

# Preface

This book is all about smart cards and security tokens in the widest sense. The aim was to provide a complete story, looking at a cross section of technologies, processes, applications and real-world usage. The original motivation for the book was to provide a suitable reference text for the aptly titled MSc module, "Smart Cards Tokens, Security and Applications" which is part of the Masters course in Information Security, run by the Information Security Group at Royal Holloway University of London. However as the planning for the book advanced we realised that various industries and government departments can become quite narrow in their understanding of smart cards/RFIDs and that looking across industry and across roles (such as technical, business and logistics) could be beneficial for a wide range of readers. To deliver such a breadth of information requires input from many experts and so we are very pleased and proud of the calibre of the authors and reviewers that have made this book possible. We hope that you will enjoy this book and find it a useful guide and reference.

## Structure of the book

This book consists of fifteen chapters. Each chapter is a completely autonomous contribution in a chained discussion which aims to bring researchers, practitioners and students up to speed with the recent developments within the smart card arena. In order to enhance the reader experience each book chapter contains its own abstract, introduction, main body and conclusion sections. Furthermore, bibliography resources can be found at the very end of each chapter. The following list provides a more detailed overview of the topics that are discussed in the different chapters of this book.

**Chapter 1** provides an introduction to a very wide range of smart card related issues. It surveys the different types of cards, tokens and it also considers the main types and capabilities of popular applications utilising smart card technology. The

chapter is considered as a good starting point for newcomers to the field and perhaps those that have perhaps focussed on one business or technical area.

**Chapter 2** discusses the different steps in the smart card production chain. The analysis covers all the main steps during the smart card manufacturing phase starting with the production of the card body, chip moulding and smart card personalisation and delivery. Finally, it concludes with current and future trends and challenges.

**Chapter 3** provides an overview of the most widely utilised smart card operating systems and platforms that enable multiple applications to be securely managed and reside in the same smart card.

**Chapter 4** discusses the role of the SIM and USIM in the mobile telecommunications industry and describes the associated standards. It presents the authentication and ciphering processes in some depth and provides a practical comparison between the two technologies prior to exploring further value added service and toolkit features. Finally, it provides some insight into the future evolution of technology.

**Chapter 5** examines the role of smart card technology within the financial payments industry. It examines how the credit card industry has evolved over the decades and explains some of the issues with magnetic stripe card technology. Subsequently, it presents the main features of smart card technology in the light of the EMV card specifications. The discussion continues with 3D secure and token authentication.

**Chapter 6** deals with the issues around content protection in the satellite TV industry. In particular it examines the commercial motivation as the driving force behind content protection, how smart card security is utilised in order to provide the necessary functionality and finally highlights how a typical pay-TV system operates.

**Chapter 7** provides and overview the Trusted Platform Module (TPM) and highlights commonalties and differences with smart cards. It provides an introduction to the security mechanisms provided by the TPM and provides a guide to the associated standards and literature.

**Chapter 8** explains how Common Criteria evolved, how it is defined and how it is used in practice. More importantly it examines how Common Criteria is applied to the complex and demanding field of smart card security evaluations.

**Chapter 9** focuses on the various attacks and countermeasures that apply to smart cards. As many applications rely on cryptographic algorithms for sensitive operations this chapter focuses on the attacks that could affect smart cards performing cryptographic operations. Furthermore, it provides references to the corresponding countermeasures and emphasises the need for rigorous design, implementation and test of cryptographic algorithms and their underlying host platforms.

**Chapter 10** provides a brief overview of the wide range of issues associated with the smart card application development processes. In particular it examines the development of an application for the popular Java Card platform. It also highlights practical issues around application development and monitoring tools. Finally it looks into development of the mobile phone applications that can exploit SIM and USIM card capabilities by using it as a trusted security element.

**Chapter 11** analyses the use of the smart card within the telecommunications industry as a managed platform. It examines how the mobile phone operators are using the necessary tools and technology in order to remotely update and enhance, Over-The-Air, the functionality of SIM and USIM cards.

**Chapter 12** provides a valuable introduction to the main standards used to manage and access smart card readers connected to personal computers. Their main functionality is analysed and attached code samples aim to provide a detailed overview, but also to enable the reader to reuse them in order to quickly develop sample host applications that will communicate with smart cards.

**Chapter 13** provides an introduction to the RFID concepts and also summarises the aspects most relevant to contactless smart card systems. Several different systems along with operating principles are described. The chapter also provides an overview of the main Radio Frequency (RF) interface and communication theory along with the various RF standards.

**Chapter 14** explains how national requirements for eID cards and e-Passports can be realised by utilising physical, logical and hardware functionality. Furthermore, it highlights the importance and requirements of the relevant standards.

**Chapter 15** first examines the historical use of technology in smart cards before highlighting the future trends. It looks into the different options and choices which can be made within a smart card scheme along with the issues which affect the design of the card and its applications. Finally it discusses issues around consumer demand and the drivers that will define the smart card technology of the future.

In order to make reading of this more convenient, we also provide a subject index at the very end of the book. Furthermore, there is also a website for this book:

<http://www.scc.rhul.ac.uk/book>

The website will allow readers to obtain additional and up-to-date information about the topics covered in the book.

Smart Cards, Tokens, Security and Applications

Mayes, D.K.; Markantonakis, K. (Eds.)

2008, XXXVII, 392 p., Hardcover

ISBN: 978-0-387-72197-2