



Gemeinsame Arbeitskonferenz: GI • OCG • BITKOM • SI • TeleTrust

D·A·CH SECURITY

Bestandsaufnahme und Perspektiven

Universität Erfurt • 25. und 26. März 2003

Programmkomitee

P. Horster Uni Klagenfurt (Vorsitz) • **J. Bizer** Uni Frankfurt • **J. Buchmann** TU Darmstadt
C. Busch FhG-IGD • **H.C. Capellaro** Ernst & Young D • **J. Dittmann** Uni Magdeburg • **C. Eckert** TU Darmstadt
B. Esslinger Deutsche Bank • **H. Federrath** FU Berlin • **D. Fox** Secorvo • **R. Haefelfinger** FI FGSec
M. Hortmann Uni Bremen • **D. Jäpel** IBM CH • **W. Kühnhauser** Uni Ilmenau • **P. Kraaibeek** secunet
M. Lutherdt Uni Erfurt • **I. Münch** BSI • **J. Nedon** ConSecur • **S. Paulus** SAP • **G. Pernul** Uni Regensburg
N. Pohlmann Utimaco • **R. Posch** TU Graz • **K. Rannenberg** Uni Frankfurt • **H. Reimer** TeleTrust
A. Roßnagel Uni GH Kassel • **C. Ruland** Uni GH Siegen • **P. Schartner** Uni Klagenfurt
J. Swoboda TU München • **S. Teiwes** Ernst & Young CH • **S. Teufel** Uni Fribourg • **G. Weck** Infodas
M. Welsch IBM D • **P. Wohlmacher** RegTP • **K.-D. Wolfenstetter** T-Nova

Organisation

H. Reimer TeleTrust • **M. Lutherdt** Uni Erfurt • **P. Kraaibeek** secunet • **D. Cechak** Uni Klagenfurt

Aktuelle Informationen: <http://syssec.uni-klu.ac.at/DACH2003/>



Microsoft



secunet





Dienstag • 25. März 2003

08.30 Uhr Registrierung, Kaffee und Tee

09.25 Uhr Begrüßung und Überblick • H. Reimer, P. Horster

Einführung • Leitung: P. Horster

09.35 Uhr TeleTrust – IT-Sicherheit als interdisziplinäre Aufgabe

- Elektronischer Rechtsverkehr
- Standardisierung
- Chipkarten und PSE
- Interoperabilität
- ISIS-MTT und Bridge CA

H. Reimer
TeleTrust

10.00 Uhr IT-Sicherheit – Quo Vadis?

- Vertrauenswürdige Geschäftsprozesse im Internet?
- Erfolg durch garantierte Verfügbarkeit
- Sicherheit – Schutz und Zuverlässigkeit
- Bewusstsein wecken: Eine gesellschaftliche Aufgabe
- Machen Sie mit: Sicherheit in der Gesellschaft für Informatik

M. Reitenspieß
Fujitsu-Siemens AG
GI-Fachbereich
Sicherheit

10.25 Uhr Entstehungsgeschichte des IT-Grundschutzhandbuchs

- IT-Sicherheitshandbuch und wie weiter?
- Konzeptionierung IT-Grundschutzhandbuch
- IT-Grundschutzhandbuch in der Praxis
- IT-Grundschutz-Zertifikat
- Zukünftige Entwicklungen

I. Münch
BSI

10.50 Uhr Kommunikationspause

Sicherheitsvorfälle • Leitung: H. Reimer

11.20 Uhr Ein Integrationsmodell für das IT-Krisenmanagement

- Spezialisiertes IT Incident Handling
- Allgemeines Krisenmanagement
- Auseinanderdriften der Fachgebiete
- IT als Sonderfall
- Integrationsmodell

R. v. Rössing
Ernst & Young
Österreich

11.45 Uhr Analytische Überlegungen zur Kalibrierung von IDS

- Kalibrierung als Kriterium für einen sinnvollen IDS-Einsatz
- Minimierung der Anzahl übersehener Angriffe
- Berücksichtigung begrenzter personeller Ressourcen
- Betrachtung von Szenarien mit unterschiedlicher Angriffslast
- Ableitung einer Kalibrierungsstrategie

A. Scheerhorn
J. Nedon
ConSecur GmbH

12.10 Uhr Netzwerk Forensik: Monitoring und Visualisierung von Vorfällen

- Finetuning der Security Assets durch Monitoring und Analyse
- Monitoring und Network Forensik
- Profiling von Objekten in Netzwerken
- Visualisierung von Logfiles aller Art, eine zeitsparende Methode
- Korrelation von Daten zur Aufdeckung von Schwachstellen

