SINGAPORE STANDARD

SS 372 : Part 4 : 1999

(ICS 35.240)

SPECIFICATION FOR

Identification cards - Integrated circuit(s) cards with contacts

Part 4 : Interindustry commands for interchange

Published by
Singapore Productivity and Standards Board
1 Science Park Drive
Singapore 118221

PSB SINGAPORE

SINGAPORE STANDARD

SS 372 : Part 4 : 1999

(ICS 35.240)

SPECIFICATION FOR

Identification cards - Integrated circuit(s) cards with contacts

Part 4 : Interindustry commands for interchange

Director
Centre for Standardisation
Singapore Productivity and Standards Board
1 Science Park Drive
Singapore 118221
Telephone: 2786666 Telefax: 2786665
Email: cfs@psb.gov.sg

ISBN 9971-67-780-6

Contents

Page

Foreword 8

SPECIFICATION

0 Introduction 9
1 Scope 9
2 Abbreviations and notation 10
3 Access conditions 11
4 Secure messaging 12
5 Secure writing 14
5.1 Power failure during overwrite of current data 14
5.2 Write error during correction procedure 14
6 Commands summary 15
7 Basic interindustry commands 15
7.1 READ BINARY command 15
7.1.1 Definition and scope 15
7.1.2 Conditional usage and security 15
7.1.3 Command message 16
7.1.4 Response message (nominal case) 16
7.1.5 Status conditions 16
7.2 WRITE BINARY command 17
7.2.1 Definition and scope 17
7.2.2 Conditional usage and security 17
7.2.3 Command message 18
7.2.4 Response message (nominal case) 19
7.2.5 Status conditions 19
7.3 UPDATE BINARY command 20
7.3.1 Definition and scope 20
7.3.2 Conditional usage and security 20
7.3.3 Command message 21
7.3.4 Response message (nominal case) 22
7.3.5 Status conditions 22
7.4 ERASE BINARY command 23
7.5 READ RECORD command 23
7.5.1 Definition and scope 23
7.5.2 Conditional usage and security 23
7.5.3 Command message 23
7.5.4 Response message (nominal case) 23
7.5.5 Status conditions 24
7.6 WRITE RECORD command 24
7.7 APPEND RECORD command 24

7.8 UPDATE RECORD command 24
7.8.1 Definition and scope 24
7.8.2 Conditional usage and security 24
7.8.3 Command message 25
7.8.4 Response message (nominal case) 25
7.8.5 Status conditions 25
7.9 GET DATA command 26
7.10 PUT DATA command 26
7.11 SELECT FILE command 26
7.11.1 Definition and scope 26
7.11.2 Conditional usage and security 26
7.11.3 Command message 26
7.11.4 Response message (nominal case) 27
7.11.5 Status conditions 27
7.12 VERIFY command 27
7.12.1 Definition and scope 27
7.12.2 Conditional usage and security 27
7.12.3 Command message 28
7.12.4 Response message (nominal case) 28
7.12.5 Status conditions 28
7.13 INTERNAL AUTHENTICATE command 29
7.14 EXTERNAL AUTHENTICATE command 29
7.15 GET CHALLENGE command 29
7.16 MANAGE CHANNEL command 29
8 Transmission-oriented interindustry commands 29
8.1 GET RESPONSE command 29
8.1.1 Definition and scope 29
8.1.2 Conditional usage and security 29
8.1.3 Command message 29
8.1.4 Response message (nominal case) 29
8.1.5 Status conditions 29
8.2 ENVELOP command 30
9 Administration commands 30
9.1 CHANGE ACCESS CONDITIONS command 30
9.1.1. Definition and scope 30
9.1.2. Conditional usage and security 30
9.1.3. Command message 31
9.1.4. Response message (nominal case) 31
9.1.5. Status conditions 31
9.2 CREATE FILE command 32
9.2.1 Definition and scope 32
9.2.2 Conditional usage and security 32
9.2.3 Command message 32
9.2.4 Response message (nominal case) 34
9.2.5 Status conditions 34

