ISO/IEC 7816-15:2016-05 (E)

Identification cards - Integrated circuit cards - Part 15: Cryptographic information application

Contents

Page

Foreword iv

Introduction vi

1 Scope 1

2 Normative references 2

3 Terms and definitions 2

4 Symbols and abbreviated terms 5
4.1 Symbols 5
4.2 Abbreviated terms 5

5 Conventions 7

6 Cryptographic information objects 7
6.1 General 7
6.2 CIO classes 7
6.3 Attributes 8
6.4 Access restrictions 8

7 CIO files 8
7.1 Overview 8
7.2 IC card requirements 8
7.3 Card file structure 9
7.4 EF.DIR 9
7.5 of DF.CIA 11
7.5.1 Overview 11
7.5.2 CIAInfo EF 11
7.5.3 EF.OD 12
7.5.4 CIO directory files 12
7.5.5 DF.CIA selection 13

8 Information syntax in ASN.1 14
8.1 Guidelines and encoding conventions 14
8.2 Basic ASN.1 defined types 14
8.2.1 Identifier 14
8.2.2 Reference 14
8.2.3 Label 14
8.2.4 CredentialIdentifier 14
8.2.5 ReferencedValue and Path 15
8.2.6 ObjectValue 16
8.2.7 PathOrObjects 17
8.2.8 CommonObjectAttributes 17
8.2.9 CommonKeyAttributes 21
8.2.10 CommonPrivateKeyAttributes 22
8.2.11 CommonPublicKeyAttributes 23
8.2.12 CommonSecretKeyAttributes 23
8.2.13 GenericKeyAttributes 24
8.2.14 KeyInfo 24

8.2.15 CommonCertificateAttributes 24
8.2.16 GenericCertificateAttributes 25
8.2.17 CommonDataContainerObjectAttributes 25
8.2.18 CommonAuthenticationObjectAttributes 25
8.2.19 CIO type 26
8.3 CIOChoice type 26
8.4 Private key information objects 27
8.4.1 PrivateKeyChoice 27
8.4.2 Private RSA key attributes 27
8.4.3 Private elliptic curve key attributes 27
8.4.4 Private Diffie-Hellman key attributes 28
8.4.5 Private DSA key attributes 28
8.4.6 Private KEA key attributes 28
8.4.7 Generic private key information objects 28
8.5 Public key information objects 29
8.5.1 PublicKeyChoice 29
8.5.2 Public RSA key attributes 29
8.5.3 Public elliptic curve key attributes 29
8.5.4 Public Diffie-Hellman key attributes 30
8.5.5 Public DSA key attributes 30
8.5.6 Public KEA key attributes 30
8.5.7 Generic public key information objects 31
8.6 Secret key information objects 31
8.6.1 SecretKeyChoice 31
8.6.2 Algorithm independent key attributes 31
8.6.3 GenericSecretKey type 31
8.7 Certificate information objects 31
8.7.1 CertificateChoice 31
8.7.2 X.509 certificate attributes 32
8.7.3 X.509 attribute certificate attributes 32
8.7.4 SPKI certificate attributes 32
8.7.5 PGP (Pretty Good Privacy) certificate attributes 33
8.7.6 WTLS certificate attributes 33
8.7.7 ANSI X9.68 domain certificate attributes 33
8.7.8 Card verifiable certificate attributes 33
8.7.9 Generic certificate attributes 34
8.8 Data container information objects 34
8.8.1 DataContainerObjectChoice 34
8.8.2 Opaque data container object attributes 34
8.8.4 Data container information objects identified by OBJECT IDENTIFIERS 34
8.9 Authentication information objects 35
8.9.1 AuthenticationObjectChoice 35
8.9.2 Password attributes 35
8.9.3 Biometric reference data attributes 38
8.9.4 Authentication objects for external and internal authentication 40
8.10 Cryptographic information file, EF.CIAInfo 40

Annex A (normative) ASN.1 module 43

Annex B (informative) CIA example for cards with digital signature and authentication functionality 59

B.1 General 59
B.2 CIOs 59
B.3 Access control 60

Annex C (informative) Example topologies 62

Annex D (informative) Examples of CIO values and their encodings 67

D.1 General 67
D.2 EF.OD 67

D.2.1 ASN.1 value notation 67
D.2.2 ASN.1 description, tags, lengths and values 68
D.2.3 Hexadecimal DER-encoding 68
D.3 EF.ClAInfo 68
D.3.1 ASN.1 value notation 68
D.3.2 ASN.1 description, tags, lengths and values 69
D.3.3 Hexadecimal DER-encoding 69
D.4 EF.PrKD 69
D.4.1 ASN.1 value notation 69
D.4.2 ASN.1 description, tags, lengths and values 70
D.4.3 Hexadecimal DER-encoding 71
D.5 EF. CD 72
D.5.1 ASN.1 value notation 72
D.5.2 ASN.1 description, tags, lengths and values 73
D.5.3 Hexadecimal DER-encoding 73
D.6 EF.AOD 74
D.6.1 ASN.1 value notation 74
D.6.2 ASN.1 description, tags, lengths and values 74
D.6.3 Hexadecimal DER-encoding 76
D.7 EF.DCOD 76
D.7.1 ASN.1 value notation 76
D.7.2 ASN.1 description, tags, lengths and values 77
D.7.3 Hexadecimal DER-encoding of DCOD 77
D.8 Application template (within the EF.DIR) 78
D.8.1 ASN.1 value notation 78
D.8.2 ASN.1 description, tags, lengths and values in ApplicationTemplate 78
D.8.3 Hexadecimal DER-encoding of ApplicationTemplate 78
D.9 GeneralizedTime encoding guidelines 78

Annex E (informative) Examples of the use of the cryptographic information application 80

E.1 General 80
E.2 Encoding of a private key 80
E.2.1 Cryptographic information application example description 80
E.2.2 ASN.1 encoding of an RSA private key 80
E.2.3 Code encoding and decoding from the ASN.1 81
E.2.4 BER encoding 84
E.3 Encoding of a protected data container 86
E.3.1 Cryptographic information application example description 86
E.3.2 ASN.1 encoding of the protected data container object 86
E.3.3 Code from the ASN.1 for encoding and decoding BER 87
E.3.4 BER encoding 95
E.4 Encoding of a certificate 95
E.4.1 Cryptographic information application example description 95
E.4.2 ASN.1 Encoding of an X.509 certificate 95
E.4.3 Code from the ASN.1 for encoding and decoding BER 97
E.4.4 BER encoding 103
E.5 Encoding of the ESIGN cryptographic information application 107
E.5.1 Cryptographic information application example description 107
E.5.2 ASN.1 encoding of the IAS cryptographic information application 107
E.5.3 Code from the ASN.1 for encoding a decoding BER 115
E.5.4 BER encoding 115

Bibliography 117