



The European  
e-Identity Conference

12-13 June 2007, Paris, France

Run jointly by



eema's 20<sup>th</sup> Anniversary Conference

## Biographies

Gold Sponsor

**THALES**

## eema would like to thank our supporters

### Gold Sponsor

# THALES

Operating in three main markets covering e-security, card payment and network security, Thales' e-Security activities address the business, government and finance industries' need for cryptographic security products and solutions. Over half of the world's banks, together with the majority of the busiest exchanges, currently use Thales technology. For more than 25 years the company has been at the forefront of security and payment technology, co-operating and contributing to set the industry standards used for financial transactions and e-commerce globally.

[www.thalesgroup.com/esecurity](http://www.thalesgroup.com/esecurity)

### Sponsors and Exhibitors



BEA Systems, Inc. (Nasdaq: BEAS) is a world leader in enterprise infrastructure software. The BEA SOA 360™ platform, the industry's most unified SOA platform for business transformation and optimization, is designed to improve processes and grow innovative services. Information about how BEA is enabling customers to achieve Business LiquidITy™ can be found at [www.bea.com](http://www.bea.com).



Every day, the world's most demanding government and commercial enterprises rely on CoreStreet technology to authorise critical events ranging from signed communications and transactions to physical access to homeland security. More information, including technical whitepapers, industry solution studies and a list of the patents awarded to the company is available at [www.corestreet.com](http://www.corestreet.com).



ENISA is a Centre of Excellence for the EU Member States and EU Institutions in Network and Information Security, giving expert advice and recommendations. It is a switchboard of information for best practices and facilitates contacts between the EU-institutions, the Member States and the private business & industry actors. [www.enisa.europa.eu/](http://www.enisa.europa.eu/)



Entrust is a world-leader in securing digital identities and information. Over 1,600 enterprises and government agencies in more than 60 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities. [www.entrust.com](http://www.entrust.com)



IdenTrust is the global leader in trusted identity solutions, recognized by global financial institutions, government agencies and departments, and commercial organizations around the world. IdenTrust enables organizations to effectively manage the risks associated with identity authentication; work interoperably with countries around the world; minimize investment in creating their own policies and legal frameworks; and deploy a spectrum of products insuring trust, smarter, faster, and more cost effectively.

[www.identrust.com](http://www.identrust.com)



From securing SSL to safeguarding complete authentication systems, nCipher's ground breaking products help organisations implement and enforce their security policy. Through strong key management controls, including split knowledge and dual control, nCipher technology is used to optimise cryptographic security, making it faster, more secure and easier to manage.

[www.ncipher.com](http://www.ncipher.com)



"Orange™ is the key brand of France Telecom, one of the world's leading telecommunications operators with more than 161 million customers on five continents. In June, 2006, as part of the France Telecom integrated operator strategy (NExT programme) to deliver simple, convergent products, Orange™ became the single brand for Mobile, internet and tv offers in France, the United Kingdom, The Netherlands and in Spain, strengthening Orange's position as the number two mobile and internet services brand in Europe. Orange™ Business Services, which operates in 220 countries or territories, became the new banner for business communications solutions and services.

[www.orange.com](http://www.orange.com)



The SafeBoot suite of data and device security solutions protects networks, data and (mobile) devices against the risks associated with loss, theft, and unauthorised access. SafeBoot solutions offer strong access control and powerful encryption technologies and our centralised management system provides small, medium, and large enterprises with operational efficiency and the lowest possible total cost of ownership.

[www.safeboot.com](http://www.safeboot.com)

**European e-Identity Conference  
Programme Day 1**

09.30	<b>ENISA Workshop Security Issues in Social Networking</b>		
09.30	Introduction		
09.35	Social networking security issues for children - <i>Josephine Fraser, Childnet</i>		
09.55	Security recommendations to social networking communities - <i>Maz Nadjm, Rareface</i>		
10.15	Implications of social networking behaviour for tomorrow's citizens and workforce - <i>Mathieu Gorge, VigiTrust</i>		
10.30	<b>Opening Session – The Challenges of Corporate, Public and Private Identities Today</b>		
	Welcome, background and introduction to the conference - <i>Roger Dean, Executive Director, eema</i>		
10.45	<b>Welcome address:</b> - <i>Philippe Duluc, Chief Security Officer, Orange/France Telecom group</i>		
11.05	<b>ENISA address:</b> <i>Alain Esterle, Head of Technical Department, ENISA</i>		
11.25	<b>The eema address:</b> The evolution of identity services, the emergence of user-centric networks and the future of eema – <i>David Goodman, eema Chair</i>		
11.45	<b>Keynote address:</b> <i>Kim Cameron, Microsoft</i>		
12.15	Opening debate with audience participation		
12.30	<b>Lunch</b>		
13.45	<b>eema Track Managing Identity</b>		<b>ENISA Workshop Social Networking cont</b>
	Chairman's introduction & opening remarks		
14.00	Totally integrated architecture, where business requirements meet technology <i>Franz-Josef Nölke, Solution Line Manager Security Applications, Siemens</i>	13.45	Netlog - Experiences from a large-scale social networking application <i>Lien Louwagie</i>
14.30	Gaining the benefit of e-ID from correctly implemented applications <i>Olivier Delos, Managing Partner, SEALED.</i>	14.05	Imagined communities: awareness, information sharing and privacy: the Facebook case <i>Alessandro Acquisti, CMU</i>
15.00	Building a solid identity management foundation layer <i>John Erik Setsaas, Senior Systems Architect, SAP AG</i>	14.25	Round table discussion
15.30	<b>Coffee – sponsored by Entrust</b>		
16.00-18.00	<b>eema Track Round Table Discussion</b>		<b>ENISA Workshop Security Issues in Reputation Systems</b>
	Round table 1 - led by CoreStreet e-ID interoperability challenges and experiences	16.00	Privacy-respecting Reputation systems for future internet communities <i>Sandra Steinbrecher, Dresden University</i>
		16.20	Threat scenarios for a Reputation community <i>Farez Rahman, redkeydigital</i>
	Round table 2 - led by nCipher Is Identity Management really delivering on security?	16.40	Building global Reputation, compliance and issue resolution technology for the e-mail ecosystem - <i>Brandon Phillips &amp; Eric Castelli, Lashback</i>
	Round table 3 - led by BEA Middleware and SOA-based identity management	17.00	Reputation management in distributed systems <i>Roberto Cascella, University of Trento</i>
		17.15	A new approach to PGP's Web of Trust <i>Rolf Haenni &amp; Jacek Jonzy, University of Biel</i>
		17.35	Round table discussion
18.00	Conclusion with a summary of each round table	18.00	Conclusion with a summary of each workshop
19.30	<b>Networking drinks reception</b> in the display area		
20.15	<b>Conference dinner</b> in Radisson SAS hotel Speaker Steve Glagow, VP Marketing Operations, Orange and eema Events Chair		

