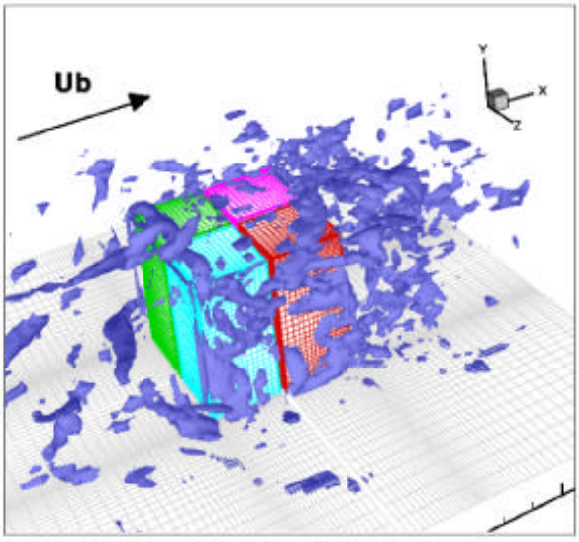
Universität Karlsruhe (TH)
Rechenzentrum

RZ-NEWS

September / Oktober 1999

"Schwarzwald" sortiert eine Billion Bytes in 17-Minuten-Rekord

Internationaler SP-Workshop: Große Resonanz in der Fachwelt



Institut für Hydromechanik: auf dem Parallelrechner IBM RS/6000 SP berechnete Umströmung eines Würfels

Nameservice: Administrative Umstellungen

Computer und Recht

PERMAS Version 7

CALFEM

XILINX Alliance 2.1-i

DCE/DFS

Iterative Löser

ISSN 1432-7015

INHALT

IMPRESSUM

Herausgeber:
Prof. Dr. Wilfried Juling
Redaktion: Ursula Scheller,
Klaus Hardardt
Tel.: 0721/608-4865

Universität Karlsruhe (TH)
Rechenzentrum
D-76128 Karlsruhe
http://www.uni-karlsruhe.de/~RZ-News/
Nummer 9,10/1999
ISSN 1432-7015

“Schwarzwald” sortiert eine Billion Bytes in 17-Minuten-Rekord

Gleicher Rechnertyp auch am Rechenzentrum

(red)

Bereits seit 1997 verfügt das Rechenzentrum der Universität Karlsruhe über einen Hochleistungsrechner vom Typ IBM RS/6000 SP. Hier erhielt er auch seinen Namen: Als vor zwei Jahren eine der ersten großen SP-Installationen in Europa am Rechenzentrum der Fridericiana durchgeführt wurde, entschieden sich die Mitarbeiter des RZ spontan, ihrem neuen Superhirn wegen seiner schwarzen Farbe und der vielen Einzelkomponenten den Namen “Black Forest - Schwarzwald” zu geben.

256-Knoten-Parallelrechner IBM RS/6000 SP am RZ mit 120 Giga Byte Speicherkapazität

Der IBM-Parallelrechner mit dem größten Hauptspeicher in Europa steht Nutzern aus Wissenschaft und Wirtschaft in ganz Deutschland zur Verfügung. Die Stabilität und Leistungsfähigkeit des Supercomputers hat zu einer breit gefächerten, bundesweiten Nutzung in den Bereichen CFD, Physik, Mathematik und Chemie geführt.

Ein Pendant des Karlsruher Uni-Parallelrechners sortierte nun in den USA eine Billion Bytes in 17 Minuten und hat damit einen neuen Weltrekord im Datensortieren aufgestellt.

Die Datenmenge entspricht umgerechnet einem Stapel herkömmlicher Disketten von 1,3 Kilometern Höhe. Mit dem neuen Rekord wurde der alte gleich um 33 Minuten verbessert. Wissenschaftler der Sandia National Laboratories (Albuquerque/New Mexiko) hatten im November vergangenen Jahres zum Sortieren der Daten mit dem Computer noch 50 Minuten gebraucht.

Um die Daten in die richtige Reihenfolge zu bringen, ist im IBM-Forschungszentrum in Poughkeepsie/New York ein Parallelrechner vom Typ RS/6000 SP, Codename: Blackforest - Schwarzwald, eingesetzt worden, teilte das Unternehmen mit.

Ein Mensch bräuchte für die gleiche Aufgabe allein 1.300 Jahre, um die Zahlen zu Papier zu bringen, vorausgesetzt er schafft 15 Einträge pro Minute. Dann wären die Daten aber noch lange nicht sortiert.

Internationaler SP-Workshop fand große Resonanz in der Fachwelt

Neue Rechnerarchitekturen und Parallelisierungskonzepte im Mittelpunkt

Nikolaus Geers, Michael Hennecke

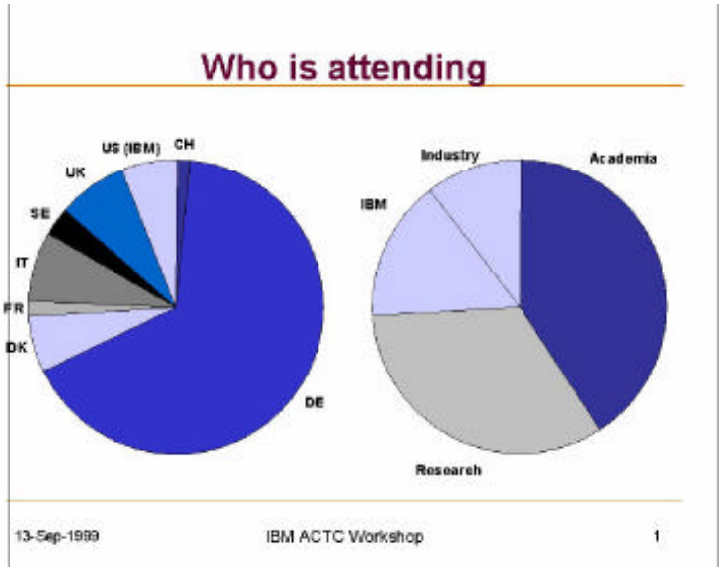
Vom 13. bis zum 15. September fand am Rechenzentrum ein internationaler Workshop zum Thema "Scientific Applications Development and Optimization on the IBM RS/6000 SP" statt. An dem Workshop, der gemeinsam mit dem IBM Advanced Computing Technology Center (ACTC) durchgeführt wurde, nahmen ca. 70 Anwender, Programmentwickler und Systemadministratoren von Höchstleistungsrechnern aus ganz Deutschland sowie dem europäischen Ausland teil.

