

Norbert Pohlmann | Helmut Reimer | Wolfgang Schneider (Eds.)

ISSE 2010 Securing Electronic Business Processes

Norbert Pohlmann | Helmut Reimer |  
Wolfgang Schneider (Eds.)

# ISSE 2010

# Securing Electronic Business Processes

Highlights of the Information Security Solutions  
Europe 2010 Conference

With 80 Figures



**VIEWEG+**  
**TEUBNER**

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

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

1st Edition 2011

All rights reserved

© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011

Editorial Office: Dr. Christel Roß | Andrea Broßler

Vieweg+Teubner Verlag is a brand of Springer Fachmedien.

Springer Fachmedien is part of Springer Science+Business Media.

[www.viewegteubner.de](http://www.viewegteubner.de)



No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the copyright holder.

Registered and/or industrial names, trade names, trade descriptions etc. cited in this publication are part of the law for trade-mark protection and may not be used free in any form or by any means even if this is not specifically marked.

Cover design: KünkelLopka Medienentwicklung, Heidelberg

Typesetting: Oliver Reimer, Jena

Printing company: MercedesDruck, Berlin

Printed on acid-free paper

Printed in Germany

ISBN 978-3-8348-1438-8

# Contents

|                                                                                                            |            |
|------------------------------------------------------------------------------------------------------------|------------|
| <b>About this Book</b>                                                                                     | <b>vii</b> |
| <b>Welcome</b>                                                                                             | <b>xi</b>  |
| <b>Germany on the Road to Electronic Proof of Identity</b>                                                 | <b>1</b>   |
| Ulrich Hamann                                                                                              |            |
| <b>Identity and Security Management</b>                                                                    | <b>11</b>  |
| <b>Security Analysis of OpenID, followed by a Reference Implementation of an nPA-based OpenID Provider</b> | <b>13</b>  |
| Sebastian Feld · Norbert Pohlmann                                                                          |            |
| <b>New Authentication Concepts for Electronic Identity Tokens</b>                                          | <b>26</b>  |
| Jan Eichholz · Dr. Detlef Hühnlein · Dr. Gisela Meister · Johannes Schmölz                                 |            |
| <b>A Simplified Approach for Classifying Applications</b>                                                  | <b>39</b>  |
| Lenka Fibikova · Roland Müller                                                                             |            |
| <b>Technical and Economical Aspects of Cloud Security</b>                                                  | <b>51</b>  |
| <b>Single Sign-on(SSO) to Cloud based Services and Legacy Applications “Hitting the IAM wall”</b>          | <b>53</b>  |
| Marcus Lasance                                                                                             |            |
| <b>Cloud &amp; SOA Application Security as a Service</b>                                                   | <b>61</b>  |
| Ulrich Lang                                                                                                |            |
| <b>Authentication and Trust: Turning the Cloud inside out</b>                                              | <b>72</b>  |
| Christian Brindley                                                                                         |            |
| <b>User Risk Management Strategies and Models – Adaption for Cloud Computing</b>                           | <b>80</b>  |
| Eberhard von Faber · Michael Pauly                                                                         |            |
| <b>Security and Compliance in Clouds</b>                                                                   | <b>91</b>  |
| Kristian Beckers · Jan Jürjens                                                                             |            |
| <b>Applying BMIS to Cloud Security</b>                                                                     | <b>101</b> |
| Rolf von Rössing                                                                                           |            |

|                                                                                                                                                      |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Security Services and Large Scale Public Applications</b>                                                                                         | <b>113</b> |
| <b>Critical Infrastructure in Finance PARSIFAL Recommendations</b>                                                                                   | <b>115</b> |
| Bernhard M. Hämmerli · Henning H. Arendt                                                                                                             |            |
| <b>The SPOCS Interoperability Framework: Interoperability of eDocuments and eDelivery Systems taken as Example</b>                                   | <b>122</b> |
| Thomas Rössler · Arne Tauber                                                                                                                         |            |
| <b>STORK: Architecture, Implementation and Pilots</b>                                                                                                | <b>131</b> |
| Herbert Leitold · Bernd Zwattendorfer                                                                                                                |            |
| <b>Secure Networking is the Key to German Public e-Health Solution: Migration Towards an Integrated e-Health Infrastructure</b>                      | <b>143</b> |
| Bernhard Weiss                                                                                                                                       |            |
| <b>Advanced Security Service cERTificate for SOA: Certified Services go Digital !</b>                                                                | <b>151</b> |
| J-C. Pazzaglia · V. Lotz · V. Campos Cerda · E. Damiani · C. Ardagna · S. Gürgens · A. Maña · C. Pandolfo · G. Spanoudakis · F. Guida · R. Menicocci |            |
| <b>Privacy and Data Protection</b>                                                                                                                   | <b>161</b> |
| <b>Data Protection and Data Security Issues Related to Cloud Computing in the EU</b>                                                                 | <b>163</b> |
| Paolo Balboni                                                                                                                                        |            |
| <b>The Mask of the Honorable Citizen</b>                                                                                                             | <b>173</b> |
| Johannes Wiele                                                                                                                                       |            |
| <b>Towards Future-Proof Privacy-Respecting Identity Management Systems</b>                                                                           | <b>182</b> |
| Marit Hansen                                                                                                                                         |            |
| <b>Privacy Compliant Internal Fraud Screening</b>                                                                                                    | <b>191</b> |
| Ulrich Flegel                                                                                                                                        |            |