**European e-Identity Conference  
Programme Day 2**

09.00	<b>eema Track Federated Identity Challenges &amp; Solutions</b>		<b>ENISA Workshop e-Authentication Interoperability e-ID / Government Schemes</b>
	Chairman's introduction & opening remarks	09.00	Chairman's introduction
09.15	Federated identity management, technology and trust <i>Simon Perry, CA</i>	09.10	Authentication Trust Levels <i>Florent Chabaud, French Ministry</i>
		09.25	Authentication in Estonia <i>Tarvi Martens, National Certification Centre, Estonia</i>
09.45	Federated identity as part of an identity solution <i>David Ramirez, Senior Manager, Alcatel-Lucent</i>	09.45	Electronic Passports <i>Zdenek Riha, JRC</i>
		10.00	eID Interoperability Large Scale Pilot, STORK, <i>Frank Leyman, FEDICT, Belgium</i>
10.15	Developing a consistent approach to identity management <i>Keiron Salt, Architecture, Analysis &amp; Design, BT</i>	10.15	Practical experiences with multiple CA interoperability in Sweden - <i>Anthony Whitehead, NordicEdge</i>
		10.30	e-ID as a public utility <i>Neil McEvoy, Consult Hyperion</i>
10.45	<b>Coffee – Sponsored by Entrust</b>		
11.15	<b>eema Track Securing Identity</b>		<b>ENISA Workshop e-Authentication Interoperability Industry and Standards</b>
11.15	Chairman's introduction & opening remarks		
11.30	Secure e-ID management architectures, pre and post issuance phases <i>Zoran Savic, CEO, NetSet Global Solutions</i>	11.15	Strong authentication in banking and beyond <i>Mike Davies, Verisign</i>
		11.30	IdenTrust - an enabler for ID assurance in a global context <i>John Bullard, IdenTrust</i>
12.00	Trust services for signature verification and e-id validation <i>Jon Ølnes, Senior Researcher DNV Research &amp; Innovation</i>	11.45	European banking - requirements and solutions for Authentication Interoperability, <i>Ulrike Linde, Association of German Banks</i>
		12.00	Certipost e-Federated Identity Management <i>Wim Coulier, Certipost</i>
		12.15	Standardised authentication protocols based on the smart card - applicability to the German e-ID card <i>Gisela Meister, Giesecke &amp; Devrient</i>
12.30	Security even outside the corporate network <i>Gerry O'Brien, Avoco Secure</i>	12.30	e-ID Interoperability through ECC standard, <i>Lorenzo Gaston (ECC, Gemalto, CEN)</i>
		12.45	Generic IAM presentation, generic processes for identity and access management FINIS <i>Dr Horst Walther, SiG Software Integration GmbH</i>
13.00	<b>Lunch</b>		
14.00	<b>eema Track Taking the Present to Build the Future</b>	14.00	<b>ENISA Workshop Round Table Discussion</b>
	Chairman's introduction & opening remarks <i>David Goodman – eema Chair</i>		Main issues to discuss:
14.15	Thales <i>Steve Brunswick, Strategy Manager, e-Security</i>		<ul style="list-style-type: none"> <li>• Trust evaluation for Authentication Mechanisms</li> <li>• What are the political issues for interoperability</li> <li>• What are the legal issues for interoperability</li> <li>• Standard descriptions of enrolment procedures</li> <li>• Standard descriptions of privacy features</li> </ul>
14.40	EU citizen's trust in future ID systems & authorities <i>Dr Ruth Halperin, Department of Management, LSE London School of Economics &amp; Political Science, UK</i>		
15.05	The future of e-ID after 2010 <i>Dr Mireille Levy, Head of Identity Management Standards, Identity and Passport Service, UK</i>		
15.30	<b>Coffee – Sponsored by Entrust</b>		

# **Day 1**

## **Biographies**

European e-Identity Conference  
12-13 June 2007, Paris  
Day 1

## **European e-Identity Conference**

### **eema Track Managing Identity**

#### **Franz-Josef Nölke, Siemens**

##### **Bio**

Franz-Josef Nölke, 40 is a seasoned IT professional working on IT-Security since 1995. Actually he is responsible Solution Line Manager for Identity Management & SmartCards Solutions at Siemens Enterprise Communications GmbH. Before this, he worked several years in different industries as a solution architect and senior consultant in large-scale IT-security projects at multi-national companies.