Ca. 15 Prozent der Teilnehmer kamen aus Industrieunternehmen, die übrigen zu etwa gleichen Teilen aus Hochschulen und öffentlichen Forschungseinrichtungen.

Nikolaus Geers vom RZ mit John Levesque, Direktor des ACTC (v. l.) *Foto: Scheller*

Im Mittelpunkt des Workshops stand die Diskussion um neue Rechnerarchitekturen und die Kombination verschiedener Parallelisierungskonzepte zur Erstellung möglichst effizienter Anwendungsprogramme.

Viele neue Höchstleistungsrechner, so auch neuere Modelle der IBM SP sind als Rechner mit verteiltem Speicher (Distributed Memory) realsiert, wobei jeder einzelne Rechenknoten aus einem Mehrprozessorsystem mit einem gemeinsamen Hauptspeicher (Shared



Memory) besteht. Bei der Programmentwicklung treffen also die verschiedenen Konzepte zur Parallelisierung von Anwendungsprogrammen aufeinander:

- explizites Message Passing mit MPI für Distributed Memory Systeme und
- Parallelisierung innerhalb eines Knotens durch die

Die internationalen Teilnehmer des Workshops kamen aus Industrie und Wissenschaft *Foto: Scheller*

Nutzung des gemeinsamen Hauptspeichers mittels OpenMP oder über die explizite Programmierung von Threads.

Michael Hennecke vom RZ im Gespräch mit Workshop-Teilnehmern (v. r.) *Foto: Scheller*

Der erste Tag des Workshops hatte das Thema "Uni-Processor Performance" und umfasste neben Präsentationen zu Optimierungstechniken und dem optimalen Einsatz der Fortran- und C-Compiler auch eine ausführliche Diskussion der aktuellen bzw. zukünftigen Prozessoren der IBM POWER-Architektur, die die Basis für neue Rechnergenerationen bilden. Abgerundet wurden dieser Tag durch Anwendervorträge über den bisherigen Einsatz von POWER 3-Prozessoren.

Am zweiten Tag wurden die verschiedenen Programmierkonzepte für die Parallelisierung (MPI, OpenMP sowie Pthreads) vorgestellt und an Beispielen die Kombination dieser unterschiedlichen Methoden aufgezeigt. Ergänzt wurden die Diskussionen durch Berichte von Anwendungsprogrammierern über erste Erfahrungen mit dem Einsatz dieses hybriden Programmiermodells.

Der dritte Tag des Workshops beschäftigte sich mit den Themen Ein-/Ausgabe und Tools zur Programmentwicklung und Programmanalyse. Vorgestellt wurden u. a. die asynchrone Ein-/Ausgabe, als zusätzliche Funktion des Fortran-Compilers, das neue Dateisystem GPFS (General Parallel File System) sowie MPI-IO als portable Schnittstelle für parallele Ein-/Ausgabe. Neben der Präsentation bereits existierender Tools (sowohl von IBM als auch von der Pallas GmbH) wurden neue Konzepte für die Entwicklung zukünftiger Softwareentwicklungstools erläutert.

In der Abschlussdiskussion sprachen sich die Teilnehmer nahezu einhellig für eine Fortsetzung der mit diesem Workshop begonnenen Diskussionen und den Erfahrungsaustausch zwischen Anwendungsprogrammierern, IBM Softwareentwicklern und den Mitarbeitern des IBM ACTC aus. Daher ist im kommenden Frühjahr ein weiterer Workshop zu diesem Thema geplant.

Darüber hinaus kam das RZ mit dem IBM Advanced Computing Technology Center am T. J. Watson Research Center überein, die außerordentlich gute Zusammenarbeit noch weiter auszubauen und zu intensivieren.

Kopien der Vortragsfolien sind im Web unter `http://www.uni-karlsruhe.de/~SP/actc-workshop/` abrufbar.

Nikolaus Geers, Tel. -3755,
E-Mail: geers@rz.uni-karlsruhe.de
Michael Hennecke, Tel. -4862,
E-Mail: hennecke@rz.uni-karlsruhe.de.

Nameservice: Administrative Umstellungen

DNS-Server und -Datenbank auf neue Systeme verlagert

Roland Laifer

Im Bereich des 'Domain Name System' (DNS) der Universität Karlsruhe wird es in den nächsten Wochen einige administrative Umstellungen geben. Zunächst wird der Primary DNS-Server auf einen leistungsstärkeren und ausfallgesicherten Rechner umziehen; die Auswirkungen dessen sollten jedoch kaum spürbar sein, weil sich Rechnername und IP-Adresse *nicht* ändern. Zu einem späteren Zeitpunkt wird dann die DNS-Datenbank (IPAVS) erweitert und auf ein neues System verlagert; ausführliche Informationen dazu gibt es in Kürze.

Im Vorfeld dieser Umstellungen sollen natürlich auch ein paar Altlasten beseitigt werden. So gibt es für ein paar ältere Rechner Alias-Einträge in allen Subdomains von `uni-karlsruhe.de`. Einige dieser Aliase

