INTERNATIONAL STANDARD

ISO/IEC 7816-15

First edition
2004-01-15

AMENDMENT 2
2008-12-15

Identification cards — Integrated circuit cards —

Part 15: Cryptographic information application

AMENDMENT 2: Error corrections and extensions for multi-application environments

Cartes d'identification — Cartes à circuit intégré —

Partie 15: Application des informations cryptographiques

AMENDEMENT 2: Corrections d'erreurs et extensions pour environnements d'applications multiples

Reference number
ISO/IEC 7816-15:2004/Amd.2:2008(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

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.

Amendment 2 to ISO/IEC 7816-15:2004 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

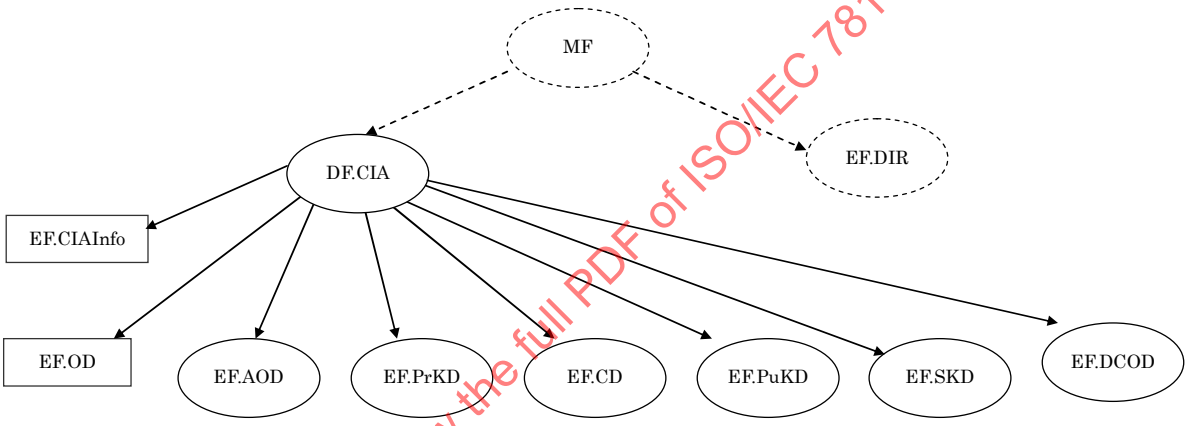
Identification cards — Integrated circuit cards —

Part 15:
Cryptographic information application

AMENDMENT 2: Error corrections and extensions for multi-application environments

Page 9, 7.3, Figure 3

Replace the existing figure with the following:



NOTE 1 For the purpose of this part of ISO/IEC 7816, EF.DIR is 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

Page 9, 7.4

Replace the first sentence with the following:

This file (file identifier: ’2F00’) shall, if present, contain one or several application templates as defined in ISO/IEC 7816-4.

Page 10, 7.4

Add following paragraph at the end of the subclause:

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.

Page 10, 7.5.2

Replace the second list item with the following:

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

Page 13, 8.2.4

Replace the existing text of **KeyIdentifiers** with the following:

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

Page 14, 8.2.4

Add the following list item at the end of the suclause:

— **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.

Page 14, 8.2.5

Replace the existing text of **Path** with the following:

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

Page 15, 8.2.5

Add the following at the end of the second paragraph, which is explaining **path.**

aid and **tag** are used for referencing from CIA of logical data structures located in application context.

Page 15, 8.2.5

Replace the last sentence of the last paragraph with the following:

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.

Page 16, 8.2.8

Replace the existing definition of **AccessMode** with the following:

```
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)
        }
```

Page 16, 8.2.8

Replace the existing text of **AuthMode** with the following:

AuthMethod ::= BIT STRING {secureMessaging(0), extAuthentication(1), userAuthentication(2), always(3)}

Page 17, 8.2.8

Add following at the end of the subclause:

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 PERFOM 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.

Page 22, 8.3

Delete the following from the end of the second paragraph:

“, if the objects and the EF.OD file have the same access control requirements”.

Page 29, 8.7.8

Replace the existing text of **CVCertificateAttributes** with the following:

```
CVCertificateAttributes ::= SEQUENCE{
    value                          ObjectValue {CIO-OPAQUE.&Type},
    certificationAuthorityReference  OCTET STRING OPTIONAL
    ... – For future extensions,
    }
```

Page 30, 8.7.8

Add the following list item at the end of the subclause:

— **CVCertificateAttributes.certificationAuthorityReference**: The value of this component shall be exactly the same as for the corresponding component in the card verifiable certificate.

Page 31, 8.9.2

Replace the existing text of **PasswordFlags** with the following:

```
PasswordFlags ::= BIT STRING {
    case-sensitive (0),
    local (1),
    change-disabled (2),
    unblock-disabled (3),
    initialized (4),
    needs-padding (5),
    unblockingPassword (6),
    soPassword (7),
    disable-allowed (8),
    integrity-protected (9),
    confidentiality-protected (10),
    exchangeRefData (11),
    resetRetryCounter1 (12),
    resetRetryCounter2 (13)
    } (CONSTRAINED BY { -- ‘unblockingPassword’ and ‘soPassword’ cannot both be set -- })
```

Page 32, 8.9.2

Add the following list item at the end of the explanation of **PasswordAttributes.pwdFlags**:

— can be reset by means of a RESET RETRY COUNTER command with P1 = '00’ (resetRetryCounter1 and resetRetryCounter2 are not set), P1 = ‘01’ (only resetRetryCounter2 is set), P1 = ‘02’ (only resetRetryCounter1 is set) or P1 = ‘03’ (both bits are set). (**resetRetryCounter1 , resetRetryCounter2**)

Page 34, 8.9.3

Replace the existing text of **BiometricInformationTemplate** and **BiometricInformationTemplateGroup** with the following:

```
BiometricInformationTemplate ::= OCTET STRING
-- Shall contain an ISO/IEC 7816-11 Biometric Information Template value

BiometricInformationTemplateGroup ::= OCTET STRING
-- Shall contain an ISO/IEC 7816-11 Biometric Information Template group template value
```

Page 39, A.2.4

Replace the existing text of **KeyIdentifiers** with the following:

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

Page 40, A.2.5

Replace the existing text of **Path** with the following:

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