A. Wagner
Silent Runner

12.35 Uhr Gemeinsame Mittagspause

Wirtschaft und Signaturen • Leitung: H. Federrath

A

13.35 Uhr Geschäftsrisiken von gläsernen Unternehmen

- Problem des gläsernen Unternehmens
- Indikatoren zum Informationsverlust
- Ansätze für Schutzmaßnahmen
- Self-Assessment als vorbeugende Maßnahme
- Praxisbeispiele

R. Rues
University of
Leicester
P. Kunz
Daimler-Crysler AG

14.00 Uhr Umsetzung der digitalen Signatur in der deutschen Wirtschaft

- Bedeutung des elektronischen Datenaustausches für die Wirtschaft
- Wo ist die Signatur im B2B-Datenaustausch relevant?
- Elektronische Rechnungsstellung: EU vs. Deutschland
- Umsetzung in EDI-Prozesse
- Wo gibt es noch Hindernisse?

K. Förderer
Centrale für
Coorganisation

Dienstag • 25. März 2003

14.25 Uhr **Trusted Signature Terminal – Vertrauenswürdige Signierumgebung**

- Rechtsverbindliche elektronische Signaturen
- Zurechenbarkeit elektronischer Signaturen zu Personen
- Vertrauenswürdige Signierumgebung
- Signaturkarte
- Biometrisches On-Card-Matching

O. Henniger
B. Struif
K. Franke
R. Ulrich
Fraunhofer-Institute

Digitale Wasserzeichen • Leitung: I. Münch

B

13.35 Uhr **Das Signatursiegel-Verfahren**

- Integrität: Technische und rechtliche Aspekte
- Kombination von Wasserzeichen und Signaturen
- Rechtsgültiger Ausdruck elektronischer Dokumente
- Stufenkonzept für die Einführung elektronischer Geschäftsprozesse
- Praxisbeispiele – IT-Sicherheit, die sich rechnet

R. Krüger
Mediasec
Technologies GmbH

14.00 Uhr **Neue Perspektiven zur Manipulationserkennung in digitalen Medien**

- Invertierbare digitale Wasserzeichen
- Kombination mit elektronischen Signaturen
- Schutz der Reproduktion des Originals
- Applikationen für den Hochsicherheitsbereich und die Archivierung
- Algorithmus für Bild- und Audiodaten

J. Dittmann
P. Pharow
Uni Magdeburg
M. Steinebach
Fraunhofer IPSI

14.25 Uhr **Universelle Parameterübergabe für digitale Wasserzeichen**

- Anpassung digitaler Wasserzeichen an Anwendungsszenarien
- Parameterlisten sind für Anwender schwer verständlich
- Konzept zur Parametrisierung digitaler Wasserzeichen
- Übersetzung von Anwenderanfragen in spezifische Parameterlisten
- Beispielanwendung

M. Steinebach
Fraunhofer IPSI
J. Dittmann
Uni Magdeburg

14.50 Uhr **Kommunikationspause**

Signaturanwendungen und eGovernment • Leitung: S. Teiwes

A

15.20 Uhr **All Sign und virtuelles Bauamt**

- Massen Anwendungen für die elektronische Signatur
- Die Funktionalitäten
- Wertschöpfung durch Vernetzung
- Organisatorische, juristische und technische Machbarkeit
- Standardisierung und Übertragbarkeit

A. Kraft
K. Rößler
Projekt MediaKomm
Esslingen

15.45 Uhr **eGovernment mit elektronischer Signatur im Land Berlin**

- Erfahrungsbericht
- Interaktion zwischen Geschäfts- und Verwaltungspartner
- Elektronisch signierte Verfahrensschritte im Bauantragsverfahren
- Mehrwert
- Nächste Schritte

B. Götz

16.10 Uhr **Zustellung im eGovernment**

- Business Case für die elektronische Zustellung
- Rechtliche und organisatorische Anforderungen
- Modell der elektronischen Hinterlegung, Vor- und Nachteile
- Schnittstellen, Authentifikation, Verschlüsselung, Datenschutz
- Stand der Arbeiten in Österreich und international, Ausblick

