INTERNATIONAL STANDARD

ISO/IEC 7816-15

Second edition
2016-05-15

Identification cards — Integrated circuit cards —

Part 15: Cryptographic information application

Cartes d'identification — Cartes à circuit intégré à contacts —

Partie 15: Application des informations cryptographiques

Reference number
ISO/IEC 7816-15:2016(E)

© ISO/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 Contents 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

© ISO/IEC 2016 – All rights reserved

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**
8.8.3 ISO/IEC 7816 data 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.CIAInfo **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**

 © ISO/IEC 2016 – All rights reserved

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

© ISO/IEC 2016 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

This second edition cancels and replaces the first edition (ISO/IEC 7816-15:2004), which has been technically revised. It also incorporates the Amendments ISO/IEC 7816-15:2004/Amd. 1:2007 and ISO/IEC 7816-15:2004/Amd. 2:2008 and the Technical Corrigendum ISO/IEC 7816-15:2004/Cor. 1:2004.

ISO/IEC 7816 consists of the following parts, under the general title *Identification cards — Integrated circuit cards*:

— *Part 1: Cards with contacts — Physical characteristics*

— *Part 2: Cards with contacts — Dimensions and location of the contacts*

— *Part 3: Cards with contacts — Electrical interface and transmission protocols*

— *Part 4: Organization, security and commands for interchange*

— *Part 5: Registration of application providers*

— *Part 6: Interindustry data elements for interchange*

— *Part 7: Interindustry commands for Structured Card Query Language (SCQL)*

— *Part 8: Commands and mechanisms for security operations*

— *Part 9: Commands for card management*

 © ISO/IEC 2016 – All rights reserved

— *Part 10: Electronic signals and answer to reset for synchronous cards*

— *Part 11: Personal verification through biometric methods*

— *Part 12: Cards with contacts — USB electrical interface and operating procedures*

— *Part 13: Commands for application management in a multi-application environment*

— *Part 15: Cryptographic information application*

© ISO/IEC 2016 – All rights reserved

Introduction

Integrated circuit cards with cryptographic functions can be used for secure identification of users of information systems, as well as for other core security services such as non-repudiation with digital signatures and distribution of enciphering keys for confidentiality. The objective of this part of ISO/IEC 7816 is to provide a framework for such services based on available International Standards. A main goal has been to provide a solution that may be used in large-scale systems with several issuers of compatible cards, providing for international interchange. It is flexible enough to allow for many different environments while still preserving the requirements for interoperability.

A number of data structures have been provided to manage private keys and key fragments to support a public key certificate infrastructure and flexible management of user and entity authentication.

This part of ISO/IEC 7816 is based on PKCS #15 v1.1 (see Reference [9]). The relationship between these documents is as follows:

— a common core is identical in both documents;

— those components of PKCS #15 which do not relate to IC cards have been removed.

This part of ISO/IEC 7816 includes enhancements to meet specific IC card requirements.

 © ISO/IEC 2016 – All rights reserved

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

1 Scope

This part of ISO/IEC 7816 specifies an application in a card. This application contains information on cryptographic functionality. This part of ISO/IEC 7816 defines a common syntax and format for the cryptographic information and mechanisms to share this information whenever appropriate.

The objectives of this part of ISO/IEC 7816 are to

— facilitate interoperability among components running on various platforms (platform neutral),

— enable applications in the outside world to take advantage of products and components from multiple manufacturers (vendor neutral),

— enable the use of advances in technology without rewriting application-level software (application neutral), and

— maintain consistency with existing, related standards while expanding upon them only where necessary and practical.

It supports the following capabilities:

— storage of multiple instances of cryptographic information in a card;

— use of the cryptographic information;

— retrieval of the cryptographic information, a key factor for this is the notion of “Directory Files”, which provides a layer of indirection between objects on the card and the actual format of these objects;

— cross-referencing of the cryptographic information with DOs defined in other parts of ISO/IEC 7816 when appropriate;

— different authentication mechanisms;

— multiple cryptographic algorithms (the suitability of these is outside the scope of this part of ISO/IEC 7816).

This part of ISO/IEC 7816 does not cover the internal implementation within the card and/or the outside world. It is not mandatory for implementations complying with this International Standard to support all options described.

In case of discrepancies between ASN.1 definitions in the body of the text and the module in Annex A, Annex A takes precedence.

