Preface

This book contains the postproceedings of the 6th European Workshop on Public Key Services, Applications and Infrastructures, which was held at the CNR Research Area in Pisa, Italy, in September 2009.

The EuroPKI workshop series focuses on all research and practice aspects of public key infrastructures, services and applications, and welcomes original research papers and excellent survey contributions from academia, government, and industry. Previous events of the series were held in: Samos, Greece (2004); Kent, UK (2005); Turin, Italy, (2006); Palma de Mallorca, Spain, (2007); and Trondheim, Norway (2008).

From the original focus on public key infrastructures, EuroPKI interests expanded to include advanced cryptographic techniques, applications and (more generally) services. The Workshops brings together researchers from the cryptographic community as well as from the applied security community, as witnessed by the interesting program.

Indeed, this volume holds 18 refereed papers and the presentation paper by the invited speaker, Alexander Dent. In response to the EuroPKI 2009 call for papers, a total of 40 submissions were received. All submissions underwent a thorough blind review by at least three Program Committee members, resulting in careful selection and revision of the accepted papers. After the conference, the papers were revised and improved by the authors before inclusion in this volume.

We thank all the people who have contributed to the success of this workshop: the submitters, the authors, the invited speaker, the members of the Program Committee, the members of the Local Organization Committee, the staff at Springer, the sponsor IIT-CNR for its support, and finally all the workshop participants. It was our pleasure to serve the EuroPKI community as program chairs. We are confident that the EuroPKI workshop will remain a valuable forum for the exchange of experiences and ideas.

June 2010

Fabio Martinelli
Bart Preneel
EuroPKI 2009

The 6th European Workshop on Public Key Services, Applications and Infrastructures

CNR Research Area, Pisa, Italy

September 10–11, 2009

Organized by the Institute of Informatics and Telematics of the National Council of Research (IIT-CNR)

General Chair

Anna Vaccarelli, National Research Council, Italy

Program Chairs

Fabio Martinelli National Research Council, Italy
Bart Preneel Katholieke Universiteit Leuven, Belgium

Program Committee

C. Boyd Queensland University of Technology, Australia
D. Chadwick Kent University, UK
C. Cremers ETH Zurich, Switzerland
G. Danezis Microsoft Research, UK
G. Dini University of Pisa, Italy
J. Domingo-Ferrer Universitat Rovira i Virgili, Catalonia
S. Farrell Trinity College Dublin, Ireland
D. Galindo University of Luxembourg, Luxembourg
K. Gjosteen NTNU, Norway
S. Gritzalis University of the Aegean, Greece
J.-H. Hoepman TNO and Radboud University Nijmegen, The Netherlands
A. Jøsang University of Oslo, Norway
S. Katsikas University of Piraeus, Greece
S. Kent BBN Technologies, USA
K. Kursawe Philips Research, The Netherlands
VIII Organization

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

C. Mitchell
Royal Holloway, University of London, UK

S. Mjølsnes
NTNU, Norway

D. Naccache
ENS Paris, France

E. Okamoto
Tsukuba University, Japan

R. Oppliger
eSECURITY Technologies, Switzerland

M. Pala
Dartmouth College, USA

T. Pedersen
Cryptomathic, Denmark

O. Pereira
Université Catholique de Louvain, Belgium

G. Pernul
University of Regensburg, Germany

R. Di Pietro
University of Rome III, Italy

B. Preneel
Katholieke Universiteit Leuven, Belgium

I. Agudo Ruiz
University of Malaga, Spain

A. Sadeghi
Ruhr-Universität Bochum, Germany

P. Samarati
University of Milan, Italy

R. Scandariato
Katholieke Universiteit Leuven, Belgium

S. Smith
Dartmouth College, USA

J. Zhou
Institute Infocomm Research, Singapore

External Reviewers

Baptiste Alcalde
Claudio Ardagna
Frederik Armknecht
Christian Broser
Lukasz Chmielewski
Claudio Cicconetti
Alessandro Colantonio
Ton van Deursen
Gianluca Dini
Markulf Kohlweiss
Stefan Dürbeck
Christoph Fritsch

Sebastian Gajek
Dimitris Geneiatakis
John Iliadis
Rieks Joosten
Elisavet Konstantinou
Benoit Libert
Jun Pang
Bo Qin
Scott A. Rea
Evangelos Rekleitis
Alfredo Rial Duran
Moritz Riesner

