

## Preface

The CQRE [Secure] conference provides a new international forum giving a close-up view on information security in the context of rapidly evolving economic processes. The unprecedented reliance on computer technology has transformed the previous technical side-issue "information security" to a management problem requiring decisions of strategic importance. Thus one of the main goals of the conference is to provide a platform for both technical specialists as well as decision makers from government, industry, commercial, and academic communities. The target of CQRE is to promote and stimulate dialogue between managers and experts, which seems to be necessary for providing secure information systems in the next millennium.

Therefore CQRE consists of two parts: Part I mainly focuses on strategic issues of information security, while the focus of Part II is more technical in nature. This volume of the conference proceedings consists of the reviewed and invited contributions of the second part.

The program committee considered 46 papers and selected only 15 for full presentation. For the participants' convenience we have also included the notes of the invited lectures and short workshop talks in this volume.

The selection of papers was a difficult and challenging task. I wish to thank the program committee members who indeed did an excellent job in reviewing and selecting the papers and providing useful feedback to authors. Each submission was blindly refereed by at least three reviewers to make the selection process as fair and objective as possible. The program committee was assisted by many colleagues who reviewed submissions in their field of expertise. My thanks to all of them.

I would also like to thank the entire CQRE-team for their kind assistance in organizing this event. My special thanks to our hosts from Messe-Düsseldorf GmbH and especially to N. Mizera, M. Kotschedoff, S. Spamer, A. Viefers, and B. Wagner who greatly contributed to the success of this challenging project with their untiring engagement and timely decisions. Furthermore I would like to thank the team from Brodeur-Kohtes & Klewes around B. Boendel and my colleagues T. Gawlick, A. M. Schlesinger, and D. Hühnlein for kindly assisting me in administrative tasks.

Last but not least, I wish to thank all the authors who submitted papers, making this conference possible, and the authors of accepted papers for updating their work in a timely manner, allowing the production of these proceedings.

September 1999

Rainer Baumgart

# CQRE [Secure]

November 30 - December 2, 1999, Düsseldorf, Germany

## Program Chair

Rainer Baumgart, Secunet, Germany

## Program Committee

Johannes Buchmann ..... University of Technology Darmstadt, Germany  
Dirk Fox .....Secorvo, Germany  
Walter Fumy ..... Siemens, Germany  
Rüdiger Grimm..... GMD, Germany  
Helena Handschuh.....Gemplus / ENS, France  
Pil Joong Lee ..... Postech, South Korea  
Alfred Menezes ..... University of Waterloo / Certicom, Canada  
David Naccache..... Gemplus, France  
Clifford Neumann..... University of Southern California, USA  
Joachim Posegga .....Deutsche Telekom, Germany  
Mike Reiter..... Bell Labs, USA  
Matt Robshaw..... RSA Labs, USA  
Richard Schlechter.....European Commission, Belgium  
Bruce Schneier ..... Counterpane, USA  
Tsuyoshi Takagi ..... NTT, Germany  
Yiannis Tsiounis .....Spendcash, USA  
Michael Waidner ..... IBM, Switzerland  
Moti Yung ..... CertCo, USA  
Robert Zuccherato ..... Entrust Technologies, Canada