© ISO/IEC 2016 – All rights reserved

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9564-1, *Final services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based system*

ISO/IEC 7816 (all parts), *Identification cards — Integrated circuit cards with contacts*

ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8824-2, *Information technology — Abstract Syntax Notation One (ASN.1): Information object specification*

ISO/IEC 8824-3, *Information technology — Abstract Syntax Notation One (ASN.1): Constraint specification*

ISO/IEC 8824-4, *Information technology — Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

ANSI X9.62, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
absolute path
path that starts with the file identifier '3F00'

3.2
application
data structures, data elements and program modules needed for performing a specific functionality

[SOURCE: ISO/IEC 7816-4:2013, 3.3, modified]

3.3
application identifier
data element that identifies an application in a card

Note 1 to entry: Adapted from ISO/IEC 7816-4.

3.4
application provider
entity providing the components required for performing an application in the card

[SOURCE: ISO/IEC 7816-4:2013, 3.7, modified]

 © ISO/IEC 2016 – All rights reserved

3.5
authentication information object
cryptographic information object that provides information about authentication related data

EXAMPLE A password.

3.6
authentication object directory file
elementary file containing authentication information objects

3.7
binary coded decimal
number representation where a number is expressed as a sequence of decimal digits and each decimal digit is encoded as a four bit binary number

3.8
cardholder
person to whom the card was issued

3.9
card issuer
organization or entity that issues cards

3.10
certificate directory file
elementary file containing certificate information objects

3.11
certificate information object
cryptographic information object that provides information about a certificate

3.12
command
message that initiates an action and solicits a response from the card

3.13
cryptographic information application
application in a card that contains information on cryptographic information objects, other security data elements and their intended use

3.14
cryptographic information object
structured information contained in a CIA, which describes a cryptographic data element

EXAMPLE A public key or a certificate.

3.15
data container information object
cryptographic information object that provides information about a data container

EXAMPLE A file.

3.16
data container object directory file
elementary file containing data container information objects

3.17
dedicated file
structure containing file control information, and, optionally, memory available for allocation

© ISO/IEC 2016 – All rights reserved

[SOURCE: ISO/IEC 7816-4:2013, 3.19]

3.18
Directory
DIR file
optional elementary file containing a list of applications supported by the card and optional related data elements

[SOURCE: ISO/IEC 7816-4:2013, 3.22, modified]

3.19
elementary file
set of data units or records or data objects sharing the same file identifier and the same security attribute(s)

[SOURCE: ISO/IEC 7816-4:2013, 3.23, modified]

3.20
file identifier
data element (two bytes) used to address a file

[SOURCE: ISO/IEC 7816-4:2013, 3.27]

3.21
function
process accomplished by one or more commands and resultant actions

3.22
master file
unique dedicated file representing the root in a card using a hierarchy of dedicated files

[SOURCE: ISO/IEC 7816-4:2013, 3.33, modified]

Note 1 to entry: The MF has file identifier ‘3F00’.

3.23
message
string of bytes transmitted by the interface device to the card or vice versa, excluding transmission-oriented characters

3.24
object directory file
mandatory elementary file containing information about other CIA directory files

3.25
password
data that may be required by the application to be presented to the card by its user for authentication purpose

[SOURCE: ISO/IEC 7816-4:2013, 3.37]

3.26
path
concatenation of file identifiers without delimitation

[SOURCE: ISO/IEC 7816-4:2013, 3.38]

3.27
private key directory file
elementary file containing private key information objects

 © ISO/IEC 2016 – All rights reserved

3.28
private key information object
cryptographic information object that provides information about a private key

3.29
provider
authority who has or who obtained the right to create a dedicated file in the card

[SOURCE: ISO/IEC 7816-4:2013, 3.41]

3.30
public key directory file
elementary file containing public key information objects

3.31
public key information object
cryptographic information object that provides information about a public key

3.32
record
string of bytes referenced and handled by the card within an elementary file of record structure

[SOURCE: ISO/IEC 7816-4:2013, 3.43]

3.33
relative path
path that starts with the file identifier of the current DF

3.34
secret key directory file
elementary file containing secret key information objects

3.35
secret key information object
cryptographic information object that provides information about a secret key

3.36
template
set of data objects forming the value field of a constructed data object

Note 1 to entry: Adapted from ISO/IEC 7816-6.

4 Symbols and abbreviated terms

4.1 Symbols

DF.*x*	dedicated file *x*, where *x* is the acronym of the file
EF.*x*	elementary file *x*, where *x* is the acronym of the file
'0' to '9' and 'A' to 'F'	hexadecimal digits

4.2 Abbreviated terms

For the purposes of this part of ISO/IEC 7816, the following abbreviated terms apply.

AID	application identifier

© ISO/IEC 2016 – All rights reserved