A smart card is a small computer with a number of interesting properties. A smart card is reliable and inexpensive, and it is packaged in the same way as a credit card. This makes it feasible to distribute smart cards to millions of users. A smart card is a programmable computer, and thus offers flexibility. Finally, a smart card can protect data from unauthorised access. These properties make smart cards suitable for a staggering number of uses in everyday life. This issue provides a perspective on the state of the art for this exciting technology.

This issue contains an invited paper and a selection of the papers presented at the second international conference on Smart Card Research and Advanced Applications (CARDIS). The conference was held in Amsterdam, The Netherlands, September 16–18, 1996. The first CARDIS conference was held in Lille, France in November 1994. Both conferences were well attended: 60 participants came to Lille and Amsterdam attracted 90.

The invited paper by Quisquater presents the past and present of smart card research and indicates possible avenues for its future. The thesis of the paper is that smart cards are in their adolescence. There is good hope that the technology will mature and come to full bloom, but more research is needed to achieve this.

The first two regular papers present novel ideas for the future use of smart cards. The paper by Schneier and Kelsey uses cryptology to certify outcomes of programs. This might ultimately make it possible to bill for software usage. The paper by Alexandre discusses biometric authentication based on the differences in the way people type on computer keyboards. This form of biometry is probably more acceptable than most other forms of biometrics.

The next three papers describe advances in the theory and practice of smart cards. The paper by Dhem and Quisquater describes different approaches to compressing information that is to be processed by a smart card. Compression is highly relevant for the severely resource constrained smart card. In the paper by Alberda et al an example is given of how formal methods can be used to reason about a programming language used to construct a trustworthy smart card operating system. In the paper by Hollmann et al an application of statistically analysing data obtained from monitoring the hardware is dis-
cussed. This study, on a possible form of attack, increases our understanding of methods to better protect smart cards.

The last two papers deal with the environment in which smart cards operate. Domingo-Ferrer discusses how a client server approach helps to securely offload compute intensive operations. The paper by Biget et al discusses how object orientation and the CORBA architecture may help to provide a distributed environment for smart cards.

On behalf of the CARDIS programme committee we thank all those who submitted papers. We thank the referees for their careful work in the reviewing and selection process.

Pieter H. Hartel, Southampton
January 1997
Table of contents

(i) The adolescence of smart cards
Jean-Jacques Quisquater
(Univ. Catholique de Louvain, Louvain-la-Neuve, Belgium)

(ii) Remote Auditing of Software Outputs using a Trusted Coprocessor
Bruce Schnier, John Kelsey
(Counterpane Systems, Minneapolis, USA)

(iii) Biometrics on Smartcards: An Approach to Keyboard Behavioral Signature
Thomas J. Alexandre
(Carnegie Mellon Univ., Pittsburgh, USA)

(iv) Lossless Compression Algorithms for Smart Cards: A Progress Report
Jean-Francois Dhem, Jean-Jacques Quisquater
(Univ. Catholique de Louvain, Louvain-la-Neuve, Belgium)

(v) Using Formal Methods to Cultivate Trust in Smart Card Operating Systems
Marjan I. Alberda, Pieter H. Hartel, Eduard K. de Jong Frz
(Univ. of Amsterdam, The Netherlands; Univ. of Southampton, UK; Integrity Arts Inc, San Mateo, USA)

(vi) Protection of Software Algorithms Executed on Secure Modules
Henk D. L. Hollmann, Jean-Paul M. G. Linnartz, Jacobus H. van Lint, Stan Baggen, Ludo M. G. Tolhuizen
(Phillips Research Laboratories, Eindhoven, The Netherlands; Eindhoven Univ. of Technology, The Netherlands)

(vii) Multi-Application Smart Cards and Encrypted Data Processing
Josep Domingo-Ferrer
(Univ. Rovira i Virgili, Tarragona, Catalonia, Spain)

(viii) How Smart Cards Can Benefit from Object-Oriented Technologies
Patrick Biget, Patrick George, Jean-Jacques Vandewalle
(RD2P, Univ. de Lille, France)