##### **Abstract**

The session will present the overall TISA architectural approach, the interaction of identity management and SmartCards, key findings experienced in many projects and practical examples of industry specific realizations of TISA.

It will demonstrate a proven way of combining industry specific business requirement to electronic identification with technology driven aspects and criteria. The audience may recognize obstacles of own projects in the past and derive alternatives and new approaches in addressing projects with TISA.

#### **Olivier Delos, SEALED**

Olivier Delos (CISSP, CISA), Managing Partner of **SEALED**, is a senior e-Security & e-Solutions consultant with more than 15 years of experience in e-Security.

From a technical background in computer sciences, information security, cryptography, and PKI topics, he acquired, through various major projects, significant experience in business representation and exploitation of these techniques. Mainly through the complete set-up of the Belgacom (and then Certipost) E-Trust Services (Trusted Third Party services such as electronic identity certification & timestamping services) and the implementation of major projects in e-Security within Belgium and Europe.

Through his career, Olivier Delos had the opportunity to manage and intervene as senior consultant in some of the most important projects related to the e-Security in Belgium and their practical implementations such as:

- The PKI certification services for the Belgian electronic identity card (eID),
- PKI solutions and Identity certification services and consultancy services for the European Commission, the Grand-Duchy of Luxembourg (LuxTrust), Belgian Notaries, Accountants, Auditors, etc.,
- e-Bidding services,
- Time Stamping Services
- Electronic registered mail,
- Securing e-invoicing services,
- PKI, eID and eSignatures consultancy for European Commission and some Member States governments.

Through **SEALED**, together with Sylvie Lacroix (CISA), they position themselves as architects of your e-Solutions and e-Security services. "Architect" in the full sense as this covers not only the analysis and design part of these services fitting your business needs but also the organisation, management and follow-up of the realisation of such solutions, either through the writing of RFPs or the selection of the most appropriate solutions builders.

European e-Identity Conference  
12-13 June 2007, Paris  
Day 1

**John Erik Setsaas, SAP**

John Erik Setsaas has been working with directories and identity management for more than 10 years, and has been engaged in several large directory projects world-wide. He has been involved in EEMA for a number of years, and participated in the Challenge-88 in Los Angeles and Challenge-97 in Maastricht. Presentations were held at EEMA conferences in Barcelona 2006, Leuven 2005, Prague 2003, Paris 2001, Paris 1999 and Melbourne in 1997, in addition to numerous other presentations.

John Erik has in-depth knowledge and experience in the areas of identity management, directories and databases, e-mail and security, and was a core member of the CEN/TC251 working group on "Security for healthcare communications".

He is employed as a senior systems architect by SAP in Trondheim, Norway. He is working with specification and design, as well as implementation and documentation of identity management and provisioning solutions.

John Erik Setsaas  
SAP Norway  
Haakon VII's gt 7B  
Trondheim  
Norway  
<http://www.maxware.com>  
<mailto:setsaas@maxware.com>

European e-Identity Conference  
12-13 June 2007, Paris  
Day 1

## **ENISA Workshop**

### **Security Issues in Social Networking**

*Social networking has undergone a huge explosion both in Europe and in the US. Nielsen/NetRatings, estimated that the top 10 social networking sites increased their audience of 46.8 million in 2005 to 68.8 million in April 2006, reaching 45 percent of active Web users.*

*Social Networking sites are now an important forum for everything from political debate to marketing tools. Many high-profile politicians now have Social Networking profiles and many brands have set up a presence - not surprising considering that 30 percent of frequent social networkers trust their peers' opinions when making a major purchase decision, but only 10 percent trust an advertisement.*

*Such exponential growth has led many of the potential technical and social threats to be ignored. Privacy is one of the most important casualties. A sense of false intimacy can result from the idea of being connected to friends, prompting users to post highly sensitive personal information which is available publicly and often permanently. Online caches are sometimes deliberately set up for "data-hostage-taking" and can make removing such posts difficult. By far the majority of users are teenagers who are usually less cautious and more vulnerable. Other common threats include bullying, identity theft, and sexual predators.*

*The Workshop will identify and discuss the threats related to Social Networking through presentations and a roundtable at the end where the audience can participate in the discussion*

#### **Josephine Fraser, Childnet**

Josie Fraser is a UK based social and educational technologist and blogger, currently working as an independent consultant. She has a broad range of experience at institutional, regional and national level, focusing on the use of Open Source and Web 2.0 technologies within formal education. She has worked at local, regional and national level promoting and developing the effective and innovative use of ICT and e-learning. She has a wealth of experience in staff development design, delivery and policy. She has worked with Government and a range of national agencies on a variety of projects, particularly around e-portfolio, personalisation and personal learning environments. She was the sole UK-based expert invited to serve on the New Media Consortium's Horizon Project Advisory Board, a group tasked with future gazing emerging technologies within the education sector. She is currently working with the charity Childnet International for the DfES, producing advice and guidance for schools on cyberbullying, and managing a project investigating the e-safety and e-literacy issues around web 2.0 for children and young people. She also the Community of Practice project manager and technical infrastructure lead for Emerge, a support project for the UK's Joint Information Systems Committee (JISC) User's and Innovation Programme. For the last two years she has managed the International Edublog Awards, and currently chairs Future Learning Online, the UK association for educators using and interested in the potential of social software and user-generated content.

