# (Vor-)Entwurf Materialsammlung Internettechnologien

Prof. Dr. Hans-Jürgen Buhl

Wintersemester 2003/04

Bergische Universität Wuppertal
Fachbereich C — Mathematik

# Inhaltsverzeichnis

# 0. Einleitung

### Internet

In Zeiten der weltweiten Vernetzung, der rapiden Zunahme von Zahlungen und Geschäften via WWW sind Internettechnologien von immer größerer Bedeutung.
Was aber genau bedeutet eigentlich das Wort *internet* bzw. *Internet*? Eine Suche im frei nutzbaren `On-line Dictionary of Computing` gibt Aufschluß:

Aus http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=internet:



---

# internet

<networking>(Note: not capitalised) Any set of networks interconnected with routers. The Internet is the biggest example of an internet. (1996-09-17)

Aus http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=Internet:

Search Home Contents Feedback Random

---

# Internet

<networking>(Note: capital "I"). The Internet is the largest internet (with a small "i") in the world. It is a three level hierarchy composed of backbone networks, mid-level networks, and stub networks. These include commercial (.com or .co), university (.ac or .edu) and other research networks (.org, .net) and military (.mil) networks and span many different physical networks around the world with various protocols, chiefly the Internet Protocol.

Until the advent of the World-Wide Web in 1990, the Internet was almost entirely unknown outside universities and corporate research departments and was accessed mostly via command line interfaces such as telnet and FTP. Since then it has grown to become an almost-ubiquitous aspect of modern information systems, becoming highly commercial and a widely accepted medium for all sort of customer relations such as advertising, brand building, and online sales and services. Its original spirit of cooperation and freedom have, to a great extent, survived this explosive transformation with the result that the vast majority of information available on the Internet is free of charge.

While the web (primarily in the form of HTML and HTTP) is the best known aspect of the Internet, there are many other protocols in use, supporting applications such as electronic mail, Usenet, chat, remote login, and file transfer.

There were 20,242 unique commercial domains registered with InterNIC in September 1994, 10% more than in August 1994. In 1996 there were over 100 Internet access providers in the US and a few in the UK (e.g. the BBC Networking Club, Demon, PIPEX).

There are several bodies associated with the running of the Internet, including the Internet Architecture Board, the Internet Assigned Numbers Authority, the Internet Engineering and Planning Group, Internet Engineering Steering Group, and the Internet Society.

See also NYsernet, EUNet.

http://www.openmarket.com/intindex - statistics about the Internet.

(2000-02-21)

**email**

Eine Möglichkeit der Internetnutzung ist der Austausch von (elektronischen) Nachrichten: email. Viele Internet-Provider bieten email-Dienste über ein Web-Interface an:

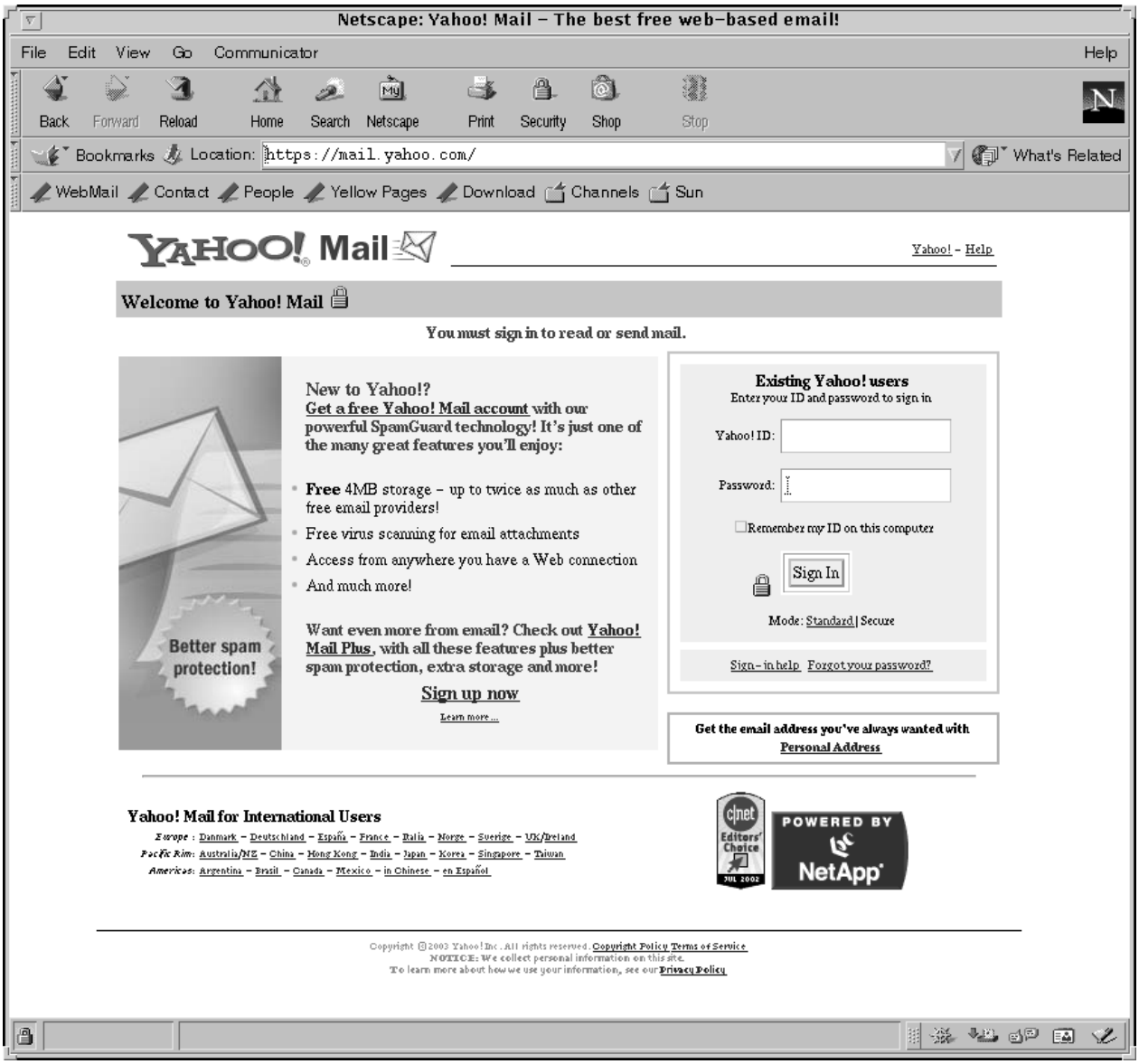



Abbildung 0.1.: E-Mail: `http://mail.yahoo.com`

Achten Sie bei Eingabeaufforderungen von Paßwörtern (zum Einloggen) bitte immer darauf, dass diese über eine verschlüsselte (sichere) Verbindung übertragen werden (`https://...` sowie beim ersten Zugang ein Zertifikatsannahme-Dialog wie folgt):

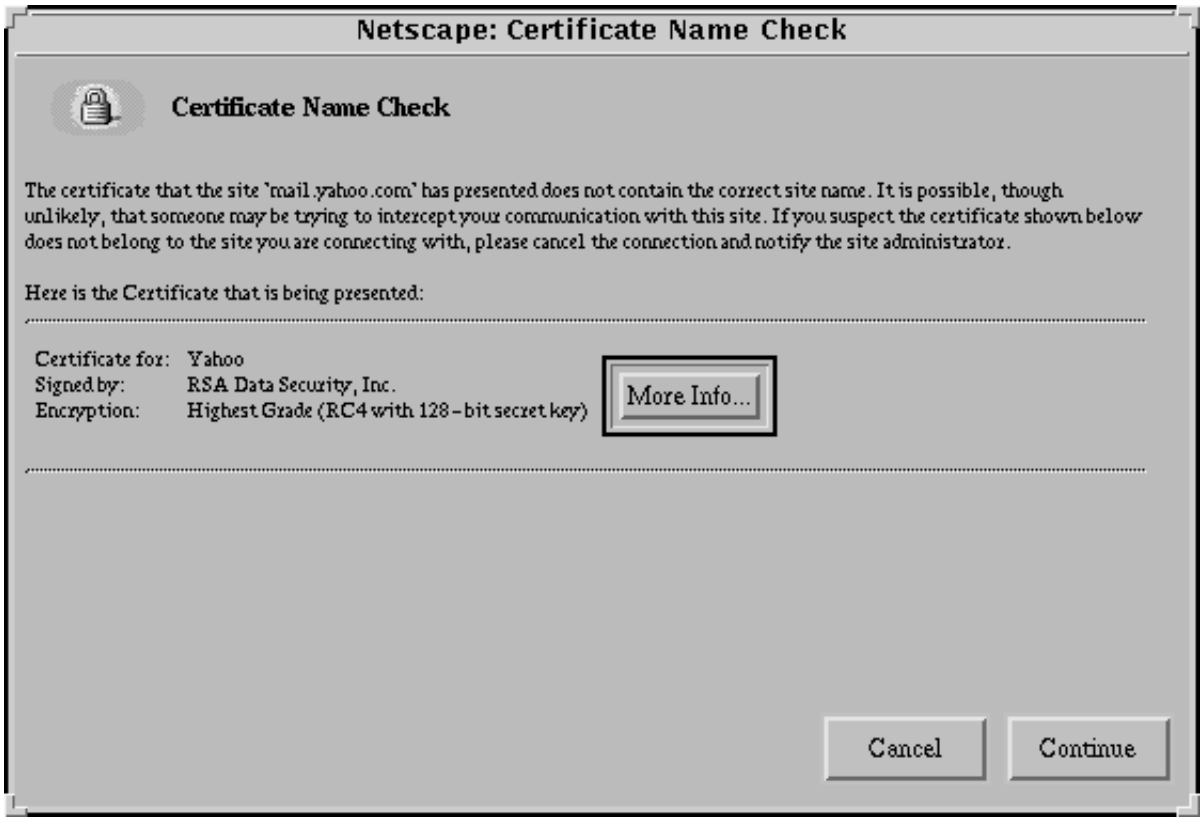



Abbildung 0.2.: E-Mail: `https`-Zertifikatsannahme-Dialog

Eine (noch flexibler nutzbare) Alternative ist der Zugriff auf einen IMAP-Server, der etwa in Netscape folgendermaßen eingerichtet werden kann (email-Account einrichten):

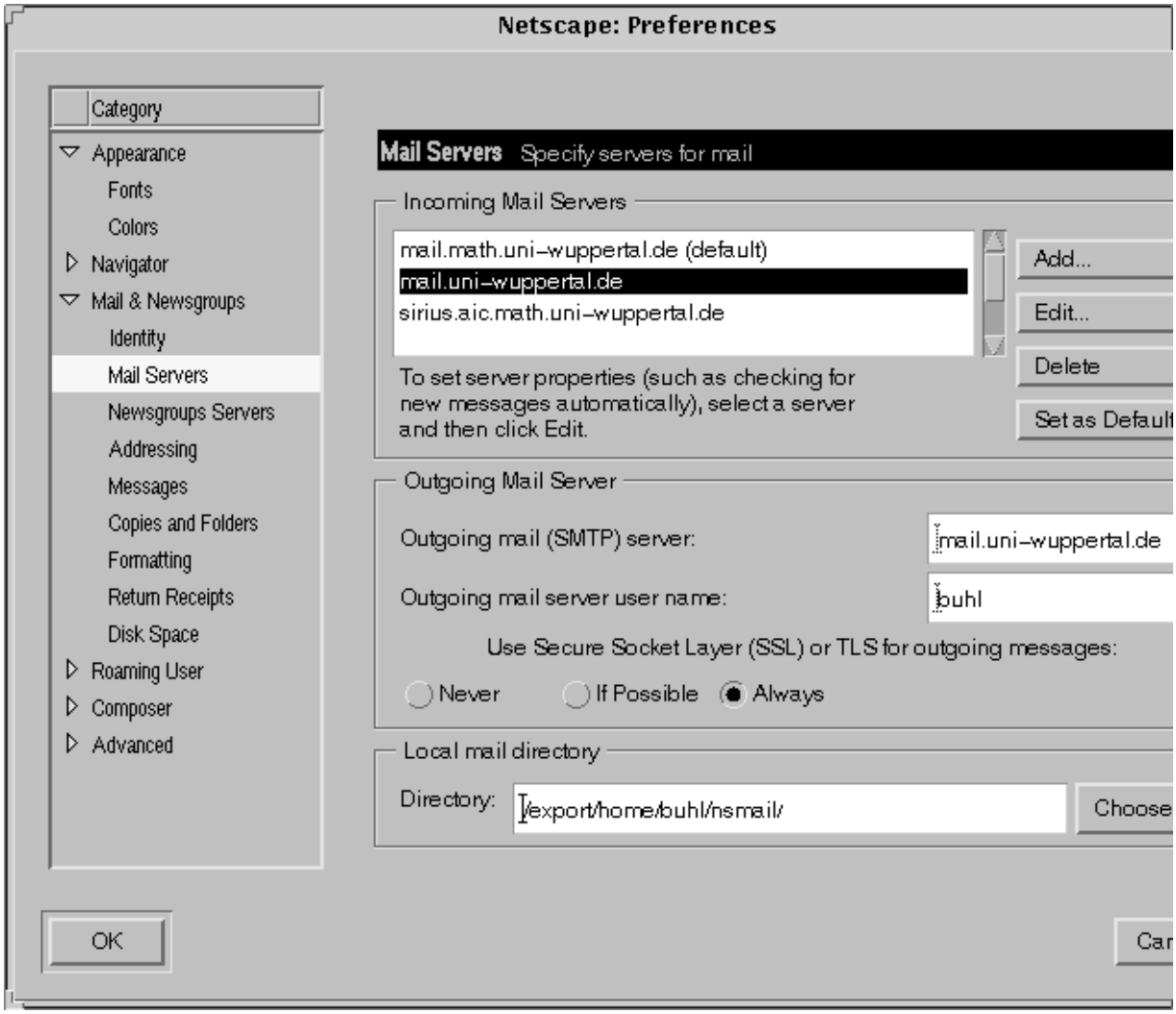



Abbildung 0.3.: E-Mail: IMAP-Account-Einrichtung I

Nach Anklicken von `Add` beziehungsweise `Edit`:

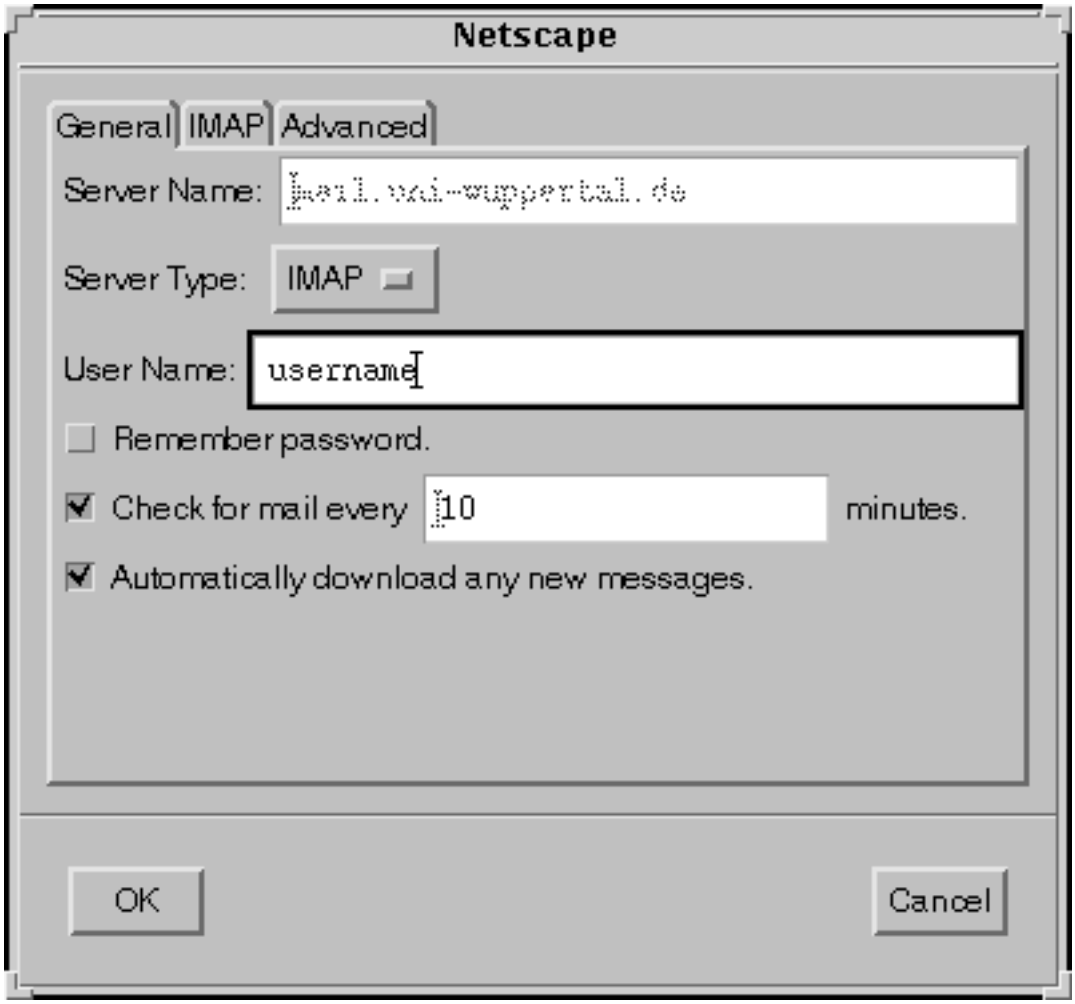



Abbildung 0.4.: E-Mail: IMAP-Account-Einrichtung II

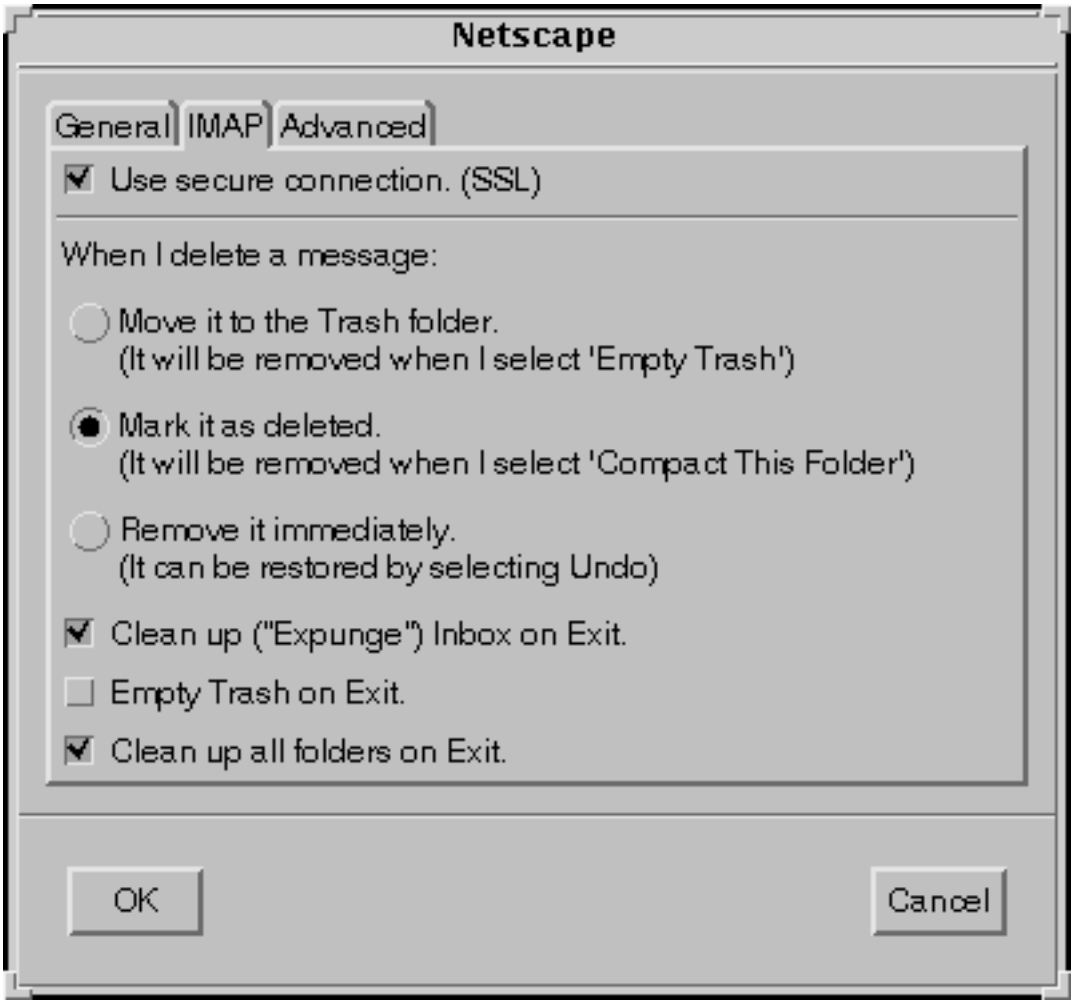



Abbildung 0.5.: E-Mail: IMAP-Account-Einrichtung III

Abbildung 0.6.: E-Mail: Netscape-Messanger als IMAP-Client

Leider wird die email-Nutzung heute sehr stark gestört durch

**SPAM — Eine Plage im Internet**
Unter SPAM versteht man im „elektronischen Post“-Bereich die Versendung unerwünschter, unangeforderter Massenwurfsendungen (meist Werbung zweifelhafter Herkunft und oft auch zweifelhaften Inhalts). http://dict.leo.org?search=spam übersetzt

2 Treffer für 'spam'

| **ENGLISCH** | **DEUTSCH** |
|---|---|
| Spam©[Amer.] | das Frühstücksfleisch |
| spam [comp.] | elektronisches Äquivalent unerwünschter Wurfsendungen |

Abbildung 0.7.: Quelle: http://dict.leo.org?search=spam

und http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=spam erläutert

# spam

1. <messaging> (From Hormel's Spiced Ham, via the Monty Python "Spam" song) To post irrelevant or inappropriate messages to one or more Usenet newsgroups, mailing lists, or other messaging system in deliberate or accidental violation of netiquette.

It is possible to spam a newsgroup with one well- (or ill-) planned message, e.g. asking "What do you think of abortion?" on soc.women. This can be done by cross-posting, e.g. any message which is crossposted to alt.rush-limbaugh and alt.politics.homosexuality will almost inevitably spam both groups. (Compare troll and flame bait).

Posting a message to a significant proportion of all newsgroups is a sure way to spam Usenet and become an object of almost universal hatred. Canter and Siegel spammed the net with their Green card post.

If you see an article which you think is a deliberate spam, DO NOT post a follow-up - doing so will only contribute to the general annoyance. Send a polite message to the poster by private e-mail and CC it to "postmaster" at the same address. Bear in mind that the posting's origin might have been forged or the apparent sender's account might have been used by someone else without his permission.

The word was coined as the winning entry in a 1937 competition to choose a name for Hormel Foods Corporation's "spiced meat" (now officially known as "SPAM luncheon meat"). Correspondant Bob White claims the modern use of the term predates Monty Python by at least ten years. He cites an editor for the Dallas Times Herald describing Public Relations as "throwing a can of spam into an electric fan just to see if any of it would stick to the unwary passersby."

Usenet newsgroup: news.admin.net-abuse.

See also http://www.nightflight.com/foldoc-bin/foldoc.cgi?netiquette

2. (A narrowing of sense 1, above) To indiscrimately send large amounts of unsolicited e-mail meant to promote a product or service. Spam in this sense is sort of like the electronic equivalent of junk mail sent to „Occupant".

In the 1990s, with the rise in commercial awareness of the net, there are actually scumbags who offer spamming as a „service" to companies wishing to advertise on the net. They do this by mailing to collections of e-mail addresses, Usenet news, or mailing lists. Such practises have caused outrage and aggressive reaction by many net users against the individuals concerned

Abbildung 0.8.: Quelle: http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=spam

SPAM-Nachrichten sehen im allgemeinen folgendermaßen aus:

```
Received: from [217.223.62.15] (helo=web.com)
by mx09.web.de with smtp (WEB.DE(Exim) 4.93 #56)
id 18L4iM-0001M6-00; Sun, 08 Dec 2002 17:55:34 +0100
Message-ID: <000c63e43c8e$1361a2a2$2dd66ac6@dyssus>
From: "Steffi" <steffivf406@web.com>
To: Markus
Subject: Ich habe Dich vermisst!
Date: Mon, 09 Dec 2002 01:27:32 -0900
Sender: steffivf406@web.com

Hallo,
jemand der sich in dich verliebt hat aber sich nicht traut es dir persönlich zu
sagen hat eine Foto Nachricht für dich hinterlassen.

Wenn du wissen willst wer dir eine Nachricht hinterlassen hat, so gehe auf unsere
Seite und wähle die Nachricht mit der Nummer Pt-224885 und benutze das Kennwort:
Pt-224live

Solltest du unsere Livesoftware noch nicht installiert haben, kannst du das jetzt
machen indem du auf folgenden Link klickst:

http://213.76.131.85/?account=dkm-10129&layout=layoutdp4&land=de&exename=live-software

Du wirst dann automatisch in unseren Mitgliederbereich geleitet.

Viel Spaß

SH Partnervermittlung



WERBUNG
==
JETZT NEU: Private Kontakte aus Deiner Stadt
http://66.46.145.36/members/testzugang01/
==
```

Abbildung 0.9.: SPAM-Nachrichten: Werbung

```
Return-Path: <m_bundu1@rediffmail.com>
Delivered-To:
Received: (qmail 29004 invoked by uid 4216); 8 Dec 2002 15:07:56 -0000
Received: from unknown (HELO 218.5.135.42) (218.5.135.42)
  by mail.telebel.de with SMTP; 8 Dec 2002 15:07:56 -0000
Received: from rly-xl04.mx.aol.com ([161.143.46.72]) by m10.grp.snv.yahoo.com with QMQP;
          Dec, 08 2002 6:43:00 AM -0700
Received: from 213.54.67.154 ([213.54.67.154]) by sparc.isl.net with esmtp;
Subject: Assistance
Sender: Michael Bundu <m_bundu1@rediffmail.com>

FROM: COL. MICHAEL BUNDU.
DEMOCRATIC REPUBLIC OF CONGO.
Tel No: Your country Intl. access code +8821652098236
email : mik_bundu1@rediffmail.com
Dear Sir/Madam


SEEKING YOUR IMMEDIATE ASSISTANCE.

Please permit me to make your acquaintance in so informal a manner. This is necessitated
by my urgent need to reach a dependable and trust worthy foreign partner. This request may
seem strange and unsolicited but I crave your indulgence and pray that you view it seriously.
My name is COL. MICHAEL BUNDU of the Democratic Republic of Congo and one of the close
aides to the former President of the Democratic Republic of Congo LAURENT KABILA of blessed
memory, may his soul rest in peace.

Due to the military campaign of LAURENT KABILA to force out the rebels in my country, I
and some of my colleagues were instructed by Late President Kabila to go abroad to purchase
arms and ammunition worth of Twenty Million, Five Hundred Thousand United States Dollars
only (US$20,500,000.00) to fight the rebel group. We were then given this money privately by
the then President, LAURENT KABILA, without the knowledge of other Cabinet Members. But
when President Kabila was killed in a bloody shoot-out by one of his bodyguards a day before
we were schedule to travel out of Congo, We immediately decided to put the funds into a private
security company here in Congo for safe keeping. The security of the said amount is presently
being threatened here following the arrest and seizure of properties of Col. Rasheidi Karesava
(One of the aides to Laurent Kabila) a tribesman, and some other Military Personnel from our
same tribe, by the new President of the Democratic Republic of Congo, the son of late President
Laurent Kabila, Joseph Kabila.
...
```

Abbildung 0.10.: SPAM-Nachrichten: Bitte um Unterstützung

Häufig sind sie noch darüber hinaus falsch codiert oder aber mit unsinnigen Zeitangaben der Versendung versehen. Auf jeden Fall stimmt die Absendeadresse nicht.

```
Return-Path: <Marshamaxi@id.ru>
Delivered-To:
Received: (qmail 1197 invoked by uid 4216); 8 Dec 2002 16:11:46 -0000
Received: from unknown (HELO yuwpd) (200.160.248.74)
  by mail.telebel.de with SMTP; 8 Dec 2002 16:11:46 -0000
From: Elena Palik <Marshamaxi@id.ru>
To:
Subject: Information sven.b1
Date: Sun, 08 Dec 2002 07:10:44 -0500
Mime-Version: 1.0
Message-Id: <aounwrravnxv@id.ru>

PEhUTUw+PFAgQUxJRO49Q0VOVEVSPjxGT05UICBTSVpFPTYgUFRTSVpFPTI0PjxCPnN2ZW4u
YjEsPEJSPgOKPC9GT05UPjxGT05UICBDT0xPUj0iI2ZmMDAwMCIgQkFDSz0iI2ZmZmZmZiIg
c3R5bGU9IkJBQ0tHUk9VTkQtQO9MT1I6ICNmZmZmZmYiIFNJWkU9NiBQVFNJWkU9MjQgRkFN
SUxZPSJTQU5TU0VSSUYiIEZBQ0U9IkFyaWFsIiBMQU5HPSIwIj48VT5Zb3UgaGF2ZSBiZWVu
IGFwcHJvdmVkLjxCUj4NCjwvRk9OVD48Rk9OVCAgQO9MT1I9IiNmZjAwMDAiIEJBQ0s9IiNm
ZmZmZmYiIHNOeWxlPSJCQUNLR1JPVU5ELUNPTE9SOiAjZmZmZmZmIiBTSVpFPTUgUFRTSVpF
PTE4IEZBTUlMWT0iUOFOU1NFUklGIiBGQUNFPSJBcmlhbCIgTEFORz0iMCI+PC9VPkNhc2gg
R3JhbnQgQW1vdW50OjxCUj4NCjwvRk9OVD48Rk9OVCAgQO9MT1I9IiMwMDAwZmYiIEJBQ0s9
IiNmZmZmZmYiIHNOeWxlPSJCQUNLR1JPVU5ELUNPTE9SOiAjZmZmZmZmIiBTSVpFPTcgUFRT
SVpFPTM2IEZBTUlMWT0iUOFOU1NFUklGIiBGQUNFPSJBcmlhbCIgTEFORz0iMCI+JDEwLDAw
MC0kNSwwMDAsMDAwPEJSPgOKPC9GT05UPjxGT05UICBDT0xPUj0iIzAwMDAwMCIgQkFDSz0i
I2ZmZmZmZiIgc3R5bGU9IkJBQ0tHUk9VTkQtQO9MT1I6ICNmZmZmZmYiIFNJWkU9NiBQVFNJ
WkU9MjQgRkFNSUxZPSJTQU5TU0VSSUYiIEZBQ0U9IkFyaWFsIiBMQU5HPSIwIj48ST48VT5E
aWQgWW91IEtub3c/PEJSPgOKPC9GT05UPjxGT05UICBDT0xPUj0iIzAwMDAwMCIgQkFDSz0i
I2ZmZmZmZiIgc3R5bGU9IkJBQ0tHUk9VTkQtQO9MT1I6ICNmZmZmZmYiIFNJWkU9NSBQVFNJ
WkU9MTggRkFNSUxZPSJTQU5TU0VSSUYiIEZBQ0U9IkFyaWFsIiBMQU5HPSIwIj48LOI+PC9J
```

Abbildung 0.11.: SPAM-Nachrichten: unbrauchbar, falsch codiert

Leider wird erst jetzt sehr zögerlich etwas vom Gesetzgeber und der Rechtssprechung gegen SPAM unternommen:

# US-Urteil gegen Spam-Versender

Über 98.000 US-Dollar soll der US-Amerikaner Jason Heckel für das Versenden von Spam-Mails bezahlen. Er verlor das Berufungsverfahren vor dem obersten Gericht des Staates Washington. Zuvor hatte ein Richter eine einzige E-Mail als ausreichenden Beweis für Heckels illegale Spam-Aktivitäten gewertet. Die Anklage warf Heckel vor, seit 1998 zwischen 100.000 und einer Million unerwünschte Werbesendungen pro Woche verschickt zu haben.

Die eigentliche Strafe von 2000 US-Dollar dürfte Heckel dabei kalt lassen. Schließlich soll er jahrelang pro Monat dreißig bis fünfzig Exemplare seiner 46-seitigen Online-Broschüre "How to Profit from the Internet" verkauft haben, für die er in den Mails geworben hat. Doch zusätzlich muss er nun auch Gerichtskosten von über 96.000 US-Dollar tragen. Heckels Anwalt kündigte an, das Urteil anzufechten. Gelingt ihm dies nicht, dürfte es in den USA als Präzedenzfall eine ganze Welle von Klagen gegen Spam-Versender nach sich ziehen.

Washington erließ 1998 als erster US-Bundesstaat ein E-Mail-Gesetz. Es stellt Werbe-Mails mit irreführendem Inhalt oder einer Absenderadresse, auf die man nicht antworten kann, unter Strafe. Inzwischen haben aber auch andere US-Staaten ähnliche Gesetze erlassen. Das nährt die Hoffnung, dass in den USA, von wo auch sehr viele Spam-Mails nach Deutschland kommen, bald gegen die Verursacher der Plage vorgegangen wird.

Mit der Internet-Seuche Spam befasst sich c't in der aktuellen Ausgabe 22/02 unter anderem mit Artikeln über Anwender- und Administrationstools gegen unerwünschte Werbe-Mails und einem Report darüber, wer hinter deutschsprachigem Spam steckt. (ad/c't)

Abbildung 0.12.: Quelle: heise online
`http://www.heise.de/newsticker/data/ad-20.10.02-002/`

Man beachte dabei, dass viele SPAM-Nachrichten auch HTML-Code verwenden. Dieser HTML-Code ist aber alles andere als sicher einzuschätzen, da auf dem eigenen Rechner Skripte ausgeführt werden und somit unter anderem Viren in das System eindringen können.
Gerade Newsreader wie Microsoft Outlook (Express) sind dabei besonders anfällig, da sie sich in den neueren Versionen nur noch schwer sicher konfigurieren lassen.
Bei diesen Newsreadern ist es wichtig,

1. die Vorschau zu deaktivieren (denn auch diese führt Skripte aus),
2. kein Öffnen von Nachrichten zweifelhaften Inhalts durchführen.

Gerade im Zusammenhang mit Windows-Systemen ergeben sich daneben immer häufiger Probleme mit sogenannten Dialern, d.h. Programmen, welche im Hintergrund teure 0190-Telefonnummern anwählen:

## Bundesregierung will besseren Dialer- und Spam-Schutz

Das Verbraucherschutzministerium dringt auf ein schärferes Vorgehen gegen die Dialer-Mafia. „Wir sehen die 0190-Problematik als einen Schwerpunkt dieser Legislaturperiode“, erklärte Georg Starke, Leiter des Referats für den wirtschaftlichen Schutz der Verbraucher im Hause von Ministerin Renate Künast, am heutigen Donnerstag am Rande einer Konferenz zur europaweiten Harmonisierung des Wettbewerbsrechts in Berlin. Die zweite Änderung der Telekommunikations-Verbraucherschutzverordnung, die Netzbetreiber zum Einrichten kostenloser Service-Nummern verpflichtet und von vielen Seiten als unzweckmäßig kritisiert wurde, sei nur „ein erster Schritt“ gewesen. Weiter gehende Schutzmaßnahmen sollen laut Starke in die anstehende und von der Branche mit Spannung erwartete Novelle des Telekommunikationsgesetzes (TKG) einfließen, für die das Wirtschaftsministerium federführend verantwortlich ist.

Wie groß das Problem mit der Abzocke über 0190-Dialer im Internet oder der Werbespam für 0190-Nummern per SMS und E-Mail ist, erfährt das Verbraucherministerium ständig am eigenen Leib. „Wir erhalten täglich unzählige Eingaben und Beschwerden zu diesem Thema“, sagte Starke. „Sie pflastern uns den Schreibtisch zu.“ Momentan prüfe sein Haus noch zusammen mit dem Wirtschafts- und Justizressort, wie der Missbrauch effektiv einzudämmen ist. Konkret kann sich der Ministerialbeamte vorstellen, „verstärkt die Regulierungsbehörde für Telekommunikation und Post in die Verantwortung zu nehmen“ und so den schwarzen Schafen unter den Anbietern zu Leibe zu rücken. Bisher sind diese von den Netzbetreibern oft nur schwer zu ermitteln; eine effektive Datenbank mit einer Übersicht über die einzelnen 0190-Dienstleister existiert nicht.

Auch im Bereich E-Mail-Spam sieht Starke Handlungsbedarf. „Bisher sind die ungewünschten Werbezusendungen nicht im Telekommunikationsgesetz erfasst“, bemängelt der Regierungsvertreter. Auch hier will das Verbraucherschutzministerium im Laufe der TKG-Novelle nachbessern. Ein großes Problem sieht Ursula Pachl vom Bureau Européen des Unions de Consommateurs, dem Dachverband der europäischen Verbraucherschutzorganisationen, allerdings nach wie vor bei internationalen Spam-Versendern, hauptsächlich aus den USA. Mit den Partnerschaftsverbänden jenseits des Atlantiks arbeite ihre Institution an einer Lösung. Über „Selbstregulierungsmaßnahmen“ der Wirtschaft gehen die Überlegungen bislang aber nicht hinaus.

Für die deutschen Wahrer der Konsumentenrechte ist die gesamte Thematik Spam und 0190-Nummern im vergangenen Jahr zum Dauerärgernis geworden. „Wir erleben einen zunehmenden Wildwuchs in der Werbung, der sich vor allem durch die Neuen Medien ergibt“, sagt Edda Müller, Vorstand Verbraucherzentrale Bundesverband (VZBV). Immer mehr Firmen würden teure 0190-Nummern verwenden, um bei den Verbrauchern „in wettbewerbswidriger Weise abzukassieren“. Zahlreiche Fälle seien aus der Gewinnspielwerbung bekannt oder im Zusammenhang des vermeintlichen „Abbestellens“ von unerwünschten kommerziellen Faxen.

xx

Abbildung 0.13.: Quelle: heise online
http://www.heise.de/newsticker/data/jk-31.10.02-006/

Der Konsument sei dagegen größtenteils machtlos, da sich die Möglichkeiten für Abmahnungen und Unterlassungserklärungen im Gesetz gegen den unlauteren Wettbewerb (UWG) als „zahnlos“ erweisen hätten. Selbst wenn eine Firma eindeutig eines Verstoßes gegen das UWG überführt worden sei, könnten die betroffenen Verbraucher keine Schadensersatzansprüche einklagen. Eine entsprechende Vorkehrung wollen die Verbraucherschützer nun aber im Rahmen der in Brüssel in den nächsten Wochen anstehenden Verhandlungen zur Harmonisierung des europäischen Wettbewerbrechts und des Grundbuchs zum Verbraucherschutz für alle Mitgliedsländer fordern. Eine „Strohmannklausel“ soll ferner verhindern, dass zwielichtige Anbieter unter Postfachadressen auf dem Markt auftreten können.

Mit der Internet-Seuche Spam befasst sich c’t in der Ausgabe 22/2002 unter anderem mit Artikeln über Anwender- und Administrationstools gegen unerwünschte Werbe-Mails und einem Report darüber, wer hinter deutschsprachigem Spam steckt. (Stefan Krempl) / (jk/c’t)

Abbildung 0.14.: Quelle: heise online Fortsetzung
`http://www.heise.de/newsticker/data/jk-31.10.02-006/`

## Regierung legt Gesetzentwurf gegen 0190-Missbrauch vor

Die Bundesregierung hat einen ersten Referentenentwurf für das neue „Gesetz zur Bekämpfung des Missbrauchs von Mehrwertdiensterufnummern“ vorgelegt. Kernstück ist die geplante Änderung des Telekommunikationsgesetzes (TKG). Ein neuer Paragraf 43a soll jeden Anbieter, der eine 0190- oder 0136-0138-Nummer zur Nutzung überlassen bekommen hat, dazu verpflichten, eine ladungsfähige Anschrift bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) zu hinterlegen.

Die RegTP selbst soll diese Angaben in Form einer Datenbank im Internet der Öffentlichkeit zugänglich machen. Außerdem soll jedermann einen Anspruch darauf haben, die Daten telefonisch erfragen zu können. Bei Verstoß gegen die Meldepflicht „kann die Zuteilung der Rufnummer durch die Regulierungsbehörde widerrufen werden“, heißt es im Gesetzentwurf. Von weiteren Sanktionierungsmaßnahmen wie etwa der Verhängung eines Bußgeldes findet sich, anders als noch im Konzeptpapier, nichts mehr im Gesetzentwurf.

Bei der Preiskappungsgrenze ist das Bundesministerium für Wirtschaft und Arbeit (BMWA) dagegen sogar noch weiter gegangen: Die Kosten für eine über frei tarifierbare Rufnummern abgerechnete Einwahl sollen demnach 30 Euro künftig nicht überschreiten dürfen. Vorgesehen waren hier zunächst 120 Euro pro Anruf. Wird entsprechend der Länge der Verbindung abgerechnet, soll das Entgelt auf zwei Euro pro Minute begrenzt werden. Abgerechnet werden soll mit einem Takt von einer Länge von maximal 60 Sekunden.

