

ISO/IEC 7816-4:2013-04 (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	2
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	14
6	Data objects	17
6.1	SIMPLE-TLV data objects	18
6.2	BER-TLV data objects	18
6.3	Constructed DOs versus primitive DOs	18
7	Structures for applications and data	19
7.1	Available structures	19
7.2	Validity area	20
7.2.1	Definitions and attributes	20
7.2.2	Basic rules for VA handling and use	20
7.3	Structure selection	21
7.3.1	Structure selection methods	21
7.3.2	File reference data element and DO	22
7.3.3	General reference data element and DO	23
7.3.4	Data referencing methods in elementary files	23
7.4	File and data control information	23
7.4.1	File control information retrieval	23
7.4.2	Data control information retrieval	24
7.4.3	Control parameters	24
7.4.4	Short EF identifier	26
7.4.5	File descriptor byte	26
7.4.6	Profile indicator	27
7.4.7	Data descriptor byte	27
7.4.8	DF and EF list data elements	27
7.4.9	Instance number data element	28

7.4.10	Life cycle status	28
7.4.11	Indirect referencing by short EF identifier using DO'A2'	28
7.4.12	Interface and life cycle status dependent security attribute template	29
8	Specific use of DOs and related concepts	30
8.1	BER-TLV payloads and padding	30
8.1.1	Padding conditions	30
8.1.2	Padding procedure	30
8.2	Current template and data object generations	31
8.2.1	Current template and current DO	31
8.2.2	Template extension	31
8.2.3	Data object sub-tree	31
8.2.4	Data object life cycle	32
8.3	Identification of data elements and data objects	32
8.3.1	Principles	32
8.3.2	Tag interpretation in command and response data fields or payloads	32
8.3.3	Tag allocation	32
8.3.4	Standard tag allocation scheme	33
8.3.5	Compatible tag allocation scheme	33
8.3.6	Coexistent tag allocation scheme	34
8.3.7	Avoidance of independent tag allocation schemes	34
8.4	Referencing and retrieval of DOs and data elements	34
8.4.1	General	34
8.4.2	Element list	35
8.4.3	Tag list	35
8.4.4	Header list	35
8.4.5	Extended header and extended header list	35
8.4.6	Resolving an extended header	36
8.4.7	Resolving an extended header list	37
8.4.8	Wrapper	37
8.4.9	Tagged wrapper	38
9	Security architecture	38
9.1	General	38
9.2	Cryptographic mechanism identifier template	39
9.3	Security attributes	40
9.3.1	Security attributes targets	40
9.3.2	Compact format	40
9.3.3	Expanded format	44
9.3.4	Access rule references	48
9.3.5	Security attributes for data objects	49
9.3.6	Security parameters template	49
9.3.7	Security attributes for logical channels	55
9.4	Security support data elements	56
10	Secure messaging	57
10.1	SM fields and SM DOs	57
10.1.1	SM protection of command payloads	57
10.1.2	SM protection of chained commands and responses	57
10.1.3	SM DOs	57
10.2	Basic SM DOs	58
10.2.1	SM DOs for encapsulating plain values	58
10.2.2	SM DOs for confidentiality	59
10.2.3	SM DOs for authentication	60
10.3	Auxiliary SM DOs	61
10.3.1	Control reference templates	61
10.3.2	Control reference DOs in control reference templates	61
10.3.3	Security environments	63
10.3.4	Response descriptor template	65
10.4	SM impact on command-response pairs	65
11	Commands for interchange	67

