infoRUM

Zentrum für Informationsverarbeitung der Universität Münster

Jahrgang 25, Nr. 1 – Februar 2001 ISSN 0931-4008

Inhalt

Impressum

infoRUM

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

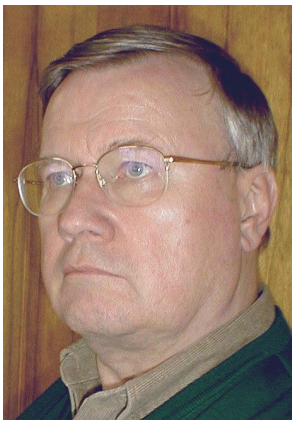
Satzsystem: Corel WordPerfect 8.0 für Windows 98/NT

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

Auflage dieser Ausgabe: 1500

In eigener Sache

H. Pudlatz



Sie vermissen unsere Rubrik RUM-Aktuell? Wir haben sie nicht aus unserem Informationsangebot gestrichen, sondern sind lediglich einen Schritt weitergegangen in Richtung der inzwischen allgemein eingeführten Terminologie. Wir haben uns eigentlich recht schnell an ZIV (gesprochen nicht wie „Zett-I-Fau“, sondern eher wie „Ziff“) gewöhnt, obwohl es gelegentlich noch vorkommt, dass der Bezeichnung „Zentrum für Informationsverarbeitung“ in Klammern erklärend „Universitätsrechenzentrum“ hinzugefügt wird. Schließlich sollen ja die 95% der vergleichbaren Institutionen an deutschen Hochschulen, die sich – wie auch wir früher – HRZ oder URZ nennen, wissen, dass bei uns auch noch gerechnet wird.

Wir haben unsere Rubriken RUM-Aktuell, RUM-Tutorial, RUM-Lehre etc. also ab sofort in ZIV-Aktuell, ZIV-Tutorial resp. ZIV-Lehre umbenannt, womit wir keineswegs 25 Jahre infoRUM-Geschichte umschreiben wollen, in der RUM nicht für das karibische Getränk, sondern für das Rechenzentrum der Universität Münster stand. Auch beabsichtigen wir nicht, den Namen unserer Informationsschrift entsprechend anzupassen, schließlich steckt in diesem Namen auch das Wort Forum. Auch zukünftig wollen wir ein Informationsforum für unsere Nutzer sein, die wir auf diesem Wege herzlich einladen, mit allgemein interessierenden Beiträgen aus dem Bereich der Informationsverarbeitung sich an diesem von uns moderierten Forum zu beteiligen. Im Übrigen kann man infoRUM auch so lesen: Informationsverarbeitung an der Universität Münster.

Nicht gerade die spannendste Lektüre, aber doch ein notwendiger Beitrag, sind die bisher regelmäßig in der Rubrik „Aktuell“ erschienenen Fingerprints. Sie finden sie in dieser Ausgabe in der Rubrik „Index“, in der auch das Stichwortverzeichnis des letzten Jahrgangs steht.

Editorial

H. Pudlatz

Vor wenigen Tagen beunruhigte das Anna-Kournikova-Virus die Mitglieder der Windows-Gemeinde, besonders diejenigen unter ihnen, die das Microsoft-Mailprogramm Outlook verwenden. Der Schädling funktionierte somit ähnlich wie der ILOVEYOU-Wurm des letzten Jahres, jedoch mit reduzierter Schadwirkung. Er trat als Mail-Anhang unter dem Namen AnnaKournikova.jpg.vbs auf und nutzte damit eine Schwäche neuer Windows-Betriebssysteme, bei denen – als Voreinstellung! – bekannte Datei-Suffixe einfach weggelassen werden, weil sie ja ohnehin als Dateityp im Explorer noch einmal genannt werden. Durch diese unbedachte Annahme wird das inkriminierte Visual-Basic-Programm (mit dem Suffix .vbs) zu einer harmlosen Grafik (Suffix .jpg). Damit sah der allem Schönen zugewandte Mail-Empfänger nach einem Doppelklick auf die Anhangsdatei leider kein Bild der attraktiven Tennis-Dame, sondern das hinterhältige Basic-Programm verschickte sich selbst an alle Adressaten des eigenen Outlook-Adressbuchs. Wer kam schon auf die Idee, den mit dem Update „Outlook 2000 SR-1“ gelieferten Mail-Filter zu nutzen, der vbs-Dateien hätte abgefangen können?

Die durch eine Nachlässigkeit der Windows-Designer begünstigte Einfalltür für Viren hätte nicht sein müssen. Um so erstaunter war man, als man neulich im „InformationWeek Daily“ las, dass Microsoft jetzt einen „Internet Security and Acceleration Server 2000“ verkauft, der auf Unternehmensebene Sicherheit und zugleich Geschwindigkeit im Netz vereinigen soll und damit ein Zwitter zwischen einem Firewall und einem Proxy-Server zu sein scheint. Der ISA-Server ist für den stattlichen Preis von knapp 6000 US-$ zu haben. Fraglich bleibt, ob das Unternehmen für eine Selbstverständlichkeit so heftig zur Kasse bitten muss, oder möchte man nur auch am Kuchen teilhaben, von dem Antivirus- und Firewall-Anbieter wegen der Sicherheitslücken zahlreicher Webprogramme im Windows-Umfeld bisher ganz gut leben?

Eine Reihe von Web- und Mail-Servern, nämlich die in anderen Betriebssystemumgebungen als Windows laufenden, sind von dieser Neuigkeit ohnehin nicht betroffen, da der ISA-Server nur für Unternehmen mit reinen Windows-Umgebungen interessant ist. Statt dessen sei als erste Schutzmaßnahme allen empfohlen, die ihre Mail unter Windows bearbeiten und nicht so schnell wieder auf den oben beschriebenen Suffix-Trick hereinfallen wollen, zur Erhöhung ihrer eigenen Sicherheit im Windows Explorer im Menüpunkt „Ansicht - Optionen“ das Kästchen „Keine Erweiterungen für registrierte Dateien“ auszuklicken. Leider gibt es dann immer noch Endungen, die nicht angezeigt werden, z. B. pif.

ZIV-Aktuell

Rechnerverbund NRW

W. Held

Der vollständige Bericht zum Thema kann unter `http://www.arnw.de/docs/rvnrw/` abgerufen werden. Wir bringen hier die Zusammenfassung.

Im Rechnerverbund NRW (RV-NRW) wurde ein einfach nutzbarer, leistungsfähiger Verbund von IT-Ressourcen eingerichtet, der derzeit konkurrenzlos ist. Die vom ZIV bereitgestellte Benutzerverwaltung ist landeseinheitlich, die Daten sind automatisch dort, wo sie benötigt werden und die Datenstrukturen sind wohl definiert. Die Ressourcen können landesweit in Anspruch genommen werden. Die weitgehende Ortsunabhängigkeit der Server, die bisher schon innerhalb einer Hochschule gegeben war, ist damit auf das Land NRW ausgedehnt worden.

Der Rechnerverbund NRW ist zu sehen vor dem Hintergrund der zunehmenden Ansprüche der Benutzer in den Hochschulen. Diese verlangen zuverlässige Mail-, Web-, Rechen-, und Datendienste (z. B. Fileserver, Archiv- und Backupserver) sowie Beratung bei der Konfiguration der i. Allg. dezentral mit Webschnittstellen zu verwaltenden Dienste. Darüber hinaus führt der ansteigende Einsatz von Simulationswerkzeugen zu einer stetig wachsenden Nachfrage an Anwenderberatung, Schulung und methodischer Unterstützung. Dies erfordert aufgrund der personellen und finanziellen Restriktionen eine andere Organisationsform, welche über die traditionellen Universitätsgrenzen hinausgeht. Mit dieser Organisation der Ressourcen ergänzen sich die Dienstleistungen der einzelnen Hochschulrechenzentren zu einem neuen Ganzen und verbessern das Niveau der IT-Versorgung damit deutlich.

Aufgaben, die in einzelnen Hochschulrechenzentren gleichermaßen anstehen, können arbeitsteilig gelöst werden, um so die dringende Weiterentwicklung der IT-Infrastrukturen und IT-Anwendungen voran zu bringen. Im Gegensatz zu der häufig diskutierten Möglichkeit des Outsourcing von Diensten verbleiben allerdings das Know-how und die Kontrolle über den Einsatz von neuen Technologien bei den Hochschulrechenzentren. Dies spart Kosten, verstärkt die Motivation der Mitarbeiter und unterstützt den Innovationsanspruch der Hochschulen.

Die mittlerweile verfügbare Softwaretechnologie erlaubt es, einen solchen landesweiten Verbund in die schon vorhandenen IT-Infrastrukturen der beteiligten Hochschulrechenzentren mit der für ein solches Projekt notwendigen Zuverlässigkeit einzubinden und mit der notwendigen Dienstgüte unter Produktionsbedingungen zu betreiben.