#### **Maz Nadjm, Rareface**

Maz Nadjm, Rareface has worked in web development and multimedia production since 1994. He has held a variety of positions over this time, ranging from raw-level coding to consultancy and technical project management. Maz is an expert in social networking technical matters.

#### **Mathieu Gorge, VigiTrust**

Mathieu Gorge is Managing Director of security consultancy firm VigiTrust (Ireland). He is an Independent Security Expert for the PASR, & the ISCC (International Security Competence Center). His articles are published in the ISSA Journal and Computer Fraud Security Journal. He specializes in Cyber-crime, PCI and ISO 27001 focusing on human aspects of security including social engineering and awareness training. He advises numerous government departments in Ireland and abroad on how to design, develop and implement security strategies.

**ENISA Workshop  
Security Issues in Social Networking cont.**

**Lien Louwagie, Netlog**

Lien Louwagie (b. 1982, Belgium) completed studies in Moral Sciences at the University of Ghent as well as in Cultural Sciences at the University of Brussels. Immediately upon graduating, she began working as a Community Manager for Incrowd BVBA, which served as the production house for Redbox.be (the first Belgian social networking website). Redbox.be is now a part of Netlog.com, which is an Alexa(tm) global top-100 site and Europe's leading portal. Now Community Director for Netlog NV, Lien is responsible for all issues related to the community of Netlog. She currently lives in Ghent, Belgium.

**Alessandro Acquisti, Facebook**

Alessandro Acquisti is an Assistant Professor of Information Technology and Public Policy at the H. John Heinz III School of Public Policy and Management, Carnegie Mellon University, and a member of Carnegie Mellon CyLab. His work focuses primarily on the economics of privacy and information security. His research in these areas has been disseminated through journals (including Marketing Science, IEEE Security & Privacy, and Rivista di Politica Economica); edited books ("Digital Privacy: Theory, Technologies, and Practices." Auerbach, 2007); book chapters; and leading international conferences.

Alessandro has received national and international awards, including the 2005 PET Award for Outstanding Research in Privacy Enhancing Technologies and the 2005 IBM Best Academic Privacy Faculty Award. He is and has been member of the program committees of various international conferences and workshops, including ACM EC, PET, WEIS, ETRICS, WPES, LOCA, QoP, and the Ubicomp Privacy Workshop at Ubicomp. In 2007 he chaired the DIMACS Workshop on Information Security Economics and the WEIS Workshop on the Economics of Information Security.

Alessandro Acquisti has lived and studied in Rome (Laurea, Economics, University of Rome), Dublin (M.Litt., Economics, Trinity College), London (M.Sc., Econometrics and Mathematical Economics, LSE), and in the San Francisco bay area, where he worked with John Chuang, Doug Tygar, and Hal Varian and received a Master and a Ph.D. in Information Management and Systems from the University of California at Berkeley.

**ENISA Workshop  
Security Issues in Reputation Systems**

*The most well-known reputation systems are used on eBay and amazon, but applications of electronic reputation are very widespread, ranging from spam-filtering and anti-phishing tools to vetting of identity documents and peer-to-peer networks.*

*Electronic reputation and its management are now an extremely valuable commodity which should be taken seriously by industry and governments alike. Reputation systems can enhance PKI infrastructures to address many of the social and architectural problems it has faced. For example trust establishment by aggregating opinions is more intuitive for end-users and more scalable than top-down, single-root trust systems. In the government area, proofing and vetting of identity documents already involves informal reputation judgements (via multiple witness-statements).*

*Reputation systems have their own threats however. They suffer from issues such as denial-of-reputation, collusion to falsify reputation, and extortion. Privacy is also a very important issue for reputation systems, since maintaining a good reputation puts pressure on the reputation owner to expose a consistent identity. Also, the more privacy a user has, the more likely they are to report honestly on another user.*

European e-Identity Conference  
12-13 June 2007, Paris  
Day 1

*The Workshop will explore the potential applications of reputation to security problems and the security problems of reputation systems themselves. There will be a roundtable at the end where the audience can participate in the discussion.*

**Sandra Steinbrecher, Dresden University**

Sandra Steinbrecher is a scientific assistant of Computer Science at Dresden University of Technology. Since her diploma that she received from University of Saarland in 2000 she has been working in several projects and areas of privacy, computer security and cryptography. Her major research interests are the modelling and measurement of anonymity in distributed networks, privacy-enhancing identity management and the design of privacy-respecting reputation systems.

**Farez Rahman, Redkey Digital Ltd**

Farez Rahman is an IT consultant with Redkey Digital Ltd, a London-based company specialising in developing systems to support online communities. Farez has a background in software engineering and network security, mainly in the areas of certification, trust and PKIs. His research in trust models for distributed systems led to several publications (one of the earliest in the field) and a PhD from University College London on trust modeling. He is currently interested in pursuing research and development collaborations in this area. His primary interest is to identify key trust factors in very specific application domains in order to build useful and realistic reputation systems.