Hintergründe, erste Reaktionen und Einschätzungen zu dem Gesetzentwurf gegen 0190-Missbrauch finden sich im Artikel auf c’t aktuell:

Erster Gesetzentwurf gegen 0190-Missbrauch
`http://www.heise.de/ct/aktuell/data/hob-18.12.02-000/`

(hob/c’t)

Abbildung 0.15.: Quelle: heise online
`http://www.heise.de/newsticker/data/hob-18.12.02-001/`

## Spam auf dem gerichtlichen Prüfstand

Der Heise-Zeitschriften-Verlag, der die Zeitschriften iX und c't, das Online-Magazin Telepolis und den Newsdienst auf heise online herausgibt, klagt vor dem Amtsgericht Hannover gegen die Firma Online-Marketing Albrecht, nachdem diese Verlagsmitarbeiter trotz einer Unterlassungsaufforderung weiterhin mit Spam-E-Mails bombardiert hatte. Dabei beruft sich der Verlag unter anderem auf die neue EU-Datenschutzrichtlinie, in der für E-Mail-Werbung ein klares „Opt-in" bestimmt wird. Diese Richtlinie ist bis zum 31. Oktober 2003 in nationale Gesetzgebung umzusetzen, sollte aber bereits jetzt Einfluss auf die deutsche Rechtsprechung haben.

Unter dem Namen „emailfuchs" versendet Bernd Albrecht in Wellen unverlangt Werbe-E-Mails an deutsche Adressen. In den Newslettern wird für Webshops, beispielsweise einen Berufsbekleider und einen Uhrenhändler, geworben. Als auch Mitarbeiter von heise online solche E-Mails erhalten hatten, forderte Heise Online-Marketing-Albrecht unter Fristsetzung auf, den unerbetenen Versand solcher Werbe-Mails zu unterlassen. Kurz danach liefen erneut Albrecht-Newsletter bei uns auf. Anstatt die entsprechende strafbewehrte Unterlassungserklärung zu unterschreiben und die Adressen des Verlages aus seinem Verteiler zu streichen, konterte Albrecht mit harsch formulierten E-Mails an den Verlag.

Der überzeugte Spammer hält es für rechtmäßig, unverlangte Werbe-E-Mails zuzusenden. Und: „Sie werden es nicht schaffen, unseren kostengüstigen und schnellen Newsletter-Versand an Millionen Leser zu blockieren", gab er sich kampfbereit. „Denken Sie daran, dass unsere Auflage weit höher ist als ihre", schrieb Albrecht und sprach von einer Pressekampagne mehrerer Verlage gegen ihn. Albrecht rechtfertigte sein Tun unter anderem unter ökologischen Gesichtspunkten: „Im Gegensatz zu den Printmedien müssen für unsere Informationen keine Bäume vernichtet werden, um eine Zeitung mit viel Werbung drucken zu müssen."

Nach Ansicht von Joerg Heidrich, Justiziar des Heise-Verlags, hat Albrecht freilich wenig Chancen, sein zweifelhaftes Anliegen vor Gericht durchzusetzen. Bis auf wenige Ausnahmen sei man inzwischen in Rechtssprechung und juristischer Literatur einhellig der Meinung, dass die unerwünschte und unaufgeforderte Zusendung von E-Mails rechtswidrig sei. Das Versenden solcher Nachrichten gegenüber Privatpersonen gilt dabei meist als Verletzung des allgemeinen Persönlichkeitsrechts des Betroffenen.

Unternehmen und Gewerbetreibende können sich auf einen Eingriff in den sogenannten „eingerichteten und ausgeübten Gewerbebetrieb" nach §§823, 1004 BGB berufen und ebenfalls Unterlassung verlangen. Ist der Empfänger der Spam-Mail darüber hinaus noch in einem ähnlichen Bereich gewerblich tätig wie der Versender, so steht ihm zusätzlich ein wettbewerbsrechtlicher Unterlassungsanspruch aus §1 UWG zu. Ein Anspruch auf Schadensersatz bei den Empfängern besteht dagegen nach bisheriger Rechtsprechung nicht. Insbesondere aufgrund der neuen EU-Richtlinie, die hinsichtlich unverlangter Werbezusendungen erstmals ein klares Verbot ausspricht, sieht Heidrich sehr gute Aussichten für die eingereichte Klage. (hob/c't)

Abbildung 0.16.: Quelle: heise online
`http://www.heise.de/newsticker/data/hob-04.12.02-000/`

# EU-Richtlinie zum Datenschutz in Kraft

*[01.11.2003 10:40 ]*

Seit dem gestrigen Freitag haben Spammer es in Europa mit einer neuen Rechtslage zu tun: Nunmehr ist das Versenden von unverlangten E-Mails oder SMS-Botschaften in der gesamten **Europäischen Union[1]** illegal.

Die seit gestern geltende **Datenschutzrichtlinie[2]** für elektronische Kommunikation legt europäische Normen für den Schutz personenbezogener Daten und der Privatsphäre in der elektronischen Kommunikation fest. Sie enthält grundlegende Verpflichtungen, die die Sicherheit und Vertraulichkeit der Kommunikation über elektronische Netze in der EU gewährleisten sollen. Dies betrifft auch das Internet und mobile Dienste.

Insbesondere führt die Richtlinie ein EU-weites Spam-Verbot ein: Sofern sie nicht der Aufrechterhaltung einer bestehenden Kundenbeziehung dient, ist E-Mail-Werbung nur mit vorheriger Einwilligung der Adressaten gestattet. Vorgetäuschte Absender und ungültige Rückadressen, wie Spam-Versender sie häufig verwenden, sind verboten. Das Erfordernis einer verbindlichen vorherigen Einwilligung ("Opt-in") gilt ebenfalls für SMS-Botschaften und andere elektronische Nachrichten, die an ein mobiles oder festes Endgerät gesendet werden. Die EU-Mitgliedstaaten können auch unerbetene elektronische Werbepost an Unternehmen verbieten.

Des weiteren dürfen unsichtbare Verfahren der Nachverfolgung, mit denen Informationen über Internetnutzer gesammelt werden können, nur verwendet werden, wenn der Nutzer deutliche Informationen über den Zweck einer solchen unsichtbaren Aktivität und das Recht erhält, diese abzulehnen. Das betrifft etwa sogenannte Spyware, aber auch den Einsatz von Cookies.

Standortdaten, die von Mobiltelefonen erzeugt werden, dürfen vom Netzbetreiber nur mit ausdrücklicher Einwilligung des Nutzers weiterverwendet oder weitergegeben werden. Einzige Ausnahmen betreffen die Übermittlung der Standortdaten an Notdienste sowie an Strafverfolgungsbehörden. Für letztere gelten strenge Voraussetzungen - sie dürfen solche Daten nur anfordern, sofern dies Zwecken der nationalen Sicherheit oder Ermittlungen in Strafrechtssachen dient.

Ab heute müssen die Mitgliedstaaten diese Regeln anwenden und wirksam durchsetzen. Die Richtlinie enthält jedoch keine rechtsverbindlichen Bestimmungen, die Maßnahmen der Mitgliedstaaten gestatten oder verhindern würden, welche die Speicherung von Verkehrs- oder Standortdaten für Strafverfolgungszwecke erfordern, da dies außerhalb ihres Geltungsbereichs liegt. Doch müssten solche Maßnahmen mit Vorkehrungen zum Schutz der Menschenrechte einhergehen, die in der Richtlinie ausgeführt werden.

Eine unmittelbare Rechtwirkung für die betroffenen Unternehmen und Bürger ergibt sich allerdings aus der EU-Richtlinie nicht. Diese richtet sich zunächst nur an die Mitgliedsstaaten, welche die Regelungen in nationales Recht umzusetzen haben. Dies hat die Bundesregierung bis zum gestrigen Stichtag allerdings versäumt. Geplant ist eine nationale Umsetzung der Richtlinie im Rahmen der Reform des Wettbewerbsrechts (UWG), welche jedoch nicht vor dem nächsten Frühjahr zu erwarten ist. Nach der derzeitigen **Planung[3]** enthält jedoch auch das neue UWG keine direkte

Abbildung 0.17.: E-Mail: Maßnahmen gegen SPAM in der EU

**Was tun gegen Spam(`http://spam.trash.net/was.shtml`)?**

Unter http://spam.trash.net/tun.shtml ist erläutert, wie Sie Spam in Zukunft vermeiden können, was Sie tun können, wenn Sie bereits spam erhalten haben, ...

- Auf keine Fall sollten Sie den Aufforderungen der Spam-Nachrichten nachkommen.
- Die Spam-Nachrichten sollten sofort gelöscht werden. Bei nur wenigen Nachrichten reicht oft noch das manuelle Löschen.
- Da die Spam-Mails immer mit neuen Absenderadressen auftauchen, helfen Einträge in lokale Filterlisten oft sehr wenig. Bei der Filterung nach Stichworten (z.B. Sex, Porno, etc.) werden leider auch gerne reguläre e-mails ausgefiltert. ...

**Filtern im Netscape-Communicator:**

- Eine Netscape Filterbeschreibung finden Sie unter
  http://www.pvc.maricopa.edu/cc/training/faqs/memo/filters.htm.
- Für Outlook Express vergleiche http://www.inboxprotector.com/.

**Weitere Informationen finden Sie zum Beispiel unter:**

- SPAM-Klassifikator der Uni-Wuppertal:
  http://www.hrz.uni-wuppertal.de/dienste/netz/email/spam/spam-filter.html
- http://www.antispam.de/
- Information zum Thema Spam
  (`http://spam.trash.net/index.shtml`)
- DFN-CERT Informationsbulletin Spam
  (`http://www.cert.dfn.de/infoserv/dib/dib-9901.html`)
- Ratgeber Kampf gegen Spam
  (`http://www.wienerzeitung.at/aktuell/2001/antispam/default.htm`)
- HRZ-Anti-Spam an der BU Wuppertal
  (`http://w3.uni-wuppertal.de/hrz/dienste/netz/email/spam.html`)
- Junk Mail und SPAM
  (`http://w3.uni-wuppertal.de/hrz/infos/hrz-info/hrz-info-9806/node16.html`)
- Spam (Auflistung von anderen Spam-Seiten)
  (`http://directory.google.com/Top/Computers/Internet/Abuse/Spam/`)

- Reading Email Headers
  (http://www.stopspam.org/email/headers/headers.html)
- Uni Bremen: Maßnahmen gegen SPAM
  (http://www.zfn.uni-bremen.de/zfn/dienste/mail/anti-spam.php3 )
- http://www.schnappmatik.de/TFFFFF/
- Uni Köln: Electronix Mail am RRZK: Spam
  (http://www.uni-koeln.de/rrzk/mail/spam/)
- Uni Köln: Spamassassin am RRZK
  (http://www.uni-koeln.de/rrzk/mail/spam/spamassassin.html)

## Gericht untersagt den Versand unverlangter Newsletter-Aktivierungsmails

Nach den Anbietern von Grußkarten könnte es nun auch den Versendern von Online-Newslettern an den Kragen gehen. Nach Auffassung des Landgerichts Berlin stellt die unerwünschte Übersendung einer Newsletter-Anmeldung per E-Mail eine unzulässige Werbung dar.

Der Antragsteller des Beschlusses vom 19. September 2002 hatte eine E-Mail erhalten, in der er aufgefordert wurde, einen Aktivierungslink anzuklicken, um in einen Newsletter-Verteiler aufgenommen zu werden. Sofern er dies nicht wolle, solle er die Mail einfach löschen. Hierin sah der Antragsteller unerwünschte Werbung und beantragte den Erlass einer einstweiligen Verfügung gegen den Betreiber des Informationsservices.

Das Landgericht bestätigte in seiner Entscheidung nochmals die mittlerweile herrschende Auffassung, dass es sich bei dem unaufgeforderten Zusenden einer E-Mail mit Werbeinhalten gegenüber Gewerbetreibenden um einen unzulässigen Eingriff in den Gewerbebetrieb handelt. Privatpersonen steht unter den Gesichtspunkten des allgemeinen Persönlichkeitsrechts gegen den Versender der Mail ebenfalls ein Unterlassungsanspruch nach §§1004, 823 Abs. 1 BGB zu.

Die Einwendung des Newsletter-Betreibers, der Antragsteller hätte die Eintragung für die Mailingliste selbst vorgenommen, ließ das Gericht nicht gelten. Nachweispflichtig für die Eintragung in eine Liste sei stets der Betreiber des Angebotes. Diesen Beweis konnte der Anbieter jedoch nicht führen. Der Beschluss ist unter Juristen umstritten. Die der Entscheidung zugrundeliegende Art des Opt-In-Verfahrens bei der Anmeldung zum Bezug eines Newsletters ist im Internet weit verbreitet und galt bisher als rechtlich unbedenklich. (Joerg Heidrich) / (em/c't)

Abbildung 0.18.: Quelle: heise online
`http://www.heise.de/newsticker/data/em-02.11.02-000`

## Spam-Versender muss sieben Millionen Dollar zahlen

**AOL ist vor einem Gericht in Virginia ein wegweisendes Kunststück gelungen: Erfolgreich klagte das Unternehmen einen pornografischen Spam-Versender in den Bankrott. Das Urteil, hoffen Millionen, könnte Schule machen.**

CN Productions kennt niemand, und doch haben Millionen Internet-Nutzer schon Post des Unternehmens im E-Mail-Empfangsordner gehabt. CN machte seine Profite mit Spam, unverlangt zugesandten Werbebotschaften. Das Unternehmen des bereits 1999 einschlägig verurteilten Jay Nelson gehörte zu den Pionieren des wohl meistgehassten Geschäftszweiges im Internet: pornografische Massenmailings.

Zum wohl endgültigen Verhängnis wurde Nelsons Firma nun ein Gesetz des US-Staates Virginia, das als Muster für den zunehmend härter geführten juristischen Kampf gegen die Müllversender gilt: Wegen Verstoßes gegen Auflagen des ersten Urteils wurde CN Productions zur Zahlung von sieben Millionen Dollar an AOL als geschädigtes Unternehmen verurteilt. Für den Pornowerber ist das der Ruin, und doch ist es fast ein mildes Urteil: Das Gesetz des Staates Virginia sieht Geldstrafen von bis zu 25.000 Dollar für einen Spambrief vor. Davon verschickte CN Productions allein an AOL-Adressen mehrere Milliarden.

Für AOL ist das ein wichtiger Sieg, von dem das Unternehmen erhofft, dass er Signalwirkung haben möge. AOL litt über Jahre unter dem Ruf, einerseits Heimat von Spam-Versendern zu sein, anderseits die eigenen User nicht davor schützen zu können.

Das Problem sind die E-Mail-Verzeichnisse von AOL, die von Spamern immer wieder gern „abgefischt“ werden: Mehr verifiziert gültige Adressen lassen sich kaum auf einen Schlag besorgen. Nutzer von AOL oder auch des Instant Messenger AIM konnten ein Lied davon singen: Es rappelte im Postfach. Heute dagegen liegt das AOL-Spam-Aufkommen sogar unter dem Durchschnitt. Der liegt - je nach Schätzung - mittlerweile bei 25 bis 50 Prozent.

AOL geht seit spätestens 1998 vehement gegen Spamer und ihre Aussendungen vor: „Wir haben die Schnauze so voll davon wie unsere Kunden“, sagte damals AOL-Chef Steve Case - und topfte ein Programm von Gegenmaßnahmen ein, die von Filtern über Rausschmisse und gerichtliche Klagen bis hin zu öffentlichen Prangern reichte. Schon 1998 landete CN Productions auf der AOL-Liste der zehn „meistgesuchten Spamer“. Vier Jahre später hat AOL seinen Peiniger erlegt, das Kopfgeld kassiert.

Abbildung 0.19.: Quelle: Spiegel Online
`http://www.spiegel.de`

## IETF gründet Anti-Spam-Arbeitsgruppe

Die Internet Engineering Task Force (IETF), eine der bedeutendsten Organisationen für Internet-Standards, will das Problem der immer größer werdenden Flut an unerwünschten E-Mails jetzt an der Wurzel packen: Im Rahmen des Forschungszweigs der IETF wurde eine Arbeitsgruppe namens Anti-Spam Research Group (ASRG) gegründet.

Bestehende Anti-Spam-Lösungen setzen nach Ansicht der ASRG-Mitglieder zu spät an, nämlich erst dann, wenn eine unerwünschte Nachricht bereits auf dem Server des Empfängers angekommen ist. Ziel der jetzt begonnenen Forschungen ist zunächst eine Machbarkeitsstudie, in der geprüft werden soll, ob man solche Nachrichten nicht bereits im Vorfeld unterdrücken und so auch die Netzwerk-Belastung verringern kann. Erreichen will man das mit einem Satz an Protokollen und Frameworks unter dem Stichwort „consent-based communication“ (zustimmungsbasierte Kommunikation). So sollen potenzielle Nachrichtenempfänger in die Lage versetzt werden festzulegen, welche Art von Mitteilungen sie überhaupt empfangen wollen. Dazu soll auch eine Möglichkeit gehören, Absender von Nachrichten zu identifizieren, die sich solchen Übereinkünften widersetzen.

Die Mitglieder der ASRG wollen sich zum ersten Mal im Rahmen des 56. IETF-Meetings zusammensetzen, das vom 16. bis zum 21. März dieses Jahres in San Francisco stattfindet. Wann mit ersten Ergebnissen zu rechnen ist und ob die Arbeit in einem offiziellen Standard münden wird, ist noch völlig offen. (hos/c't)

Abbildung 0.20.: Quelle: heise online
`http://www.heise.de/newsticker/data/hos-01.03.03-000/`

## Künast: Schärferes Gesetz gegen Spam im Herbst

Eine Art große Koalition bildet sich gegen unverlangt eingesandte Werbe-Mail und ihre Versender heraus: Nachdem CDU/CSU bereits forderte, Spammer zur Kasse zu bitten und die SPD am vergangenen Freitag „Wege aus der Vermüllung“ suchte, geht Verbraucherschutzministerin Renate Künast (Grüne) mit Ankündigungen neuer Gesetzesinitativen in die Öffentlichkeit. Die Versender unerwünschter Werbe-Mails im Internet müssen sich auf drastische Gegenmaßnahmen einstellen, verspricht Künast. Im Herbst werde der Bundestag eine Gesetzesverschärfung beschließen, wonach E-Mail-Werbung nur noch mit vorheriger Zustimmung des Empfängers verschickt werden darf, sagte der Berliner Zeitung. Gewinne, die unter Verstoß gegen diese Bestimmung erzielt werden, könnten dann bei dem betroffenen Unternehmen eingezogen werden.

Künast setzte sich ebenfalls für internationale Vereinbarungen gegen so genannte Spam-E-Mails ein. „Das könnten zum Beispiel Mindeststandards für Provider sein“, sagte Künast. „Es ist ein klassischer Dienst am Kunden, unverlangte E-Mails auszufiltern.“ Nur Anbieter mit einem solchen Service würden sich langfristig am Markt halten können.

Künast reagiert mit der Ankündigung des neuen Gesetzes allerdings nur auf bereits beschlossene EU-Regelungen: Die Europäische Union hat bereits vor einem Jahr eine Richtlinie gegen Spam erlassen. Darin wird eine Opt-in-Regelung verlangt. „Die Bekämpfung des Spammings geht uns alle an und ist mittlerweile zu einem Hauptaspekt des Internet geworden“, hatte Erkki Liikanen, EU-Kommissar für die Informationsgesellschaft, betont, als er die EU-Staaten daran erinnerte, dass sie bis Ende Oktober die Richtlinie in nationales Recht umzusetzen müssten. (jk[7]/c't)

Abbildung 0.21.: Quelle: heise online
`http://www.heise.de/newsticker/data/jk-21.07.03-000/`

**Intranet, Extranet, Internet als Intranet, VPNs**
Bitte klären Sie die obigen Begriffe mit Hilfe von

FOLDOC (`http://www.nightflight.com/foldoc-bin/foldoc.cgi`).

**Eine Web-Firmenpräsentation**
Das Web stellt vielfältige Informationen benutzerfreundlich zur Verfügung.
Wir wollen uns typische Inhalte einer „Firmenpräsentation“ an Hand der Webseiten des Fachbereichs Mathematik der Universität Wuppertal genauer ansehen:
Wichtig ist neben einer klar gegliederten Webangebotsübersicht das Impressum, bestehend aus einem email-Link

`mailto:webmaster@math.uni-wuppertal.de`,

sowie der Postadresse inklusive Telefon-, Fax- und email-Adresse.

## Impressum einer Homepage muss gut auffindbar sein

Das Impressum auf einer Homepage muss gut auffindbar und schnell zu erkennen sein. Das geht aus einem Beschluss des Landgerichts Hamburg hervor (Az.: 416 O 94/02), über den die Zeitschrift Verbraucher und Recht in der Ausgabe 11/2002 berichtet. So müsse das nach Paragraf 6 des Teledienstegesetzes vorgeschriebene Impressum auf der Startseite auch eindeutig gekennzeichnet werden.

In dem verhandelten Fall hatte ein Anbieter von Edutainment-Software das Impressum auf seiner Homepage unter dem Unterpunkt „Backstage“ geführt. Dagegen hatte ein Konkurrenzunternehmen Beschwerde eingelegt mit der Begründung, die Bezeichnung aus der Bühnensprache sei nicht allgemein geläufig. Der Rechtsstreit wurde beigelegt, nachdem das beklagte Unternehmen sich verpflichtete, die Angaben zu Namen und Anschrift des Anbieters künftig als „Impressum/Infos“ zu kennzeichnen.
(dpa) / (anw/c’t)

Abbildung 0.22.: Quelle: heise online
`http://www.heise.de/newsticker/data/anw-21.11.02-003`

## Verstoß gegen Web-Impressumspflicht wettbewerbswidrig

Ein Verstoß gegen die Kennzeichnungspflicht auf Websites nach §§3, 6 des Teledienstegesetzes (TDG) ist wettbewerbswidrig im Sinne der §§1 und 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Dies entschied das Landgericht Düsseldorf nach Berichten von Jur-Text und erließ am 7. und 25. November zwei entsprechende einstweilige Verfügungen (Az. 34 O 172/02, Az. 34 O 188/02).

Die Frage, ob die Regelungen des neuen TDG einen Verstoß gegen Wettbewerbsrecht begründen können, war bislang zwischen Juristen umstritten. Die 12. Kammer des Landgerichts Düsseldorf (Az. 12 O 311/01) sowie das Landgericht Hamburg (Az. 312 O 512/00) hatten eine solche Haftung noch mit der Begründung abgelehnt, die Regelungen des TDG über die Impressumspflicht stellten eine reine Ordnungsvorschrift da, die keinen wettbewerbsrechtlichen Charakter habe. Diese Entscheidungen bezogen sich jedoch noch auf das alte TDG, in dem die Impressumspflichten wesentlich weniger umfangreich festgelegt waren.

Nach Ansicht der Kammer für Handelssachen des Landgerichts Düsseldorf dienen die neugestalteten Vorschriften des TDG jedoch dem Kunden- und Mitbewerberschutz. Ein Verstoß gegen die Regelungen unterfällt demnach als „Vorsprung durch Rechtsbruch“ dem UWG. Nach Auskunft von Rechtsanwalt Tim Geißler war in einem der vorliegenden Fälle ein Impressum zwar als „Kontakt“ grundsätzlich vorhanden, es fehlten jedoch die ordnungsgemäße Bezeichnung des Unternehmens, die Angabe des Geschäftsführers, die notwendigen Angaben zur Handelsregistereintragung sowie die Angabe der Umsatzsteueridentifikationsnummer, die in § 6 TDG festgelegt sind. Ob gegen die Beschlüsse Rechtsmittel eingelegt werden, steht derzeit noch nicht fest.

Die Neuregelung des der Kennzeichnungspflichten des TDG war in den vergangenen Monaten die Grundlage für zahlreiche, zum Teil äußerst fragwürdige Serienabmahnungen. Jüngst hatte das LG Hamburg bereits eine auf einem Verstoß des TDG beruhende Abmahnung bestätigt. Website-Betreiber sind in jedem Fall gut beraten, ihre Online-Präsenz noch einmal kritisch auf eine korrekte Kennzeichnung zu überprüfen. (Joerg Heidrich) / (jk/c't)

Abbildung 0.23.: Quelle: heise online
`http://www.heise.de/newsticker/data/jk-26.11.02-005`

Daneben ist die Verfügbarkeit einer lokalen „Suchmaschine“ für den Inhalt des Firmen-Webauftritts bei einem größeren Informationsangebot schon fast Usus.

Ein Bereich der Homepage für (aktuelle) Neuigkeiten (eventuell durch dynamische Effekte hervorgehoben) solle nicht zu groß sein. Schließlich ist die Angabe des Datums der letzten Änderung der Seite sehr empfehlenswert. Dies sollte automatisch aus den Modifikationsdatum der zugehörigen Datei im Filesystem des Webservers geschehen, was zum Beispiel mittels der folgenden JavaScript-Funktion geschehen kann!

Listing 1: Letzte Änderung

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
<base href="http://www.math.uni-wuppertal.de/">
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<TITLE> Testseite
</TITLE>
</HEAD>

<body bgcolor=white>

<!-- ------------------------------------------------ -->

<noscript>
 <p><h3>   This page uses Javascript. Please enable Javascript
    features in your browser.</h3>
</noscript>


<script language="JavaScript" type="text/javascript">
<!-- hide to non JavaScript browsers
function ModDate()
{
lastmod = self.document.lastModified // last modified date
while (isNaN(lastmod.substring(0,1))) { lastmod = lastmod.substring(1,100) }
// delete Mo..So
return lastmod
}

window.status='Document last modified: '+ModDate();
// -->
</script>

<p>Dies ist meine Web-Testseite!
</p>

<hr>
<p>Hans Mustermann; </p>
<script type="text/javascript">
<!-- hide to non JavaScript browsers
document.writeln('Letztes Modifikationsdatum: ', ModDate());
// -->
</script>

<a href="http://validator.w3.org/check/referer"><img border="0" src="http://www.math.
    uni-wuppertal.de/images/valid-html401.gif"
alt="W3C HTML 4.01 checked" height="31" width="88" align="right">
</a>