Neubeschaffungen im Unix-Server-Bereich

St. Ost

Die Rechnerausstattung des ZIV für die Basis-Dienste wurde verstärkt.

Ende des Jahres gelang es, die Server-Ausstattung des ZIV zu verstärken. Neben 14 kleineren Servern, die vor allem für Mail-, Web- und Netzbasis-Dienste gedacht sind und die vorhandene ältere Systeme ablösen oder ergänzen, konnten drei größere Server beschafft werden. So verfügen wir jetzt über einen zweiten TSM-Backup-Server, der die Kapazitäts-Probleme des bisher einzigen Backup-Servers beheben hilft. Zusätzlich wurde eine weitere Tape-Library beschafft, die im augenblicklichen Ausbaustand eine Kapazität von 7,2 TB besitzt und mit einem schon vorhandenen Server die Backup-Kapazität erweitert. Die beiden anderen Server sind für das Netzwerk-Management und die Netzwerkdatenbank vorgesehen.

Der TSM-Backup-Server ist mit der alten Tape-Library bereits in Produktion. Die anderen Server werden nach Abschluss der Umbaumaßnahmen im Gebäude Einsteinstraße die Produktion aufnehmen.

Neues DCE/DFS-Gateway für Windows und Linux

St. Ost

Entwicklung für RV-NRW hält Einzug in die WWU.

Der Wunsch ist relativ häufig: Sie möchten von ihrem Windows- oder Linux-PC aus, einerlei ob Sie zu Hause arbeiten oder in der Universität, auf ihre im DCE/DFS gespeicherten Daten zugreifen – und zwar ohne dazu ein File-Transfer-Programm wie „ftp“ oder „scp“ zu benutzen. Und natürlich wollen Sie deswegen keine zusätzliche Software auf Ihrem Rechner installieren müssen.

Bislang haben Sie vielleicht hierzu das WWUDCE-Gateway benutzt. Sowohl die Software als auch die Hardware des Gateways sind in die Jahre gekommen. Die betriebliche Stabilität und Performance ist daher manchmal nicht so, wie sie sein sollte.

Auf dem Rechner `samba1` gibt es nun ein zweites DCE/DFS-Gateway. Wie der Rechnername schon vermuten läßt, beruht dieses Gateway auf einem Samba-Server. Samba-Server verhalten sich gegenüber Windows- und Linux-Klienten wie NT-Fileserver. `samba1` ist ein AIX-Rechner und hat als solcher quasi natürlichen Zugriff auf die DCE/DFS-Daten. Der Samba-Server auf `samba1` stellt diese Daten wie ein NT-Fileserver zur Verfügung. Die Gateway-Funktion besteht nun darin, die zwischen Windows-Client und Fileserver stattfindende Authentifizierung auszunutzen und aus ihr den Dateizugriff ins DCE/DFS abzuleiten.

Die zur DCE/DFS-Unterstützung notwendigen Änderungen am Samba-Server wurde von einem Mitarbeiter des ZIV (Jürgen Hölters) im Rahmen des Rechnerverbund-NRW-Projekts entwickelt. Freie Software, deren Source-Code zur Verfügung steht und angepasst werden kann, ist wirklich von großem Vorteil.

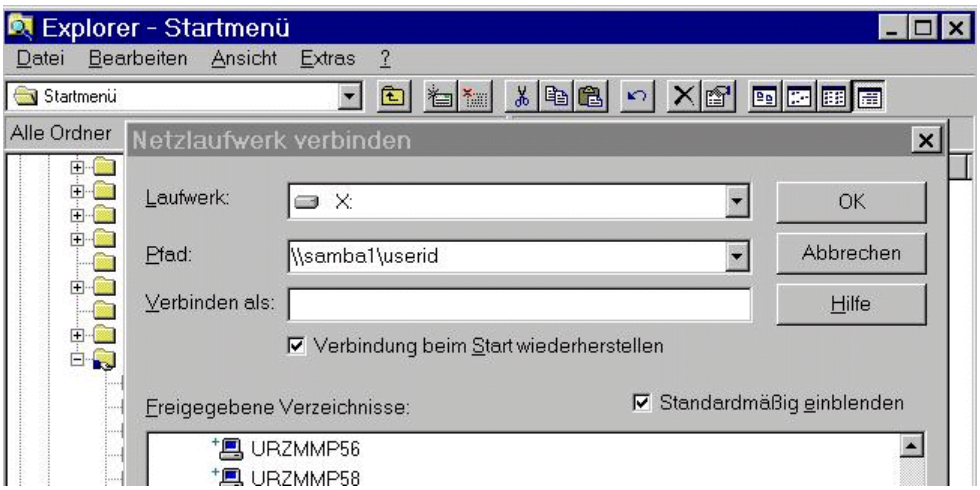
Was muss man tun, um das Gateway benutzen zu können? Zunächst einmal muss das Gateway freigeschaltet werden. Diese Funktionalität haben wir in den Routinen zur Passwort-Änderung versteckt, die Sie über die ZIV-Web-Seiten unter der URL

```
https://user.uni-muenster.de/exec/passwd
```

erreichen. Das Gateway ist mit Ihrer nächsten Passwort-Änderung freigeschaltet. Und das bleibt es auch so lange, wie Sie alle etwaigen zukünftigen Passwort-Änderungen ausschließlich über diese Web-Seite vornehmen. Bei diesem Passwort handelt es sich um das Passwort, das Sie zum Mail-Lesen oder beim Anmelden auf dem Rechner `asterix` verwenden.

Benutzer von Windows 95 und Windows 98 müssen noch eine zweite Voraussetzung erfüllen: Richten Sie einen lokalen Windows-Benutzer ein, der genauso heißt wie Ihre vom ZIV zugeteilte Benutzerkennung.

Windows-NT- und Windows-2000-Nutzer dagegen können beim Einbinden des Laufwerks die ZIV-Benutzerkennung angeben. Diese kann von Ihrer lokalen Kennung verschieden sein.



Das Einbinden des Laufwerks kann z. B. im Windows Explorer geschehen durch Anklicken des Icons „Netzlaufwerk verbinden“ in der Menü-Leiste und Ergänzen der Pfadangabe, wie nebenstehend gezeigt, wobei für „userid“ Ihre Benutzerkennung einzusetzen ist. Nach dem Bestätigen haben Sie mit dem (hier beispielhaften) X-Laufwerk Zugriff auf Ihre DCE/DFS-Daten.

EASA 2000

B. Süselbeck

Vom 26. bis 28. November fand im World Trade Center in Rotterdam das Finale des European Academic Software Award (EASA 2000) statt. Dabei wurden die 29 Finalisten aus 7 europäischen Ländern von einer internationalen Jury begutachtet und die 10 Preisträger ermittelt.

Bei diesem wichtigen europäischen Software-Wettbewerb konnten sich Studenten und Wissenschaftler aus allen Hochschulen in Europa beteiligen. Die Finalisten wurden aus über 300 Einreichungen ausgewählt, die in einer ersten, einjährigen Phase sorgfältig getestet und von internationalen Experten bewertet wurden. Somit stellte schon die Teilnahme an der Endrunde eine Auszeichnung dar und bot den Entwicklern die Möglichkeit, ihr Produkt einem kritischen Fachpublikum zu präsentieren. Ein Gewinn des Preises bringt Anerkennung innerhalb und außerhalb der akademischen Welt und kann die Basis für eine erfolgreiche Vermarktung des Programms sein.

Der niederländische Minister für Wissenschaft und Forschung Loek Hermans überreichte die Preise im Rahmen einer Konferenz über Einsatz von Software in Forschung und Lehre und hob in seiner Rede die Bedeutung des EASA 2000 für die Entwicklung und Verbreitung innovativer Softwarelösungen in der akademischen Welt hervor, insbesondere auch als Gegengewicht zu der Dominanz Nordamerikas in diesem Bereich.

Aus deutscher Sicht erfreulich ist, dass 7 der 29 Finalisten aus Deutschland stammen, davon 3 aus Nordrhein-Westfalen. Die deutschen Gewinner sind:

***Cinderella*: Ulrich Kortenkamp, Jürgen Richter-Gebert (Koautor), Freie Universität Berlin**

"Cinderella is a sophisticated interactive Geometry software for use in teaching and self learning and research. It can be used to create geometric constructions, animations and interactive exercises that can be exported to the WWW."

Herr Kortenkamp ist Absolvent der Universität Münster. Er war 1995 Diplomand von Prof. Clausing am Institut für Informatik.

***Interactive Screen Experiments (ISE)*: Jürgen Kirstein, Technische Universität Berlin**

"Interactive Screen Experiments are a new concept of using multimedia technology in education. They are designed to represent real experiments in physics within muldimedia learning environments which supports individual learning processes."