**W. Brandon Phillips, Lashback LLC**

Chief Executive Officer and Co-Founder

Once the driving force behind national sales efforts in electronics, telecom and software verticals, Brandon now drives the efforts of the LashBack company toward the same fast growth success. He sees the future of email taking a radically different shape as LashBack successfully enforces every person's right to choose what email they wish to receive. Brandon's deep experience in online and traditional marketing, advertising and sales has propelled LashBack to grow by 400% in 2006. By bridging the traditional gap between technology development and sales, he has been able to lead diverse internal efforts such as product development and usability as well as brand and business development with ease. He is a recognized expert on email marketing and its micro and macroeconomic effects on business and consumers. Brandon has been featured by many media outlets including WIRED, eWeek and DM News for his outspoken vision for email. He is available as an expert for litigation support in email related court cases.

**Eric Castelli, Lashback LLC**

Chief Technology Officer and Co-Founder

Eric is the named inventor for LashBack's intellectual property. He has led a team of developers through the launch of five groundbreaking products for consumers and the email industry.

As a recognized compliance and reputation expert for email marketing, Mr. Castelli has actively participated with the Federal Trade Commission in CAN-SPAM rulemakings, enforcement and served as an expert witness in the FTC's 2005 report to Congress. Eric is also a leading voice on developing compliance guidelines, best practices and raising the value of email for consumers and email marketers. He has been invited to speak on these topics by the Authentication and Online Trust Association, The Direct Marketing Association and Return-Path.

Prior to LashBack, Mr. Castelli spent several years in technology consulting across numerous industries, including direct mail and email. These experiences helped drive LashBack's quest to make unsubscribe work for the email community and consumers across the globe. Mr. Castelli graduated from St. Louis University with a degree in business.

European e-Identity Conference  
12-13 June 2007, Paris  
Day 1

**Roberto Cascella, University of Trento**

Roberto G. Cascella received the Degree "Laurea" in Telecommunication Engineering from Politecnico di Torino and the M.Sc. in Electrical Engineering from the Royal Institute of Technology (KTH) in Stockholm both in 2003. During 2002-2003, he was an intern at the Wireless@Kth, Center for Wireless Systems (Stockholm, Sweden), where he performed a M.Sc. thesis on service discovery in reconfigurable networks. Currently, he is a doctoral student at University of Trento where he is working on trust and reputation management schemes. He is also involved in two European projects, CASCADAS and BIONETS, on autonomic communication systems.

**Rolf Haenni, University of Biel**

Rolf Haenni is a lecturer in Computer Science at the Berne University of Applied Sciences in Biel, Switzerland, and an assistant professor in Computer Science at the University of Bern, Switzerland.

He has a diploma and a PhD degree in Computer Science from the University of Fribourg, Switzerland. As a post-doc researcher, he has formerly been involved in the following projects: "Defeasible Reasoning and Management of Uncertainty" (European Basic Research Activity, 1993-1996), "Symbolic and Probabilistic Argumentation Systems" (Swiss National Science Foundation, 1996-1998), "Inference and Deduction: an Integration of Logic and Probability" (Swiss National Science Foundation, 1998-2000), "Inference and Applications of Probabilistic Argumentation Systems" (University of California, Los Angeles, USA, 2001-2002), and "Philosophy, Probability, and Modeling" (University of Konstanz, Germany, 2002-2004). His main research interest is the integration of logical and probabilistic methods in the domain of uncertain reasoning and applications thereof.

**Jacek Jonczyk, University of Biel**

Jacek Jonczyk is a computer scientist and PhD student at the Institute of Computer Science and Applied Mathematics at the University of Berne, Switzerland. He received his BSc and MSc degrees in Computer Science from the University of Fribourg, Switzerland. His research interests include reasoning under uncertainty, trust and authenticity management, cryptography, and network reliability

European e-Identity Conference  
12-13 June 2007, Paris  
Day 2

# **Day 2**

# **Biographies**

European e-Identity Conference  
12-13 June 2007, Paris  
Day 2

## **European e-Identity Conference – Day 2**

### **eema Track Federated Identity Challenges & Solutions**

**Simon Perry, CA**

#### **David Ramirez, Alcatel-Lucent Bio**

David has recently finished his MSc on Information Security at Westminster University, London. He holds several industry certifications including CISSP, CISM and BS7799 Lead Auditor; and technology certifications including MCSE Security and ISS Certified Engineer. David is fluent in English and Spanish.

He began his career as a networking specialist. Subsequently he joined a consulting company managing the Information Risk Management practice implementation where he was involved in risk assessments for more than 80 companies.

In 2002 David moved to a UK Risk Management company as part of their new Information Security division. In that role, he was responsible for developing the methodologies for the practice, covering Penetration testing and ISO 17799 compliance including disaster recovery. During this time he was involved in security projects for Banks in Latin America, Middle East, Far East and North America; plus projects in the areas of Security Awareness, Disaster Recovery & Business Continuity, Security Policies, Security Architecture, Managed Security Services and compliance with international standards.

David joined Lucent's Security Consulting Practice in March 2005; his responsibilities include Technology and Innovation and thought leadership within the practice.

David wrote an IPTV Security chapter for USTA Book on IPTV in June 2005. He has also written articles for several magazines and newspapers on the subject of information security including the IEC Magazine.

