ISO/IEC 24727-3:2008-12 (E)

Identification cards - Integrated circuit card programming interfaces - Part 3: Application interface

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 3

5 Organization for interoperability 4
5.1 General 4
5.2 Computation model 4
5.3 Entity relationships on the application interface 5
5.4 Security model 13

6 Card-application-service access 16
6.1 General 16
6.2 Initialize 16
6.3 Terminate 17
6.4 CardApplicationPath 18

7 Connection service 19
7.1 General 19
7.2 CardApplicationConnect 20
7.3 CardApplicationDisconnect 21
7.4 CardApplicationStartSession 22
7.5 CardApplicationEndSession 23

8 Card-application service 24
8.1 General 24
8.2 CardApplicationList 25
8.3 CardApplicationCreate 26
8.4 CardApplicationDelete 27
8.5 CardApplicationServiceList 28
8.6 CardApplicationServiceCreate 29
8.7 CardApplicationServiceLoad 30
8.8 CardApplicationServiceDelete 31
8.9 CardApplicationServiceDescribe 32
8.10 ExecuteAction 33

9 Named data service 34
9.1 General 34
9.2 DataSetList 35
9.3 DataSetCreate 36
9.4 DataSetSelect 37
9.5 DataSetDelete 38
9.6 DSIList 39
9.7 DSICreate 40

9.8 DSIDelete 41
9.9 DSIWrite 42
9.10 DSIRead 43

10 Cryptographic service 44
10.1 General 44
10.2 Encipher 45
10.3 Decipher 46
10.4 GetRandom 47
10.5 Hash 48
10.6 Sign 49
10.7 VerifySignature 50
10.8 VerifyCertificate 51
11 Differential-identity service 52
11.1 General 52
11.2 DIDList 53
11.3 DIDCreate 54
11.4 DIDGet 55
11.5 DIDUpdate 56
11.6 DIDDelete 57
11.7 DIDAuthenticate 58
12 Authorization service 59
12.1 General 59
12.2 ACLList 60
12.3 ACLModify 61

Annex A (normative) Authentication protocols 62

A.1 General 62
A.2 Common Definitions 63
A.3 Simple Assertion 64
A.4 Asymmetric Internal Authenticate 66
A.5 Asymmetric External Authenticate 69
A.6 Symmetric Internal Authenticate 72
A.7 Symmetric External Authenticate 75
A.8 Compare 78
A.9 PIN Compare 81
A.10 Biometric Compare 84
A.11 Mutual Authentication with Key Establishment 87
A.12 Client-Application Mutual Authentication with Key Establishment 90
A.13 Client-Application Asymmetric External Authenticate 93
A.14 Modular Extended Access Control Protocol (M-EAC) 96
A.15 Key Transport with mutual authentication based on RSA 100
A.16 Age Attainment 104
A.17 Asymmetric Session Key Establishment 107
A.18 Secure PIN Compare 114
A.19 EC Key Agreement with Card-Application Authentication 118
A.20 EC Key Agreement with Mutual Authentication 122
A.21 Simple EC-DH Key Agreement 128
A.22 GP Asymmetric Authentication 132
A.23 GP Symmetric Authentication (Explicit Mode) 138
A.24 GP Symmetric Authentication (Implicit Mode) 142

Annex B (normative) Cryptographic algorithms 145

B.1 Interoperability requirements 145
B.2 Symmetric Algorithms 146
B.3 Asymmetric Algorithms 149
B.4 Elliptic Curve Algorithms 150
B.5 Hash Functions 151
B.6 Message Authentication Codes 152
B.7 Key Establishment 153

Annex C (normative) ASN.1 Representation 154

C.1 General 154

Bibliography 193