

Preface

Smart cards have been driven by the need for a secure, portable, computing platform. Hence it is no surprise that security considerations dominated their research. The CARDIS conferences were created to provide a forum for this research.

CARDIS 1998 is the third international conference on Smart Card Research and Advanced Applications, held in Louvain-la-Neuve, Belgium, 14-16 September 1998. The first CARDIS was held in Lille, France in November 1994, and the second was held in Amsterdam, The Netherlands in September 1996. The fourth CARDIS is scheduled to take place in Bristol, UK in September 2000 (<http://www.cardis.org>).

This volume contains the refereed papers presented at CARDIS 1998. These 35 papers were first published in a pre-proceedings and distributed to the attendees at the conference; they have subsequently been revised and updated for this volume.

The papers discuss all aspects of smart-card research: Java cards, electronic commerce applications, efficiency, security (including cryptographic algorithms, cryptographic protocols, and authentication), and architecture. Submissions from Europe, the U.S., Asia, and Australia show that this is indeed an international area of research, and one that is becoming more popular as practical demand for smart cards increase.

We wish to thank the Program Committee members who did an excellent job in reviewing papers and providing feedback to the authors.

All credit for the smooth editing submission process goes to Damien Giry, who handled all aspects and delivered a convenient directory full of submissions and editing postscript, PDF (and Troff !) submissions so that they would view and print acceptably; Catherine Rouyer, Patricia Focant and Catherine Konstantinidis for secretarial help, particularly in helping to organize the whole conference.

We also thank Professor Benoit Macq for the involving of his group during the conference.

Finally, we wish to thank all the authors who submitted papers, making this conference possible, and the authors of accepted papers for updating their papers with care and patience during the lengthy production of these proceedings.

June 2000

Jean-Jacques Quisquater
Bruce Schneier
Program Chairs
CARDIS '98

CARDIS '98

September 14 – 16, 1998, Louvain-la-Neuve, Belgium

Sponsored by
Belgacom
Europay International

Program Chairs

Jean-Jacques Quisquater, UCL, Belgium
Bruce Schneier, Counterpane, USA

Program Committee

William Caelli QUT Brisbane, Australia
Vincent Cordonnier R2DP Lille, France
David Chan HP Labs Bristol, UK
Jean-François Dhem Belgacom, Belgium
Jan Eloff RAU, South Africa
Marc Girault CNET, France
Louis Guillou CNET, France
Pieter Hartel Southampton, UK and Amsterdam, Netherlands
Peter Honeyman Michigan Univ, USA
Pierre Paradinas Gemplus, France
Sihan Qing Acad. Sciences Beijing, China
Michel Ugon Bull CP-8, France
Doug Tygar Carnegie-Mellon Univ., USA
Anthony Watson ECU Perth, Australia
Wijang Zhang Shanghai, China

Steering Committee

Vincent Cordonnier, R2DP Lille, France

Local Organizing Committee

Catherine Rouyer, UCL, Belgium
Patricia Focant, UCL, Belgium
Catherine Konstantinidis, UCL, Belgium
Benoît Macq, UCL, Belgium
Damien Giry, UCL, Belgium (editing and printing)