Der EASA wird alle zwei Jahre von der „European Knowledge and Media Association" (EKMA) veranstaltet, deren Ziel die Verbreitung und Entwicklung neuer Medien in Forschung und Lehre ist. EKMA ist eine internationale Vereinigung mit zur Zeit 8 Mitgliedsländern: Niederlande, Österreich, Schweiz, Frankreich, Großbritannien, Schweden, Norwegen und Deutschland. Partner für Deutschland ist das Zentrum für Informationsverarbeitung der Westfälischen Wilhelms-Universität Münster.

Der Wettbewerb EASA wird jedesmal von einem anderen Mitgliedsland organisiert. Die Endrunde des EASA 2002 wird von Schweden ausgerichtet.

Das ZIV als Partner des EASA 2000

Das ZIV hat die Betreuung des EASA für Deutschland im Mai 2000 (nach dem Ausscheiden des bisherigen Partners) während des laufenden Wettbewerbs unter schwierigen Bedingungen übernommen. Dabei wurden neben umfangreichen administrativen Aufgaben auch die Funktionen als Disziplinkoordinator Ingenieurwissenschaften und Gutachter im Finale wahrgenommen. Die Arbeiten wurden vom Ministerium für Schule, Wissenschaft und Forschung Nordrhein-Westfalen großzügig und unbürokratisch unterstützt.

Nach dem Finale ist vor dem Finale

Zur Zeit laufen schon die Vorbereitungen für EASA 2002, dessen Finale im Herbst 2002 in Schweden stattfinden soll. Das ZIV wird rechtzeitig über die genauen Modalitäten für eine Teilnahme informieren und hofft auf eine rege deutsche Beteiligung, natürlich insbesondere auch aus unserer Universität.

Neues von WWWplot

E. Sturm

Nach der Anschaffung neuer Drucker „kennt“ WWWplot jetzt auch Schwarzweißlaserdrucker und mehr Warteschlangen.

Nicht jeder braucht Farbbilder, und Studierende nur mit DaWIN-Kennung dürfen nicht auf unseren Farblasern drucken. Für diese Fälle gab es bisher nur den Endlosdrucker IBM 3835, dessen Auflösung von 240 dpi aber eher an die Redewendung von Ofen und Hund erinnert.

Hier bieten die neuen Schwarzweißlaserdrucker HP 8100 deutlich mehr, und Zugangsbeschränkungen für Studierende gibt es auch nicht. Wenn Sie also Bilder in schwarzweiß drucken wollen, brauchen Sie jetzt bei WWWplot nur den neuen Punkt „als Papierbild ausdrucken auf Schwarzweißlaserdrucker“ anzuhaken und auf „Start der Aktion“ zu klicken. Als Sonderwünsche stehen die schon bekannte Exemplaranzahl und die Option zur Verfügung, das Papier nur einseitig zu bedrucken – für den Fall, dass Sie entgegen den Intentionen von WWWplot mehrere Bilder in eine Datei gepackt haben. Voreingestellt ist aus Papierersparnisgründen natürlich „doppelseitig“.

Mit der Einführung neuer Drucker wurden auch neue Warteschlangen eingerichtet. Die Warteschlange `ein-ps` für Schwarzweißlaserdrucker ist tatsächlich die letzte vor dem Drucker. Was man dort nicht mehr sieht, ist an den Drucker weitergeleitet worden. Und was Sie dort sehen, können Sie mit Hilfe von WWWplot auch tatsächlich streichen, wenn Sie wollen.

Nicht ganz so perfekt ist die neue Warteschlange `ein-cps` für Farblaserdrucker. Sie ist zwar die letzte vor dem Drucker, aber nicht die einzige für diese Druckerklasse. Schicken Sie ein Bild ohne Sonderwünsche zum Drucker, ist alles so, wie man es sich vorstellt: Man sieht seinen Druckauftrag und kann ihn ggf. auch streichen. Hatten Sie aber einen Sonderwunsch gehabt, wollten etwa 2 Exemplare ausgeben oder auf Folie drucken, so wandert der Auftrag über zwei Warteschlangen. Befindet er sich noch in der ersten, sehen Sie seinen Namen und können ihn auch streichen. Befindet er sich in der zweiten, so sehen Sie nur noch eine Nummer, können allenfalls raten, welcher Auftrag es ist (falls mehrere Aufträge von Ihnen unterwegs sind), und ein Streichwunsch wird ignoriert.

Einen Hinweis möchte hier wiederholen: Wenn Sie den Dateinamen eingegeben haben und auf „Start der Aktion“ klicken, wird die angegebene Datei zum Server übertragen. Aus programmiertechnischen Gründen geschieht dies auch dann, wenn Sie auf „Sonderwünsche“ geklickt haben – nur vermutet man es dann noch nicht.

Ach so (falls Sie es noch nicht wissen): WWWplot finden Sie auf der Web-Startseite des ZIV unter dem Punkt „Drucken im ZIV“.

NIC_online – Endgeräteverwaltung über das WWW

M. Kamp

Informationen zu angemeldeten Datenendgeräten können jetzt online verwaltet werden.

Seit kurzer Zeit befindet sich NIC_online (`www.nic.uni-muenster.de`) im Probebetrieb. NIC_online ermöglicht, den **leitend und technisch Verantwortlichen** für Datenendgeräte im Netz (Rechner, Netz-Drucker, etc.) einen einfachen und direkten Zugang zur Netz-Datenbank des Zentrums für Informationsverarbeitung (ZIV). Es können bereits fast alle Informationen zu Endgeräten verändert oder ergänzt werden.

Beispielsweise ist der Einbau einer neuen Netzwerkkarte jetzt mit wenigen Mausklicks in der Datenbank des Netz-Informations-Center (NIC) dokumentiert und der DHCP-Server liefert die richtige IP-Adresse für diese Netzkarte. Weiterhin können Windows-Domänen angemeldet und verwaltet werden, damit diese auf den WINS-Servern der Universität bekannt sind. Der Funktionsumfang wird in der nächsten Zeit noch erheblich anwachsen, geplant sind unter anderem die Delegation von Verwaltungsaufgaben an andere Personen

sowie die Online-Anmeldung von Datenendgeräten.

Voraussetzung für die Nutzung ist, dass Sie über eine zentrale vom ZIV verwaltete Nutzerkennung verfügen, die in der Netz-Datenbank des NIC bekannt sein muss. Ob dies bereits der Fall ist, können Sie durch einen Anmeldeversuch auf den NIC_online-Seiten herausfinden.

Falls Ihre Kennung noch nicht bekannt ist, können Sie diese dem NIC (Zentrum für Informationsverarbeitung; Abteilung für Kommunikationssysteme, Röntgenstr. 9-13, 48149 Münster) in einem formlosen Schreiben mitteilen, der Zugang wird dann umgehend freigeschaltet. Wir bitten Sie um Verständnis, dass wir aus Datenschutzgründen und zu Ihrer Sicherheit auf einem schriftlichen Anmeldemodus bestehen müssen.

Funk-LANs an der WWU

W. Held / G. Richter

Das ZIV hat das lokale Rechnernetz in der WWU, das bisher auf Glasfaser- und Kupfer-Kabeltechnik beruhte, in zahlreichen Räumen verschiedener Fachbereiche unter Einsatz von Funk-LANs erweitert und Hörsäle, Labor- und Praktikumräume, Seminarräume, Lesesäle in Bibliotheken sowie Sitzecken für Studierende eingebunden. Außerdem wurden und werden noch LANs einiger Gebäude, die über das Festnetz nur mit sehr hohem Kostenaufwand erreichbar sind, über Funkstrecken verbunden.

Bereiche, die über Funk-LAN erreichbar sind, erkennt man daran, dass dort entsprechende Plakate „Hier funkt‘s“ Aufmerksamkeit wecken sollen (s. Abb.).

Der Aufbau der Funk-LANs wurde vom Bundesministerium für Bildung und Forschung kurzfristig initiiert und dankenswerterweise finanziell unterstützt. Die Hälfte der Mittel wurde von der WWU selbst dazu getan. Die Durchführung des Pilotprojektes wurde auf Antrag des ZIV und der WWU vom Ministerium für Schule, Wissenschaft und Forschung in NRW zur Realisierung vorgeschlagen.

Die Mobilität der Studierenden sowie der Wissenschaftlerinnen und Wissenschaftler wird mit dem Einsatz der Funk-LANs wesentlich erhöht werden. Die Arbeitsmöglichkeiten der Studierenden werden dadurch insbesondere auch in Pausen zwischen Lehrveranstaltungen verbessert werden. Studierende konnten bisher umfangreiche Daten aus Computer-Pools in der Universität nur schwer auf häusliche Arbeitsplätze übertragen, da sie ihre Laptops nicht einfach in die bisherigen LANs integrieren konnten. Dies wird durch die Funk-LANs deutlich verbessert, denn der eigene Laptop kann in den Funk-LAN-Bereichen einfach aufgestellt und ohne Übertragungskosten betrieben werden, wenn er mit einer entsprechenden Funk-LAN-Karte ausgestattet ist.