#### **Abstract**

The standards based solution to identity and authentication problems comes with the hand of the Federated Identity solutions. Based on previous experiences and the understanding of the building blocks for any Federated identity model, it is important to undertake a review of the existing Identity Management model and map the existing elements against the requirements for a Federated Identity architecture and create a blueprint of the areas already covered by the existing Identity Management (IdM) and those areas that must be implemented. Entities already have many elements required for deploying a Federated Identity Solution; they just need to articulate the elements and add the missing pieces. Federation standards play a critical role in enabling cross-departmental, cross-organizational, cross-security domain integration. Leveraging an existing standard model, cross-domain identity integration can be attained as part of a cost effective and repeatable process.

#### **Keiron Salt, BT**

Keiron has worked across markets sectors for BT and Syntegra for over ten years. He is the lead architect for GUIDE (Government User IDentity for Europe) which is a EU funded Research project.

**eema Track**  
**Securing Identity**

**Zoran Savic, NetSet Global Solutions**

**Abstract**

In this paper, a real design experience and implementation challenges in building complex centralized and distributed e-ID issuing systems are presented.

A robust and secure implementation of the NetSeT IDMS (Identity and Document Management System) architecture is described as well as the role of its components in all e-ID issuing and usage phases: registering, storing, approval, production and on-field identity verification and credential validation.

Introduction and implications of the EAC security mechanism are discussed and challenges of CV (Card Verifiable) certificate management have been addressed. Real experience of implementing complex national Identity-centric management projects with NetSeT IDMS is shown. Special focus is put on NetSeT IDMS security and flexibility, which is based on a secure Web-services technology and fault tolerant J2EE platform. In the paper is discussed how this type of multi-tier architecture is able to match requirements for complete end-to-end "chain of trust" implementation in centralized and distributed e-ID issuing architectures. Finally, we address the importance of a full citizen e-ID life cycle management including post-issuance phase as well. In particular, an efficient and secure national eID validation architecture and its importance for consolidated authentication and access control management have been pointed out.

**Biography**

Zoran Savic holds the B.S.E.E. and M.Sc.C.S. degrees in Electrical Engineering and Computer Sciences from Faculty of Electrical Engineering, University of Belgrade, Serbia. For more than fifteen years he has been a leading researcher and manager of the Computer and network security department at the "Institute of applied mathematics and electronics", Belgrade. In 1999 he joined the National bank of Yugoslavia as a special advisor for secure financial IT infrastructure and development of the new Serbian financial network. He was the founder of the Information Security and Certification Center of the National Bank of Serbia. From 2003 Mr. Savic has been acting as founder and CEO of the companies SmartIS Group and NetSeT Global Solutions.

Recently, as a partner of G&D-Germany he has been leading several e-ID and ICAO e-Passport projects such as the National Issuing System for the Serbian e-ID documents and project of the New National Identity Documents of the Republic of Macedonia.

For more than 10 years Mr Savic has been a lecturer on the Military high-school academy in Belgrade for "*Computer communications and networks*" and "*Secure IT systems*" courses. He is one of the founders of the ASIT - Serbian Association for Computing, Telecommunications and New Media, where he holds a Chairman of the Board position.

His research interests are in the architecture of secure computer systems and networks, integrated hw/sw security solutions, public key infrastructure, secure payment smart card schemes, secure e-ID and ICAO e-Passport issuing and management systems and their applications in e-government.

**Jon ØInes, DNV Research & Innovation**

**Abstract**

The receiver of a digitally signed document (or an e-ID used in any other way) shall ultimately be able to accept any signature regardless of the eID selected by the signer(s) and other characteristics of the signature(s). This must include assessment of quality, trustworthiness and legal status of signatures and eIDs. Trust services for signature verification and eID validation, targeted specifically at the receiver, allow outsourcing of the handling of this complexity. Use of Web Services and XML for requests and responses enables easy integration in service oriented architectures. The receiver obtains validity of eIDs and

European e-Identity Conference  
12-13 June 2007, Paris  
Day 2

signatures, information on quality and legal standing, and further auxiliary information as requested. Such validation functionality is seen as possibly a crucial component for ensuring interoperability of eIDs and signatures.

### **Biography**

Jon Ølnes is senior researcher at DNV Research & Innovation. He is among Norway's most well-known experts in PKI, eID and use of electronic signatures, being active in this area for more than 10 years doing research, consultancy, service development, and lecturing. At present, Jon works on DNV's initiative on trusted validation authority services for eID and signatures. Jon Ølnes has an M.Sc in informatics from the University of Oslo.

DNV R&I is a division of Det Norske Veritas, an independent foundation offering classification and certification services from offices in more than 100 countries.

Jon Ølnes, Senior Researcher  
DNV Research & Innovation  
Veritasveien 1  
N-1322 Høvik  
Norway

jon.olnes@dnv.com  
+47 47846094 (mobile)

### **Gerry O'Brien, Avoco Secure**

#### **Taking the present to build the future**

### **Steve Brunswick, Thales**

### **Dr Ruth Halperin, Dept of Management, LSE London School of Economics & Political Science,**

Dr Ruth Halperin holds a PhD from the London School of Economic and Political Science, where currently she is a Research Fellow in the Information Systems and Innovation Group of the Department of Management. Her current research focuses on the social aspects of Identity in the Information Society. She is a member of the EU funded Network of Excellence FIDIS (Future of Identity in the Information Society) since its inception in 2004 and has co-edited and authored research reports and articles in the areas of Interoperable Identity Management Systems and Profiling. Since 1996, she has undertaken teaching and research in several academic institutions. Prior to joining the LSE in 2002, she was a Project Manager and a member of the product management team of a leading software development company specializing in E-learning and KM technologies.

