

---

# ISSE 2012 Securing Electronic Business Processes

---

Helmut Reimer • Norbert Pohlmann  
Wolfgang Schneider (Eds.)

# ISSE 2012 Securing Electronic Business Processes

Highlights of the Information Security  
Solutions Europe 2012 Conference

*Editors*

Helmut Reimer  
TeleTrust Deutschland e.V., Erfurt  
Germany

Wolfgang Schneider  
Wiesbaden  
Germany

Norbert Pohlmann  
Aachen  
Germany

ISBN 978-3-658-00332-6  
DOI 10.1007/978-3-658-00333-3

ISBN 978-3-658-00333-3 (eBook)

Library of Congress Control Number: 2012948599

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

Springer Vieweg

© Springer Fachmedien Wiesbaden 2012

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein

Printed on acid-free paper

Springer Vieweg is a brand of Springer DE. Springer DE is part of Springer Science+Business Media  
[www.springer-vieweg.de](http://www.springer-vieweg.de)

# Contents

<b>About this Book</b>	<b>ix</b>
------------------------	-----------

<b>Data Loss Prevention in Real Life</b>	<b>1</b>
--	----------

Thorsten Scharmatinat

<b>Information Security Strategy Enterprise and Cloud Computing Security</b>	<b>9</b>
--	----------

<b>Threats, Risks and the Derived Information Security Strategy</b>	<b>11</b>
---	-----------

Lenka Fibikova · Roland Mueller

<b>Information Security Management – Best Practice Guidelines for Managers</b>	<b>21</b>
--	-----------

Werner Wüpper · Iryna Windhorst

<b>IT Security Investment and Costing Emphasizing Benefits in Times of Limited Budgets</b>	<b>37</b>
--	-----------

Mechthild Stöwer · Reiner Kraft

<b>A Modern Approach on Information Security Measurement</b>	<b>48</b>
--	-----------

Frederik Humpert-Vrielink · Nina Vrielink

<b>e-Identity – Monetization and Interoperability</b>	<b>54</b>
---	-----------

Marc Sel

<b>The PoSecCo Security Decision Support System</b>	<b>64</b>
---	-----------

Cataldo Basile · Antonio Lioy · Stefano Paraboschi

<b>Enterprise Mobility – A Balancing Act between Security and Usability</b>	<b>75</b>
---	-----------

Patrick Michaelis

<b>A Systematic Holistic Approach for Providers to Deliver Secure ICT Services</b>	<b>80</b>
--	-----------

Eberhard von Faber · Wolfgang Behnsen

<b>Implementing Least Privilege for Interconnected, Agile SOAs/Clouds</b>	<b>89</b>
---	-----------

Dr. Ulrich Lang · Rudolf Schreiner

<b>Security and Privacy Impact of Green Energy</b>	
<b>Human Factors of IT Security</b>	<b>103</b>
<b>Privacy-Preserving Smart Metering</b>	<b>105</b>
Alfredo Rial · George Danezis	
<b>Smart Metering, Common Criteria and European Privacy Needs</b>	<b>116</b>
Markus Bartsch	
<b>Securing the Smart Grid with Hardware Security Modules</b>	<b>128</b>
Dieter Bong · Andreas Philipp	
<b>The Human Aspect in Data Leakage Prevention in Academia</b>	<b>137</b>
Elham Rajabian Noghondar · Konrad Marfurt · Bernhard Haemmerli	
<b>Solutions for Mobile Applications</b>	
<b>Identity &amp; Access Management</b>	<b>147</b>
<b>Security of Mobile Devices, Applications and Transactions</b>	<b>149</b>
Daniel Borleteau · Nicolas Bousquet · Thierry Crespo · Xavier Dubarry · Jan Eichholz · Virginie Galindo	
<b>Management and Use of ID Credentials on NFC Enabled Phones: Use Cases, Challenges, Technologies and Standards</b>	<b>161</b>
Philip Hoyer	
<b>Malware Detection in Ubiquitous Environments</b>	<b>171</b>
Manuel García-Cervigón · Roberto Morales	
<b>A New Security Architecture for Smartcards Utilizing PUFs</b>	<b>180</b>
Thomas Esbach · Walter Fumy · Olga Kulikovska · Dominik Merli · Dieter Schuster · Frederic Stumpf	
<b>Strong Authentication of Humans and Machines in Policy Controlled Cloud Computing Environment Using Automatic Cyber Identity</b>	<b>195</b>
Libor Neumann · Tomáš Halman · Pavel Rotek · Alexander Boettcher · Julian Stecklina · Michal Sojka · David Núñez · Isaac Agudo	

