ISO/IEC 24727-2:2008-10 (E)

Identification cards - Integrated circuit card programming interfaces - Part 2: Generic card interface

Contents

Page

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 2

5 Organization for interoperability 2
5.1 Command-response pairs for interoperability 2
5.1.1 Command and response encoding 2
5.1.2 Class byte 3
5.1.3 Instruction byte 3
5.1.4 File descriptor byte 5
5.2 Card states for interoperability 6
5.3 Status words for interoperability 7
5.4 Data structures for interoperability 8
5.5 Card-applications for interoperability 9
5.5.1 Alpha card-application 9
5.5.2 Cryptographic information application 9

6 Capability descriptions 10
6.1 Card capability description (CCD) 10
6.2 Application capability description (ACD) 11
6.3 Procedural elements 11
6.3.1 Model of computation for procedural elements 12
6.3.2 Use of procedural elements 12
6.4 Determining the value of capability descriptions 13
6.4.1 General principle 13
6.4.2 Determining the value of the CCD 13
6.4.3 Determining the value of an ACD 13

Annex A (informative) Profiles for the cryptographic information application on the generic card interface 14

A.1 Profile A 14
A.1.1 EF.CIAInfo 14
A.1.2 EF.OD 14
A.1.3 EF.PrKD 14
A.1.4 EF.PuKD 14
A.1.5 EF.SKD 15
A.1.6 EF.CD 15
A.1.7 EF.AOD 15
A.1.8 EF.DCOD 15

Annex B (informative) Instances of profile A 16

B.1 eSign K Specification 16

Annex C (normative) Cryptographic information application for card-application service description 23

Annex D (informative) Example of cryptographic information application for card-application service description 28

Annex E (informative) DID Discovery 33

Bibliography 35