# **Threats and Countermeasures \_\_\_\_\_ 201**

## **Malware Detection and Prevention Platform: Telecom Italia Case Study \_\_\_\_\_ 203**

Luciana Costa · Roberta D'Amico

## **Defining Threat Agents: Towards a More Complete Threat Analysis \_\_\_\_\_ 214**

Timothy Casey · Patrick Koeberl · Claire Vishik

## **A Mechanism for e-Banking Frauds Prevention and User Privacy Protection \_\_\_\_\_ 226**

Rosalia D'Alessandro · Manuel Leone

## **Countering Phishing with TPM-bound Credentials \_\_\_\_\_ 236**

Ingo Bente · Joerg Vieweg · Josef von Helden

# **Smart Grid Security and Future Aspects \_\_\_\_\_ 247**

## **Security Challenges of a Changing Energy Landscape \_\_\_\_\_ 249**

Marek Jawurek · Martin Johns

## **Privacy by Design: Best Practices for Privacy and the Smart Grid \_\_\_\_\_ 260**

Ann Cavoukian

## **A Policy-based Authorization Scheme for Resource Sharing in Pervasive Environments \_\_\_\_\_ 271**

Roberto Morales · Jetzabel Serna · Manel Medina

## **Visual Representation of Advanced Electronic Signatures \_\_\_\_\_ 280**

Nick Pope

## **DSKPP and PSKC, IETF Standard Protocol and Payload for Symmetric Key Provisioning \_\_\_\_\_ 291**

Philip Hoyer

## **Silicon PUFs in Practice \_\_\_\_\_ 300**

Patrick Koeberl · Jiangtao Li · Anand Rajan · Claire Vishik

|                                                                                                          |            |
|----------------------------------------------------------------------------------------------------------|------------|
| <b>Biometrics and Technical Solutions</b>                                                                | <b>313</b> |
| <b>Visa Applications in TG Biometrics for Public Sector Applications</b>                                 | <b>315</b> |
| Dr. Sibylle Hick · Fares Rahmun · Ernest Hammerschmidt                                                   |            |
| <b>Taking Signatures Seriously – Combining Biometric and Digital Signatures</b>                          | <b>323</b> |
| Santiago Uriel Arias                                                                                     |            |
| <b>Automatic Configuration of Complex IPsec-VPNs and Implications to Higher Layer Network Management</b> | <b>334</b> |
| Michael Rossberg · Günter Schäfer · Kai Martius                                                          |            |
| <b>SCADA and Control System Security: New Standards Protecting Old Technology</b>                        | <b>343</b> |
| Scott Howard                                                                                             |            |
| <b>A Small Leak will Sink a Great Ship: An Empirical Study of DLP Solutions</b>                          | <b>354</b> |
| Matthias Luft · Thorsten Holz                                                                            |            |
| <b>eID and the new German Identity Card</b>                                                              | <b>365</b> |
| <b>The New German ID Card</b>                                                                            | <b>367</b> |
| Marian Margraf                                                                                           |            |
| <b>AusweisApp and the eID Service/Server – Online Identification Finally more Secure</b>                 | <b>374</b> |
| Werner Braun · Dirk Arendt                                                                               |            |
| <b>Postident Online with the new Personal Identity Card</b>                                              | <b>385</b> |
| Jens Terboven                                                                                            |            |
| <b>The eID Function of the nPA within the European STORK Infrastructure</b>                              | <b>392</b> |
| Volker Reible · Dr. Andre Braunmandl                                                                     |            |
| <b>Polish Concepts for Securing E-Government Document Flow</b>                                           | <b>399</b> |
| Mirosław Kutylowski · Przemysław Kuba                                                                    |            |
| <b>Index</b>                                                                                             | <b>409</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 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 eighth ISSE book – another mark of the event's success – and with about 40 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 and GI e.V. (Germany)
- **Gunter Bitz**, SAP (Germany)
- **Ronny Bjones**, Microsoft (Belgium)
- **Lucas Cardholm**, Ernst&Young (Sweden)
- **Roger Dean**, eema (United Kingdom)
- **Steve Purser**, ENISA
- **Jan De Clercq**, HP (Belgium)
- **Marijke De Soete**, Security4Biz (Belgium)
- **Jos Dumortier**, K.U. Leuven (Belgium)
- **Walter Fumy**, Bundesdruckerei (Germany)
- **Robert Garskamp**, Everett (The Netherlands)
- **Riccardo Genghini**, S.N.G. (Italy)

