsätzlichen, aber auch mit unmittelbarem Nutzen für die Praxis näher zu bringen.

Eine Anmeldung ist erforderlich im Geschäftszimmer des ZIV (mit E-Mail-Adresse). Sofern noch ausreichend Platz zur Verfügung steht, sind auch andere Interessierte (z. B. Studierende, IV-Nutzer) eingeladen. Über die aktive Teilnahme kann ein Zertifikat ausgestellt werden.

### **260145 Kolloquium des Zentrums für Informationsverarbeitung**

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

# ZIV-Regularia

## Fingerprints

R. Perske

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

Bei E-Mails, WWW-Servern und an vielen anderen Stellen wird zunehmend mit Verschlüsselung und elektronischen Unterschriften gearbeitet. Dabei besitzt mindestens einer der Kommunikationspartner (beispielsweise der WWW-Server) einen öffentlichen Schlüssel, der vom anderen Partner (beispielsweise Ihrem WWW-Browser) zum Verschlüsseln oder zum Überprüfen einer elektronischen Unterschrift benutzt wird.

Um zu verhindern, dass Ihnen falsche öffentliche Schlüssel untergeschoben werden, sollten Sie überprüfen, ob der jeweilige Schlüssel tatsächlich zur angegebenen Person bzw. zum angegebenen Server gehört. Zu diesem Zweck sind die Schlüssel häufig mit Zertifikaten versehen, das sind elektronische Beglaubigungen, ausgestellt von sog. Zertifizierungsstellen, in denen die Eigentümerschaft bestätigt wird.

Im Bereich des deutschen Wissenschaftsnetzes erstellen die DFN-PCA als übergeordnete Zertifizierungsinstanz und die WWUCA als Zertifizierungsstelle der Universität Münster solche Zertifikate, siehe <http://www.dfn-pca.de> und <http://www.uni-muenster.de/WWUCA/>. Seit Januar 2004 zertifiziert die WWUCA auch RSAv4- und DSS/DH-Schlüssel, die mit Gnu PG, PGP 8 u. Ä. erzeugt wurden.

DFN-PCA und WWUCA unterstützen zwei verschiedene Verschlüsselungs- und Zertifizierungssysteme: Die PGP-Familie (Pretty Good Privacy), zu der auch GnuPG (Gnu Privacy Guard) gehört, wird meistens bei E-Mail eingesetzt. Die X.509-Familie wird beispielsweise bei abhörsicheren WWW-Servern, bei S/MIME und bei Object Signing verwendet.

Zum Überprüfen der von DFN-PCA und WWUCA ausgestellten Zertifikate benötigen Sie deren öffentliche Schlüssel. Diese finden Sie auf <http://www.uni-muenster.de/WWUCA/zertifikate.html> (X.509 und PGP) oder auch an anderen Stellen wie beispielsweise der perMail-Titelseite <http://permail.uni-muenster.de> (nur X.509), der ZIVprint-Einstiegsseite <http://www.uni-muenster.de/ZIV/zivprint.html> (nur X.509) oder der ZIV-Mitarbeiterliste <http://www.uni-muenster.de/ZIV/Mitarbeiter/> (nur PGP).

Die Fingerabdrücke (Fingerprints) dieser Schlüssel sind nachfolgend abgedruckt, damit Sie beim Aktivieren der Schlüssel auf Ihrem Rechner kontrollieren können, dass Sie tatsächlich die echten Zertifizierungsschlüssel erhalten haben.

### PGP-Kommunikationsschlüssel

Da die Zertifizierungsschlüssel ausschließlich zum Zertifizieren verwendet werden, gibt es gesonderte Kommunikationsschlüssel, die Sie bitte verwenden, wenn Sie eine verschlüsselte E-Mail an die jeweilige Zertifizierungsstelle schreiben möchten:

KeyID 4CB7658D: Zertifizierungsstelle Universitaet Muenster (E-Mail) <ca@uni-muenster.de>

