1st EURO_PKI

1st European PKI Workshop: Research and Applications

June 25-26, 2004, Samos island, GREECE

www.aegean.gr/EuroPKI2004

University of the Aegean
Greece

Workshop Programme

Thursday, June 24

18:00-21:00 **Registration ("Samaina Inn" Hotel)**

20.45-22:00 ***Cocktail (by the "Samaina Inn" Hotel pool)***

Friday, June 25

8:30-9:00 **Registration**

9:00-9:10 **Opening: Prof. Sokratis K. Katsikas, University of the Aegean, Greece, Workshop General Chair**

9:10-10:00 **Keynote address: *"PKI: Past, Present, and Future"*, Prof. David W. Chadwick, University of Salford, UK**

10:00-10:15 ***Coffee/Tea/Refreshments Break***

10:15-11:55 **Session Chair: Sokratis K. Katsikas, University of the Aegean, Greece**

Introduction to the Belgian EID card: *Danny De Cock, Karel Wouters, and* ***Bart Preneel*** *(Katholieke Universiteit Leuven, Belgium)*

The EuroPKI experience: ***Antonio Lioy****, Marius Marian, Natalia Moltchanova, and Massimiliano Pala (Politecnico di Torino, Italy)*

CERVANTES - A Certificate Validation Test-bed: ***Jose L. Muñoz,*** *Jordi Forne, Oscar Esparza, and Miguel Soriano (Technical University of Catalonia, Spain)*

Flexible and Scalable Public Key Security for SSH: *Yasir Ali, and* ***Sean Smith*** *(Dartmouth College, USA)*

11:55-12:15 ***Coffee/Tea/Refreshments Break***

12:15-13:30 **Session Chair: Bart Preneel, Katholieke Universiteit Leuven, Belgium**

What is Possible with Identity Based Cryptography for PKIs and What Still Must Be Improved: ***Benoit Libert*** *(UCL, Belgium and Ecole Polytechnique, France), and Jean-Jacques Quisquater (UCL, Belgium)*

Identity-based Cryptography in Public Key Management: ***Dae Hyun Yum****, and Pil Joong Lee (POSTECH, Republic of Korea)*

Pre-production Methods of a Response to Certificates with the Common Status -- Design and Theoretical Evaluation: ***Satoshi Koga*** *(Kyushu University, Japan), Jae-Cheol Ryou (Chungnam National University, Korea), and* ***Kouichi Sakurai*** *(Kyushu University, Japan)*

13:30-15:00 ***Lunch Break***

15:00-16:15 **Session Chair: Spyros Kokolakis, University of the Aegean, Greece**

Filling the Gap between Requirements Engineering and Public Key/Trust Management Infrastructures: ***Paolo Giorgini*** *(University of Trendo, Italy), Fabio Massacci (University of Trendo, Italy), John Mylopoulos (University of Trendo, Italy and University of Toronto, Canada), and Nicola Zannone (University of Trendo, Italy)*

A Framework for Evaluating the Usability and Utility of PKI-enabled Applications: ***Tobias Straub****, and Harald Baier (Darmstadt University of Technology, Germany)*

Using LDAP Directories for Management of PKI Processes: ***Vangelis Karatsiolis*** *(Technische Universitat Darmstadt and Fraunhofer Institute for Secure Telecooperation, Germany), Marcus Lippert (Technische Universitat Darmstadt, Germany), and Alexander Wiesmaier (Technische Universitat Darmstadt, Germany)*

16:15-16:35 ***Coffee/Tea/Refreshments Break***

16:35-18:20 **Session Chair: Gerald Guirchmayr, University of Vienna, Austria**

Recursive Certificate Structures for X.509 Systems: ***Selwyn Russell*** *(Queenslad University of Technology, Australia)*

A Probabilistic Model for Evaluating the Operational Cost of PKI-based Financial Transactions: ***Agapio Platis***, *Costas Lambrinoudakis, and Asimakis Leros (University of the Aegean, Greece)*

A practical approach of X.509 Attribute Certificate Framework as support to obtain Privilege Delegation: *Jose A. Montenegro, and Fernando Moya (University of Malaga, Spain)*

