BS ISO/IEC 7816-15:2016+A1:2018

BSI Standards Publication

Identification cards — Integrated circuit cards

Part 15: Cryptographic information application

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

National foreword

This British Standard is the UK implementation of ISO/IEC 7816-15:2016+A1:2018. It supersedes BS ISO/IEC 7816-15:2016, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 99331 2

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2016.

Amendments/corrigenda issued since publication

Date	Text affected
30 June 2018	Implementation of ISO/IEC amendment A1:2018: Sections 8.4.1, 8.5.1, A.4.1 and A.5.1 amended

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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)

Documents
Document Sharing Hub
© ISO/IEC 2016

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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

Documents
Document Sharing Hub

© ISO/IEC 2016 – All rights reserved

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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

Documents
Document Sharing Hub

© ISO/IEC 2016 – All rights reserved

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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

Documents
Document Sharing Hub

© ISO/IEC 2016 – All rights reserved

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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*

AVA Documents Document Sharing Hub

© ISO/IEC 2016 – All rights reserved

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

— *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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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
AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

[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
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

AOD	authentication object directory
BCD	binary-coded decimal
CD	certificate directory
CDE	cryptographic data element
CIA	cryptographic information application
CIO	cryptographic information object
C-RP	command –response pair
CV	card-verifiable
DCOD	data container object directory
DDO	discretionary data object
DF	dedicated file
DH	Diffie-Hellman
DSA	digital signature algorithm
EC	elliptic curve
EF	elementary file
IDO	interindustry data object, as defined in ISO/IEC 7816-6
IFD	interface device
KEA	key exchange algorithm
MF	master file
OD	object directory
PKCS	public-key cryptography standard
PrKD	private key directory
PuKD	public key directory
RSA	Rivest-Shamir-Adleman
SKD	secret key directory
SPKI	simple public key infrastructure
UCS	universal multiple-octet coded character set (see ISO/IEC 10646)
URL	uniform resource locator
UTC	coordinated universal time
UTF-8	UCS transformation format 8

AVA Documents
Document Sharing Hub

© ISO/IEC 2016 – All rights reserved

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

WTLS wireless application protocol transport layer security

5 Conventions

This part of ISO/IEC 7816 presents ASN.1 notation in the **bold Helvetica** typeface. When ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in the **bold Helvetica** typeface. The names of commands, typically referenced when specifying information exchanges between cards and IFDs, are differentiated from normal text by displaying them in `Courier`.

If the items in a list are numbered (as opposed to using "–" or letters), then the items shall be considered steps in a procedure.

6 Cryptographic information objects

6.1 General

This part of ISO/IEC 7816 provides

— descriptions of objects describing cryptographic information contained in the card,

— descriptions of the intended use of this information,

— ways to retrieve this information (when appropriate),

— an abstract syntax for the information which provides the basis for encodings, and

— an object model for the information.

The information, which also may include access control information, is described in the form of CIOs.

6.2 CIO classes

This part of ISO/IEC 7816 defines four classes of CIOs as follows:

— cryptographic key information objects;

— certificate information objects;

— data container information objects;

— authentication information objects.

The logical structure of these CIOs is shown in Figure 1. The object class of cryptographic key information objects has three subclasses: private key, secret key, and public key information objects. CIOs inherit attributes from higher-level classes and may be instantiated on cards.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

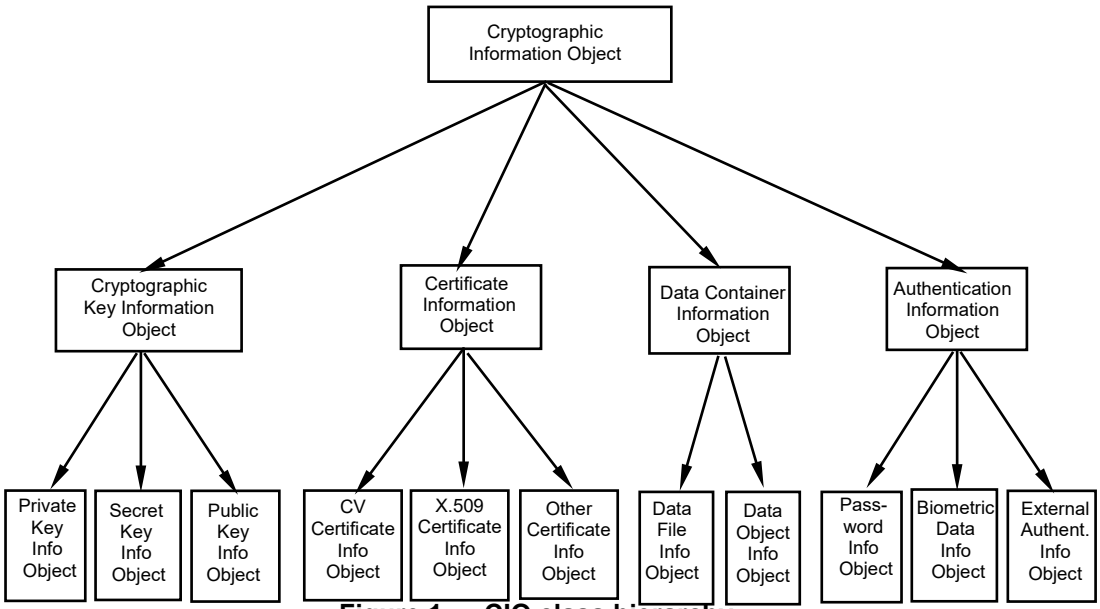


Figure 1 — CIO class hierarchy

6.3 Attributes

All CIOs have a number of attributes. Type-specific attributes are always present. Group-specific attributes and attributes common to all CIOs may be inherited as shown in Figure 2. Attributes are defined in Clause 8.

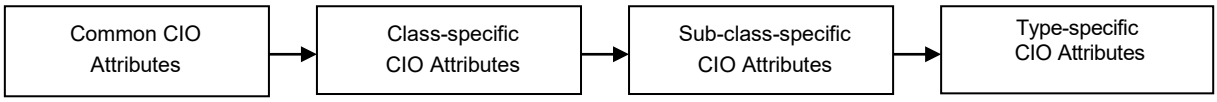


Figure 2 — Attribute inheritance concept

6.4 Access restrictions

CDEs can be private, meaning that they are protected against unauthorized access, or public. Access (read, write, etc.) to private CDEs is described by authentication information objects (which also includes authentication procedures). Conditional access (from a cardholder's perspective) is achieved with knowledge-based user information, biometric user information, or cryptographic means. Public CDEs are not protected from read-access.

7 CIO files

7.1 Overview

A CIO is contained in an elementary file, and refers, in general, to a CDE; a CIO may in some cases contain the CDE directly. A dedicated file (DF.CIA) contains CIO elementary files. Certain CIO files may be present under other dedicated files, in which case, they are referenced to from the DF.CIA.