</body>
</html>
```

**Bemerkungen:**

- Web-Seiten sollten syntaktisch korrekt sein;

  vergleiche 
  
  .

- **Beachte:** Webseiten werden für eine Vielzahl von Lesern entwickelt nicht für bestimmte Browser! Man benutze deshalb nur solche HTML-Eigenschaften, die „überall“ funktionieren.

- Der Fußbereich unter der horizontalen Linie der Fachbereichs-Homepage (`http://www.math.uni-wuppertal.de`) enthält einige Links, die früher einmal im Bereich Neuigkeiten angeboten wurden.

- Sprachvarianten (deutsch/englisch/...) können durch „Flaggen“ umschaltbar angeboten werden oder mit Hilfe des in `http 1.1` vorhandenen Inhaltsvarianten-„Verhandlungssystems“ (http://httpd.apache.org/docs/content-negotiation.html und http://www.apacheweek.com/features/negotiation) gesteuert werden.

**Typische Inhalte eines Webauftritts:**

Auf den Seiten des Fachbereichs Mathematik (`http://www.math.uni-wuppertal.de`) der Bergischen Universität Wuppertal (`http://www.uni-wuppertal.de`) werden folgende Informationen dargestellt:

- Selbstdarstellung
  - Organisation (Dekanat, Prüfungsämter, Fachbereichsrat, Fachschaft, ...)
  - Organisatorische Unterbereiche (Labore, Institute,...)
  - „Verwandte“ Organisationen/Organisationseinheiten
  - Tipps für Studieninteressierte
  - Tipps für Besucher/Gäste
- Personalverzeichnis
  - Listen mit Telefonnummern, email-Adressen, Web-Homepages, ...
  - email-Aliases für Verteilerlisten
  - Listen mit Rollen-Aliases (dekan, dekanat)
  - Liste der e-mail Adressen der Studenten
- Termine
- Mitteilungen/schwarzes Brett
- Dienstleistungen
  - DV-Dienstleistungen per Web für Mitglieder des FBs,... (Anforderungen von Formularen, Änderung der Daten im Personalverzeichnis, ...)
- Forschung
  - Forschungsgruppen
  - Preprints
  - Promotionen
  - Software
- Lehre
  - Studiengänge
  - Prüfungsordnungen/Studienordnungen
  - Vorlesungsverzeichnisse

  - Projekte/Praktika
- Links
  - Rechenzentrum
  - Bibliothek
  - Fachinformationszentren
  - ...

Aufgabe: Erstellen Sie ein Analogon für eine Firmenpräsentation.

**Weitere Dienste im Internet:**

- **e-mail mit Sondermerkmalen:**
  - normal
  - mit Vesandtvermerk (Priorität,...)
  - mit Unterschrift („Selbstbeglaubigung“)
  - verschlüsselt für ...
  - verschlüsselt für ... und mit Unterschrift
  - mit Rückschein (Empfangsbestätigung)
    - ▷ Bestätigung des Empfangs im Ziel-Emailserver
    - ▷ Bestätigung des Betrachtens im Ziel-Email-Client
  - Absenderangaben
    - ▷ `~/.signature` Text
    - ▷ `text/x-vcard` Visitenkarten
- **e-mail Adressbücher**
  - Netscape Adressbuch oder `wab` (Windows address book):
    - ▷ lokale Adressbücher
    - ▷ LDAP-Directories, z.B.

      FB7-Studenten
      `wmit00.it.math.uni-wuppertal.de`
      `ou=students,ou=math,o=uni-wuppertal,c=de`
    - ▷ Web-Gateways für LDAP-Server, z.B.

      `http://wmit00.it.math.uni-wuppertal.de:1760/ou=math,o=uni-wuppertal,c=de`

      bzw.

      `http://sites.inka.de:8002/web2ldap/` mit

      `wminf0.math.uni-wuppertal.de`
      `ou=math,o=uni-wuppertal,c=de`
- **e-mail Aliases**
  - lokal als Spitznamen (nur für User)
  - lokal als Verteilerlisten (nur für User)
  - nichtlokal für Rollennamen, Spitznamen, Verteilerlisten in `/etc/aliases` (für alle User eines Rechners bzw. nichtlokal)
  - nichtlokal auf Mailservern

- **Usenet News-Gruppen**
  - Diskussionsforen wie z.B.
    news:de.answers
    news:de.newusers.questions
    news:de.newusers.infos
    news:news.answers
    news:news.newusers.questions
    news:news.announce.newsgroups
- **Nachschlagewerke und Suchmaschinen**
  - http://www.google.com
    für die Suche nach Bildern, Dokumenten, Newsnachrichten, ...
  - http://sdb.suse.de
    als Servicedatenbank für das Suse-Linux-Betriebssystem
  - http://www.teleauskunft.de
    für Telefon- und Faxnummern
  - http://www.telekom.de
    für online verfügbare Handbücher zur T-NetBox, von Telefonanlagen, ...
  - http://www.hp.com
    für neueste Drucker, Druckertreiber, ...
  - http://www.Matheprisma.de/Module/
    für Online-Lerneinheiten zur Mathematik.
  - und viele andere mehr
- **Applikationsserver**
  - X-Window unter Unix auf einem entferneten –remote– Rechner mitbenutzen

    ```
    ssh -X rechner.de -l username
    ```

    für remote Login bzw.

    ```
    X :1 -query rechner.de -once&
    ```

    für die Benutzung des Display-Servers von rechner.de (der eigene Rechner ist nur X-Terminal)
  - Windows-Server mit Terminalserver-Software von Microsoft/Citrix

    ```
    wfcmgr&
    ```
- **Firmennetze mit dem Internet als Transportmedium**
  - VPN (virtual private net)
  - MobileIP

# 1. Internetnutzung

## 1.1. Informationsgewinnung und -austausch

### 1.1.1. Adressbücher

Nichtlokale Adressbücher können in Form von LDAP-Directory-Servern (Verzeichnisservern) für die automatische Adressergänzung sowohl im Netscape-Messenger als auch in Outlook/Outlook Express genutzt werden:
Dazu wird das Netscape-Adressbuch aufgerufen und z.B. der LDAP[1]-Server des Fachbereichs Mathematik der Bergischen Universität den Verzeichnisdiensten hinzugefügt:

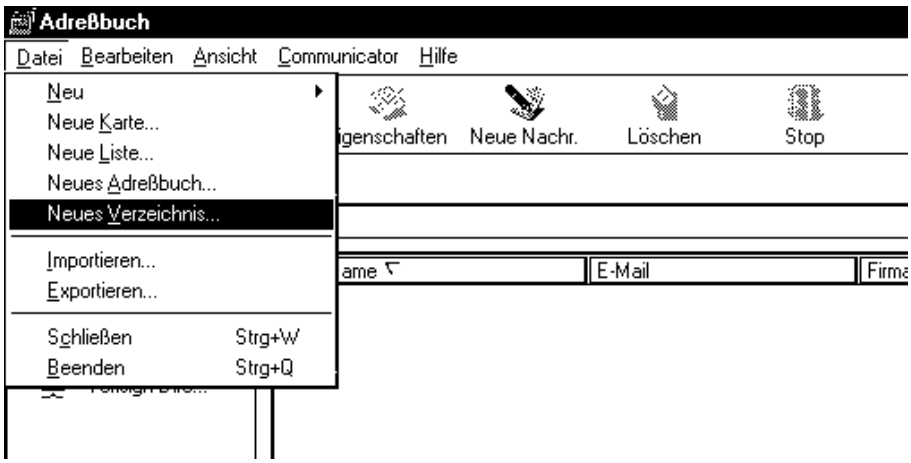



Abbildung 1.1.: LDAP-Dienste-Auruf im Netscape-Adreßbuch

Ähnlich kann und Windows `wab` (Windows adress book) aufgerufen werden und z.B. der hochschulinternen LDAP-Server des Personals der Bergischen Universität Wuppertal gemäß den Abbildungen (1.3) bis (1.6) zur Benutzung bereitgestellt werden.

[1] LDAP=light weight directory access protocol.
Ein Verzeichnisdienst ist eine Informationsdatenbank, die auf häufige Anfragen optimiert ist, jedoch nicht auf häufige Änderungen/Modifikationen,

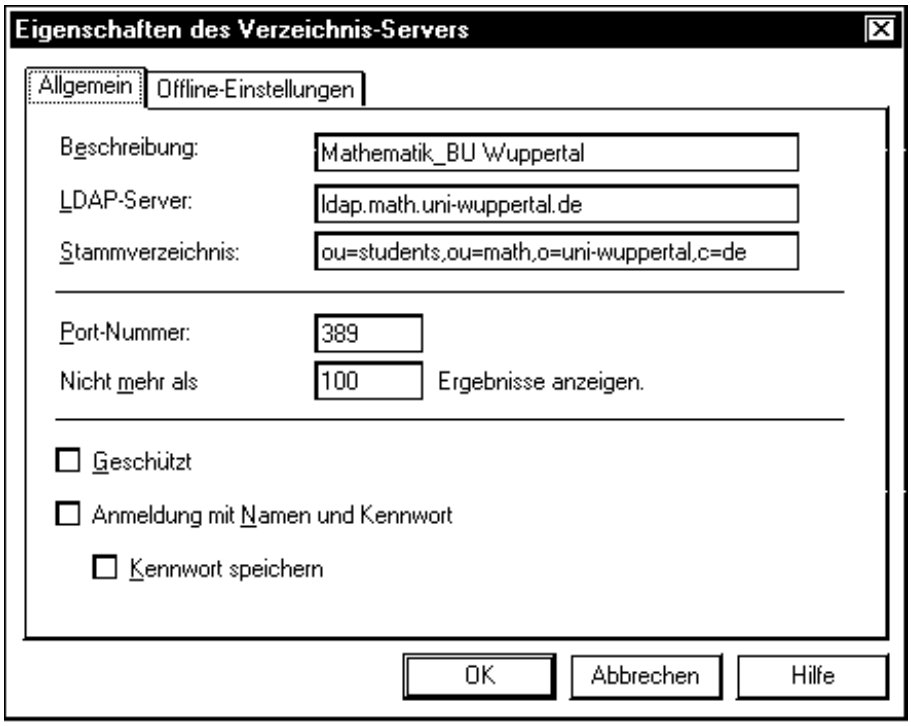



Abbildung 1.2.: LDAP-Server Einrichtung in Netscape

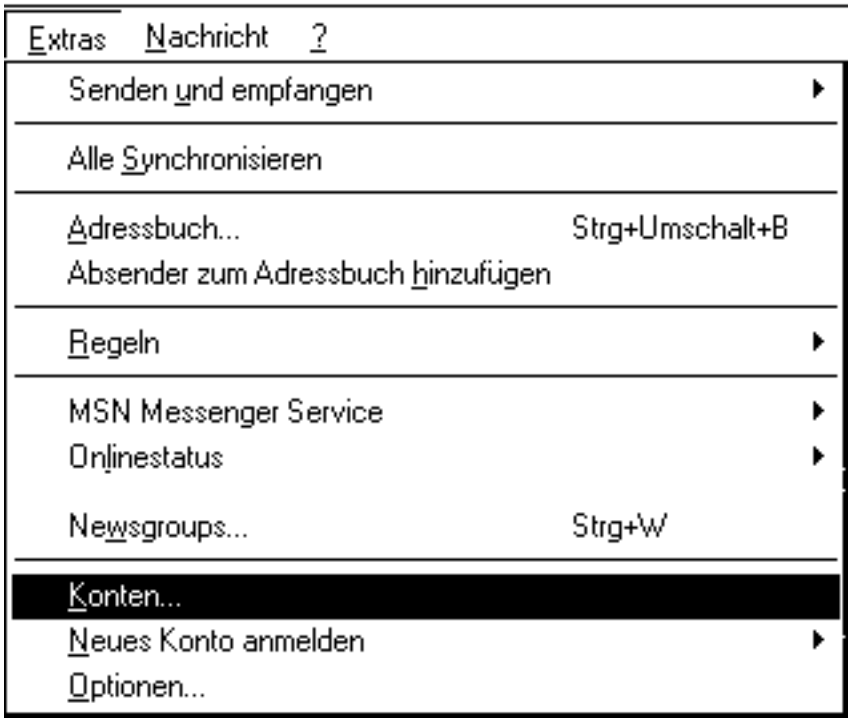



Abbildung 1.3.: LDAP-Dienste-Auruf in Outlook-Express I

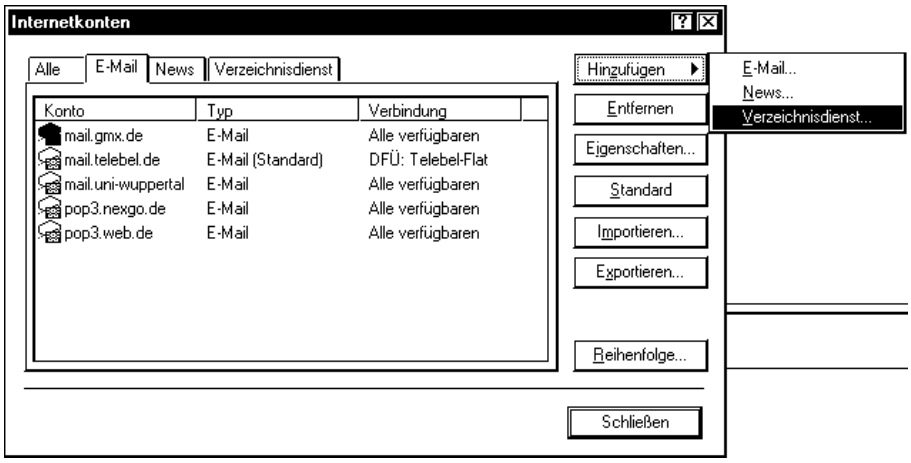



Abbildung 1.4.: LDAP-Dienste-Auruf in Outlook-Express II

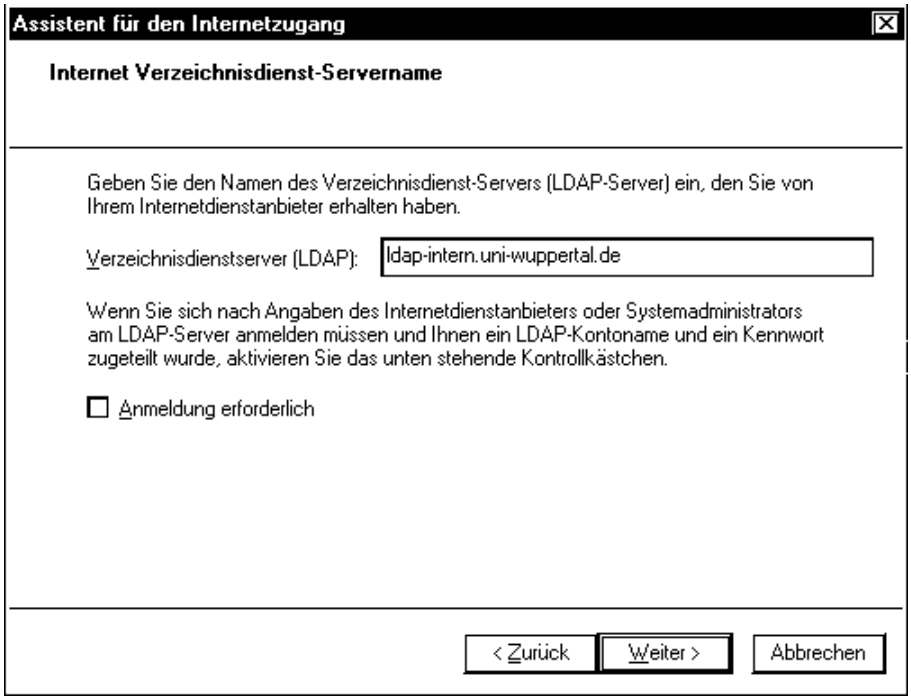



Abbildung 1.5.: LDAP-Dienste-Einrichtung in Outlook-Express I

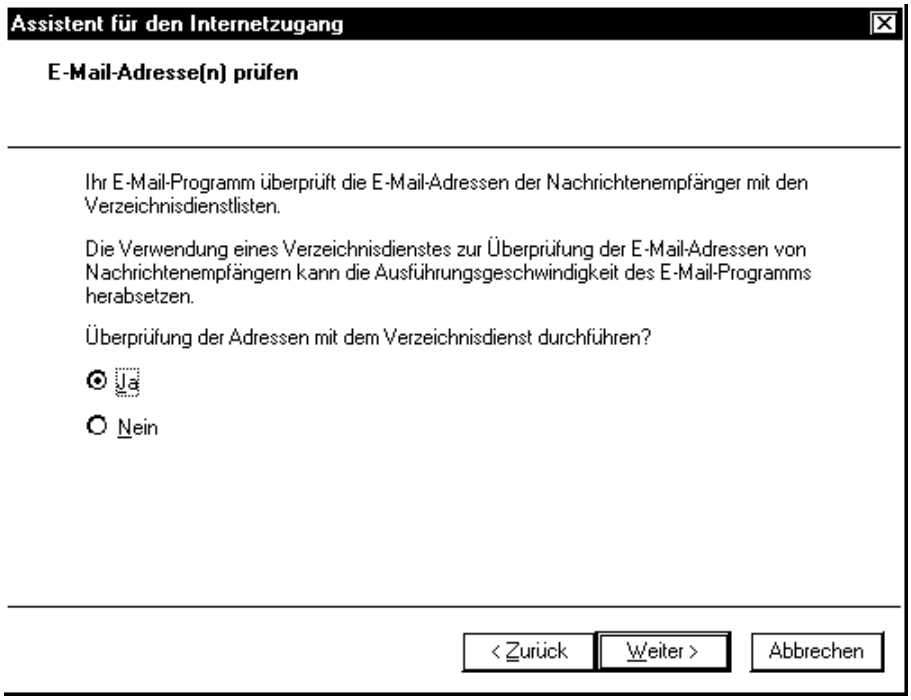



Abbildung 1.6.: LDAP-Dienste-Einrichtung in Outlook-Express II

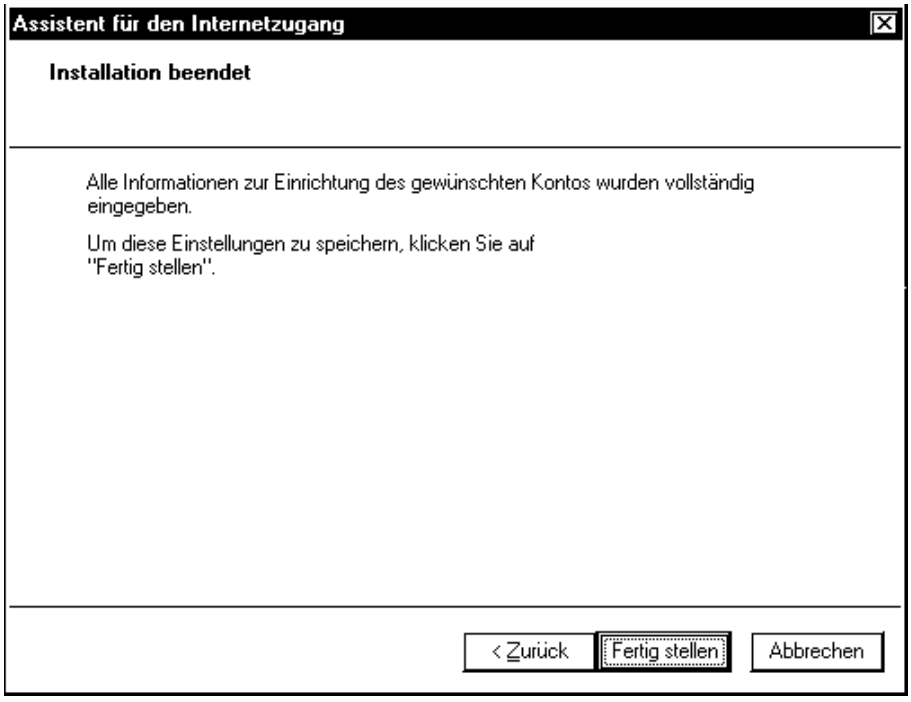



Abbildung 1.7.: LDAP-Dienste-Einrichtung in Outlook-Express III

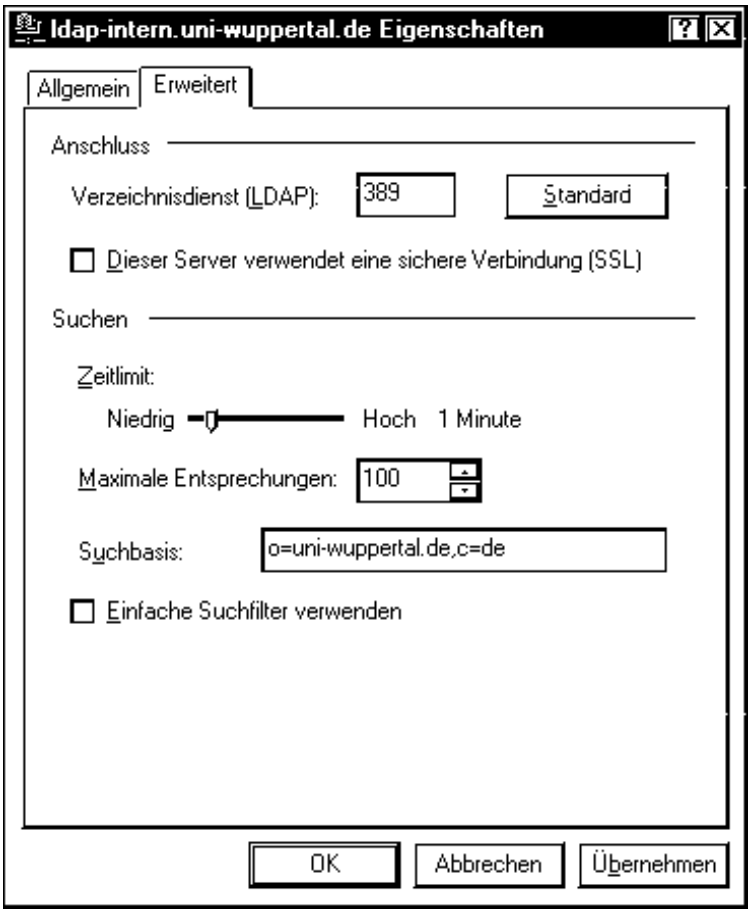



Abbildung 1.8.: LDAP-Dienste-Einrichtung in Outlook-Express IV

Durch die Suchbasis (search root) kann man „Unterabteilungen“ von Organisationen barumartig getrennt ansprechen:

| | |
|---|---|
| Organisationsunit | ou=math |
| Organisation | o=uni-wuppertal |
| Land (country) | c=de |

bzw.

| | |
|---|---|
| | ou=groups |
| | ou=math |
| | o=uni-wuppertal |
| | c=de |

usw.

Es gibt auch zwei verbreitete Softwareprodukte, die den Zugang zu LDAP-Servern mittels Web-Browser ermöglichen:
Eines ist web500gw:

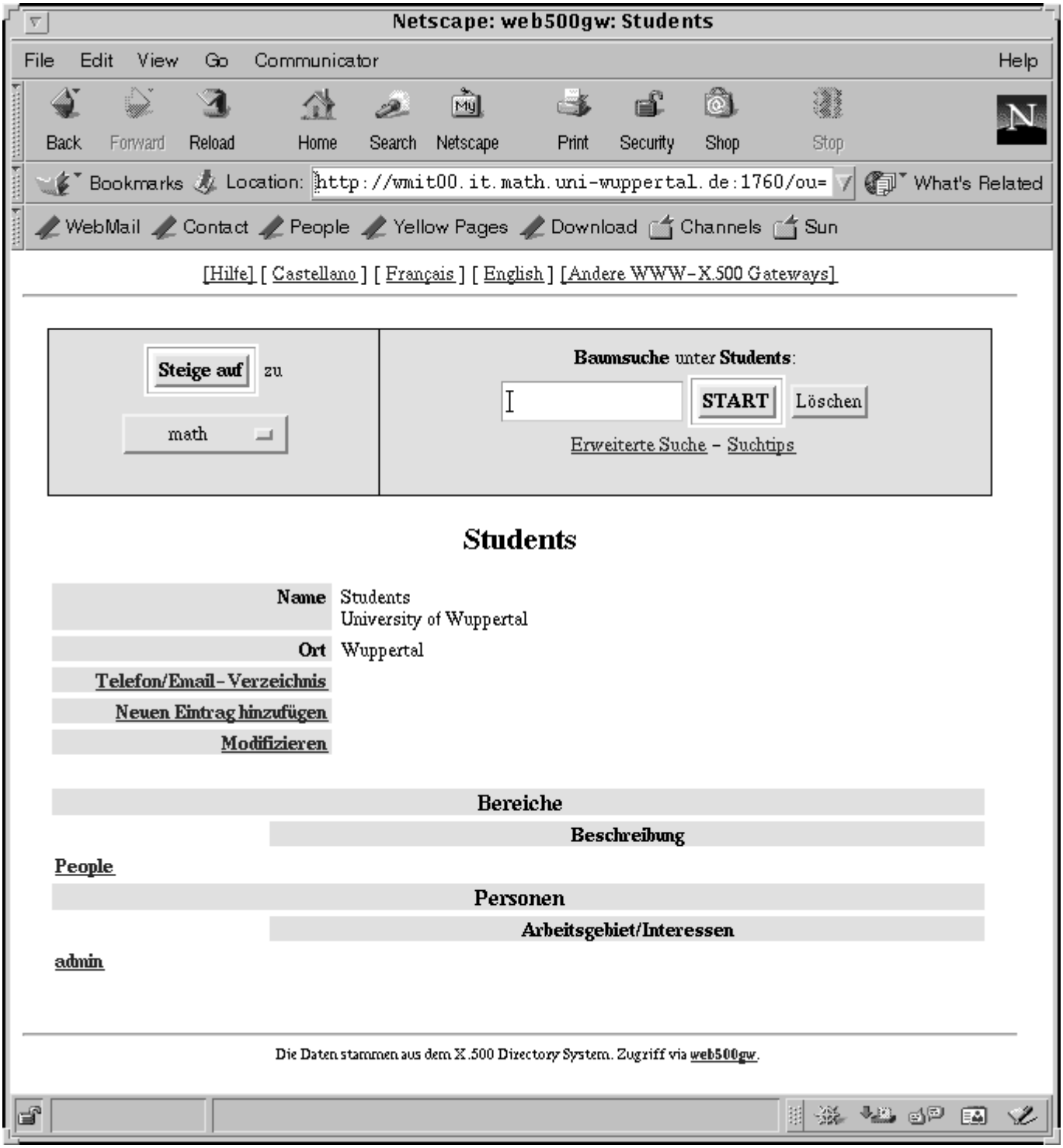



Abbildung 1.9.: web500gw
`http://wmit00.it.math.uni-wuppertal.de:1760/ou=students,ou=math,o=uni-wuppertal,c=de`

**Aufgabe:** Suchen Sie nach allen Studenten mit Vornamen Bernd und lassen Sie sich deren Business card (vcard) anzeigen.

Durch Anklicken des Wortes `People` bekommen Sie eine Liste aller im Adressbuch vorhandenen Einträge angezeigt.

Das andere heißt `web2ldap`. Mit diesem können Sie beispielsweise unter

`http://sites.inka.de:8002/web2ldap/`

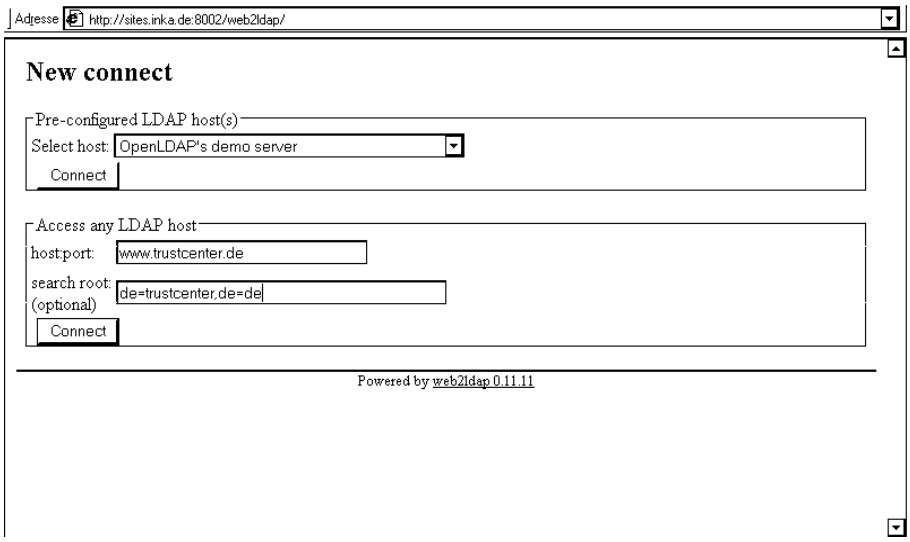



Abbildung 1.10.: web2ldap I
`http://sites.inka.de:8002/web2ldap/`

nach dem S/MIME-Zertifikat von Herrn Feuerstein suchen.

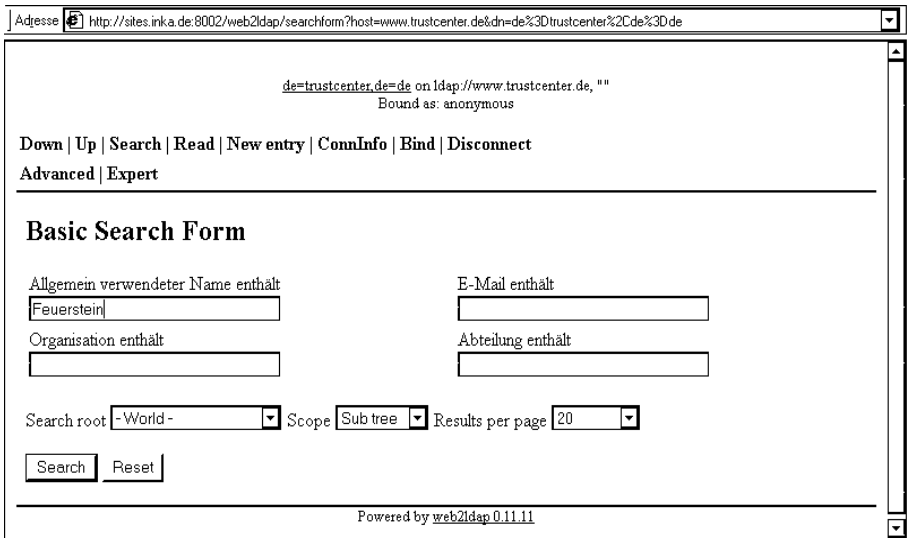



Abbildung 1.11.: web2ldap II
`http://sites.inka.de:8002/web2ldap/`

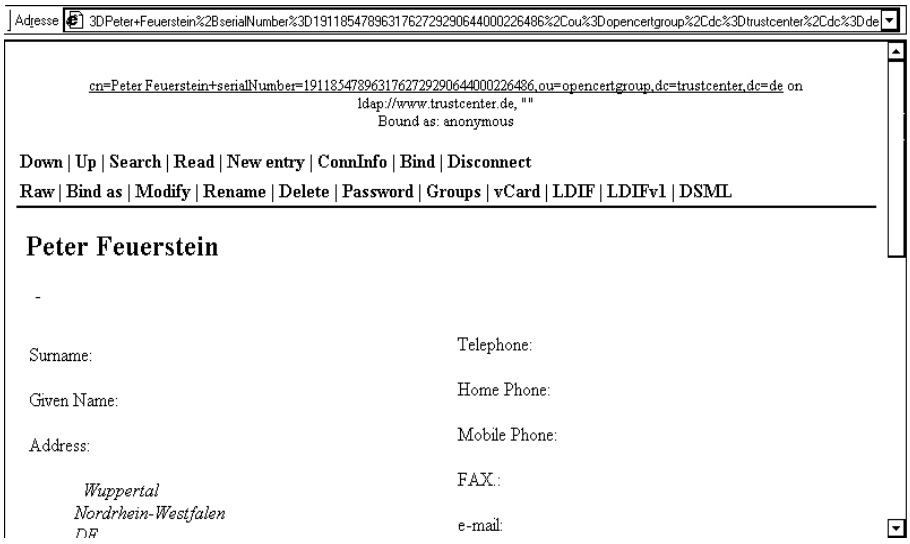



Abbildung 1.12.: web2ldap III
`http://sites.inka.de_8002/web2ldap/`


Abbildung 1.13.: web2ldap IV
`http://sites.inka.de_8002/web2ldap/`

Über den Punkt `Read` kann dann dort `userCertificate; binary` mittels `View` gewählt werden und damit das S/MIME X.509v3-Zertifikat von Herrn Feuerstein erhalten werden.

**Bemerkung:** Die Erweiterung der Webadresse um `:1760` bzw. `:8002` sind sogenannte Port-Nummern. Über diese Nummern kann ein entsprechender Internetdienst des aufgerufenen Rechners ausgewählt werden. `http` enstpricht dabei standardmäßig dem Port 80, `https` dem Port 443[2].

[2]Vergleiche hierzu `/etc/services` auf Unix-Rechnern.

`gq` als Bestandteil der `gnome`-Oberfläche des Linux-Betriebssystems[3] ermöglicht nicht nur eine Abfrage von LDAP-Servern sondern auch deren Verwaltung:

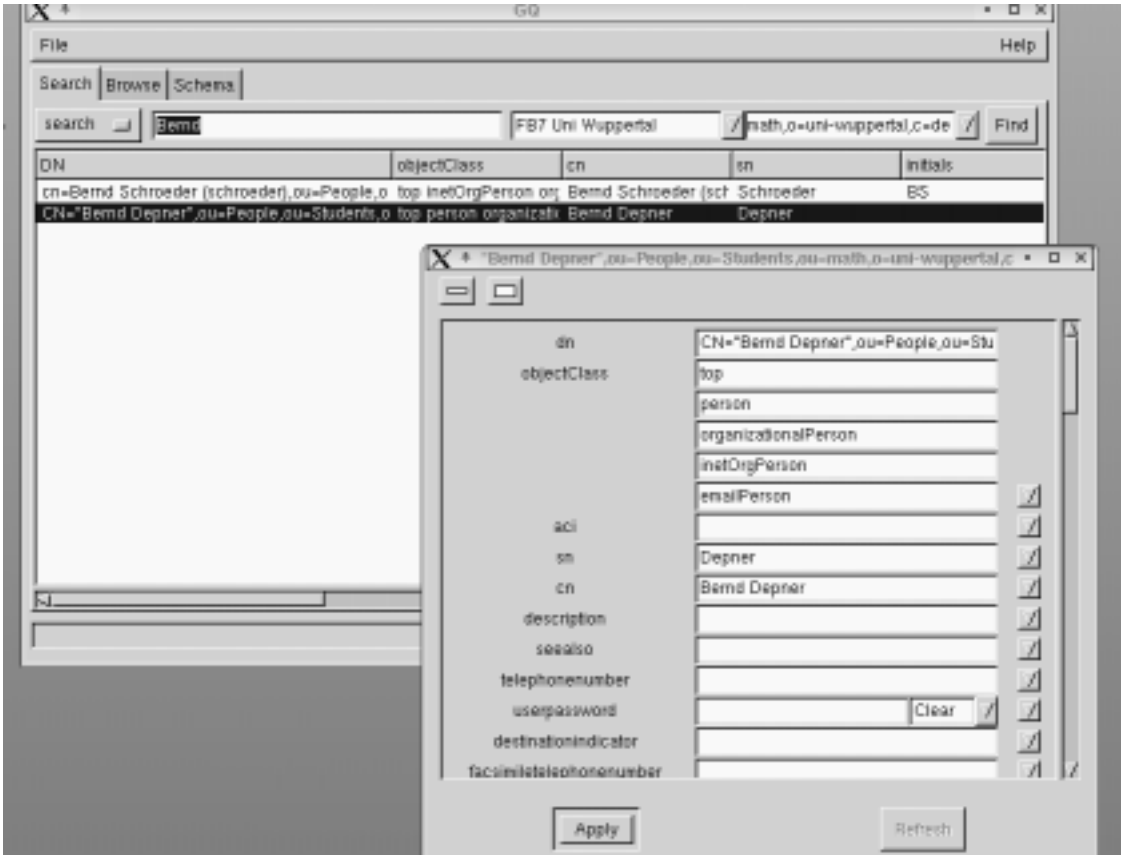



Abbildung 1.14.: web500gw
`http://wmit00.it.math.uni-wuppertal.de:1760/ou=students,ou=math,o=uni-wuppertal,c=de`

[3] Es ist auch unter `kde` lauffähig

### 1.1.2. email

Neben den in der Einleitung schon besprochenen Möglichkeiten, email mittels Netscape-Messanger bzw. Outlook/Outlook Express zu nutzen,

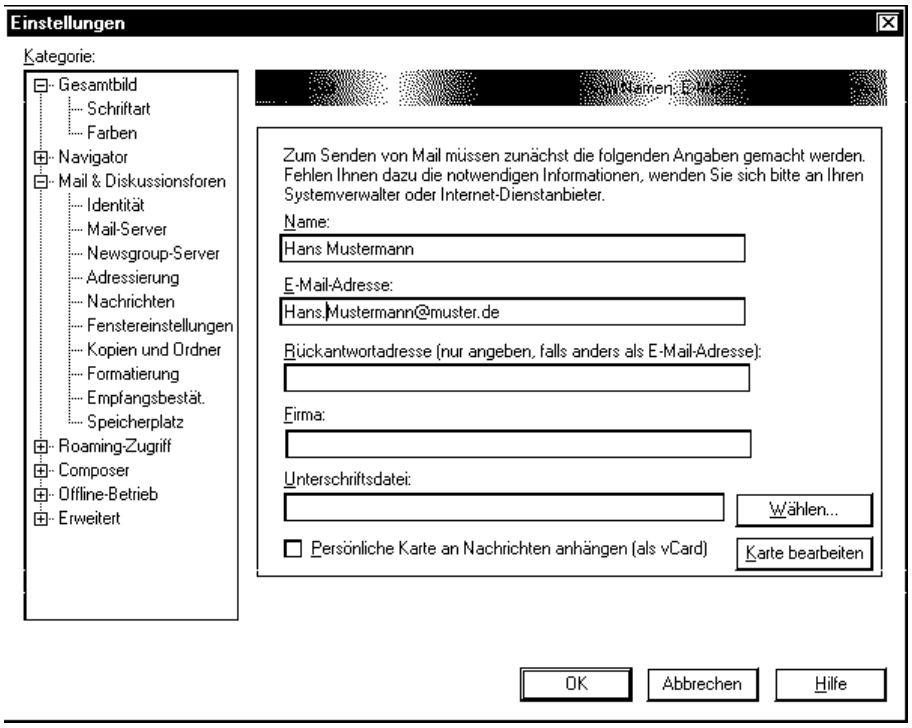



Abbildung 1.15.: email-Konfiguration im Netscape Messenger I

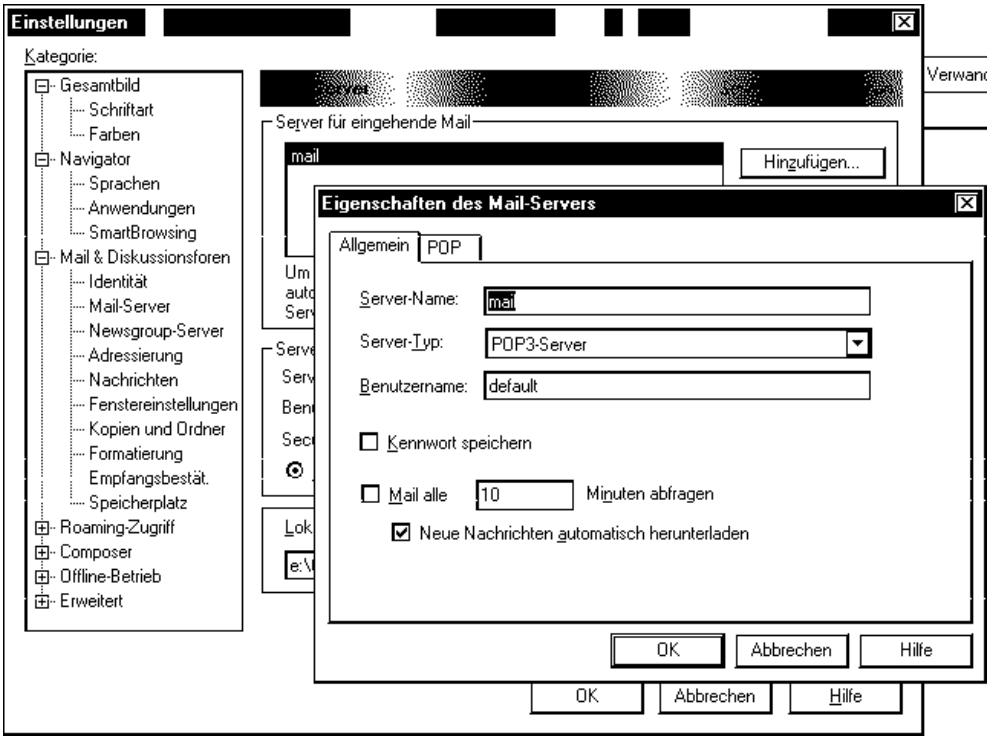



Abbildung 1.16.: email-Konfiguration im Netscape Messenger II

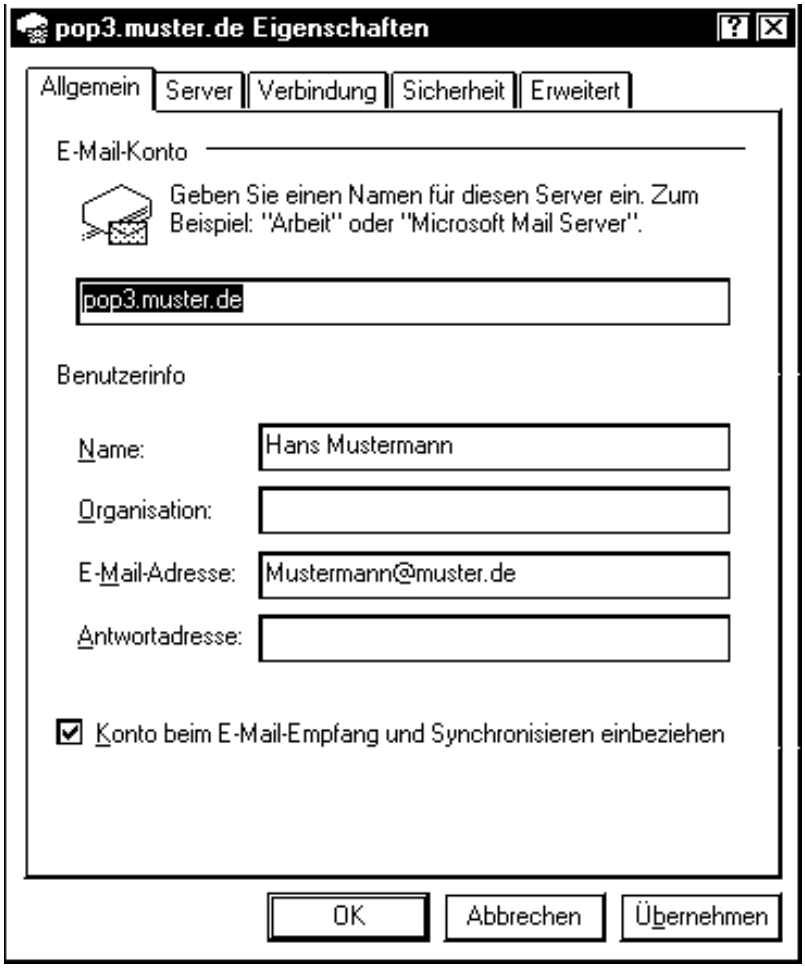



Abbildung 1.17.: email in Outlook Express

existieren auch IMAP[4]-Server mit Web-Oberfläche.


Abbildung 1.18.: email mit IMAP-Server I


Abbildung 1.19.: email mit IMAP-Server II

[4]Internet Mail Access Protocol

Die verschiedenen Anbieter und deren Einstellungen zeigt folgende Tabelle:

| Anbieter | Anmeldung für POP | POP-Server | SMTP-Server |
|---|---|---|---|
| Arcor | Beispiel.Nutzer | pop3.arcor.de | mail.arcor.de |
| Compuserve | Beispiel.Nutzer | pop.compuserve.de | smtp.compuserve.de |
| DirectBox | Beispiel.Nutzer | pop3.directbox.com | smtp.directbox.com |
| GMX | Beispiel.Nutzer@gmx.de | mail.gmx.de | smtp.gmx.de |
| Epost | Beispiel.Nutzer | mail.epost.de | mail.epost.de |
| Firemail | Beispiel.Nutzer@firemail.de | pop.firemail.de | smtp.firemail.de |
| Freenet | Beispiel.Nutzer | pop3.freenet.de | mx.freenet.de |
| T-Online[a] | Egal/Keiner | pop.t-online.de | mailto.t-online.de bzw. smtprelay.t-online.de[b] |
| Web.de | Beispiel.Nutzer | pop3.web.de | smtp.web.de |
| Yahoo Mail | Beispiel.Nutzer | pop.mail.yahoo.de | smtp.mail.yahoo.de |
| uni-wuppertal.de | account_name | mail.math.uni-wuppertal.de | mail.math.uni-wuppertal.de[c] |

[a] erreichbar nur bei Interneteinwahl über t-online
[b] mit beliebiger from-Zeile, kostenpflichtig
[c] mit SSL-Anmeldung dann auch von außerhalb erreichbar

**Bemerkung:** Kostenlose SMTP-Relay-Server mit beliebiger Absenderadresse nach Anmeldung bieten etwa

Freenet (`http://www.freenet.de`)
Arcor (`http://www.arcor.de`)

**Eigenheiten der SMTP-Sever**

Im Gegensatz zu POP-Servern unterstützen im Moment noch wenige SMTP-Server eine Anmeldung (GMX unterstützt die Anmeldung am SMTP-Server seit kurzem). Man kann also theoretisch Mails verschicken ohne dass der Server überprüft, ob man der ist, der man zu sein behauptet.

Das birgt natürlich gewisse Gefahren in sich, weshalb die Provider den Zugriff auf ihre SMTP-Server auf anderem Wege beschränken.

Internet-Provider wie Compuserve, aber auch Universitäten behelfen sich, indem sie das Versenden von Mails über ihren SMTP-Server nur erlauben, wenn man auch mit dem passenden Provider eingewählt ist.

Freemailanbieter wie Web.de können diesen Weg nicht gehen, da sie keinen eigenen Internet-Zugang anbieten. Sie setzen deshalb das Verfahren „SMTP after POP“ ein. Das bedeutet, daß der SMTP-Server erst Mails annimmt, wenn derselbe Computer vorher schon versucht hat Mails vom POP-Server abzuholen. Diese Freischaltung ist dann eine Zeit lang gültig und wird anschließend wieder zurückgenommen.

Eine weitere Eigenheit der meisten SMTP-Server ist, dass sie keine Mails annehmen, die eine Absenderadresse eines fremden Anbieters tragen.

### 1.1.3. Absenderangaben, Formulare und Visitenkarten

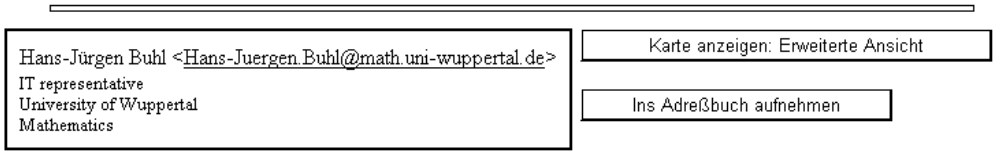
**Subject:** Anforderung von...
**Content-type:** MULTIPART/MIXED; BOUNDARY=...
**X-Accepted-Language**: en, de
**X-Virus-Scanned:** by amavisd-milter (http:/amavis.org)
**References:** ...
**X-Priority:** 1 (Highest)

Lieber Herr Mustermann,

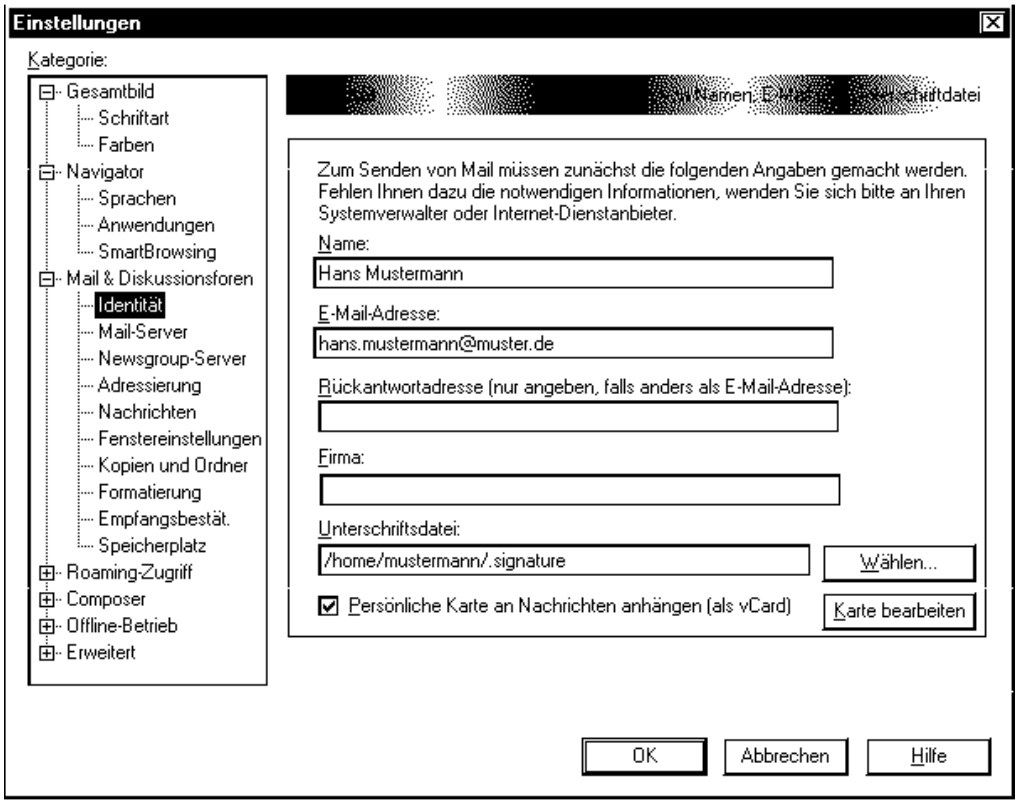
...

Gruß
Hans-Jürgen Buhl

```
--
-------------------------------------------------------------------
Prof. Dr. Hans-Juergen Buhl University of Wuppertal
Fachbereich Mathematik & Institut fuer Angewandte Informatik
-------------------------------------------------------------------
Phone: +49 202 2422009 Fax: +49 202 2422011
mailto: Hans-Juergen.Buhlmath.uni-wuppertal.de
WWW: http://www.math.uni-wuppertal.de/~buhl
smail: University, Gauss-Strasse 20, D-42119 Wuppertal, Germany
-------------------------------------------------------------------
```

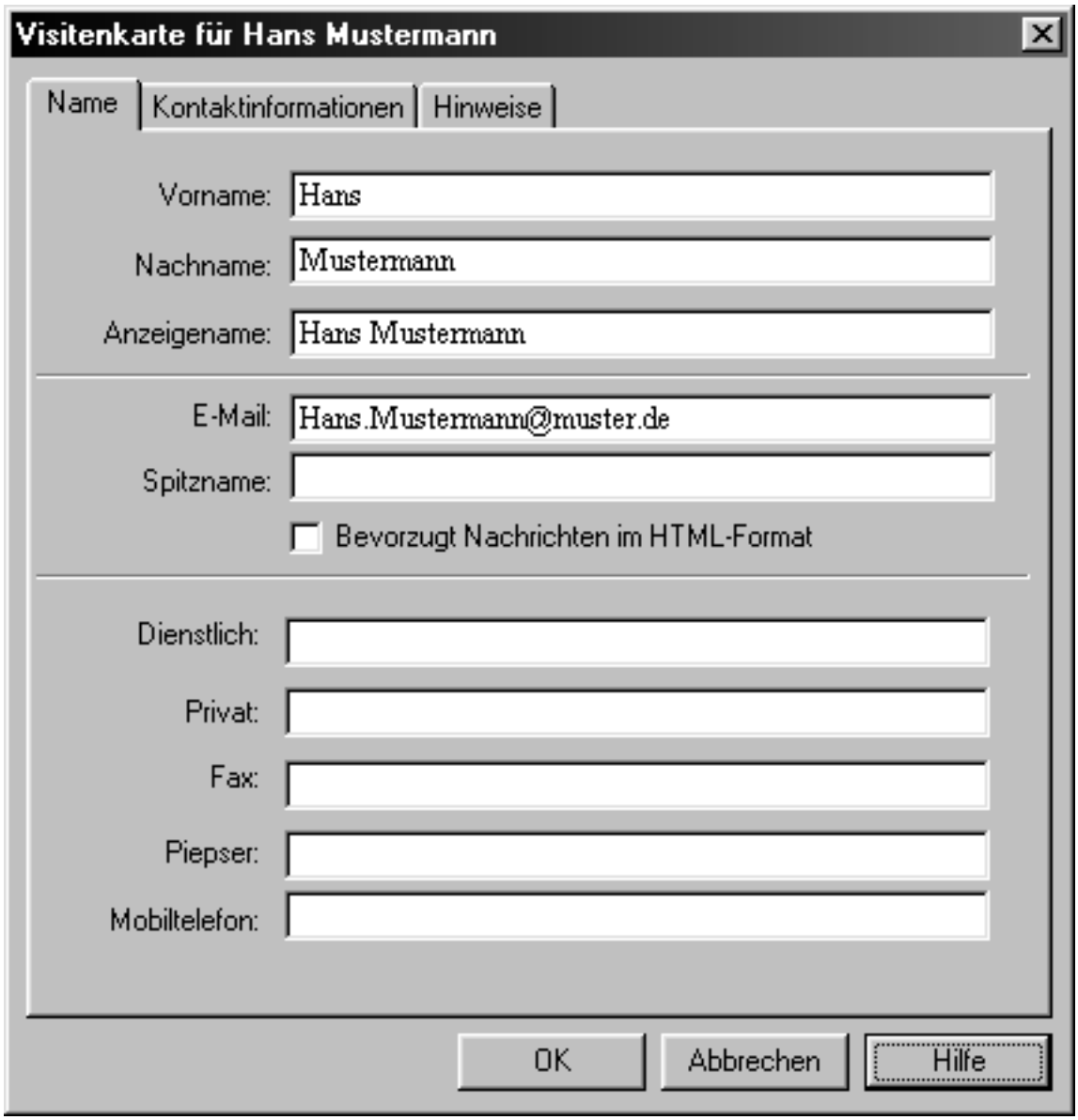



Obige email enthält zwei Arten von Absenderangaben. Die erste, die sogenannte `signature`, wird üblicherweise als reine Textdatei von wünschenswerterweise weniger als fünf Zeilen in der Datei `$HOME/.signature` abegelegt und dann automatisch von den Kommandos `mail, mailx, ...` an jede ausgehende email angehängt. Auch Netscape kann man so konfiguerieren, dass




der Inhalt einer Datei (am besten ebenfalls `$HOME/.signature`) in jedem neu geöffneten Composer-Fenster im Sinne eines Default-Formulares automatisch eingefügt erscheint. Solche Absenderangaben kann jeder auch nur rein textbasiert arbeitende email-Client vernünftig anzeigen.

Eine Visitenkarte – die zweite besprochene Art von Absenderangaben – kann durch Anwählen des Punktes `Attach my personal card to messages` ebenfalls automatisch an abgehende emails angehängt werden. Solche Karten können durch Klicken auf `Edit Card` erstellt werden.




Der Empfänger einer solchen email kann dann eine solche Visitenkarten durch einfaches Klicken auf den Knopf


in sein persönliches Adressbuch übernehmen.

**Vorsicht:** Bitte reines ASCII ohne Umlaute benutzen, da ansonsten die Sortierungsreihenfolge des persönlichen Adressbuches durcheinanderkommen kann.

Visitenkarten können sowohl in Netsacpe als auch in Outlook/Outlook Express genutzt werden und funktionieren auch, wenn Absender und Empfänger verschiedene email-Klienten benutzen[5]. Das liegt daran, dass für Visitenkarten der MIME[6]-Typ `text/x-vcard` benutzt wird und die Mailnachricht (body) sowie die Visitenkarte als zwei Teile einer mehrteiligen `MULTIPART/MIXED` email versendet werden. Rein textbasierte Mailreader zeigen dann auch etwa folgenden Inhalt an:

```
Sender: buhl@mail.urz.uni-wuppertal.de
Message-ID: <3E56228D.13DCD010@math.uni-wuppertal.de>
Date: Fri, 21 Feb 2003 13:58:53 +0100
From: Hans-Juergen Buhl <Hans-Juergen.Buhl@math.uni-wuppertal.de>
Organization: University of Wuppertal
X-Mailer: Mozilla 4.76 [en] (X11; U; SunOS 5.3 sun4m)
X-Accept-Language: en
MIME-Version: 1.0
To: ...
Subject: ...
References: <3E3522EB.D7B0E8D9@math.uni-wuppertal.de> <001401
    c2d9a3$9d70b0a0$492b14d5@muster>
Content-Type: multipart/mixed;
 boundary="------------B9A8CF31DD617289BA8FD894"
X-Virus-Scanned: by amavisd-milter (http://amavis.org/)

This is a multi-part message in MIME format.
--------------B9A8CF31DD617289BA8FD894
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit

...