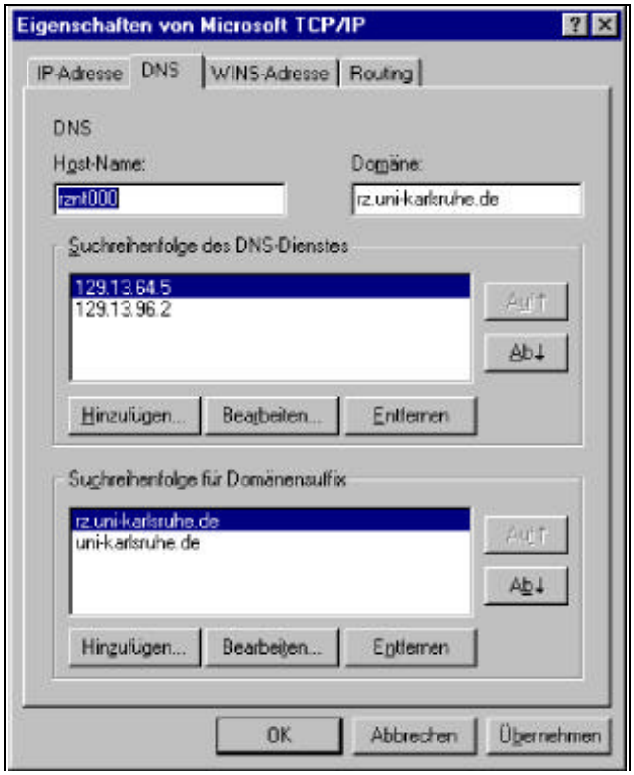
werden Anfang Oktober gelöscht, denn einerseits haben viele zentrale Rechner keine solchen Aliase und andererseits läßt sich die gleiche Funktionalität durch die Konfiguration von Domain-Suchlisten erreichen. Solche Domain-Suchlisten bestimmen, welche Domain-Suffixe an einen unvollständigen Rechnernamen nacheinander angehängt werden, um einen passenden DNS-Eintrag zu suchen.

Auf UNIX-Systemen wird die Domain-Suchliste typischerweise in der Datei `/etc/resolv.conf` über die `search`-Direktive konfiguriert. Angenommen, ein Rechner hat folgende `search`-Direktive in `/etc/resolv.conf`: `search physik.uni-karlsruhe.de uni-karlsruhe.de`. *Vor* der Umstellung funktioniert das Kommando `slogin rz70` aufgrund des Aliases `rz70.physik.uni-karlsruhe.de` nach `rz70.rz.uni-karlsruhe.de`. *Nach* der Umstellung wird der kurze Rechnername `rz70` nicht mehr gefunden, was allerdings durch folgende Erweiterung der `search`-Direktive behoben werden kann:

```
search physik.uni-karlsruhe.de rz.uni-karlsruhe.de uni-karlsruhe.de.
```

Die Kommandos `slogin rz70.rz` und `slogin rz70.rz.uni-karlsruhe.de` funktionieren dagegen mit beiden `search`-Direktiven.

Auf Windows-Systemen wählt man über *Arbeitsplatz, Systemsteuerung, Netzwerk, Protokolle* durch Doppelklicken das *TCP/IP-Protokoll* und dann *DNS* und trägt die Domain-Suffixe im unteren Fenster ein (siehe Abb. unten).



Konfiguration der Domain-Suchliste unter Windows

Roland Laifer, Tel. -4861,
E-Mail: Laifer@rz.uni-karlsruhe.de.

Finite Elemente

Update: PERMAS Version 7 auf SP-Parallelrechner und Compute-Server

Neues Modul für nichtlineare statische Analyse

Dr. Paul Weber

Auf dem Parallelrechner IBM RS/6000 SP und dem Compute-Server RZANW1 ist jetzt die neue Version 7 des Finite-Elemente-Programms PERMAS der Firma INTES GmbH installiert. Neben zahlreichen Verbesserungen der bestehenden Module gibt es jetzt auch ein neues Modul für die nichtlineare statische Analyse.

Diese Modul bietet die folgenden Materialmodelle an:

- Nichtlineare Elastizität
- Plastizität
- Kriechen

Diese Modelle können auch bei Kontaktproblemen verwendet werden.

Die Dokumentation wurde komplett neu überarbeitet und steht als PostScript-Datei im Verzeichnis `/usr/common/rzserv/permas/doc` zur Verfügung:

- PERMAS User's Reference Manual I - III
- PATRAN Door User's Manual
- Examples Manual
- PERMAS Release Notes

Auch die PERMAS-Kurzanleitung des Rechenzentrums wurde überarbeitet und ist unter der URL `http://www.uni-karlsruhe.de/~PERMAS/` zu finden.

Auf den beiden Plattformen ist zurzeit die serielle Version von PERMAS installiert, eine parallele Version wird es auf der IBM RS/6000 SP demnächst ebenfalls geben.

Die Installation auf der SP enthält die sogenannte PATRAN Door zu PATRAN 8.5. Das bedeutet, dass aus einem PATRAN-Modell, welches unter der PERMAS-Präferenz erstellt wurde, die PERMAS-Eingabedateien erzeugt und auch die PERMAS-Ergebnisse wieder in PATRAN dargestellt werden können. Eine Beschreibung der Vorgehensweise ist in der PERMAS-Kurzanleitung zu finden.

Dr. Paul Weber, Tel. -4035,
E-Mail: Paul.Weber@rz.uni-karlsruhe.de.

Neu: CALFEM - Finite-Elemente-Toolbox zu MATLAB

Dr. Paul Weber

CALFEM Version 3.2 ist eine Finite-Elemente-Toolbox zu MATLAB, die von der Division of Structural Mechanics und dem Department of Solid Mechanics an der Lund University in Schweden entwickelt wurde.

Die Toolbox steht sowohl auf dem Parallelrechner IBM RS/6000 SP als auch auf den vom RZ unterstützten HP- und SGI-Maschinen zur Verfügung. Die Elemente-Bibliothek umfasst

- Stäbe und Balken in 2D und 3D
- 2- und 3-dimensionale Kontinuumselemente
- Platten
- 2- und 3-dimensionale Wärmeleitungselemente
- Federelemente

Die Stoffgesetze sind
- linear elastisch
- elastisch-plastisch

und das Problemspektrum, das gelöst werden kann umfasst

- lineare und nichtlineare Statik
- transiente Vorgänge
- Eigenwerte und -frequenzen
- Antwortspektren

Die Ergebnisse können als 2D-Strukturplots, Verschiebungen, Konturplots oder XY-Plots dargestellt werden.

Die Dokumentation besteht aus einem Handbuch, das neben der Beschreibung der CALFEM-M-Files eine kurze Einführung in MATLAB sowie Beispiele enthält. Leider liegt das Handbuch nicht online vor, Interessenten können sich das Buch allerdings bei mir ausleihen.

CALFEM ist in die MATLAB-Installation, die über die kleine Baumschule verteilt wird, integriert. Institute, die MATLAB lokal bei sich installiert haben, können sich die Diskette ebenfalls ausleihen.

Dr. Paul Weber, Tel. -4035,
E-Mail: Paul.Weber@rz.uni-karlsruhe.de.