Peter van Rossum
Stefan Schiffler
Koen Simoens
Angelo Spognardi
Douglas Stebila
Klara Stokes
Patrick Tsang
Marcel Winandy
Qianhong Wu
Michele Zanda
Lei Zhang
# Table of Contents

## Certificateless Encryption

A Brief Introduction to Certificateless Encryption Schemes and Their Infrastructures .................................................. 1  
*Alexander W. Dent*

## Certificates and Revocation

*Gabriel A. Weaver, Scott Rea, and Sean W. Smith*

Resource Management with X.509 Inter-domain Authorization Certificates (InterAC) .................................................. 34  
*Vishwas Patil, Paolo Gasti, Luigi Mancini, and Giovanni Chiola*

Reducing the Cost of Certificate Revocation: A Case Study .......... 51  
*Mona H. Ofigsbø, Stig Frode Mjølnes, Poul Heegaard, and Leif Nilsen*

## Cryptographic Protocols

Automatic Generation of Sigma-Protocols .................................... 67  
*Endre Bangerter, Thomas Briner, Wilko Henecka, Stephan Krenn, Ahmad-Reza Sadeghi, and Thomas Schneider*

A Secure and Efficient Authenticated Diffie–Hellman Protocol .......... 83  
*Augustin P. Sarr, Philippe Elbaz-Vincent, and Jean-Claude Bajard*

Key Management for Large-Scale Distributed Storage Systems .......... 99  
*Hoon Wei Lim*

## PKI in Practice

Nationwide PKI Testing – Ensuring Interoperability of OCSP Server and Client Implementations Early during Component Tests .......... 114  
*Christian Schanes, Andreas Mauczka, Uwe Kirchengast, Thomas Grechenig, and Sven Marx*

On Device Identity Establishment and Verification ......................... 130  
*Roberto Gallo, Henrique Kawakami, and Ricardo Dahab*

ABUSE: PKI for Real-World Email Trust ................................. 146  
*Chris Masone and Sean W. Smith*
# Table of Contents

## Encryption and Auctions

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public-Key Encryption with Registered Keyword Search</td>
<td>163</td>
</tr>
<tr>
<td>Qiang Tang and Liqun Chen</td>
<td></td>
</tr>
<tr>
<td>Practicalization of a Range Test and Its Application to E-Auction</td>
<td>179</td>
</tr>
<tr>
<td>Kun Peng and Feng Bao</td>
<td></td>
</tr>
<tr>
<td>Timed-Ephemerizer: Make Assured Data Appear and Disappear</td>
<td>195</td>
</tr>
<tr>
<td>Qiang Tang</td>
<td></td>
</tr>
</tbody>
</table>

## Reputation and User Aspects

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Liveliness for Reputation Systems</td>
<td>209</td>
</tr>
<tr>
<td>Stefan Schiffner, Sebastian Clauss, and Sandra Steinbrecher</td>
<td></td>
</tr>
<tr>
<td>A Multidimensional Reputation Scheme for Identity Federations</td>
<td>225</td>
</tr>
<tr>
<td>Isaac Agudo, Carmen Fernandez-Gago, and Javier Lopez</td>
<td></td>
</tr>
<tr>
<td>On the Usability of User Interfaces for Secure Website Authentication</td>
<td>239</td>
</tr>
<tr>
<td>in Browsers</td>
<td></td>
</tr>
<tr>
<td>Massimiliano Pala and Yifei Wang</td>
<td></td>
</tr>
</tbody>
</table>

## Digital Signatures

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validity Models of Electronic Signatures and Their Enforcement in Practice</td>
<td>255</td>
</tr>
<tr>
<td>Harald Baier and Vangelis Karatsiolis</td>
<td></td>
</tr>
<tr>
<td>Biometric Identity Based Signature Revisited</td>
<td>271</td>
</tr>
<tr>
<td>Neyire Deniz Sarier</td>
<td></td>
</tr>
<tr>
<td>How to Construct Identity-Based Signatures without the Key Escrow Problem</td>
<td>286</td>
</tr>
<tr>
<td>Tsz Hon Yuen, Willy Susilo, and Yi Mu</td>
<td></td>
</tr>
</tbody>
</table>

## Author Index

<table>
<thead>
<tr>
<th>Author Index</th>
<th>303</th>
</tr>
</thead>
</table>