### **Dr Mireille Levy, Identity & Passport Service, UK**

After a distinguished career in scientific research, Dr Levy joined the UK Home Office in 2001 as the Head of Radio Planning. In 2006, she joined the Identity and Passport Service as the Head of Identity Management Standards, to establish cross-government standards and lead UK international identity management activities. She has extensive experience of EU eID issues and is the UK representative on the European Commission eID Expert Group and IDABC eID Interoperability Expert Group. Dr Levy is a Chartered Engineer, Member of Institution of Engineering and Technology, and a Fellow of the Institute of Mathematics and its Applications.

## ENISA Workshop

### **e-Authentication Interoperability**

*The landscape of Authentication is highly fragmented despite much effort currently being made at a co-ordinated strategy and European and Global levels. The aim of this workshop is to discuss how to make sure that the enormous amounts of work being done lead to an interoperable authentication infrastructure.*

*Our speakers represent all the important pieces of the Authentication Interoperability puzzle:*

- \* *National e-ID card schemes and interoperability pilots*
- \* *Electronic Passports*
- \* *Banking Industry*
- \* *Smart Card Industry*
- \* *Standardization*
- \* *IT consultancy industry*

*The workshop will include a 90 minute roundtable to ensure adequate discussion and will produce a public report which will input to ENISA's Authentication Interop Language Special Interest Group. ENISA is particularly interested in how to evaluate trust in authentication mechanisms for example in large-scale cross-border or web-services environments where the mechanism is potentially unknown to the evaluator.*

### **e-ID/Government Schemes**

#### **Florent Chabaud, French Ministry**

Florent Chabaud got a PhD degree in computer science in cryptography under direction of Professor Jacques Stern in 1996 and became research engineer in information system security for French delegation for armament. In 2000 he joined newly created DCSSI to take the lead of its information technology laboratory. Since 2004, he serves as head of the scientific subdirection of DCSSI, which gathers the three technical laboratories of the directorate: cryptography, information technology, compromising signals.

#### **Tarvi Martens, National Certification Centre, Estonia**

Tarvi Martens, born in 1969, has been a key figure in the Estonian IT and infosecurity field for the past dozen years. He has an MSc degree from Tallinn Technical University, with his thesis being on the theme "On Evidential Value of Digital Signatures".

Tarvi's first major achievement was leading Estonian Data Communication Department, the government agency responsible for building and managing governmental network, from 1993 to 1997. During that period, Internet penetration in Estonian public sector achieved 97%. He has been development director of Cybernetica (1997-2000), was the founder of Cybernetica's spin-off Privador, and led the company as CEO, working in the field of development and sales of communications security and PKI products and services.

Tarvi was among the originators of the Estonian ID card project in 1996 and has been a supporter and dedicated evangelist of it ever since. In 2002, Tarvi joined SK where he laid down the original concept of DigiDoc, the national *de facto* standard in Estonia for digital signatures. Today, this work is about to go international.

In 2003 Tarvi started with the e-voting project with National Electoral Committee in order to provide Estonian electoral system with Internet voting capability. As a result there were elections in autumn 2005 where Internet voting was official and accessible for the whole nation in the very first time in the history.

Tarvi has often written articles and given presentations at various events to popularise the Internet usage and applications in Estonia. He was also the author of first original Estonian book about the Internet in 1996.

**Zdeněk Říha, European Commission**

Zdeněk Říha graduated from the Faculty of Informatics, Masaryk University in Brno, where he also received his Ph.D. in 2002. In 2004 he graduated from the Faculty of Economy and Administration of the Masaryk University. He works as an Assistant professor at the Faculty of Informatics of the Masaryk University in Brno. Currently he is seconded to the Joint Research Centre (JRC) of the European Commission in Ispra in Italy, where he takes part in the Border Security action within the Institute for the Protection of the Security of the Citizen. His research interests include PKI, biometric systems and the security of electronic documents and operating systems.

**Frank Leyman, FEDICT**

Frank Leyman holds a degree in Marketing and in Applied Economics from the University of Mons in Belgium. He started his career with IBM Belgium as a telecom Marketing specialist. After 6 years he joined the Belgian national Telecom operator BELGACOM where he was in charge of setting up the Corporate Services Sector. After 3 year he was appointed as Distribution Channels Director for the Belgacom Group. In 1999 he left Belgacom for a more international career by joining the company PROTON WORLD. This company is specialized in large scale smartcard based projects. He has been in charge of business development in the Middle-East and African Region and has co-developed the complete Government offering. Since mid 2005 he works for FEDICT (the Federal Public Service for ICT) where he manages International Relations as well as the relations with European Commission, UN and OECD. He is 45, married and has 2 boys.

**ENISA Workshop  
e-Authentication Interoperability**

**Mike Davies, Regional Marketing Director, VeriSign EMEA**

Davies joined VeriSign from Visa Europe, where he was marketing network services to Visa member banks through which he gained a deep understanding of the payment processing environment. Previously, he was at Thales, where he helped lead the rollout of Smart cards primarily into the financial and government sectors. Whilst at Thales, Davies acted as vice chair of the Marketing Committee of GlobalPlatform, an industry body setting standards for multi application smart cards.

Davies' involvement with online security dates back to his experience working in the technology arm of the Royal Mail as part of the Emerging Technologies division, where he was responsible for taking PKI and SSL solutions to market.

