INTERNATIONAL STANDARD

ISO/IEC 7816-15

First edition
2004-01-15

Identification cards — Integrated circuit cards with contacts —

Part 15: Cryptographic information application

Cartes d'identification — Cartes à circuit intégré à contacts —
Partie 15: Application des informations cryptographiques

Reference number
ISO/IEC 7816-15:2004(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 7816-15 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

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

— *Part 1: Physical characteristics*

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

— *Part 3: Electronic signals and transmission protocols*

— *Part 4: Organisation, 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 for security operations*

— *Part 9: Commands for card management*

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

— *Part 11: Personal verification through biometric methods*

— *Part 15: Cryptographic information application*

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 the bibliography). 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.

Identification cards — Integrated circuit cards with contacts —

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; and

— 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 shall not be 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.

2 Normative references

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

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

ISO/IEC 8824-1:1998, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8824-2:1998, *Information technology — Abstract Syntax Notation One (ASN.1): Information object specification*

ISO/IEC 8824-3:1998, *Information technology — Abstract Syntax Notation One (ASN.1): Constraint specification*

ISO/IEC 8824-4:1998, *Information technology — Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*

ISO/IEC 8825-1:1998, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO 9564-1:2002, *Banking — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

ISO/IEC 9594-8:1998, *Information technology — Open Systems Interconnection — The Directory: Authentication framework*

ISO/IEC 10646-1:2000, *Information technology — Universal Multiple-Octet Coded Character Set (UCS) — Part 1: Architecture and Basic Multilingual Plane*

ANSI X9.42-2001, *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*

ANSI X9.62-1998, *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

[ISO/IEC 7816-4]

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

NOTE Adapted from ISO/IEC 7816-4.

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

[ISO/IEC 7816-4]

3.5
authentication information object
cryptographic information object that provides information about authentication related data, e.g. 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, e.g. a public key or a certificate

3.15
data container information object
cryptographic information object that provides information about a data container, e.g. 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 7816-4]

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

[ISO/IEC 7816-4]

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

[ISO/IEC 7816-4]

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

[ISO/IEC 7816-4]

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

[ISO/IEC 7816-4]

NOTE 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

[ISO/IEC 7816-4]

3.26
path
concatenation of file identifiers without delimitation

[ISO/IEC 7816-4]

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

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

[ISO/IEC 7816-4]

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

[ISO/IEC 7816-4]

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 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' – '9' and 'A' – 'F' Hexadecimal digits

4.2 Abbreviated terms

For the purposes of this document, the following abbreviations apply.

AID	Application identifier
AOD	Authentication object directory
BCD	Binary-coded decimal
CD	Certificate directory
CDE	Cryptographic data element
CIA	Cryptographic information application
CIO	Cryptographic information object
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 10646-1)
URL	Uniform resource locator

UTC	Coordinated universal time
UTF-8	UCS transformation format 8
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 Introduction

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:

— cryptographic key information objects;

— certificate information objects;

— data container information objects; and

— 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.

