

Sachar Paulus
Norbert Pohlmann
Helmut Reimer

**ISSE 2004 –
Securing Electronic Business Processes**

The Efficiency of Theorem Proving Strategies

by David A. Plaisted and Yunshan Zhu

Applied Pattern Recognition

by Dietrich W. R. Paulus and Joachim Hornegger

SAP® R/3® Interfacing using BAPIs

by Gerd Moser

Scalable Search in Computer Chess

by Ernst A. Heinz

The SAP® R/3® Guide to EDI and Interfaces

by Axel Angeli, Ulrich Streit and Robi Gonfalonieri

**Optimising Business Performance
with Standard Software Systems**

by Heinz-Dieter Knöll, Lukas W. H. Kühl,
Roland W. A. Kühl and Robert Moreton

ASP – Application Service Providing

by SCN Education B.V.

Customer Relationship Management

by SCN Education B.V.

Data Warehousing

by SCN Education B.V.

Electronic Banking

by SCN Education B.V.

Mobile Networking with WAP

by SCN Education B.V.

Efficient eReporting with SAP EC®

by Andreas H. Schuler and Andreas Pfeifer

Interactive Broadband Media

by Nikolas Mohr and Gerhard P. Thomas

Sales and Distribution with SAP®

by Gerhard Oberriedermaier and Tamara Sell-Jander

Efficient SAP R/3-Data Archiving

by Markus Korschen

Computing Fundamentals

by J. Stanley Warford

Process Modeling with ARIS®

by Heinrich Seidlmeier

Securing Electronic Business Processes

by Sachar Paulus, Norbert Pohlmann and Helmut Reimer

ISSE 2004 – Securing Electronic Business Processes

by Sachar Paulus, Norbert Pohlmann and Helmut Reimer

Sachar Paulus
Norbert Pohlmann
Helmut Reimer

ISSE 2004 – Securing Electronic Business Processes

**Highlights of the Information
Security Solutions Europe 2004
Conference**



Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliographie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

Many of designations used by manufacturers and sellers to distinguish their
products are claimed as trademarks.

1st edition September 2004

All rights reserved

© Friedr. Vieweg & Sohn Verlagsgesellschaft/GWV Fachverlage GmbH, Wiesbaden 2004

Vieweg is a company of Springer Science+Business Media.

www.vieweg.de



No part of this publication may be reproduced, stored in a retrieval system or
transmitted, mechanical, photocopying or otherwise without prior permission
of the copyright holder.

Cover design: Ulrike Weigel, www.CorporateDesignGroup.de

Typesetting: Oliver Reimer, Ilmenau

Printing and binding: Lengericher Handelsdruckerei, Lengerich

Printed on acid-free paper

ISBN-13: 978-3-528-05910-1

e-ISBN-13: 978-3-322-84984-7

DOI: 10.1007/978-3-322-84984-7

Preface

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by EEMA and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar. The aim of ISSE is to support the development of a European information security culture and especially a cross-border framework for trustworthy IT applications for citizens, industry and administration. Therefore, it is important to take into consideration both international developments and European regulations and to allow for the interdisciplinary character of the information security field. In the five years of its existence ISSE has thus helped shape the profile of this specialist area.

The integration of security in IT applications was initially driven only by the actual security issues considered important by experts in the field; currently, however, the economic aspects of the corresponding solutions are the most important factor in deciding their success. ISSE offers a suitable podium for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- Jan Bartelen, ABN AMRO (The Netherlands)
- Ronny Bjonnes, Microsoft (Belgium)
- Alfred Buellesbach, DaimlerChrysler (Germany)
- Lucas Cardholm, Ernst&Young (Sweden)
- Roger Dean, EEMA (UK)
- Marijke De Soete (Belgium)
- Jos Dumortier, KU Leuven (Belgium)
- Loup Gronier, XP conseil (France)
- John Hermans, KPMG (The Netherlands)
- Frank Jorissen, Silicomp Belgium (United Kingdom)
- Jeremy Hilton, EEMA (United Kingdom)
- Matt Landrock, Cryptomathic (Denmark)
- Karel Neuwirt, The Office for Personal Data Protection (Czech Republic)
- Sachar Paulus, SAP (Germany)
- Norbert Pohlmann, TeleTrusT (Germany)
- Reinhard Posch, TU Graz, (Austria)
- Bart Preneel, KU Leuven (Belgium)
- Helmut Reimer, TeleTrusT (Germany)
- Paolo Rossini, TELSIS, Telecom Italia Group (Italy)
- Ulrich Sandl, BMW (Germany)
- Wolfgang Schneider, GMD (Germany)
- Robert Temple, BT (United Kingdom)

Many of the presentations at the conference are of use as reference material for the future, hence this publication. The contributions are based on the presentations of the authors and thus not only document the key issues of the conference but make this information accessible for further interested parties.

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers.