A. Hollosi
P. Reichsstädter
BMöLS
Stabsstelle
IKT-Strategie
des Bundes

16.35 Uhr **Digitale Signaturen im elektronischen Materialzeugniswesen**

- Elektronische Materialzeugnisse
- Intermediärer Austausch elektronischer Materialzeugnisse
- Relevante Bedrohungen
- Digitale Signaturen als wichtiger Erfolgsfaktor
- Sicherheitskonzept für den Austausch der Materialzeugnisse

P. Laing
RWTH Aachen
N. Pohlmann
Utimaco
Safeware AG

Infrastrukturen und Management • Leitung: C. Eckert

B

- 15.20 Uhr Benutzerbezogenes Sicherheitsmanagement – Standortbestimmung**
- Ganzheitliches Sicherheitsmanagement
 - Rollenbasierte Zugriffskontrolle
 - Identity Management
 - Security Provisioning
 - Automatisierte Benutzeradministration
- 15.45 Uhr Benutzer- und Berechtigungsmanagement**
- Entwicklung der Berechtigungsmodelle
 - Stand und Entwicklung des Benutzer- und Berechtigungsmanagements
 - Konzeption und Technik
 - Probleme des Ausbaus aktueller Rollenmodelle
 - Integration in bestehende Infrastruktur-Systeme
- 16.10 Uhr Sicherheitsimplikationen einer serverorientierten PKI**
- Client-Server Modell für PKI
 - Sicherheit von zentralisierten PKI Diensten
 - Delegieren kryptografischer Operationen
 - Aufbau sicherer Kommunikationskanäle
 - Betrachtungen zur Serversicherheit
- 16.35 Uhr Sind Linkzertifikate ein Ausweg aus der Zertifikatsflut?**
- Personengebundene Zertifikate
 - Problem von Attributen bzw. Zertifikaten auf Zeit
 - Open Mobile Access Network (OMAN)
 - Struktur von Linkzertifikaten im OMAN-Modell
 - Sind Linkzertifikate der Ausweg?
- A. Kern**
M. Kuhlmann
Systor GmbH&Co KG
- R. Holtkämper**
U. Tipp
M. Vogel
secunet AG
- B. Filipović**
Fraunhofer SIT
- S. Wappler**
Noventum
Consulting

Perspektiven • Moderation: P. Horster

- 17.15 Uhr Trustworthy Computing – Die neue Microsoft Sicherheitsstrategie**
- Sicherheit als globale Herausforderung für alle IT-Hersteller
 - Vernetzung und Sicherheit erfordern ganzheitliches Denken
 - Wege zu besserer Produktqualität und Sicherheit
 - Umgang mit Sicherheitslücken bei Standardsoftware
 - Ausblick: Hardwarebasiertes Sicherheitskonzept (Palladium)
- Gerold Hübner**
Microsoft GmbH

19.30 Uhr Gemeinsames Abendessen

... als Referenten haben sich zusätzlich zur Verfügung gestellt:

- Datenschutz im Gesundheitswesen – Ausgewählte Aspekte**
- Datenschutzgrundsätze für das Gesundheitswesen
 - Die Rechte der Betroffenen (Patienten und Mediziner)
 - Datensicherheitsmechanismen
 - Elektronische Archive und digitale Patientenakte
 - Gesundheitskarte und Gesundheitspass
- P. Pharow**
B. Blobel
Uni Magdeburg
- Steganographisches Illustrieren: Neue Perspektiven für Try & Buy**
- Steganographie zur Interaktion mit Bildern
 - Semantische Auszeichnung von Objekten im Bild
 - Textuelle Annotationen zu Objekten im Bild
 - Geschäftsmodelle auf Basis digitaler Wasserzeichen
 - Try&Buy-Angebote
- J. Dittmann**
K. Hartmann
H. Sonnet
F. Ritter
T. Strothotte
Uni Magdeburg
- Netzwerksicherheit mit SAP-Rollen**
- LDAP basierte Benutzer- und Rollenverwaltung
 - Verbindung von Netzwerk- und Applikationssicherheit
 - Sicherheit für eBusiness-Prozesse
 - IEEE 802.1X – Port based Network Access Control
 - UPN – User Personalized Network
- G. Schneider**
SecurIntegration GmbH
- Standardisierung auf dem Gebiet der IT-Sicherheit**
- Standardisierung zur IT-Sicherheit und angrenzender Bereiche
 - Projekte und Standards zur IT-Sicherheit
 - Identifikationskarten und Personenidentifikation
 - Biometrische Verfahren und Anwendungen für Identifikation und Authentifizierung
 - Möglichkeiten zur Mitwirkung
- I. Wende**
DIN
Deutsches Institut für Normung e. V.
- Die Beiträge dieser Referenten finden Sie auch im Tagungsband.**