Gruß
Hans-Jürgen Buhl

--
-------------------------------------------------------------------------
 Prof. Dr. Hans-Juergen Buhl                 University of Wuppertal
 Fachbereich Mathematik & Institut fuer Angewandte Informatik
-------------------------------------------------------------------------
 Phone:  +49 202 2422009                       Fax:   +49 202 2422011
 mailto: Hans-Juergen.Buhl@math.uni-wuppertal.de
 WWW:    http://www.math.uni-wuppertal.de/~buhl
 smail:  University, Gauss-Strasse 20, D-42119 Wuppertal, Germany
-------------------------------------------------------------------------
--------------B9A8CF31DD617289BA8FD894
Content-Type: text/x-vcard; charset=us-ascii;
 name="Hans-Juergen.Buhl.vcf"
Content-Transfer-Encoding: 7bit
Content-Description: Card for Hans-Juergen Buhl
Content-Disposition: attachment;
 filename="Hans-Juergen.Buhl.vcf"

begin:vcard
n:Buhl;Hans-Juergen
tel;fax:+49 202 2422011
tel;home:+49 202 2422003
tel;work:+49 202 2422009
x-mozilla-html:FALSE
url:http://www.math.uni-wuppertal.de/~buhl
org:University of Wuppertal;Mathematics/Computer Science
adr:;;Gauss-Strasse 20;Wuppertal;;D-42119;Germany
```

[5]Einige Visitenkartenfelder gehen dabei aber jeweils verloren.

[6]Multiple purpose internet mail extensions

```
version:2.1
email;internet:Hans-Juergen.Buhl@math.uni-wuppertal.de
title:IT representative
note:Member of the Institute for Applied Computer Science (IAI)
x-mozilla-cpt:;26880
fn:Prof. Dr. Hans-Juergen Buhl
end:vcard

--------------B9A8CF31DD617289BA8FD894--
```

Deshalb bleibt eine Absenderangabe im Sinne der Textdatevariante `$HOME/.signature` als zweite redundante Absenderangabe solange sinnvoll, wie einige email-Korrespondenten noch solche textbasierte email-Reader benutzen.

**Bemerkung:** Leider scheinen Outlook und Outlook Express auch `MULTIPART/MIXED` emails zu erzeugen, deren ersten beiden Teile (Versand von gleichzeitig Text- und HTML-Version einer Nachricht) von Netscape als ein gemeinsamer Text-Teil interpretiert wird:

```
Message-ID: <006301c2de5b$42f2e500$08bcb9d9@pater>
From: "Hans Müller" <mueller@mueller.de>
To: "Hans Mustermann" <hans.mustermann@muster.de>
Subject: Muster
Date: Thu, 27 Feb 2003 13:25:04 +0100
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_000_0060_01C2DE63.A3A19740"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4807.1700
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4807.1700

This is a multi-part message in MIME format.

------=_NextPart_000_0060_01C2DE63.A3A19740
Content-Type: text/plain;
        charset="Windows-1252"
Content-Transfer-Encoding: quoted-printable

Hallo lieber Herr Mustermann,

hier ist die angeforderte Muster-Email

Viele Gr=FC=DFe


------=_NextPart_000_0060_01C2DE63.A3A19740
Content-Type: text/html;
        charset="Windows-1252"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Dwindows-1252">
<META content=3D"MSHTML 5.50.4807.2300" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY>
<DIV><FONT face=3DArial size=3D2></FONT><FONT face=3DArial =
size=3D2>Hallo lieber Herr=20
Mustermann,</FONT></DIV>
<DIV><FONT face=3DArial size=3D2></FONT> </DIV>
<DIV><FONT face=3DArial size=3D2>hier ist die angeforderte =
```

```
Muster-Email</FONT></DIV>
<DIV><FONT face=3DArial size=3D2></FONT> </DIV>
<DIV><FONT face=3DArial size=3D2>Viele Gr=FC=DFe</FONT></DIV>
<DIV> </DIV></BODY></HTML>

------=_NextPart_000_0060_01C2DE63.A3A19740--
```

**Formulare**

...zum Beispiel zum Austausch von Terminen aus einer Terminplanersoftware einfach per „*drag and drop*“ Mail-Klient von/nach Terminplanersoftware:

```
** Calendar Appointment **

Date: 3/14/03
Start: 2:00pm
End: 3:15pm
Repeat: One Time
What: Mustertermin
```

Abbildung 1.20.: in `mailtool`

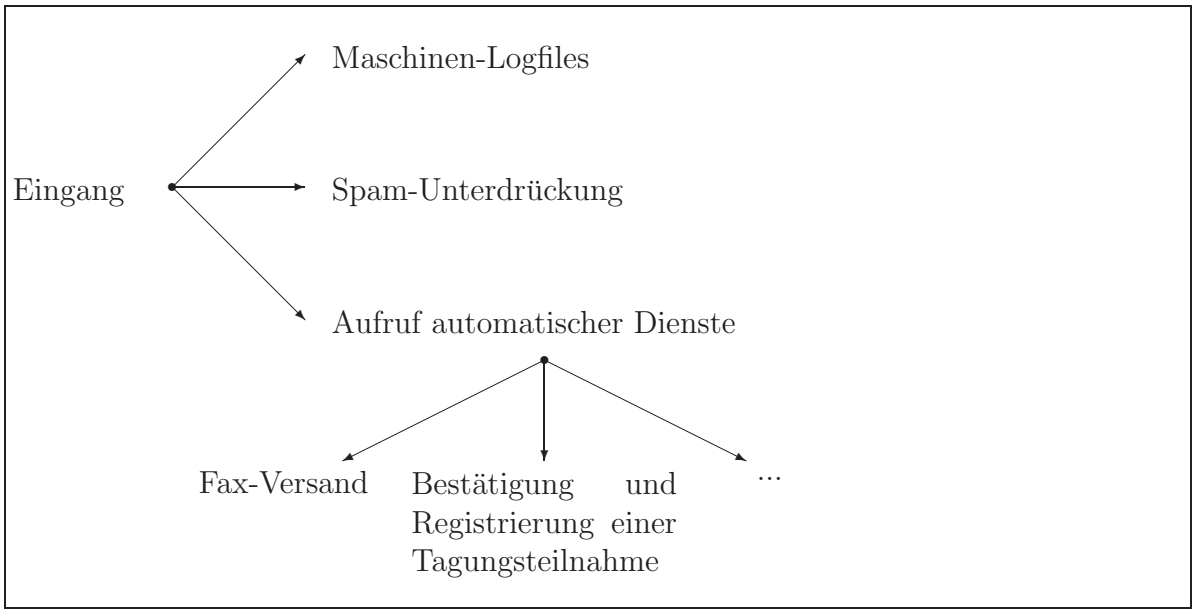
```
Organisator: Niemand@nirgendwo
Zusammenfassung: Muster
Anfangsdatum: 14.03.2003
Beginn um: 12:00
Ende um: 14:00
```

Abbildung 1.21.: in `KOrganizer`

Dazu ist jedoch eine Interoperationalität des Mail-Klienten mit der Terminkalendersoftware nötig, welche heute meist mittels (syntaktisch) festgelegtem Textformat und noch nicht über MIME-Typen realisiert wird.

### 1.1.4. Mailfilter


Abbildung 1.22.: Klassifizierung von „Mails“ und (automatische) „Bearbeitung“ I




Mailfilter können zur automatische Vorverarbeitung von eingehenden Mails benutzt werden:

- Ausdruck oder Weiterleitung
- Löschen von Massenwurfsendungen
- Sammeln von Routinemeldungen (log-Files, ...)
- Weiterleitung an Dienste (wie Fax-Versand, ...)

- automatische Empfangsbestätigung von Tagungsanmeldungen
- ...

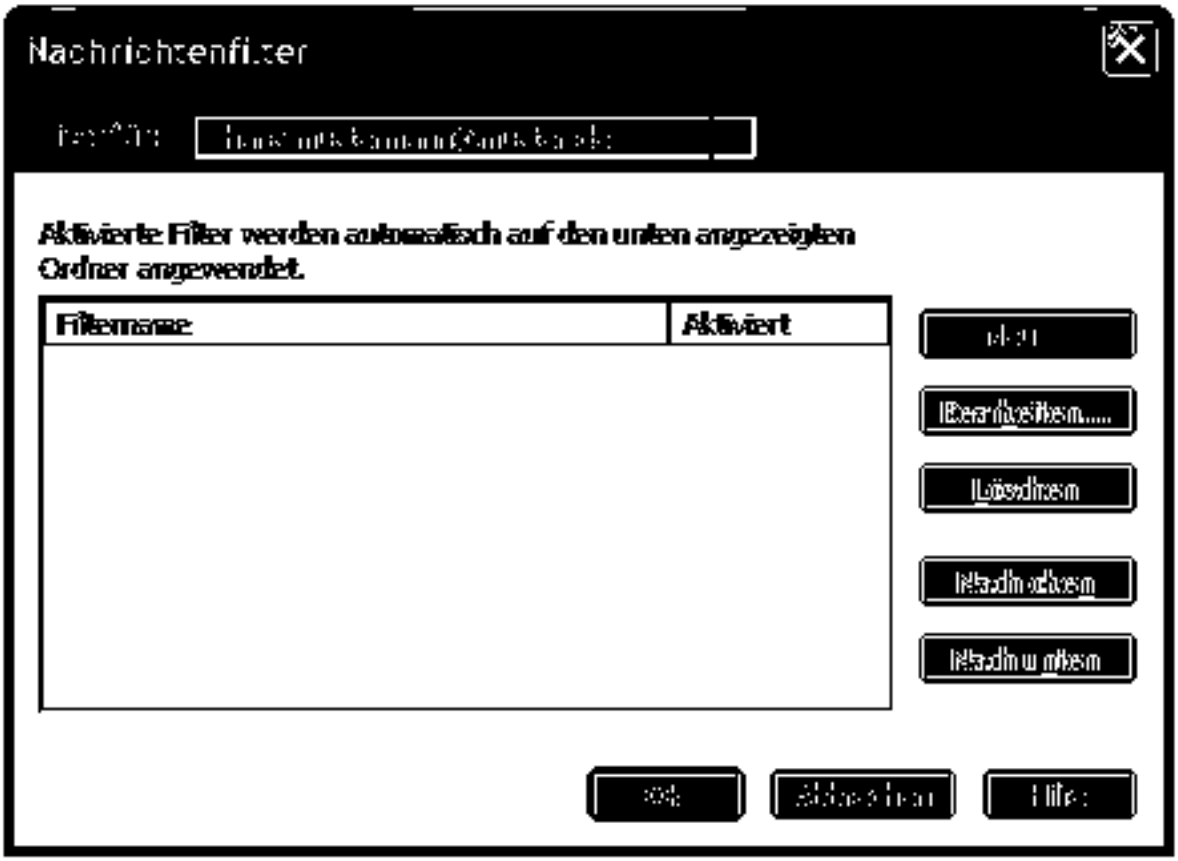



Abbildung 1.23.: Klassifizierung von „Mails“ und (automatische) „Bearbeitung“ II

Sie bieten eine Auswahl von durchführbaren Aktionen bei Textmatching meist der Mail-Headerzeilen, machmal auch des gesamten Mail-Textes an. Aktionen sind

- Verschieben in (Unter-)Ordner,
- Prioritätsordnung,
- Löschung,
- als gelesen kennzeichnen,
- markieren,
- mit einem Label versehen,
- ...

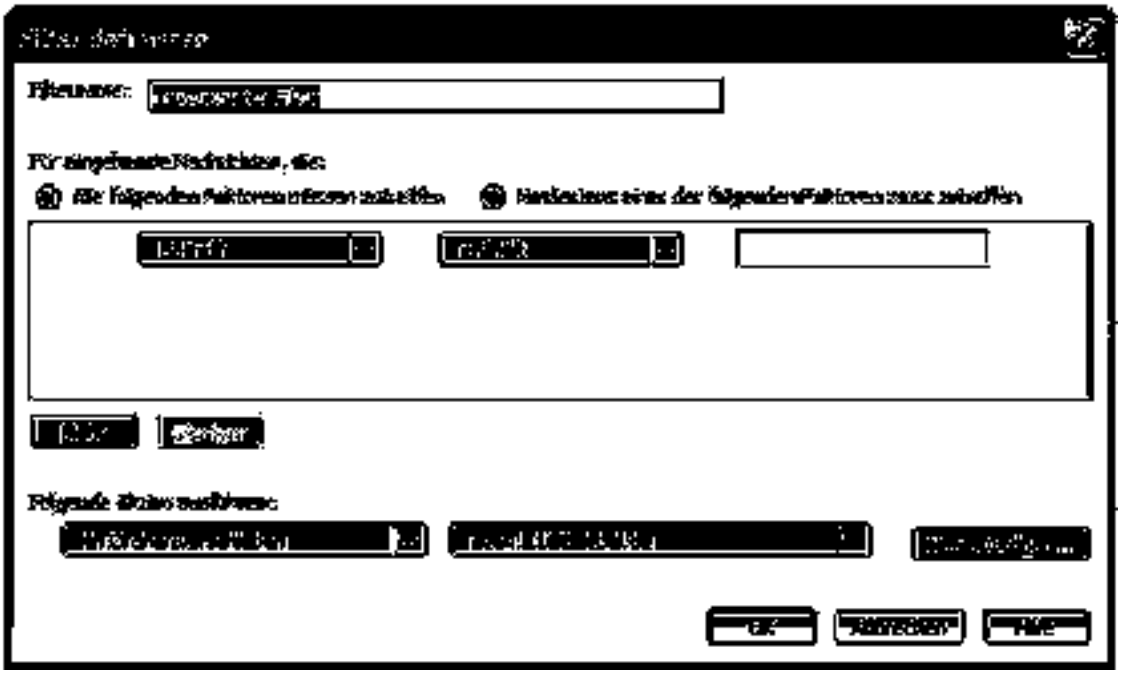


Abbildung 1.24.: Klassifizierung von „Mails“ und (automatische) „Bearbeitung“ III

**Bemerkung:** Filter in Mail-Klienten arbeiten natürlich nur dann, wenn diese gestartet sind und Verbindung zum Mailserver aufgenommen haben. Es gibt auch Mailserver, auf denen die Benutzer selbst Filter einrichten dürfen und die dann unabhängig vom Laufen irgendwelcher Mail-Klienten arbeiten.

Mittels der Datei `/etc/aliases` können selbst Filter in der Art

```
loginname: “Filterprogramm“
loginname2: /dev/null
```

(siehe `man aliases` und `man sendmail`) implementiert werden, die gemäß To-Headerzeile ausgewählt werden.

### 1.1.5. Nachsendeaufträge

Mittel der Datei ∼/.forward können Nachsendeaufträge realisiert werden, die Sie etwa bei Abwesenheit am Dienstort (durch Weiterleitung an einen Kollegen oder an einen Gast-Account am Dienstreiseort, ...) oder zur Sammlung aller Mails an etwa existierende verschiedene Mailadressen auf nur einem Mailsever einsetzen können:

```
\loginname, gast@yourfirma.de
```

Abbildung 1.25.: Datei ∼/.forward

Der Teil \loginname sorgt dafür, dass der User loginname auch eine lokale Kopie auf dem Rechner behält, auf dem die ∼ /.forward-Datei vorliegt.
Auf POP3/IMAP-Mailserver kann häufig ebenfalls Forwarding mit einer vom Serveranbieter bereitgestellten Seite eingeschaltet werden.

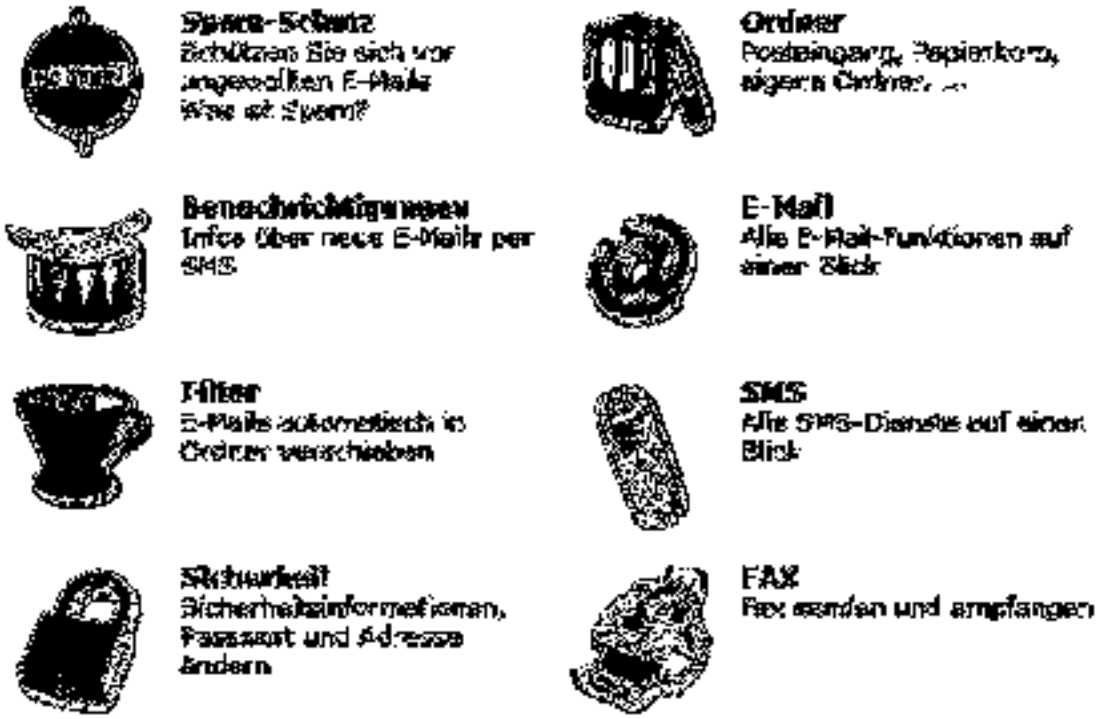



Abbildung 1.26.: Forwarding in Web.de

**Bemerkung:** Mailfilter in Mail-Klienten sollten für diese Funktionalität nicht benutzt werden (warum?).

Auf dem IMAP/POP3-Server des Rechenzentrums der Universität Wuppertal kann das Forwarding unter

https://userdb.uni-wuppertal.de/userdb/passwort/mail_info_vd_user.php

genutzt werden.
Quelle: http://www.hrz.uni-wuppertal.de/aktuelles/webshots.html

---

**Änderung von Benutzerdaten per Web-Schnittstelle: Einzelheiten, Screenshots**
Derzeit unterscheidet das HRZ drei Arten von Accounts:

- Projekt-Accounts (auch: Accounts für Nicht-Studierende),
- Studierenden-Accounts,
- Internetcafe-Accounts.

Auch Studierende können Projekt-Accounts erhalten, wenn sie in einem Fachbereich an einem Projekt mitarbeiten. Ebenso gelten die Accounts immatrikulierter Mitarbeiter als Projekt-Accounts.

Nur Studierende erhalten derzeit bei der Immatrikulation eine zwölfstellige PIN (Persönliche Identifikations-Nummer); das Verfahren soll mittelfristig auf die Mitarbeiter ausgedehnt werden.

Wenn man auf der **Passwortseite**

https://userdb.uni-wuppertal.de/userdb/passwort/

oder auf der **Mail-Alias/Mail-Forwarding-Seite**

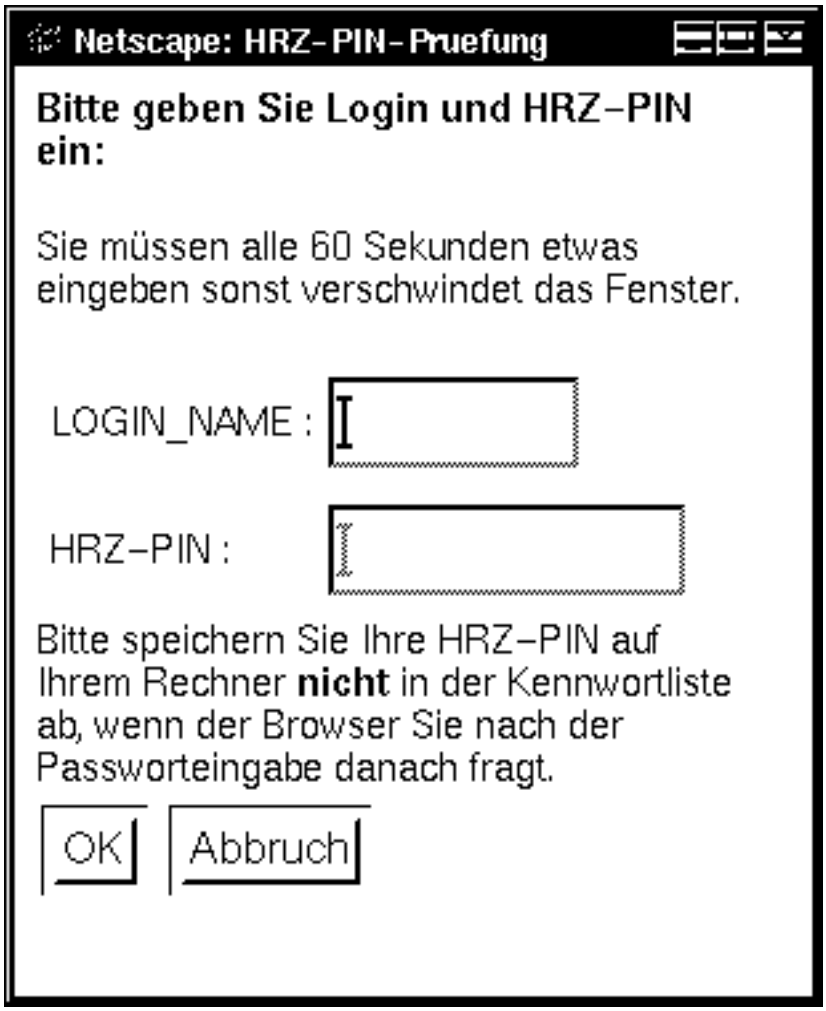
https://userdb.uni-wuppertal.de/userdb/passwort/mail_info_vd_user.php

je nach Account eine der beiden Schaltflächen das erste Mal betätigt, wird man von Netscape (oder einem anderen Browser) in einen länglichen Sicherheitsdialog verwickelt (http://www.hrz.uni-wuppertal.de/aktuelles/webshot-dialog.html): Der Browser kennt das HRZ der Uni Wuppertal nicht als autorisierte Zertifizierende Stelle für sichere Verschlüsselung — woher auch... Daraus resultieren entsprechende Warnungen, die man über sich ergehen lassen muss. Den von uns vergebenen Schlüssel muss man akzeptieren - sonst ist eine verschlüsselte Passwortänderung nicht möglich.

Nach Betätigung der Schaltfläche „*Änderung des Passworts für Nicht-Studierende*“ bzw. „*Mailforwarding/Mailalias für Nicht-Studierende*“ poppt das folgende Fenster auf:

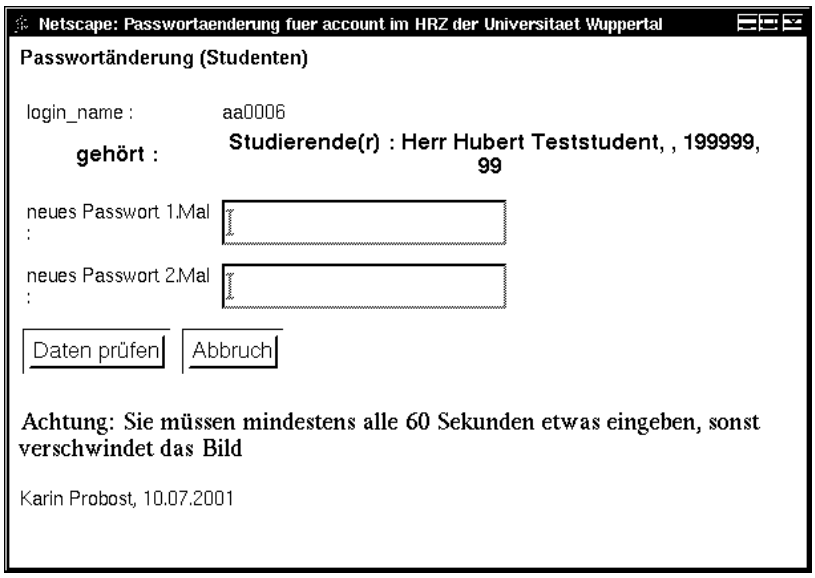

In diese Maske sind der Login-Name und das Passwort einzugeben.

Nach Betätigung der Schaltfläche „*Änderung des Passworts für Studierende*“ bzw. „*Mail-forwarding/Mailalias für Studierende*“ poppt eine andere Maske auf:




In diese Maske sind der Login-Name und die PIN einzugeben.

Bei korrekter Eingabe von Passwort bzw. PIN folgt auf der Passwortseite (`https://userdb.uni-wuppertal.de/userdb/passwort/`) die eigentliche Maske zum Ändern des Passwortes:




In diese Maske ist das neue Passwort zweimal korrekt und identisch einzugeben. Wirksam wird es erst am nächsten Tag.

Bei korrekter Eingabe von Passwort bzw. PIN folgt auf der

Mail-Alias/Mail-Forwarding-Seite
(`https://userdb.uni-wuppertal.de/userdb/passwort/mail_info_vd_user.php`)

die eigentliche Maske zum Ändern der E-Mail-Daten:


In diese Maske kann dann eine **Vorwärts-Adresse** eingetragen werden, an die hier eingehende Mail weiter geleitet werden soll, bzw. ein E-Mail-Alias eingegeben werden. Ein Beispiel wäre `petra.mustermann` für die Zweit-Mail-Adresse `petra.mustermannuni-wuppertal.de`. Dabei gilt das „Windhundprinzip“ („Wer zuerst kommt...“): Eine bereits besetzte E-Mail-Adresse wird nicht akzeptiert. Falls bisher noch kein Mail-Alias eingegeben wurde, wird die Original-Mail-Adresse (im Beispiel `aa0006`) dafür verwendet. Wirksam wird alles erst am nächsten Tag.

Der SUSE-Mailserver enthält beispielsweise die Möglichkeit server-seitig Mailfilter nach dem Internetstandard

RFC 3028 SIEVE(`http://www.faqs.org/rfcs/rfc3028.html`)

einzusetzen.


Unter http://www.cyrusoft.com/sieve/ findet man interessante Beispielanwendungen.

### 1.1.6. Aliases (Spitznamen/Pseudonyme/Rollennamne/Positionen)

Alieses können als Zweit-, Dritt-, ... Mailadressen für verschiedene Zwecke benutzt werden:

- Persönliche Namen statt nur kryptische Loginnamen:

  `vorname.nachname@mycomp.de` statt `x2144@mycomp.de`

- Spitznamen statt langer Mailadressen
- Pseudonyme zur Verschleierung persönlicher Daten
- Rollennamen/Positionen wie z.B.

  `dekan@math.uni-wuppertal.de`

- Verteilerlisten wie z.B.

  `inf@math.uni-wuppertal.de`

- e-Mail-Listen (LISTSERV) zu Diskussionbszwecken ähnlich zu den Usenet-News, z.B.

  riscs (`http://catless.ncl.ac.uk/Risks/info.html`) Mailingliste statt `news:comp.risks`

  (meist Majordomo [`http://www.greatcircle.com/majordomo/FAQ.html`] basiert)

- Spezial-e-Mail-Adressen z.B. zur Registrierung eines Tagungsteilnahmewunsches,...

Aliases können lokal client-seitig (`$HOME/.mailrc` oder im Mailclient selbst (Adressbuch von Netscape, ...)), smpt-Serverseitig (`/etc/aliases` o.ä.) bzw. durch Web-Interfaces zu MTA's[7] eingerichtet werden.

In `/etc/aliases` kann zum Beispiel auch eine Einspeisung in den Standard-Input von Programmen vorgenommen werden

`/etc/aliases`

```
...
fax: "| /opt/local/bin/faxmail"
majordomo: "|/usr/lib/majordomo/wrapper majordomo"
...
```

[7] Mail transfer agent wie, z.B. `sendmail`, `smail`, `postfix`,...

### 1.1.7. Urlaubsbenachrichtigungen

Urlaubsbenachrichtigungen über momentane Abwesenheit können mit Hilfe von `vacation`

http://www.udel.edu/topics/e-mail/vacation.html

eingerichtet werden. Benutzt wird dabei der Mechanismus der `$HOME/.forward`-Datei.

**Bemerkung:**

- `vacation`-Benachrichtigungen sollten nie an LISTSERV-Listen auf den Eingang deren Nachrichten hin versandt werden
- `vacation`-Benachrichtigungen können Diebe von der Abwesenheit eines potentiellen Opfers informieren.

### 1.1.8. Literatur zum Kapitel 1.1

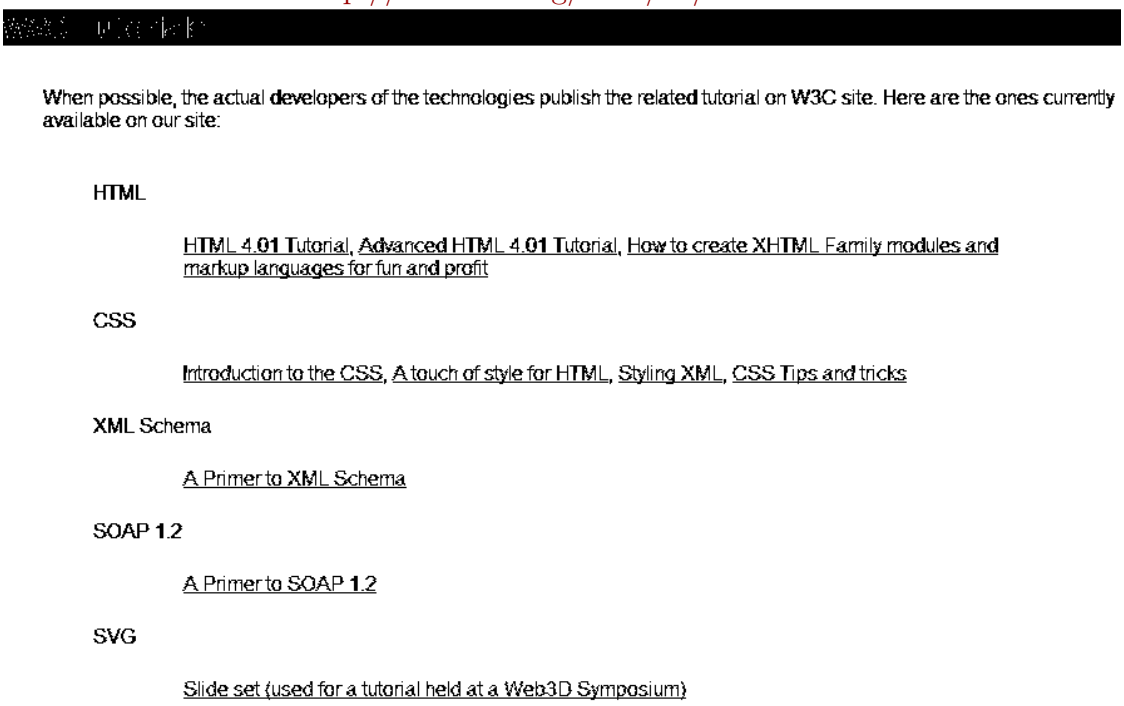

- The Whole Internet User's Guide, O'Reilly, 1994
- E. Krol et al.: The Whole Internet: The next Generation, O'Reilly, 1999
- W.G. Lehnert: Lights on the Web, Addison-Wesley, 2002

## 1.2. Bereitstellung von Internetinhalten

### 1.2.1. Eigene Webseiten/HTML

Arbeiten Sie die HTML[8]-Tutorials unter

http://www.w3.org/2002/03/tutorials



When possible, the actual developers of the technologies publish the related tutorial on W3C site. Here are the ones currently available on our site:

HTML

HTML 4.01 Tutorial, Advanced HTML 4.01 Tutorial, How to create XHTML Family modules and markup languages for fun and profit

CSS

Introduction to the CSS, A touch of style for HTML, Styling XML, CSS Tips and tricks

XML Schema

A Primer to XML Schema

SOAP 1.2

A Primer to SOAP 1.2

SVG

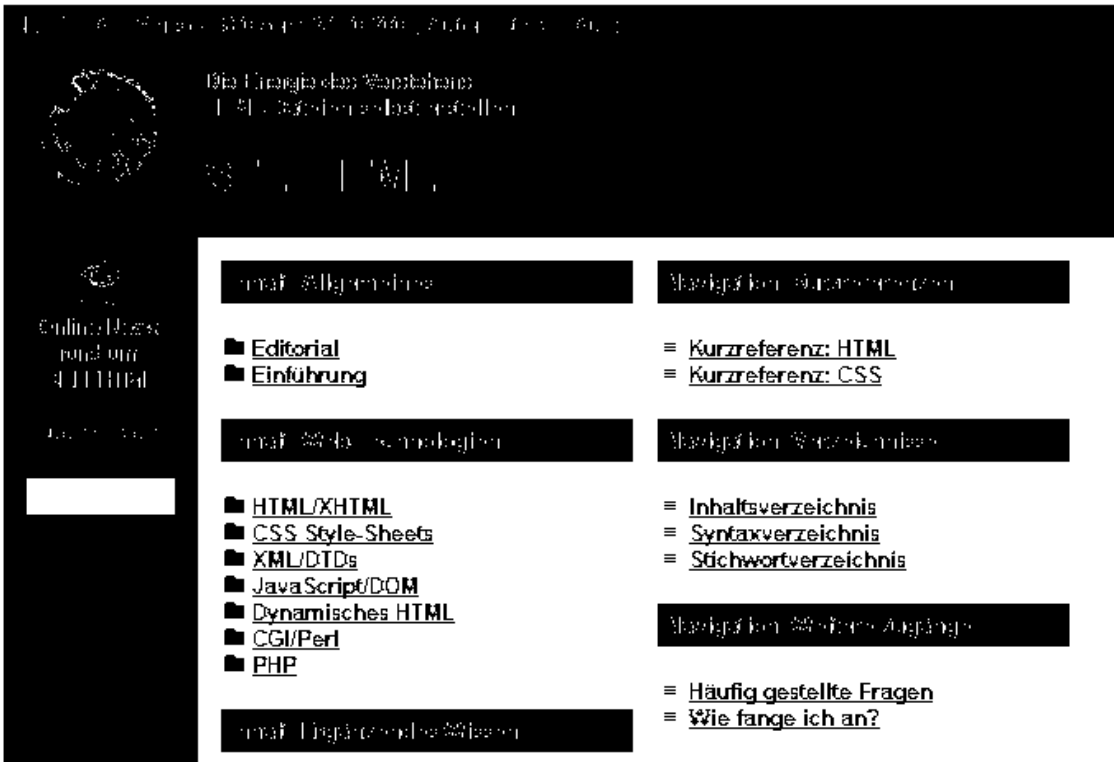
Slide set (used for a tutorial held at a Web3D Symposium)

selbstständig durch. Informieren Sie sich danach über Style Sheets (CSS), XML und SOAP.

[8]Hypertext markup language

Vertiefen Sie Ihre Kenntnisse mittels:

http://selfhtml.teamone.de/




Sehen Sie sich hier insbesondere die Kapitel über Javascript, dynamisches HTML und PHP sowie mySQL an. Benutzen Sie diese Kenntnisse, um eine eigene kleine Firmenpräsentation zu erstellen.

Über das bisher Empfohlene ist folgende Literatur nützlich (erhältlich z.B. bei einem der vielen EDV-Buchversand-Firmen (hier: `http://www.edv-buchversand.de`):

**Programmieren mit PHP**
Dynamische Webseiten erstellen
Verfasser/Autor: Lerdorf, Rasmus / Tatroe, Kevin
Verlag: O'Reilly Verlag
Sprache: deutsch
erschienen: 10/2002
Bestellnummer: OR-177
Preis: EUR 40,00

**PHP lernen**
Anfangen, Anwenden, Verstehen
Verfasser/Autor: Adler, Olivia / Holzgraefe, Hartmut
Verlag: Addison-Wesley
Sprache: deutsch

erschienen: 09/2002
Bestellnummer: AW-2000
Preis: EUR 24,95

**Programmieren lernen in PHP 4**
Ein kompakter Einstieg in die Webserverprogrammierung
Verfasser/Autor: Krause, Jörg
Verlag: Hanser
Sprache: deutsch
erschienen: 07/2001
Bestellnummer: HA-21754
Preis: EUR 24,90

**PHP 4 Kochbuch**
Lösungen, Bibliotheken, und Applikationen der PHP-Community
Verfasser/Autor: Krause, Jörg / Injac, Ilija
Verlag: Hanser
Sprache: deutsch
erschienen: 05/2002
Bestellnummer: HA-21856
Preis: EUR 49,90

**PHP 4 - Grundlagen und Profiwissen**
Webserver-Programmierung unter Windows und Linux
Verfasser/Autor: Krause, Jörg
Verlag: Hanser
Sprache: deutsch
erschienen: 04/2003
Bestellnummer: HA-22234
Preis: EUR 49,90

**PHP 4 - Die Referenz**
Aktuell zu PHP 4.0.5
Verfasser/Autor: Krause, Jörg
Verlag: Hanser
Sprache: deutsch
erschienen: 03/2001
Bestellnummer: HA-21687
Preis: EUR 34,90

**Bemerkung** zu in diesem Zusammenhang auftauchende Begriffen (vgl. z.B. http://www.w3.org):

**HTML:** hypertext markup language, eine Dokumentsbeschreibungs-Sprache mit „anklickbaren Referenzen“

**dynamische HTML, Javascript, ...:** Erweiterung rein statischer HTML-Dokumentbeschreibungseigenschaften um die Möglichkeiten „dynamischer“ Inhaltsänderungen

**CSS (Level 1 und 2):** cascading style sheets, Hilfsmittel zur einheitlichen stilistischen Modifikation des grafischen Erscheinungsbild der HTML-Elemente mehrerer HTML-Seiten

**DOM:** document object model, das plattformen- und sprachenunabhängig Programmen und Skripten den (auch modifizierenden) Zugriff auf Webseiteninhalte erlaubt.

**SGML:** standard generalized markup language, allgemeine sehr mächte (aber auch kompliziert zu nutzende) Dokumentsbeschreibungssprache. HTML ist eine spezielle „Anwendung“ von SGML.

**XML:** extensible markup language, ein (einfacherer) Sprachdialekt von SGML

**XHTML:** eine minimale Modifikation von HTML, so dass es, XHTML, ein gültiger XML-Unterdialekt wird.

**MathML:** mathematical markup language, das zusätzlich mathematisch Formeln als (nichtgraphisches) Dokumentenelement erlaubt.

**XSL:** extensible stylesheet language, Standard für Stylesheets in und für XML.

**XSLT:** extensible stylesheet language transformations, Standard für die Umwandlung von XML-Dokumenten in andere XML-Formate.

**SMIL:** synchronized multimedia integration language

**SVG:** scalable vector graphics, Standard für skalierbare Graphiken in XML.

**PHP:** hyptertext processor, eine Skriptsprache für dynamische HTML unsbesondere für Datenbankanbindung (mysql, ...) benutzt.

**Java:** objektorientierte plattformunabhängige Programmiersprache, deren Applets (im Web einbindbares Java-Programm) in Webseiten eingebunden werden können.

**Javas Server Pages, Servlets:** ein vom HTTP-Server bei den Seitenaufruf ausführbares Java-Programm.

**Java Entprise Beans:** modulare wiederverwendbare Java-Komponente.

**Sun One (Open Network Environment), Mircrosoft .Net:** Inegrationsplattform für Unternehmens-Middleware im IT-Bereich

Die Formeln

$$\nabla \cdot E = \frac{\rho}{\epsilon_0} \qquad \nabla \times E = -\frac{\partial B}{\partial t} \qquad c^2 \nabla \times B = \frac{\partial E}{\partial t} + \frac{j}{\epsilon_0} \qquad \nabla \cdot B = 0$$

werden in MathML etwa folgendermaßen dargestellt:

```
<mrow>
  <mi fontstyle="normal">&dtri;</mi>
  <mo>&middot;</mo>
  <mi fontstyle="normal">E</mi>
</mrow>
<mo>=</mo>
<mfrac>
  <mi>&rho;</mi>
  <msub>
    <mi>&epsiv;</mi>
    <mn>0</mn>
  </msub>
</mfrac>
<mrow>
  <mi fontstyle="normal">&dtri;</mi>
  <mo>&times;</mo>
  <mi fontstyle="normal">E</mi>
</mrow>
<mo>=</mo>
<mrow>
  <mo>-</mo>
  <mfrac>
    <mrow>
      <mi>&part;</mi>
      <mo>&ApplyFunction;</mo>
      <mi fontstyle="normal">B</mi>
    </mrow>
    <mrow>
      <mi>&part;</mi>
      <mo>&ApplyFunction;</mo>
      <mi>t</mi>
    </mrow>
  </mfrac>
</mrow>
```

⋮

Hier kommen noch Tabellen hin (ich weiß aber nicht mehr welche), die fanden sich nicht in der Datei! Da müßten Sie vielleicht noch einmal das alte Info II-Skript übersetzen und schauen

**Aufgaben:**

- Informieren Sie sich mit Hilfe des

  Free On-line Dictionary of Computing
  http://www.nightflight.com/foldoc/index.html

  über das Umfeld obiger Begriffe.

- Lesen Sie weitere Artikel und Tutorials unter

  http://www.w3.org

  und

  http://selfhtml.teamone.de

- Lesen Sie das LAMP- bzw. das LAMPS-Tutorial unter

  http://www.linux.computerbraxas.de

  bzw.

  http://www.baach.de

Eine Web-Seite sollte typischerweise folgenden Aufbau haben

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
        "http://www.w3.org/TR/html4/transitional.dtd">
<html>


<head>
<meta http-equiv="content-type" content="text/html; charset=iso-8859-1">
<!-- ... andere Angaben im Dateikopf ... -->
<title>Text des Titels</title>
</head>


<body>
<p>Dist ist der Text meiner Testseite
</p>


<address>
<a href="mailto:autorDieserSeite@firma.de">autorDieserSeite</a>
<br>
Firmenname, Straße und Hausnummer, PLZ und Ort, Land
<br>
&copy;  Hans MusterAutor
</address>

</body>


</html>
```

**Bemerkungen:**

- Die ersten Zeilen spezifizieren den Dokumententyp, in dem die Webseite geschrieben wurde. Dies sollte immer geschehen, damit Browser und Syntaxchecker die Seite möglichst genau darstellen bzw. überprüfen können.
- Damit Besucher der Webseite nicht durch von deren Browsern nicht unterstützten HTML-Erweiterungen „geärgert“ werden, sollte *immer* ein HTML-Standard-Dokumenttyp benutzt werden.
- Durch Angabe des benutzten Zeichensatzes im Meta-Tag können auch wirkliche Umlaute wie etwa

  äöüÄÖÜß

  benutzt werden und müssen nicht umständlich via

  ä ...

  kodiert werden. Der Webserver übermittelt nämlich diese Zeichensatzspezifikation, die dann vom Browser zur richtigen Seitendarstellung benutzt werden kann.
- Bei jeder Webseite darf die Nennung des presserechtlich Verantwortlichen nicht vergessen werden. Web-Präsentationen sollten professionell wirken. Deshalb dürfen nur syntaktisch korrekte Webseiten ins Netz gestellt werden.