<b>Trustworthy Infrastructures</b>	
<b>Separation &amp; Isolation</b>	<b>207</b>
<b>eConsent Management and Enforcement in Personal Telehealth</b>	<b>209</b>
Muhammad Asim · Paul Koster · Milan Petković · Martin Rosner	
<b>Information Management and Sharing for National Cyber Situational Awareness</b>	<b>217</b>
Florian Skopik · Thomas Bleier · Roman Fiedler	
<b>Analyzing G-20's Key Autonomous Systems and their Intermeshing using AS-Analyzer</b>	<b>228</b>
Sebastian Feld · Norbert Pohlmann · Michael Sparenberg · Bastian C. Wichmann	
<b>Intention Semantics and Trust Evidence</b>	<b>243</b>
Claire Vishik · David Ott · David Grawrock	
<b>Applying a Security Kernel Framework to Smart Meter Gateways</b>	<b>252</b>
Michael Gröne · Marcel Winandy	
<b>Securing Smartphone Compartments: Approaches and Solutions</b>	<b>260</b>
Ammar Alkassar · Steffen Schulz · Christian Stüble · Sven Wohlgemuth	
<b>EU Digital Agenda</b>	
<b>Cyber Security: Hackers &amp; Threats</b>	<b>269</b>
<b>ETSI STF 428 – Accelerating Deployment of Interoperable Electronic Signatures in Europe</b>	<b>271</b>
Juan Carlos Cruellas · Andrea Caccia · Konrad Lanz · Giulana Marzola · Luigi Rizzo · Laurent Velez	
<b>PEPPOL – Experience from Four Years Work on eSignature Interoperability</b>	<b>282</b>
Jon ØInes	
<b>Exploiting Virtual File Formats for Fun and Profit</b>	<b>296</b>
Enno Rey · Pascal Turbing · Daniel Mende · Matthias Luft	
<b>Anonymous, a new Civil Disobedience Phenomenon</b>	<b>306</b>
Vaclav Jirovsky	
<b>Building Technologies that Help Cyber-Defense: Hardware-enabled Trust</b>	<b>316</b>
Claire Vishik · Ruby B. Lee · Fred Chong	
<b>Index</b>	<b>327</b>

# 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 range of topics has changed enormously since the founding of ISSE. In addition to our ongoing focus on securing IT applications and designing secure business processes, protecting against attacks on networks and their infrastructures is currently of vital importance. The ubiquity of social networks has also changed the role of users in a fundamental way: requiring increased awareness and competence to actively support systems security. ISSE offers a perfect platform 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 tenth ISSE book – another mark of the event's success – and with about 30 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:

- **Ammar Alkassar**, Sirrix AG (Germany)
- **Ronny Bjones**, Microsoft (Belgium)
- **John Colley**, EMEA & (ISC)<sup>2</sup> (United Kingdom)
- **Roger Dean**, eema (United Kingdom)
- **Jan De Clercq**, HP (Belgium)
- **Marijke De Soete**, Security4Biz (Belgium)
- **Jos Dumortier**, KU Leuven (Belgium)
- **Walter Fumy**, Bundesdruckerei (Germany)
- **Michael Hartmann**, SAP (Germany)
- **Jeremy Hilton**, Cranfield University (United Kingdom)
- **Francisco Jordan**, Safelayer (Spain)

- **Frank Jorissen**, tygris (Belgium)
- **Marc Kleff**, Siemens Enterprise Communications (Germany)
- **Hasse Kristiansen**, Ernst & Young (Norway)
- **Jaap Kuipers**, DigiNotar (The Netherlands)
- **Manuel Medina**, ENISA
- **Patrick Michaelis**, Research In Motion (Germany)
- **Norbert Pohlmann** (chairman), Institute for Internet Security, Westfälische Hochschule, Gelsenkirchen (Germany)
- **Bart Preneel**, KU Leuven (Belgium)
- **Helmut Reimer**, TeleTrusT (Germany)
- **Wolfgang Schneider**, Fraunhofer Institute SIT (Germany)
- **Jon Shamah**, EJ Consultants (United Kingdom)
- **Claire Vishik**, Intel (United Kingdom)

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. With this book TeleTrusT aims to continue documenting the many valuable contributions to ISSE. We would like to thank Bundesdruckerei GmbH Berlin and itWatch GmbH Munich for their support.

*Norbert Pohlmann*

*Helmut Reimer*

*Wolfgang Schneider*



## TeleTrusT – IT Security Association Germany

TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities.

TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is carrier of the “European Bridge CA” (provision of public key certificates for secure e-mail communication), the quality seal “IT Security made in Germany” and runs the IT expert certification program “TeleTrusT Information Security Professional (T.I.S.P.)”. TeleTrusT is member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

Keeping in mind the raising importance of the European security market, TeleTrusT seeks co-operation with European and international organisations and authorities with similar objectives. Thus, this year’s European Security Conference ISSE is being organized in collaboration with eema and LSEC and supported by the European Commission and ENISA.

### Contact:

TeleTrusT – IT Security Association Germany  
Dr. Holger Muehlbauer  
Managing Director  
Chausseestrasse 17  
10115 Berlin  
GERMANY  
Tel.: +49 30 4005 4306  
Fax: +49 30 4005 4311  
<http://www.teletrust.de>

## eema

For 25 years, EEMA has been Europe’s leading independent, not-for-profit e-Identity & Security association, working with its European members, governmental bodies, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

EEMA’s remit is to educate and inform over 1,500 Member contacts 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 reports 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.

Examples of recent EEMA events include The European e-ID interoperability conference in Biel, Switzerland (Featuring STORK, TDL (Trust in Digital Life), SSEDIC & GINI) and The European e-Identity Management Conference in Paris.

EEMA and its members are also involved in many European funded projects including STORK2, SSEDIC, ETICA and Future eID

Any organisation involved in e-Identity or Security (usually of a global or European nature) can become a member of EEMA, and any employee of that organisation is then able to participate in EEMA activities. Examples of organisations taking advantage of EEMA membership are Siemens, Hoffman la Roche, KPMG, Deloitte, ING, Novartis, , TOTAL, PGP, McAfee, Adobe, Magyar Telecom Rt, Nets, National Communications Authority, Hungary, Microsoft, HP, and the Norwegian Government Administration Services to name but a few.

Visit [www.eema.org](http://www.eema.org) for more information or contact the association on +44 1386 793028 or at [info@eema.org](mailto:info@eema.org)