Mikroelektronik

XILINX Alliance 2.1-i verfügbar

Verbesserte Module

Dieter Kruk

Die Version 2.1-i der Entwicklungssoftware für programmierbare ICs unterstützt jetzt auch die Bausteinserie XILINX 9500XV, eine CPLD-Familie für den Betrieb mit 2,5 V.

Verschiedene Softwaremodule sind überarbeitet oder ausgetauscht worden. So ist jetzt für die Komponente Virtex ein Floorplanner vorhanden; das bisherige Modul EPIC wurde durch den neuen FPGA_Editor ersetzt, der jetzt übrigens auch eine eingebaute Testfunktion enthält. Das Analysemodul für das Zeitverhalten einer Mikroschaltung liefert nun zur Verbesserung der Übersichtlichkeit eine hierarchisch aufgebaute Ausgabe. Generell werden Zeitdiagramme wie auch das I/O register timing ähnlich der Darstellung in Datenblättern ausgegeben. Auch ein CPLD-Baustein-Betrachter ist jetzt vorhanden. Die Version ist jahr-2000-fest. Das Neuheiten-Paket wird einschließlich Dokumentation bei Bedarf allen bisherigen EURO-PRACTICE-XILINX-Anwendern zur Verfügung gestellt.

Hinweis: Am Donnerstag, den 28.10.99, findet von 16.15 bis 17.00 Uhr ein Anwendertreffen der EURO-PRACTICE-Teilhaber auf dem Campus statt (siehe auch Rubrik Vorträge, Workshops und Kurse). Hierbei werden u.a. weitere Neuheiten aus dem EDA-Bereich, Dienstleistungen, die die IC-Herstellung betreffen, sowie Termine von Fachtagungen bekanntgegeben. Darüber hinaus vermittelt das RZ auch Software-Lizenzen, die innerhalb des Campus durch den Abschluß von Projekten frei geworden sind, an neue Eigentümer.

Dieter Kruk, Tel. -3785l
E-Mail: kruk@rz.uni-karlsruhe.de.

Vorlesungsankündigung

Iterative Löser für lineare und nichtlineare Gleichungssyteme

Priv. Doz. Dr. Rüdiger Weiß

Im WS 1999/2000 werde ich die Vorlesung "Iterative Löser für lineare und nichtlineare Gleichungssyteme" halten. Dies ist eine interdisziplinäre Vorlesung über wissenschaftliches und Höchstleistungs-Rechnen. Sie wendet sich an Studierende und Doktoranden aller Fachrichtungen.

Die Lösung von Gleichungssystemen tritt als Kernalgorithmus bei der Simulation fast aller technischen Probleme auf. Daher ist man an schnellen Lösungsverfahren interessiert. Iterative Verfahren haben sich in den letzten Jahren als Standard etabliert. Leider gibt es nicht nur ein optimales iteratives Verfahren, sondern eine Vielzahl von unterschiedlichen Lösern. In dieser Vorlesung wird ein Überblick gegeben und die Vielzahl von Verfahren klassifiziert. Daraus entstehen Rezepte, wann welcher Löser geeignet ist.

Ziel der Vorlesung ist es, die Prinzipien moderner Löser zu erkennen und Zusammenhänge zu verstehen, und nicht, mathematische Formalismen zu entwickeln. Da technische Probleme meistens auf Superrechnern gelöst werden, umfasst die Vorlesung auch eine Einführung in Rechnerarchitekturen und die daraus entstehenden Programmiermodelle.

Die Teilnehmer sollen nach der Vorlesung in der Lage sein, ihre eigenen Probleme effizient lösen zu können. Es werden keine speziellen Vorkenntnisse auf dem Gebiet erwartet. Etwas Computerkenntnis und die

Freude, über den Tellerrand hinwegzusehen, sind allerdings notwendig.

Die Vorlesung umfasst auch multimediale Lerneinheiten über das Internet zur Vertiefung und zur individuellen Auswahl. Dieses neue Angebot ist ein Versuch, mittels neuer Medien effizienter und individueller zu lernen.

Beginn: 27.10.1999
Zeit: Mittwochs, 11.30 - 13.00 Uhr
Ort: Seminarraum S34, Mathematikgebäude

Priv. Doz. Dr. Rüdiger Weiß, Tel. -4034,
E-Mail: Rüdiger.Weiss@rz.uni-karlsruhe.de.

Tutorium: Benutzung von DCE und DFS

Roland Laifer

Das Distributed Computing Environment (DCE) wird an der Universität und am Forschungszentrum Karlsruhe bereits auf über 400 Rechnern eingesetzt, darunter auch die 256 Knoten des Höchstleistungsrechners IBM RS/6000 SP.

Für die Benutzer ist die wichtigste Komponente des DCE das Distributed Filesystem (DFS). DCE/DFS wird derzeit auf der SP, im AB-Pool und im RZ-Pool als Filesystem für die Homedirectories eingesetzt. Darüber hinaus ist DFS auf einigen Dutzend Rechnern im Campus auf unterschiedlichen Betriebssystemen (HP-UX, Windows NT, Solaris, IRIX) installiert.

Das Rechenzentrum veranstaltet daher am 21. Oktober 1999 ein Tutorium zum Thema “Benutzung von DCE und DFS”.

Datum: 21.10.99
Zeit: 14.00 - 15.30 Uhr
Ort: RZ, Raum 217, 2. OG

Bei dieser Veranstaltung sollen Hinweise zum praktischen Arbeiten mit DCE und DFS gegeben werden; insofern richtet sich die Veranstaltung an alle Benutzer auf den oben genannten Rechnern. Im Idealfall sollten die Benutzer natürlich möglichst wenig von DCE und DFS bemerken, aber es gibt einige zusätzliche Kommandos, u.a. zur Abfrage der Disk-Quotas. Die Veranstaltung bietet zudem Hinweise und Vorführungen zum Arbeiten mit DFS auf verschiedenen Hardware-Plattformen, u.a. Windows NT. Desweiteren wird erklärt, wie über das sogenannte *DFS/NFS-Gateway* von NFS auf DFS zugegriffen werden kann.

Roland Laifer, Tel. -4861,
E-Mail: Laifer@rz.uni-karlsruhe.de.

Computer und Recht

Die digitale Signatur und ihre juristische Bedeutung

Rechtsanwalt Dr. Stefan Ernst, Freiburg/Br.

