Sachar Paulus
Norbert Pohlmann
Helmut Reimer

# ISSE 2006 – Securing Electronic Business Processes

vieweg-it

**Understanding MP3**
by Martin Ruckert

**Neuro-Fuzzy Systems**
by Detlef Nauck, Christian Borgelt, Frank Klawonn and Rudolf Kruse

**Applied Pattern Recognition**
by Dietrich W. R. Paulus and Joachim Hornegger

**From Enterprise Architecture to IT Governance**
by Klaus D. Niemann

**Beyond Compliance**
by Ralf-T. Grünendahl and Peter H. L. Will

**Microsoft Navision 4.0**
by Paul M. Diffenderfer and Samir El-Assar jr.

**Process Modeling with ARIS®**
by Heinrich Seidlmeier

www.vieweg.de

Sachar Paulus
Norbert Pohlmann
Helmut Reimer

# ISSE 2006 – Securing Electronic Business Processes

## Highlights of the Information Security Solutions Europe 2006 Conference

With 130 illustrations

vieweg

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



1st edition October 2006



Editorial office: Günter Schulz / Andrea Broßler

Vieweg is a company of Springer Science+Business Media.
www.vieweg.de




Cover design: Ulrike Weigel, www.CorporateDesignGroup.de
Typesetting: Oliver Reimer, Ilmenau
Printing and binding: LegoPrint SpA, Lavis
Printed on acid-free paper
Printed in Italy

ISBN-10 3-8348-0213-1
ISBN-13 978-3-8348-0213-2

# Contents

**Preface** ____ xi

**About this Book** ____ xiii

**ISCOM: On the Way for ICT Security in Italy** ____ xv

**RFID, e-ID Cards, Trusted Computing, Interoperability** ____ 1

Radio Frequency Identification (RFID) and Data Protection Legal Issues
*Zoi Talido* ____ 3

e-ID and Smartcards – Current Status, Hopeful Developments and Best Practices
*Graham Williamson* ____ 17

European Citizen Card Combined with Travel Document Function, Convergence or Divergence?
*Detlef Houdeau* ____ 25

Physical Unclonable Functions for enhanced security of tokens and tags
*Pim Tuyls, Boris Škorić* ____ 30

Hardware Security Features for Secure Embedded Devices
*Helena Handschuh, Elena Trichina* ____ 38

Security in Next Generation Consumer Electronic Devices
*Tom Kan, Tim Kerins, Klaus Kursawe* ____ 45

Security Architecture for Device Encryption and VPN
*Ammar Alkassar, Michael Scheibel, Christian Stüble, Ahmad-Reza Sadeghi, Marcel Winandy* ____ 54

TPM Enterprise Key Management requires centralized Hardware-based Security
*Bernhard Weiss* ____ 64

Implementation of DRM Systems under the EU Legal Framework
*Pius Alexander Benczek* 72

IT-Grundschutz: Two-Tier Risk Assessment for a Higher Efficiency in IT Security Management
*Angelika Jaschob, Lydia Tsintsifa* 95

ISO/IEC 24727 – A Future Standard for Smart Card Middleware
*Stephan Spitz, Jens Urmann, Gisela Meister* 102

Information Security Standardization – the ETSI Perspective
*Charles Brookson, Dionisio Zumerle* 108

Digital Signatures without the Headaches
*Nick Pope, Juan Carlos Cruellas* 119

Could Test Standards Help on the Way to Achieve Global e-Passport Interoperability?
*Andreas M. Wolf* 129

A New Standard Based Road to Interoperable Strong Authentication
*Philip Hoyer* 139

**Identity Management, Biometrics, PKI-Solutions, Network Security 149**

Identifying Patterns of Federation Adoption
*Heather Hinton, Mark Vandenwauver* 151

Fidelity: Federated Identity Management Security based on Liberty Alliance on European Ambit
*Manel Medina, Miquel Colomer, Sandra García Polo, Antoine de Poorter* 161

Deflecting Active Directory Attacks
*Jan De Clercq* 168

Implementing role based access control – How we can do it better!
*Marko Vogel* 176