9.3 GET INFO command 35
9.3.1 Definition and scope 35
9.3.2 Conditional usage and security 35
9.3.3 Command message 35
9.3.4 Response message (nominal case) 36
9.3.5 Status conditions 37
9.4 INIT ADMIN command 38
9.4.1 Definition and scope 38
9.4.2 Conditional usage and security 39
9.4.3 Command message 39
9.4.4 Response message (nominal case) 39
9.4.5 Status conditions 40
9.5 SET PERSONALIZED command 40
9.5.1 Definition and scope 40
9.5.2 Conditional usage and security 40
9.5.3 Command message 40
9.5.4 Response message (nominal case) 40
9.5.5 Status conditions 41
9.6 SET PROTOCOL command 41
9.6.1 Definition and scope 41
9.6.2 Conditional usage and security 41
9.6.3 Command message 41
9.6.4 Response message (nominal case) 41
9.6.5 Status conditions 42
9.7 START DF command 42
9.7.1 Definition and scope 42
9.7.2 Conditional usage and security 42
9.7.3 Command message 42
9.7.4 Response message (nominal case) 42
9.7.5 Status conditions 42
9.8 UPDATE LOG command 43
9.8.1 Definition and scope 43
9.8.2 Conditional usage and security 43
9.8.3 Command message 43
9.8.4 Response message (nominal case) 43
9.8.5 Status conditions 44
9.9 VERIFY AND CHANGE command 44
9.9.1 Definition and scope 44
9.9.2 Conditional usage and security 45
9.9.3 Command message 45
9.9.4 Response message (nominal case) 45
9.9.5 Status conditions 46
10 Status bytes 47

Foreword

This Singapore Standard was prepared by the Smart Card Technical Committee under the direction of the IT Standards Committee.

This Singapore Standard is related to ISO/IEC 7816-4:1995 Identification cards – Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange (hereinafter referred to as "ISO/IEC 7816-4:1995"). Hence, it needs to be used in conjunction with ISO/IEC 7816-4:1995.

References was also made to the following standards:

SS 372:Part 1:1994/ ISO 7816-1:1987(E)	Specification for identification cards – Integrated circuit(s) cards with contacts Part 1: Physical characteristics
SS ISO 7816-2:1988	Specification for identification cards – Integrated circuit(s) cards with contacts Part 2 : Dimensions and location of the contacts
SS 372:Part 3:1995	Specification for identification cards – Integrated circuit(s) cards with contacts Part 3: Electronic signals and transmission protocols
ISO/IEC 7816-4:1995	Specification for identification cards – Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange

NOTE

1. *Singapore Standards are subject to periodic review to keep abreast of technological changes and new technical developments. The revisions of Singapore Standards are announced through the issue of either amendment slips or revised editions.*

2. *Compliance with a Singapore Standard does not exempt users form legal obligations.*

Specification for identification cards – Integrated circuit(s) cards with contacts – Part 4 : Interindustry commands for interchange

0 Introduction

This standard is intended as a supplement to ISO/IEC 7816-4 : 1995. It provides more specific implementations for selected ISO/IEC 7816-4 : 1995 commands, in addition to specifying additional commands, classified in this standard under 'Administration Commands'. This document should be used together with ISO/IEC 7816-4 : 1995.

Clauses 3 through 5 define more specifically implementation details for functions related to Access Conditions, Secure Messaging and Secure Writing, and should be used in conjunction with the relevant specifications in ISO/IEC 7816-4 : 1995.

The 'Administration Commands' are listed in Clause 9.

Note that in this Singapore Standard, secure messaging commands have been extended to support the SAFER-SK128 (12 rounds) encryption algorithm – in addition to DES and Triple-DES. In particular, the CREATE FILE command has been extended whereby the ALGO byte attribute has been modified so that the '10' value indicates SAFER-SK128. The support for SAFER-SK128 is optional and will be decided by the specific buyer (project management organisation). At the present moment, the support for SAFER-SK128 is only required for the commands listed in this document, and does not affect the 'Stored Value Card Application Standard' (the 'purse' commands). It can be assumed that the 'purse' commands will never be activated on a 'SAFER key file', and even in that event, the Smart Card should merely return an 'incorrect parameters' error status.

1 Scope

This standard specifies implementations of selected ISO/IEC 7816-4 : 1995 commands used within the Singapore context. This document covers Access Conditions, Secure Messaging, Secure Writing, Basic Interindustry commands and Transmission-oriented Inter-industry commands. Additional commands required by key applications in Singapore are set out under Administration commands.

The Access Conditions of various operations on MF, DF and EFs include access condition groups, its interpretation, and access condition coding.

Secure Messaging in this specification includes the description of two methods : Encrypted data in the data field and Plain data plus padding 3 bytes of cryptographic checksum in the data field, with further description of the secure messaging process using the second method. The Secure Messaging process covers commands that send data to the card and commands that only receive data from the card, for both the terminal and the card.

The commands added to this specification over and above ISO/IEC 7816-4 : 1995 are covered in this document under the following headings: Definition and Scope, Conditional Usage and Security, Command Message, Response Message and Status Conditions.