Die syntaktische Korrektheit der HTML-Inhalte (und natürlich auch der CSS-Stylesheets) kann mittels eines Online-Überprüfungsdienstes des W3C überprüft werden. Am besten kann man dazu ein Markenzeichen (der syntaktische Korrektheit) in jede der Seiten einbauen:

```
<a href="http://validator.w3.org/check/referer">
<img border=0 src="http://www.math.uni-wuppertal.de/images/valid_html4.gif"
                align="right" alt="W3C 4.0 Checked!" width="88" height="31"></a>
```

**HTTP und Webinhalte**
Ein HTTP-Server übermittelt durch eine URI („uniform resource identifier“; früher URL=„uniform resource locator“) spezifizierte Resource als typlose Bytedatei.

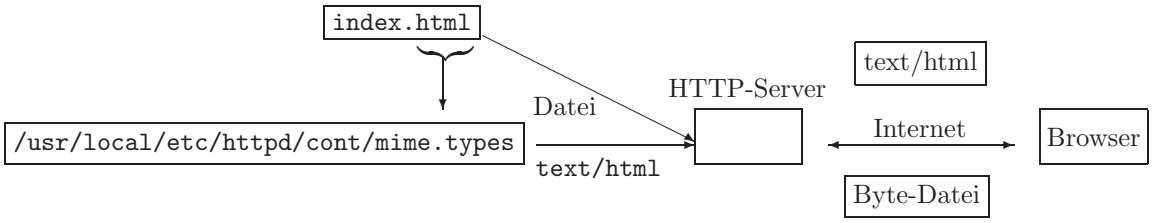
URI's, die häufig genutzt werden:

```
file://home/user/index.html
ftp://ftp.uni-stuttgart.de/pub/src
http://www.math.uni-wuppertal.de/~fpf
https://userdb.uni-wuppertal.de/userdb/passwort/
imap://imap.firma.de?fetch>...
news://news.uni-wuppertal.de/de.test
ldap://ldap.firma.de/o=firma,c=de
mailto:name@firma.de
```

Der Multimedia-Inhaltstyp wird durch den Dialog von Webserver und Browser in Form einer MIME-Kennung wie z.B.

```
image/gif
text/html
text/plain
text/css
  ⋮
```

vereinbart. Der Server entnimmt diesen Typ der Dateinamenserweiterung:




Mittels des Programms `wget` kann man das überprüfen:

```
% wget --verbose http://www.math.uni-wuppertal.de/css/math.css
--09:47:38--  http://www.math.uni-wuppertal.de/css/math.css
           => ‘math.css’
Resolving www.math.uni-wuppertal.de... done.
Connecting to www.math.uni-wuppertal.de[132.195.94.49]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,479 [text/css]

100%[====================================>] 2,479          2.36M/s    ETA 00:00

09:47:38 (2.36 MB/s) - ‘math.css’ saved [2479/2479]
```

Auch das Page-Info-Fenster von Netscape bietet diese Anzeige der „Eigenschaften“ einer durch URI spezifizierten Web Bytedatei.
Um z. B. ein S/MIME-Zertifikat downloadbar anzubieten, reich es für den Internet Explorer, dessen Dateinamen auf „`.der`„ enden zu lassen, sauberer aber — und für z. B.

Mozilla notwendig — ist es jedoch, den Web-Server für diese .der-Dateien den MIME-Typ

application/x-x509-email-cert

übermitteln zu lassen. Dies geschieht am besten durch hinzufügen der Zeile

```
AddType application/x-x509-email-cert .der
```

zur Datei `/etc/httpd/httpd.cont`[9].

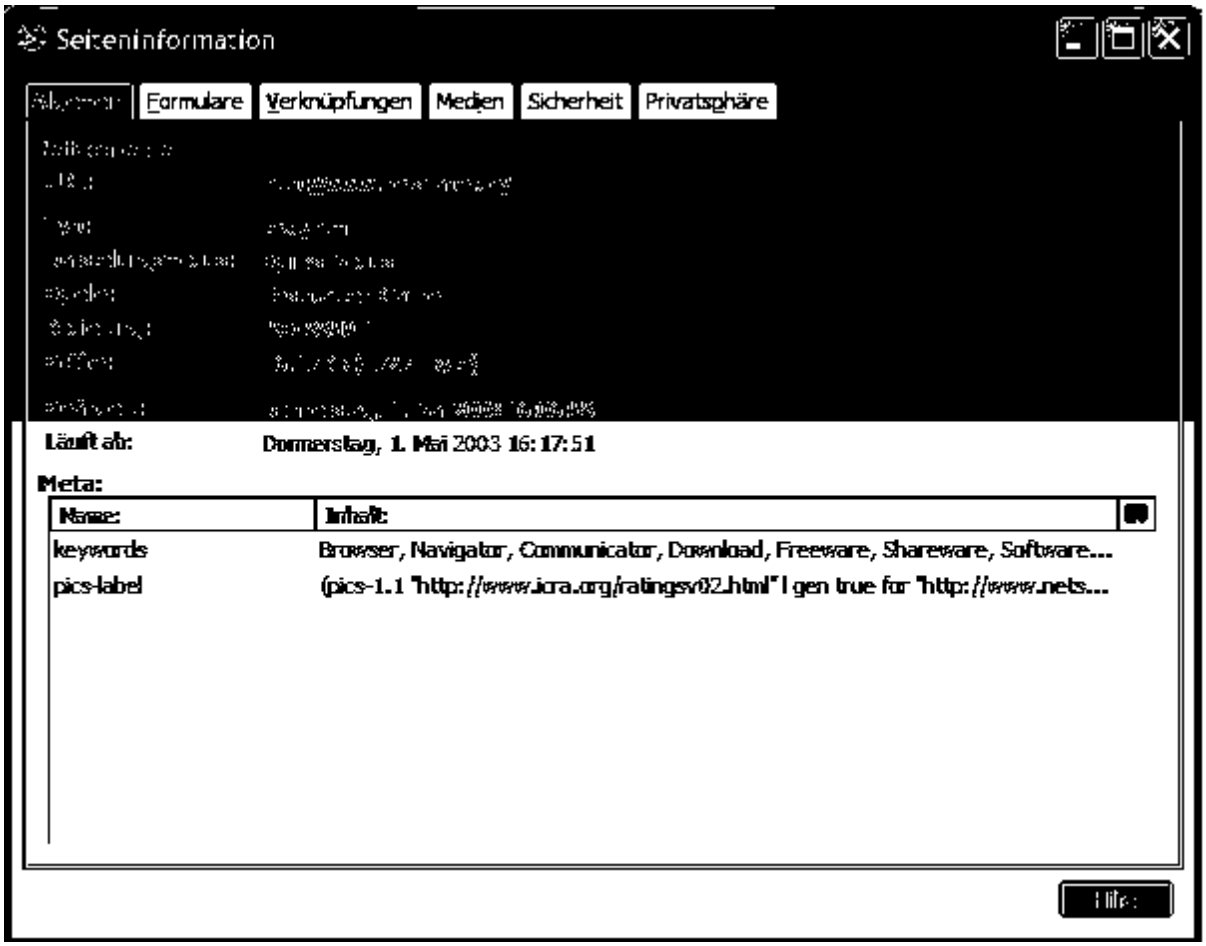



BILD bitte zuschicken

[9]Die Datei `/etc/httpd/mime.types` sollte nicht analog geändert werden, da sie bei jedem Update des http-Servers überschrieben wird und die Änderungen deshalb wieder entfallen würde!

#### 1.2.1.1. pdf-Dokumente im Web

Hinweise zu (hier aus LaTeXerzeugten) pdf-Dokumenten im Web:

---

Zur PDF-Wandlung aus .dvi-Dateien sollten folgende Gesichtspunkte berücksichtigt werden:

a). Wenn PS/EPSF-Dateien eingebunden sind, sollten diese durch Tools erzeugt werden, die eine „`%%BoundingBox:`“-Zeile erzeugen.

b). Benutzen Sie das LaTeX-Package:

```
\usepackage[dvips]{hyperref}
```

Dann sind folgende Möglichkeiten gegeben:

b1) Links auf externe Dokumente wie in:

```
\href{ftp://host.math.uni-wuppertal.de/pub/XXX/YYY}{Linktext}}
```

b2) Typische Texreferenzen werden automatisch zu in-Dokument Links verarbeitet:
Inhaltsverzeichnis-Einträge
Abbildungsverzeichnis
Tabellenverzeichnis
Index
Literaturverzeichnis (`\cite{}`)
Refenrenzen mittels `\ref{}` und `\pageref{}`

b3) Links von außen (HTML) in pdf-Dokumente hinein kann man mittels

```
<a href="script.pdf#section.1.1">
```

erzeugen.

b4) Durch

```
\clearpage
\pdfbookmark{Inhaltsverzeichnis}{Inh}
\tableofcontents
...
```

kann man Bookmarks für Inhaltsverzeichnis ... erzwingen.

b5) pdf-Dokumentinfos können durch

```
\hypersetup{%
pdftitle = {Titel der Arbeit},
pdfsubject = {xxx, yyy, ...},
pdfkeywords = {zzz, aaa, ...},
pdfauthor = {\textcopyright\ Dr. xxx yyyy},
bookmarksnumbered = true,
bookmarks = true,
bookmarksopen = true,
colorlinks = true
}
```

erzeugt werden.

---

**Bemerkung:**

- LaTeX Postscript-Dateien für das Web sollten nur dann in pdf gewandelt wernden, wenn sie lediglich Type1-Fonts (vektorbasiert und deshalb auch auf die Bildschirmauflösung skaliert gut lesbar, vergleiche auch http://www.dante.de/faq/de-tex-faq/html/fonts1.html) enthalten, was durch die Option `-Pwww` oder `-Ppdf -G0` bei dvips erreicht werden kann:

```
% latex Document
% dvips -Pwww -o Document.ps Document.dvi
% distill Document.ps
% acroread Document.pdf&
```

- Sollte die Windows-Version des Acrobat Distillers eingesetzt werden, so muss durch eine Option sichergestellt werden, dass alle benutzten (auch die Windows-) Fonts in das pdf-Dokument eingefügt werden: Dann sind solche pdf-Dokument auch problemlos auf anderen Rechner-Plattformen nutzbar!

#### 1.2.1.2. Tabellen und Frames

Tabellen ohne Begrenzungslinien (`border=0`) können zur zweidimensionalen Gestaltung von Webseiten genutzt werden, vergleiche

`http://www.math.uni-wuppertal.de`.

Alle solchermaßen aufgebauten Seiten sind vollfunktional nutzbar:

- Bookmarks (Lesezeichen) funktionieren,
- Links sind als email versendbar,
- Links im Web auf solche Seiten sind direkt möglich.

Seiten die mit Hilfe von Frames, vergleiche

`http://selfhtml.teamone.de/frames`,

angelegt werden, sind eher für ein applikationsähnliches Web-Design geeignet. Die obige Funktionalität der genauen Lokalisierung von Unterseiten ist bei der Verwendung von Frames *nicht* mehr möglich.

| |
|---|
| Darum sind immer durch Tabellen mit Hilfe von Musterseiten erzeugte[10] Webauftritte einem Webauftritt mit Frames vorzuziehen. |

Zudem arbeiten viele Suchmaschinen mit Frames nicht mehr wie bei Seiten ohne Frames. So werden Suchwörter im Seitentext nicht gefunden und damit die Relevanz des Auftritts niedriger eingestuft.

**Bemerkung:**
Frames werden häufig zur URI-Umleitung eingesetzt

- nach Umorganisation von Webservern,
- zur „Verschleierung“ von (sich eventuell ändernden) URI's,
- zur („unsichtbaren“) Umleitung auf einen anderen Webserver, wobei die Adressleiste immer noch die Urpsrungs-URI anzeigt,
- ...

[10] siehe auch Abschnitt 1.2.3

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
        "http://www.w3.org/TR/html4/transitional.dtd">
<html>


<head>
...
</head>

<frameset cols="100%,*" border="0" frameborder="0" framespacing="0">
        <frame scr="http://www.test.de" noresize frameborder="0">
</frameset>

<body>
<noframes>
...
</noframes>
</body>
</html>
```

Dies bewirkt, dass eine einziger unsichtbarer Frame für die ganze Seite eingerichtet wird, in den dann die Zielseite geladen wird, Um dieses Frameset einzurichten, muss man etwas mit den Tücken der unterschiedlichen Browser kämpfen, `cols="100%"` würde theoretisch genügen, um einen einzelnen Frame über die ganze Seite einzurichten. Netscape möchte aber mindestens zwei Frames habenm deshalb ist die Angabe `cols="100%,*"` erforderlich, Damit werden zwei Frames eingerichtet, einer mit 100 % Breite und einer für den Rest (also nichts). Außerdem gibt es Unterschiede bei den Browsern, wenn es darum geht, den Frame-Rahmen unsichtbar zu machen. Für Netscape schreibt man `frameborder="0"` innerhalb des `<frameset>`-Tags, für Microsoft `frameborder="0" framespacing="0"`. `frameborder="0"` innerhalb des `<frame>`-Tags ist schließlich die Notation, die die HTML 4.0-Spezifikation vorsieht.
Zum Umleiten kann auch ein Meta-Tag im `head`-Teil einer normalen HTML-Seite dienen:

```
...
<meta http-equiv="refresh" content=5"; URL=http://www.meinefirma.de/neu/">
...
```

(Zusätzlich gibt es noch Web-Server-Redirects).

Man beachte, dass bei Redirects der Zurück-Knopf des Web-Browsers in Funktion bleiben sollte: Man verzögere also die Redirects mindestens um ein paar Zehntel Sekunden, so dass der doppelte Klick auf den Zurück-Knopf noch funktioniert.

### 1.2.2. Dynamic HTML und Javascript

Mittels „dynamic HTML“ lassen sich Elemente einer Scriptsprache (php oder hier Javascript) zur „automatischen Erzeugung von HTML-Zeilen einsetzen: Die volle Dynamik (Schleifen, Fallunterscheidungen, ...) einer „Programmiersprache“ steht dann also auch für HTML-Seiten zur Verfügung.

Einfache Effekte mittels Javascript werden auf der Seite

http://www.math.uni-wuppertal.de/org/web-ag/Muster/TUTORIUM/

beschrieben.

- Seitenzählung
- Knöpfe zum Blättern in einer Präsentation
- überblendbare Bilder bis hin zur „Video“-Animation
- Öffnen neuer Fenster und automatische Schließen solcher Fenster beim Verlassen der Webseite
- rechteckige Hypertext-Ankerbereiche in Bildern
- ...

Eine Vertiefung ist mittels

http://selfhtml.teamone.de/javascript/

bzw.

http://selfhtml.teamone.de/dhtml/index.htm

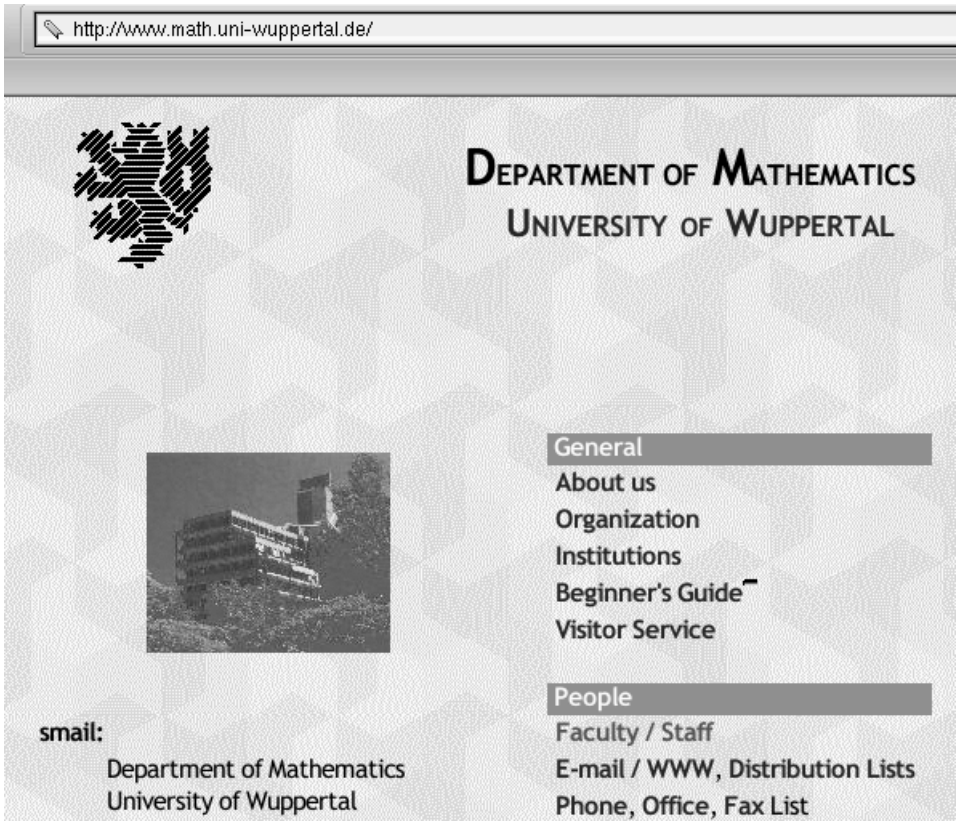
und

http://devedge.netscape.com/library/manuals/2000/javascript/1.5/guide

möglich.

### 1.2.3. Eine zentrale Stelle für die gemeinsamen Inhaltsanteile einer Sammlung von HTML-Seiten

... am Beispiel der Webseite des Fachbereichs Mathematik der Universität Wuppertal.




```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
        "http://www.w3.org/TR/html4/loose.dtd">
<HTML>
<HEAD>
<base href="http://www.math.uni-wuppertal.de/" >
   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" >
   <title> Universitaet Wuppertal / Fachbereich Mathematik: WWW Startseite
  </title>
<link rel="stylesheet" href="http://www.math.uni-wuppertal.de/css/math.css" type="text/
    css" >
...
```

Ein gemeinsamer Stil für das Web-Subsystem wird im css-File `math.css` definiert:

```
A, BLOCKQUOTE, BODY, CITE, CODE, DD, DEL, DFN,
DIV, DL, DT, EM, FORM, H1, H2, H3, H4, H5, H6, IFRAME, IMG, KBD,
LI, OBJECT, OL, P, Q, SAMP, SMALL, SPAN, STRONG, SUB, SUP, UL, VAR,
APPLET, BIG, CENTER, DIR, FONT, HR, MENU, PRE,
ABBR, BDO, BUTTON, FIELDSET, INS, LABEL {
   word-spacing : normal;
   letter-spacing : normal;
   text-transform : none;
   text-decoration : none;
   border-color : black;
   border-style : none;
}
```

```
BODY, P, H1, H2, H3, H4, H5, H6, DT, TH {
   font-family : 'Trebuchet MS', Verdana, 'Myriad Web', Syntax, arial, helvetica, sans-
       serif;
}

BODY {
   background : url(http://www.math.uni-wuppertal.de/bg/hg2_128c.gif) repeat fixed 0 0;
   padding : 0;
   border-width : 0;
   width : auto;
}

VAR, CITE, DFN, .note {
   font-style : italic;
}

UL, OL, LI,
P, HR, H1, H2, H3, H4, H5, H6,
STRONG, STRONG EM, EM STRONG, EM,
DIV, DL, DD, DT, COLGROUP, COL, BLOCKQUOTE,
TABLE, TR, THEAD, TH, TFOOT, TD, TBODY {
   color : black;
}

TABLE, TR, TD, TBODY {
   text-decoration : none;
   border-style : none;
   border-color : black;
}

STRONG EM, EM STRONG {
   font-style : normal;
   font-weight : bolder;
   text-transform : uppercase;
}

STRONG {
   font-style : italic;
   font-weight : bold;
}

INS {
   background : yellow;
}

I {
   font-style : italic;
}

EM {
   font-style : normal;
   font-weight : bold;
}

DEL {
   background : #f66;
}

COLGROUP, COL {
   text-decoration : none;
   border-style : none;
   border-color : black;
}

B {
```

```
   font-weight : bold;
}

ADDRESS, ACRONYM {
   word-spacing : normal;
   letter-spacing : 0.1em;
   text-transform : none;
   text-decoration : none;
   border-color : black;
   border-style : none;
}

ADDRESS {
   font-style : normal;
   color : black;
}

ACRONYM {
   font-variant : small-caps;
}

A:visited {
   font-weight : bold;
   color : #008080;
   text-decoration : none;
}

A:link {
   font-weight : bold;
   color : #0000ff;
   text-decoration : none;
}

A:hover {
   color : #f00;
   text-decoration : none;
}

A:active {
   font-weight : bold;
   color : #008080;
   text-decoration : none;
}

A.offsite {
   font-weight : normal;
   color : #c66;
   text-decoration : none;
}

.warning {
   font-style : normal;
   font-weight : bolder;
   color : black;
   text-transform : none;
}

.blue {
   color : blue;
}

.brown {
   color : rgb(165,42,42) ;
}

#colophon {
```

```
   display : none;
}

#auto3173331733 {
   text-decoration : none;
}

#auto3173231732 {
   text-decoration : none;
}
```

Weiter geht es mit gemeinsamen Javascript-Funktionen,

```
...

<script src="http://www.math.uni-wuppertal.de/js/math.js" type="text/javascript">
</script>
</HEAD>

<body>

<!-- ========================================== -->

<noscript>
<p>    Diese Seite benutzt Javascript und sollte deshalb nur unter
    Javascriptfähigen Browsern betrachtet werden.</p>
</noscript>

...

<!-- :::::::::::::::::::::::::::::::::::::::::: -->



<script  type="text/javascript">
<!--
footer("800");
// -->
</script>

</body>
</html>
```

die mittels der Javascript-Funktion `footer()` die gemeinsamen Fußzeilen aller Seiten des Web-Subsystems zentral an einer Stelle definieren:

```
function footer(xwidth) // table width string
{
if (xwidth == null) { xwidth = "100%" }
lastmod = self.document.lastModified   // last modified date
while (isNaN(lastmod.substring(0,1))) { lastmod = lastmod.substring(1,100) } // delete
    Mo..So
document.writeln('<div align="center"><center>')
document.writeln('<table border="0" width="',xwidth,'">')
document.writeln(' <tr><td colspan=5><hr></td></tr>')
document.writeln(' <tr><td>')
document.writeln('     <a href="http://www.aic.uni-wuppertal.de/FB7/Math-Net/index_en.
    htm" target="_top">')
document.writeln('     <img src="http://www.math.uni-wuppertal.de/images/mathnet2.gif"
    alt="local MathNet Guide" border="0"></a>')
document.writeln('  </td><td>')
document.writeln('    <font color="#000000"><B>',lastmod,'</B></font>')
document.writeln('  </td><td>')
document.writeln('    <a href="mailto:webmaster@math.uni-wuppertal.de">')
document.writeln('       <img alt="" src="http://www.math.uni-wuppertal.de/images/
    letter.gif" align="bottom" border="0">')
```

```
document.writeln('        <font color="#000000">Webmaster</font></A>')
document.writeln('  </td><td>')
document.writeln('   <object>')
document.writeln('   <a href="http://validator.w3.org/check/referer"><img border="0"')
document.writeln('       src="http://www.math.uni-wuppertal.de/images/valid-html401.gif
    "')
document.writeln('       alt="W3C HTML 4.01 checked" height="31" width="88" align="
    right"></a>')
document.writeln('   </object>')
document.writeln('  </td><td>')
document.writeln('   <object>')
document.writeln('    <a href="http://www.MathePrisma.uni-wuppertal.de/MathePrisma/"
    target="_top">')
document.writeln('    <img src="http://www.math.uni-wuppertal.de/images/Mathe-Prisma.
    gif" alt="Mathe-Prisma" border="0" align="right"></a>')
document.writeln('   </object>')
document.writeln(' </td></tr>')
document.writeln('</table>')
document.writeln('</center></div>')
}
```

Damit ist das Problem gelöst, dass bei Benutzung von Tabellen statt Framesets zunächst bei notwendigen nachträglichen Änderungen (hier z.B. der Fußzeilen) viele Dateien geändert werden müssten. Bei Benutzung von Javascript reicht die Änderung an einer zentralen Stelle! Jedoch ist aus Sicherheitsgründen auf einigen Systemen potentieller „Kunden“ Javascript deaktiviert, so dass ein `<noscript>`-Bereich um so wichtiger wird.

## 1.2.4. Formulare in Webseiten

Die Interaktion des Web-Seiten browsenden Internetnutzers mit dem Betreiber des Web-Servers kann mittels HTML-Formularen in der folgenden Weise geschehen:

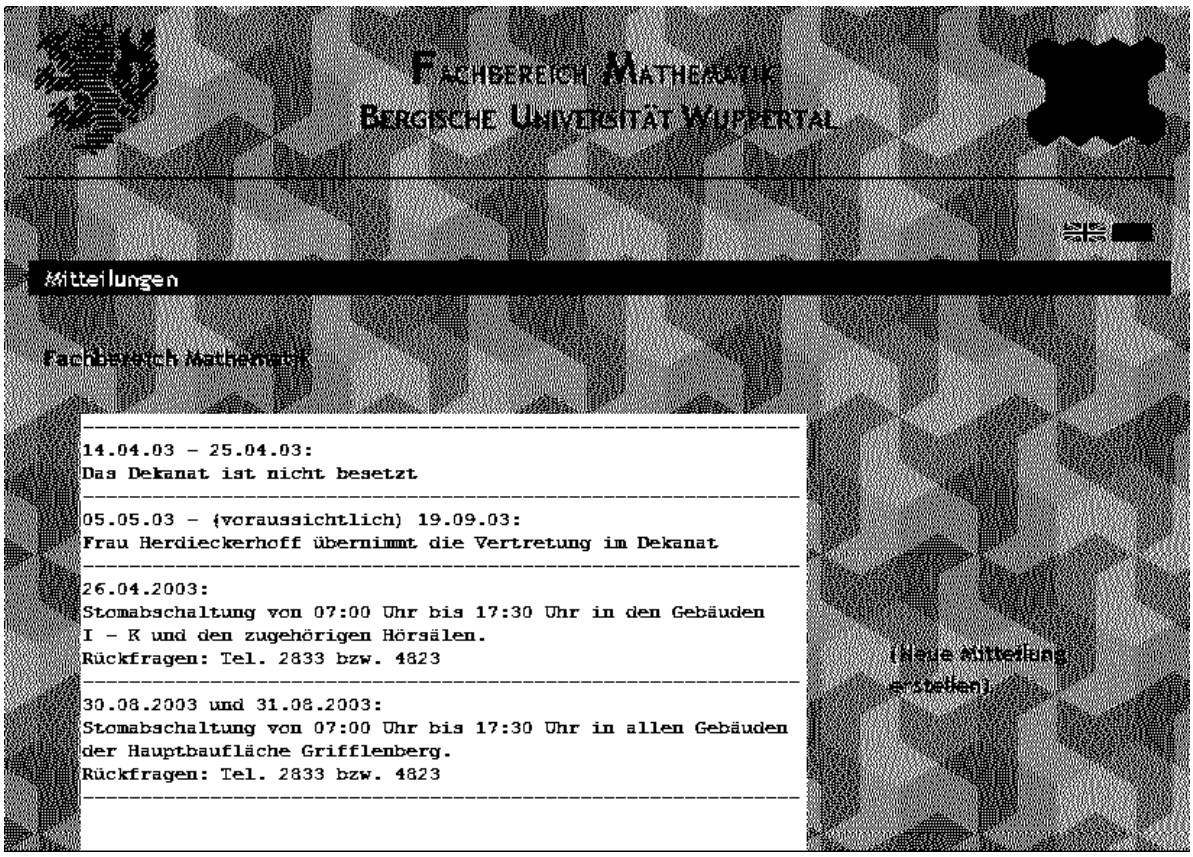

in HTML sieht das folgendermaßen aus:

```
...
<td align="left">
     <b>Bitte neue Mitteilung eintragen und absenden!</b>


     <form method="post" action="mailto:webmaster@math.uni-wuppertal.de"
        enctype="text/plain">
      <p>
      <textarea name="Message" rows="4" cols="80"></textarea>
      <p>
      <input type="submit" value="absenden">   
      <input type="reset" value="löschen">
     </form>

</td>
...
```

Wenn der Internetnutzer auf den Absende-Knopf klickt, wird der Inhalt des Textbereichs als email an die `mailto`-URI gesendet. Der Adressat fungiert als Moderator und kann den übermittelten Inhalt zum Beispiel in eine Webseite (schwarzes Brett) übertragen:




die email sieht dabei ähnlich zu

| | |
|---|---|
| **Content-type:** | text/plain |
| **Content-disposition:** | inline;form-data= |
| **Content-Transfer-encoding:** | 8BIT |
| **X-Accept-Language:** | en |

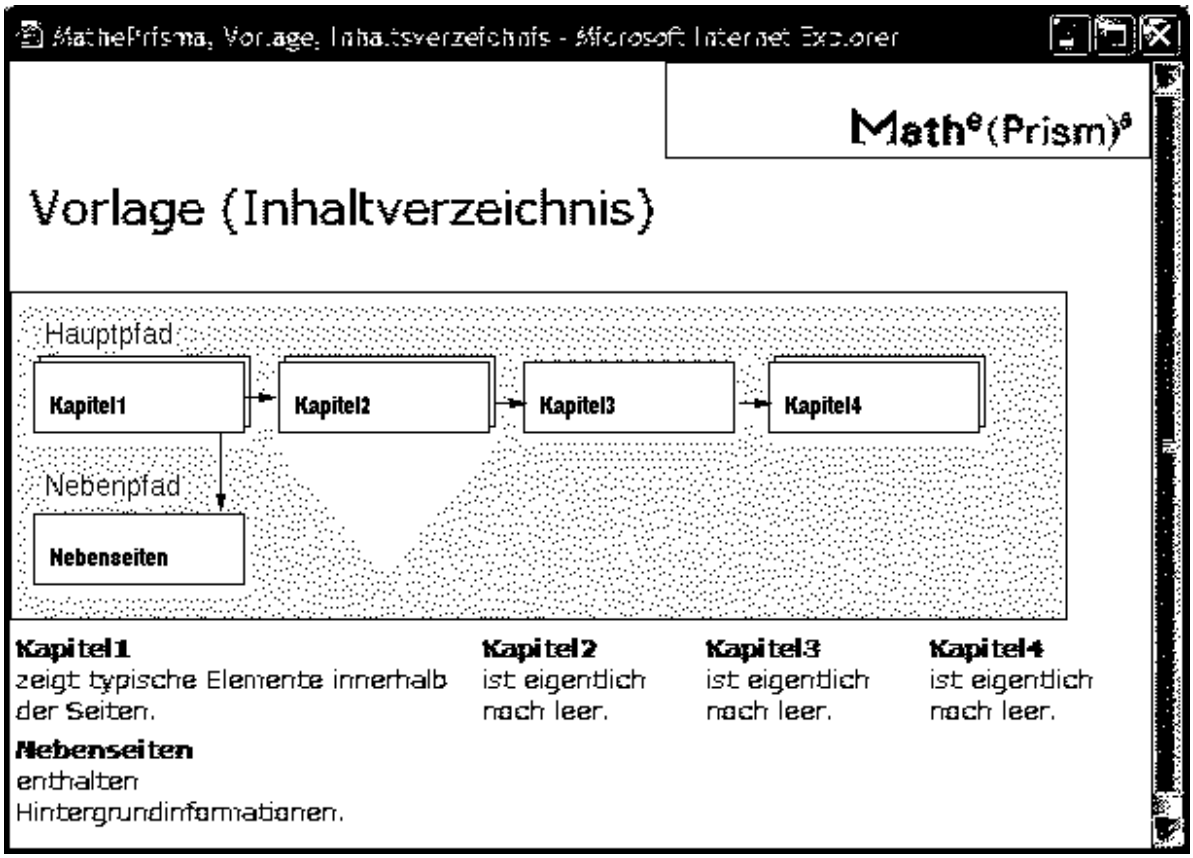
Message=Testnachricht für Internettechnologien

aus, das heißt

Name_des_Formular_Elements=Interaktionsinhalt

### 1.2.5. Client-seitige Maps

In Bildern können Rechteck-, Kreis oder Polygonbereiche als anklickbare Anker für URI's benutzt werden. Die Inhaltsübersicht




unterlegt man folgendermaßen

```
<MAP NAME="Uebersicht">
  <AREA ALT="" NAME="Kapitel1"   COORDS= " 12, 35, 120,  72"  a href="Seite01.html">
  <AREA ALT="" NAME="Kapitel2"   COORDS= "139, 35, 246,  72"  a href="Seite03.html">

  <AREA ALT="" NAME="Kapitel3"    COORDS= "265, 35, 372,  72"  a href="Seite05.html">

  <AREA ALT="" NAME="Kapitel4"    COORDS= "390, 35, 499,  72" a href="Seite06.html">

  <AREA ALT="" NAME="Nebensei" COORDS= "12, 114, 120, 150" a href="Nebensei.html">
 </MAP>

<IMG SRC="Pics/uebersic.jpg" HEIGTH="169" WIDTH="544" BORDER=0 USEMAP= "#Uebersicht"
    ALT="">
```

mit rechteckigen Hypertext-Links. Dazu muss man zunächst die Koordinaten der linken oberen Ecke und der rechten unteren Ecke der jeweiligen Rechtecke (zum Beispiel mit xv) bestimmen:

Kapitel 1

(12,35),(120,72)

...

Nebenseiten

(12,114),(120,150)

### 1.2.6. Standardisierung von Web-Subsystemen

Arbeitet ein Team an gemeinsamen Seiten einer Abteilung, eines Projekts, einer Firma, ..., so sollte der gemeinsame Stil neben der Vorgabe einer zu benutzenden CSS-Datei durch Festlegungen wie etwa dem folgenden standardisiert werden:

**Muster-Standardisierung**

| | **Layoutvorschriften**<br>**- Wenige, aber unbedingt einzuhaltende Vereinbarungen -** |
|---|---|
| Text in der linken Spalte steht rechtsbündig und ist etwas kleiner als rechts. | Auf dieser Seite sollen die wichtigsten Layoutvorgaben zur Erstellung von HTML-Seiten für MathePrisma-Module zusammengefaßt werden. Es geht hier nicht darum, wie diese mit dem PageComposer zu realisieren sind. Informationen darüber finden Sie hier (`http://www.math.uni-wuppertal.de/org/web-ag/Muster/TUTORIUM/develop1.htm`).<br><br>Ferner sind auf dieser Seite lediglich die Layoutvorschriften notiert. Sprachliche Hinweise und Leitlinien zur didaktischen Aufbereitung finden Sie anderswo...<br><br>• Eine MathePrisma Seite ist grundsätzlich als zweispaltige Tabelle aufgebaut. Die linke Spalte erhält 18%, die rechte 82% der Gesamtbreite. Auf dieser Seite sind die Rahmen dieser Tabelle sichtbar, die in den fertigen Modulen unsichtbar sind.<br><br>• Während in der rechten Spalte der fortlaufende Haupttext steht, ist die linke Spalte für kurze Randnotizen reserviert.<br><br>• Für die linken Spalte sind folgende Vereinbarungen gültig:<br>– Der Text steht rechtsbündig.<br>– Wir benutzen Heading 5.<br><br>• Für Text in der rechten Spalte verwenden wir die Voreinstellungen. |

| | |
|---|---|
| | • Damit die Randnotizen gleicher Höhe mit dem Haupttext stehen, ist es notwendig, die Tabelle in mehrere Zeilen zu unterteilen. Die Randnotizen werden dann entsprechend ausgerichtet.<br>• Als Hintergrund ist die Datei „MathePBg.gif“ zu verwenden. |

zur Gestaltung des Haupttextes

Damit der Haupttext nicht zu einem Bandwurm entartet, hier einige Regeln zur Auflockerung:

- Als gestalterische Mittel sind bevorzugt zu verwenden:
  - Einrückungen
  - Listen
  - Aufzählungen
  - Rahmen und (dezentes!) farbliches Unterlegen
  - Skizzen, Bilder
- Worauf man weitgehend verzichten sollte, sind Hervorhebungen einzelner Wörter im Text.

**Faustregel**
uf hundert Wörter sollten Sie nicht mehr als eins hervorheben.

- Wenn Sie trotzdem nicht auf Hervorhebung einzelner Wörter verzichten möchten, so ist dies durch Benutzung festgelegter Farben zu realisieren:
  - Als Verknüpfung mit blauer Farbe (Farbsymbol `"blue"`; RGB: 0 0 255 bzw. 00 00 FF hex.)
  - Als normaler Text in brauner Farbe (Farbsymbol `"brown"`; RGB: 165 42 42 bzw. A5 2A 2A hex.)
- Weitere Stilmittel sind NICHT erlaubt, also
  - kein Unterstreichen ,
  - nix *Kursives*,
  - kein **Fettdruck**,
  - keine anderen Schriftgrößen,
  - und auch sonst nichts außer den beiden Farben.
- Um die Titelzeile abzusetzen, empfehlen wir Heading 3.

| | |
|---|---|
| Titeleintrag nicht vergessen! | • Zu jeder Seite gehört ein Titeleintrag, der in der obersten Zeile des Browsers erscheint und auch von Suchmaschinen oft referiert wird. Für den Eintrag benutzen wir folgende Konvention:<br>  |
| Kurzübersicht | • Zu jedem Modul gehört eine Kurzübersicht. Diese dient als Navigationshilfe durch das Modul. Themen der Haupt- und Nebenpfade werden dargestellt.<br>• Der Hauptpfad enthält nur die Informationen, die zum Verständnis eines Moduls unbedingt notwendig sind.<br>• Ergänzende Inhalte, wie z.B.<br>– Ergänzungen zur Begriffsbildung, Technik,...<br>– Erklärung von Fachausdrücken, soweit sich diese nicht auch intuitiv verstehen lassen, man aber exakt bleiben möchte.<br>– Evtl. Beweise von Sätzen<br>– weitere oder komplexere Beispiele<br>– Lebensläufe, Anekdoten...<br>gehören in die Nebenpfade. |
| Seitenlayout | • Versuchen Sie, Ihr Modul in kurze Seiten zu unterteilen, so daß der Anwender möglichst nicht scrollen muss. Bedenken Sie dabei auch, daß die Module in einen Frame eingebettet werden und daher das Sichtfenster weiter verkleinert wird.<br>• Um einen Eindruck vom Aussehen der Seite auf der 800x600 Zielplattform zu erhalten, starten Sie bitte Netscape mit dem Kommando<br>netscape -geom 800x600 &<br>und wählen eine Font-Größe von 14.0. |

| | |
|---|---|
| Navigationsleiste | • Jede Seite wird abgeschlossen durch eine Navigationsleiste. Unter einem horizontalem Strich befinden sich ein Vorwärts- und ein Rückwärtsknopf, mit denen man zur vorhergehenden bzw. nächsten Seite des Hauptpfades (siehe Kurzübersicht) springen kann. Neben dem rechten Knopf kann ein kurzer Hinweis stehen. |
| |  nächstes Kapitel: Tutorial  |

### 1.2.7. Überprüftes syntaktisch korrektes HTML — ein Gütezeichen einer Präsentation

Jede HTML-Seite sollte auf syntaktische Korrektheit überprüft werden. Heute sollte man eine der HTML-Versionen

HTML 4.01,

XHTML 1.0

oder

XHTML 1.1

benutzen. Alte nicht zu aktualisierende HTML-Seiten dürfen durchaus auch eine älteren Version benutzen.
Baut man auf jeder Seite als Markenzeichen einen Link der Form


mittels