Im Zeitalter des Internet ist es ohne weiteres möglich, Bücher, Reisen oder andere Annehmlichkeiten online per Mausklick oder E-Mail zu bestellen. Dies ist rechtlich ebenso verbindlich wie eine Bestellung per Brief, Fax oder am Telefon. Praktische Probleme treten allerdings auf, wenn der Besteller davon nichts mehr wissen und die Rechnung nicht bezahlen will oder eine Bestellung unter falschem Namen abgibt. In diesen Fällen ist es Sache des Verkäufers, zu beweisen, dass der vermeintliche auch der tatsächliche Besteller ist. Kann er dies nicht, geht er leer aus.

Bei einer Bestellung per Brief ist der Beweis in der Regel recht einfach. Auch ein Fax wird meist vom Absender unterschrieben sein. Zumindest gibt es in diesen Bereichen zuverlässige Rechtsprechung zur Bewertung der Beweisqualität. Digitale Nachrichten aber

sind nur wenig vertrauenswürdig. Es ist oft nicht feststellbar, ob die Nachricht authentisch und ob der angegebene Absender auch der Verfasser ist.

Der folgende Beitrag setzt sich mit den Möglichkeiten auseinander, dennoch Verträge auf elektronischem Wege zu schließen - und dies auch zu beweisen.

I. Der Beweis vor Gericht

Vor Gericht stehen dem Kläger fünf Arten von Beweismitteln zur Verfügung:

- Zeugenvernehmung
- Parteivernehmung (Kläger/Beklagter selbst)
- Sachverständigengutachten
- Augenschein (der Richter schaut sich etwas an)
- Urkunden

Normale Briefe können sowohl als Augenscheinsobjekte als auch als Urkunden in Frage kommen. **Urkunden** sind sie unter zwei Voraussetzungen:

1. Sie müssen so **verkörpert** sein (im Normalfall auf Papier), dass eine Veränderung bemerkbar ist (es wurde radiert, durchgestrichen, weggeschnitten, nachträglich hinzugefügt etc.).
2. Sie müssen **unterschrieben** sein und dadurch hinreichend verlässlich auf den Aussteller hinweisen.

Die hervorragenden Funktionen einer Urkunde bestehen also in der Gewährleistung von

- **Authentizität** = der Aussteller ist der Unterzeichner (durch die Unterschrift) und
- **Integrität** = der Inhalt ist unverfälscht (durch die Verkörperung auf Papier).

Aus diesem Grunde besitzen Urkunden vor Gericht einen **erhöhten Beweiswert** (§§ 416, 440 Zivilprozessordnung (ZPO)):

> § 416 ZPO: Privaturkunden begründen, sofern sie von den Ausstellern unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind, vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind.

Andere Schriftstücke, z.B. Notizen, können zwar auch vor Gericht als Beweismittel vorgelegt werden. Sie unterliegen jedoch lediglich als **Augenscheinsobjekte** der freien richterlichen Beweiswürdigung (§ 286 ZPO) und besitzen keine in besonderem Maße erhöhte Beweiskraft. Hier obliegt es dem Richter, die Zuverlässigkeit des präsentierten Beweismittels zu prüfen und zu bewerten.

II. Der Beweiswert elektronischer Dokumente

Die Funktionen einer Urkunde sind bei einfachen elektronischen Dokumenten nicht gewährleistet. Elektronische Nachrichten können **verfälscht** werden, ohne dass man es ihnen hinterher ansehen könnte. Die Absenderangabe einer E-Mail kann verändert oder eine E-Mail mit einem falschen Absender verschickt werden, ohne dass dies für den Adressaten feststellbar wäre. Der Name, der im Absenderfeld angezeigt wird, wird vom Absender selbst willkürlich eingetragen. Damit **fehlt** es an **Authentizität**. Der Adressat hat keine Sicherheit hinsichtlich des wahren Absenders. Dies gilt erst recht für das Gericht, da auch der Adressat die Nachricht manipulieren kann.

Elektronische Urkunden sind zudem nicht auf Papier verkörpert, sondern in Dateien, die ebenfalls verändert werden können, ohne dass dies dem Außenstehenden deutlich wird. Damit **fehlt** es an der **Integrität**. Der Empfänger kann nicht sicher sein, ob die ihm vorliegende Nachricht auch in dieser Form vom Absender stammt. Darüber hinaus kann er sie selbst verändern und vor Gericht behaupten, er habe sie in der geänderten Variante erhalten.

Aus diesen Gründen sind elektronische Dokumente keine Urkunden im Sinne des § 416 ZPO, sondern lediglich Augenscheinsobjekte (§§ 371 ff. ZPO). Als solche aber kommt ihnen vor Gericht ein sehr **geringer Beweiswert** zu. Die Vorlage einer E-Mail mit der Bestellung eines Fitnessgerätes für DM 1.000,- wird nicht ausreichen, um den vermeintlichen Absender zur Zahlung zu verurteilen.

III. Die digitale Signatur

Erhöhte Aufmerksamkeit verdient daher die digitale Signatur. Bei diesem Verfahren wird durch eine Kombination von **privatem und öffentlichem Schlüssel** (Public Key System) eine Prüfsumme erstellt, die Authentizität und Integrität gewährleisten kann. Die Verwaltung dieser Schlüssel obliegt einer Zertifizierungsstelle (**Trust Center**). Sie teilt die individuellen und geheimzuhaltenden privaten Schlüssel zu. Der öffentliche Schlüssel dient nur der Entschlüsselung und ist allgemein zugänglich.

Das Signaturverfahren selbst trennt sich in zwei Schritte:

- **Signaturerzeugung** beim Absender (mit dem privaten Schlüssel)
- **Signaturprüfung** beim Adressaten (mit dem öffentlichen Schlüssel)

Die Signatur wird dabei bei ihrer Erzeugung auf Verlangen zu Beweiszwecken von der Zertifizierungsstelle mit einem **Zeitstempel** versehen. Eigentlich ist dies in den Fällen nicht erforderlich, in denen das signierte Dokument ein Datum enthält, das ja nach der Signatur nicht mehr verändert werden kann.