7.2 IC card requirements

Cards shall comply with the appropriate parts of ISO/IEC 7816, when using

— hierarchic logical file systems,

— direct or indirect application selection,

— access control mechanisms,

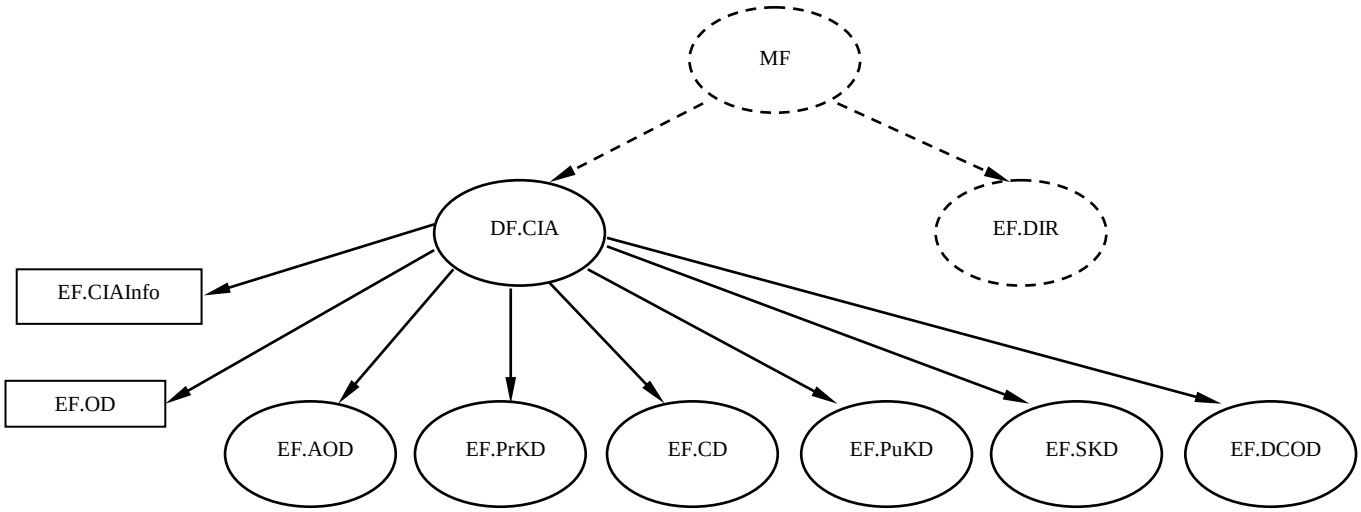
— read operations, and

— cryptographic operations.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

7.3 Card file structure

A typical card supporting this part of ISO/IEC 7816 will have the following layout:



NOTE 1 For the purpose of this part of ISO/IEC 7816, EF.DIR is only needed on cards that do not support application selection using AID as DF name as defined in ISO/IEC 7816-4 or when multiple CIAs reside on a single card.

NOTE 2 Square element files are mandatory for this part of ISO/IEC 7816 (see Table 1). MF may not be seen at the interface (see ISO/IEC 7816-4).

Figure 3 — Example contents of DF.CIA

Other possible topologies are discussed in Annex C. The contents and purpose of each file and directory are described below.

7.4 EF.DIR

This file (file identifier: '2F00') shall, if present, contain one or several application templates as defined in ISO/IEC 7816-4. The application template (tag '61') for a CIA shall at least contain the following IDOs:

— application identifier (tag '4F'), value defined in 7.5.5;

— path (tag '51'), value supplied by application provider; if **Path** is missing, it denotes a virtual DF.CIA the CIO files of which are hosted by an application, either implicitly known or defined by the CIODDO (tag '73').

— CIODDO (tag '73') conditional, with **odfPath** and **ciaInfoPath** reference CIOs; it shall be present if **Path** is missing.

Other IDOs from ISO/IEC 7816-4 may, at the application provider's discretion, be present as well. In particular, it is recommended that application providers include both the "Discretionary data objects" data object (tag '73') and the "Application label" data object (tag '50'). The application label shall contain a UTF-8 encoded label for the application, chosen by the application provider. The "Discretionary data objects" data object shall, if present, contain a DER-encoded (ISO/IEC 8825-1:1998) value of the ASN.1 type **CIODDO**:

```
CIODDO ::= SEQUENCE {
    providerId      OBJECT IDENTIFIER OPTIONAL,
    odfPath         Path OPTIONAL,
    ciaInfoPath     [0] Path OPTIONAL,
    aid             [APPLICATION 15] OCTET STRING (SIZE(1..16)),
                    (CONSTRAINED BY {-- Must be an AID in accordance with ISO/IEC 7816-4--})
                    OPTIONAL,
```

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

```
securityFileOrObject      SET OF SecurityFileOrObject OPTIONAL,
 ... -- For future extensions
 } -- Context tag 1 is historical and shall not be used
```

NOTE 1 PKCS #15 uses this tag.

NOTE 2 In accordance with ISO/IEC 7816-4, and when present in an application template, the tag **[APPLICATION 19]** ('73') replaces the **CIODDO SEQUENCE** ('30') tag, due to implicit tagging. See D.8 for an example.

NOTE 3 When located under a DF or an ADF other than DF.CIA, the by-default FileID and Short EF Identifier of EF.OD and EF.CIAInfo are respectively as defined in Table 1 unless specified otherwise by the discretionary data object CIODDO or explicit file ID definition is preferred.

```
SecurityFileOrObject ::= SEQUENCE {
        label                   Label OPTIONAL,
        communicationMode       CommunicationMode OPTIONAL,
        fileOrObjectPath        Path,
        cioSecurityId           INTEGER      OPTIONAL,
        protocol                OBJECT IDENTIFIER OPTIONAL,
        index                   [0] INTEGER (0..cia-ub-index) OPTIONAL,
        precondition            [1]INTEGER (0..cia-ub-index) OPTIONAL,

... -- For future extensions

}
```

The **providerId** component, if present, shall contain an object identifier uniquely identifying the CIA provider. The **odfPath** and **ciaInfoPath** components shall, if present, contain paths to elementary files EF.OD and EF.CIAInfo respectively or to constructed data objects nesting these files' respective contents. This provides a way for issuers to use non-standard file identifiers for these files or, alternatively, data objects tags without sacrificing interoperability. If data objects are employed, they shall be constructed without control parameter template (see ISO/IEC 7816-4). It also provides card issuers with the opportunity to share CIAInfo files between CIAs, when several CIAs reside on one card. The **aid** component shall, if present, indicate the application to which this CIA applies. The **securityFileOrObject** optional extension of **CIODDO** container refers to security protocol descriptors, i.e. OIDs nested in a logical data structure, of which the execution priority shall be ordered according the **index** value of the **precondition** attribute. **securityFileOrObject** components are

- **fileOrObjectPath**: path to the file or data object nesting a set of OIDs and further protocol relevant parameter denoting security protocols,
- **index**: attribute index assigned to **SecurityFileOrObject**,
- **precondition**: cross-reference to the index of the **SecurityFileOrObject** protocol(s) of which the execution is mandated prior to the current **SecurityFileOrObject** ones,
- **label**: attribute that may serve to identify the security file or object,
- **communicationMode**: physical interface as defined in 8.2.8 and to which the protocols listed in **fileOrObjectPath** apply. If the required communication mode cannot be fulfilled by the IFD, the **SecurityFileOrObject** may be not accessible by the IFD,
- **cioSecurityId**: identifier used as cross-reference to the authentication object required for the preleminary protocol to be executed by the IFD, and
- **protocol**: determines which of the possibly multiple protocols defined in **fileOrObjectPath** referenced structures is to be used.

In case the ICC wants to enforce a high level of privacy, **CIODDO** may only contain **SecurityFileOrObject** structure to indicate to the IFD the preliminary protocol(s) to perform. If multiple **SecurityFileOrObject** containers are present, which do not refer to each other as precondition, they are meant as alternatives. For examples of EF.DIR content with privacy-enabling features, see Table C.1; the table provides EF.DIR description for the file system topology on Figure C.5 and shows how **securityFileOrObject** component is implemented to ensure data minimization principle through access control according to ISO/IEC 7816-4.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

The use of a EF.DIR file will simplify application selection when several CIAs reside on one card. Its use is described in ISO/IEC 7816-4.

If within the application template for a CIA, one or more nested application templates (tag '61') are present, they may contain the application identifier (tag '4F'). Each application template corresponds to an application to which this CIA applies.

7.5 Contents of DF.CIA

7.5.1 Overview

Table 1 lists elementary (mandatory and optional) files in the DF.CIA, along with their reserved file identifiers. File types (linear record or transparent) are indicated in the last column.

Table 1 — Elementary files in DF.CIA

File	Mandatory	(Default) File identifier	Short EF identifier	File type
CIAInfo	X	'5032'	'12'	Transparent
OD	X	'5031'	'11'	Linear record or transparent
AODs				Linear record or transparent
PrKDs				Linear record or transparent
PuKDs				Linear record or transparent
SKDs				Linear record or transparent
CDs				Linear record or transparent
DCODs				Linear record or transparent
—		'5033'		Reserved for historical reasons

7.5.2 CIAInfo EF

The CIAInfo EF shall contain information about the card and its capabilities, pertaining to the use of CIOs. The following information shall always be present:

— version number;

— card characteristics (e.g. read only).