TACAR - A simple and fast way for building trust among PKIs: *Diego R. Lopez (RedIRIS, Spain)*, ***Chelo Malagon*** *(RedIRIS, Spain), and Licia Florio (TERENA, The Netherlands)*

On the Synergy Between Certificate Verification Trees and PayTree-Like Micropayments: ***Josep Domingo-Ferrer*** *(Universitat Rovira i Virgili, Catalonia, Spain)*

19:50 ***Gala Dinner***

Saturday, June 26

9:15-10.30 **Session Chair: Costas Lambrinoudakis, University of the Aegean, Greece**

A Socially Inspired Reputation Model: ***Nicola Mezzetti*** *(University of Bologna, Italy)*

Using EMV Cards for Single Sign-On: ***Andreas Pashalidis***, *and Chris J. Mitchell (Royal Holloway, University of London, UK)*
Distributing Security-Mediated PKI: ***Gabriel Vanrenen***, *and Sean Smith (Dartmouth College, USA)*

10.30-10:50 ***Coffee/Tea/Refreshments Break***

10:50-12:05 **Session Chair: Stefanos Gritzalis, University of the Aegean, Greece**

Distributed CA-based PKI for Mobile Ad hoc Networks using Elliptic Curve Cryptography: ***Charikleia Zouridaki*** *(George Mason University, USA), Brian L. Mark (George Mason University, USA), Kris Gaj (George Mason University, USA), and Roshan K. Thomas (McAfee Research, Network Associates, Inc., USA)*

AETHER - An Authorization Management Architecture for Ubiquitous Computing: ***Patroklos G. Argyroudis,*** *and Donal O'Mahony (University of Dublin, Trinity College, Ireland)*

Trustworthy Accounting for Wireless LAN Sharing Communities: ***Elias C. Efstathiou***, *and George C. Polyzos (Athens University of Economics and Business, Greece)*

12:05-12:25 ***Coffee/Tea/Refreshments Break***

12:25-13:35 **Session Chair: Antonio Lioy, Politecnico di Torino, Italy**

Mobile Qualified Electronic Signatures and Certification on Demand: ***Heiko Rossnagel*** *(Johann Wolfgang Goethe University Frankfurt, Germany)*

Performance Evaluation of Certificate Based Authentication in Integrated Emerging 3G and Wi-Fi Networks: ***George Kambourakis*** *(University of the Aegean, Greece), Angelos Rouskas University of the Aegean, Greece), and Dimitris Gritzalis (Athens University of Economics and Business, Greece)*

A Credential Conversion Service for SAML-based scenarios: *Oscar Cánovas*, ***Gabriel López***, *and Antonio F. Gómez-Skarmeta (University of Murcia, Spain)*

A New Design of Privilege Management Infrastructure with Binding Signature Semantics: ***Kemal Bicakci***, *and Nazife Baykal (Middle East Technical University, Turkey)*

13:35-15:00 ***Lunch break***

15:00-16:40 **Session Chair: Javier Lopez, University of Malaga, Spain**

How to Qualify Electronic Signatures and Time stamps: ***Detlef Huehnlein*** *(secunet Security Networks AG, Germany)*

An Efficient Revocation Scheme for Stateless Receivers: ***Yong Ho Hwang*** *(POSTECH, Korea), Chong Hee Kim (POSTECH and Samsung Electronics Co., Korea), and Pil Joong Lee (POSTECH, Korea)*

On the use of Weber Polynomials in Elliptic Curve cryptography: ***Elisavet Konstantinou*** *(Computer Technology Institute and University of Patras, Greece), Yannis Stamatiou (Computer Technology Institute and University of the Aegean, Greece), and Christos Zaroliagis (Computer Technology Institute and University of Patras, Greece)*

Threshold Password-Based Authentication Using Bilinear Pairings: *Songwon Lee (Information and Communications University, Korea)*, ***Kyusuk Han*** *(Information and Communications University, Korea), Seok-kyu Kang (Information and Communications University, Korea), Kwangjo Kim (Information and Communications University, Korea), and So Ran Ine (NITZ. Corp., Korea)*

50’ **Round Table: Identifying and Overcoming Obstacles to PKI Deployment and Usage**

17:30 **Workshop closing - "2nd European PKI Workshop" announcement**