

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)



This is a preview of "ISO/IEC 7816-15:2004". [Click here to purchase the full version from the ANSI store.](#)

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2004

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "ISO/IEC 7816-15:2004". Click here to purchase the full version from the ANSI store.

## Contents

Page

Foreword .....	iv
Introduction .....	v
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 .....	6
5 Conventions .....	7
6 Cryptographic information objects .....	7
6.1 Introduction .....	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 .....	10
8 Information syntax in ASN.1 .....	13
8.1 Guidelines and encoding conventions .....	13
8.2 Basic ASN.1 defined types .....	13
8.3 The CIOChoice type .....	22
8.4 Private key information objects .....	23
8.6 Secret key information objects .....	27
8.7 Certificate information objects .....	27
8.8 Data container information objects .....	30
8.9 Authentication information objects .....	31
8.10 The cryptographic information file, EF.CIAInfo .....	35
Annex A (normative) ASN.1 module .....	38
Annex B (informative) CIA example for cards with digital signature and authentication functionality .....	52
Annex C (informative) Example topologies .....	55
Annex D (informative) Examples of CIO values and their encodings .....	57
Bibliography .....	70

## 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*

This is a preview of "ISO/IEC 7816-15:2004". [Click here to purchase the full version from the ANSI store.](#)

## 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.