Das ZIV wird zur „Initialzündung“ zunächst 100 Funk-LAN-Karten gegen Hinterlegung einer Kaution an Studierende ausleihen. Weitere Einzelheiten finden Sie unter

`http://www.uni-muenster.de/ZIV/funklan`

ZIV-Tutorial

Sicherer Zugang zu Daten und Informationen durch Smart-Karte und elektronisches Buch

H.-W. Kisker

Dieser Artikel wird auch im Tagungsband zum cHL-Tag 2000 erscheinen (vgl. infoforum Nr. 3/2000).

Einleitung

Sicherheit ist ein sprödes Thema. Dieser Artikel behandelt den speziellen Aspekt der Authentifizierung und zwei darauf basierende Anwendungen: die *Smart-Karte* und das *elektronische Buch*. Das Beispiel elektronisches Buch zu diesem Thema mag den einen oder anderen überraschen. Wir werden jedoch sehen, dass erst die Lösung des Authentifizierungsproblems das elektronische Buch für die kommerziellen Verlage als Auslieferungsmedium akzeptierbar gemacht hat.

Die Notwendigkeit, eine sichere Authentifizierung und zwar in beiden Richtungen zu gewährleisten, wird mit der Verbreitung von Diensten im Netz immer dringlicher. Nur wenn ein Rechnersystem zweifelsfrei die Identität eines Benutzers festgestellt hat, kann es diesem vertrauliche Informationen übermitteln, z. B. Prüfungsergebnisse. Nur wenn eine Person absolut sicher ist, dass sie mit einem bestimmten Rechner kommuniziert, wird sie diesem geheime Daten anvertrauen, z. B. die Geheimnummer der Kreditkarte. Nur wenn zwei Personen, die über das Netz miteinander kommunizieren, gegenseitig keinen Zweifel an der Identität des anderen haben, werden sie persönliche Mitteilungen austauschen.

Insbesondere der eCommerce ist auf Dauer ohne eine nicht verfälschbare Authentifizierung nicht denkbar.

Die Smart-Karte

In der Realität bietet die heute übliche Authentifizierung ein gehöriges Maß an Unsicherheit. Üblicherweise ist zur Authentifizierung erforderlich:

1. eine Benutzerkennung,
2. ein dem Benutzer und dem System bekanntes Geheimnis (z. B. ein Passwort).

Das große Problem bei diesem Verfahren ist der Punkt 2. Passwörter sind vielfältigen Gefährdungen ausgesetzt. Sie werden vergessen, weitergegeben, abgehört und geknackt. Einen substantiellen Gefährdungsabbau bringt die Forderung, zusätzlich und zweifelsfrei den Besitz eines realen Objekts nachzuweisen, z. B. den Besitz einer eindeutig identifizierbaren Smart-Karte. Zur Authentifizierung ist dann erforderlich:

1. eine Benutzerkennung (z. B. TEDDY),
2. ein Passwort (z. B. HONIG) und
3. die eindeutig identifizierbare Smart-Karte (s. Abb. oben)

Dabei ist anzumerken, dass i. Allg. das Passwort hier nicht mehr an den Rechner übertragen wird, sondern nur noch als sogenannte PIN an die Smart-Karte. Eine solche PIN kann länger sein als vier Ziffern und kann beliebige alphanumerische Zeichen enthalten.

Das übliche Nutzungsprofil für Smart-Karten propagiert eine lange Liste von Leistungen,

die hiermit realisiert werden können:

- Ausweisfunktion (Authentifizierung),
- Nachweis persönlicher Daten (z. B. für Prüfungsanmeldung),
- Abrufen persönlicher Daten (z. B. Prüfungsergebnisse),
- Zugang zu Räumen,
- Arbeitszeiterfassung (Gleitzeitregelung)
  usw.

Bei unserem Ansatz wird die Smart-Karte selbst ausschließlich für den ersten Punkt, die *Ausweisfunktion*, genutzt. Sie dient also dazu, sich einem Rechnersystem gegenüber auszuweisen. Alle weiteren Funktionen werden dann nachgeschaltet von dem Rechnersystem aus gesteuert. Hier sind Daten und Berechtigungen in Datenbanken abgelegt. Diese Vorgehensweise bringt eine Reihe von Vorteilen mit sich. Die Karte selbst sagt nur noch etwas darüber aus, wer man ist. Was man ist oder wozu man berechtigt ist, ist nicht Inhalt der Karte. Um Änderungen vorzunehmen, muss die Karte nicht verfügbar sein. Um z. B. einer Person der Zugang zu einem Raum zu gestatten (oder zu verwehren), ist nur eine Änderung in der Datenbank erforderlich. Die Konsequenzen des Verlusts einer Karte sind begrenzt. Es wird eine neue Karte ausgestellt und deren Identifikation der betroffenen Person zugeordnet. Beim Ausscheiden aus der Universität muss die Karte nicht eingezogen werden, statt dessen wird ihre Zuordnung zu einer Person in der Datenbank gelöscht. In beiden Fällen wird die Karte selbst wertlos.

Der kritische Punkt bei der Authentifizierung mit Smart-Karten ist die eindeutige Identifizierbarkeit. Dies wird gewährleistet durch den Einsatz der *Public-Key-Technologie*.

Das Prinzip der öffentlichen Schlüssel

Den meisten bekannt sind die üblichen Verschlüsselungsmechanismen. Die Kommunikationspartner teilen sich hierbei ein gemeinsames Geheimnis – den Schlüssel S. Text, der mit diesem Schlüssel verschlüsselt wird, kann mit dem gleichen Schlüssel auch wieder entschlüsselt werden. Ein dritter, der den Schlüssel nicht kennt, kann die Kommunikation nicht belauschen. Man spricht in diesem Fall von *symmetrischer Verschlüsselung*.

Bei der *Public-Key-Verschlüsselung* verfügt dagegen jeder Kommunikationspartner über ein eigenes Paar zusammengehöriger Schlüssel S und P. Die Schlüssel sind nicht auseinander ableitbar. Die beiden Schlüssel haben die Eigenschaft, dass ein Text der mit S verschlüsselt wird, nur mit P wieder entschlüsselt werden kann und umgekehrt. Der Schlüssel S wird der geheime Schlüssel genannt. Er ist nur dem Eigentümer bekannt und wird zu keinem Zeitpunkt einem anderen Kommunikationspartner offenbart. Der Schlüssel P wird als öffentlicher Schlüssel behandelt. Er wird beliebig veröffentlicht und verbreitet. Möchte man mit einem Partner sicher kommunizieren, so besorgt man sich dessen öffentlichen Schlüssel. Mit diesem verschlüsselt man den zu übertragenden Text und übermittelt ihn zum Partner. Nur dieser kann den verschlüsselten Text mit seinem nur ihm bekannten geheimen Schlüssel entschlüsseln. Dieses Prinzip wird nun genutzt, um die Identität eines Kommunikationspartners zu überprüfen. Dabei wird das folgende als *Challenge/Response* bezeichnete Verfahren verwendet.

1. Man besorgt sich den öffentlichen Schlüssel des zu überprüfenden Kommunikationspartners.
2. Man bildet (würfelt) einen Zufallstext, verschlüsselt ihn mit dem öffentlichen Schlüssel und überträgt den verschlüsselten Text an den zu überprüfenden Partner.
3. Der Partner entschlüsselt den Text mit seinem geheimen Schlüssel und sendet den entschlüsselten Text zurück.
4. Der zurückübertragene Text wird mit dem Ursprungstext verglichen. Sind die beiden identisch, so ist der Partner authentifiziert, da nur der Besitzer des geheimen Schlüssels den Text entschlüsseln konnte.

Zertifikate

Der Punkt 1 des Challenge/Response-Verfahrens beinhaltet ein nicht zu unterschätzendes Problem. Zwar ist der öffentliche Schlüssel meines Kommunikationspartners keineswegs geheim. Wahrscheinlich kann man auch davon ausgehen, dass er an vielen Stellen zu finden ist. Aber woher weiß ich, dass es sich bei dem Schlüssel, der als der meines Partners ausgegeben wird, wirklich um seinen handelt? Ein Fehler in der Einschätzung kann unangenehme Folgen haben. Ich übermittle dann möglicherweise vertrauliche Daten an eine fremde Person, die mir einen falschen Schlüssel untergeschoben hat. Eine Scheinlösung dieses Problems wäre es, dass sich jeder eine Sammlung von öffentlichen Schlüsseln seiner Kommunikationspartner anlegt, die er auf sicherem Wege (z. B. persönlich oder per Briefpost) bekommen hat. Dies führt zu einer umfangreichen Schlüsselsammlung bei jedem Einzelnen, die gepflegt und gewartet werden muss. Auch kann ich vertraulich nur mit Personen kommunizieren, mit denen ich vorher schon einen Kontakt zur Schlüsselübermittlung hatte. Betrieblich ist dies ein schwerfälliges Verfahren.

