ISO/IEC 7816-4:2020-05 (E)

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

Contents

Page

Foreword vii

Introduction viii

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 7

5 Command-response pairs 8
5.1 Conditions of operation 8
5.2 Syntax 9
5.3 Chaining procedures 10
5.3.1 General 10
5.3.2 Payload fragmentation 10
5.3.3 Command chaining 10
5.3.4 Response chaining 11
5.4 Class byte 12
5.4.1 Coding 12
5.4.2 Logical channels 13
5.5 Instruction byte 14
5.6 Status bytes 17

6 Data objects 19
6.1 General 19
6.2 SIMPLE-TLV data objects 19
6.3 BER-TLV data objects 20
6.4 Constructed DOs versus primitive DOs 20

7 Structures for applications and data 20
7.1 Available structures 20
7.2 Validity area 22
7.2.1 Definitions and attributes 22
7.2.2 Basic rules for VA handling and use 22
7.3 Structure selection 23
7.3.1 Structure selection methods 23
7.3.2 File reference data element and DO 24
7.3.3 General reference data element and DO 25
7.3.4 Data referencing methods in elementary files 25
7.4 File and data control information 26
7.4.1 File control information retrieval 26
7.4.2 Data control information retrieval 26
7.4.3 Control parameters 27
7.4.4 Short EF identifier 28
7.4.5 File descriptor byte 28
7.4.6 Profile indicator 29
7.4.7 Data descriptor byte 30
7.4.8 DF and EF list data elements 30

7.4.9 Instance number data element 30
7.4.10 Life cycle status 30
7.4.11 Indirect referencing by short EF identifier using DO'A2' 31
7.4.12 Interface and life cycle status dependent security attribute template 31

8 Specific use of DOs and related concepts 33
8.1 ber-tlv payloads and padding 33
8.1.1 General 33
8.1.2 Padding conditions 33
8.1.3 Padding procedure 33
8.2 Template referenced by curConstructedDO and data object generations 34
8.2.1 Template referenced by curConstructedDO and DO referenced by curDO 34
8.2.2 Template extension 34
8.2.3 Data object pruned-tree 35
8.2.4 Data object life cycle 35
8.3 Identification of data elements and data objects 35
8.3.1 Principles 35
8.3.2 Tag interpretation in command and response data fields or payloads 35
8.3.3 Tag allocation 36
8.3.4 Standard tag allocation scheme 36
8.3.5 Compatible tag allocation scheme 36
8.3.6 Coexistent tag allocation scheme 37
8.3.7 Avoidance of independent tag allocation schemes 37
8.4 Referencing and retrieval of DOs and data elements 37
8.4.1 General 37
8.4.2 Element list 38
8.4.3 Tag list 38
8.4.4 Header list 38
8.4.5 Extended header and extended header list 38
8.4.6 Resolving an extended header 39
8.4.7 Resolving an extended header list 40
8.4.8 Wrapper 40
8.4.9 Tagged wrapper 41

9 Security architecture 41
9.1 General 41
9.2 Cryptographic mechanism identifier template 43
9.3 Security attributes 43
9.3.1 General 43
9.3.2 Security attributes targets 43
9.3.3 Compact format 44
9.3.4 Expanded format 48
9.3.5 Access rule references 52
9.3.6 Security attributes for data objects 53
9.3.7 Security parameters template 54
9.3.8 Security attributes for logical channels 59
9.4 Security support data elements 60

10 Secure messaging 61
10.1 General 61
10.2 SM fields and SM DOs 61
10.2.1 SM protection of command payloads 61
10.2.2 SM protection of chained commands and responses 61
10.2.3 SM DOs 62
10.3 Basic SM DOs 63
10.3.1 SM DOs for encapsulating plain values 63
10.3.2 SM DOs for confidentiality 63
10.3.3 SM DOs for authentication 64
10.4 Auxiliary SM DOs 66
10.4.1 General 66
10.4.2 Control reference templates 67

