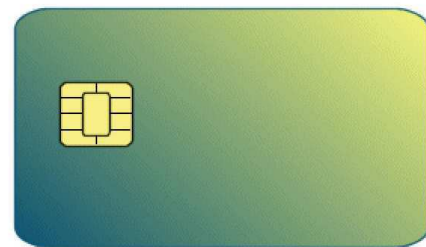




Programming Smart Cards

Part 1:
Basic Notions
ISO 7816 Specifications
Samples with Virtual Smart Card



Ugo Chirico



Ugo Chirico

Programming Smart Cards

Part 1

Basic Notions ISO 7816 Specifications Sample with Virtual Smart Card

Copyright © 2009 by Ugo Chirico All rights reserved.

No part of the contents of this book may be reproduced or transmitted in any form without the written permission of the publisher.

All product and company names mentioned herein may be the trademarks of their respective owners.

Acknowledgments

Many thanks goes to:

Ornella Simeoli for her invaluable suggestions and support during the writing of this book,

Salvatore Petrona for the library of functions upon which the smart card emulator has been based.

The Author



Ugo Chirico is graduate with a Master Degree in Physics and Cybernetics at University of Naples "Federico II" and currently is the Director of Mobile Development of KeyVision (<http://www.key-vision.com>) and is the owner of Cryptware (<http://www.cryptware.it>).

He wrote numerous articles on several technical magazines such as "Computer Programming" and "Dev" and he is an expert in software designing and development in C/C++, C#, VB, Java, Prolog e LISP on .NET platform, Win32, Linux, Symbian, Windows Mobile, iPhone and BlackBerry and embedded systems. It is also passionate in Artificial

Intelligence. His personal web site is: <http://www.ugochirico.com>

Table of Contents

Acknowledgments.....	2
Smart Cards.....	6
1.1 Brief History	6
1.2 HW/SW Architecture of a Smart Card Based System.....	6
1.3 Smart Cards And Cryptography.....	8
1.4 Smart Cards and Authentication Processes.....	8
1.5 Applications	9
1.6 Standards.....	10
1.7 Case Studies	11
1.7.1 Corporate Card.....	11
1.7.2 E-Poll Project	12
1.7.3 Italian Military Defense Multi-Service Card	13
Basis.....	15
2.1 Smart Card	15
2.1.1 Memory Cards.....	15
2.1.2 Microprocessor-based Cards.....	16
2.1.3 Contact, Contactless and Dual Interface Smart Card.....	16
2.1.4 USB Token.....	17
2.2 Microchip Architecture	18
2.3 Smart Card Manufacturing.....	20
2.4 Operating System.....	20
2.5 Smart Cards and Data Protection.....	20
2.6 Smart Card Selection Criteria	21
ISO 7816 Specification	22
3.1 Standard technical specifications	22
3.2 Physical and Electrical Characteristics	23
3.3 ATR.....	23
3.4 Transmission Protocols	24
3.4.1 T = 0 Protocol	24
3.4.2 T = 1 Protocol	24
3.4.3 Synchronous Protocols.....	25
3.5 Structure and format of EEPROM-stored data	25
3.5.1 File System.....	25
3.5.2 Files Typology and Format	26
3.5.3 File Access Permissions.....	26
3.5.4 Secure Messaging	27
3.6 Command Set.....	27
3.6.1 Command APDU	27
3.6.2 Response APDU	28
3.6.3 TPDU	29
3.6.4 Basic Commands.....	29
3.6.4 Advanced Command Set.....	30
3.7 Smart Card Emulator	31
3.7.1 Setup.....	32
3.7.2 The virtual smart card	32

3.7.3 Smart card lifecycle	33
3.7.4 Microchip Information	33
3.7.5 Formatting the Smart Card.....	33
3.7.6 File System Creation	34
3.7.7 Populating the Smart Card	36
3.7.8 Using the Smart Card	36
Appendix A.....	37
Virtual Smart Card Reference Manual.....	37
Bibliography.....	43
Web References	45

Introduction

Over the last few years, smart card based technologies received huge attention in IT and telecommunications industries thanks to its special security features that solve almost all the security leaks which affect communications over Internet. In fact, Internet, as it currently is, doesn't offer a valid mechanism to identify both parties of a transmission and doesn't supply an adequate level of protection for the information transmitted.. Those security leaks caused big investments by a lot of IT companies producing a fast and amazing technological enhancements.

Nowadays, smart card related technologies are popular and reliable, and they are stimulating a de facto revolution about patterns used for accessing, using and handling information.

That revolution goes through a total reformulation of security paradigms for protecting reserved information and, more generally, for protecting information systems.

The good news represented by smart cards, which is also their main advantage, is the possibility to store securely reserved information in an electronic device which could be easily bring in a wallet, analogue to an ordinary credit card. Such a feature enabled the implementation several new interesting applications in a lot of fields. Just to cite a few: security (automated and certificated identification of individuals in particular), mobile communications, *PayTV*, e-commerce and banking systems; SIM/USIM cards (in GSM/UMTS respectively), electronic IDs, bank payment cards, company badges, prepaid cards and loyalty cards. Those are just some of the feasible applications based on a smart card, which is becoming an invaluable tool in the real life.

Though smart card technology is consolidated there are several differences between the numerous kinds of smart cards and the various fields of application. Several standards and technical specifications has been defined in order to identify a unique working platform in which smart cards from distinct vendors can easily interoperate.

Navigating in this so rich panorama of technical specifications and programming paradigms, sometimes almost equivalent from various points of view, it is very hard and especially it's very hard to understand the differences (sometimes philosophical) between the distinct specifications and platforms. As result it isn't easy to choose the subset of technical specifications which meet all requirements for a specific application.

The aim of this book is to offer a brief guide, whilst a complete and thorough one, to all technological aspects, standards and specifications related to smart cards, firstly providing an high level overview of the technological panorama and, later, offering an in-depth technical coverage, targeted especially to programmers, about architectures, programming paradigms and APIs related to the each standard or technical specification.

The first part of the book introduces the smart cards' technology, all general concepts and a few *case studies*. It is addressed also to non-technical reader who wishes an overview of fascinating world of smart cards .

Instead the second part of the book constitutes a more technical guide to all smart card-oriented specifications and programming paradigms

Each chapter on the second part introduces some starting sections on the general topics about the examined technology, therefore accessible to non-technical readers too, while the following sections will be devoted to dive into technical topics about smart programming and applications development, so it requires some skills on basic programming techniques. Specifically, it requires skills in C/C++ languages in chapters related to PC/SC and PKCS#11 specifications, skill in C# in chapters related to .NET framework, skill in Java in chapters describing the Java Card platform and the *OpenCard Framework* and, finally, skill in Visual Basic for some sections of the chapter about PC/SC specifications.