```
<p>
 <a href="http://validator.w3.org/check/referer"><img border="0"
        src="http://www.w3.org/Icons/valid-html401" alt="W3C HTML 4.01 checked" height=
            "31" width="88"></a>
</p>
```

ein, so ist man durch einfaches Anklicken in der Lage, einen erneuten Syntaxcheck durchzuführen:

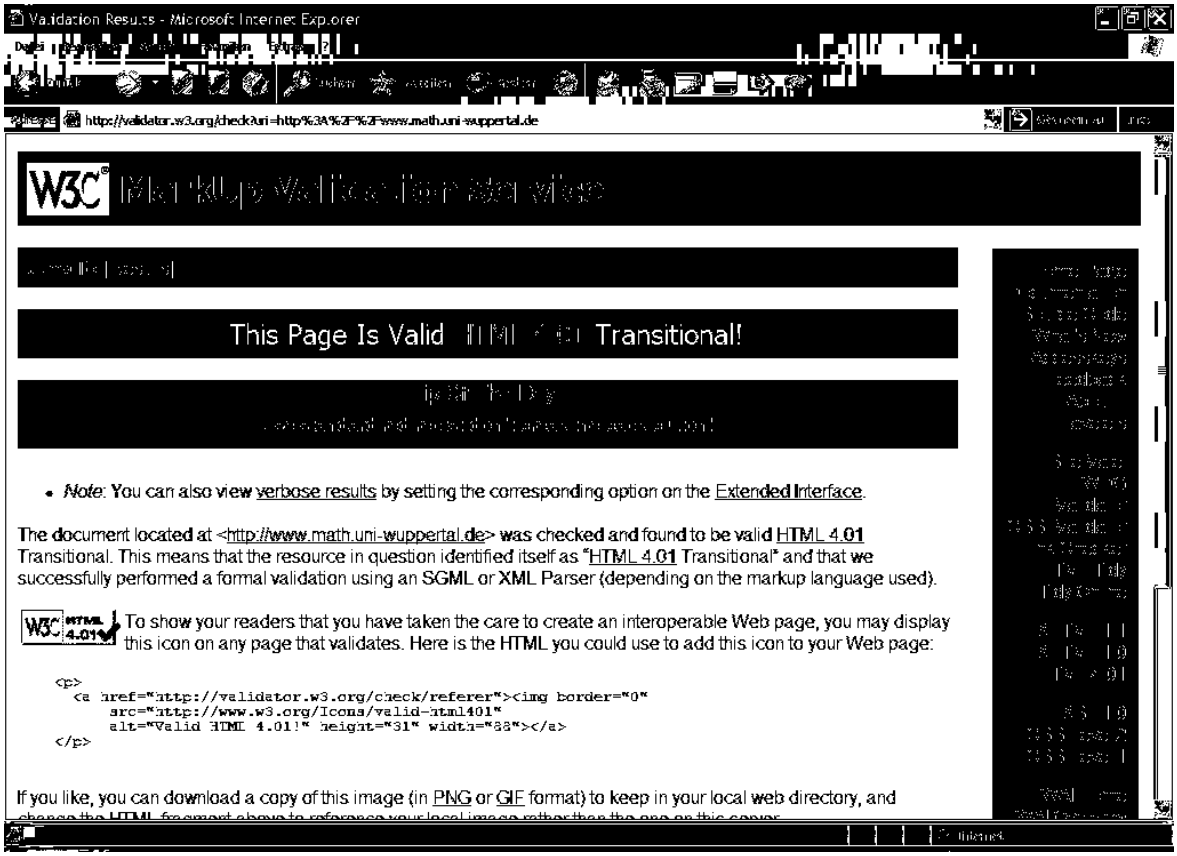



Abbildung 1.27.: HTML 4.01 Validierung

**Bemerkung:** Zur Auswahl der richtigen Version sollte in jeder HTML-Seite die `doctype`-Zeile nicht vergessen werden.

**Aufgabe:** Welche Vorteile hat es, wenn man ein syntaktisch korrektes HTML anbietet?

### 1.2.8. Webangebote in Varianten

Verschiedene Sprachen kann man seit der Existenz von HHTP 1.1 mit einem Variantenaushandlungssystem (für Sprachen, für Qualitätsstufen von Multimediaangeboten, ...) am günstigsten durch die Bereistellung von zum Beispiel

index.html.de,

index.html.en,

...

statt

index.html

bereitstellen. Der Apache-Webserver bietet sie den automatisch dem (richtig konfigurierten) Webbrowser an.

### 1.2.9. Einbinden von Flash-Animationen

Mit

```
<object classid="CLSID:D27CDB6E-AE6D-11cf-96B8-444553540000"
        codebase="http://active.macromedia.com/flash2/cabs/swflash.cab#version=4,0,0,0"
        width="90" height="40"> <param name="movie" VALUE="test.swf">
        <param name="quality" value="high">
        <param name="scale" value="exactfit">
        <param name="menu" value="true">
        <param name="bgcolor" value="#000040">
</object>
```

können Flash-Animationen in den HTML-Quelltext eingebunden werden.

# Literatur:


- Flash MX professionell, Carlo Blatz und die Powerflasher **Galileo Design** 598 S., 2002, mit CD, ISBN: 3-89842-222-4
- ActionScript. Das Praxisbuch., Matthias Kannengiesser, **Franzis**, 850 S., Oktober 2002, ISBN: 3-77236-797-6
- Flash MX. Grundlagen und Praxiswissen, Sascha Wolter , Saban Ünlü, **Galileo Press** , 425 S, Juni 2002, mit CD, ISBN: 3-89842-220-8
- Macromedia Flash MX - Das offizielle Trainingsbuch, Chrissy Rey, Macromedia Inc., 330 Seiten, **Markt & Technik Buch und Softwareverlag GmbH**, September 2002, 3-82726-352-2

## 1.3. Ausblick: Java

Mittels der Zeile

```
<appelt codebase="Applet1" code=stat.class width=90 height=20>
```

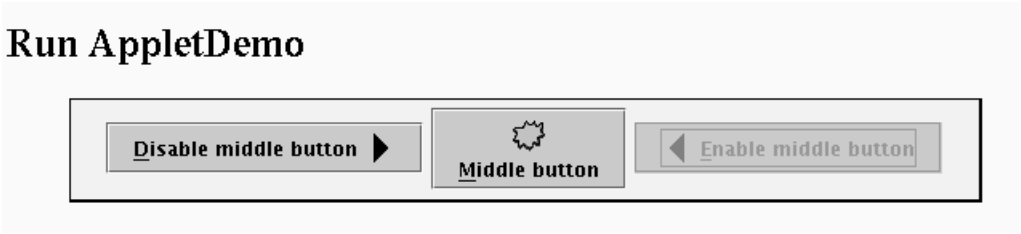
oder alternativ

```
<object classid="java:stat.class" codetyte="application/java-vm" width="90"
        height="20"> </object>
```

kann man ganze Java-Applikationen als HTML-Objekte in ein Websystem einbauen. Genaueres erfährt man in:

- D. Flanagan: Java in a Nutshell, O'Reilley,
- D. Flanagan: Java Enterprise in a Nutshell, O'Reilley,
- ...

Ein Beispiel:




Der dazugehörige Java-Quellcode:

```
/*
 * Swing 1.1 version (compatible with both JDK 1.1 and Java 2).
 */
import javax.swing.*;
import java.awt.*;
import java.awt.event.*;
import java.net.URL;

public class AppletDemo extends JApplet
                        implements ActionListener {
    protected JButton b1, b2, b3;

    protected static final String DISABLE = "disable";
    protected static final String ENABLE = "enable";

    protected String leftButtonFilename = "images/right.gif";
    protected String middleButtonFilename = "images/middle.gif";
    protected String rightButtonFilename = "images/left.gif";

    private boolean inAnApplet = true;
    URL codeBase; //used for applet version only

    //Hack to avoid ugly message about system event access check.
    public AppletDemo() {
        this(true);
    }
```

```
    public AppletDemo(boolean inAnApplet) {
        this.inAnApplet = inAnApplet;
        if (inAnApplet) {
            getRootPane().putClientProperty("defeatSystemEventQueueCheck",
                                            Boolean.TRUE);
        }
    }

    public void init() {
        setContentPane(makeContentPane());
    }

    public Container makeContentPane() {
        ImageIcon leftButtonIcon;
        ImageIcon middleButtonIcon;
        ImageIcon rightButtonIcon;

        if (inAnApplet) {
            URL leftButtonURL = getURL(leftButtonFilename);
            URL middleButtonURL = getURL(middleButtonFilename);
            URL rightButtonURL = getURL(rightButtonFilename);

            leftButtonIcon = new ImageIcon(leftButtonURL);
            middleButtonIcon = new ImageIcon(middleButtonURL);
            rightButtonIcon = new ImageIcon(rightButtonURL);
        } else {
            leftButtonIcon = new ImageIcon(leftButtonFilename);
            middleButtonIcon = new ImageIcon(middleButtonFilename);
            rightButtonIcon = new ImageIcon(rightButtonFilename);
        }

        b1 = new JButton("Disable middle button", leftButtonIcon);
        b1.setVerticalTextPosition(AbstractButton.CENTER);
        b1.setHorizontalTextPosition(AbstractButton.LEFT);
        b1.setMnemonic(KeyEvent.VK_D);
        b1.setActionCommand(DISABLE);

        b2 = new JButton("Middle button", middleButtonIcon);
        b2.setVerticalTextPosition(AbstractButton.BOTTOM);
        b2.setHorizontalTextPosition(AbstractButton.CENTER);
        b2.setMnemonic(KeyEvent.VK_M);

        b3 = new JButton("Enable middle button", rightButtonIcon);
        //Use the default text position of CENTER, RIGHT.
        b3.setMnemonic(KeyEvent.VK_E);
        b3.setActionCommand(ENABLE);
        b3.setEnabled(false);

        //Listen for actions on buttons 1 and 3.
        b1.addActionListener(this);
        b3.addActionListener(this);

        b1.setToolTipText("Click this button to disable the middle button.");
        b2.setToolTipText("This middle button does nothing when you click it.");
        b3.setToolTipText("Click this button to enable the middle button.");

        //Add Components to a JPanel, using the default FlowLayout.
        JPanel pane = new JPanel();
        pane.add(b1);
        pane.add(b2);
        pane.add(b3);
        pane.setBackground(new Color(255,255,204));
        pane.setBorder(BorderFactory.createMatteBorder(1,1,2,2,Color.black));

        return pane;
    }
```

```
    public void actionPerformed(ActionEvent e) {
        if (e.getActionCommand().equals(DISABLE)) {
            b2.setEnabled(false);
            b1.setEnabled(false);
            b3.setEnabled(true);
        } else {
            b2.setEnabled(true);
            b1.setEnabled(true);
            b3.setEnabled(false);
        }
    }

    /* One day, JApplet will make this method obsolete. */
    protected URL getURL(String filename) {
        URL url = null;
        if (codeBase == null) {
            codeBase = getCodeBase();
        }

        try {
            url = new URL(codeBase, filename);
        } catch (java.net.MalformedURLException e) {
            System.out.println("Couldn't create image: badly specified URL");
            return null;
        }

        return url;
    }

    public static void main(String[] args) {
        JFrame frame = new JFrame("Application version: AppletDemo");

        frame.addWindowListener(new WindowAdapter() {
            public void windowClosing(WindowEvent e) {
                System.exit(0);
            }
        });

        AppletDemo applet = new AppletDemo(false);
        frame.setContentPane(applet.makeContentPane());
        frame.pack();
        frame.setVisible(true);
    }
}
```

In eine Webseite kann das compilierte Applet mittels folgendem Code eingebunden werden:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<html>
<head>
<title>Run AppletDemo</title>

<script language="JavaScript">
<!-- hide
function openWin(term) {
  url="../../information/glossary.html#" + term;
  myWin= window.open(url, "Glossary",
              "width=400,height=150,scrollbars=yes,status=no,toolbar=no,menubar=no");
  myWin.focus();
}
//-->
</script></head>
```

```
<body bgcolor="#ffffff" link="#000099">
<b><font size="-1">The Java</font><sup><font size="-2">TM</font></sup> <font size="-1">
    Tutorial</font></b>
<br>
<img src="AppletDemo_dateien/blueline.gif" width="550" height="8" align="bottom"
    naturalsizeflag="3" alt="">
<br>

<font size="-1">
<b>Trail</b>: Creating a GUI with JFC/Swing
<br>
<b>Lesson</b>: Getting Started with Swing
</font>

<h2>
Run AppletDemo
</h2>
<blockquote>
<applet code="AppletDemo.class" codebase="example-swing" archive="applets.jar"
                width="570" height="65">
</applet>


<blockquote><hr><strong>Note:</strong> If you don't see the applet running above, you
    need to install Java Plug-in, which happens automatically when you
<a href="http://java.sun.com/j2se/downloads.html" target="_blank">install the J2SE JRE
    or SDK</a>.
We strongly recommend that you install the latest version; at least
1.3.1 is required for all our applets. You can find more information in
the <a href="http://java.sun.com/products/plugin" target="_blank">Java Plug-in home
    page.</a><hr></blockquote>
</blockquote>

<img src="AppletDemo_dateien/blueline.gif" width="550" height="8" align="bottom"
    naturalsizeflag="3" alt="">
<p>
<font size="-1">
<a href="http://java.sun.com/docs/books/tutorial/information/copyright.html">Copyright
    </a>
1995-2003 Sun Microsystems, Inc.  All rights reserved.
</font>
</p>
</body></html>
```

# 2. Zu sichereren Netzwerkdiensten

## 2.1. S/MIME

Secure MIME bietet die Möglichkeiten, den email-Transfer etwas sicherer zu gestalten. Mittels zertifizierter Codierungsschlüssel wird die

Authentizität

mit Hilfe von „unterschriebener“ email-Nachrichten beziehungsweise die

Geheimhaltung

mittels „codierter“ emails erreicht.

### S/MIME-Zertifikate

Das Versenden von signierten, verschlüsselten bzw. signierten und verschlüsselten e-mail's sollte mit Hilfe von S/MIME-Zertifikaten (X.509-Zertifikaten) und mail-Clients wie Netspace oder Explorer durchgeführt werden.

Vor der Anforderung des Zertifikates empfiehlt es sich, auf eine neuere Netscape- bzw. Explorerversion zu wechseln, die volle (US-)Sicherheit (strong, 128Bit-Schlüssel) unterstützt, z.B.:

Communicator 4.79 with string encription, ...

### Quellen für öffentliche Zertifikate

1. S/MIME-mail's enthalten den öffentlichen Schlüssel des Absender, Beispiel:

   www.trustcenter.de
   buhl@math.uni-wupertal.de

2. Zertifikat-Verzeichnisse von Zertifikatanbieter:

   Über die WWW-Seite

   https://www.trustcenter.de:443/html/Zertifikate/309.htm

können in der Gruppe „öffentliche Gruppe“ PGP und S/MIME-Zertifikate eingesehen werden, die das Trustcenter ausgestellt hat. S/MIME-Zertifikate (X.509) können dann mittels des Knopfes „Installieren“ in die Netscapedatenbank übernommen werden; PGP-Zertifikate sollten in eine Datei heruntergeladen und dann mittels „`pgp -ka Dateiname`“ der öffentlichen PGP-Datenbank hinzugefügt werden.

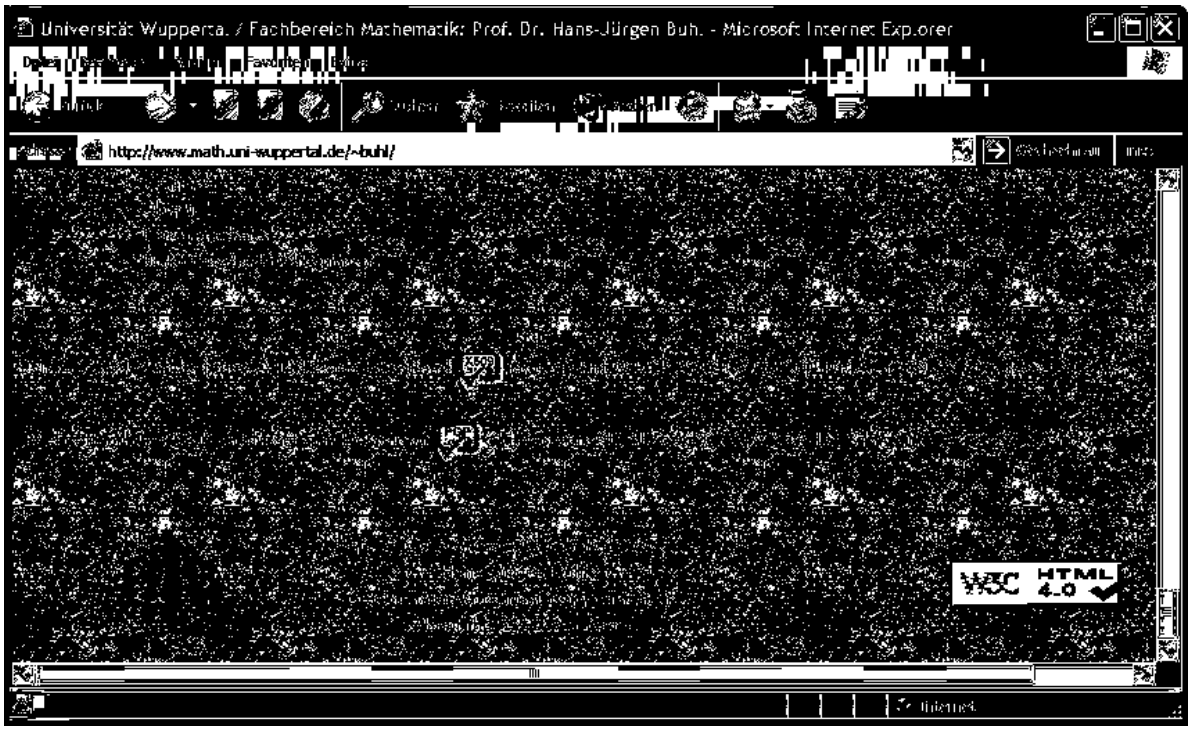
3. LDAP-Verzeichnisse: Trägt man den LDAP-Server von Trustcenter als Verzeichnisdienst in das Adressbuch ein, wie in

   `https://www.trustcenter.de:443/html/Zertifikate/LDAP/1806.htm`

   beschrieben, so können Zertifikate anderer Trustcenterkunden erfragt werden.

4. Dateien in Form von `.pcm`- oder `.der`-Dateien

5. Zertifikate auf http-Server:



### 2.1.1. Unterschriften und Zertifikate

**Erwerben eines „kostenlosen“ Class1-Zertifikats für Privatkunden**

Ueber die WWW-Seite

https://www.trustcenter.de:443/fcgi-bin/Request.cgi?Product=TempPriv&KindOfCert=Client&Customer=Private&Page=SelectCustomer

kann ein kostenloses Class1-Privatkundenzertifikat oder ein Class3-Privatkundenzertifikat für z.Zt. 31,-Euro/Jahr bezogen werden.

**Versenden von signierten Dateien mittels Netscape (/Explorer)**

Dazu klickt man den Knopf `Signed` bei den Optionen im Compose-Window vor dem Abschicken an.

Als spezielles Attachment wird ein „externe“ `x-pkcs7`-signature mitgeschickt, die auch den öffentlichen S/MIME-Schlüssel enthält.

Ein e-mail Korrespondent kann die Mail auf Authentizität überprüfen (inklusive Datum den Unterzeichnung) und Netscape speichert den öffentlichen Schlüssel automatisch in seiner Zertifikat-Datenbasis (People) ab, so dass der Korrespondent ab sofort verschlüsselte Nachrichten schicken kann (sofern er selbst ein Zertifikat besitzt).

Eine unterschriebene (eigentlich: mit Beglaubigung versehende) email sieht dann in Klatext wie folgt aus:

```
From - Tue Jul  8 18:39:55 2003
Received: from wminf0.math.uni-wuppertal.de by wmwap3.math.uni-wuppertal.de
 (Sun Internet Mail Server sims.3.5.1998.08.08.00.06)
 with ESMTP id <0HGX00802RAJQ7@wmwap3.math.uni-wuppertal.de> for
 buhl@sims-ms-daemon; Mon, 23 Jun 2003 15:11:08 +0200 (MET DST)
Received: from math.uni-wuppertal.de
 (wmam3.math.uni-wuppertal.de [132.195.95.99]) by wminf0.math.uni-wuppertal.de
 (8.9.3+Sun/8.9.3) with ESMTP id PAA29859 for
 <hans-juergen.buhl@math.uni-wuppertal.de>; Mon,
 23 Jun 2003 15:11:06 +0200 (MEST)
Date: Mon, 23 Jun 2003 15:11:01 +0200
From: Peter Feuerstein <fpf@math.uni-wuppertal.de>
Subject: Signierte Mail
Sender: Peter.Feuerstein@math.uni-wuppertal.de
To: "Hans-Juergen Buhl (buhl)" <hans-juergen.buhl@math.uni-wuppertal.de>
Message-id: <3EF6FC65.9A5D5862@math.uni-wuppertal.de>
Organization: FB 7 - Mathematik, BUGH Wuppertal
MIME-version: 1.0
X-Mailer: Mozilla 4.77 [en] (X11; U; SunOS 5.5.1 sun4u)
Content-type: multipart/signed; protocol="application/x-pkcs7-signature";
 micalg=sha1; boundary="------------msB24799379B02F5524859EAC5"
X-Accept-Language: de, en

This is a cryptographically signed message in MIME format.

--------------msB24799379B02F5524859EAC5
Content-Type: multipart/mixed;
 boundary="------------EBB47411FBBBCCA0A1F6F075"

This is a multi-part message in MIME format.
--------------EBB47411FBBBCCA0A1F6F075
Content-Type: text/plain; charset=us-ascii
```

```
Content-Transfer-Encoding: 7bit

Signiert...

--
__ Frank Peter Feuerstein _____________________________________________
___ University of Wuppertal, FB7-Mathematik
____ mailto:fpf@math.uni-wuppertal.de    Phone:+49 202 439-2818
_____ http://www.math.uni-wuppertal.de/~fpf    Fax: +49 202 439-2853
--------------EBB47411FBBBCCA0A1F6F075
Content-Type: text/x-vcard; charset=us-ascii;
 name="fpf.vcf"
Content-Transfer-Encoding: 7bit
Content-Description: Card for Peter Feuerstein
Content-Disposition: attachment;
 filename="fpf.vcf"

begin:vcard
n:Feuerstein;Frank Peter
tel;fax:+49 202 439-2853
tel;work:+49 202 439-2818
x-mozilla-html:FALSE
url:http://www.math.uni-wuppertal.de/~fpf
org:BUGH Wuppertal;FB7-Mathematik & IAI
adr:;;Gaussstraße 20;Wuppertal;;D-42097;Germany
version:2.1
email;internet:fpf@math.uni-wuppertal.de
title:Dr.rer.nat., Dipl.-Math.
note:Angewandte Mathematik & Informatik
x-mozilla-cpt:;23168
fn:Frank Peter Feuerstein
end:vcard

--------------EBB47411FBBBCCA0A1F6F075--

--------------msB24799379B02F5524859EAC5
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIIF1gYJKoZIhvcNAQcCoIIFxzCCBcMCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCC
A3QwggNwMIIC2aADAgECAg5eQwAAAAK1336k7q48tjANBgkqhkiG9w0BAQQFADCBvDELMAkG
A1UEBhMCREUxEDAOBgNVBAgTB0hhbWJ1cmcxEDAOBgNVBAcTB0hhbWJ1cmcxOjA4BgNVBAoT
MVRDIFRydXN0Q2VudGVyIGZvciBTZWN1cml0eSBpbiBEYXRhIE5ldHdvcmtzIEdtYkgxIjAg
BgNVBAsTGVRDIFRydXN0Q2VudGVyIENsYXNzIDEgQ0ExKTAnBgkqhkiG9w0BCQEWGmNlcnRp
ZmljYXRlQHRydXN0Y2VudGVyLmRlMB4XDTAyMDUwNjA4MzkwOVoXDTAzMDYyNjA4MzkwOVow
gYQxCzAJBgNVBAYTAkRFMRwwGgYDVQQIExNOb3JkcmhlaW4tV2VzdGZhbGVuMRIwEAYDVQQH
EwlXdXBwZXJ0YWwxGTAXBgNVBAMTEFBldGVyIEZldWVyc3RlaW4xKDAmBgkqhkiG9w0BCQEW
GWZwZkBtYXRoLnVuaS13dXBwZXJ0YWwuZGUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AMShFuPBaEFLsiSb9+X0pBUjR7GmrVfOi0o5Q0SoBtDDjXrPLOHKmbaApojiXePxynwTkuTU
RyxIwBWTAOhIY4a3w7oV9i5meMge2zFqJhV7kJM6R/98j69n2RIKT1WPn/FQXEyniVvlI0PB
QvA9mpFBAyYfn4Ib6cHWzjLYM9wdAgMBAAGjgaowgacwMwYJYIZIAYb4QgEIBCYWJGh0dHA6
Ly93d3cudHJ1c3RjZW50ZXIuZGUvZ3VpZGVsaW5lczARBglghkgBhvhCAQEEBAMCBaAwXQYJ
YIZIAYb4QgEDBFAWTmh0dHBzOi8vd3d3LnRydXN0Y2VudGVyLmRlL2NnaS1iaW4vY2hlY2st
cmV2LmNnaS81RTQzMDAwMDAwMDJCNURGN0VBNEVFQUUzQ0I2PzANBgkqhkiG9w0BAQQFAAOB
gQBiO5fhD8LPxnVlWZ1Etd+7PT394tavSTq2uXsZFsd71fWRZlX0iElbTy7HWaomSLMh/qD3
+JB3Vg/AOW/qsX0b7zH31+EnsEGDuVxyQ8c/UBkGbP5KgeYwXrkEGG2ypSEigVs817mmFcrn
xNoiJG4dcxfBA+jdrO36gZ2FUbALDTGCAiowggImAgEBMIHPMIG8MQswCQYDVQQGEwJERTEQ
MA4GA1UECBMHSGFtYnVyZzEQMA4GA1UEBxMHSGFtYnVyZzE6MDgGA1UEChMxVEMgVHJ1c3RD
ZW50ZXIgZm9yIFNlY3VyaXR5IGluIERhdGEgTmV0d29ya3MgR21iSDEiMCAGA1UECxMZVEMg
VHJ1c3RDZW50ZXIgQ2xhc3MgMSBDQTEpMCcGCSqGSIb3DQEJARYaY2VydGlmaWNhdGVAdHJ1
c3RjZW50ZXIuZGUCDl5DAAAAArXffqTurjy2MAkGBSsOAwIaBQCggbEwGAYJKoZIhvcNAQkD
MQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMDMwNjIzMTMxMTAxWjAjBgkqhkiG9w0B
CQQxFgQUajnllHHSR+q/AlqAt0yxXuiBkSEwUgYJKoZIhvcNAQkPMUUwQzAKBggqhkiG9w0D
BzAOBggqhkiG9w0DAgICAIAwBwYFKw4DAgcwDQYIKoZIhvcNAwICAUAwDQYIKoZIhvcNAwIC
```

```
ASgwDQYJKoZIhvcNAQEBBQAEgYCJ94vHBp6bzuH17ftaB6kMRS05P1cQV3jkEoT6jEpCYRUA
RP5dsnmhM1NqeWJC4Jhc9MSd1JH7QFdo+wHQLGMItwGAVTMvUVvee/AeR+qvNWOsHSukhBny
8ywYOzMXYXHqYsLL9znECEf/ATEPZo5CIqGtOn4mSkr0Wiz7ID0OIw==
--------------msB24799379B02F5524859EAC5--
```

Das `smime.p7s`-Attachment enthält den öffentlichen Schlüssel des Versenders sowie eine Prüfsumme des Textinhaltes der email. Mit Hilfe des öffentlichen Schlüssels wird die Prüfsumme der angekommenen Mail erneut berechnet und mit der übersendeten Prüfsumme verglichen. Außerdem wird der öffentliche Schlüssel des Absenders auf Gültigkeit überprüft, indem er über die ausstellende Zertifizierungsstelle (zum Beispiel http://www.trustcenter.de) verifiziert wird.

### 2.1.2. Codierte Mail

**Versenden von codierten Mails mittels Netscape (/Explorer)**

Dazu klickt man den Knopf `Encrypted` bei den Optionen im Compose-Window vor dem Abschicken an.

Man muss den (oder die) öffentlichen X.509-Schlüssel des (der) Adressaten besitzen, sonst funktioniert die Verschlüsselung nicht!

Man bittet gegebenenfalls den Adressaten um eine signierte S/MIME-Mail (dann wird bei deren Empfang dessen öffentlicher Schlüssel automatisch für zukünftige Verschlüsselungen gespeichert) oder lädt dessen öffentlichen Schlüssel über „Other People's Certificates", „Search Directory" von einer LDAP-Datenbank.

Eine codierte Mail sieht im Klartext folgendermaßen aus:

```
From - Tue Jul  8 18:39:29 2003
Received: from wminf0.math.uni-wuppertal.de by wmwap3.math.uni-wuppertal.de
 (Sun Internet Mail Server sims.3.5.1998.08.08.00.06)
 with ESMTP id <0HGX00802R9RQ0@wmwap3.math.uni-wuppertal.de> for
 buhl@sims-ms-daemon; Mon, 23 Jun 2003 15:10:39 +0200 (MET DST)
Received: from math.uni-wuppertal.de
 (wmam3.math.uni-wuppertal.de [132.195.95.99]) by wminf0.math.uni-wuppertal.de
 (8.9.3+Sun/8.9.3) with ESMTP id PAA29856 for
 <hans-juergen.buhl@math.uni-wuppertal.de>; Mon,
 23 Jun 2003 15:10:37 +0200 (MEST)
Date: Mon, 23 Jun 2003 15:10:36 +0200
From: Peter Feuerstein <fpf@math.uni-wuppertal.de>
Subject: Codierte Mail
Sender: Peter.Feuerstein@math.uni-wuppertal.de
To: "Hans-Juergen Buhl (buhl)" <hans-juergen.buhl@math.uni-wuppertal.de>
Message-id: <3EF6FC4C.47240C11@math.uni-wuppertal.de>
Organization: FB 7 - Mathematik, BUGH Wuppertal
MIME-version: 1.0
X-Mailer: Mozilla 4.77 [en] (X11; U; SunOS 5.5.1 sun4u)
Content-type: application/x-pkcs7-mime; name="smime.p7m"
Content-description: S/MIME Encrypted Message
Content-disposition: attachment; filename="smime.p7m"
Content-transfer-encoding: base64
X-Accept-Language: de, en

MIAGCSqGSIb3DQEHA6CAMIACAQAxggLWMIIBZwIBADCBzzCBvDELMAkGA1UEBhMCREUxEDAO
BgNVBAgTB0hhbWJ1cmcxEDAOBgNVBAcTB0hhbWJ1cmcxOjA4BgNVBAoTMVRDIFRydXN0Q2Vu
dGVyIGZvciBTZWN1cml0eSBpbiBEYXRhIE5ldHdvcmtzIEdtYkgxIjAgBgNVBAsTGVRDIFRy
dXN0Q2VudGVyIENsYXNzIDEgQ0ExKTAnBgkqhkiG9w0BCQEWGmNlcnRpZmljYXRlQHRydXN0
Y2VudGVyLmRlAg5eQwAAAAK1336k7q48tjANBgkqhkiG9w0BAQEFAASBgB7b10kDLBQbw9+S
rnFtT8QJevwWXPm/H4arxpvAQXLaTVlZe4RjSc99Ml169dsFUlc95IoyrRR290ysRSfY5cK2
CxICtgZ76kAzT1zIGpMpBsYvDiQzYPQ56rix/JPYxBrqaG8cSq4q3dyyRUgMe44OV2AOKYoX
bECm/Q/amcAlMIIBZwIBADCBzzCBvDELMAkGA1UEBhMCREUxEDAOBgNVBAgTB0hhbWJ1cmcx
EDAOBgNVBAcTB0hhbWJ1cmcxOjA4BgNVBAoTMVRDIFRydXN0Q2VudGVyIGZvciBTZWN1cml0
eSBpbiBEYXRhIE5ldHdvcmtzIEdtYkgxIjAgBgNVBAsTGVRDIFRydXN0Q2VudGVyIENsYXNz
IDEgQ0ExKTAnBgkqhkiG9w0BCQEWGmNlcnRpZmljYXRlQHRydXN0Y2VudGVyLmRlAg4bVwAA
AAJuJvAzGVHhTjANBgkqhkiG9w0BAQEFAASBgKRqp0aN/NMtuGs9QGLlB4ysT4GSPpelTl7h
6AD5J2YbQJjuEy/kBJV3RR5elgJR2AzaO0L1DdRCyAZsyM8oPo47WnMkznZ1R7O57hsXlYu1
YBNyb/vdYvGGDAh+95AKGfEj7zfD+K1FDyHx1fD8ijjHR/V6V8wpJsx5TtivFSsaMIAGCSqG
SIb3DQEHATAUBggqhkiG9w0DBwQIYjbQCf60/wyggARQQl+RmLzW9d8Ku5n6hhC7HRRD3rvl
Qe0yqylfHN8hndkuDhTriwn6SSQXdSTrTVmlbE4M79JaX5euLjzrAznamyVWvVgj8jeSSAD4
rb5h0MQEMF0Oa180Ydg5rCT0r/rJ6fReq7yMXFMI1fIo3pJRAV0DMAQf3t5JN8cr+8XMVwzi
5QQoxquOLmHGTSGQk1uoII/eAuRj53H5V+oLLjIPxAMDxYULwgUcMFsInQQopK+sOMLC+uxa
vQVB8m2Mn6vb1mtrSwOnuGDREmV0GC0frgpxMdEpXwQgGLsAVdFKQ+N9CJJkM7u2CAMgtINt
uT6JPtXgHOE8ZTYECOfhL7602Zl9BAhSL8plUBLKUAQIh25jm5+XbgoESCmlzpTnP0HP63gu
seFupEdj5kj3t6RdE0uaw//DcWOUBIkuHEAM2sHG0JOYtV5bkU5g780PohsxhVqduwP+nbrf
```

```
OsQDvrvMXAQokM7SdHzRyR01SpbdEC0wekMXXPqRnBvi59iV2oUqnIoTCnYjbdZuZQRIBEJn
dVOs+ZTIMzO+Jo5dW7dHBwP4W7UqNXwN11e2pf+zusM28j1X1WoCoy/DCuq/anhZwgQZJi/m
NHuxOcopqLu0ahIVQ7lTBECciUvn0+OM4L79XXgHsrcvL/jGA+I20JZW8u9aJveu/t3QXNrD
rVlXNMkNrdHmPcJPZqD/ZtSqYhKzNDo/dIa7BAjFHKaNAXoxkwQgzAbTKcHRvQ5i6WCvCaOA
7Hrl2mj1uY9McBwACWVdvXYEQBvv9uwxDPajOPBzdiYGBCym4W/SYTLyvlxA/o0viBVy0s8Z
BBrszNOGvSjj7bMPAL/+cQximNKA+00EMfwEEaQEgYiCK/WHCQ+zkHlBA/+IPw+edOoNB/FO
4SCwkGXaNKBltBzFSj/U0h3Ou7FlitK8sl1RLpR9vH9WivI2IO6baIONwOx1QYqOCqICQzuR
PeWH7FafRASdw/UfJSz0XNFarMK6Laf9dTePGO95IeXxy/HWnucZBoXPaqsBt/rxlE9GvAS0
RKoxJVE9BAgfDySJzJbEeAQIRGZCWhH2BKUEIMricybhWAaWl0yYNxvUGZfVlrPVDDldaIlq
TF5GnC1vBBhaIrw5qvMK6ytBVt90JVp+1ouhD4P4rgUEGAHuoDfHKZwpIwrRcYI2bBkQf51x
fZNcpgQYgmey0FIZGEHhUFUfoJI32JFS8t9xUnjjBCj9xI6zGe20gMVqIcADroOpJuzA0m7g
XKvlGS+iWgKDJycm2R/kYuQDBCiLaE/0eLGaG3KJbEUnX9wplYMB9VXyL9v6BYi3DCfkxOqX
WeSO1AwABDiCz2J3OcBJg1YZ5j9djSduXiI30c1pFNGIlBLybwFKphDVrgq9C1u9C7m3Qwv0
gNv4aAz+j/zgNQQIMAMMi7wnnWQEKPaRRdjf302iLm7/A20AJLQZudI6EI6BeF7upN7NX0xB
QyKlBQRs4WkEILir9XlJPbJNNw16MYbKXqbiZ7XiB0JUeYaiJEjimXRQBDCj5ldTAaBctjF2
7CPC1ovhx+Cdrr65m2r0z/4rMhh7o7zqnBLSuptm60iZspBMNOQEEMnxF46irngBjRSMs3t/
TC4EIBKuMk5wz6aRDQlmzpT57zJNHeN3UW6KdyeRRn48i5gCBAiAgawt/2aPJQQIxFlIC3cv
TQwEIDf7uxMOokFZTQWO1Chm9r8vYEBPd8bTildLAVEAsMH8BAgkIkxif1dqYwQIW8uCLt/+
uF8AAAAAAAAAAAA
```

