EuroPKI 2011 Programme

Thursday, September 15th, 2011

09:00 – 09:15 Opening – Welcome

09:15 – 10:45 Session 1: Authentication Mechanisms
Chair: Javier Lopez

Secret Handshake Scheme with Request-Based-Revealing
*Yutaka Kawai and Noboru Kunihiro*

Password Based Signatures
*Oystein Thuen and Kristian Gjøsteen.*

Isolating Partial Information of Indistinguishable Encryptions
*Jean Lancrenon and Roland Gillard*

10:45 – 11:15 Coffee Break

11:15 – 12:15 Keynote Talk
Chair: Andreas Pashalidis

New architectures for identity management - unifying security infrastructures
Chris Mitchell, Royal Holloway, University of London

12:30 – 14:00 Lunch

14:00 – 17:00 LSEC Event --- Program (tentative)

14:00 – 14:15 Introduction
Ulrich Seldeslachts, CEO LSEC

14:15 – 15:00 Overview of PKI developments and services
Jack Straw, Professional Services Manager, Verizon Business Ireland

15:00 – 15:30 Overview of PKI developments and services
Wim Mintiens, Certipost

15:30 – 16:00 Coffee Break

16:00 – 16:30 Overview of PKI developments and services
Bart Renard (tbc), Vasco Data Security

16:30 – 17:00 Panel Discussion on future research topics and business use cases

17:00 Concluding remarks
09:00 – 10:30  Session 2: Privacy Preserving Techniques  
Chair: Andreas Pashalidis  

Design and Evaluation of a Privacy-Preserving Architecture for Vehicle-to-Grid Interaction  
Mark Stegelmann and Dogan Kesdogan  

Insider attacks and privacy of RFID protocols  
Ton Van Deursen and Sasa Radomirovic.  

Cell-based Roadpricing  

10:30 – 11:00  Coffee Break  

11:00 – 12:00  Keynote Talk  
Chair: Svetla Nikova  

Running Mixnet-Based Elections with Helios  
Olivier Pereira (UCL, Belgium)  

12:30 – 14:00  Lunch  

14:00 – 15:00  Keynote Talk  
Chair: Bart Preneel  

PKI as Part of an Integrated Risk Management Strategy for Web Security  
Peter Gutmann, University of Auckland  

15:00 – 15:30  Session 3: PKI Applications  
Chair: Eric Verheul  

A PKI-based mobile banking demonstrator  
Karel Wouters, Gauthier Van Damme and Nicolas Luyckx.  

15:30 – 16:00  Coffee Break  

16:00 – 16:30  Session 3: PKI Applications (continued)  
Chair: Eric Verheul  

Certification Validation: Back to the Past  
Moez Ben Mbarka and Julien Stern  

16:30 – 17:30  Session 4: Secure Applications  
Chair: Chris Mitchell  

A Hijacker’s Guide to the LPC Bus  
Johannes Winter and Kurt Dietrich  

Secure Event Logging in Sensor Networks  
An Braeken, Antonio De La Piedro and Karel Wouters  

17:30 Closing