Identity and Access Control – Demonstrating Compliance
*Marc Sel, Bart Van Rompay* 186

Robust and Secure Biometrics: Some Application Examples
*T. Kevenaar, G.J. Schrijen, A. Akkermans, M. Damstra, P. Tuyls, M. van der Veen* 196

Selecting the Optimal Biometric 2-factor Authentication Method – a User's Viewpoint
*Gunter Bitz* 204

A Face Recognition System for Mobile Phones
*Paolo Abeni, Madalina Baltatu, Rosalia D'Alessandro* 211

Advanced certificate validation service for secure Service-Oriented Architectures
*Antonio Ruiz-Martínez, Daniel Sánchez-Martínez, C. Inmaculada Marín-López, Antonio F. Gómez-Skarmeta* 218

An Introduction to Validation for Federated PKIs
*Robert Dulude, David Engberg, Seth Hitchings* 228

MADSig: Enhancing Digital Signature to Capture Secure Document Processing Requirements
*Jean-Christophe Pazzaglia, Stefano Crosta* 241

PKI Consolidation Project and Multiapplicative Smart Payment Cards
*Milan Marković, Miloš Kilibarda, Aleksandar Milošević* 249

Security Analysis and Configuration of Large Networks
*Antonio Lioy* 259

S-VPN Policy: Access List Conflict Automatic Analysis and Resolution
*Simone Ferraresi, Stefano Pesic, Livia Trazza, Andrea Baiocchi* 266

Lock-Keeper: A New Implementation of Physical Separation Technology
*Feng Cheng, Christoph Meinel* 275

SPEECH: Secure Personal End-to-End Communication with Handheld
*A. Castiglione, G. Cattaneo, A. De Santis, F. Petagna, U. Ferraro Petrillo* 287

Finding the Mobile Trusted Element
*Fabio Ricciato, Maura Turolla, Antonio Varriale* 298

**Security Management, Applications 309**

Centrally Administered COIs Using Cross-Organizational Trust
*Kevin Foltz, Coimbatore Chandersekaran* 311

Improving Assurance of Information Security RoI
*Michael D. Barwise* 318

Modelling the Economics of Free and Open Source Software Security
*Anas Tawileh, Jeremy Hilton, Steve McIntosh* 326

Securing service-oriented applications
*Anthony Nadalin, Nataraj Nagaratnam, Maryann Hondo* 336

A Service Oriented Trust Development Platform
*Helena Rifà, Francisco Jordán* 344

A Trust Label for Secure and Compliant e-ID Applications: The Belgian Experience
*Geert Somers, Jos Dumortier* 356

Electronic signature in Italy after ten years of "running in"
*Giovanni Manca* 363

**Awareness Raising, Compliance, Data Protection, Cyberspace Regulation** 375

Internet Early Warning System: The Global View
*Norbert Pohlmann, Marcus Proest* 377

IT Security Vulnerability and Incident Response Management
*Wim Hafkamp* 387

Blending Corporate Governance with Information Security
*Yves Le Roux* 396

On Privacy-aware Information Lifecycle Management in Enterprises: Setting the Context
*Marco Casassa Mont* 405

Regulation of State Surveillance of the Internet
*Murdoch Watney* 415

How Can NRA Contribute to the Improvement of IT Security?
*Rytis Rainys* 426

Information Security Regulation: Tomorrow Never Dies?
*Andreas Mitrakas* 433

Introducing Regulatory Compliance Requirements Engineering
*Shahbaz Ali, Jon Hall* 439

Legal Issues in Secure Grid Computing Environments
*Irene Kafeza, Eleanna Kafeza, Felix Wai-Hon Chan* 448

The Impact of Monitoring Technology on the Law
*Pieter Kleve, Richard De Mulder, Kees van Noortwijk* 455

**Index** 467

# Preface

ENISA is proud to be working with eema, TeleTrusT, ISCOM (the Italian Institute for Communications and Information Technologies) and the German Federal Ministry of the Interior as well as the German Federal Office for Information Security for this year's 8th annual Information Security Solutions Europe Conference.

The aim of ISSE has always been to support the development of a European information security culture. ENISA is committed to this goal, in our work to assist and advise the European Commission, Member States as well as business community on network, information security and legislative requirements and we are delighted to support ISSE again this year.