- **John Hermans**, KPMG (The Netherlands)
- **Jeremy Hilton**, Cardiff University (United Kingdom)
- **Francisco Jordan**, Safelayer (Spain)
- **Frank Jorissen**, McAfee (Belgium)
- **Bernd Kowalski**, BSI (Germany)
- **Jaap Kuipers**, DigiNotar (The Netherlands)
- **Matt Landrock**, Cryptomathic (Denmark)
- **Marian Margraf**, BMI (Germany)
- **Madeleine McLaggan-van Roon**, Dutch Data Protection Authority (The Netherlands)
- **Norbert Pohlmann (chairman)**, University of Applied Sciences Gelsenkirchen (Germany)
- **Bart Preneel**, K.U. Leuven (Belgium)
- **Helmut Reimer**, TeleTrusT (Germany)
- **Joachim Rieß**, Daimler (Germany)
- **Volker Roth**, Freie Universität Berlin (Germany)
- **Wolfgang Schneider**, Fraunhofer Institute SIT (Germany)
- **Jean-Pierre Seifert**, TU Berlin (Germany)
- **Jon Shamah**, EJ Consultants (United Kingdom)
- **Robert Temple**, BT (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.

*Norbert Pohlmann*

*Helmut Reimer*

*Wolfgang Schneider*

## TeleTrusT Deutschland e.V. www.teletrust.de

TeleTrusT Germany ("TeleTrusT Deutschland e.V.") was founded in 1989 as a not-for-profit organisation promoting the trustworthiness of information and communication technology in open systems environments.

Today, as an IT security association, TeleTrusT counts more than 100 members from industry, science and research as well as public institutions. Within the last 20 years TeleTrusT evolved to a well known and highly regarded competence network for IT security whose voice is heard throughout Germany and Europe.

In various TeleTrusT working groups ICT security experts, users and interested parties meet each other in frequent workshops, round-tables and expert talks. The activities focus on reliable and trustworthy solutions complying with international standards, laws and statutory requirements.

TeleTrusT is keen to promote the acceptance of solutions supporting identification, authentication and signature (IAS) schemes in electronic business and its processes.

TeleTrusT facilitates information and knowledge exchange between vendors, users and authorities. Subsequently, innovative ICT security solutions can enter the market more quickly and effectively. TeleTrusT aims on standard compliant solutions in an interoperable scheme.

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, ENISA and the German Federal Ministry of the Interior.

Contact:

Dr. Holger Muehlbauer

Managing Director of TeleTrusT Deutschland e.V.

holger.muehlbauer@teletrust.de

## eema www.eema.org

For 23 years, eema has been Europe's leading independent, non-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 Brussels (Featuring STORK, PEPPOL, SPOCS & epSOS) and The European e-Identity Management Conference in London in partnership with OASIS

EEMA and its members are also involved in many European funded projects including STORK, ICEcom and ETICA

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 Volvo, Hoffman la Roche, KPMG, Deloitte, ING, Novartis, Metropolitan Police, TOTAL, PGP, McAfee, Adobe, Magyar Telecom Rt, BBS, 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).

# Welcome

**Ladies and gentlemen,**

It is a particular honour to invite you to the twelfth ISSE Conference, taking place in Berlin on 5 - 7 October 2010, this year hosted by the Federal Ministry of the Interior.

The independent ISSE Conference focuses on secure information systems solutions in a globally networked world. Since the advent of the Internet, countless business, administrative and consumer solutions have transformed our society and the base of economic cooperation around the world. Without doubt, secure and trustworthy information systems are key for the reliability of any ICT infrastructure and future economic prosperity, particularly since more and more fixed and mobile business processes use the Internet.



The ISSE Conference offers the best environment to discuss innovations and new technical solutions for IT security in Europe. We expect more than 400 specialists, researchers, business leaders and policy makers from all over Europe to join us at ISSE to share information and best practices through thoughtful discussions and thorough debates.

Best wishes for a successful and productive conference. I look forward to seeing you in Berlin!

A handwritten signature in black ink, which appears to read 'Thomas de Maizière'. The signature is stylized with a large, sweeping initial 'T' and a long, horizontal stroke extending to the right.

*Thomas de Maizière*  
Federal Minister of the Interior