The following information may be found:

— CIA serial number;

— manufacturer identification;

— card label;

— allocated security environments;

— file structures;

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

— supported algorithms;

— issuer identification;

— holder authentication;

— time of last update.

7.5.3 EF.OD

The object directory file (EF.OD) is an elementary file, unless specified otherwise by CIODDO, which may contain references to other CIO EFs. Figure 4 shows the relationship between EF.OD and other CIO EFs (for a reason of simplicity, only one referenced file of each type is shown). The ASN.1 syntax for the contents of EF.OD is described in 8.3.

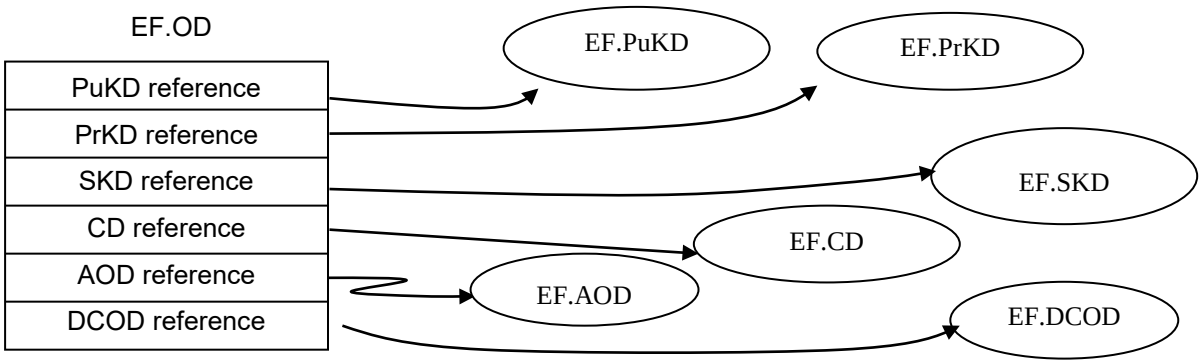


Figure 4 — Indirect retrieval of CIOs using EF.OD

7.5.4 CIO directory files

Each CIO directory file contains CIOs of a certain kind:

— private key directory files contain private key information objects;

— public key directory files contain public key information objects;

— secret key directory files contain secret key information objects;

— certificate directory files contain certificate information objects;

— data container object directory files contain data container information objects;

— authentication object directory files contain authentication information objects.

Multiple CIO directory files of the same kind may be present in a DF.CIA.

The object directory file EF.OD is unique and contains references to CIO directory files.

NOTE 1 If a CIO directory file of a certain kind exists in a DF.CIA, it will usually not be empty.

NOTE 2 CIO directory files may also be found in other DFs in the card.

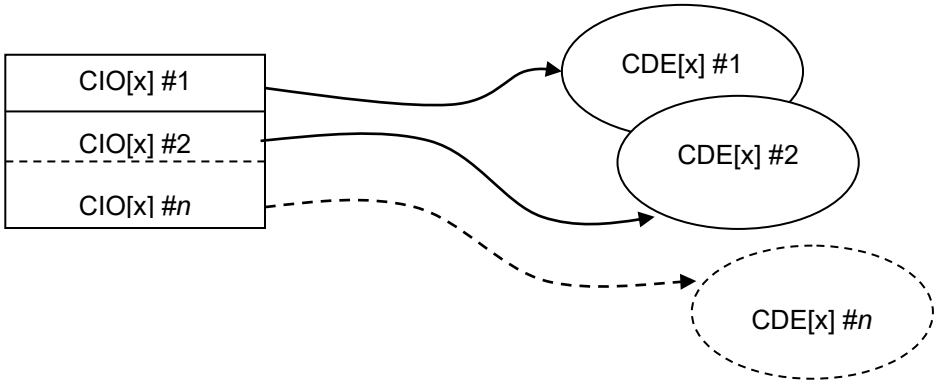
NOTE 3 CIOs can be stored directly in an EF.OD (without any indirection) or in CIO directory files. CDEs can likewise be stored directly in CIOs or be referenced by them.

The use of indirection simplifies personalization, allows for more flexible access rules, and is recommended.

When CIOs reference CDEs that are logically linked (e.g. a private key CIO and a corresponding public key CIO), the CDEs shall have the same CIO identifier.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

Figure 5 describes the general structure of these files.



NOTE Letter *x* stands for the kind of the information object which holds the information.

Figure 5 — Indirect retrieval of CDEs using CIOs

7.5.5 DF.CIA selection

The AID of a DF.CIA consists of two fields, the standard identifier E8 28 BD 08 0F (mandatory), optionally followed by either

— a one-byte index in the range ‘00’ to ‘7F’, followed by a proprietary application identifier extension (PIX), or

— a (possibly right-truncated) AID (e.g. of an application using this CIA) using a registered application provider identifier from registration category 'A' or 'D' (see ISO/IEC 7816-4).

The length of the AID shall not exceed 16 bytes. The format of the AID is therefore:

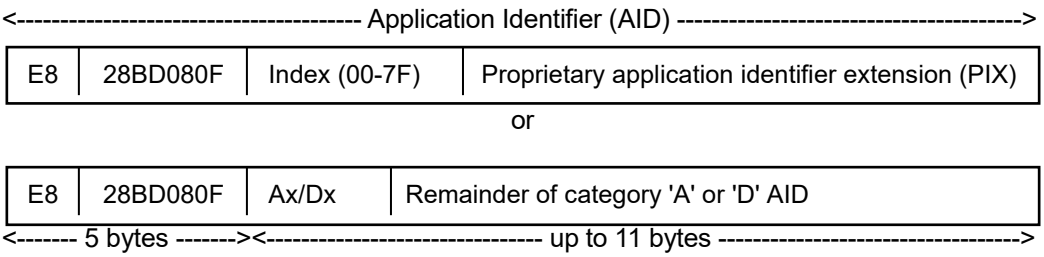


Figure 6 — AID formats

DF.CIA may be selected using its AID by cards supporting direct application selection.

NOTE For historical reasons, DF.CIA may be selected using the AID: A0 00 00 00 63 50 4B 43 53 2D 31 35.

If direct application selection is not possible, an EF.DIR file with contents as specified in 7.4 shall be used.

When several DF.CIAs reside on one card, they may be distinguished by information in the application template in EF.DIR. It is recommended that the application label (tag ‘50’) also be present to simplify the man-machine interface (e.g. vendor name in short form).

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

8 Information syntax in ASN.1

8.1 Guidelines and encoding conventions

This part of ISO/IEC 7816 uses ASN.1 [see ISO/IEC 8824 (all parts)] to describe CIOs. When stored in a card, DER-encoding of CIO values are assumed. Annex A contains a complete specification in ASN.1 of all CIOs; the text of this clause is explanatory only.

The contents of a CIO directory file is the concatenation of 0, 1 or more DER-encoded values of the same type; see, e.g. Annex D.

NOTE In this part of ISO/IEC 7816, BIT STRING type can be declared as extensible with extension markers provided related list is always numbered with consecutive numbers and it is recommended accordingly to enforce consecutive positions of extended bits.

8.2 Basic ASN.1 defined types

8.2.1 Identifier

```
Identifier ::= OCTET STRING (SIZE (0..cia-ub-identifier))
```

The **Identifier** type is used as a CIO identifier. For cross-reference purposes, two or more CIOs may have the same **Identifier** value. One example of this is a private key and one or more corresponding certificates.

8.2.2 Reference

```
Reference ::= CHOICE {
    uniqueByteRef     INTEGER (0..cia-ub-reference),
    multiByteRef      [1] OCTET STRING(SIZE(4..20))
}
```

This type is used for generic reference purposes; for a multiple-byte reference or a reference value exceeding 255, multiByteRef may be used.

