

Goals and Topics of Interest

The most significant changes that have resulted from the rapid technological evolution in Information and Communication Technologies (ICT) are related to the way private & public sector organizations transform their conventional operating models to internet-based service models (eBusiness, eCommerce & eGovernment). Specifically, companies, institutions and organizations, irrespective of their size, are utilizing the Internet for communicating with their customers, suppliers and partners, for facilitating the interconnection of their employees and branches, for connecting to their back-end data systems and for performing commercial transactions. In such an environment new dependencies and risks arise.

Public Key Infrastructure (PKI) is probably one of the most important items in the arsenal of security measures that can be brought to bear against the aforementioned growing risks and threats. Furthermore, **Public Key Cryptography (PKC)** services and applications make steady inroads into the various information security solutions needed, providing genuine benefits in selected application areas.

The 7th *European Workshop on Public Key Services, Applications and Infrastructures (EuroPKI'10)* will provide an international forum for researchers and practitioners to exchange information regarding advancements in the state of the art and the practical aspects of Public Key services, applications and infrastructures.

EuroPKI'10 seeks papers, work-in-progress reports and presentation of applications – services – practical experiences on topics related, but not limited to:

- Anonymity
- Applications of PKI & PKC
- Architecture & Modeling
- Authentication
- Authorization and Delegation
- Bridge CA
- Case Studies
- Certificates Status
- Certification Policy & Practices
- Credentials
- Cross Certification
- Cryptanalysis & protocol Weaknesses
- Digital Signatures
- Directories
- Distributed Crypto-Computing
- eCommerce / eGovernment
- Evaluation
- Fault-Tolerance and reliability
- Federations
- Formal methods
- Group signatures
- Identification
- Identity-Based schemes
- Identity Management & eID
- Implementations
- Interoperability
- Key Agreement / Establishment
- Key Management
- Legal issues
- Long-time archiving
- Mobile PKI
- Multi-Party/Group Protocols
- Multi-signatures
- Novel Public-key Cryptosystems
- Optimization
- PKC e-voting schemes
- Policies & Regulations
- Privacy
- Privilege Management
- Protocols
- Reliability in PKI
- Repositories
- Risk & attacks
- Standards
- Threshold Cryptosystems
- Timestamping
- Trust management
- Trusted Computing
- Ubiquitous scenarios
- Usage Control
- Verification
- Web services security

Call for papers
23 - 24 September, 2010
Athens, Greece



Special Issue on
Mathematical &
Computer Modelling
in Public Key Services &
Infrastructures
(EUROPKI 2010)



Important dates

Submission deadline:

~~May 16, 2010~~

Extended to May 28, 2010

Notification to authors:

~~June 27, 2010~~ July 2, 2010

Camera-ready version:

July 18, 2010

General co-Chairs

Gollmann, Dieter

Hamburg University of
Technology-TUHH (Germany)

Gritzalis, Stefanos

University of the Aegean (Greece)

Program Committee co-Chairs

Camenisch, Jan

IBM Research - Zurich (Switzerland)

Lambrinoudakis, Costas

University of Piraeus (Greece)

Organized by the
Department of Digital Systems,
University of Piraeus, Greece



For more information:
<http://www.ds.unipi.gr/europki10>

EuroPKI'10

23 - 24 September, 2010
Athens, Greece

Submission Details

Authors are invited to submit original papers not previously published nor submitted in parallel for publication to any other conference, workshop or journal. All submissions will be blind reviewed by at least three reviewers.

As in previous years it is planned to have post-proceedings published by Springer in the Lecture Notes in Computer Science (LNCS) series. All submissions should comply with the "Authors Instructions" that can be found at: <http://www.springer.de/comp/lncs/authors.html> and should not exceed 16 pages including references (Appendices are not included in the 16-page limit but, in case the paper is accepted for publication, they will be removed from the camera ready version).

The submission must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. It should begin with a title, a short abstract, and a list of keywords. Submissions not meeting these guidelines risk rejection without consideration of their merits.

Papers must be submitted electronically in PDF format. A detailed description of the electronic submission procedure is available at <http://www.ds.unipi.gr/europki10/psub.php>

Authors should note that, after the Workshop, a Special Issue of EuroPKI'2010 with extended versions of the best workshop papers will be published in the **Mathematical and Computer Modelling journal, Elsevier**. The papers included in this special issue will undergo another review round.

For further inquiries, please contact one of the program committee chairs at clam@unipi.gr or jca@zurich.ibm.com

7th European Workshop on Public Key Services, Applications and Infrastructures

Program Committee Members

- I. Agudo *University of Malaga (Spain)*
- L. Batina *Katholieke Universiteit Leuven (Belgium)*
- D. Chadwick *Kent University (UK)*
- M. Cremonini *University of Milano (Italy)*
- S. De Capitani di Vimercati *University of Milano (Italy)*
- C. Diaz *K.U.Leuven (Belgium)*
- R. Di Pietro *University of Rome III (Italy)*
- S. Farrell *Trinity College Dublin (Ireland)*
- S. Furnell *University of Plymouth (UK)*
- D. Galindo *University of Luxembourg (Luxembourg)*
- J. Gonzalez-Nieto *Queensland University of Technology (Australia)*
- J. Guajardo *Philips Research Europe (Netherlands)*
- J. Hoepman *Radboud University Nijmegen (Netherlands)*
- S. Katsikas *University of Piraeus (Greece)*
- S. Kent *BBN Technologies (USA)*
- D. Kesdogan *University Siegen (Germany)*
- E. Konstantinou *University of the Aegean (Greece)*
- D. Lekkas *University of the Aegean (Greece)*
- A. Lioy *Politecnico di Torino (Italy)*
- J. Lopez *University of Malaga (Spain)*
- D. M'Raihi *Verisign (USA)*
- F. Martinelli *National Research Council (Italy)*
- S. Mauw *University of Luxembourg (Luxembourg)*
- C. Meadows *NRL (USA)*
- A. Meliones *University of Piraeus (Greece)*
- C. Mitchell *Royal Holloway College (UK)*
- S. Mjolsnes *Norwegian University of Science & Technology (Norway)*
- Y. Mu *University of Wollongong (Australia)*
- D. Naccache *ENS (France)*
- S. Nikova *Katholieke Universiteit Leuven and University of Twente (Belgium)*
- C. Ntantogian *University of Athens (Greece)*
- M. Pala *Dartmouth College (USA)*
- O. Pereira *UCL (Belgium)*
- G. Pernul *University of Regensburg (Germany)*
- D. Polemi *University of Piraeus (Greece)*
- B. Preneel *Katholieke Universiteit Leuven (Belgium)*
- S. Radomirovic *University of Luxembourg (Luxembourg)*
- P. Rizomiliotis *University of the Aegean (Greece)*
- P. Samarati *University of Milan (Italy)*
- R. Scandariato *Katholieke Universiteit Leuven (Belgium)*
- S. Smith *Dartmouth College (USA)*
- Y. Stamatou *University of Ioannina (Greece)*
- C. Xenakis *University of the Piraeus (Greece)*
- J. Zhou *Institute for Infocomm Research (Singapore)*

Organized by the
Department of Digital Systems,
University of Piraeus, Greece



For more information:
<http://www.ds.unipi.gr/europki10>