

Fabio Martinelli Bart Preneel (Eds.)

Public Key Infrastructures, Services and Applications

6th European Workshop, EuroPKI 2009
Pisa, Italy, September 10-11, 2009
Revised Selected Papers

 Springer

Volume Editors

Fabio Martinelli
National Research Council (CNR)
Institute of Informatics and Telematics (IIT)
Pisa Research Area, Via G. Moruzzi 1, 56125 Pisa, Italy
E-mail: fabio.martinelli@iit.cnr.it

Bart Preneel
Katholieke Universiteit Leuven
Dept. Electrical Engineering-ESAT/COSIC
Kasteelpark Arenberg 10, Bus 2446, 3001 Leuven, Belgium
E-mail: bart.preneel@esat.kuleuven.be

Library of Congress Control Number: 2010936512

CR Subject Classification (1998): K.6.5, C.2, E.3, D.4.6, J.1, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-16440-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-16440-8 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

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
Bart Preneel

National Research Council, Italy
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. Gjøsteen	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

A. Liou	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. Mjøl̄snes	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	Sebastian Gajek	Peter van Rossum
Claudio Ardagna	Dimitris Geneiataakis	Stefan Schiffner
Frederik Armknecht	John Iliadis	Koen Simoens
Christian Broser	Rieks Joosten	Angelo Spognardi
Lukasz Chmielewski	Elisavet Konstantinou	Douglas Stebila
Claudio Cicconetti	Benoit Libert	Klara Stokes
Alessandro Colantonio	Jun Pang	Patrick Tsang
Ton van Deursen	Bo Qin	Marcel Winandy
Gianluca Dini	Scott A. Rea	Qianhong Wu
Markulf Kohlweiss	Evangelos Rekleitis	Michele Zanda
Stefan Dürbeck	Alfredo Rial Duran	Lei Zhang
Christoph Fritsch	Moritz Riesner	

Table of Contents

Certificateless Encryption

A Brief Introduction to Certificateless Encryption Schemes and Their Infrastructures	1
<i>Alexander W. Dent</i>	

Certificates and Revocation

A Computational Framework for Certificate Policy Operations	17
<i>Gabriel A. Weaver, Scott Rea, and Sean W. Smith</i>	
Resource Management with X.509 Inter-domain Authorization Certificates (InterAC)	34
<i>Vishwas Patil, Paolo Gasti, Luigi Mancini, and Giovanni Chiola</i>	
Reducing the Cost of Certificate Revocation: A Case Study	51
<i>Mona H. Ofigsbø, Stig Frode Mjølunes, Poul Heegaard, and Leif Nilsen</i>	

Cryptographic Protocols

Automatic Generation of Sigma-Protocols	67
<i>Endre Bangerter, Thomas Briner, Wilko Henecka, Stephan Krenn, Ahmad-Reza Sadeghi, and Thomas Schneider</i>	
A Secure and Efficient Authenticated Diffie–Hellman Protocol	83
<i>Augustin P. Sarr, Philippe Elbaz-Vincent, and Jean-Claude Bajard</i>	
Key Management for Large-Scale Distributed Storage Systems	99
<i>Hoon Wei Lim</i>	

PKI in Practice

Nationwide PKI Testing – Ensuring Interoperability of OCSP Server and Client Implementations Early during Component Tests	114
<i>Christian Schanes, Andreas Mauczka, Uwe Kirchengast, Thomas Grechenig, and Sven Marx</i>	
On Device Identity Establishment and Verification	130
<i>Roberto Gallo, Henrique Kawakami, and Ricardo Dahab</i>	
ABUSE: PKI for Real-World Email Trust	146
<i>Chris Masone and Sean W. Smith</i>	

Encryption and Auctions

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

Reputation and User Aspects

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

Digital Signatures

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

Author Index	303
-------------------------------	------------