Es gibt eine Vielzahl von Systemen zur Erzeugung digitaler Signaturen mit unterschiedlicher Verlässlichkeit. Von der mathematischen Sicherheit des jeweiligen Verfahrens hängt auch der Wert der aus ihr resultierenden Signaturen ab.

IV. Das Signaturgesetz

Am 01.08.1997 trat im Rahmen des Informations- und Kommunikationsdienste-Gesetzes (sog. Multimediagesetz) das Gesetz zur digitalen Signatur (SigG) in Kraft. Ziel dieses Signaturgesetzes ist es, durch die Regelung eines technischen Verfahrens die Manipulationsmöglichkeiten an elektronischen Dokumenten zu minimieren. Eine digitale Signatur im Sinne des SigG wird definiert als

> "ein mit einem privatem Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines dazugehörigen öffentlichen Schlüssels, das mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle ... versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschbarkeit der Daten erkennen läßt" (§ 2 Abs. 1 SigG).

Es sollen Rahmenbedingungen geschaffen werden, unter denen digitale Signaturen als fälschungssicher gelten können (§ 1 Abs. 1 SigG). Andere Verfahren sollen zwar nicht verboten werden, doch wird nur bei Verwendung des im Gesetz beschriebenen Systems ein Zertifikat vergeben. Nur in diesem Fall wird gesetzlich vermutet, dass die Signaturen sicher sind.

SigG und Signaturverordnung (SigV) gewährleisten in der Tat einen hochgradigen Sicherheitsstandard bei der Feststellung von Integrität und Authentizität der nach ihrem Standard signierten Dokumente.

Inhaber eines Zertifikats können nur natürliche Personen sein (§ 2 II SigG). Juristische Personen können sich auch nicht durch natürliche vertreten lassen. Dreh- und Angelpunkt der vom SigG und der ergänzenden Signaturverordnung (SigV) definierten Sicherheitsinfrastruktur sind die Zertifizierungsstellen. Diese sollen die Verlässlichkeit der im Verkehr befindlichen Signaturen sicher stellen. Diese **Trust Center** werden selbst streng **kontrolliert.** Potentielle Zertifizierungsstellen müssen von der Regulierungsbehörde für Post und Telekommunikation (RegPT) **lizenziert** werden (§ 4 SigG). Daher müssen sie dieser erst einmal selbst ein entsprechendes Konzept vorlegen und nachweisen, dass ihr Verfahren sicher ist. Ein konkretes Verfahren selbst ist ihnen nämlich nicht vorgeschrieben.

Auch in der Europäischen Gesetzgebung hat die digitale Signatur inzwischen Berücksichtigung gefunden. Eine entsprechende **EU-Richtlinie** ist in Vorbereitung, die allerdings nicht mit einer, sondern mit zwei verschiedenen Formen der digitalen Signatur (Zweiklassensystem) operiert. Die einfache elektronische Form gewährleistet dabei nur die Integrität, die fortgeschrittene elektronische Form sowohl Integrität als auch Authentizität. Da das deutsche Signaturgesetz daneben weiter bestehen kann, wird dies letztlich dazu führen, dass in Zukunft womöglich vier verschiedene Formen digitaler Signaturen nebeneinander bestehen werden:

- die digitale Signatur im Sinne des Signaturgesetzes
- die einfache elektronische Signatur der EU-Richtlinie
- die fortgeschrittene elektronische Signatur der EU-Richtlinie
- alle übrigen Formen digitaler Signaturen (z.B. Pretty Good Privacy)

V. Digitale Signaturen vor Gericht

SigG und SigV regeln allerdings nur die technischen Anforderungen an die digitale Signatur. Gesetzliche Konsequenzen werden hieran nicht geknüpft. Daher stellt sich die Frage der Beweisqualität im Rahmen der oben genannten Normen. Es ist zu klären, ob ein Anwalt, der mit dem Notebook zum Gerichtstermin erscheint, das als beweisschwaches Augenscheinsobjekt zu qualifizierende einfache elektronische Element durch eine Signatur nach dem SigG aufgrund dieser hochgradigen Sicherheit in gesteigertem Maße verwerten kann. Dies ist zu bejahen. Eine digitale Signatur macht aus einem elektronischen Dokument zwar

noch **keine Urkunde** im Sinne der ZPO, doch steigert sie aufgrund der ihr innewohnenden Verlässlichkeit den Beweiswert des signierten Dokuments so stark, dass vor Gericht im Rahmen der **Augenscheinsprüfung** eine **Vermutung** für Urheber und Inhalt der Urkunde sprechen sollten. Obgleich in diesem Bereich noch keinerlei Rechtsprechung existiert, ist davon auszugehen, dass digital signierte Dokumente einen erheblich **gesteigerten Beweiswert** besitzen. Die rechtliche Qualität hängt dann im einzelnen vom jeweiligen Verfahren ab. So wird die einfache digitale Signatur der EU-Richtlinie weniger Beweiswert besitzen als diejenige nach dem SigG.

VI. Haftungsfragen

Die digitale Signatur bietet natürlich auch **Risiken**. Selbst wenn das Verfahren fälschungssicher sein sollte, ist die größte Schwachstelle wie immer der Anwender. Er mag seine PIN-Nummer für den privaten Schlüssel unbeaufsichtigt lassen oder gar an andere weitergeben. Aber auch mögliche Pflichtverletzungen von Zertifizierungsstellen sind rechtlich einzuordnen. Schließlich hat die signierte Willenserklärung erhebliche Auswirkungen auf das Verhalten Dritter. Durch das in sie gesetzte Vertrauen werden möglicherweise hohe Investitionen getätigt (Beispiel: Eine Firma liefert auf eine signierte elektronische Bestellung teure Waren aus, wird aber nicht bezahlt, weil die Signatur gefälscht war).

Nachlässiger Umgang mit dem privaten Schlüssel

Es mag vorkommen - ähnlich wie auch bei EC-Karten -, dass der Inhaber eines privaten Schlüssels seine Zugangsdaten zur Verschlüsselung unbeaufsichtigt und offen liegen läßt, obgleich er dazu verpflichtet ist, dieses stets für Dritte unzugänglich aufzubewahren. Führt dies zu unbefugter Schlüsselverwendung hat der Inhaber gleichwohl einen Vertrauenstatbestand geschaffen. Ist der Täter nicht ausfindig zu machen, haftet er für den entstandenen Schaden. Hat der Täter kein Geld, gilt Gleiches. Er kann eine vom Unberechtigten abgegebene Bestellung zwar anfechten - wenn er den Missbrauch beweisen kann -, muss aber die entstandenen Kosten tragen.