Die Lösung sind Zertifikate. Innerhalb der Kommunikationsgemeinde einigt man sich auf eine für alle vertrauenswürdige Instanz: die CA (= *Certificate Authority*). Diese übernimmt es die Echtheit von öffentlichen Schlüsseln zu beglaubigen – oder wie man sagt, zu zertifizieren. Hierzu werden wiederum Public-Key-Mechanismen eingesetzt. Die CA verfügt ebenfalls über ein Schlüsselpaar. Ihr öffentlicher Schlüssel wird allen Mitgliedern der Kommunikationsgemeinde auf einem sicheren(!) Wege zugeleitet. Der übliche Kommunikationsweg (insbesondere das Internet) ist hierfür unbrauchbar. Eine Möglichkeit der sicheren Verteilung ergibt sich, wie wir sehen werden, beim Aufbau einer Smartkarten-Infrastruktur automatisch.

Ein Anwender, der ein Zertifikat benötigt, bildet ein Schlüsselpaar und legt den öffentlichen Schlüssel der CA zur Zertifizierung vor. Nach sorgfältiger Überprüfung der Identität bildet die CA daraufhin eine Aussage der Art:

```
Der öffentliche Schlüssel der Person ... lautet ...
```

Diese Aussage wird mit dem geheimen Schlüssel der CA verschlüsselt und dann dem Antragsteller auf einem sicheren (!) Weg als sein Zertifikat ausgehändigt. Die genaue Form und der tatsächliche Inhalt der Zertifikate ist in den X.509-Spezifikationen festgelegt. Diesem Zertifikat kann nun jeder, der CA vertraut, den öffentlichen Schlüssel zweifelsfrei entnehmen. Dazu entschlüsselt er das Zertifikat mit dem öffentlichen Schlüssel der CA und übernimmt so Name und zugehörigen öffentlichen Schlüssel. Für den einzelnen Benutzer entfällt so die Anlage einer Schlüsselsammlung. Er muss nur **einen** Schlüssel bei sich selbst aufbewahren – den öffentlichen Schlüssel der CA. Alle anderen öffentlichen Schlüssel entnimmt er dem Zertifikat, das entweder der Meldung angehängt oder auf öffentlichen Servern gespeichert ist.

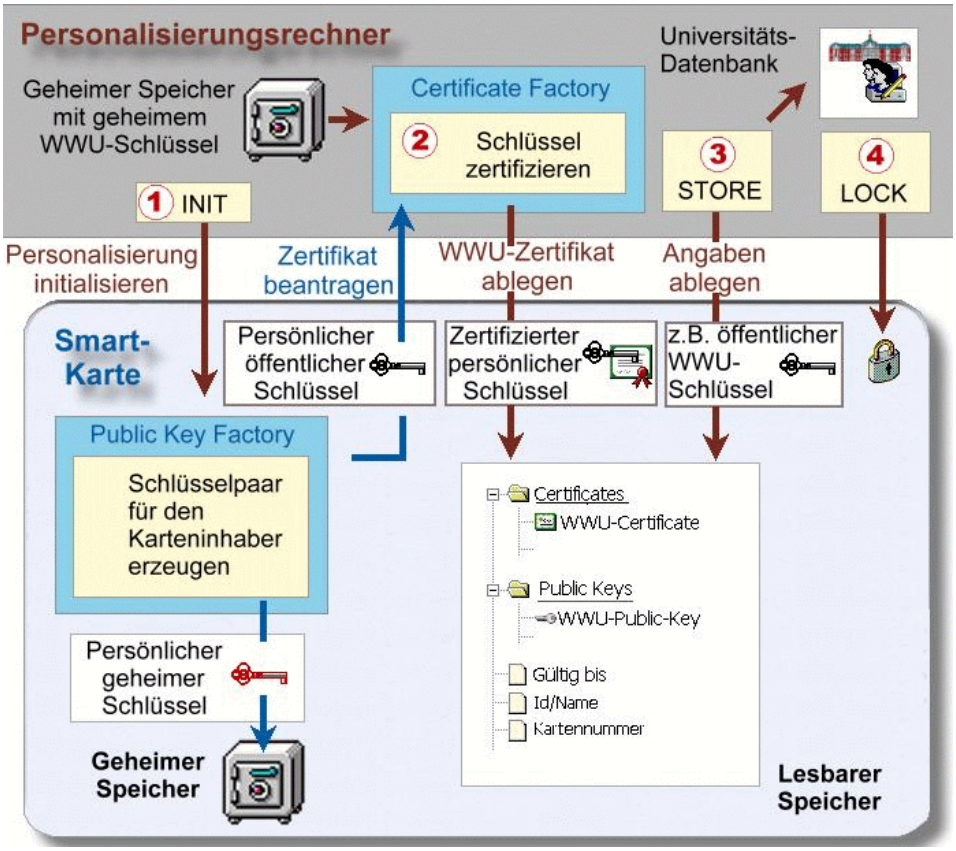
Der innere Aufbau der Smart-Karte

Eine Smart-Karte besteht aus einem Rechner mit Prozessor, Programmspeicher und Datenspeicher. Auf den Speicher kann nicht direkt zugegriffen werden, sondern nur mit Hilfe des Prozessors. Die Sicherheit, die eine Smart-Karte bietet, hängt damit entscheidend von dem Programm ab, nach dem die Smart-Karte arbeitet. Nur über das implementierte Programm können Zugriffe auf Daten gestattet oder verweigert werden. Für die Schnittstelle zur Smart-Karte gibt es verschiedene Normen. Basis sind die Normen ISO 7810 und ISO 7816. MasterCard-, Visa- oder GSM-Karten und auch PC/SC (PC/SmartCard), die Schnittstelle für den PC, sind hiervon abgeleitet.

Für die Authentifizierung wird eine Karte mit Software für Public-Key-Mechanismen benötigt. Solche Karten werden von verschiedenen Anbietern, z. B. GemPlus oder Schlumberger, angeboten. Diese Karten stellen die folgenden Funktionsgruppen zur Verfügung:

1. **Public Key Factory:** Das erforderliche Schlüsselpaar wird auf der Karte gebildet.
2. **Authentication Unit:** Die Karte kann sowohl Challenge/Response-Anfragen beantworten, als auch selbst solche anstoßen, um sich von der Identität eines Systems zu überzeugen.
3. **Geheimer Speicher:** Für die in diesem Teil des Speichers abgelegten Daten ist sichergestellt, dass sie nie die Smart-Karte verlassen. Hier wird z. B. der geheime Schlüssel aufbewahrt.
4. **Zugänglicher Speicher:** Auf der Karte kann es auch einen Bereich geben, der von Außen lesbare Informationen enthält. Hier kann z. B. der öffentliche Schlüssel untergebracht sein.
5. **Verriegelung:** Die Smart-Karte wird in einem Zustand ausgeliefert, in dem sie noch verändert werden kann. Z. B. wird das Schlüsselpaar erst vor Ort beim *Personalisieren* (s. u.) gebildet. Auch können noch Angaben wie z. B. Name des Benutzers oder ausstellende Institution aufgebracht werden. Ist die Karte so aufbereitet, dass sie ausgegeben werden kann, wird die Verriegelung aktiviert. Danach kann die Karte nicht mehr geändert, sondern nur noch als Ausweis genutzt werden. Auch Kopieren der Kartendaten ist nicht mehr möglich. Der Vorgang der Verriegelung ist irreversibel.
6. **Zugangsschutz durch PIN:** Die Authentifizierung mit Hilfe der Smart-Karte ist indirekt. Tatsächlich wird überprüft, ob die Karte einer bestimmten Person präsentiert wurde. Da die Zuordnung von Person zu Karte eindeutig und fälschungssicher ist, schließt man vom Vorhandensein der Karte auf das Vorhandensein der Person. Oder anders ausgedrückt: Wer die Karte einer bestimmten Person besitzt, wird auch von allen Systemen als diese Person akzeptiert. Um so wichtiger ist es, die Auswirkung des Verlustes oder gar des Diebstahls der Karte zu begrenzen. Hierzu dient die PIN. Sie kann deutlich länger als die im Bankbereich üblichen vier Ziffern sein, und sie kann aus beliebigen alphanumerischen Zeichen bestehen. Mit der PIN weist sich der Besitzer der Karte gegenüber aus. Nur wenn diese Kennung korrekt übermittelt wurde, ist die Karte funktionsbereit.