11.1	Selection	67
11.1.1	SELECT command	67
11.1.2	MANAGE CHANNEL command	69
11.2	Data unit handling	70
11.2.1	Data units	70
11.2.2	General	70
11.2.3	READ BINARY command	71
11.2.4	WRITE BINARY command	71
11.2.5	UPDATE BINARY command	72
11.2.6	SEARCH BINARY command	72
11.2.7	ERASE BINARY command	72
11.2.8	COMPARE BINARY function	73
11.3	Record handling	73
11.3.1	Records	73
11.3.2	General	74
11.3.3	READ RECORD (S) command	74
11.3.4	WRITE RECORD command	76
11.3.5	UPDATE RECORD command	77
11.3.6	APPEND RECORD command	77
11.3.7	SEARCH RECORD command	78
11.3.8	ERASE RECORD (S) command	79
11.3.9	ACTIVATE RECORD (s) command	80
11.3.10	DEACTIVATE RECORD (s) command	80
11.3.11	COMPARE RECORD function	81
11.4	Data object handling	81
11.4.1	General	81
11.4.2	SELECT DATA command	82
11.4.3	GET DATA/GET NEXT DATA commands - even INS code	86
11.4.4	GET DATA/GET NEXT DATA command - odd INS codes	87
11.4.5	General properties of PUT/PUT NEXT/UPDATE DATA commands	89
11.4.6	PUT DATA command	89
11.4.7	PUT NEXT DATA command	90
11.4.8	UPDATE DATA command	91
11.4.9	COMPARE DATA function	91
11.5	Basic security handling	91
11.5.1	General	91
11.5.2	INTERNAL AUTHENTICATE command	92
11.5.3	GET CHALLENGE command	92
11.5.4	EXTERNAL AUTHENTICATE command	93
11.5.5	GENERAL AUTHENTICATE command	94
11.5.6	VERIFY command	95
11.5.7	CHANGE REFERENCE DATA command	96
11.5.8	ENABLE VERIFICATION REQUIREMENT command	96
11.5.9	DISABLE VERIFICATION REQUIREMENT command	97
11.5.10	RESET RETRY COUNTER command	97
11.5.11	MANAGE SECURITY ENVIRONMENT command	97
11.6	Miscellaneous	99
11.6.1	COMPARE command	99
11.6.2	GET ATTRIBUTE command	101
11.7	Transmission handling	101
11.7.1	GET RESPONSE command	101
11.7.2	ENVELOPE command	101
12	Application-independent card services	102
12.1	Card identification	102
12.1.1	Historical bytes	102
12.1.2	Initial data string recovery	106
12.2	Application identification and selection	107
12.2.1	EF.DIR	107
12.2.2	EF.ATR/INFO	107
12.2.3	Application identifier	108
12.2.4	Application template and related data elements	109

12.2.5	Application selection	110
12.3	Selection by path	111
12.4	Data retrieval	111
12.5	Card-originated byte strings	111
12.5.1	Triggering by the card	112
12.5.2	Queries and replies	112
12.5.3	Formats	112
12.6	General feature management	112
12.6.1	On-card services	113
12.6.2	Interface services	113
12.6.3	Profile services	113
12.6.4	Provision of additional information	114
12.7	APDU management	114
12.7.1	Extended length information	114
12.7.2	List of supported INS codes	114
Annex A (informative) Examples of object identifiers and tag allocation schemes		115
A.1	Object identifiers	115
A.2	Tag allocation schemes	115
Annex B (informative) Examples of secure messaging		117
B.1	Cryptographic checksum	117
B.2	Cryptograms	121
B.3	Control references	121
B.4	Response descriptor	121
B.5	ENVELOPE command	122
B.6	Synergy between secure messaging and security operations	122
Annex C (informative) Examples of AUTHENTICATE functions by GENERAL AUTHENTICATE commands		125
C.1	GENERAL AUTHENTICATE using witness-challenge-response triples	125
C.2	GENERAL AUTHENTICATE for a multi-step authentication protocol	129
NA.1.1	Terminal Authentication protocol	131
NA.1.2	Chip Authentication protocol	132
Annex D (informative) Application identifiers using issuer identification numbers		133
D.1	Background information	133
D.2	Format	133
Annex E (informative) BER Encoding Rules		134
E.1	BER-TLV tag fields	134
E.2	BER-TLV length fields	135
E.3	BER-TLV value fields	135
Annex F (informative) BER-TLV data object handling		136
F.1	Generations and templates in a constructed DO	136
F.2	Referencing by an extended header	137
F.3	Use of the UPDATE DATA command	139
F.4	Security attribute for one DO	141
F.5	Example of key referencing in a self-controlled DO	142
Annex G (informative) Template extension by tagged wrapper		144
G.1	General	144

G.2	Referencing within the current EF	144
G.3	Referencing within the current application DF, first example	145
G.4	Referencing in the current application DF, second example	146
G.5	Referencing out of the current application DF	147
G.6	Warnings	147
Annex H (informative) Parsing an extended header against its target DO		148
Bibliography		149