10.4.3 Control reference DOs in control reference templates 67
10.4.4 Security environments 69
10.4.5 Response descriptor template 71
10.5 SM impact on command-response pairs 71

11 Commands for interchange 73
11.1 General 73
11.2 Selection 73
11.2.1 General 73
11.2.2 select command 73
11.2.3 manage channel command 76
11.3 Data unit handling 77
11.3.1 Data units 77
11.3.2 General 77
11.3.3 read binary command 78
11.3.4 write binary command 78
11.3.5 update binary command 79
11.3.6 search binary command 79
11.3.7 erase binary command 80
11.3.8 compare binary function 80
11.4 Record handling 80
11.4.1 Records 80
11.4.2 General 81
11.4.3 read record (s) command 82
11.4.4 write record command 84
11.4.5 update record command 85
11.4.6 append record command 87
11.4.7 search record command 88
11.4.8 erase record (s) command 92
11.4.9 activate record (s) command 93
11.4.10 deactivate record (s) command 94
11.4.11 compare record function 95
11.5 Data object handling 95
11.5.1 General 95
11.5.2 select data command 96
11.5.3 get data/get next data commands -- even INS codes 100
11.5.4 get data/get next data commands -- odd INS codes 102
11.5.5 General properties of put data/put next data/update data commands 103
11.5.6 put data command 104
11.5.7 put next data command 104
11.5.8 update data command 105
11.5.9 compare data function 106
11.6 Basic security handling 106
11.6.1 General 106
11.6.2 internal authenticate command 107
11.6.3 get challenge command 108
11.6.4 external authenticate command 108
11.6.5 general authenticate command 109
11.6.6 verify command 111
11.6.7 change reference data command 112
11.6.8 enable verification requirement command 112
11.6.9 disable verification requirement command 112
11.6.10 reset retry counter command 113
11.6.11 manage security environment command 114
11.7 Miscellaneous 115
11.7.1 compare command 115
11.7.2 get attribute command 117
11.8 Transmission handling 118
11.8.1 get response command 118
11.8.2 envelope command 118

12 Application-independent card services 119

12.1 General ... 119
12.2 Card identification ... 119
12.2.1 General ... 119
12.2.2 Historical bytes ... 120
12.2.3 Initial data string recovery ... 124
12.2.4 Waiting time management ... 124
12.3 Application identification and selection ... 126
12.3.1 General ... 126
12.3.2 EF.DIR ... 126
12.3.3 EF.ATR/INFO ... 127
12.3.4 Application identifier ... 127
12.3.5 Application template and related data elements ... 129
12.3.6 Application selection ... 129
12.4 Selection by path ... 130
12.5 Data retrieval ... 131
12.6 Card-originated byte string ... 131
12.6.1 General ... 131
12.6.2 Triggering by the card ... 131
12.6.3 Queries and replies ... 132
12.6.4 Formats ... 132
12.7 General feature management ... 132
12.7.1 General ... 132
12.7.2 On-card services ... 132
12.7.3 Interface services ... 133
12.7.4 Profile services ... 133
12.7.5 Provision of additional information ... 133
12.8 APDU management ... 134
12.8.1 Extended length information ... 134
12.8.2 List of supported INS codes ... 134

Annex A (informative) Examples of object identifiers and tag allocation schemes ... 135

Annex B (informative) Examples of secure messaging ... 138

Annex C (informative) Examples of authenticate functions by general authenticate commands ... 146

Annex D (informative) Application identifiers using issuer identification numbers ... 155

Annex E (informative) BER encoding rules ... 156

Annex F (informative) ber-tlv data object handling ... 158

Annex G (informative) Template extension by tagged wrapper ... 166

Annex H (informative) Parsing an extended header against its target DO ... 170

Annex I (informative) Use case of WTX (waiting time extension) procedure and application waiting time procedure ... 172

Bibliography ... 176