Die Personalisierung



Die Public-Key-Smart-Karten werden üblicherweise in einem Rohzustand ausgeliefert. Sie enthalten noch kein Schlüsselpaar und die Schreibfunktion ist noch aktiviert. Sie werden erst bei der Ausgabe an Ihren Besitzer für diesen *personalisiert*. Dieser Vorgang erfordert eine Umgebung (Personal, Ausstattung) mit hohem Sicherheitsstandard. Während der Personalisierung kann von einem Zustand des absoluten Vertrauens ausgegangen werden.

Bei der Personalisierung für eine bestimmte Person wird eine Rohkarte in den Leser des Personalisierungsrechners eingelegt. Dieser sendet der Karte ein Initialisierungskommando. Die Karte bildet daraufhin intern ein persönliches Schlüsselpaar für die Person. Der geheime Schlüssel wird im geheimen Speicher abgelegt. Er ist **nie** von außen auslesbar. Der öffentliche Schlüssel wird an den Personalisierungsrechner zurückübertragen. Von jetzt an ist das Initialisierungskommando gesperrt. Die Sperrung ist irreversibel.

Der Personalisierungsrechner stellt nun ein Zertifikat aus, das den Namen der Person mit dem von der Karte übermittelten öffentlichen Schlüssel verbindet. Hierzu muss der Personalisierungsrechner natürlich Zugriff auf den geheimen Schlüssel der CA haben. Das ausgestellte persönliche Zertifikat wird an die Karte übertragen. Ebenfalls übertragen werden einige Zusatzangaben:

1. **Gültigkeit:** Jedes Zertifikat wird nur für einen gewissen Zeitraum ausgestellt. Danach muss es erneuert werden.
2. **Identifikation:** Der Personalisierungsrechner bildet für jede Person eine eindeutige Identifikationskennung. Dies kann eine Matrikel- oder Personalnummer sein, aber auch eine aus dem Namen abgeleitete Buchstabenkennung.
3. **Der öffentliche Schlüssel der CA:** Für die Verteilung des öffentlichen Schlüssel der CA ist ein sicherer, vertrauenswürdiger Kanal unbedingt erforderlich (s. o.). Der Vorgang der Personalisierung bietet einen Zustand auf hohem Sicherheits- und Vertrauensniveau. Die Personalisierung ist also prädestiniert dafür, den öffentlichen Schlüssel der CA weiterzugeben.

Persönliches Zertifikat und Zusatzangaben werden im öffentlichen Speicher der Smart-Karte abgelegt. Anschließend wird die Smart-Karte verriegelt. Der öffentliche Speicher kann dann zwar noch gelesen, aber nicht mehr beschrieben werden. Abschließend wird der visuelle Teil der Karte durch Aufdrucken von Name, Bild und Gültigkeitszeitraum personalisiert. Dann kann die Karte ihrem Besitzer ausgehändigt werden.

Für den eigentlichen Gebrauch der Smart-Karte ist es nicht erforderlich, dass die CA irgendwelche Angaben über ihre Personalisierungsaktivitäten speichert. In der Praxis wird es jedoch administrative, von der Smart-Karte unabhängige Erfordernisse geben, die eine Speicherung von Daten über die Person erfordern (Studentendatei, Mitarbeiterdatei der Verwaltung).

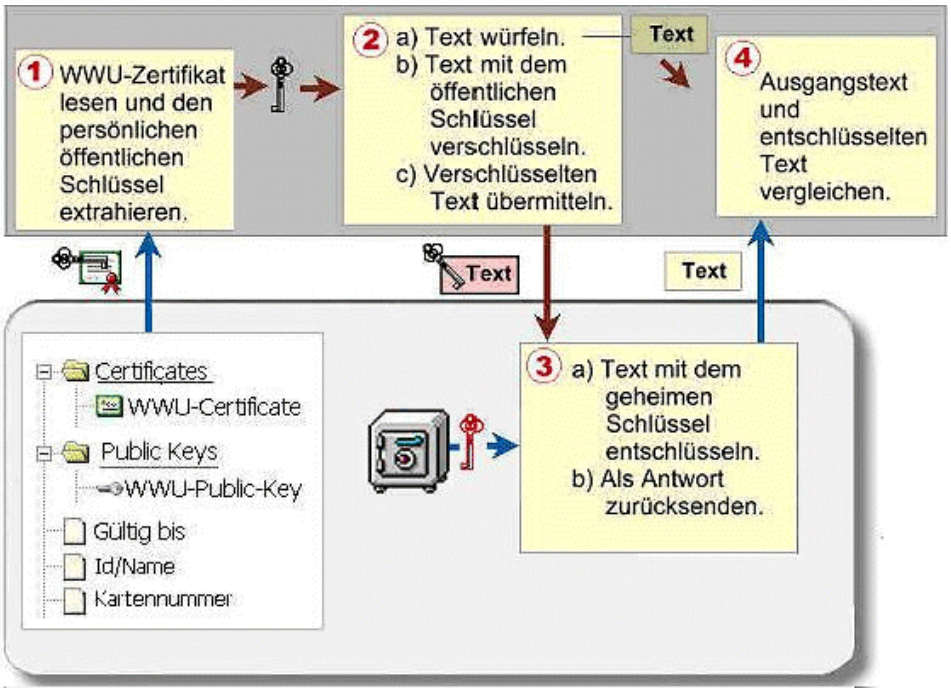
Außerdem gehört es zu den Aufgaben der CA, eine öffentliche Liste der widerrufenen Zertifikate zu führen (*Revoke-Liste*). Um aber bei dem Verlust und insbesondere dem Diebstahl einer Karte das darauf abgelegte Zertifikat in diese Liste aufnehmen zu können, muss es natürlich bei der CA noch vorrätig sein. Es ist für eine CA also dringend geboten, eine Sammlung aller ausgestellten Zertifikate aufzubauen.

Der Betrieb der CA

Ein Plädoyer für die Obrigkeit

Für öffentliche Einrichtungen, wie Universitäten, stellt sich die Frage der Organisation der CA. Deren Betrieb und insbesondere der Vorgang der Personalisierung erfordert erheblichen Aufwand an Personal, Zeit und Ausstattung. Um hier die Kosten leicht überschaubar zu halten, gibt es starke Tendenzen, diese Aufgaben an kommerzielle Partner weiterzugeben.

Ich halte dies für einen schweren Fehler. Den kommerziellen Firmen wächst durch diese Aufgabe eine ungeheure Macht zu. In der aufziehenden Welt der Kommunikationsgesellschaft wird man ohne ein persönliches Zertifikat nicht existieren. Man kann nicht kommunizieren, nicht am Konsum teilnehmen, nicht wählen usw. usw. Neben der Übernahme des Gewaltmonopols gehört es mit zu den vornehmsten Aufgaben eines Staates, seinen Bürgern Identität zu geben. Dies ist auch in der Kommunikationswelt eine Aufgabe des Staates.



Authentifizierung

Will man sich mit einer Smart-Karte einem Rechner-System gegenüber ausweisen, so wird beim Einlegen der Karte in den Leser und nach Eingabe der korrekten PIN das persönliche Zertifikat an den Rechner übertragen. Der Rechner extrahiert hieraus den persönlichen öffentlichen Schlüssel und führt mit ihm ein Challenge-Response-Verfahren (s. o.) der Karte gegenüber durch. Geht das Verfahren positiv aus, ist also Ausgangstext und entschlüsselter Text identisch, so gilt der Besitzer der Karte als authentifiziert. Welche Rechte er nun auf dem Rechner hat, worauf er Zugriff hat, was er nutzen kann oder was der Rechner für ihn leistet, ist ausschließlich von den Benutzerrechten, die im Rechner verwaltet werden, abhängig. Die Smart-Karte spielt hierfür keine Rolle mehr.

Das elektronische Buch

Elektronische Bücher stellen allenfalls eine Randerscheinung auf dem heutigen Buchmarkt dar. Allerdings werden sie von einigen großen und namhaften Verlagen unterstützt. Auch das Angebot an englischsprachiger Literatur ist beachtlich umfangreich.

Dass Verlagshäuser überhaupt bereit waren, Produkte im als unkontrollierbar geltenden Internet bereit zu stellen, hat seinen Grund in der besonderen Form der Auslieferungstechnik. Jedes elektronische (Hardware-)Buch besitzt intern ebenfalls ein diesem Buch zugeordnetes Schlüsselpaar. Wenn ein Benutzer nun von einem der Literaturanbieter ein (Software-)Buch erwirbt, so wird der öffentliche Schlüssel dieses Paares genutzt, um den Text des erworbenen Buches zu verschlüsseln. Der so verschlüsselte Text wird zum Käufer übertragen. Lädt er den Text auf sein elektronisches Buch, so kann dieser mit dem geheimen Schlüssel des elektronischen Buches intern entschlüsselt und angezeigt werden. Für alle anderen elektronischen Bücher ist der Text wertlos. Zwar kann er kopiert und weitergegeben werden, aber kein anderes elektronisches Buch kann ihn entschlüsseln.