Eine codierte und signierte Mail sieht folgendermaßen aus:

```
From - Tue Jul  8 18:40:21 2003
Received: from wminf0.math.uni-wuppertal.de by wmwap3.math.uni-wuppertal.de
 (Sun Internet Mail Server sims.3.5.1998.08.08.00.06)
 with ESMTP id <0HGX00802RBKQG@wmwap3.math.uni-wuppertal.de> for
 buhl@sims-ms-daemon; Mon, 23 Jun 2003 15:11:44 +0200 (MET DST)
Received: from math.uni-wuppertal.de
 (wmam3.math.uni-wuppertal.de [132.195.95.99]) by wminf0.math.uni-wuppertal.de
 (8.9.3+Sun/8.9.3) with ESMTP id PAA29868 for
 <hans-juergen.buhl@math.uni-wuppertal.de>; Mon,
 23 Jun 2003 15:11:42 +0200 (MEST)
Date: Mon, 23 Jun 2003 15:11:41 +0200
From: Peter Feuerstein <fpf@math.uni-wuppertal.de>
Subject: Codierte und signierte Mail
Sender: Peter.Feuerstein@math.uni-wuppertal.de
To: "Hans-Juergen Buhl (buhl)" <hans-juergen.buhl@math.uni-wuppertal.de>
Message-id: <3EF6FC8D.A3677D9A@math.uni-wuppertal.de>
Organization: FB 7 - Mathematik, BUGH Wuppertal
MIME-version: 1.0
X-Mailer: Mozilla 4.77 [en] (X11; U; SunOS 5.5.1 sun4u)
Content-type: application/x-pkcs7-mime; name="smime.p7m"
Content-description: S/MIME Encrypted Message
Content-disposition: attachment; filename="smime.p7m"
Content-transfer-encoding: base64
X-Accept-Language: de, en

MIAGCSqGSIb3DQEHA6CAMIACAQAxggLWMIIBZwIBADCBzzCBvDELMAkGA1UEBhMCREUxEDAO
BgNVBAgTB0hhbWJ1cmcxEDAOBgNVBAcTB0hhbWJ1cmcxOjA4BgNVBAoTMVRDIFRydXN0Q2Vu
dGVyIGZvciBTZWN1cml0eSBpbiBEYXRhIE5ldHdvcmtzIEdtYkgxIjAgBgNVBAsTGVRDIFRy
dXN0Q2VudGVyIENsYXNzIDEgQ0ExKTAnBgkqhkiG9w0BCQEWGmNlcnRpZmljYXRlQHRydXN0
Y2VudGVyLmRlAg5eQwAAAAK1336k7q48tjANBgkqhkiG9w0BAQEFAASBgB9pxKDTiFy7qGfU
bh2Tlakb84qJwz5Nzu+BMdyAV3VtXrVkII2QzHDyot1E1rbnts3nwA6Z4iJQpN0lsazwNZ7M
9gRbJ9U8zNS7rykubiNXZ6ILKNeKCsjsFlNkxZc3n0NG82OYgRCHoy98XqCU1GvAE7Zcx8vM
DtOGSX+MmDLsMIIBZwIBADCBzzCBvDELMAkGA1UEBhMCREUxEDAOBgNVBAgTB0hhbWJ1cmcx
EDAOBgNVBAcTB0hhbWJ1cmcxOjA4BgNVBAoTMVRDIFRydXN0Q2VudGVyIGZvciBTZWN1cml0
eSBpbiBEYXRhIE5ldHdvcmtzIEdtYkgxIjAgBgNVBAsTGVRDIFRydXN0Q2VudGVyIENsYXNz
IDEgQ0ExKTAnBgkqhkiG9w0BCQEWGmNlcnRpZmljYXRlQHRydXN0Y2VudGVyLmRlAg4bVwAA
AAJuJvAzGVHhTjANBgkqhkiG9w0BAQEFAASBgG7sYewr3mgQASiixl+FJzPWrBFDKqdokiXU
M5txVVCL1B8kd8K3l2rVoOU0zaOMvtj2v/6t/3ZUW7BjMrhbsb/YwObuFQoH4HTrEw0vi2cL
P3Go/oj91NFEmENskMjM6RPHsq/2fb/ac208/JgE4V2RW9Cs85lcJNQ9MOv4SBe1MIAGCSqG
SIb3DQEHATAUBggqhkiG9w0DBwQIlwNHgOqUn5yggASBsHNHBA+y8vMfLuZBsU9CIi+ES0PR
hqN4xRnhOAr2q4MOP7pp4+3kXycuq1uhW7BMe5f8CjIB69VU0xZccAc4InM/RChPba6KPXEc
6zu8Fnxo6izj6ULJBBL4yNAXfJjT2FDgmuFN8hxTaCuieM0+e8rJr2Ka8P3MhsaHZJ2v6qwW
NdUaDCM58+ghd4/UCwlReer4aOaoXpl1R5ePQ3988XrBXkBXHSVDnUThm32QMP94BFjqrWta
d9fKvYjvnGdijWpxioBJ3DUNCvMMOJTh/gbWu+ZIuSXapDdZvuxwzpR/2WqqdTRNZLBAU7cD
```

```
25QDvalWUpNNwcUTz4ji4TFIMZmiktou++JmkmqwBChyIGwEr4bt6waT1R+M+UwsHw1MgzIJ
R5sa1NBZ8ivjB8dY9Eu/3q+xBAhrOgAmz6d2swQgggI1+lZfXRBZ2mc/0pzgnTDcZVIUtFGW
aywVY5QFNdUECN+MJAi9gjVvBCjf+Wss8zBGKtKqiTvwTS81Y+NsQnHqcuSJTOFR7BroMo4a
yKguWddSBCCwqaJ4SvNHjh1pjeQ/THo+3qY+NJepNSw/C6qR5iOTbwQgKKwWn17NZtvyv68U
NBZHWOCHbTHp9Hadm8TiIndgnIIESFxMGIyMvgsHxVKOOB3NaBZyR4FE5IVYPMYKuNo+jCV8
zppVVJgFZa+D3DfIHVTE5wdZWY/diURRcYNBARjfJnAKIwJ2pTON6gQwsv7Utkux2zHISERU
iDfcQXyXsAu+Wvg0vYhbT7lS7cx2U4qi2zn100IZzAatH7yoBEC3V7uvVimWCND7llKmHxeY
sRakTMaXV+6mjiKjJ4YCAN2gc7Bs/NKLgrJm6lPfrDOz6B5ftQO/LRVaa+4u7J3HBEDWHUE7
EOnKKQy97lcgV1n9X+INFrdF4Cy242JZzXwqpFA+roVgNZKkQWYsNCMJj/CY75YHMzrTJL2r
pmq3gdmLBAgy9CpB6+prZgQgRf2RlsG1RMEjSZQX+567Ed95vRwzBqJXAFvJgYpdjzsECIJd
WjawzMJ/BEAopVbPGjN3u+5VKfRMU21TDoQwLrlSEe+umMfacGB05BDOGQav92eCmpd7o9Tk
xO77GKErJBgODi8n+xkdz+6GBIGIUe4P53ViJhgY+lthv+poMrOixGWYB3cVsFGojCTyMuxe
m06/Rc7d+lTZSh4ftfOnPu50mU/CfrgyCpB4LN39PtqwIfujcRK/EErSqduRqOgPhaTI0LG8
Ljb0xZEDNjBw0Xt0KoiO7DIOJpynR9OyZCwp1+jpBo8bXeG0lB1/lZyFb3csyXCUoQQQlv6q
0nAaq6mPrZ786ZdZcwQYf14u9LY5yUcnWdX1xA87+I/stNZcuxosBBgWL4SvLVT5nWa0+D6Z
xExC99p7RxJXnwYEIBi97oCH5gaYCpdpjww4Wx1qU3eMECOzSgd4ysAQDnoEBBANPs6b3gmI
mBP+1UKi6jLsBDDoEKgDt9nD8s/lNLM6KqMFeE/hb7WvUJZAfEmX5h3SNgmJCi5JIBVex8Av
FrvR9jcEKP39WQpo2Jx+kz8wc8v7/72nGOpgjFo6Ro6HdCuFEKuWFLJTjAWxD58EMD5v1NJj
cU6vmjUOPLythdXggH5kt0WzTAqdXyJErWfAbK0Tbifh1lbXLjXUeolupAQQXbyn9qGbk1MX
YCibmSjp1QQou1I6Nfz8xlbpk1ULTcUs+U8wfsBGgRKMIuAxyJHtMnWrAyYoMpLS6wQgXKNu
TSPH68ybulAOSpZioNLIL6UWlPUsZOT1jknjWewEKOpEoSomU/sC92FHPZDbfFVhizZXM6SB
AVVdXm0k5dvnwrYt0l1nUZYEGBQ8OBxMZBHVcJ9+a5b787+LZ2pM24hM3QQYAtb94tAl2LFi
n06VAVkAsceQOP6/A5igBAjM7O0wAkGgbQQIRndfQYhI4KIEIC/cMUpro/naKSQAzkbEW53p
VuLeaioExcBS9/Y1OLn5BAhE0DeSHM8N0QSB+BFjXXYdWUj47LQSLGlfkhSXLKLkVuubk59l
PZaRMX285BdHlSUtIN8tboht21fEoSHtq37sZ7YyLqyzHyPzRoJRm2upDsXBrEQv9+6f6UiG
CXaOIwN73YA/g1DN+YqmTExY8cJUkapIw+Gbe3XgHoodgcYRgw43+sXWCCf7a2MoyMlVmFJL
QB3X3INvWAadcYfeQjfpC0iGotQmE2Yau3L0kaVC4T0C64a4GJYBeda9h2+lG8dSyI1d1mB3
AI2fMn9KTDXU84h9vemQN0uAkdncje705MZNBQUC/M4iEE1bAMG0LAX2XUbIPFNCvp+wm9YL
/kDXyvfABAg33KFPYxxORgQQ2T+QCi1UJpT4YI+/iSx2QgQIc2tY3mzgNvIECGo6O3cYtXEa
BAh7lqu5hI2TgAQIXOGAE1/keDcEELMXZR+ocaRCa9g9NM1rZk4ECGW023+n26AmBEgn+ZOA
6m3nq00Lwk9plZztcbabZakRS6zsothm0xhOAnp4hSeUDa2TIOq82cg7nrSQOFWi+NF59jAv
D85cEZ0bArGhDqaIQ+cESF1pK6lY/U5ODrjdJYDX3JsnfGfNDFBZAOssT2HH4CttqTx1mYmc
9zzLfZeawkDd9ktVBceHip4RskMOvYcZKHd58kYaKUzo4QRI8k4NZFmJfrLqWh0hRJGuPm9O
R7vKAWqXTUmmSB+6eM3slUtdRDLQ3wWVIFDHIXnLV+24Pc6BmbcIYzFuZ+U2R5cKR1d389yH
BFBv/d4OiuaPSEVv2jiKtjokoCHvh1sf4TdXmHQ2NuCMm7puMAwp1Xg7Q8B9R+DYkQus26w/
Vs2BCcXJaug10mOPBV3R5TDN4B5FnKE1nVBa5wRI4xnKLbgAbNNejE2ViRqzYkiygEA7kvl1
aP3kEY+6XVLGgnABtwix7RMnPldSzGW3IpKAIhexCbqZJNSE1Ehe74/+y/zxNrghBEjVzOge
12o99Ovn4g/0ZWVX3gZhL/PDdG3FfDcA/4XITdLTjXj3Xx9vY9mJ4wHJSlonsGunTKnN2cvd
gIaBgNq0w+MqgwnEH6IESPn6nc0zFAd0g353iR3xtixmX4uVVBQdwlDORG++JnomR8nw3TVU
mjMn1pXolh9WjB/87rww75fS8mbBJeo2HHxcLBpf8ZzSiARQehM+Ti3/syEI3Cs14ypxN+1N
8LpA4ZY10moaTfb37LVDz6u55st1nswKcb+jj3luTnCZOjQwXveXpXhCzuAHG8wHkbB8O6Q4
LzBdjCRB5V4ESJ48guD/bc1vTN6BtAXkPKdyRFBJoZAOdnEtaH80QjD7qSiCej1+nantrr+/
mB/BhXfFv2ZcRDuxYaVdWTbt1ttfRYv96cxwlwRIGNJcJz+4JnCi+LaBphcpGbXbXNw+7X8J
5BDa3yn8S4JVBuUXhTGj8xDgH9mDu7GrNOGlHcc44YQles5x7TbpO7l/yhcSRrefBEgp4Ap3
ZT74o4jiE9M/D6UJG+b3/UDUzDG9im50RqPZrUjhfRiAf61h+KabWwWlNLsUtFhaPITS8I65
/8gYiBEDGOz8dowZlEkEUOV+Dm1hsTLbQY2BBj3qv9RBcXnkukNqZPIJje4A1I2PVS8u5YQU
/QmehK1755UE9uAn0VjbDBIu3zKa3q4slaoUObzTY4DB3hlOny2pLLbLBEjTMNxfl5PC7N1/
AzVhB2sIP7qiZ14aKUgqbiAA1AWwcQis9jSlxBgn/47Vstt0yl6QaJfecIpxtRGPSxGP1hJy
kOGkYF8Qbc4ESEL1AyURc9ne59Xa/vjjXCYM4HN0GoCF+HCTB/FBuZEI8+CGs45o1RPha/4q
u1MuicC1MPUpOoauqh3jkmeh0fwfCZ2s6zrqVgRIxRXm5EXvSp6w2xOTtsNavtDUVJlCzfUd
NTGETYITRosXbnoycPlWMsVarXifJTaVVF2ip55Fi9/LyInUgJ0hCSnN1muX0boGBFDjbaur
EaC7nLQ0ZVKNxwMZPfO9GY7lQaBy2udkweNlUgzNVWt6D74ZMSl2RApacIoaLU/BzZbnt3sr
S9mdTBzKQizz0TLU90M1hvtJlJLgiAQYQpvQSsM/a17ze/qdBO9H/ir0XtnCfEXEBAhZFeiC
y1FP5gQI42cM35OE8TcECMnQIwCR5p6WBAgCKuONhycUrgQI1AU3Z4oCl6oECO4yEGNuJquW
BAgwppyfYsUX0AQI1hurobDwjbMECJLoXt88+UysBAj+6ux+N67hlgQIo+FcTL3YZOwECO8P
5GuxL9NLBAi/4VbSpKqvXgQQkjkj2t2JG5rX/XZcenB/1AQ4rrnqMZXRbSl77sXErz1oKBK/
KIMUkgJNzTMwM2inAUeKGtscq4hZ6nOq3Lw5c/GhDZXVE0hD3wYECPCan/HiPN4rBAjJyJf+
+5bzyQQgqzcqGyLtrUqXSQE0KdTAteFQmQZjaKs/FgP5u117/V0ECPV4Tvrx8fbOBAhIUWLu
p3W/uAQgwEygn+txKUovQdz9+RC6cMbznlBDEmpLsL5qZOoV1GsECD6NffvPyeCSBAiNDk5t
dWbqNAQQuUOIEyJ9btuspPiu15riwAQI5Q7QL5FqvCQECGQsOaJ+ZisKBAiRsptcwcX91wQQ
BksFNCSv7PwjKvXBWe7WOgQQsweqCGpS7d5XsTf+3qylEwQQ4rB5TTYTTzL8UGa5J7vSHwQI
U293DtXSwMEEEFOB3O1fY9Uvc5wW6talLR8EEA//oOTpUCrsTQvoTGGKrAUECC+LjflfmTqD
BBirefpwYJg2JLE1dy23Qq1a6cvPNoHJLIoECC77v+owJN4VBBB8fsEnSJpBABpCPEgSpGrz
BBBplDi/xYaOcyn4JxpksSf6BFAm5QE4s1J5UFVv9MnaXJiU7sh87/zLoU+tqsAJDLaRzUiY
UHHtwM+3E+MVYJKt3fp2kgFzDTpqWkRboWwv3nlxdkwQx9dr+ga7A8lC0UR3fQQIAYYsi0k0
NZcECD76rbUFMbKzBAiyVK/EGiuzugQwtj2tXxuf0TjoChWNEvZ4+p4ZXfiiFVwvbgHVgOJd
```

```
U3QMkpLFTt74c8l7xrr1fUnJBEhmbMmIrqJB40QIjCMLE/+OdPfCCYFXzptJClKS5T01Rrqu
fRCj5Eyot3m6PuvPgJMCFAou4kVW1o36MMiTEquWQnC/955OQvEEOJ2kxbbM8n5wl2AuAJx8
lRqVd/TLvGAQrdueEiG8Pv4hh4mOda9hss9ZWIJHdj+stgQjNsMTv+zrBDD46bOdn2Ed1Ibj
qse9YWrokdiBz4Ind7dN5bkPUmi31wUwvE1LYxwff15ScSycyTQECB7OuUxLR14xAAAAAAAA
AAAAA==
```

### 2.1.3. Dokumentation

- Jalal Feghhi u.a.: Digital Certificates, Addison Wesley, 1999
- http://www.rsasecurity.com/standards/smime/faq.html

## 2.2. PGP und Dateicodierung

PGP (Pretty Good Privacy) ist ein Verschlüsselungsprogramm für email und Dateien. Mit PGP können emails elektronisch unterschrieben (unterzeichnet/signiert) werden. PGP ist weit verbreitet und gilt mittlerweile als ein Standard der Kryptografie, da es für Privatpersonen und gemeinnützige Organisationen kostenlos ist.

### 2.2.1. Lokales Verschlüsseln und Entschlüsseln von Dateien

Statt des unsicheren `crypt`-Kommandos des UNIX-Betriebssystems sollte `pgp` zur Verschlüsselung/Entschlüsselung von Dateien mit sensitivem Inhalt benutzt werden.
PGP bietet zunächst sogenannte symmetrische Verschlüsselungen an, d.h. beim Verschlüsseln einer Datei wird derselben Schluessel (**Mantra**) wie bei der späteren Entschlüsselung verwendet. Es bietet sich an, als Mantra eine PassPhrase (d.h. ein nicht nur ein Wort sondern einen geeigneten Satz) zu verwenden!

Ein Beispiel:

```
% pgp -c Sieb.p
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:51 GMT

Du brauchst ein Mantra zum Verschlüsseln der Datei.
Gib das Mantra ein: <----- Eine Passphrase zur Verschluesselung nur dieser Datei
Wiederhole das Mantra: <----- Wiederholung
Einen Augenblick, bitte....
Verschlüsselte Datei: Sieb.p.pgp

% ls -al Sieb.p*
-rw-r--r-- 1 buhl inf 1680 Oct 28 1999 Sieb.p
-rw------- 1 buhl inf 655 Jun 14 18:50 Sieb.p.pgp
```

Das Entschlüsseln erfolg mittels:

```
% pgp Sieb.p.pgp
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:55 GMT

Diese Datei ist konventionell verschlüsselt.

Du brauchst ein Mantra zum Entschlüsseln dieser Datei.
Gib das Mantra ein:
Einen Augenblick, bitte....
Das Mantra scheint zu stimmen.
.
Dateiname des Klartextes: Sieb.p
Die Ausgabedatei 'Sieb.p' existiert bereits. Überschreiben? (j/N) j
```

**Bemerkung:** „`pgp -cw Sieb.p`“ löscht nach Erzeugung von `Sieb.p.pgp` das Original `Sieb.p`.

**Bemerkung:** `pgp.p.pgp` ist eine Binaerdatei. Wollen Sie eine per e-mail versendbare ASCII-Datei erzeugen geht das mittels “`pgp -cwa Sieb.p`“. Die codierte Datei hat dann den Namen `Sieb.p.asc`.

### 2.2.2. uuencode, uudecode

Eine Möglichkeit, binäre Dateien (d.h. genauer nicht rein ASCII 7 Bit-Dateien) via email zu versenden ist, stellt `uuencode` (Unix to Unix Encode) dar. Die meisten E-Mail-Clients erledigen diese Aufgabe inzwischen automatisch, sobald sie auf eine Binärdatei treffen:

> Das Internet war zunächst nicht zur Übertragung von binären Daten (Programme und andere Dateien, bei denen es sich nicht um reine Textdateien handelt) gedacht. Es ist lediglich in der Lage, Dateien zu übertragen, die aus „normalen“ Zeichen besteht (druckbare ASCII-Zeichen).
> Um diese Beschränkungen zu überwinden, wurden unter anderem das Verfahren `uuencode` entwickelt. Alle diese Ansätze, arbeiten nach dem gleichen Prinzip: Sie wandelt binäre Dateien (die ja wie bereits erwähnt nicht über das Internet verschickt werden können) in Dateien um, die nur ASCII Zeichen enthalten und somit über das Internet verschickt werden können. Dieser Vorgang ist das Kodieren (encoding). Der Empfänger der so umgewandelten Datei, kann dann den Vorgang wieder umkehren: Die reinen ASCII-Zeichen werden dann wieder in eine binäre Datei umgewandelt (also die ursprüngliche Datei).
>
> Quelle: WinZip (`http://www.winzip.de/uu00002.htm`)

Die `man`-Pages geben Aufschluss über die Verwendung der beiden Befehle (http://campuscgi.princeton.edu/man?uuencode):

```
NAME

     uuencode, uudecode - encode a binary file, or decode its
     encoded representation

SYNOPSIS

     uuencode [ source-file ] decode_pathname

     uudecode [ -p ] [ encoded-file ]

DESCRIPTION
  uuencode

     uuencode converts a binary file into an encoded representation
     that can be sent using mail(1). It encodes the contents of
     source-file, or the standard input if no sourcefile argument
     is given. The decode_pathname argument is required. The
     decode_pathname is included in the encoded file's header as
     the name of the file into which uudecode is to place the binary
     (decoded) data. uuencode also includes the permission modes of
     source-file, (except setuid, setgid, and sticky-bits), so that
     decode_pathname is recreated with those same permission modes.
```

uudecode

uudecode reads an encoded-file, strips off any leading and trailing lines added by mailer programs, and recreates the original binary data with the filename and the mode specified in the header.

The encoded file is an ordinary portable character set text file; it can be edited by any text editor. It is best only to change the mode or decode_pathname in the header to avoid corrupting the decoded binary.

OPTIONS

uudecode

-p

decode encoded-file and send it to standard output. This allows uudecode to be used in a pipeline.

OPERANDS

uuencode

The following operands are supported by uuencode:

decode_pathname

The pathname of the file into which the uudecode utility will place the decoded file. If there are characters in decode_pathname that are not in the portable filename character set the results are unspecified.

source-file

A pathname of the file to be encoded.

uudecode

The following operand is supported by uudecode:

encoded-file

The pathname of a file containing the output of uuencode.

USAGE

See largefile(5) for the description of the behavior of uuencode and uudecode when encountering files greater than or equal to 2 Gbyte (2**31 bytes).

ENVIRONMENT

See environ(5) for descriptions of the following environment variables that affect the execution of uuencode and uudecode: LC_CTYPE, LC_MESSAGES, and NLSPATH.

OUTPUT

stdout

The standard output is a text file (encoded in the character set of the current locale) that begins with the line:

"begin/\%s/\%s\n", <mode>, decode_pathname and ends with the line:

end\n

In both cases, the lines have no preceding or trailing blank characters.

The algorithm that is used for lines in between begin and end takes three octets as input and writes four characters of output by splitting the input at six-bit intervals into four octets, containing data in the lower six bits only. These octets are converted to characters by adding a value of 0x20 to each octet, so that each octet is in the range 0x20-0x5f, and then it is assumed to represent a printable character. It then will be translated into the corresponding character codes for the codeset in use in the current locale. (For example, the octet 0x41, representing A , would be translated to A in the current codeset, such as 0xc1 if it were EBCDIC.) Where the bits of two octets are combined, the least significant bits of the first octet are shifted left and combined with the most significant bits of the second octet shifted right. Thus the three octets A, B, C are converted into the four octets:

0x20 + (( A >> 2 ) & 0x3F)

0x20 + (((A << 4) | ((B >> 4) & 0xF)) & 0x3F)

0x20 + (((B << 2) | ((C >> 6) & 0x3)) & 0x3F)

0x20 + (( C ) & 0x3F)

These octets are then translated into the local character set.

Each encoded line contains a length character, equal to the number of characters to be decoded plus 0x20 translated to the local character set as described above, followed by the encoded characters. The maximum number of octets to be encoded on each line is 45.

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

ATTRIBUTES

See attributes(5) for descriptions of the following attributes:

| ATTRIBUTE TYPE | ATTRIBUTE VALUE |
|---|---|
| Availability | SUNWesu |

SEE ALSO

mail(1), mailx(1), uucp(1C), uux(1C), attributes(5), largefile(5)

NOTES

The encoded file's size is expanded by 35% (3 bytes become 4, plus control information), causing it to take longer to transmit than the equivalent binary.

The user on the remote system who is invoking uudecode (typically uucp) must have write permission on the file specified in the decode_pathname.

If you uuencode then uudecode a file in the same directory, you will overwrite the original file.

### 2.2.3. base64

Eine modernere Möglichkeit für die Übertragung von Binärdateien im Internet stellt die base64-Methode gemäß RFC 1521 dar. Die große Verbreitung dieser Methode basiert darauf. dass die Base64-Kodierung mit einem sehr eingeschränkten Alphabets von nur 64 Zeichen auskommt. Damit genügen für die Darstellung eines codierten Zeichen 6 Bit. Die Man-Page ist unter http://www.fourmilab.ch/webtools/base64/ einsehbar:

```
NAME

    base64 - encode and decode base64 files

SYNOPSIS

    base64 [ -d / -e ] [ options ] [ infile ] [ outfile ]

DESCRIPTION

    The MIME (Multipurpose Internet Mail Extensions) specification
    (RFC 1341 and successors) defines a mechanism for encoding
    arbitrary binary information for transmission by electronic
    mail. Triplets of 8-bit octets are encoded as groups of four
    characters, each representing 6 bits of the source 24 bits.
    Only characters present in all variants of ASCII and EBCDIC
    are used, avoiding incompatibilities in other forms of encoding
    such as uuencode/uudecode. base64 is a command line utility
    which encodes and decodes files in this format. It can be used
    within a pipeline as an encoding or decoding filter, and is
    most commonly used in this manner as part of an automated mail
    processing system.

OPTIONS

    --copyright

        Print copyright information.

    -d, --decode

        Decodes the input, previously created by base64, to
        recover the original input file.

    -e, --encode

        Encodes the input into an output text file containing
        its base64 encoding.

    -n, --noerrcheck
```

Suppress error checking when decoding. By default, upon encountering a non white space character which does not belong to the base64 set, or discovering the input file is incorrectly padded to a multiple of four characters, base64 issues an error message and terminates processing with exit status 1. The -n option suppresses even this rudimentary error checking; invalid characters are silently ignored and the output truncated to the last three valid octets if the input is incorrectly padded.

-u, --help

Print how to call information and a summary of options.

--version

Print program version information.

EXIT STATUS

base64 returns status 0 if processing was completed without errors, 1 if an I/O error occurred or errors were detected in decoding a file which indicate it is incorrect or incomplete, and 2 if processing could not be performed at all due, for example, to a nonexistent input file.

FILES

If no infile is specified or infile is a single \-\, base64 reads from standard input; if no outfile is given, or outfile is a single \-\, output is sent to standard output. The input and output are processed strictly serially; consequently base64 may be used in pipelines.

BUGS

Little or no error checking is done when decoding, other than validating that the input consists of a multiple of four characters in the encoding set. This is inherent in the design of base64, which assumes transmission integrity is the responsibility of a higher-level protocol.

SEE ALSO

qprint(1), uudecode(1), uuencode(1), RFC 1341

AUTHOR

John Walker

http://www.fourmilab.ch/

Christian Ferrari contributed code which permits the base64 utility to work on EBCDIC based systems such as UNIX Services for OS/390 2.7 (ESA/390). This software is in the public domain. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, without any conditions or restrictions. This software is provided \as is\ without express or implied warranty.

### 2.2.4. md5

`md5`[1] (Message Digest 5) ist ein sogenannter Message Digest [2]-Algorithmus, der aus beliebigem Text eine 128-Bit lange digitale Kennung erzeugen kann, die bei minimaler Textänderung nicht mehr stimmen würde
`md5` wird daher auch häufig als Authentifizierungsverfahren eingesetzt.

Die Man-Page ist unter http://campuscgi.princeton.edu/man?md5 verfügbar:

```
NAME

     md5 - calculate a message-digest fingerprint (checksum) for a
     file

SYNOPSIS

     md5 [ -t | -x | -sstring | filename(s) ]

DESCRIPTION

     md5 takes as input a message of arbitrary length and produces
     as output a 128-bit "fingerprint" or "message digest" of the
     input. It is conjectured that it is computationally infeasible
     to produce two messages having the same message digest, or to
     produce any message having a given prespecified target message
     digest. The MD5 algorithm is intended for digital signature
     applications, where a large file must be compressedïn a secure
     manner before being encrypted with a private (secret) key under
     a public-key cryptosystem such as RSA.

OPTIONS

     The following four options may be used in any combination,
     except that filename(s) must be the last objects on the command
     line.
     -s

         string prints a checksum of the given "string".

     -t

         runs a built-in time trial.

     -x
```

[1] gemäß RFC 1321
[2] Botschaften-Auszug

```
        runs a built-in test script.

    filename(s) prints a checksum(s) for each of the files.

SEE ALSO

    sum(1)

    RFC 1321 describes in detail the MD2, MD4, and MD5
    messagedigest algorithms.

ACKNOWLEDGEMENTS

    This program is placed in the public domain for free general
    use by RSA Data Security.
```

Ein Benutzungsbeispiel bei der elektornischen Veröffentlichung von Dissertationen ist etwa unter

http://elpub.bib.uni-wuppertal.de/edocs/dokumente/fb07/diss2002/huebschen/authcode.txt

zu finden:

MD5 für MS-DOS:
Bergische Universität - Gesamthochschule Wuppertal,

Dissertation
Hübschen,Thorsten
Lokale Fortsetzbarkeit holomorpher Abbildungen im nicht-pseudokonvexen Fall
2002

MD5 (d070201.pdf) = 60ce41e3a6d3456a9578ad85564f06fe

### 2.2.5. Verschlüsseln und Entschlüsseln von Dateien zum Austausch mit Anderen

Da ein symmetrisches Verschlüsselungsverfahren[3] zum Austausch von Nachrichten/Dateien/... mit anderen nicht geeignet ist, wird hier ein RSA-Verfahren mit einem Schlüsselpaar beschrieben. Dabei besteht das Schlüsselpaar aus einem geheimem nur dem Absender bekannten Schlüssel und einem öffentlichen der ganzen Welt oder doch zumindest dem Empfänger, dem Sie die Nachricht/Datei/... zugänglich machen wollen, bekannten Schlüssel)

**Erzeugen eines RSA Schlüsselpaares** Ein RSA-Schlüsselpaar wird folgendermaßen erzeugt

```
% mkdir $HOME/.pgp
% pgp -kg

Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:38 GMT

Wähle die Länge Deines RSA-Schlüssels aus:
1) 512 Bits: 'einfach kommerziell', schnell,
aber nicht ganz so sicher
2) 768 Bits: 'hochgradig kommerziell', mittelmäßig schnell,
recht sicher
3) 1024 Bits: 'militärisch', langsam, jedoch maximale
Sicherheit
Auswahl (1,2,3 oder die Länge des Schlüssels in Bits [384 bis 2048]): 3

Ich erzeuge einen RSA-Schlüssel mit einem 1024-Bit-Modulus.

Du brauchst eine Benutzer-ID für Deinen öffentlichen Schlüssel. Das
übliche Format für diese Benutzer-ID ist Dein Realname,
gefolgt von Deinem Usernamen in <spitzen Klammern>, falls
Du per E-Mail erreichbar bist.
Beispiel: Helmut Kohl <BIRNE@LINK-BN.cl.sub.de>
Gib die Benutzer-ID für Deinen öffentlichen Schlüssel ein:

Titel Vorname Nachname <Vorname.Nachname@math.uni-wuppertal.de>

Du brauchst ein Mantra, um Deinen privaten RSA-Schlüssel zu schützen.
Dein Mantra kann jeder beliebige Satz oder Zeichenfolge sein und darf
aus vielen Worten, Leerzeichen oder anderen druckbaren
Zeichen bestehen.

Gib das Mantra ein: xxxxxx xxxxxx xxxxxxx xxxxxxxxxx xxxxxx

Wiederhole das Mantra: xxxxxx xxxxxx xxxxxxx xxxxxxxxxx xxxxxx

Beachte, daß die Schlüsselerzeugung eine zeitaufwendige Sache ist.

Wir müssen 783 zufällige Bits erzeugen. Dies wird durch Messung
der Abstände zwischen Deinen Anschlägen bewerkstelligt. Bitte gib
irgendwelchen beliebigen Text auf der Tastatur ein, bis es piepst:
783 xxxxxxxxxxxxxxx
...
.....**** ...****
```

[3] beim Verschlüsseln wird derselbe Schlüssel wie beim Entschlüsseln benutzt

```
Das Mantra ist richtig.

Einen Augenblick, bitte....

Der Schlüssel wurde mit Deiner Unterschrift beglaubigt.

Die Erzeugung des Schlüssels ist beendet.
```

Das Überprüfen des Schlüssels kann folgendermaßen geschehen:

```
% pgp -kv
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:45 GMT

Schlüsselbund '/home/buhl/.pgp/pubring.pgp':

Typ Bits/ID Datum Benutzer
öff 1024/5647284D 2000/06/14 Titel Vorname Nachname
<Vorname.Nachname@math.uni-wuppertal.de>
Es wurde ein passender Schlüssel gefunden.
```

bzw.

```
% pgp -kvv
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/14 16:45 GMT

Schlüsselbund '/home/buhl/.pgp/pubring.pgp':

Typ Bits/ID Datum Benutzer
öff 1024/5647284D 2000/06/14 Titel Vorname Nachname
<Vorname.Nachname@math.uni-wuppertal.de>
Unt 5647284D Titel Vorname Nachname <Vorname.Nachname@math.uni-wuppertal.de>
Es wurde ein passender Schlüssel gefunden.
```

**Zertifizierung des PGP-Schlüssels** Zur Erhöhung der Vertrauenswürdigkeit eines öffentlichen Schlüssels kann man diesen bei Bedarf kostenlos zertifizieren lassen. Zunächst extrahiert man diesen in ASCII-Form:

```
% pgp -kxa Nachname nachname.pub
% cat nachname.pub.asc
```

Dazu konnte bislang die Seite

https://www.trustcenter.de

des Trustcenter aufgesuchte werden und der öffentliche PGP-Schlüssel dort (kostenlos) als Class1-Privatkunde zertifiziert werden. Trustcenter hat aber diesen Dienst eingestellt, lediglich bestehende Zertifizierungen können noch verlängert werden.
Ein ähnliches Angebot für Mitglieder der Universität Münster stellt deren Zertifizierungsstelle

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

dar. Ein Zertifizierungsantrag geht etwa wie folgt vor sich:

Nach Aufruf einer der obigen Seiten und folgen der Anweisungen, erhält man zunächst eine mittels PGP verschlüsselte e-mail, die in eine Datei geschrieben und dann mittels „`pgp Dateiname`“ entschlüsseln werden muss (den Hinweis auf die nicht überprüfbare Unterschrift ignorieren Sie hier einfach noch!).
In der Nachricht wird man nun aufgefordert, zur Verifizierung der eigenen e-mail Adresse eine Bestätigungsmail mit fest vorgeschriebenem Inhalt an die Zertifizierungsstelle zu senden. Nachdem dies geschehen ist, erhält man eine weitere e-mail, die den zertifizierten öffentlichen Schlüssel und die öffentlichen Signierschlüssel der Zertifizierungsstelle enthält.
Den zertifizierten öffentlichen Schlüssel (und eventuell auch die Trustcenter-Schlüssel) kann man nun mittels

```
% pgp -ka Dateiname.pub
```

dem eigenen Schlüsselring hinzufügen.

#### 2.2.5.1. Sichern von Dateien gegen unbefugtes Lesen (Codieren)

Um verschlüsselte Dateien beispielsweise einem Kollegen zuzusenden, wird dessen öffentlicher Schlüssel benötigt. Hat man diesen noch nicht erfahren so kann man versuchen über

http://www.pca.dfn.de/dfnpca/pgpkserv/#extract

den Schlüssel zu erhalten.

Im Besitz des Schlüssels, einer Datei `xxx.pub` mit einem Inhalt ähnlich zu

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 5.0
Comment: PGP Key Server 0.9.4

mQCNAzONkfwAAAEEANyx5XD9uAk8e3b5cQQ3WyhaeVkNadH2BPovm28ctAirF0D/
...
HLMc4crlQm2Ev8RYWzzjkGbQnzjudtUyHingfBc=
=zRXA
-----END PGP PUBLIC KEY BLOCK-----
```

sollte dieser mittels

```
% pgp -ka xxx.pub
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 07:35 GMT

Suche nach neuen Schlüsseln...
öff 1024/94DB4A21 1997/05/29 Holger Wirtz <wirtz@dfn.de>

Überprüfung der Unterschriften...
öff 1024/94DB4A21 1997/05/29 Holger Wirtz <wirtz@dfn.de>
Unt! 94DB4A21 1997/05/29 Holger Wirtz <wirtz@dfn.de>


Die Datei enthält folgende Schlüssel:
1 neü(n) Schlüssel

Ein oder mehrere neue Schlüssel sind nicht ausreichend beglaubigt.
Willst Du sie selbst beglaubigen? (j/N) n
```

dem eigenen öffentlichen Schlüsselring hinzugefügt werden.

Codiert man nun die eine Datei für Holger Wirtz `<wirtz@dfn.de>`, so erreicht man dies analog zu:

```
% pgp -e Sieb.p wirtz
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:14 GMT


Verschlüsselung mit Empfänger-Schlüssel(n).

Schlüssel für Benutzer-ID "Holger Wirtz <wirtz@dfn.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 94DB4A21, erzeugt am: 1997/05/29.
```

```
WARNUNG: Da dieser öffentliche Schlüssel nicht mit einer
vertraünswürdigen Unterschrift beglaubigt ist, ist nicht
sicher, daß er wirklich zu "Holger Wirtz <wirtz@dfn.de>" gehört.

Bist Du sicher, daß Du diesen Schlüssel benutzen willst? (j/N) j
.
Verschlüsselte Datei: Sieb.p.pgp
```

Die Datei `Sieb.p.pgp` kann nun nur noch vom Besitzer des privaten Schlüssels von "`Holger Wirtz <wirtz@dfn.de>`" entschlüsselt werden:

```
% pgp Sieb.p.pgp
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:15 GMT

Die Datei ist verschlüsselt. Zum Lesen wird der private
Schlüssel benötigt.

Diese Nachricht kann nur gelesen werden von:
Holger Wirtz <wirtz@dfn.de>

Dir fehlt der private Schlüssel zum Entschlüsseln dieser Datei.

Eine Übersicht der PGP-Befehle erhältst Du mit: pgp -h
Ausführlichere Hilfe findet sich in der PGP-Anleitung.
```

Soll die codierte Datei ebenfalls von uns decodiert werden können, so muss für die Verschlüsselung der eigne Name (hier: Nachname) angegeben werden:

```
% pgp -e Sieb.p wirtz Nachname
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:22 GMT


Verschlüsselung mit Empfänger-Schlüssel(n).

Schlüssel für Benutzer-ID "Holger Wirtz <wirtz@dfn.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 94DB4A21, erzeugt am: 1997/05/29.

WARNUNG: Da dieser öffentliche Schlüssel nicht mit einer
vertraünswürdigen Unterschrift beglaubigt ist, ist nicht
sicher, daß er wirklich zu
"Holger Wirtz <wirtz@dfn.de>" gehört.
Aber Du hast diesen Schlüssel trotzdem bereits benutzt...

Schlüssel für Benutzer-ID "Titel Vorname Nachname
<Vorname.Nachname@math.uni-wuppertal.de",
1024-Bit-Schlüssel, Schlüssel-ID: 5647284D, erzeugt am: 2000/06/14.
.
Verschlüsselte Datei: Sieb.p.pgp
```

Jetzt können "`Holger Wirtz <wirtz@dfn.de>`" und "`Titel Vorname Nachname <Vorname.Nachname@math.uni-wuppertal.de`" die Datei decodieren:

```
pgp Sieb.p.pgp
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die
Massen.
```

```
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:27 GMT

Die Datei ist verschlüsselt. Zum Lesen wird der private
Schlüssel benötigt.

Schlüssel für Benutzer-ID "Titel Vorname Nachname <Vorname.Nachname@math.uni-wuppertal.
    de",
1024-Bit-Schlüssel, Schlüssel-ID: 5647284D, erzeugt am: 2000/06/14.

Du brauchst ein Mantra, um Deinen privaten RSA-Schlüssel zu benutzen.
Gib das Mantra ein: ...
```

mit Ihrem Nachnamen ausgeführt werden!

**Bemerkung:** „`pgp -ew`“ und „`pgp -ea`“, „`pgp -ewa`“ sind analog wie oben benutzbar.

#### 2.2.5.2. Sichern von Dateien gegen Fälschungsversuche (Signieren)/Unterschrift

**Sichern von Dateien für den lokalen Gebrauch** Beim Signieren wird nur das eigene RSA-Schlüsselpaar benötigt: Der die signierte Datei Überprüfende benötigt jedoch den öffentlichen Schlüssel des Signierenden. Signierte Dateien sind ein Mittel, Erstveröffentlichungrechte von elektronischen Publikationen, ... zu sichern - die Bibliothek der Universität Wuppertal (http://www.bib.uni-wuppertal.de benutzt zur Zeit im Wuppertaler Hochschulschriftenserver zur Sicherstellung der Authentizität der elektronischen Dokumente den MD5-Digest, wird jedoch zukünftig wahrscheinlich externe PGP-Unterschriften (die ein Datum und die Unterschrift/Signierung enthalten) benutzen.
**Beispiel:**

```
MD5 für MS-DOS:
Bergische Universität - Gesamthochschule Wuppertal,

Dissertation
Hübschen,Thorsten
Lokale Fortsetzbarkeit holomorpher Abbildungen im nicht-pseudokonvexen Fall 2002

MD5 (d070201.pdf) = 60ce41e3a6d3456a9578ad85564f06fe
```

Dateien werden durch

```
% pgp -sb übung9.pdf
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:38 GMT

Für eine Unterschrift wird ein privater Schlüssel benötigt.
Da Du keine Benutzer-ID für Deinen privaten Schlüssel angegeben hast,
wird der letzte zum privaten Schlüsselbund hinzugefügte Schlüssel
benutzt.