Mittwoch • 26. März 2003

Sicherheitsmanagement • Leitung: D. Fox

A

09.00 Uhr Sicherer IT-Betrieb: Ganzheitliches Sicherheitsmanagement

- Externe Anforderungen an IT der Finanzdienstleister
- Relevante nationale und internationale Standards
- Einheitliche Betrachtung von IT-Sicherheit und IT-Betrieb
- Zielgruppen des Rahmenwerkes Sicherer IT-Betrieb
- Praktische Erfahrungen aus der Umsetzung

M. Jurečić

D. Bartl
SIZ

09.25 Uhr Unternehmenssicherheit bei T-Systems International

- Unternehmenssicherheit versus IT-Sicherheit
- Prozesse, Standards, Maßnahmen
- Organisation im Management, Umsetzungsaspekte
- Kommunikation, Eskalation, Reporting
- Bedeutung für T-Systems, Kunden und Mitarbeiter

K. Hinterland

T-Systems
International GmbH

09.50 Uhr Effizientes IT-Sicherheitsmanagement – Controlling-orientiert

- IT-Sicherheitsmanagement
- Formale Definition des Begriffs Risiko
- Betriebswirtschaftliche Betrachtung von Risiken
- Controlling-orientiertes Sicherheitsmanagement
- Vorteile und Grenzen des Ansatzes

J. Bachinger

Hewlett-Packard
GmbH

10.15 Uhr Sicherheitsanalysen als Bestandteil der Unternehmensphilosophie

- Bewusstseinsbildung für Sicherheitsmaßnahmen in Unternehmen
- Start eines kontinuierlichen Verbesserungsprozesses
- Vorstellung und Einsatz der SecuQuest Methodik
- Das Konzept des Self-Assessments
- Benchmarking (intern/extern)

C. Kollmitzer

ARC Seibersdorf
M. Malle
M. Stimpfl
MPS consult

Sicherheits- und Signaturmechanismen • Leitung: N. Pohlmann

B

09.00 Uhr ReEncryption – Konzept für den umfassenden Datenschutz

- Sicherheit in geschlossenen Nutzergruppen
- Dokumentenzentrierte Sicherheitsmechanismen
- Digitale Wasserzeichen
- Betriebssystem-Ergänzungsmechanismen
- Verteilte Sicherheitsarchitekturen

S.D. Wolthusen

Fraunhofer IGD
F. Prediger
ReEncryption
Development GmbH

09.25 Uhr Erhalt der Beweiskraft elektronischer Signaturen durch Neusignatur

- Verfahren zur Neusignierung
- Zeiträume, die Neusignaturen erfordern
- Gesammeltes Neusignieren vieler Dokumente
- Neusignatur allein mit einem Zeitstempel
- Verwendung zweier verschiedener Hash-Algorithmen

R. Schneider

TÜV-Informationstechnik GmbH

09.50 Uhr Aspekte der Massensignatur

- Rechtliche Aspekte der Massensignatur
- Signaturgesetz
- Anwendungsgesetze (§14 UStG, §36 SRVwV)
- Sicherheitsaspekte
- Hashketten und Stapelsignaturen

D. Hühnlein

Y. Knosowski
secunet AG

10.15 Uhr Analyse moderner Mixschemata in offenen Umgebungen

- Eigenschaften moderner Mixschemata
- Sicherheitsanforderungen
- Sicherheitsbetrachtung bezüglich aktiver Angriffe
- Praktische Einsetzbarkeit verschiedener Schemata
- Probleme in offenen Umgebungen

O. Berthold

FU Berlin

10.40-Uhr Kommunikationspause

Einsatz biometrischer Verfahren • Leitung: J. Dittmann

A

11.10 Uhr Integration biometrischer Verfahren in Sicherheitsinfrastrukturen

- Biometrie und IT-Sicherheit
- Wie sicher sind biometrische Verfahren?
- Biometriegestützte Authentifikation
- Aktivierung der elektronischen Signatur
- Erfahrungen aus der Praxis

N. Pohlmann
Utimaco
Safeware AG

11.35 Uhr Schutz biometrischer Daten zur Authentisierung auf Smartcards

- Smartcards mit Sicherheitsfunktionen und sensitiven Daten
- Benutzer-Authentisierung alternativ mit PIN oder Biometrie
- Problem der Öffentlichkeit biometrischer Daten
- Sicherheitskonzept für die Authentizität biometrischer Daten
- Mögliche Anwendung in Signaturumgebungen