8.2.3 Label

```
Label ::= UTF8String (SIZE(0..cia-ub-label))
```

This type is used for all labels (i.e. user assigned object names).

8.2.4 CredentialIdentifier

```
CredentialIdentifier {KEY-IDENTIFIER : IdentifierSet} ::= SEQUENCE {
        idType  KEY-IDENTIFIER.&id ({IdentifierSet}),
        idValue KEY-IDENTIFIER.&Value ({IdentifierSet}{@idType})
        }

KeyIdentifiers KEY-IDENTIFIER ::= {
        issuerAndSerialNumber          |
        issuerAndSerialNumberHash      |
        subjectKeyId                   |
        subjectKeyHash                 |
        issuerKeyHash                  |
        issuerNameHash                 |
        subjectNameHash                |
        pgp2KeyId                      |
        openPGPKeyId                   |
        certificateHolderReference,
        ... -- For future extensions
        }

KEY-IDENTIFIER ::= CLASS {
        &id  INTEGER UNIQUE,
```


© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

```
&Value
} WITH SYNTAX {
SYNTAX &Value IDENTIFIED BY &id
}
```

The **CredentialIdentifier** type is used to identify a particular key or certificate. There are currently nine members in the set of identifiers for private keys and certificates, **KeyIdentifiers**.

— **issuerAndSerialNumber**: The value of this type shall be a **SEQUENCE** consisting of the issuer's distinguished name and the serial number of a certificate which contains the public key associated with the private key.

— **issuerAndSerialNumberHash**: As for **issuerAndSerialNumber** but the value is an **OCTET STRING** which contains a SHA-1 hash value of this information in order to preserve space.

— **subjectKeyId**: The value of this type shall be an **OCTET STRING** with the same value as the **subjectKeyIdentifier** certificate extension in an ISO/IEC 9594-8 certificate which contains the public key associated with the private key. This identifier can be used for certificate chain traversals.

— **subjectKeyHash**: An **OCTET STRING** which contains the SHA-1 hash of the public key associated with the private key.

— **issuerKeyHash**: An **OCTET STRING** which contains the SHA-1 hash of the public key used to sign the requested certificate.

— **issuerNameHash**: An **OCTET STRING** that contains a SHA-1 hash of the issuer's name as it appears in the certificate.

NOTE This identifier can, in conjunction with the **subjectNameHash** identifier, also be used for certificate chain construction.

— **subjectNameHash**: An **OCTET STRING** that contains a SHA-1 hash of the subject's name as it appears in the certificate.

— **pgp2KeyId**: An **OCTET STRING (SIZE(8))** that contains a PGP2 key identifier.

NOTE PGP 2 key identifiers are defined in IETF RFC 4880 (see Reference [4]).

— **openPGPKeyId**: An **OCTET STRING (SIZE (8))** that contains an OpenPGP key identifier.

NOTE OpenPGP key identifiers are defined in IETF RFC 4880 (see Reference [4]).

— **certificateHolderReference**: An OCTET STRING that denotes the holder of an ISO/IEC 7816-8 card verifiable certificate and that is used as subject key identifier to reference the public key of the certificate holder.

8.2.5 ReferencedValue and Path

```
ReferencedValue ::= CHOICE {
        path        Path,
        url         URL
        } -- The syntax of the object is determined by the context

URL ::= CHOICE {
        url         CHOICE {printable PrintableString, ia5 IA5String},
        urlWithDigest [3] SEQUENCE {
            url             IA5String,
            digest          DigestInfoWithDefault
            }
        }

Path ::= SEQUENCE {
        efidOrTagChoice CHOICE {
```

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

```
        efidOrPath OCTET STRING,
        tagRef    [0]  SEQUENCE {
                  tag OCTET STRING,
                  efidOrPath OCTET STRING OPTIONAL
                        },
        appFileRef [1]  SEQUENCE        {
                  aid [APPLICATION 15] OCTET STRING,
                  efidOrpath OCTET STRING
        },
        appTagRef [2]  SEQUENCE{
                  aid [APPLICATION 15] OCTET STRING,
                  tag OCTET STRING,
                  efidOrPath OCTET STRING OPTIONAL
        }
                  },
        index             INTEGER (0..cia-ub-index) OPTIONAL,
        length            [0] INTEGER (0..cia-ub-index) OPTIONAL
        }( WITH COMPONENTS {..., index PRESENT, length PRESENT}|
           WITH COMPONENTS {..., index ABSENT, length ABSENT})
```

A **ReferencedValue** is a reference to a CIO value of some kind. This can either be some external reference (captured by the **url** choice) or a reference to a file on the card (the **path** identifier). The syntax of the value is determined by the context.

In the **path** case, identifiers **index** and **length** may specify a specific location within the file. If the file is a linear record file, **index**, when present, shall specify the record number (in the ISO/IEC 7816-4 definition) and **length** can be set to **0** (if the card's operating system allows an L_e parameter equal to '00' in a 'READ RECORD' command). Lengths of fixed records may be found in the **CIAInfo** file as well (see 8.10). If the file is a transparent file, **index**, when present, shall specify an offset within the file, and **length,** the length of the segment (**index** would then become parameter P_1 and/or P_2 and **length** the parameter L_e in a 'READ BINARY' command). By using **index** and **length**, several objects may be stored within the same transparent file. **aid** and **tag** are used for referencing from CIA of logical data structures located in application context.

NOTE From the above follows that a **length** of **0** indicates that the file pointed to by **efidOrPath** is a linear record file.

When **efidOrPath** is

— empty, no file is referenced by it,

— one byte long, it references a short EF identifier in the most significant five bits (bits b3, b2 and b1 shall be set to 0),

— two bytes long, it references a file by its file identifier,

— longer than two bytes and consists of an even number of bytes, it references a file either by an absolute or relative path (i.e. concatenation of file identifiers), and

— longer than two bytes and consists of an odd number of bytes, it references a qualified path (see ISO/IEC 7816-4).

In the **url** case, the URL may either be a simple URL or a URL in combination with a cryptographic hash of the object stored at the given location. In the **urlWithDigest** case, assuming that the CIO card is protected against unauthorized data modifications, the **digest** component will protect the externally protected object against unauthorized modifications too.

NOTE The URL syntax is defined in IETF RFC 3986 (see Reference [3]).

8.2.6 ObjectValue

```
ObjectValue { Type } ::= CHOICE {
        indirect   ReferencedValue,
        direct     [0] Type,
```


© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

```
        ... -- For future extensions
        }
```

An object value of type **ObjectValue** type shall, unless otherwise mentioned, be stored by indirect reference (i.e. by pointing to another location where the actual value resides).

8.2.7 PathOrObjects

```
PathOrObjects {ObjectType} ::= CHOICE {
        path        Path,
        objects     [0] SEQUENCE OF ObjectType,
        ... -- For future extensions
        }
```

The **PathOrObjects** type is used to reference sequences of objects residing either within the OD or in another file. If the **path** alternative is used, the referenced file shall contain the concatenation of 0, 1 or more DER-encoded values of the given type. Any number of 'FF' or '00' octets may occur before, between or after the values without any meaning (i.e. as padding for unused space or deleted values). The **path** alternative is strongly recommended (see Note 4 in 7.5.4).

