INTERNATIONAL STANDARD

ISO/IEC 7816-15

Second edition
2016-05-15

AMENDMENT 1
2018-06

Identification cards — Integrated circuit cards —

Part 15: **Cryptographic information application**

AMENDMENT 1

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

Partie 15: Application des informations cryptographiques

AMENDEMENT 1

Reference number
ISO/IEC 7816-15:2016/Amd.1:2018(E)

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

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 voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 17, *Cards and personal identification*.

Identification cards — Integrated circuit cards —

Part 15:
Cryptographic information application

AMENDMENT 1

Page 27, 8.4.1

Replace the PrivateKeyChoice ASN.1 definition with:

```
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
}
```

Page 27, 8.4.1

Add at the end of the text under the two ASN.1 definitions the following:

> When **KeyAttributes** are used as an EF reference, the **othergenericPrivateKey** CHOICE may apply.

Page 27, 8.4.1

Add right after the first paragraph under the two ASN.1 definitions, the following one:

```
  OtherGenericKeyAttributes::= ReferencedValue
```

Page 29, 8.5.1

Replace the PublicKeyChoice ASN.1 definition with:

```
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
}
```

Page 29, 8.5.1

Add at the end of the text under the two ASN.1 definitions the following:

> When **KeyAttributes** are used as an EF reference, the **othergenericPublicKey** CHOICE may apply.

Page 49, A.4.1

Replace the PrivateKeyChoice ASN.1 definition with:

```
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
}
```

Page 50, A.4.1

Add right after the second ASN.1 definition, the following one:

```
  OtherGenericKeyAttributes::= ReferencedValue
```