Sachar Paulus

Norbert Pohlmann

Helmut Reimer

<p>EEMA (www.eema.org):</p> <p>For 16 years, EEMA has been Europe’s leading independent, non-profit e-Business association, working with its European members, governmental bodies, standards organisations and e-Business initiatives throughout Europe to further e-Business technology and legislation.</p> <p>EEMA’s remit is to educate and inform around 200 Member organisations on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas. The work produced by the association with its Members (projects, papers, seminars, tutorials and re-ports etc) is funded by both membership subscriptions and revenue generated through fee-paying events. All of the information generated by EEMA and its Members is available to other members free of charge.</p> <p>Examples of papers produced in recent months are:- Role Based Access Control – a User’s Guide, Wireless Deployment Guidelines, Secure e-Mail within the Organisation, The impact of XML on existing Business Processes, PKI Usage within User Organisations. EEMA Members, based on a requirement from the rest of the Membership, contributed all of these papers. Some are the result of many months’ work, and form part of a larger project on the subject.</p>	<p>TeleTrusT (www.teletrust.de):</p> <p>TeleTrusT was founded in 1989 to promote the security of information and communication technology in an open systems environment.</p> <p>The non-profit organization was constituted with the aim of:</p> <ul style="list-style-type: none"> • achieving acceptance of the digital signature as an instrument conferring legal validity on electronic transactions; • supporting research into methods of safeguarding electronic data interchange (EDI), application of its results, and development of standards in this field; • collaborating with institutes and organizations in other countries with the aim of harmonizing objectives and standards within the European Union. <p>TeleTrusT supports the incorporation of trusted services in planned or existing IT applications of public administration, organisations and industry. Special attention is being paid to secure services and their management for trustworthy electronic communication.</p>
---	---

Table of Contents

Strategy	1
True Economics of a Security Infrastructure <i>Andrew Oldham</i>	3
ROI+ Methodology to Justify Security Investment <i>Philippe Lemaire, Jean-Luc Delvaux</i>	12
Basel II and Beyond: Implications for e-Security <i>Thomas Kohler</i>	23
The Role of Attack Simulation in Risk Management Automation <i>Avi Corfas</i>	30
Secure ICT Architectures for Efficient Detection and Response <i>György Endersz</i>	38
Biometric Identity Cards: Technical, Legal, and Policy Issues <i>Gerrit Hornung</i>	47
New Initiatives and New Needs for Privacy Enhancing Technologies <i>Alexander Dix</i>	58
Data Protection Aspects of the Digital Rights Management <i>Alfred Büllersbach</i>	66
Big Brother does not Keep your Assets Safe <i>Johannes Wiele</i>	75

Technology	87
Identity Federation: Business Drivers, Use Cases, and Key Business Considerations <i>J. Matthew Gardiner</i>	89
Trusted Computing and its Applications: An Overview <i>Klaus Kursawe</i>	99
RFID Privacy: Challenges and Progress <i>Burt Kaliski</i>	108
Light-weight PKI-Enabling through the Service of a Central Signature Server <i>Malek Bechlaghem</i>	117
Massmailers: New Threats Need Novel Anti-Virus Measures <i>David Harley</i>	127
OpenPMF: A Model-Driven Security Framework for Distributed Systems <i>Ulrich Lang, Rudolf Schreiner</i>	138
Is Grid Computing more Secure? <i>Thomas Obert</i>	148
Tamper-Resistant Biometric IDs <i>Darko Kirovski, Nebojša Jojić, Gavin Jancke</i>	160

Application	177
Spam is Here to Stay <i>Andreas Mitrakas</i>	179
The Key to My On-Line Security <i>Paul Meadowcroft</i>	186
Dealing with Privacy Obligations in Enterprises <i>Marco Casassa Mont</i>	198
Trusted Computing: From Theory to Practice in the Real World <i>Alexander W. Koehler</i>	209
Electronic Signatures – Key for Effective e-Invoicing Processes <i>Stefan Hebler</i>	219
Legally Binding Cross Boarder Electronic Invoicing <i>Georg Lindsberger, Gerold Pinter, Alexander Egger</i>	228
SecMGW – An Open-Source Enterprise Gateway for Secure E-Mail <i>Tobias Straub, Matthias Fleck, Ralf Grewe, Oliver Lenze</i>	237
Web Service Security – XKMS (TrustPoint) <i>Daniel Baer, Andreas Philipp, Norbert Pohlmann</i>	250
EPM: Tech, Biz and Postal Services Meeting Point <i>José Pina Miranda, João Melo</i>	259

Practice	269
Managing Trust in Critical Infrastructure Protection Information Sharing Systems <i>John T. Sabo</i>	271
Legal Status of Qualified Electronic Signatures in Europe <i>Jos Dumortier</i>	281
The Finnish Ecosystem for Mobile Signatures <i>Werner Freystätter, Samu Kontinen</i>	290
e-Transformation Turkey Project <i>Aysegul Ibrisim, Rasim Yilmaz</i>	299
Asia PKI Interoperability Guideline <i>InKyung Jeun, Jaeil Lee, SangHwan Park</i>	309
Recent PKI Experiences in Serbia <i>Milan Marković</i>	321
CCTV and Workplace Privacy – Italy <i>Paolo Balboni</i>	333
Enhancing Security of Computing Platforms with TC-Technology <i>Oliver Altmeyer, Ahmad-Reza Sadeghi, Marcel Selhorst, Christian Stüble</i>	346
Index	363