8.2.8 CommonObjectAttributes

NOTE This type is a container for attributes common to all CIOs.

```
CommonObjectAttributes ::= SEQUENCE {
        label               Label OPTIONAL,
        flags               CommonObjectFlags OPTIONAL,
        authId              Identifier OPTIONAL,
        userConsent         INTEGER (1..cia-ub-userConsent) OPTIONAL,
        accessControlRules  SEQUENCE SIZE (1..MAX) OF AccessControlRule OPTIONAL,
        currentLCS          LifeCycleStatus OPTIONAL,
    ...

        } (CONSTRAINED BY {-- authId should be present if flags.private is set.
        -- It shall equal an authID in one authentication object in the AOD -- })

CommonObjectFlags ::= BIT STRING {
        private             (0),
        modifiable          (1),
        internal            (2)
        } -- Bit (2) is present for historical reasons and shall not be used

AccessControlRule ::= SEQUENCE {
        accessMode          AccessMode,
        securityCondition   SecurityCondition,
        communicationMode       CommunicationMode OPTIONAL,
        lifeCycleStatus         LifeCycleStatus OPTIONAL,
        verifLimitDates         RangeOfDate  OPTIONAL,

        ... -- For future extensions
        }

AccessMode ::= BIT STRING {
        read        (0),
        update      (1),
        execute     (2),
        delete      (3),
        attribute   (4),
        pso_cds     (5),
        pso_verif   (6),
        pso_dec     (7),
        pso_enc     (8),
        int_auth    (9),
        ext_auth    (10)

        }
```

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

```
CommunicationMode::= BIT STRING {
   contact (0),
   contactLess (1),
   usb (2),
   nfc (3),
   contactC6 (4)

}

LifeCycleStatus::=  ENUMERATED  {creation(0),  init(1),  op-activated(2),  op-deactivated(3),  termination(4),
proprietary(5),…}

RangeOfDate ::= SEQUENCE {
      startDate            GeneralizedTime   OPTIONAL,
      endDate              [0] GeneralizedTime     OPTIONAL
}


SecurityCondition ::= CHOICE {
            always                  NULL,
            authId                  Identifier,
            authReference           AuthReference,
            not                     [0] SecurityCondition,
            and                     [1] SEQUENCE SIZE (2..cia-ub-securityConditions) OF SecurityCondition,
            or                      [2] SEQUENCE SIZE (2..cia-ub-securityConditions) OF SecurityCondition,
            ... -- For future extensions
            }
AuthReference ::= SEQUENCE {
            authMethod      AuthMethod,
            seIdentifier    Reference OPTIONAL
            }
AuthMethod ::= BIT STRING {secureMessaging(0), extAuthentication(1), userAuthentication(2), always(3)}
```

The **label** is purely for display purposes (man-machine interface), for example, when a user has several certificates for one key pair (e.g. “bank certificate”, “e-mail certificate”).

The **flags** component indicates whether the particular object is private or not and whether it is of type read-only or not. A **private** object may only be accessed after proper authentication (e.g. password verification). If an object is marked as **modifiable**, it should be possible to update the value of the object. If an object is both **private** and **modifiable**, updating is only allowed after successful authentication, however.

The **authId** component gives, in the case of a private object, a cross-reference back to the authentication object used to protect this object (for a description of authentication objects, see 8.9).

The **userConsent** component gives, in the case of a private object (or an object for which access conditions has been specified), the number of times an application may access the object without explicit consent from the user (e.g. a value of **3** indicates that a new authentication will be required before the first, the 4th, the 7th, etc. access). The card may enforce this value, e.g. through the use of “counter objects” (see ISO/IEC 7816-8). A value of **1** means that a new authentication is required before each access.

The **accessControlRules** component gives an alternative, and more fine-grained, way to inform a host-side application about security conditions for various methods of accessing the object in question. Any Boolean expression in available authentication methods is allowed. If a certain access mode is not allowed, there shall be no access control rule for it (i.e. it is implicit). If this component is not present, access control rules will have to be deduced by other means. The **authReference** option allows for a closer coupling with other parts of ISO/IEC 7816, through the reference to Security Environments and identification of the class of authentication method (**authMethod**).

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

The **AccessMode** component gives information of access mode to the object or its attribute. **read**, **update**, **execute**, and **delete** are access mode for the object itself and **attribute** is for its attribute change, for example, resetting key retry counter.

Other access mode attributes are intended for the completion of the **execute** access mode meaning. Those further attributes are to be set along with **execute** attribute to describe the action. **pso_cds** is for PERFORM SECURITY OPERATION (PSO) COMPUTE DIGITAL SIGNATURE command, **pso_verify** for PSO VERIFY CERTIFICATE command, **pso_dec** for PSO DECIPHER command, **pso_enc** for PSO ENCIPHER command, **int_auth** for INTERNAL AUTHENTICATE command, and **ext_auth** for EXTERNAL AUTHENTICATE command.

The **CommunicationMode** component indicates for which physical interface the accessControlRule applies. The **nfc** option relates to Near Field Communication protocol (see ISO/IEC 18092); the **usb** option relates to Universal Serial Bus protocol (see ISO/IEC 7816-12); the **contactC6** option is provided for legacy cards using contact C6 for programming power required to write or to erase the internal non-volatile memory (see ISO/IEC 7816-3); the **contactLess** option relates to proximity cards supporting ISO/IEC 14443; the **contact** option relates to cards with contacts (see ISO/IEC 7816-3). These options are according the transport type descriptor as per ISO/IEC 7816-4:2012, 7.4.12.1.

The **LifeCycleStatus** component indicates the life cycle status to which the AccessControlRule applies for any file or data object (see ISO/IEC 7816-4:2012, 7.4.12 for definitions).

— **creation**: Creation state

— **init**: Initialisation state

— **op-activated**: Operational (activated)

— **op-deactivated**: Operational (deactivated)

— **termination**: Termination state

— **proprietary**: Proprietary state

The **verifLimitDates** component is optional and provides the time interval during which the **AccessControlRule** to which it is attached is allowed for verification; outside the limit dates indicated by either both or one of **startDate** and **endDate** attributes, the **AccessControlRule** cannot be verified anymore. To achieve the fit between **verifLimitDates** and the actual date, i.e. date of the day, when **AccessControlRule** verification occurs, a time-stamped token may, as example, be delivered to the card to check the date of the day. As application examples: (1) an IFD presents its certificate with extension denoting a range of dates; if the verification limit dates indicated in Access Control rules (**startDate**, **endDate**) fit the range presented in the certificate, the IFD can authenticate to the card and access the authorized services accordingly; (2) A cryptographic object lifespan can be set to a determined interval of time, between **startDate** and **endDate**, so that, once the validity period after card issuance is elapsed, the cryptographic object is locked and may require a specific activation to resume. Each time this object is requested by the outside world, a timestamp may be presented to the ICC; (3) A quality control procedure on batches of cards protected by a password based mechanism (of which the password should only be known to the card owner) may resort to a temporary password for quality control purposes; such a password can be valid only during the interval between **startDate** and **endDate**.

— **startDate** and **endDate** components shall be encoded as a DO with a tag of [UNIVERSAL 24] class (ASN.1 encoding rules, ISO/IEC 8825-1), i.e. DO'18', and nested within a SEQUENCE. See D.9 for **GeneralizedTime** encoding guidelines conformant to ISO/IEC 8825-1.

NOTE 1 When the **accessControlRules** component and the **authID** component both are present, information in the **accessControlRule** component takes precedence. This can occur for backwards-compatibility reasons.

NOTE 2 Since properties related to access control can be deduced, e.g. by studying EFs FCI, such information is optional and not necessary when these circumstances applies (see also ISO/IEC 7816-4).

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

NOTE 3 The access control information represented in these structures reflects access control rules in the card but is not necessarily used as such by the card.

NOTE 4 When present, **currentLCS** component may reflect the **LifeCycleStatus** of the CIO.

