

ISO/IEC 24727-5:2011-03 (E)

Identification cards - Integrated circuit card programming interfaces - Part 5: Testing procedures

Contents		Page
Foreword		vi
Introduction		vii
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Symbols and abbreviated terms	3
5	Testing methodology	4
5.1	Terms of testing	4
5.1.1	Purpose of testing	4
5.1.2	Testing objective	4
5.1.3	Testing Principles	4
5.1.4	GCI under test:	6
5.1.5	SAL under test:	6
5.1.6	Conformance attainment	7
5.2	Conformance vector	8
5.3	Structure of tests	10
5.4	Test environment	12
5.4.1	Stack configurations	12
5.4.2	Card-application emulators	12
5.4.3	Verification and logging capability of components	12
5.4.4	Procedural element	12
6	Components	12
6.1	Service access layer API	12
6.1.1	Basic tests	12
6.1.2	Discoverability tests	12
6.2	Generic card interface	15
6.2.1	Basic test	15
6.2.2	Processing tests	15
6.2.3	Discoverability tests	17
6.3	Interface device API	19
6.4	Trusted channel API	19
6.4.1	TC_API_Open	19
6.4.2	TC_API_Close	19
6.4.3	TC_API_Write	19
6.4.4	TC_API_Read	19
6.5	SAL on-card implementation component testing	20
7	Authentication protocols	20
7.1	General	20
7.2	SAL security test sequences	21
7.2.1	Cryptographic operations	22
7.2.2	Simple assertion	26
7.2.3	Asymmetric internal authenticate	27
7.2.4	Asymmetric external authenticate	28

7.2.5	Symmetric internal authenticate	30
7.2.6	Symmetric external authenticate	31
7.2.7	Compare	33
7.2.8	PIN compare	35
7.2.9	Biometric compare	36
7.2.10	Mutual authentication with key establishment	37
7.2.11	Client-application mutual authentication with key establishment	39
7.2.12	Client-application asymmetric external authenticate	41
7.2.13	Modular extended access control protocol (M-EAC)	43
7.2.14	Key transport with mutual authentication based on RSA	45
7.2.15	Age attainment	47
7.2.16	Asymmetric session key establishment	48
7.2.17	Secure PIN compare	49
7.2.18	EC key agreement with card-application authentication	51
7.2.19	EC key agreement with mutual authentication	52
7.2.20	Simple EC-DH key agreement	54
7.2.21	GP asymmetric authentication	55
7.2.22	GP symmetric authentication (explicit mode)	56
7.2.23	GP symmetric authentication (implicit mode)	58
8	Secure messaging	60
9	Marshalling	61
9.1	ASN.1 representation	61
9.2	Web-services representation	61
10	Stack configuration testing	61
10.1	Testable interface definitions	61
10.1.1	Full-network-stack	63
10.1.2	Loyal-stack	64
10.1.3	Opaque-ICC-stack	65
10.1.4	Remote-loyal-stack	66
10.1.5	ICC-resident-stack	67
10.1.6	Remote-ICC-stack	68
11	Operational testing	68
11.1	SAL test sequences	69
12	Operational test reporting	69
13.1	SAL test sequences	70
13.2	Reference model implementations	70
13.2.1	Off card-application	70
13.2.2	Card-application emulator or test card use	70
Annex A (normative) SAL operational test sequence descriptions		71
A.1	Application management - alpha card-application data structure construction	71
A.2	Application management - first application data structure construction	92
A.3	Application management - application data structure construction error conditions	148
A.4	Application management - second application data structure construction	163
A.5	Data manipulation - card application path	207
A.6	Data manipulation - general	215
A.7	Data manipulation - global authentication	255
A.8	Application management - data structure destruction	282
Annex B (informative) Envelope APDU implementation ICC-Resident stack expected component test inputs and outputs		326
B.1	Application management - alpha card-application data structure construction	326
B.2	Application management - first application data structure construction	434
B.3	Application management - application data structure construction error conditions	755

B.4	Application management - second application data structure construction	907
B.5	Data manipulation - card application path	1156
B.6	Data manipulation - general	1271
B.7	Data manipulation - global authentication	1633
B.8	Application management - data structure destruction	1913
Annex C (informative) Non ICC-Resident stack expected component test inputs and outputs		2346
C.1	Application management - alpha card-application data structure construction	2346
C.2	Application management - first application data structure construction	2443
C.3	Application management - application data structure construction error conditions	2734
C.4	Application management - second application data structure construction	2884
C.5	Data manipulation - card application path	3112
C.6	Data manipulation - general	3228
C.7	Data manipulation - global authentication	3579
C.8	Application management - data structure destruction	3855
Annex D (informative) TLS implementation ICC-Resident stack expected component test inputs and outputs		4277
D.1	Application management - alpha card-application data structure construction	4277
D.2	Application management - first application data structure construction	4329
D.3	Application management - application data structure construction error conditions	4501
D.4	Application management - second application data structure construction	4578
D.5	Data manipulation - general	4711
D.6	Data manipulation - global authentication	4908
D.7	Application management - data structure destruction	5060
Annex E (informative) WSDL encoded IFD data structures		5307
E.1	Establish Context	5307
E.2	ReleaseContext	5308
E.3	ListIFDs	5308
E.4	GetIFDCapabilities	5309
E.5	GetStatus	5310
E.6	Wait	5312
E.7	Cancel	5314
E.8	ControlIFD	5315
E.9	Connect	5315
E.10	Disconnect	5316
E.11	BeginTransaction	5317
E.12	EndTransaction	5317
E.13	Transmit	5318
E.14	VerifyUser	5319
E.15	ModifyVerificationData	5320
E.16	Output	5321
E.17	SignalEvent	5322
Bibliography		5656