

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Stig F. Mjølsnes Sjouke Mauw  
Sokratis K. Katsikas (Eds.)

# Public Key Infrastructure

5th European PKI Workshop:  
Theory and Practice, EuroPKI 2008  
Trondheim, Norway, June 16-17, 2008  
Proceedings

## Volume Editors

Stig F. Mjølsnes  
Norwegian University of Science & Technology (NTNU)  
Department of Telematics  
7491 Trondheim, Norway  
E-mail: sfm@item.ntnu.no

Sjouke Mauw  
Université du Luxembourg  
Faculté des Sciences, de la Technologie et de la Communication (FSTC)  
6 rue Richard Coudenhove-Kalergi, 1359 Luxembourg-Kirchberg, Luxembourg  
E-mail: sjouke.mauw@uni.lu

Sokratis K. Katsikas  
University of Piraeus  
Department of Technology Education & Digital Systems  
150 Androutsou St., 18532 Piraeus, Greece  
E-mail: ska@unipi.gr

Library of Congress Control Number: 2008928842

CR Subject Classification (1998): E.3, D.4.6, C.2.0, F.2.1, H.3, H.4, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743  
ISBN-10 3-540-69484-6 Springer Berlin Heidelberg New York  
ISBN-13 978-3-540-69484-7 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 is a part of Springer Science+Business Media  
springer.com

© Springer-Verlag Berlin Heidelberg 2008  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 12320028 06/3180 5 4 3 2 1 0

# Preface

This book contains the proceedings of the 5th European Public Key Infrastructure Workshop: Theory and Practice, EuroPKI 2008, which was held on the NTNU campus Gløshaugen in Trondheim, Norway, in June 2008.

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.

Simply put, public keys are easier to distribute than secret keys. Nevertheless, constructing effective, practical, secure and low cost means for assuring authenticity and validity of public keys used in large-scale networked services remains both a technological and organizational challenge. In a nutshell, this is the PKI problem, and the papers presented herein propose new solutions and insight for these questions.

This volume holds 16 refereed papers including the presentation paper by the invited speaker P. Landrock. In response to the EuroPKI 2008 call for papers, a total of 37 paper proposals were received. All submissions underwent a thorough blind review by at least three PC members, resulting in a careful selection and revision of the accepted papers. The authors came from 10 countries: Belgium, Brazil, Canada, Finland, Germany, Japan, Malaysia, Norway, Spain, and the USA. The accepted papers were organized into the topical sessions: Invited Talk, Certificates, Authentication, Practice, Signatures, Analysis, and Networks.

The use and exploitation of large-scale public key infrastructures have arrived at a slower tempo and perhaps in other directions than originally envisioned a decade ago. A case in point, only 2 out of 16 authors in this workshop found it convenient to provide a digital signature on the copyright transfer form for the submitted paper. So we are not there yet!

We thank all the people who contributed to this workshop: the authors, the invited speaker, the members of the Program Committee, the members of the Organization Committee, the staff at Springer, the sponsors for their support, and finally all the workshop participants. They all made this workshop successful.

June 2008

Stig F. Mjølsnes  
Sjouke Mauw  
Sokratis Katsikas

# Organization

EuroPKI 2008 was hosted by NTNU.

## Chairs

General Chair	Stig F. Mjølsnes, Norwegian University of Science and Technology (Norway)
Program Chairs	Sjouke Mauw, University of Luxembourg (Luxembourg) Sokratis Katsikas, University of Piraeus (Greece)
Organizing Chair	Martin Eian, Norwegian University of Science and Technology (Norway)

## Program Committee

I. Agudo Ruiz, University of Malaga, Spain  
S. De Capitani di Vimercati, University of Milan, Italy  
D. Chadwick, Kent University, UK  
C. Cremers, ETHZ, Switzerland  
M. Cremonini, University of Milan, Italy  
E. Dawson, Queensland University of Technology, Australia  
S. Farrell, Trinity College Dublin, Ireland  
S. Furnell, University of Plymouth, UK  
K. Gjøsteen, Norwegian University of Science and Technology, Norway  
D. Gollmann, Technical University Hamburg, Germany  
S. Gritzalis, University of the Aegean, Greece  
D. Gritzalis, Athens University of Economics and Business, Greece  
J. Guajardo, Philips Research Europe, The Netherlands  
P. Gutmann, University of Auckland, New Zealand  
A. Jøsang, Queensland University of Technology, Australia  
S. Kent, BBN Technologies, USA  
D. Kesdogan, Siegen University, 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  
F. Martinelli, CNR, Italy  
F. Massacci, University of Trento, Italy  
C. Meadows, NRL, USA  
C. Mitchell, Royal Holloway College, UK