NOTE 5 If implemented by the card, **verifLimitDates** attribute may require recording by the card of the first trusted time reference delived to the card, i.e. timestamp for the current date from a trusted party, which may be updated each time a more recent subsequent timestamp is presented to the card, or rejected otherwise.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

8.2.9 CommonKeyAttributes

```
CommonKeyAttributes ::= SEQUENCE {
        iD              Identifier,
        usage           KeyUsageFlags,
        native          BOOLEAN DEFAULT TRUE,
        accessFlags     KeyAccessFlags OPTIONAL,
        keyReference    KeyReference OPTIONAL,
        startDate       GeneralizedTime OPTIONAL,
        endDate         [0] GeneralizedTime OPTIONAL,
        algReference    [1] SEQUENCE OF Reference OPTIONAL,
        ... -- For future extensions
        }

KeyUsageFlags ::= BIT STRING {
        encipher            (0),
        decipher            (1),
        sign                (2),
        signRecover         (3),
        keyEncipher         (4),
        keyDecipher         (5),
        verify              (6),
        verifyRecover       (7),
        derive              (8),
        nonRepudiation      (9)
        }

KeyAccessFlags ::= BIT STRING {
        sensitive           (0),
        extractable         (1),
        alwaysSensitive     (2),
        neverExtractable    (3),
        cardGenerated       (4)
        }

KeyReference ::= INTEGER
```

The **iD** component shall be unique for each key information object, except when a public key information object and its corresponding private key information object are stored on the same card. In this case, the information objects shall share the same identifier (which may also be shared with one or several certificate information objects; see 8.2.15).

The **usage** component (**encipher, decipher, sign, signRecover, keyEncipher, keyDecipher, verify, verifyRecover, derive** and **nonRepudiation**) signals the possible usage of the key. Actual algorithms and methods used for these operations are implicit and not defined in this part of ISO/IEC 7816. To map between ISO/IEC 9594-8 **keyUsage** flags for public keys, CIO flags for public keys, and CIO flags for private keys, use Table 2.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

Table 2 — Mapping between CIO key usage flags and ISO/IEC 9594-8 key usage flags

Key usage flags for public keys in ISO/IEC 9594-8 public key certificates	Corresponding CIO key usage flags for public keys	Corresponding CIO key usage flags for private keys
DataEncipherment	Encipher	Decipher
DigitalSignature, keyCertSign, cRLSign (signature algorithms without message recovery)	Verify	Sign
DigitalSignature, keyCertSign, cRLSign (signature algorithms with message recovery)	VerifyRecover	SignRecover
KeyAgreement	Derive	Derive
KeyEncipherment	KeyEncipher	KeyDecipher
NonRepudiation	NonRepudiation	NonRepudiation
NOTE 1 Implementations should verify that all key usage flags for a particular key pair is consistent. NOTE 2 Only those ISO/IEC 9594-8 key usage flags that are relevant for this part of ISO/IEC 7816 have been given a mapping.		

The **native** component identifies whether the cryptographic algorithms associated with the key are implemented in the card hardware.

The interpretation of the **KeyAccessFlags** bits shall be as follows:

— **sensitive** indicates that the key material cannot be revealed in plaintext outside the card;

— if **extractable** is not set, the key material cannot be extracted from the card, even in encrypted form;

— **alwaysSensitive** indicates that the key has always been **sensitive**;

— **neverExtractable** indicates that the key has never been **extractable**;

— **cardGenerated** indicates that the key was randomly generated on the card.

The **accessFlags** component may be absent in cases where its value can be deduced by other means.

The **keyReference** component is only applicable for cards with cryptographic capabilities. If present, it contains a card-specific reference to the key in question (for further information, see ISO/IEC 7816-4 and ISO/IEC 7816-8).

NOTE The value of the **keyReference** component is intended for use in key reference DOs (ISO/IEC 7816-4) and any values, also negative values, are conceivable.

The **startDate** and **endDate** components, if present, indicate the period during which the key is valid for use.

The **algReference** component identifies algorithms the key may be used with by referencing **supportedAlgorithm** values from the EF.CIAInfo file.

8.2.10 CommonPrivateKeyAttributes

```
CommonPrivateKeyAttributes ::= SEQUENCE {
        name            Name OPTIONAL,
        keyIdentifiers  [0] SEQUENCE OF CredentialIdentifier {{KeyIdentifiers}} OPTIONAL,
        generalName     [1] GeneralNames OPTIONAL,
```


© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

```
        keyUsageConstraints     [2] KeyUsageConstraints OPTIONAL,
    ... -- For future extensions
    }
(CONSTRAINED BY {-- if keyUsageConstraints present, CommonObjectAttributes.userConsent should be set--})
```

The **name** component, when present, names the owner of the key, as specified in a corresponding certificate's **subject** component.

Values of the **keyIdentifiers** component can be matched to identifiers from external messages or protocols to select the appropriate key to a given operation. The values can also be transmitted to a receiving party to indicate which key was used. A number of mechanisms for identifying a key are supported (see 8.2.4).

The **generalName** component, when present, provides other ways to identify the owner of the key.

```
KeyUsageConstraints ::= SEQUENCE {
        keyUsageConstraintsFlag   BIT STRING {
        immediateUsage  (0)

            },
        refOID     OBJECT IDENTIFIER OPTIONAL,
        …-- For future extensions
        }
```

CommonPrivateKeyAttributes.keyUsageConstraintsFlag: this component indicates whether

— the interface device is not allowed to send a C-RP between the preparation phase and the usage phase on the logical channel used for key usage, i.e **immediateUsage** set to 1, or

— that the interface device may send one or several C-RP(s) between the preparation phase and the usage phase, on arbitrary logical channels, i.e. **immediateUsage** not set.

The OID reference **refOID,** if present, shall provide details for key usage constraints. If both **userConsent** attribute (see 8.2.8) and **keyUsageConstraints** component are implemented, **userConsent** shall be correlated with **keyUsageConstraints** to set the number of times an application may access the key object without explicit consent from the user.

8.2.11 CommonPublicKeyAttributes

```
CommonPublicKeyAttributes ::= SEQUENCE {
        name            Name OPTIONAL,
        trustedUsage    [0] Usage OPTIONAL,
        generalName     [1] GeneralNames OPTIONAL,
        keyIdentifiers  [2] SEQUENCE OF CredentialIdentifier {{KeyIdentifiers}} OPTIONAL,
        ... -- For future extensions
        }
```

The interpretation of the **name**, **generalName** and **keyIdentifiers** components of the **CommonPublicKeyAttributes** type shall be the same as for the corresponding components of the **CommonPrivateKeyAttributes**.

The **trustedUsage** component indicates one or more purposes for which the public key is trusted by the cardholder (see 8.2.15).

NOTE The exact semantics of "trust" is outside the scope of this part of ISO/IEC 7816.

8.2.12 CommonSecretKeyAttributes

```
CommonSecretKeyAttributes ::= SEQUENCE {
        keyLen    INTEGER OPTIONAL, -- keylength (in bits)
        ... -- For future extensions
        }
```

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

The optional **keyLen** component signals the key length used, in those cases where a particular algorithm can have a varying key length.

8.2.13 GenericKeyAttributes

```
GenericKeyAttributes ::= SEQUENCE {
        keyType  CIO-ALGORITHM.&objectIdentifier ({AllowedAlgorithms}),
        keyAttr   CIO-ALGORITHM.&Parameters ({AllowedAlgorithms}{@keyType})
        }

AllowedAlgorithms CIO-ALGORITHM ::= {...}
```

This type is intended to contain information specific to a key of a given kind. The definition of the **AllowedAlgorithms** information object set is deferred, perhaps to standardized profiles or to protocol implementation conformance statements. The set is required to specify a table constraint on the components of **GenericKeyAttributes**.

8.2.14 KeyInfo

```
KeyInfo {ParameterType, OperationsType} ::= CHOICE {
        paramsAndOps SEQUENCE {
            parameters ParameterType,
            operations  OperationsType OPTIONAL
            },
        reference        Reference -- Historical, not to be used
        }
```

NOTE PKCS #15 uses the **reference** option.

This type, which is an optional part of each private and public key type, contains either algorithm-specific details about the parameters of the key and operations supported by the card or a reference to such information. If present, algorithm-specific values override any values referenced by the **CommonKeyAttributes.algReference** component.

