We cannot have any security without at least some sort of trust. Building a secure system, small or large, always assumes a certain trust model. Let us take an example. The GSM cellular communication system has been around for almost two decades. It contains, as an essential ingredient, a global security system that allows every user to be authenticated and every call to be secured. This can be guaranteed whether the user is near home or travelling on the other side of the world. To enable all this, a complex trust network exists between mobile operators. As part of the trust network, operators from different parts of the world have to settle roaming agreements and exchange session keys and other authentication data. It is vital for each operator to maintain a good reputation as a trustworthy roaming partner.

Continuing with our example, trust plays a major role also on the user’s side. Authentication of the user depends on the assumption that user takes good care of the little smart card inside the mobile device. Furthermore, the user has to have some degree of trust to each person who can have access to the mobile device because it is fairly easy to replace the SIM card inside the device by another one (a handy feature that makes it possible to change the mobile device without a need to contact the operator). From the user’s point of view, the smart card itself needs to be trusted: it has to function as it is intended to do. Of course, the user has to have a lot of trust on the operator, especially for correct billing.

The example of the GSM security system highlights several crucial aspects of trust that today everybody is exposed to. The co-existence and convergence of physical and digital worlds imply new notions of trust that people are not yet used to. One aspect is reputation on the global scale, required by (e.g., on-line shopping). Another aspect is dependence on correct behavior of technology around us (e.g., need for trusted hardware and software). Furthermore, popular social networking services have shown that we need to re-evaluate the role of trust as regards the other users of the same services.

This book sheds light on the intriguing notion of trust from all of the angles mentioned above. Dr. Zheng Yan has succeeded in collecting a comprehensive and impressive selection of chapters, each of which stems from practical issues in the modern digital world and shows the way forward in managing these issues via better understanding of trust as a key concept. Several chapters of the book are devoted to each of the following key questions in trust management:

- how to provide trustworthy technologies?
- how to evaluate and measure trust?
- how do people understand and use trust in different contexts?

Trust modeling and management are becoming more and more important areas because of increased usage of automation and people’s presence in both physical and digital dimensions. There is a lot that research can do in helping us to meet the challenges ahead. Chapters in this book give overwhelming evidence on the power of research and they also serve as great stimulation for further research.
Valtteri Niemi  
Nokia Fellow  
Chairman of the 3GPP security working group  
Nokia Research Center, Switzerland

Valtteri Niemi received a PhD degree from the University of Turku, Finland, Mathematics Department, in 1989. After serving in various positions in the University of Turku, he was an Associate Professor in the Mathematics and Statistics Department of the University of Vaasa, Finland, during 1993-97. He joined Nokia Research Center (NRC), Helsinki in 1997 and in 1999 he was nominated as a Research Fellow. During 2004-2006, he was responsible for Nokia research in wireless security area as a Senior Research Manager. During 2007-2008, Dr. Niemi led the Trustworthy Communications and Identities team in the Internet laboratory of NRC, Helsinki. He recently moved to the new NRC laboratory in Lausanne, Switzerland, where his main focus is on privacy-enhancing technologies. He was also nominated as a Nokia Fellow in 2009. Dr. Niemi’s work has been on security issues of future mobile networks and terminals, the main emphasis being on cryptological aspects. He has participated 3GPP SA3 (security) standardization group from the beginning. Starting from 2003, he has been the chairman of the group. Before 3GPP, Niemi took part in ETSI SMG 10 for GSM security work. In addition to cryptology and security, Dr. Niemi has done research on the area of formal languages. He has published more than 40 scientific articles and he is a co-author of three books.