U. Waldmann
D. Scheuermann
C. Eckert
Fraunhofer SIT

12.00 Uhr Handschriftliche biometrische Signaturen

- Biometrie in elektronischen Signaturen
- Funktionen von Handschrift und Unterschrift
- Strukturelle Modelle
- Heutige Ansätze und Perspektiven
- Problemfelder

C. Vielhauer
R. Steinmetz
TU Darmstadt

Anwendungen und Infrastrukturen • Leitung: S. Paulus

B

11.10 Uhr Sicherheitskonzept einer universitären Prüfungsverwaltung

- Risiken und Sicherheitsanforderungen
- Sicherheitspolitik und Sicherheitsarchitektur
- Angewandte Public-Key-Infrastrukturen
- Sicherheitstoken und Chipkarten
- Internetzugang zu sensiblen Daten

W. Kühnhauser
T. Pomierski
TU Ilmenau

11.35 Uhr Mobile Universität – Realisierung an der Universität Gießen

- Eine wahrlich multifunktionale Karte
- Warum eine eigene CA?
- Anwendungen für eine mobile Universität
- Entwicklungsprojekt mit großer Flexibilität
- Weitere Planungen

F. Ziemke
InterCard GmbH

12.00 Uhr Privilege Management und Zugriffskontrolle im Gesundheitswesen

- Verteilte Gesundheitsinformationssysteme
- Zugangs- und Zugriffskontrolle
- Verwaltung der Privilegien und Rechte
- Authentifikationsmechanismen und Policies
- Sicherheitsobjekte und ihre Klassifikation

B. Blobel
P. Pharow
Uni Magdeburg
R. Nordberg
Sahlgrens University
Hospital, Göteborg

12.25 Uhr Gemeinsame Mittagspause

Mobile IT-Geräte • Leitung: W. Kühnhauser

13.25 Uhr Einsatz von mobiler Kommunikation in der Speditionslogistik

- Problemfeldbetrachtung in der Speditionslogistik
- Anwendungsszenario
- Architektur eines Kommunikationssystems
- Aspekte einer mobilen Kommunikation
- Praxisbeispiel

V. Gruhn
M. Hülder
Uni Leipzig
L. Schöpe
Informatik Centrum
Dortmund e.V.

13.50 Uhr Subscriptionless Mobile Networking

- Registrierungslose Nutzung von Diensten mit mobilen Clients
- Potenzielle Gefahren für die informationelle Selbstbestimmung
- Bluetooth und Personal Area Networking
- Identitätsmanagement und Security Association Management
- Implementierung in Linux und Open Source

M. Schmidt
Uni Siegen

14.15 Uhr Sind mobile Endgeräte als Personal Trusted Devices geeignet?

- Personal Trusted Devices als mobile sichere Endgeräte
- Sicherheitsanforderungen an PTDs und Begriffsbestimmung
- Existierende mobile persönliche Endgeräte
- Analyse und Kritik existierender Systeme
- Entwicklungen hin zu echten PTDs

H. Görl
A. Buchmann
S. Lachmund
TU München

14.40 Uhr Kommunikationspause

Rechtliche Aspekte • Leitung: P. Kraaibeek

15.10 Uhr eBilling rechtskonform – Ein ganzheitlicher Ansatz

- Rechtslage in Deutschland und Österreich
- Notwendige technische Maßnahmen
- Nachweisbare Zustellung
- Ganzheitlicher Lösungsansatz
- Kostenanalyse

G. Lindsberger

G. Pinter

XiCrypt

Technologies GmbH

15.35 Uhr Informationspflichten und rechtsverbindliche Kommunikation

- Vertragsarten im Fernhandel
- Anforderungen an die Ausgestaltung des Vertragsabschlusses
- Notwendige Produktinformationen bei Online-Angeboten
- Ausübung und Folgen des Widerrufsrechts für Verbraucher
- Einfluss von Sicherheitskomponenten

R.M. Straub

Ernst & Young AG

Schweiz

16.00 Uhr Kryptographierechtliche Aspekte globaler Unternehmenskommunikation

- Vertraulichkeit versus staatlicher Sicherheit
- Export-, Import- und Domestic-Controls
- Rechtsquellen des Kryptographierechts
- Beispiele staatlicher Kontrollsysteme
- Konsequenzen für die IT-Sicherheit im Unternehmen