2048 Bits, Fingerprint: 383D 0F16 CEFC 1F9E B7C3 04B1 2020 FCE6

KeyID 94E799B5: DFN-PCA (2004), ENCRYPTION Key <dfnpca@dfn-pca.de>

2048 Bits, Fingerprint: A9F8 2DC4 09CC DA7F DC67 8FE5 28DE AAAC

### PGP-Zertifizierungsschlüssel der WWUCA

KeyID 38B7A481: Zertifizierungsstelle Universitaet Muenster 2004-2005

2048 Bits, Fingerprint: 973E 0725 040B 1745 F272 180D 08C2 C15A

KeyID BC811EB1: Zertifizierungsstelle Universitaet Muenster 2002-2003

2048 Bits, Fingerprint: 2864 01BC F0EF D5BA D9A0 866C 4379 4C1D

KeyID 313C02F5: Zertifizierungsstelle Universitaet Muenster 2000-2001

2048 Bits, Fingerprint: 3762 F5E0 C278 7697 530F 2DF2 F3B3 27F5

KeyID EF750F1D: Rainer Perske +49(251)83-31582 Certification Key

2048 Bits, Fingerprint: 2F38 6EF8 DC2E D85E 5B35 DB49 8AE4 52AF

## PGP-Zertifizierungsschlüssel der DFN-PCA

KeyID FDCB1C33: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005)  
 <<http://www.dfn-pca.de/>>  
 2048 Bits, Fingerprint: 96B0 AD7F B8DC 0018 DCA0 7053 1C3B 4DA5

KeyID F2D58DB1: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003)  
 <<http://www.dfn-pca.de/>>  
 2048 Bits, Fingerprint: DE31 690D BC6A E779 4DCD A1B5 8180 FE7B

KeyID 63EB5391: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2001)  
 <not-for-mail>  
 2048 Bits, Fingerprint: CFAF 6C29 4E57 4E0E E81C BDB4 54FD 2AAB

KeyID F7E87B9D: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1999-2000)  
 <not-for-mail>  
 2048 Bits, Fingerprint: 6570 7274 B5E0 3FF0 EA7C ABE4 465F B8B2

KeyID 35DBF565: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1997-1998)  
 <not-for-mail>  
 2048 Bits, Fingerprint: 097C 0919 D3C3 86DC 7A30 1511 1295 8DE3

## X.509-Zertifikate der WWUCA

Inhaber: C=DE, O=Universitaet Muenster,  
 CN=Zertifizierungsstelle 2004-2005/Email=ca@uni-muenster.de  
 Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,  
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de  
 Seriennummer: 64774066 (0x3dc5fb2)  
 MD5-Fingerprint: 2619 6BEF 66B2 7044 52CC BE11 4C5F 3CB8  
 SHA1-Fingerprint: 1765 AE6D 57C7 7914 D2AF BAF3 439C E139 66E1 A0AE

Inhaber: C=DE, O=Universitaet Muenster,  
 CN=Zertifizierungsstelle 2002-2003/Email=ca@uni-muenster.de  
 Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,  
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de  
 Seriennummer: 1774668 (0x1b144c)  
 MD5-Fingerprint: A431 AD41 D8F2 1856 4E31 CC69 71E6 174F  
 SHA1-Fingerprint: 6945 20CA 1AFE 5CFA 6C37 52EB B772 B054 90EC D979

## X.509-Wurzelzertifikat der DFN-PCA

Inhaber: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,  
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de  
 Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,  
 CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de  
 Seriennummer: 1429501 (0x15cffd)  
 MD5-Fingerprint: 3E1F 9EE6 4C6E F022 0825 DA91 2308 0503  
 SHA1-Fingerprint: 8E24 22C6 7E6C 86C8 90DD F69D F5A1 DD11 C4C5 EA81

Alle Angaben zur DFN-PCA ohne Gewähr.

Liebe Leserin, lieber Leser,

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

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

Vielen Dank!

Redaktion i



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

- Meine Anschrift hat sich geändert.  
Alte Anschrift:

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

Absender:

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

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

Straße: \_\_\_\_\_

Außerhalb der Universität:  
\_\_\_\_\_

*(Bitte deutlich lesbar in Druckschrift ausfüllen!)*

Ich bin damit einverstanden, dass diese Angaben in der i

-Leserdatei gespeichert werden (§ 4 DSGVO).

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

\_\_\_\_\_  
Unterschrift