8.2.15 CommonCertificateAttributes

```
CommonCertificateAttributes ::= SEQUENCE {
        iD               Identifier,
        authority        BOOLEAN DEFAULT FALSE,
        identifier       CredentialIdentifier {{KeyIdentifiers}} OPTIONAL,
        certHash         [0] CertHash OPTIONAL,
        trustedUsage     [1] Usage OPTIONAL,
        identifiers      [2] SEQUENCE OF CredentialIdentifier {{KeyIdentifiers}} OPTIONAL,
        validity         [4] Validity OPTIONAL,
        ... -- For future extensions
        } -- Context tag [3] is reserved for historical reasons
```

NOTE PKCS #15 uses context tag [3].

```
Usage ::= SEQUENCE {
        keyUsage KeyUsage OPTIONAL,
        extKeyUsage SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER OPTIONAL,
        ... – For future extensions
        } (WITH COMPONENTS {..., keyUsage PRESENT} | WITH COMPONENTS {..., extKeyUsage PRESENT})
```

When a public key in a certificate referenced by a certificate information object corresponds to a private key referenced by a private key information object, then the information objects shall share the same value for the **iD** component. This requirement simplifies searches for a private key corresponding to a particular certificate and vice versa. Multiple certificates for the same key shall share the same value for the **iD** component.

The **authority** component indicates whether the certificate is for an authority (e.g. certification authority) or not.

The **identifier** component is present for historical reasons only and the **identifiers** component shall be used instead.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

The **certHash** component is useful from a security perspective when a certificate is stored externally to the card (the **url** choice of **ReferencedValue**) since it enables a user to verify that no one has tampered with the certificate.

The **trustedUsage** component indicates one or more purposes for which the certified public key is trusted by the cardholder. Object identifiers for the **extKeyUsage** component may be defined by any organization with a need. For actual usage, the intersection of the indicated usage in this component and the **keyUsage** extension (if present) in the certificate itself should be taken. If the **trustedUsage** component is absent, all usage is possible.

NOTE 1 The exact semantics of "trust" is outside the scope of this part of ISO/IEC 7816.

NOTE 2 To find a cardholder certificate for a specific usage, use the **commonKeyAttributes.usage** component and follow the cross-reference (**commonKeyAttributes.iD**) to an appropriate certificate.

The **identifiers** component simplifies the search of a particular certificate when the requester knows (and conveys) some distinguishing information about the requested certificate. This can be used, for example, when a user certificate has to be chosen and sent to a server as part of a user authentication, and the server provides the client with distinguishing information for a particular certificate. Use of the **subjectNameHash** and **issuerNameHash** alternatives may also facilitate fast chain building.

The **validity** component provides information about the certificate's validity period.

8.2.16 GenericCertificateAttributes

```
GenericCertificateAttributes ::= SEQUENCE {
        certType CIO-OPAQUE.&id ({AllowedCertificates}),
        certAttr   CIO-OPAQUE.&Type ({AllowedCertificates}{@certType})
        }

AllowedCertificates CIO-OPAQUE ::= {...}
```

This type is intended to contain information specific to a certificate of any kind. The definition of the **AllowedCertificates** information object set is deferred, perhaps to standardized profiles or to protocol implementation conformance statements. The set is required to specify a table constraint on the components of **GenericCertificateAttributes**.

8.2.17 CommonDataContainerObjectAttributes

```
CommonDataContainerObjectAttributes ::= SEQUENCE {
        applicationName      Label OPTIONAL,
        applicationOID       OBJECT IDENTIFIER OPTIONAL,
        iD                   Identifier OPTIONAL,
        ... -- For future extensions
        } (WITH COMPONENTS {..., applicationName PRESENT}
        | WITH COMPONENTS {..., applicationOID PRESENT})
```

The **applicationName** component is intended to contain the name or the application to which the data container object in question "belongs".

The **applicationOID** component is intended to contain the registered object identifier for the application to which the data container object in question 'belongs'.

In order to avoid application name collisions, at least the **applicationOID** alternative is recommended. As indicated in ASN.1, at least one of the components has to be present in a value of type **CommonDataContainerObjectAttributes**.

The **iD** component may be used to associate a certain data container object with some other CIO, e.g. a private key information object.

8.2.18 CommonAuthenticationObjectAttributes

```
CommonAuthenticationObjectAttributes ::= SEQUENCE {
```

Documents
Document Sharing Hub

© ISO/IEC 2016 – All rights reserved

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

```
        authId          Identifier OPTIONAL,
        authReference   Reference OPTIONAL,
        seIdentifier    [0] Reference OPTIONAL,
        ... -- For future extensions
        }
```

The **authId** shall be a unique identifier. It is used for cross-reference purposes from private CIOs.

The **authReference** component, when present, shall contain a value of a "key reference" object (see ISO/IEC 7816-4), which is the way to reference these keys in Security Environments.

The **seIdentifier** component, when present, identifies the security environment to which the authentication object belongs.

8.2.19 CIO type

This type is a template for all kinds of CIOs. It is parameterized with object class attributes, object subclass attributes and object type attributes.

```
CIO {ClassAttributes, SubClassAttributes, TypeAttributes} ::= SEQUENCE {
        commonObjectAttributes   CommonObjectAttributes,
        classAttributes          ClassAttributes,
        subClassAttributes       [0] SubClassAttributes OPTIONAL,
        typeAttributes           [1] TypeAttributes
        }
```

8.3 CIOChoice type

```
CIOChoice ::= CHOICE {
        privateKeys              [0] PrivateKeys,
        publicKeys               [1] PublicKeys,
        trustedPublicKeys        [2] PublicKeys,
        secretKeys               [3] SecretKeys,
        certificates             [4] Certificates,
        trustedCertificates      [5] Certificates,
        usefulCertificates       [6] Certificates,
        dataContainerObjects     [7] DataContainerObjects,
        authObjects              [8] AuthObjects,
        ... -- For future extensions
        }

PrivateKeys ::=     PathOrObjects {PrivateKeyChoice}

PublicKeys  ::=     PathOrObjects {PublicKeyChoice}

SecretKeys  ::=     PathOrObjects {SecretKeyChoice}

Certificates ::=    PathOrObjects {CertificateChoice}

DataContainerObjects ::= PathOrObjects {DataContainerObjectChoice}

AuthObjects ::=     PathOrObjects {AuthenticationObjectChoice}
```

EF.OD shall contain the concatenation of 0, 1 or more DER-encoded **CIOChoice** values. Any number of 'FF' or '00' octets may occur before, between, or after the values without any meaning (i.e. as padding for unused space or delete values). A specific choice may appear more than once in the file (which may be done, for example, to apply different access control rules to separate collections of objects of the same type).

It is expected that an EF.OD entry will usually reference a separate file (the **path** choice of **PathOrObjects**) containing CIOs of the indicated type. An entry may, however, hold CIOs directly (the **objects** choice of **PathOrObjects**).

The **trustedPublicKeys** component references public key information objects describing public keys that are trusted by the cardholder for some purpose, such as being the trust point (root) for certificate path processing.

The **certificates** choice references certificate information objects describing certificates issued to the card or the cardholder.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

The **trustedCertificates** component references certificate information objects describing certificates trusted by the cardholder for their indicated purposes. For instance, CA certificates referenced by this component may be used as trust points (roots) during certificate path processing.

To maintain the desired trust in given certificates and/or public keys, their associated CIOs within **trustedCertificates** and/or **trustedPublicKeys** components need appropriate protection against modification (i.e. appropriate access control). This protection shall apply to the EF.OD file, any CIO file referenced by the **trustedCertificates** or **trustedPublicKeys** components, and any actual key or certificate file referenced from the individual CIOs.

A **usefulCertificates** component references certificate information objects describing certificates that do not belong in either a **trustedCertificates** or **certificates** component. It may be used to store either end-entity or CA certificates that may be useful, e.g. a certificate for a colleague's encryption key or intermediate CA certificates to simplify certificate path processing.