Vollmachtsüberschreitung

Der Fall, dass der Schlüsselinhaber einem Dritten gestattet, in seinem Namen Erklärungen abzugeben und digital zu signieren, dies aber intern auf bestimmte Geschäfte begrenzt, ist bei Überschreiten dieser Vollmacht genauso zu behandeln. Das Risiko eines Missbrauchs der Vertretungsmacht trägt dann grundsätzlich der Vertretene. Der vermeintlich berechtigte Vertreter haftet zwar persönlich, doch nützt das dem Vertretenen nicht viel, wenn er seinen Regressanspruch nicht realisieren kann. Der Vertretene haftet allerdings dann nicht, wenn der Vertragspartner wusste oder erkennen konnte, dass die Vollmacht überschritten wurde.

Diebstahl

Wurde der Schlüssel trotz hinreichender Absicherung (Beweis!) von einem Dritten erlangt – etwa durch Diebstahl oder Erpressung - haftet der Vertretene grundsätzlich nicht. Der geschädigte Vertragspartner muß sich an den Dieb halten.

Haftung der Zertifizierungsstellen

Schlampt die Zertifizierungsstelle bei der Vergabe von oder beim Umgang mit dem Schlüssel, haftet sie, wenn dem Schlüsselinhaber hierdurch ein Schaden entsteht. Vergeben Mitarbeiter bewusst falsche Zertifikate zu Betrugszwecken, so haften sie selbst zusammen mit demjenigen, der die Zertifikate im Rechtsverkehr benutzt für den entstandenen Schaden. Ob die Zertifizierungsstelle hierfür ebenfalls haftet, hängt vom Einzelfall ab.

VII. Formvorschriften

Für den Abschluss vieler Vertragsarten sieht das Gesetz zwingend eine bestimmte Form vor. Die digitale Signatur ist aber eben doch keine handschriftliche Unterzeichnung. So ist etwa ein Abonnementvertrag oder die Bürgschaft eines Verbrauchers nur wirksam, wenn sie **schriftlich** abgegeben wurde. Dieser Form kann auch durch eine **digitale Signatur nicht** genügt werden. Um hier eine Erleichterung zu schaffen, müssten die entsprechenden Formvorschriften gelockert werden. In Frage käme in manchen Fällen eine Erleichterung derart, dass eine einfache elektronische Erklärung zwar noch nicht, wohl aber eine digital signierte ausreichen würde ("**Textform**" bzw. "**elektronische Form**"). Deratige Pläne liegen bereits seit geraumer Zeit in den Schubladen des Gesetzgebers, sind aber noch in ihrer Ausgestaltung umstritten.

Die digitale Signatur sollte aber nicht überall als Substitut der Unterschrift gelten dürfen. Die gesetzli-

che Schriftform hat nicht selten in erster Linie Warnfunktion. Der Unterzeichner soll wissen, dass er eine Erklärung abgibt, die eine nicht unerhebliche Bedeutung besitzt und ihn womöglich weitreichend verpflichtet. Dieser Warnfunktion kann bei einer elektronischen Erklärung kaum genügt werden. Ob dies bei einer elektronischen Erklärung mit digitaler Signatur der Fall wäre, ist dem Einzelfall zu überlassen. Eine Bürgschaft sollte in keinem Fall elektronisch wirksam abzugeben sein. Eine Zeitschriftenabonnement online signiert zu bestellen, erscheint unproblematisch.

Vereinzelt wird auch zwischen Vertragsparteien **freiwillig** vereinbart, nur schriftliche Abmachungen oder Vertragsänderungen zu akzeptieren. Wird in diesem Fall eine Änderung nur per E-Mail angezeigt, sollte man eigentlich von einer Unwirksamkeit ausgehen. Allerdings ist eine solche gewillkürte Formvereinbarung auch - und sogar formlos - **aufhebbar**. Je nach Einzelfall kann es also sein, dass die Parteien das Schriftformerfordernis mündlich oder per E-Mail wieder aufgehoben haben. Dann kann eine - aus Sicherheitsgründen signierte - E-Mail auch für weitere Vereinbarungen genügen.

VIII. Fazit

Die digitale Signatur soll als eine Art Äquivalent zur Unterschrift dienen. Sie wird auch zu erheblich mehr Sicherheit im elektronischen Geschäftsverkehr führen. Gleichwohl ist die Gesetzgebung zur digitalen Signatur - sowohl Signaturgesetz als auch Signaturrichtlinie - als gesetzgeberischer Akt eigentlich nur bedingt nützlich, da sie in rechtlicher Hinsicht keine wirklichen Veränderungen trifft. Die rechtliche **Einordnung** von digitalen Signaturen wird auch in der Zukunft allein **durch die Gerichte** erfolgen, die die Einordnung der verschiedenen Formen der digitalen Signatur in das System der ZPO vorzunehmen haben. Diese Einordnung wird von der tatsächlichen **Verlässlichkeit** des jeweils vom Absender verwendeten Signaturverfahrens abhängen. Aufgrund der besonderen Qualität des SigG ist insoweit von einem hohen Sicherheitsgrad auszugehen. Es sei jedoch vor zu viel Optimismus gewarnt. Wer zum gegenwärtigen Zeitpunkt tatsächlich mit dem Notebook vor Gericht auftauchen will, muß mit viel Unverständnis beim Richter rechnen. Es ist nicht auszuschließen, dass ein Richter zunächst einen Sachverständigen beauftragen würde, was das Verfahren verzögert und verteuert. Wer sich auf die Zuverlässigkeit seines Gegenüber nicht verlassen will, sollte also in Zukunft vielleicht doch noch auf eine schriftliche Bestätigung mit der “gelben” Post bestehen.

Personalia

Prof. Juling Mitglied der Kommission für Rechenanlagen der DFG

(red)

Prof. Dr. Wilfried Juling, Leiter des Universitätsrechenzentrums, wurde vom Hauptausschuss der Deutschen Forschungsgemeinschaft mit sofortiger Wirkung als Mitglied in die Kommission für Rechenanlagen gewählt.

