ISO/IEC 7816-4:2005-01 (E)

Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Symbols and abbreviated terms 5

5 Organization for interchange 7
5.1 Command-response pairs 7
5.2 Data objects 13
5.3 Structures for applications and data 17
5.4 Security architecture 22

6 Secure messaging 28
6.1 SM fields and SM data objects 28
6.2 Basic SM data objects 29
6.3 Auxiliary SM data objects 31
6.4 SM impact on command-response pairs 35

7 Commands for interchange 36
7.1 Selection 36
7.2 Data unit handling 39
7.3 Record handling 41
7.4 Data object handling 47
7.5 Basic security handling 50
7.6 Transmission handling 57

8 Application-independent card services 57
8.1 Card identification 58
8.2 Application identification and selection 61
8.3 Selection by path 64
8.4 Data retrieval 65
8.5 Data element retrieval 65
8.6 Card-originated byte strings 67

Annex A (informative) Examples of object identifiers and tag allocation schemes 69

Annex B (informative) Examples of secure messaging 71

Annex C (informative) Examples of AUTHENTICATE functions by GENERAL AUTHENTICATE commands 78

Annex D (informative) Application identifiers using issuer identification numbers 82

Bibliography 83