8.4 Private key information objects

8.4.1 PrivateKeyChoice

```
PrivateKeyChoice ::= CHOICE {
        privateRSAKey               PrivateKeyObject {PrivateRSAKeyAttributes},
        privateECKey                [0] PrivateKeyObject {PrivateECKeyAttributes},
        privateDHKey                [1] PrivateKeyObject {PrivateDHKeyAttributes},
        privateDSAKey               [2] PrivateKeyObject {PrivateDSAKeyAttributes},
        privateKEAKey               [3] PrivateKeyObject {PrivateKEAKeyAttributes},
        genericPrivateKey           [4] PrivateKeyObject { GenericKeyAttributes},
        othergenericPrivateKey      [5] PrivateKeyObject {OtherGenericKeyAttributes},
        ... – For future extensions
        }
PrivateKeyObject {KeyAttributes} ::= CIO {
        CommonKeyAttributes, CommonPrivateKeyAttributes, KeyAttributes}
```

This type contains information pertaining to a private key. Each value consists of attributes common to any object, any key, any private key and attributes particular to the key. When **KeyAttributes** are used as an EF reference, the **othergenericPrivateKey** CHOICE may apply.

```
OtherGenericKeyAttributes::= ReferencedValue
```

8.4.2 Private RSA key attributes

```
PrivateRSAKeyAttributes ::= SEQUENCE {
        value               Path,
        modulusLength       INTEGER, -- modulus length in bits, e.g. 1024
        keyInfo             KeyInfo {NULL, PublicKeyOperations} OPTIONAL,
        ... -- For future extensions
        }
```

The interpretation of the components shall be as follows.

— **PrivateRSAKeyAttributes.value**: The value shall be a path to a file containing a private RSA key. If there is no need to specify a path to a file, the path value may be set to the empty path.

— **PrivateRSAKeyAttributes.modulusLength**: On many cards, one needs to format data to be signed prior to sending the data to the card. In order to be able to format the data in a correct manner, the length of the key shall be known. The length shall be expressed in bits, e.g. 1 024.

— **PrivateRSAKeyAttributes.keyInfo:** Information about parameters that applies to this key and operations the card can carry out with it. The values override any **CIAInfo.supportedAlgorithms** value referenced by the **CommonKeyAttributes.algReference** component. The component is not needed if the information is available through other means.

8.4.3 Private elliptic curve key attributes

```
PrivateECKeyAttributes ::= SEQUENCE {
        value     Path,
        keyInfo   KeyInfo {Parameters, PublicKeyOperations} OPTIONAL,
          ... -- For future extensions
        }
```

Documents
Document Sharing Hub

© ISO/IEC 2016 – All rights reserved

Full document details: BS ISO/IEC 7816-15:2016+A1:2018

The interpretation of the components shall be as follows.

— **PrivateECKeyAttributes.value**: The value shall be a path to a file containing a private elliptic-curve key. If there is no need to specify a path to a file, the path value may be set to the empty path.

— **PrivateECKeyAttributes.keyInfo**: See corresponding component in 8.4.2.

NOTE 1 For **Parameters** definition, this part of ISO/IEC 7816 references the module from ANSI X9.68:1998.

NOTE 2 The OID referencing ANSI X9.62 is updated in this part of ISO/IEC 7816 (see Annex A) to solve the conflict identified on **{iso(1) member-body(2) us(840) ansi-x962(10045) module(4) 1}** that incidentally referred to both ECDSA signatures with SHA1 and to ANSI X9.62 module.

8.4.4 Private Diffie-Hellman key attributes

```
PrivateDHKeyAttributes ::= SEQUENCE {
        value      Path,
        keyInfo    KeyInfo {DomainParameters, PublicKeyOperations} OPTIONAL,
        ... -- For future extensions
        }
```

The interpretation of the components shall be as follows.

— **PrivateDHKeyAttributes.value**: The value shall be a path to a file a private Diffie-Hellman key. If there is no need to specify a path to a file, the path value may be set to the empty path.

— **PrivateDHKeyAttributes.keyInfo**: See corresponding component in 8.4.2.

8.4.5 Private DSA key attributes

```
PrivateDSAKeyAttributes ::= SEQUENCE {
        value      Path,
        keyInfo    KeyInfo {DomainParameters, PublicKeyOperations} OPTIONAL,
        ... — For future extensions
        }
```

The interpretation of the components shall be as follows.

— **PrivateDSAKeyAttributes.value**: The value shall be a path to a file containing a private DSA key. If there is no need to specify a path to a file, the path value may be set to the empty path.

— **PrivateDSAKeyAttributes.keyInfo**: See corresponding component in 8.4.2.

8.4.6 Private KEA key attributes

```
PrivateKEAKeyAttributes ::= SEQUENCE {
        value      Path,
        keyInfo    KeyInfo {DomainParameters, PublicKeyOperations} OPTIONAL,
        ... -- For future extensions
        }
```

The interpretation of the components shall be as follows.

— **PrivateKEAKeyAttributes.value**: The value shall be a path to a file containing a private KEA key. If there is no need to specify a path to a file, the path value may be set to the empty path.

— **PrivateKEAKeyAttributes.keyInfo**: See corresponding component in 8.4.2.

8.4.7 Generic private key information objects

This type is intended to contain information specific to a private key of any kind. See 8.2.13.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018

8.5 Public key information objects

8.5.1 PublicKeyChoice

```
PublicKeyChoice ::= CHOICE {
        publicRSAKey                PublicKeyObject {PublicRSAKeyAttributes},
        publicECKey                 [0] PublicKeyObject {PublicECKeyAttributes},
        publicDHKey                 [1] PublicKeyObject {PublicDHKeyAttributes},
        publicDSAKey                [2] PublicKeyObject {PublicDSAKeyAttributes},
        publicKEAKey                [3] PublicKeyObject {PublicKEAKeyAttributes},
        genericPublicKey            [4] PublicKeyObject { GenericKeyAttributes},
        othergenericPublicKey       [5]  PublicKeyObject {OtherGenericKeyAttributes},
        ... – For future extensions }

PublicKeyObject {KeyAttributes} ::= CIO {
        CommonKeyAttributes, CommonPublicKeyAttributes, KeyAttributes}
```

This type contains information pertaining to a public key. Each value consists of attributes common to any object, any key, any public key and attributes particular to the key. When **KeyAttributes** are used as an EF reference, the **othergenericPublicKey** CHOICE may apply.

8.5.2 Public RSA key attributes

```
PublicRSAKeyAttributes ::= SEQUENCE {
        value               ObjectValue {RSAPublicKeyChoice},
        modulusLength       INTEGER, -- modulus length in bits, e.g. 1024
        keyInfo             KeyInfo {NULL, PublicKeyOperations} OPTIONAL,
        ... -- For future extensions
        }

RSAPublicKeyChoice ::= CHOICE {
        raw     RSAPublicKey,
        spki    [1] SubjectPublicKeyInfo, -- See ISO/IEC 9594-8. Must contain a public RSA key.
        ... – For future extensions
        }

RSAPublicKey ::= SEQUENCE {
        modulus             INTEGER,
        publicExponent      INTEGER
        }
```

The interpretation of the components shall be as follows.

— **PublicRSAKeyAttributes.value**: The value shall be a path to a file containing either an **RSAPublicKeyChoice** value or (some card-specific representation of) a public RSA key.

— **PublicRSAKeyAttributes.modulusLength**: On many cards, one shall format data to be encrypted prior to sending the data to the card. In order to be able to format the data in a correct manner, the length of the key shall be known. The length shall be expressed in bits, e.g. 1 024.

— **PublicRSAKeyAttributes.keyInfo:** See corresponding component in 8.4.2.

8.5.3 Public elliptic curve key attributes

```
PublicECKeyAttributes ::= SEQUENCE {
        value       ObjectValue {ECPublicKeyChoice},
        keyInfo     KeyInfo {Parameters, PublicKeyOperations} OPTIONAL,
        ... -- For future extensions
        }

ECPublicKeyChoice ::= CHOICE {
        raw     ECPoint, -- See ANSI X9.62,
        spki    SubjectPublicKeyInfo, -- See ISO/IEC 9594-8. Must contain a public elliptic-curve key
        ... – For future extensions
        }
```

The interpretation of the components shall be as follows.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-15:2016+A1:2018