J. Tröber

Rechtsanwälte

Dr. Schmitz

und Kollegen

16.25 Uhr Konferenzende

Partner der Konferenz:



SAP AG

SAP ist führender Anbieter von eBusiness-Softwarelösungen. Die effiziente Absicherung von Transaktionen und der Aufbau zuverlässiger Vertrauensbeziehungen gehören dabei zu den Grundvoraussetzungen. Mit spezialisierten Partnern werden umfassende und individuell auf die Anforderungen des einzelnen Unternehmens abgestimmte Sicherheitslösungen entwickelt.

www.sap.com/technology



eBusiness Institut

Als gemeinsame Einrichtung von Unternehmen und der Universität Klagenfurt entwickeln und adaptieren wir Geschäftsmodelle für die verschiedenen Formen des eBusiness. Wir bieten projektorientierte angewandte Forschung, Beratung und Wissenstransfer in den Bereichen Customer Relationship Management, Knowledge Management und IT Security.

www.biztec.org



secunet Security Networks AG

secunet ist ein führender europäischer Dienstleister auf dem Gebiet hochkomplexer IT-Sicherheitssysteme. Das Unternehmen ist herstellernerutral und bietet mit 200 Mitarbeitern die komplette Leistungsbandbreite der IT Security an. Kunden erhalten Beratung, Implementierung, Schulung und Service aus einer Hand.

www.secunet.com



secure-it.nrw.2005

Die Landesinitiative für mehr Sicherheit und Vertrauen in elektronische Geschäftsprozesse hat das Ziel, innovative Geschäftsprozesse auszubauen und zu fördern. Die Aktivitäten umfassen die Förderung der IT-Sicherheit und der Akzeptanz elektronischer Geschäftsprozesse unter Erschließung innovativer Wachstumsfelder.

www.secure-it.nrw.de



Microsoft GmbH

Microsoft hat mit der „Trustworthy Computing Initiative“ das Thema Sicherheit im umfassenden Sinne zur obersten Priorität des Unternehmens gemacht. Mit dieser Initiative beabsichtigt Microsoft Produkte zu entwickeln und anzubieten, die bezüglich Sicherheit, Schutz der Privatsphäre und Zuverlässigkeit zum Referenzpunkt für die gesamte Industrie werden.

www.microsoft.com



Anmeldung & Teilnahmebedingungen

D•A•CH Security 2003

25. und 26. März 2003

Universität Erfurt



via Fax an: ++49 (0)5921-722-493

oder Online-Formular unter: <http://syssec.uni-klu.ac.at/DACH2003/html/anmeldung.html>
oder an:

Organisationskomitee D•A•CH Security

Peter Kraaibeek

Bogenstr. 5a

D-48529 Nordhorn

Telefon: ++49 (0)5921-722-490

eMail: Peter@Kraaibeek.com

Anmeldung zur Konferenz

.....
Name

.....
Firma

.....
Funktion

.....
Straße

.....
PLZ/Ort

.....
Tel.-Nr.

.....
Fax-Nr.

.....
eMail

- Hiermit melde ich mich verbindlich zur Arbeitskonferenz D•A•CH Security 2003 am 25. und 26. März 2003 an der Universität Erfurt an.
- Ich bin damit einverstanden, in die Teilnehmerliste (Name, Firma, Ort) aufgenommen zu werden.
- Ich kann an der Tagung nicht teilnehmen, bestelle aber ein Exemplar des Tagungsbandes zum Preis von € 59,- (inkl. MwSt.)

Teilnahmebedingungen

Bei Anmeldung bis zum 10. Februar 2003 beträgt die Teilnahmegebühr € 275 (Frühanmeldegebühr), anschließend € 310, jeweils zuzüglich der gesetzlichen MwSt.

Die Teilnahmegebühr beinhaltet ein Exemplar des Tagungsbandes, Pausengetränke, Mittagessen an beiden Konferenztagen und ein gemeinsames Abendessen am 25. März 2003.

Bei Stornierung der Anmeldung bis 3. März 2003 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75 (inkl. MwSt.) erhoben. Nach dem 3. März 2003 ist die volle Tagungsgebühr zu entrichten. Es ist jederzeit die Benennung einer Ersatzperson ohne zusätzliche Kosten möglich.

Die Teilnahmegebühr überweise ich sofort nach Erhalt der Anmeldebestätigung und Rechnung unter Angabe der Rechnungsnummer auf das Tagungskonto.

.....
Ort und Datum

.....
Unterschrift