The security of communication networks and information systems is of increasing concern. In order to face today's complex information security challenges it is clear that working collaboratively with one another is the key to generating new strategies to address these problems. It has been an exciting opportunity to facilitate this collaboration at ISSE 2006, and pull together the wealth of industry knowledge, information and research that we hold in Europe, and across the globe.

The success of this event in generating ideas and frank, lively debate around the complex topic of IT security is due also to the independent, varied nature of the programme, which was selected by world-wide industry specialists.

Some of the key topics explored at this year's conference have been chosen as the basis for this book, which is an invaluable reference point for anyone involved in the IT security industry.

We hope that you will find it a thought-provoking and informative read.

Andrea Pirotti, Executive Director, ENISA

# About this Book

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 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.

From the beginning ISSE has been carefully prepared. The organisers succeeded in giving the conference a profile that combines a scientifically sophisticated and interdisciplinary discussion of IT security solutions while presenting pragmatic approaches for overcoming current IT security problems.

An enduring documentation of the presentations given at the conference which is available to every interested person thus became important. This year sees the publication of the third ISSE book – another mark of the event's success – and with about 50 carefully edited papers it bears witness to the quality of the conference.

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

- **Ronny Bjones,** Microsoft (Belgium)
- **Alfred Büllesbach,** Daimler Chrysler (Germany)
- **Lucas Cardholm,** Ernst&Young (Sweden)
- **Roger Dean,** eema (UK)
- **Marijke De Soete,** Security4Biz (Belgium)
- **Jos Dumortier,** KU Leuven (Belgium)
- **Walter Fumy,** Siemens (Germany)
- **Boaz Gelbord,** ENISA (Greece)
- **David Goodman,** eema (UK)
- **Michael Hange,** Federal Office for Information Security (Germany)
- **John Hermans,** KPMG (Netherlands)
- **Jeremy Hilton,** Cardiff University (UK)
- **Alison James,** eema (UK)
- **Frank Jorissen,** SafeBoot (Belgium)
- **Matt Landrock,** Cryptomathic (Denmark)
- **Tim Mertens,** ENISA (Greece)
- **Andreas Mitrakas,** ENISA (Greece)
- **David Naccache,** ENS (France)
- **Sachar Paulus,** SAP (Germany)

- **Daniele Perucchini,** Fondazione Ugo Bordoni (Italy)
- **Attila Péterfalvi,** Parliamentary Commissioner for Data Protection and Freedom of Information (Hungary)
- **Norbert Pohlmann,** University of Applied Sciences Gelsenkirchen (Germany)
- **Bart Preneel,** KU Leuven (Belgium)
- **Helmut Reimer,** TeleTrusT (Germany)
- **Paolo Rossini,** Telsy Italia (Italy)
- **Wolfgang Schneider,** Fraunhofer SIT (Germany)
- **Robert Temple,** BT (UK)

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*

**eema (www.eema.org):**

Established in 1987, eema is an independent association of IT professionals, businesses and governments providing business and technical networking opportunities at both local and regional levels in the broad areas associated with digital identity and its applications, such as security. Our mission is to stimulate the growth and effectiveness of our members' business in these areas through increased market awareness, cooperation and opportunity creation.

We aim to bring over 1,500 member representatives together in a neutral environment for education and networking puposes. We enable members to share experiences and best practice by holding meetings and conferences, by facilitating working groups who produce reports on topical subjects, and by helping members to connect with the right person to help them solve business issues or develop beneficial business relationships. All work produced by members is available free to other members, and previous papers include: Towards Understanding Identity, Role Based Access Control – a Users Guide, Secure e-mail within a Corporate Environment and Secure e-mail between Organisations.

For more information contact:
alison.james@eema.org.

**TeleTrusT (www.teletrust.de):**

In the 16 years of its existence TeleTrusT has evolved into a competence network for applied Cryptography and Biometrics with over 90 institutional members.

The TeleTrusT working groups produce results which create an advantageous framework for trustworthy solutions of daily business processes as well as contributing to their acceptance.