Du brauchst ein Mantra, um Deinen privaten RSA-Schlüssel zu benutzen.
Schlüssel für Benutzer-ID "Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 8EC88425, erzeugt am: 2000/06/03.

Gib das Mantra ein:
Das Mantra ist richtig.

Einen Augenblick, bitte....
Unterschriftsdatei: übung9.pdf.sig
```

oder mittels

```
% pgp -sba übung9.pdf
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die
Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:38 GMT

Für eine Unterschrift wird ein privater Schlüssel benötigt.
Da Du keine Benutzer-ID für Deinen privaten Schlüssel angegeben hast,
wird der letzte zum privaten Schlüsselbund hinzugefügte Schlüssel
benutzt.

Du brauchst ein Mantra, um Deinen privaten RSA-Schlüssel zu benutzen.
```

```
Schlüssel für Benutzer-ID "Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 8EC88425, erzeugt am: 2000/06/03.

Gib das Mantra ein:
Das Mantra ist richtig.

Einen Augenblick, bitte....
Dateiname der Versandhülle: übung9.pdf.asc
```

signiert.

### Überprüfen von signierten Dateien auf Authentizität

```
% pgp übung9.pdf.asc
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die
Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 08:40 GMT

Diese Datei trägt eine Unterschrift.
Zur Überprüfung wird der öffentliche Schlüssel benötigt.

Die Datei 'übung9.pdf.$00' enthält eine Unterschrift, aber keinen Text.
Der Text könnte sich in der Datei 'übung9.pdf' befinden.
.
BESTÄTIGTE Unterschrift von "Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>",
Unterschrift erzeugt am 2000/06/15 08:38 GMT mit 1024-Bit-Schlüssel 0x8EC88425.

Unterschrift und Text sind getrennt. Es wurde keine Ausgabedatei erzeugt.
```

#### 2.2.5.3. Sichern von Dateien gegen Fälschungsversuchen beim Austausch mit anderen

Kehren wir zu unserem Beispiel zurück, in dem wir einem Kollegen eine Datei übermitteln wollten. Der Empfänger möchte dann natürlich die Datei auf Authentizität überprüfen und benötigt dazu unseren öffentlichen Schlüssel. Er muss den Schlüssel mittels „`pgp -ka`“ seinem Schlüsselring hinzufügen. Dann kann er ebenfalls durch

```
% pgp Datei.Extension.asc
```

oder

```
% pgp Datei.Extension.sig
```

die Authentizität der übermittelten Datei überprüfen.

**Codieren und Signieren von Dateien**
Mittels „`pgp -sea`“ ist das Codieren mit dem Signieren kombinierbar.

### 2.2.5.4. Austausch des öffentlichen PGP-Schlüssels

**per e-mail** Ein Kollege möchte eine von uns signierte Datei auf Authentizität überprüfen und bittet uns, ihm unseren öffentlichen Schlüssel zu schicken. Das kann man folgendermaßen bewerkstelligen:

```
% pgp -kxa buhl buhl.pub
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 09:07 GMT

Extrahieren aus dem Schlüsselbund: '/home/buhl/.pgp/pubring.pgp'
Benutzer-ID " buhl ".

Schlüssel für Benutzer-ID "Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>",
1024-Bit-Schlüssel, Schlüssel-ID: 8EC88425, erzeugt am: 2000/06/03.

Dateiname der Versandhülle: buhl.pub.asc

Schlüssel extrahiert in Datei 'buhl.pub.asc'.
```

Nun müssen wir ihm den Inhalt der gerade erzeugten Datei zuschicken, der folgende Gestalt haben könnte:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAzk5RF4AAAEEANn+XJ7G/eqjFnpfVNrz4iwLs0x7OjIJi/ynNTOgirD5VF7k
LcH6lOPX2+gbYMneXjA4mcp453H1NihqeZEfzfT9L6ZX6HNEQguU5NgwXP3JZXDT
/WopNMaKrULckUgrJadu174DKeK4ERL34Pvc3XctM4haVUfg6obmfx2OyIQlAAUT
tEVQcm9mLiBEci4gSGFucy1KdWVyZ2VuIEJ1aGwgPEhhbnMtSnVlcmdlbi5CdWhs
QG1hdGgudW5pLXd1cHBlcnRhbC5kZT6JAJUDBRA5OURehuZ/HY7IhCUBAW8UA/9E
AfiYTATybYe3m7FXZ7VkBj/jA5IR4U+eHjJbnJtCgiVsE9wwvNbqpa6HAvI+488n
i4TlLgKHXc7Yh0A+vWYhnPpEa01HZ9At3A+0bYvL7CEGq2g1Zar/dlylHK2WxTMQ
1MLGxoM3C872yDhyqWhsWSNCuwHjgC0goTEimm11Lw==
=xPxi
-----END PGP PUBLIC KEY BLOCK-----
```

Unser Kollege erzeugt sich jetzt eine eigene Datei `buhl.pub` mit obigem Inhalt und fügt unseren öffentlichen Schlussel seinem Schlüselring hinzu:

```
% pgp -ka buhl.pub
```

Eventuell möchte er sich davon überzeugen, dass auf dem Mailwege nicht eine Verfälschung des Schlüssels erfolgte und überprüft den Fingerprint unseres Schlüssels:

```
% pgp -kvc
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 09:13 GMT

Schlüsselbund '/home/buhl/.pgp/pubring.pgp':

Typ Bits/ID Datum Benutzer
öff 1024/8EC88425 2000/06/03 Prof. Dr. Hans-Jürgen Buhl
```

```
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>
Fingerabdruck des Schlüssels: 0D 8D 6A 80 A9 A3 4A D8 84 A8 EA 2E 92 33 A6 F6
Es wurde ein passender Schlüssel gefunden.
```

Jetzt könnte er uns per Telefon bitten, die Übereinstimmung des Fingerabdrucks zu überprüfen:

```
% pgp -kvc buhl
Pretty Good Privacy(tm) 2.6.3ia - Public-key-Verschlüsselung für die Massen.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
Internationale Version - nicht in den USA verwenden! Benutzt nicht
RSAREF.
Aktuelles Datum und Uhrzeit: 2000/06/15 09:16 GMT

Schlüsselbund '/home/buhl/.pgp/pubring.pgp':
Suche nach Benutzer-ID "buhl":

Typ Bits/ID Datum Benutzer
öff 1024/8EC88425 2000/06/03 Prof. Dr. Hans-Jürgen Buhl
<Hans-Jürgen.Buhl@math.uni-wuppertal.de>
Fingerabdruck des Schlüssels: 0D 8D 6A 80 A9 A3 4A D8 84 A8 EA 2E 92 33 A6 F6
Es wurde ein passender Schlüssel gefunden.
```

**auf dem (weltweiten) PGP-Schlüssel-Server (WWW-Interface)** Auf der WWW-Seite

http://www.pca.dfn.de/dfnpca/pgpkserv/#submit

können Email-Adressen und zugehörige PGP-Schlüssel abgespeichert werden. Dazu muss nur auf der obigen Internet-Seite die e-mail Adresse sowie im Feld "`ASCII-Version Ihres Schlüssels`" den mit "`-----BEGIN PGP PUBLIC KEY BLOCK-----`" beginnenden Teil des Outputs von "`pgp -kxaf IhrName`" eingegeben werden und auf "`Absenden an den Key Server!`" geklickt werden.

#### 2.2.5.5. Abfrage eines öffentlichen PGP-Schlüssels

**auf dem (weltweiten) PGP-Schlüssel-Server (WWW-Interface)** Benötigen wir z.B. den öffentlichen Schlüssel von unserem Kollegen Herrn Holger Wirtz (`wirtz@dfn.de`), so können wir diesen über das oben besprochene WWW-Interface erhalten.
Dazu einfach in das Such-String-Feld der WWW-Seite

http://www.pca.dfn.de/dfnpca/pgpkserv/#extract

oder der Seite

http://www.pgp.net/pgpnet/wwwkeys.html

`Holger Wirtz` eingeben und auf den "`Suche starten!`"-Knopf drücken:

```
Public Key Server -- Index ‘‘holger wirtz ’’

Type bits/keyID Date User ID
pub 1024/94DB4A21 1997/05/29 Holger Wirtz <wirtz@dfn.de>
pub 1024/155FD609 1995/08/21 Holger Wirtz <root@midips.snafu.de>
Holger Wirtz <wirtz@dfn.de>
Holger Wirtz <chick@midips.snafu.de>
```

Klickt man jetzt auf `wirtz@dfn.de` so erhält man

```
Public Key Server -- Get ‘‘0x94DB4A21 ’’

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 5.0
Comment: PGP Key Server 0.9.4

mQCNAzONkfwAAAEEANyx5XD9uAk8e3b5cQQ3WyhaeVkNadH2BPovm28ctAirFOD/
L3j67I5ql1v5ü129zhbcwhCvXU1u+ig3zgy+ZjXkZF9UW31bRvxUYlm+6jCnpSA
vYTODu5D19tD+FJJRDNwsfVCS396Jqx9GHsiJ0urZRHiCo2psmn58OWU20ohAAUR
tBtIb2xnZXIgV2lydHogPHdpcnR6QGRmbi5kZT6JAJUDBRAzjZH8afnw5ZTbSiEB
AVM4A/9NyNc7NLjF/t7qfc8DSKWSyxI7mTSO7LrpZQMh8Zm5WcicO1QsYo7kB48m
uBGFMtAIwQo5Ea6qDCgcWzj7YqY60m3uZH/jQPS3V+wQs9lUsqdvKLdlTKn6Ouw8
mKTxyRpmF3jQ1RNkXD38cnTXyevnn0bM3kZnljecLy+Z8ceeu4kBFQMFEDOf5fmT
76X8/pPquQEBccYH/1TaA8Z+7jxnDhlJZnIj8rfs4Y3Z/EXNcv+Maw6WpCzKf61Q
kQNyYpN7+Qd0HdrgvKQ7iOqlSBJtVSnrlTduzzMYJN15K4döuIVe4dDPSNfy4P5
rkxbzZWVSQcöA/tfUks4dDCdwTLmDGmTsswFFAF2ayTRJYU+1By6Dbpn+cjFC+X
B1FPgZu2birz0KTfATkOIGFmVRjh3iOvPeNXHcCLlrQ/bEBuCgKbjJiUKHOGhy7u
S2QR4RMGlSoVFm1faXcmCTHcaTRiP/9W6rUAEgT3ufHvAXpjGebpUGhrL3fMeX2x
HLMc4crlQm2Ev8RYWzzjkGbQnzjudtUyHingfBc=
=zRXA
-----END PGP PUBLIC KEY BLOCK-----
```

(Den Fingerabdruck kann man sich über den Knopf "`Anzeige der Fingerprints`" anzeigen lassen.)

**auf dem Trustcenter Zertifikat-Suchserver (WWW-Interface)** Über die WWW-Seite

https://www.trustcenter.de:443/fcgi-bin/search.cgi

oder

https://www.trustcenter.de:443/certservices/search/de/pgp_suche.htm

kann man PGP und S/MIME-Zertifikate suchen, die das Trustcenter ausgestellt hat. PGP-Zertifikate sollten in eine Datei heruntergeladen und dann mittels "`pgp -ka Dateiname`" der PGP-Datenbank hinzugefügt werden.

#### 2.2.5.6. PGP unter Windows

**Die Aegis-Shell als GUI für PGP unter Windows** Im Fachbereich Mathematik kann eine CD ausgeliehen werden, die die Binaries fur PGP und eine GUI-basierte Shell für PGP enthält.

Alternativ kann dies auch im Internet gefunden werden:

PGP (`http://www.pgp.com`)

Aegis-Shell (`http://www.aegis.com`)

## Verschlüsselungs-Software PGP 8.0 ist fertig

Nachdem die ersten Beta-Versionen bereits anständig funktionierten, stellt – wie bereits angekündigt – die PGP Corporation jetzt die Final-Version von PGP 8.0 für Windows und Macintosh zum Download bereit. PGP (Pretty Good Privacy) ist die am weitesten verbreitete Verschlüsselungs-Software nach dem OpenPGP-Standard.

Für die neue Ausgabe gibt es jetzt vier Preismodelle. Nach wie vor gibt es eine Freeware-Version (`http://www.pgp.com/display.php?pageID=83`), die für die private Nutzung kostenlos ist. Dazu kommt die "Desktop Edition" für 80 US-Dollar, die die bekannte Festplattenverschlüsselung PGP Disk und Mail-Plugins bietet. Die "Enterprise Edition" kommt auf 125 US-Dollar und bietet zusätzlich ADK-Support (Additional Decryption Keys) und Komfortfunktionen für Administratoren. Die "Personal Edition" für 39 US-Dollar ist eine abgespeckte Desktop Edition, in der die Integration mit Microsoft Exchange und Lotus Notes fehlt. (pab/c't)

Abbildung 2.1.: Quelle: heise online
`http://www.heise.de/newsticker/data/pab-03.12.02-001/`

#### 2.2.5.7. Dokumentation von PGP

- `man pgp` (http://www.menet.umn.edu/docs/pgp/pgp.txt)
- http://www.menet.umn.edu/docs/pgp/pgpdoc1.txt
- http://www.menet.umn.edu/docs/pgp/pgpdoc2.txt
- http://www.foebud.org/pgp/
- http://senderek.de/security/schutz.html
- Simon Garfinkel: PGP, O'Reilly, 1996

#### 2.2.5.8. Quellen

- ftp://ftp.dfn.de/pub/net/mail/pgp262uis.tar.gz
- CD des FB7 mit Windows-Versionen von pgp, Aegis und ssh2.1.0
- SuSE HowTos http://www.suse.de/de/private/support/howto/index.html
- Aegis http://www.aegis.com

## 2.3. SSL und https

Um codierte Übertragungen von Geschäftsdaten im Web zu realisieren, *muss* das https (s=secure)-Protokoll benutzt werden. Dazu wird der „secure socket layer“ (ssl) auf dem Server benötigt. Mann muss als neben z. B. Apache (als http-Server) noch `openssl` installieren.
Genaueres findet man unter:

- M.D. Bauer: Buidling Secure Servers with Linux, O'Reilly and Associates
- `http://www.apache.org`
- Laurie and P. Laurie. Apache: The Denitive Guide. O'Reilly and Associates
- `http://www.openssl.org`
- J. Viega, M. Messier, and P. Chandra, Network Security with OpenSSL, 2002, O'Reilly and Associates
- `http://lamps.efactory.de`
- `http://www.onlamp.com/pub/a/onlamp/2002/04/18/ssl.html`

**Bemerkung:** Verlangt man von seinen Kunden beim Ausfüllen von Formularen persönliche und/oder Kontodaten, so muss dieses immer auf https-Seiten geschehen! Außerdem müssen diese persönlichen Daten möglichst sicher vor Ausspähung verwahrt werden.

## 2.4. Secure Shell und sichere X-Verbindungen

Statt `telnet`, `ftp`, `rsh`, `rlogin` und `rexec` sollte heute aus Sicherheitsgründen (alle genannte Tools übertragen die Loginprozedur bis hin zur Passworteingabe völlig uncodiert über das Netz) nur noch die „secure shell“ (`ssh`) benutzt werden.

### 2.4.1. Einrichten eines Accounts zur ssh-Benutzung (inkl. RSA-Schlüsselerzeugung)

Möchte man häufiger von der eigenen Maschine (`woher`) aus über das Netz auf anderen Maschinen (`wohin`) arbeiten, so sollte die `ssh` benutzt werden. Dazu bereitet man den Arbeitsplatz folgendermaßen vor:
Erzeugen des `ssh`-RSA-Schlüsselpaars auf `woher` :

```
woher% ssh-pubkeymgr

Running ssh-pubkeymgr..
Used keypair: id_dsa_1024_a and id_dsa_1024_a.pub

Checking for existing user public keys..
Couldn't find your DSA keypair.. I'll generate you a new set..
Running ssh-keygen2... don't forget to give it a passphrase!
Generating 1024-bit dsa key pair
3 o.oOo..oOo.o
Key generated.
1024-bit dsa, userAufWoher@woher <mailto:userAufWoher@woher>, Fri Jun 16 2000 11:58:05
Passphrase : <- einen geheimen Satz
Again :
Private key saved to /home/userAufWoher/.ssh2/id_dsa_1024_a
Public key saved to /home/userAufWoher/.ssh2/id_dsa_1024_a.pub
Creating your identity file..
Creating your authorization file..

Note: You'll need to edit this appropriately.
Creating your local host public key..
Adding your local host in case you don't want to go anywhere ;

Do you want to add any hosts public keys
(files already locally existing in /home/userAufWoher/.ssh2/)
in into your authorization file? (Default: no) <cr>
Skipping editing the authorization file..

All the new files (if any needed to be created) are in your ~/.ssh2 directory.

Do you want to upload your public key file userAufWoher-woher.pub
to a remote host? (Default: no) <cr>
Skipping local user public key uploads..

Do you want to download user-hostname.pub key file
from a remote host? (Default: no) <cr>
Skipping local user public key uploads..


Don't forget to run ssh-pubkeymgr on any remote hosts you sent
your public key to.

Done.
woher%
```

Um jetzt die remote-Computerarbeitsplätze, auf denen häufig gearbeitet wird (`wohin`), für eine sichere `ssh`-Verbindung herzurichten (eigenes RSA-Schlüsselpaar und öffentlichen Schlüssel von woher), ist folgendermaßen vorzugehen

```
woher% ssh wohin -l userAufWohin
Are you sure you want to continue connecting (yes/no)? yes
userAufWohin's password: xxxxxx
Last login: Tue Feb 29 2000 08:51:29 from woher.math.uni-
Sun Microsystems Inc. SunOS 5.x Generic July 19nn
No mail.

wohin% ssh-pubkeymgr
Running ssh-pubkeymgr..
Used keypair: id_dsa_1024_a and id_dsa_1024_a.pub

Checking for existing user public keys..
Couldn't find your DSA keypair.. I'll generate you a new set..
Running ssh-keygen2... don't forget to give it a passphrase!
Generating 1024-bit dsa key pair
2 Oo.oOo.oOo.o <-- dauert recht lang!
Key generated.
1024-bit dsa, userAufWohin@wohin <mailto:userAufWohin@wohin>, Mon Jun 05 2000 11:51:24
Passphrase : <-- hier einen mehrwörtigen Satz eingeben
Again :
Private key saved to /home/userAufWohin/.ssh2/id_dsa_1024_a
Public key saved to /home/userAufWohin/.ssh2/id_dsa_1024_a.pub
Creating your identity file..
Creating your authorization file..

Note: You'll need to edit this appropriately.
Creating your local host public key..
Adding your local host in case you don't want to go anywhere ;

Do you want to add any hosts public keys
(files already locally existing in /home/userAufWohin/.ssh2/)
in into your authorization file? (Default: no) <CR>
Skipping editing the authorization file..

All the new files (if any needed to be created) are
in your ~/.ssh2 directory.

Do you want to upload your public key file userAufWohin-wohin.pub
to a remote host? (Default: no) <CR>
Skipping local user public key uploads..

Do you want to download user-hostname.pub key file
from a remote host? (Default: no) yes
Download from which host?
woher
Which user account?
userAufWoher
Now running scp2 to connect to woher..
Most likely you'll have to type a password :)
Are you sure you want to continue connecting (yes/no)? yes
userAufWoher-woher.pub | 728B | 0.7 kB/s | TOC: 00:00:01 | 100%

You added userAufWoher at woher as a trusted login.

Press yes to download from more hosts or return for skipping.
...
```

**Bemerkung:**
Wenn die verwendeten Systeme `woher` und `wohin` kein Tool `ssh-pubkeymgr` besitzen, kann etwas umständlicher wie folgt vorgegangen werden:

Man erzeugt mittels

```
wpher% ssh-keygen -t dsa
```

ein Schlüsselpaar

```
woher% cd $HOME/.ssh            (bzw. ssh2)
woher% ls -l
-rw------- ... id_dsa
-rw-r-r--- ... id_dsa.pub
```

und überträgt den öffentlichen Schlüssel sodann mittels

```
woher% scp id_dsa wohin:woher_id_dsa.pub
```

auf den Zielrechner `wohin`.

**Bemerkung:** Die Rechte jedes `$HOME/.ssh`-Ordners müssen `0700` sein!

Nach Wechsel auf den Zielrechner

```
woher% ssh wohin
wohin passwort: ...
```

legt man dort das `.ssh`-Verzeichnis an

```
wohin% mkdir .ssh
wohin% chmod 700 .ssh
wohin% cd .ssh
```

und erlaubt dem gerade übertragenen Schlüssel künftiges Einloggen nur mit Passphrase und ohne Passwort

```
wohin% cut $HOME/woher_id_dsa.pub>authorized_keys2
```

Beim nächsten Einlogversuch von `woher` nach `wohin` wird man dann statt nach dem (codiert über das Netz übertragenen) Passwort nach der (nicht mehr über das Netz übertragenen) Passphrase gefragt:

```
woher% ssh wohin
Enter passphrase for key 'home/user/.ssh/id_dsa':
```

Die Beispiel gilt für die `openssh`. Sollte die Zielmaschine ein Solaris9-Compter mit der `sun_ssh.1.0` sein, so muss der öffentliche Schlüssel des Rechners, dem Zugriff erlaubt werden soll, analog in die Datei

`.ssh/authorized_keys`

übertragen werden.
Sollte die Zielmaschine jedoch mit einer kommerziellen `ssh` (`www.ssh.com`) ausgestattet sein, ist der öffentliche Schlüssel zunächst in ein alternatives Format,

```
woher% cd $HOME/.ssh
woher% ssh-keygen -e -f id_dsa.pub>id_dsa_secsh.pub
```

das „SECSH Public Key File Format“, umzuwandeln, diese Version sodann ins Verzeichnis `.ssh2` auf den Zielrechner zu übertragen und sodann in `wohin:.ssh2/authorization` die Zeile

```
key id_dsa.secsh.pub
```

einzutragen.
Alternativ kann der öffentliche Schlüssel im SECSH-Format aus dem privaten Schlüssel erzeugt und übetragen werden mittels

```
woher% ssh-keygen -e -f id_dsa > id_dsa_secsh.pub
```

**Bemerkung:** Die Option `-i` des openssh-Kommandos `ssh-keygen` erlaubt es, im SECSH-Format vorliegende unkodierte, d.h. mit leerer Passphrase angelegte, öffentliche und private Schlüssel in das openssh-Format zu übersetzen.

Will man die Einlog-Vorgänge per `ssh` in Logfiles festhalten, ist folgendes zu beachten:

1. Die openssh trägt eine Zeile der Form

   ```
   Aug 05 08:21:11 wohin sshd[4136]: Accepted
           plubickey for user from woher port 21111 5212
   ```

   in die Datei `/usr/log/messages` ein.

2. Auf Solaris-Rechnern hat man in der Datei `etc/syslog.conf` eine Zeile

   ```
   auth.notice ifdef(`LOGHOST`,/var/log/authlog,@loghost)
   ```

   zu aktivieren. Dann wird die Benutzung einer kommerziellen `ssh` automatisch in Datei `/var/log/authlog` protokolliert, sofern diese einmal mittels

   ```
   wohin% touch /var/log/authlog
   ```

   angelegt wurde:

   ```
   Aug 05 08:21:11 wohin sshd2[4133]: User user,
           coming from unt-at-hsw9.dialin.de, authenticated.
   ```

3. Bei Benutzung der Sun-`ssh` ist zusätzlich deren Konfiguration in `/etc/ssh/sshd_config` auf

   ```
   SyslogFacility          auth
   LogLevel                info
   ```

   zu ändern. Zugleich ist in `/etc/syslog.conf`

   ```
   auth.info       ifdef(`LOGHOST`,/var/log/authlog,@loghost)
   ```

   zu nutzen.

### Erzeugen eines privaten openssh-Format- und SECSH-Format-Schlüssel für alle „sicheren“ Maschinen

Mit der Option `-e` der `openssh` kann man auch den privaten Schlüssel der kommerziellen ssh (im SECSH-Format) ins `openssh`-Format wandeln. Dazu muss der Schlüssel aber unkodiert (leere Passphrase) als Datei vorliegen. Das Umwandeln des privaten Schlüssels auf der Maschine mit der `openssh` geschieht dann mittels

```
wminf7% ssh-keygen -e id_dsa_1024_a
Passphrase needed for key "1024-bit dsa, buhl@wminf7 <mailto:buhl@wminf7>, Thu May
     11 2000 16:52:37".
Passphrase :
Do you want to edit key "1024-bit dsa, buhl@wminf7 <mailto:buhl@wminf7>, Thu May
     11 2000 16:52:37" (yes or no)? yes
Your key comment is "1024-bit dsa, buhl@wminf7 <mailto:buhl@wminf7>, Thu May
     11 2000 16:52:37". Do you want to edit it (yes or no)? no
Do you want to edit passphrase (yes or no)? yes
New passphrase :
Again :
Do you want to continue editing key "1024-bit dsa, buhl@wminf7 <mailto:buhl@wminf7>,
    Thu May 11 2000 16:52:37" (yes or no)? no
Do you want to save key "1024-bit dsa, buhl@wminf7 <mailto:buhl@wminf7>, Thu May
     11 2000 16:52:37" to file id_dsa_1024_a (yes or no)? yes
wminf7% ls -al id_dsa_1024_a id_dsa_1024_a.old
-rw------- 1 buhl inf 859 Aug 19 15:06 id_dsa_1024_a
-rw------- 1 buhl inf 867 Aug 18 14:41 id_dsa_1024_a.old
```

in diese uncodierte Form[4]. Nach Übertragung auf eine `openssh`-Maschine kann dort durch

```
buhl@wminf11:~/tmp <mailto:buhl@wminf11:~/tmp>> ssh-keygen -i -f id_dsa_1024_a.
    withoutPassphrase
-----BEGIN DSA PRIVATE KEY-----
MIIBugIBAAKBgQCn09z+PBQnveR01feCdzkD/kugdvp2LBhAuAEqAYgPbA4vzfcG
1nf07H2YjO3eie2gdUGIglxJi77U7F+E3gN5kBMjUj+8zzEZq0h4ZBPVX4LYTToa
/VhINbNfBvBBWRNxkb2DJGjGYTt7jAWai1Ra2FvUKx66MyCG75BYjiMF5QIVALyV
PZZZ7EllO/ZNATgUUh1dMr7BAoGAYKiB6YqZjqa9kjHVGKURy2Ac4U5Syf+2R1dS
dxVQ0m8Toar6NjYH5oKFevTVbQbW1hUcrfdJ+84wNoTqqRE9JTHJYNVL4pp4SxMX
1hFeY89Rnhf2+qi5vdT+42dN1Pe585DJKew2iqpjFlu+Z5qPw3mqG73sND+8/FJ+
pSk/YF4CgYA3HHfTihco/O8MnkPCfbuzU1ae5NrABDPr+OXSEJVZO8WZAUJPLWXp
dPHw8Jl7AeKJ5kXZCVX/j2s9BgcIcthMK74w6c7evbnFD/3FYZ3dnfFXAzAAg0yf
moewOfMcx5pByonL2x+VcanEhSOCi0W03nptR57ToXCqbjbi7zn29AIUfivx/ivB
aveeFTkZO5zXcncmQuM=
-----END DSA PRIVATE KEY-----
buhl@wminf11:~/tmp <mailto:buhl@wminf11:~/tmp>> ssh-keygen -i -f id_dsa_1024_a.
    withoutPassphrase > id_dsa
buhl@wminf11:~/tmp <mailto:buhl@wminf11:~/tmp>> chmod go-r id_dsa
```

der SECSH-Schlüssel importiert, mittels

```
buhl@wminf11:~/tmp <mailto:buhl@wminf11:~/tmp>> ssh-keygen -p -f id_dsa
Key has comment 'id_dsa'
Enter new passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase.
```

mit einer Passphrase versehen und anschließend der zugehörige öffentliche Schlüssel[5] in

[4] **Beachte:** Nach der Übertragung des privaten Schlüssels ist dieser wieder mit einer Passphrase zu schützen!

[5] der entweder durch `ssh-keygen -y -f id_dsa > id_dsa.pub` erzeugt oder wie oben beschrieben aus dem SECSH-Format konvertiert wurde

die Datei `authorized_keys` geschrieben werden, damit man sich selbst ohne Passwort per `ssh`

```
%ssh localhost
 Enter passphrase for key '/home/buhl/ssh/id_dsa':
```

einloggen kann.

**Bemerkung:** *Rollen-Schlüssel* etwa für den Postmaster einer Firma, den Systemadministrator einer Firma, ... erzeugt man anlog und kann dann in der Datei `authorized_keys` rollenspezifisch den Zugang erlauben.

**Bemerkung:** Auf „unsicheren Maschinen“ kann man sich mittels `authorized_keys` den Zugang über den eigenen üblichen Schlüssel erlauben, sollte aber **niemals** seinen privaten Schlüssel dort ablegen.

**Bemerkung:** Mehr als ein privater Schlüssel kann mittels

```
ssh -i $HOME/.ssh/id_dsa2 wohin
```

benutzt werden, was auch für Rollenschlüssel nutzbar ist.

### 2.4.2. „Remote Login“ mit verschlüsselter Datenübertragung (Passwort, Daten, ....)

Beim nächsten Loginversuch von woher nach wohin wird nicht mehr nach dem Passwort auf `wohin` gefragt

```
woher% ssh wohin -l userAufWohin
Passphrase for key "/home/userAufWoher/.ssh2/id_dsa_1024_a"
with comment "1024-bit dsa, userAufWoher@woher <mailto:userAufWoher@woher>,
Thu May 11 2000 16:52:37": <- Ihre PassPhrase
Last login: Mon Jun 19 2000 12:29:38
No mail.
Sun Microsystems Inc. SunOS 5.6 Generic August 1997
whine%
```

sondern nach der Passphrase auf der lokalen Maschine `woher` (diese wird also nicht mehr über das Netz geschickt!).
Wechselt man häufiger Maschinen oder führt man `remote`-Kommandos aus, so kann die wiederholte Abfrage der Passphrase auf eine einmalige Abfrage abgekürzen werden:

Vgl. »Vermeidung der „dauernden“ Abfrage der Passphrase: `ssh-agent`, `ssh-add`«, Abschnitt 2.4.6

### 2.4.3. „Remote Command“ mit verschlüsselter Datenübertragung (Passwort, Daten, ....)

```
woher% ssh wohin -l userAufWohin df -k
Passphrase for key "/home/userAufWoher/.ssh2/id_dsa_1024_a"
with comment "1024-bit dsa, userAufWoher@woher <mailto:userAufWoher@woher>,
Thu May 11 2000 16:52:37": <- Ihre PassPhrase

Filesystem kbytes used avail capacity Mounted on
/dev/dsk/c0t0d0s0 61735 35469 20093 64% /
/dev/dsk/c0t0d0s6 306367 215665 60066 79% /usr
...
```

Wechselt man häufiger Maschinen oder führt man `remote`-Kommandos aus, so kann die wiederholte Abfrage der Passphrase auf eine einmalige Abfrage abgekürzen werden:

Vgl. »Vermeidung der „dauernden“ Abfrage der Passphrase: `ssh-agent`, `ssh-add`«, Abschnitt 2.4.6

### 2.4.4. „Remote Copy“ mit verschlüsselter Datenübertragung (Passwort, Daten, ....)

```
woher% scp xxx/localfilename user@host:xxx/remotefilename
localfilename | 30kB | 29.5 kB/s | TOC: 00:00:01 | 100%
woher%
```

oder

```
woher% scp user@host:remotefilename  localfilename
```

oder

```
woher% scp -pr localdir user@host:remoteparentdir (Kopie eines ganzen Dateibaums)
```

Wechselt man häufiger Maschinen oder führt man `remote`-Kommandos aus, so kann die wiederholte Abfrage der Passphrase wieder vermieden werden gemäß Abschnitt 2.4.6.

### 2.4.5. „Secure ftp“ mit verschlüsselter Datenübertragung (Passwort, Daten, ....)

```
woher$ sftp user@host
Passphrase for key "/home/buhl/.ssh2/id_dsa_1024_a"
with comment "1024-bit dsa, buhl@wminf7
Thu May 11 2000 16:52:37":
Secure FTP client Sftp2
Copyright (c) 1999, 2000 SSH Communications Security, Finland.

Type 'help <topic>', where <topic> is one of the following commands:

sftp> help
open localopen close quit cd
lcd pwd lpwd ls lls
get mget put mput rm
lrm mkdir lmkdir rmdir lrmdir
sftp> quit
...
```

### 2.4.6. Vermeidung der „dauernden“ Abfrage der Passphrase: `ssh-agent`, `ssh-add`

Die Passphrase sollte nicht auf der Festplatte des Arbeitsplatzes abgelegt werden. Es ist in UNIX jedoch recht sicher, die einmal zugänglich gemachten privaten Schlüssel im Hauptspeicher weiterhin für alle Kindprozesse ohne weitere Passphrase-Abfrage bereit zu halten. Das geschieht durch:

```
woher% ssh-agent -1 csh (oder: ssh-agent -1 xterm& )

woher% ssh-add -l
Listing identities.
The authorization agent has no keys.

woher% ssh-add
Adding identity: /home/userAufWoher/.ssh2/id_dsa_1024_a.pub
Need passphrase for /home/userAufWoher/.ssh2/id_dsa_1024_a
```

```
(1024-bit dsa, userAufWoher@woher, Tue May 23 2000 17:30:19).
Enter passphrase:
woher%

woher% ssh-add -l
Listing identities.
The authorization agent has one key:
id_dsa_1024_a: 1024-bit dsa, userAufWoher@woher, Tue May 23 2000 17:30:19
woher%

...
```

Jetzt sind alle zukünftigen von dieser Shell aus versuchten `ssh`-Logins bzw. `ssh`-Kommandos auch ohne Passphrase-Abfrage möglich.

**Bemerkung:** Loggt man sich von `woher` auf `wohin1` und von dort auf `wohin2` ... ein, so wird die `ssh-agent` Datenbank immer mitvererbt, so dass man im ganzen „Netz“ keine Passphrase mehr eintippen muss.

(Arbeitet man auf einer Solaris-Workstation unter X-Window (OpenWindows oder CDE), ist es am einfachsten den Login umzukonfigurieren:

Hier ein Beispiel für Solaris7 unter `dtlogin`:

```
cd $HOME
vi .dtprofile
eval `/opt/local/Sys/bin/ssh-agent -1`
```

**für CDE:**

```
cd $HOME/.dt/sessions
vi sessionetc
/opt/local/Sys/bin/ssh-add < /dev/null&

chmod 755 sessionetc

vi sessionexit
pkill -9 ssh-agent

chmod 755 sessionexit
```

**für OW:**

```
cd $HOME
mv .xinitrc .xinitrc.old
cp /usr/openwin/lib/Xinitrc $HOME/.xinitrc
vi $HOME/.xinitrc
```

und statt der Zeile `wait $wmpid #...` die folgenden Zeilen einfügen:

```
/opt/local/Sys/bin/ssh-add < /dev/null&
wait $wmpid # Wait for wm (key client) to exit
pkill -9 ssh-agent
```

**Bemerkungen:**

1. Bei Solaris 2.6 und früher ersetzt man die Zeile `pkill -9 ssh-agent` jeweils durch

```
kill -9 $SSH2_AGENT_PID
```

2. Sollte das System kein `pkill` besitzen, so kann `pkill` durch folgendes Skript ersetzt werden:

```
#!/bin/csh
# sucht im 5. Feld von "/usr/ucb/ps ax", d.h. dem ersten Wort des Kdos nach $1
set PATTERN=$1
/usr/ucb/ps ax | grep $PATTERN > /tmp/$$
awk "$ 5 ~ /($PATTERN)/ {print $ 1}" /tmp/$$ >/tmp/$$-2
alias rm rm
rm /tmp/$$

foreach i ( `cat /tmp/$$-2` )
kill -9 $i
end
rm /tmp/$$-2
```

**Für Linux und kde:**

```
% cd
% cp .cinitrc .cinitrs.old
```

```
% vi .xinitrc

...

#
# Add your own lines here...
#
. $HOME/.kdestart
# day planer daemon
# pland &

# finally start the window manager
# exec $WINDOWMANAGER
exec $HOME/.kde-script-copy
#call sailsafe
exit 0
<ESC> wq
```

```
% cp /usr/X1126/bin/kde .kde-script-copy
% ri .kde-script-copy
. $HOME/.kdeexit
<ESC> wq
```

```
% vi .kdestart
eval `ssh-agent`
(ssh-add </dev/null;\
 ssh-add $HOME/.ssh/id_dsa2 </dev/null;\ &
<ESC> wq
```

```
% ri .kdeexit
kill -q $SSH_AGENT_PID
<ESC> wq
```

)

### 2.4.7. Die ssh für PC's unter Windows:

Im Fachbereich Mathematik kann eine CD ausgeliehen werden, die die Binaries einer für den Fachbereich Mathematik der Universität Wuppertal lizensierten `ssh2` enthält.

**Bemerkungen:** Wenn vor Benutzung der `ssh` die Environmentvariable `DISPLAY` gesetzt ist, so ist sie auch nach einem `remote` Login gesetzt und zwar solcher Art, dass *auch* die X-Window Verbindung verschlüsselt über das Netz erfolgt! (D.h. `xhost + ...` ist nicht mehr nötig!)
`ssh-pubkeymgr` ist zur Zeit nur zur Benutzung mit kurzen Hostname's eingerichtet!
Die oben genannte Art der Userauthentifizierung mit RSA-Schlüsseln funkioniert nur mit `wohin`-Rechnern, auf denen `sshd2` installiert ist.
Sollte man mit einer Gegenstation arbeiten müssen, wo nur `sshd1` läuft, so muss man folgendermaßen vorgehen:

```
woher% ssh-keygen1
Initializing random number generator...
Generating p: .................++ (distance 352)
Generating q: ..............++ (distance 244)
Computing the keys...
Testing the keys...
Key generation complete.
Enter file in which to save the key (/homeuserAufWoher/.ssh/identity):
Enter passphrase:
Enter the same passphrase again:
Your identification has been saved in /home/userAufWoher/.ssh/identity.
Your public key is:
1024 35 12584.....................567231 userAufWoher@woher
Your public key has been saved in /home/buhl/.ssh/identity.pub


woher% ssh1 wohin -l userAufWohin
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Host 'wohin' added to the list of known hosts.
userAufWohin@wohin's  password:
Last login: Mon Jun 19 18:07:42 2000 from woher
...
wohin% ssh-keygen
...
wohin% cd $HOME/.ssh
wohin% vi authorized_keys
1024 37 132...234 userAufWoher@woher
        <- pubkey $HOME/.ssh/identity.pub von userAufWoher auf woher
```

Es wird empfohlen, wann immer möglich mit der `ssh` und User-Authentifizierung, statt mit `rsh`, `rlogin`, `rcp`, `ftp`, `telnet` zu arbeiten!
`ftp` ist nur noch für `anonymous-ftp` zu nutzen. Aber nach dem Download von sicherheitskritischer Software sollte vor deren Installation die in der Regel immer vorhandene Signatur der Distribution auf Authentizität überprüft werden (vgl. PGP-Signaturen).
`$HOME/.rhosts`-Dateien sollten nie benutzt werden. Für `crontab`-Skripte, in denen keine Passphrase abgefragt werden kann, kann dazu notfalls auf Hostauthentifizierung mit RSA-Schlüsseln und `$HOME/.shosts`) zurückgegriffen werden:

Vorbereitung von `wohin` auf Hostauthentifizierung:

```
wohin% ssh woher -l userAufWoher
```

```
        <- damit der Hostkey von woher
        <- in $HOME/.ssh2/hostkeys/key_22_woher.pub
        <- angelegt wird
...
wohin% mkdir $HOME/.ssh2/knownhosts
wohin% cd $HOME/.ssh2/knownhosts
wohin% cp ../hostkeys/key_22_woher.pub woher.math.uni-wuppertal.de.ssh-dss.pub

wohin% cd $HOME
wohin% vi .shosts (oder "mv .rhosts .shosts")
woher.math.uni-wuppertal.de userAufWoher
```

Falls auf `wohin` nur `sshd1` läuft, statt dessen:

```
wohin% cd $HOME/.ssh
wohin% vi known_hosts
```

und einfügen der Zeile:

```
woher.math.uni-wuppertal.de 1024 33 12373843...
```

mit vollem Hostnamen. Diese Zeileninhalt wird auf `woher` durch

```
cat /etc/ssh_host_key.pub
```

erhalten und entsprechend umgestellt (voller Hostname am Anfang statt `user@host` am Ende der Zeile).

### 2.4.8. Dokumentation