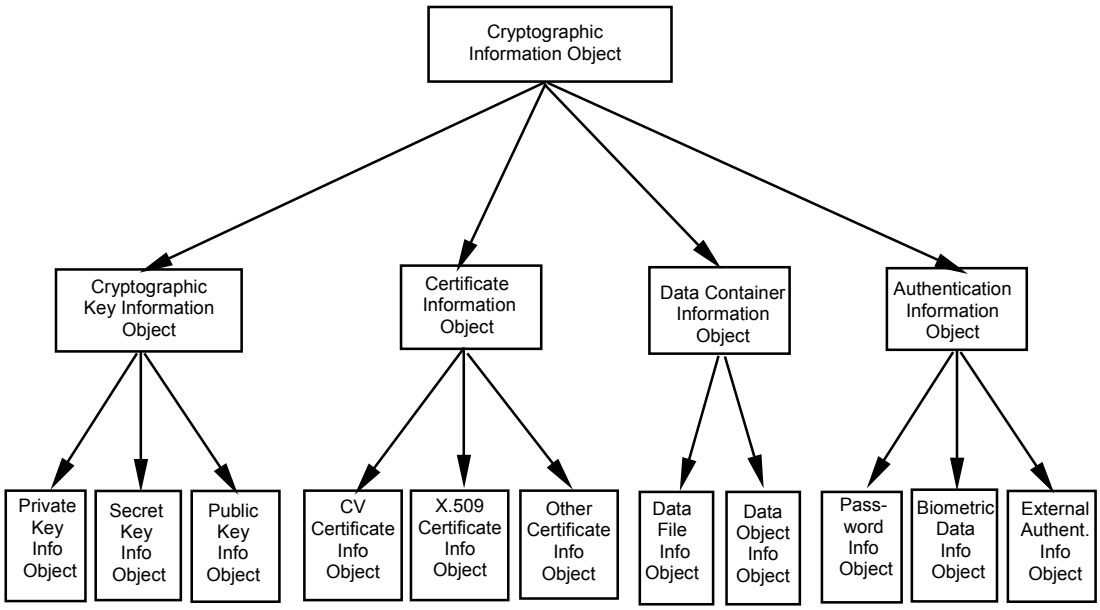


Figure 1 — CIO class hierarchy

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;

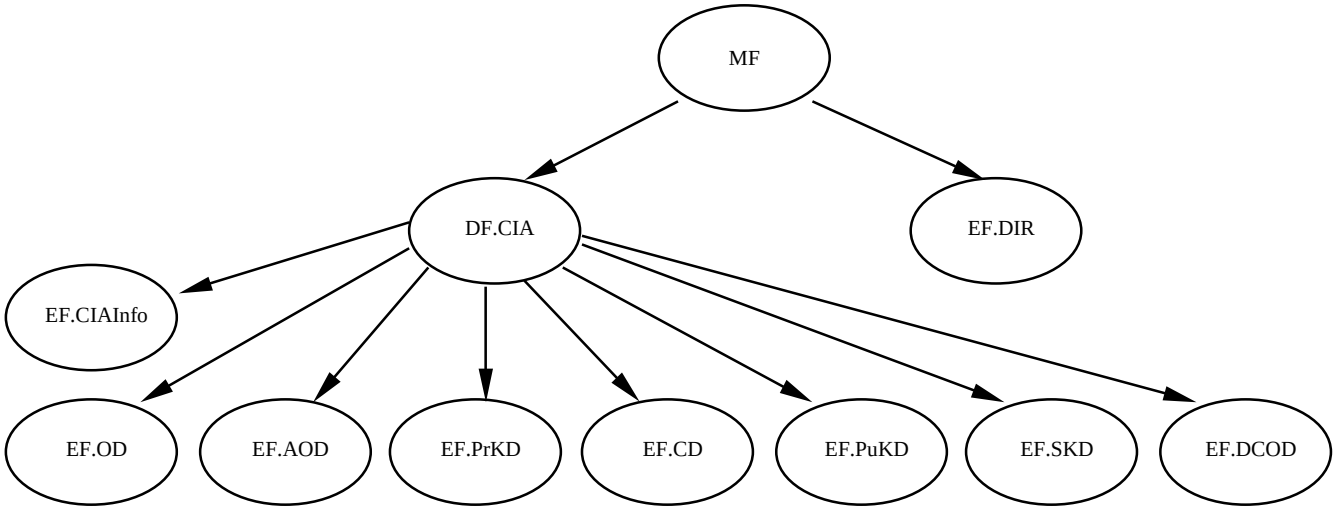
— access control mechanisms;

— read operations; and

— cryptographic operations.

7.3 Card file structure

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



NOTE 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.

Figure 3 — Example contents of DF.CIA

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

7.4 EF.DIR

This file under the MF (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

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 an 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,
    ... -- For future extensions
    } -- Context tag 1 is historical and shall not be used
```

NOTE 1 PKCS #15 uses this tag.