S. Mjølunes, Norwegian University of Science and Technology, Norway  
Y. Mu, University of Wollongong, Australia  
E. Okamoto, Tsukuba University, Japan  
R. Oppliger, eSECURITY Technologies, Switzerland  
T. Pedersen, Cryptomathic, Denmark  
G. Pernul, University of Regensburg, Germany  
D. Polemi, University of Piraeus, Greece  
B. Preneel, Katholieke University Leuven, Belgium  
S. Radomirović, University of Luxembourg, Luxembourg  
M. Roe, Microsoft, UK  
C. Rong, University of Stavanger, Norway  
K. Sakurai, Kyushu University, Japan  
R. Sandhu, University of Texas San Antonio, USA  
B. Schoenmakers, Eindhoven University of Technology, The Netherlands  
S. Smith, Dartmouth College, USA  
Y. Stamatou, University of Ioannina, Greece  
G. Tsudik, University of California Irvine, USA  
J. Zhou, Institute for Infocomm Research, Singapore  
S. Zhu, Penn State University, USA  
C. Xenakis, University of Piraeus, Greece

## Organization Committee

Jorunn Sommervold, Peter Herrmann, NTNU  
Ingrid Melve, Torgim Lauritsen, UNINETT

## Sponsoring Institutions

- Department of Telematics, NTNU
- Faculty of Information Technology, Mathematics and Electrical Engineering, NTNU
- UNINETT
- NISNET (Information Security Research Network Project supported by The Research Council of Norway )

# Table of Contents

## Invited Talk

New PKI Protocols Using Tamper Resistant Hardware.....	1
<i>Peter Landrock</i>	

## Certificates

Validation Algorithms for a Secure Internet Routing PKI .....	17
<i>David Montana and Mark Reynolds</i>	
Instant Revocation .....	31
<i>Jon A. Solworth</i>	
Optimized Certificates – A New Proposal for Efficient Electronic Document Signature Validation .....	49
<i>Ricardo Felipe Custódio, Martín A. Gagliotti Vigil, Juliano Romani, Fernando Carlos Pereira, and Joni da Silva Fraga</i>	

## Authentication

An Efficient and Provable Secure Identity-Based Identification Scheme in the Standard Model.....	60
<i>Ji-Jian Chin, Swee-Huay Heng, and Bok-Min Goi</i>	
Trust-Rated Authentication for Domain-Structured Distributed Systems .....	74
<i>Ralph Holz, Heiko Niedermayer, Peter Hauck, and Georg Carle</i>	
Levels of Assurance and Reauthentication in Federated Environments .....	89
<i>Manuel Sánchez, Óscar Cánovas, Gabriel López, and Antonio F. Gómez-Skarmeta</i>	

## Practice

Current Status of Japanese Government PKI Systems .....	104
<i>Yasuo Miyakawa, Takashi Kurokawa, Akihiro Yamamura, and Yasushi Matsumoto</i>	
A Privacy-Preserving eHealth Protocol Compliant with the Belgian Healthcare System .....	118
<i>Bart De Decker, Mohamed Layouni, Hans Vangheluwe, and Kristof Verslype</i>	

## Signatures

Fast Point Decompression for Standard Elliptic Curves . . . . .	134
<i>Billy Bob Brumley and Kimmo U. Järvinen</i>	
An Efficient Strong Key-Insulated Signature Scheme and Its Application . . . . .	150
<i>Go Ohtake, Goichiro Hanaoka, and Kazuto Ogawa</i>	
Efficient Generic Forward-Secure Signatures and Proxy Signatures . . . . .	166
<i>Basel Alomair, Krishna Sampigethaya, and Radha Poovendran</i>	

## Analysis

Fault Attacks on Public Key Elements: Application to DLP-Based Schemes . . . . .	182
<i>Chong Hee Kim, Philippe Bulens, Christophe Petit, and Jean-Jacques Quisquater</i>	
Weaknesses in BankID, a PKI-Substitute Deployed by Norwegian Banks . . . . .	196
<i>Kristian Gjøsteen</i>	

## Networks

An Open Mobile Identity Tool: An Architecture for Mobile Identity Management . . . . .	207
<i>Konstantin Hyppönen</i>	
PEACHES and Peers . . . . .	223
<i>Massimiliano Pala and Sean W. Smith</i>	

<b>Author Index</b> . . . . .	239
-------------------------------	-----