Die Kommission für Rechenanlagen berät den Hauptausschuss der DFG in wichtigen technischen und grundsätzlichen Fragen, die sich im Zusammenhang mit DV-Anlagen in den Förderungsverfahren der Deutschen Forschungsgemeinschaft ergeben. Die Kommission gibt darüber hinaus für die Forschungsgemeinschaft die Stellungnahmen ab zu den Anmeldungen von Rechnern und Rechnersystemen im Rahmen des Finanzierungsverfahrens nach dem Hochschulbauförderungsgesetz (HBFG).

Vorträge, Workshops und Kurse
auf einen Blick

Mikroelektronik:
Treffen der EUROPRACTICE-Anwender

Neue Software-Angebote, neue Technologien für die IC-Fertigung, Software für den MEMS-Entwurf (Mikro-Elektro-Mechanische Systeme).

Dieter Kruk

Datum: Do., 28.10.1999
Zeit: 16.15 - 17.00 Uhr
Ort: RZ, Raum 217, 2. OG

DCE und DFS

Roland Laifer

Datum: 21.10.99
Zeit: 14.00 - 15.30 Uhr
Ort: RZ, Raum 217, 2. OG

Einführungsveranstaltungen zu JAVA und UNIX-Werkzeugen

Harald Meyer

Alle Veranstaltungen finden im RZ-Gebäude (20.21) im Raum 217 (2.OG) statt.

Weitere Informationen finden Sie im Web unter `http://www.rz.uni-karlsruhe.de/~Harald.Meyer/veranstaltungen.html`

Java-Veranstaltungen:

- Semesterbegleitende Einführung in die Programmiersprache Java und das Java Development Kit (Version 1.1 und 1.2)
  Beginn: mittwochs, 27.10.1999
  Zeit: 14.00 Uhr - 15.30 Uhr

- Datenbankanbindung in Java mit dem Paket "Java Database Connectivity" (JDBC)
  Teil 1
  Datum: Donnerstag, 11.11.1999
  Zeit: 14.00 Uhr - 15.30 Uhr
  Teil 2
  Datum: Donnerstag, 18.11.1999
  Zeit: 14.00 Uhr - 15.30 Uhr

- Einführung in Swing / Java Foundation Classes (Aufbau grafischer Benutzeroberflächen)
  Teil 1
  Datum: Donnerstag, 2.12.1999
  Zeit: 14.00 Uhr - 15.30 Uhr
  Teil 2
  Datum: Donnerstag, 9.12.1999
  Zeit: 14.00 Uhr - 15.30 Uhr

- Dynamische Webseitenerstellung mit dem Element Construction Set aus dem Apache-Projekt
  Datum: Donnerstag, 13.1.2000
  Zeit: 14.00 Uhr - 15.30 Uhr

- Einführung in das Java Servlet Development Kit (mit Apache JServ)
  Datum: Donnerstag, 27.1.2000 und Donnerstag, 3.2.2000
  Zeit: jeweils 14.00 Uhr - 15.30 Uhr

Allgemeine UNIX-Tools

- Übersetzen und Binden von Programmen unter UNIX
  Datum: Donnerstag, 11.11.1999
  Zeit: 16.00 Uhr - 17.30 Uhr

- Kompressions- und Archivierungswerkzeuge unter UNIX
  Datentransfer mit der Windows-95/NT-Welt
  Datum: Donnerstag, 18.11.1999
  Zeit: 16.00 Uhr - 17.30 Uhr

- Einführung in Make
  Datum: Donnerstag, 25.11.1999
  Zeit: 14.00 Uhr - 15.30 Uhr

- Einführung in Perl
  Teil 1
  Datum: Donnerstag, 2.12.1999
  Zeit: 16.00 Uhr - 17.30 Uhr
  Teil 2
  Datum: Donnerstag, 9.12.1999
  Zeit: 16.00 Uhr - 17.30 Uhr

- Einführung in das Revision Control System (RCS)
  Datum: Donnerstag, 13.01.2000
  Zeit: 16.00 Uhr - 17.30 Uhr

Erste Ansprechpartner
auf einen Blick

So erreichen Sie uns

Telefonvorwahl: +49 721/608-
Fax: +49 721/32550
E-Mail: Vorname.Nachname@rz.uni-karlsruhe.de

BIT8000 (Help Desk)	Tel. -8000, E-Mail: BIT8000@rz.uni-karlsruhe.de
Sekretariat	Tel. -3754, E-Mail: rz@uni-karlsruhe.de
Information	Tel. -4865, E-Mail: info@rz.uni-karlsruhe.de
MicroBIT-Hotline	Tel. -2997, E-Mail: microbit@rz.uni-karlsruhe.de
Anwendungen	Tel. -4031/4035, E-Mail: anwendung@rz.uni-karlsruhe.de
Netze	Tel. -2068/4030, E-Mail: netze@rz.uni-karlsruhe.de
UNIX	Tel. -4038/4039, E-Mail: unix@rz.uni-karlsruhe.de
Virus-Zentrum	Tel. 0721/9620122, E-Mail: virus@rz.uni-karlsruhe.de
ASKnet GmbH (SW-Lizenzen)	Tel. 0721/964580, E-Mail: info@asknet.de
Zertifizierungsstelle (CA)	Tel. -7705, E-Mail: ca@uni-karlsruhe.de
PGP-Fingerprint	pub 1024/A70087D1 1999/01/21 CA Universität Karlsruhe 7A 27 96 52 D9 A8 C4 D4 36 B7 32 32 46 59 F5 BE
Mailing-Liste für Internetmissbrauch	abuse@uni-karlsruhe.de

Öffentliche Rechnerzugänge

World Wide Web:
http://www.rz.uni-karlsruhe.de/ (Informationssystem des Rechenzentrums der Universität Karlsruhe)
http://www.uni-karlsruhe.de/Uni/CA/ (Zertifizierungsstelle am Rechenzentrum der Universität Karlsruhe)
http://www.ask.uni-karlsruhe.de (Informationssystem der Akademischen Software Kooperation ASK)

Ftp:
ftp.rz.uni-karlsruhe.de; Benutzernummer: ftp (anonymer Ftp-Server des Rechenzentrums)
ftp.ask.uni-karlsruhe.de; Benutzernummer: ftp (anonymer Ftp-Server der ASK)