Die Entwicklung der Akzeptanz der elektronischen Bücher ist nicht sehr hoch einzuschätzen. Für heutige Ansprüche bieten sie auch einen recht geringen Darstellungskomfort: nur schwarz-weiß, grobe Auflösung. Die nächste Generation von elektronischen Büchern verspricht hier Fortschritte. Eine bessere Auflösung, eine größere Lesefläche und Farben sind angekündigt. Auch die Nutzung des Internets soll über das elektronische Buch möglich sein.

ZIV-Lehre

Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2001)

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

Wegen der Begrenzung der Teilnehmerzahl ist für alle Veranstaltung eine Anmeldung am Service-Schalter des Zentrums für Informationsverarbeitung, Einsteinstraße 60, erforderlich. Eintragungen in die Anmeldelisten sind ab dem 15. Januar 2001 möglich.

260010 Sichere Kommunikation im Internet — Perske, R.
vom 19.02. bis 23.02.2001, ganztägig
Hörsaal: Raum 206, Röntgenstr. 11, Beginn: 19.02.2001, 10 Uhr

260044 Systemadministration für Windows-Systeme (für Fortgeschrittene) [1] — Kämmerer, M.
vom 05.03. bis 09.03.2001, ganztägig
Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 05.03.2001, 9 Uhr

260030 Einführung in Mathematica — Süselbeck, B.
vom 05.03. bis 09.03.2001, ganztägig
Hörsaal: Raum 745, Instituts-Gruppe I, Beginn: 05.03.2001, 9 Uhr

260063 Computerunterstütztes Publizieren mit LaTeX — Kaspar, W.
vom 12.03. bis 23.03.2001, ganztägig
Hörsaal: M4, Einsteinstr. 64, Beginn: 12.03.2001, 11 Uhr

260025 Programmieren in Fortran — Reichel, K.
vom 12.03. bis 23.03.2001, nachmittags
Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 12.03.2001, 13 Uhr

260059 Windows: Einführung und Grundlagen [2] — Kisker, H.-W.
vom 12.03. bis 23.03.2001, ganztägig
Hörsaal: Neuer CIP-Pool, Einsteinstr. 60, Beginn: 12.03.2001, 9 Uhr

260097 Einführung in Linux [2] — Ost, St.
vom 26.03. bis 06.04.2001, ganztägig
Hörsaal: M4, Beginn: 26.03.2001, 11 Uhr

260101 Systemadministration für Linux-Systeme (für Fortgeschrittene) [1] — Hölters, J./ Grote, M.
vom 26.03. bis 30.03.2001, ganztägig
Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 26.03.2001, 9 Uhr

260078 Statistische Datenanalyse mit dem Programmsystem SPSS — Zörkendörfer, S.
vom 12.03. bis 23.03.2001, ganztägig
Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 12.03.2001, 9 Uhr

260082 Programmieren in Java (für Fortgeschrittene) — Süselbeck, B.
vom 19.03. bis 30.03.2001, vormittags
Hörsaal: M4, Einsteinstr. 64, Beginn: 19.03.2001, 9 Uhr

---

[1] Diese Veranstaltung wird insbesondere für Mitarbeiter in IV-Versorgungseinheiten angeboten; jedoch kann eine Anmeldung auch von anderen Interessenten erfolgen, sofern noch freie Plätze vorhanden sind.

[2] Bei dieser Veranstaltung werden Studierende im Zusatzstudiengang Angewandte Informatik vorrangig berücksichtigt.

Veranstaltungen in der Vorlesungszeit (Sommersemester 2001)

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

Wegen der Begrenzung der Teilnehmerzahl ist für alle Veranstaltung eine Anmeldung am Service-Schalter des Zentrums für Informationsverarbeitung, Einsteinstraße 60, erforderlich. Eintragungen in die Anmeldelisten sind ab dem 12. März 2001 möglich.

260116	Kommunikation und Information im Internet Mi 13–15 Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 18.04.2001	Mertz, K.-B.
260120	Publizieren im Internet mit HTML und XML Mi 15–17 Hörsaal: M4, Einsteinstr. 64, Beginn: 25.04.2001	Neukäter, B.
260135	Programmieren in Java Mi 13–15 Hörsaal: M4, Einsteinstr. 64, Beginn: 25.04.2001	Pudlatz, H.
260140	Programmieren in C++ Di 13–15 Hörsaal: M4, Einsteinstr. 64, Beginn: 24.04.2001	Mersch, R.
260154	Statistische Datenanalyse mit dem Programmsystem SPSS Do 11–13 Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 26.04.2001	Nienhaus, R.
260169	Betriebssystem Windows NT/2000 Mi 11–13 Hörsaal: M4, Einsteinstr. 64, Beginn: 25.04.2001	Sturm, E.
260173	Rechnernetze und Internet – Ausgewählte Themen Do 10–12 Hörsaal: Raum 206, Röntgenstr. 13, Beginn: 26.04.2001	Richter, G./ Kamp, M./ Speer, M./ Wessendorf, G.
260188	Kolloquium des Zentrums für Informationsverarbeitung Fr 14–16 Hörsaal: Raum 206, Röntgenstr. 13	Held, W.

Kommentare zu den Lehrveranstaltungen

260010 Sichere Kommunikation im Internet

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

In der Veranstaltung wird gezeigt, welche Gefahren bestehen und wie man sich ohne große Mühe vor diesen Gefahren schützen kann. Praktisch geübt werden kurz das Absichern des eigenen Rechners sowie ausführlich das Einrichten und die Benutzung entsprechender Software zur sicheren Kommunikation:

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

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

Vorausgesetzt werden Erfahrungen im Umgang mit den Internet-Anwendungen E-Mail, WWW, Telnet und FTP sowie Grundkenntnisse der Funktionsweise (wozu braucht man IP-Adressen? Portnummern? Nameserver? Router?), wie sie beispielsweise durch den Besuch der Veranstaltung „Kommunikation und Information im Internet“ erworben werden können.

260044 Systemadministration für Windows-Systeme (für Fortgeschrittene)

Für Hörerinnen und 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 User-Verwaltung 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`

260030 Einführung in Mathematica

„Mathematica is a system for doing mathematics by computer.“ Dieser Satz von Stephen Wolfram, dem Autor des Systems, umreißt schon die wesentlichen Merkmale dieser interaktiven Programmiersprache aus dem Bereich der Computer-Algebra. In der Vorlesung erfolgt zunächst eine Einführung in das symbolische Rechnen. Anschließend werden die vielfältigen Möglichkeiten von Mathematica als Anwendungssystem zur Lösung von Problemen aus Analysis, Linearer Algebra und anderen Gebieten der Mathematik aufgezeigt. Der zweite Teil der Veranstaltung ist dem Thema Visualisierung gewidmet und stellt Mathematica als Grafiksystem vor. Die grundlegenden Techniken von Mathematica als Programmiersprache bilden den letzten Teil des Kurses.

260063 Computerunterstütztes Publizieren mit LaTeX

LaTeX ist ein mächtiges und flexibles Satzsystem, das sich besonders für wissenschaftliche und technische Publikationen eignet. Der Autor kann aus einer Vielzahl von fertigen Layouts auswählen und diese seinen eigenen Vorstellungen anpassen. Mit speziellen Komponenten, z. B. zur Erzeugung von PDF- oder HTML-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- und HTML-Dokumenten,

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

Die Hörerinnen und Hörer sollten Grundkenntnisse im Umgang mit PCs besitzen.

LAMPORT: *Das LaTeX-Handbuch*, Addison-Wesley
ABDELHAMID: *Das Vieweg LaTeX2e-Buch*, Vieweg
DETIG: *Der LaTeX Wegweiser*, Thomson
KOPKA: *LaTeX – Band 1: Einführung*, Addison Wesley
GOOSSEN, *Mittelbach, Samarin: Der LaTeX Begleiter*, Addison-Wesley
KLÖCKL: *LaTeX2e: Tips und Tricks*, dpunkt

260025 Programmieren in Fortran

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

In dieser Vorlesung sollen die Hörerinnen und Hörer lernen, wie Programme systematisch konstruiert werden. Gleichzeitig wird ihnen zunächst der Fortran-77-Standard, anschließend darauf aufbauend der neueste 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

260059 Windows: Einführung und Grundlagen

1. Die Bedienoberfläche von Windows
   Look and Feel; Standardprogramme
2. Betriebssystemarchitektur
   Dateisystem; Registry; Systemsteuerung; Dienste; Benutzerverwaltung; Zugriffsrechte; Krypthographie; 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. Entwicklungswerkzeuge und -umgebungen
   Programme, Objekte: Visual C/Basic/Java; Delphi
   Web-Gestaltung und Verwaltung: FrontPage; VisualInterDev; ASP

6. Sicherheit
   Viren; Netzangriffe; Absicherung des PCs; McAfee; Personal FireWall
7. PC-Hardware
   Bus-System; Plattentechnologien; Speicher; Peripherie
8. Rückblick und Ausblick
   DOS; WfW; Windows'95/98/ME; Windows NT/2000; Whistler
   Architekturunterschiede; Stärken und Schwächen der aktuellen Versionen

260097 Einführung in Linux

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

260101 Systemadministration für Linux-Systeme (für Fortgeschrittene)

Die Vorlesung richtet sich an fortgeschrittene Linux-Anwenderinnen und -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 Teilnehmerinnen und 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.