Davies gained a BA (hons) Business studies from the University of Plymouth Business School.

**Ulrike Linde, Association of German Banks**

Ms Ulrike Linde, Division Manager in the Department for Retail Banking and Banking Technology at the Association of German Banks, co-ordinates the development of electronic services such as online banking and internet payment systems. Secure identification on the internet is of fundamental importance in this context.

**ENISA Workshop  
Authentication Interoperability**

**Anthony Whitehead**

Anthony Whitehead is a British national currently living and working in Sweden for NordicEdge as a systems integrator and security expert. His current assignments include strong authentication solutions and secure identity management for several large Swedish organisations. Previous to NordicEdge, Anthony was employed at the Swedish Social Security Agency as a UNIX and infrastructure technician.

**John G Bullard, IdenTrust**

Global Ambassador, IdenTrust Inc. John has a background of over 20 years in banking- with Barclays in the UK, US (California 1980's & Wall Street 1990's), and Europe; responsibilities centered primarily around business management for Financial Institutions and Corporate Banking; in the mid 90's he "crossed the Rubicon"/crossed the Business/Tech divide, and Director Barclays Computer Operations responsible for BizDev/Partnering externally, and then Director Group Operational Risk (eCommerce) at Barclays corporate HQ.

John joined IdenTrust at its original foundation in 1999 as a bank consortium (Barclays was a founder shareholder), and has managed much of the worldwide (mainly non US) external-facing issues, as the young enterprise charted its way through its early years.

Now as Global Ambassador, he brings a wealth of experience and insight particularly from the end-Customer perspective about what is needed in managing operational risk for businesses and the Public Sector in the era of a global "Network Economy".

John is based at IdenTrust's offices in London with a team focused on successful partnering and collaborative working in the e-ID space

**Neil McEvoy, Consult Hyperion**

Neil McEvoy Consult Hyperion is the managing director of Consult Hyperion, of which he was one of the founders in 1986. In the field of Digital Identity, Neil is currently leading the team specifying a smart Public Services Card for the Republic of Ireland and the team acting as client technical advisors for an identity card project in a major Middle Eastern nation. Previously he led the Consult Hyperion team specifying Hong Kong's smart identity card.

**Wim Coulier, Certipost**

Wim Coulier graduated as Engineer in Electromechanics and postgraduated in Multimedia & Virtual Reality. He started his career at Procter & Gamble as Research Associate in the packaging domain, but soon oriented himself in IT. He pursued his IT career further at Belgacom as Project Manager for complex to very complex customer projects. Working with the Belgacom E-Trust Certificate Authority team, Wim became an expert in Identity Management. This included a.o. Project Leadership of the FedPKI project for the Belgian government which included the full analysis covering all aspects regarding the set-up of a full grown PKI environment (including Time Server, Time Stamping, OCSP, SRAO, ...). As a natural follow up Wim took on the technical coördination and quality assurance of the Certification Services related descriptive deliverables for the Belgian eID card. When the new company Certipost ([www.certipost.be](http://www.certipost.be)) was created, Wim, together with the whole E-Trust team, was transferred from Belgacom to Certipost.

Currently Wim is active in the following areas:

- Customer consultancy: Consultancy projects for customers regarding strategic new products / projects that require authentication and attribution of external users or require consolidated and secured communication services.
- Product management and business development of Certipost e-Federated Identity Management, the Certipost ASP offering for Federated Identity Management, as a solution for complex Identity & Access Management situations involving a lot of organization external players. A basic version of this is currently marketed as Certipost SSO.
- Product management and business development of Certipost e-Signing, the Certipost ASP offering for the creation of electronic signatures with guarantee of legal equivalent to handwritten signature, see [www.e-signing.be](http://www.e-signing.be).

European e-Identity Conference  
12-13 June 2007, Paris  
Day 2

- Chairman of the Certipost PKI management board: The Certipost PKI management board manages all decisions related to the Certipost CSP activities (including the Belgian eID certificate CSP activities)

**Gisela Meister, Giesecke & Devrient**

Study of Mathematics and Economics at the University Münster, since end of 1989 occupied as security expert with G&D Munich, division Smart Cards. She is head of the department "Security & Evaluation" as well as head of the Standardisation office with G&D. Gisela Meister is a member of national and international standardisation groups and co-ordinates national and European specifications e.g. she is the convenor of the national smart card body for contact oriented cards DIN NI 17.4 as well as the chair of the German DIF group for smart cards and she chairs the European Smart Card standardisation group for PKI CEN TC 224 WG 16. Fraunhofer Smart card prize 2004.

**Lorenzo Gaston, ECC, Gemalto, CEN**

**Dr Horst Walther**

- president of the SiG Software Integration GmbH
- partner of Kuppinger, Cole + Partner
- founder of the initiative GenericIAM

Dr. Horst Walther is a Partner at Kuppinger Cole + Partner, a leading German analyst group focusing on issues of Digital Identity, Identity Management and IT security. He initially studied chemistry, business and computer science, completing his PhD in theoretical chemistry. Since 1975 he has worked in the computer industry as a consultant and project engineer. He is the founder of SiG Software Integration Inc., a provider of management and consulting services to major corporations in the fields of IT, financial services, automotive, chemicals, shipping and other verticals. At KCP he focuses on generic IAM processes, project management, it-audits and it-strategy issues. He is founder and speaker of the standardization initiative GenericIAM.