TeleTrusT brings together the interests of users and vendors. Thus vendors can satisfy the users' demands more effectively with marketable products and services, in which scalable security mechanisms are implemented.

TeleTrusT seeks and cultivates the cooperation with other organisations with similar objectives – in Germany and internationally. Thus ISSE has been organised in cooperation with EEMA, ENISA and ISCOM in Rome this year.

For further information contact:
sophie.hellmann@teletrust.de

# ISCOM:
# On the Way for ICT Security in Italy

The Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM) was established in 1907 as a technical-scientific department belonging to the Italian Communication Ministry. Considering its role as a nonpartisan public institution, the Institute's value added in terms of reliability and expertise is the aspect which characterizes the technical support and consultancy services it provides to businesses and entities in the TLC sector. The role of ISCOM in providing services to ICT Companies, government agencies and users is manifold, spanning from experimental and research activities to specialized training and education in the TLC field.

One of ISCOM's main missions is its proactive role in national and international law-making activities, in order to ensure greater transparency and better access to services for users, manufacturers and TLC network administrators alike.

As far as research is concerned, ISCOM is essentially focused on developing and improving TLC and IT related services. Hence, activities involve almost all areas in these fields, from telephony to television, to signal processing and treatment, from network architecture to service implementation.

ISCOM runs the Post-Graduate Specialization School in TLC (which began its activity in 1923), which provides higher education in electronic communication and information technologies; it also provides technical training and updating courses on electronic communications and information technologies, security, multimedia applications, and Quality of Service to both Ministry and government staff in general, to enhance their technical know-how and skills.

ISCOM works with several Certification Bodies to verify and control Corporate Quality System compliance with UNI EN ISO 9000 standards, is involved in monitoring Accredited Laboratory compliance with UNI CEI EN ISO/IEC 17025 rules and is a Notified Body for activities envisaged by Legislative Decree n. 269 of May 9, 2001. It is also a Notified Body under the EU Directive on radio equipment and telecommunications terminal equipment as well as a Competent Body and Notified Body on electromagnetic compatibility. In 2002, the Institute became the International Certification Body for the TETRA MoU.

Among all the numerous ISCOM fields of activity, ICT security is getting an increasing relevance. Here, ISCOM plays a leading role in various contexts, some of which are briefly summarized below:

- Due to his widely recognized non-partisan role, a government decree dated october 30, 2003 appointed ISCOM the Certification Body within the Italian certification scheme for commercial security systems and products. The Certification Body supervises all the

activities carried out within the certification scheme, which operates according to the international evaluation criteria ITSEC and Common Criteria.

- ISCOM is an Evaluation Center (Ce.Va.) for ICT systems and products dealing with classified data. The center, the only one belonging to the Italian Public Administration which has been accredited by the Autorità Nazionale per la Sicurezza (ANS), carries out evaluation activities according to ITSEC and Common Criteria.
- ISCOM runs the Training Center on ICT Security for Public Administration personnel. The Training Center provides training and raises awareness amongst government employees on ICT security, through the development of a centralized and coordinated Training and Awareness-Raising Plan aimed at disseminating security principles and methodologies throughout the Administration.
- The Institute acts as promoter and leader of several initiatives aimed at raising the national level of ICT security, by gathering the expertise of the major subjects operating in the ICT field. Among these initiatives we can recall the redaction of three guidelines, in English and Italian, on "*The quality of service in ICT networks*", "*Risk analysis and protection strategies for network security*" and "*Network security in critical infrastructures*", carried out with the contribution of experts from institutions and industry. Six more guidelines are being released; these will be focused on deepenings on risk analysis, on the outsourcing of security services, on QoS in UMTS, on QoS in broadband networks, on local emergency handling and on security certification. Moreover, ISCOM has promoted the creation of ISAC on network security, currently involving all the major Italian network operating companies.

ISCOM hosting of ISSE 2006 is a further prove of our desire to play a role in fostering the European information security debate. We look forward to a great opportunity for the exchange of ideas and experiences.

Luisa Franchina,

PhD, General Director of Istituto Superiore delle Comunicazioni
E delle Tecnologie dell'Informazione