Da voraussichtlich 12-16 PCs zur Verfügung stehen werden, ist die Teilnehmerzahl auf diese Anzahl begrenzt. Eine Anmeldung ist erforderlich.

260078, 260154 Statistische Datenanalyse mit dem Programmsystem SPSS

Das statistische Programmsystem SPSS (Statistical Package for the Social Sciences) wird in dieser Veranstaltung in der neusten 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.

260082 Programmieren in Java (für Fortgeschrittene)

In der Vorlesung sollen einige fortgeschrittene Konzepte der Programmiersprache Java vorgestellt werden.

Am Anfang der Lehrveranstaltung stehen Techniken zur Unterstützung der parallelen Programmierung (Multithreading) in Java. Im Anschluss daran erfolgt eine Übersicht zu IO in Java (Streams-Konzept).

Als internetbasierte Sprache bietet Java eine Reihe von Werkzeugen zur Netzwerkprogrammierung. Neben der Vorstellung der entsprechenden Grundlagen erfolgt eine Übersicht zu den darauf aufbauenden Themen wie Remote Method Invocation, Datenbankzugriff und Servlets.

Einen weiteren Themenschwerpunkt bilden schließlich neuere Konzepte zur Gestaltung grafischer Benutzeroberflächen wie Java-Beans und die Swing-Klassen.

Eine Anmeldung beim Dozenten wird zur Unterstützung der Planung erbeten. (E-mail: `suselbe@uni-muenster.de`)

260116 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 Theorie und praktischen Übungen vermittelt, 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 und mit der MS-DOS-Eingabeaufforderung umgeht und welchem Zweck die DOS-Befehle `cd`, `mkdir`, `rmdir` usw. dienen.

260120 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.

260135 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, sogenannte 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.

Diese Vorlesung ist auch für Hörerinnen und Hörer ohne Vorkenntnisse im Programmieren geeignet.

260140 Programmieren in C++

C++ erweitert die Programmiersprache C mit ihren durch Assembler-ähnliche Sprachelemente einerseits und Elemente moderner blockstrukturierter Sprachen andererseits sehr vielseitigen Einsatzmöglichkeiten, um objektorientierte Konzepte. Diese Verbindung einer sehr erfolgreichen Programmiersprache mit einem seit einigen Jahren boomenden Programmier-Paradigma macht C++ zu einer der am meisten benutzen Programmiersprachen.

In der Lehrveranstaltung wird C++ gemäß dem 1998 erschienenen ISO/ANSI-Standard von Grund auf vorgestellt. Kenntnisse einer anderen Programmiersprache wären hilfreich, werden aber nicht vorausgesetzt.

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

260169 Betriebssystem Windows NT/2000

Windows NT und dessen Nachfolger Windows 2000 sind Betriebssysteme, die für den professionellen Einsatz gedacht sind (im Gegensatz zu Window 98 und Windows ME). Kompatibilität zu DOS war kein Design-Kriterium. Es ist aber davon auszugehen, dass zukünftige Windows-Versionen für Normalverbraucher auf Windows 2000 basieren werden.

In dieser Veranstaltung wird sowohl der Einsatz von Windows 2000 als auch die Betriebssystemarchitektur vorgestellt. Dabei soll u. a. auf Installation, Konfiguration, Bedienoberfläche und Kommunikation in Internet und lokalem Netz eingegangen werden. Hinzu kommen Sicherheitsmaßnahmen und die Benutzung frei verfügbarer Programme wie GhostScript und PGP.

Die Hörerinnen und Hörer sollten praktische Erfahrung mit PCs besitzen.

260173 Rechnernetze und Internet – Ausgewählte Themen

1. Zugangstechnologien: Modem, ISDN, ADSL, ...
2. virtuelle Netzstrukturen: VLANs, ELANs, VPN
3. Netzwerkpolicies
4. Sicherheit in Rechnernetzen: Firewalls, IPsec
5. Multimediaanwendungen in Datennetzen: Voice over IP, Digitales Video
6. Internet Protocol Version 6: IPv6
7. Netzwerkmanagement

260188 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-Index

Stichwörter infoRUM Jahrgang 24

Im Index bedeutet der Verweis „24,3-15“: Jahrgang 24, Heft 3, Seite 15

Fingerprints

R. Perske

Unter dieser Rubrik erscheinen regelmäßig die aktuellen kryptografischen Prüfsummen der öffentlichen Schlüssel, die von der WWUCA und vom Zentrum für Informationsverarbeitung verwendet werden.

Sie finden die nachfolgend genannten Zertifikate und Schlüssel auf den WWW-Seiten der WWUCA unter

```
https://www.uni-muenster.de/WWUCA/
http://www.uni-muenster.de/WWUCA/
```

X.509-Zertifikat der WWUCA

Zum Ausstellen von X.509-Zertifikaten für SSL-/TLS-Server und -Clients und für S/MIME-Schlüssel verwendet die WWUCA den in folgendem Zertifikat enthaltenen Schlüssel:

Version: 3 (0x2)
Serial Number: 16 (0x10)
Issuer:
    C=DE
    O=Deutsches Forschungsnetz
    OU=DFN-PCA
    CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
Validity
    Not Before: Jun 5 15:35:24 2000 GMT
    Not After: Jun 5 15:35:24 2002 GMT
Subject:
    C=DE
    O=Universitaet Muenster
    CN=Zertifizierungsstelle 2000-2001/Email=ca@uni-muenster.de
MD5-Fingerprint=DA:E3:E2:5D:BC:93:EF:03:37:96:4E:25:C1:AB:2B:D1
SHA1-Fingerprint=A764 5575 E0AD 9A2C 0CB4 C8ED BEE0 BFD4 726C 5CB2

Der mit diesem Zertifikat versehene Schlüssel wird von der WWUCA ausschließlich zum

Ausstellen von X.509-Zertifikaten, zum Signieren der Policy und zum Signieren von X.509-Widerruflisten (*Certificate Revocation List*, CRL) verwendet, und zwar nur bis Ende 2001. Danach wird es einen neuen Zertifizierungsschlüssel geben.

Der Fingerprint des Wurzelzertifikats 1999-2000 der DFN-PCA lautet:

MD5-Fingerprint=45:BB:9B:C8:8A:A4:84:8B:2D:A0:08:8F:9E:B6:B8:10
SHA1-Fingerprint=DFA5 6FB5 FC41 E3A8 921F 77AD 1622 EEFD 9152 A5AD

PGP-Zertifizierungsschlüssel der WWUCA

Zum Zertifizieren von PGP-Schlüsseln verwendet die WWUCA folgenden Schlüssel:

Bits: 2048
KeyID: 313C02F5
Date: 2000/03/24
User ID: Zertifizierungsstelle Universitaet Muenster 2000-2001
Key fingerprint = 37 62 F5 E0 C2 78 76 97 53 0F 2D F2 F3 B3 27 F5

Dieser Schlüssel wird von der WWUCA ausschließlich zum Ausstellen von PGP-Zertifikaten, zum Signieren der Policy und zum Signieren von PGP-Widerruflisten verwendet, und zwar nur bis Ende 2001. Danach wird es einen neuen Zertifizierungsschlüssel geben.

Dieser Schlüssel ist bereits durch den neuen DFN-PCA-Schlüssel rezertifiziert worden:

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

PGP-Kommunikationsschlüssel der WWUCA

Bei jeder Kommunikation mit der Zertifizierungsstelle sollte der folgende Schlüssel verwendet werden:

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

Dieser Schlüssel ist durch die WWUCA zertifiziert und auf unbestimmte Zeit gültig.

Mit Testschlüsseln erzeugte X.509-Zertifikate

Einige WWW-Server in der Universität besitzen noch keine von der WWUCA ausgestellten Zertifikate, sondern arbeiten noch mit Test-Zertifikaten. Dazu gehört insbesondere:

user.uni-muenster.de
MD5-Fingerprint=4F:D7:42:05:05:AA:EE:80:FF:35:C7:B4:53:09:6C:1F
SHA1-Fingerprint=4D8C 5645 DA83 73FD 879B 30FA 8188 CAAE 129B 2CB8

Liebe Leserin, lieber Leser,
wenn Sie infoWUM regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von infoWUM 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 infoWUM

☐ 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 infoWUM
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 infoWUM-Leserdatei gespeichert werden (§ 4 DSG NW).

_____ _____

Ort, Datum Unterschrift