
**Information technology — Identification cards
— Integrated circuit(s) cards with contacts —**

Part 4:
Interindustry commands for interchange

*Technologies de l'information — Cartes d'identification — Cartes à circuit(s)
intégré(s) à contacts —*

Partie 4: Commandes intersectorielles pour les échanges

Reference number
ISO/IEC 7816-4 : 1995 (E)

Contents

Page

Foreword	iii
Introduction	iv
1 Scope	1
2 Normative references	1
3 Definitions	2
4 Abbreviations and notation	3
5 Basic organizations	3
5.1 Data structures	3
5.2 Security architecture of the card	6
5.3 APDU message structure	7
5.4 Coding conventions for command headers, data fields and response trailers	9
5.5 Logical channels	12
5.6 Secure messaging	12
6 Basic interindustry commands	16
6.1 READ BINARY command	16
6.2 WRITE BINARY command	17
6.3 UPDATE BINARY command	17
6.4 ERASE BINARY command	18
6.5 READ RECORD(S) command	19
6.6 WRITE RECORD command	20
6.7 APPEND RECORD command	21
6.8 UPDATE RECORD command	22
6.9 GET DATA command	23
6.10 PUT DATA command	24
6.11 SELECT FILE command	25
6.12 VERIFY command	26
6.13 INTERNAL AUTHENTICATE command	27
6.14 EXTERNAL AUTHENTICATE command	27
6.15 GET CHALLENGE command	28
6.16 MANAGE CHANNEL command	29
7 Transmission-oriented interindustry commands	29
7.1 GET RESPONSE command	30
7.2 ENVELOPE command	30
8 Historical bytes	31
9 Application-independent card services	33
Annexes	
A Transportation of APDU messages by T=0	35
B Transportation of APDU messages by T=1	39
C Record pointer management	41
D Use of the basic encoding rules of ASN.1	42
E Examples of card profiles	43
F Use of secure messaging	45

© ISO/IEC 1995

All rights reserved. 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 the publisher. ISO/IEC Copyright Office, P.O. Box 56, CH-1211 Geneva 20, Switzerland. Printed in France

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) together form a system for worldwide standardization as a whole. 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 JTC1. Draft International Standards adopted by the joint technical committee are circulated to the national bodies for voting. Publication as an International Standard requires at least 75 % approval by the national bodies casting a vote.

International Standard ISO/IEC 7816-4 was prepared by Joint Technical Committee ISO/IEC JTC1, *Information Technology*.

Annexes A and B form an integral part of this part of ISO/IEC 7816.

Annexes C, D, E and F are for information only.

ISO/IEC 7816 is a multi-part standard, under the general title of, *Information technology — Identification cards — Integrated circuit(s) cards with contacts*.

- Part 1: *Physical characteristics*,
- Part 2: *Dimensions and location of the contacts*,
- Part 3: *Electronic signals and transmission protocols*,
- Part 4: *Interindustry commands for interchange*,
- Part 5: *Numbering system and registration procedure for application identifiers*,
- Part 6: *Interindustry data elements*.

Introduction

This part of ISO/IEC 7816 is one of a series of standards describing the parameters for integrated circuit(s) cards with contacts and the use of such cards for international interchange.

These cards are identification cards intended for information exchange negotiated between the outside and the integrated circuit in the card. As a result of an information exchange, the card delivers information (computation results, stored data), and/or modifies its content (data storage, event memorization).

Information technology — Identification cards — Integrated circuit(s) cards with contacts —

Part 4: Interindustry commands for interchange

1 Scope

This part of ISO/IEC 7816 specifies

- the content of the messages, commands and responses, transmitted by the interface device to the card and conversely,
- the structure and content of the historical bytes sent by the card during the answer to reset,
- the structure of files and data, as seen at the interface when processing interindustry commands for interchange,
- access methods to files and data in the card,
- a security architecture defining access rights to files and data in the card,
- methods for secure messaging,
- access methods to the algorithms processed by the card. It does not describe these algorithms.

It does not cover the internal implementation within the card and/or the outside world.

It allows further standardization of additional interindustry commands and security architectures.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 7816. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 7816 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 3166: 1993, *Codes for the representation of names of countries*.

ISO/IEC 7812-1: 1993, *Identification cards — Issuer identification — Part 1: Numbering system*.

ISO/IEC 7816-3: 1989, *Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols*.

Amendment 1:1992 to ISO/IEC 7816-3: 1989, *Protocol type T=1, asynchronous half duplex block transmission protocol*.

Amendment 2: 1994 to ISO/IEC 7816-3: 1989, *Revision of protocol type selection*.

ISO/IEC 7816-5: 1994, *Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers*.

ISO/IEC 7816-6: 199X, *Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements*.

ISO/IEC 8825: 1990, *Information technology — Open systems interconnection — Specification of basic encoding rules for abstract syntax notation one (ASN.1)*.

ISO/IEC 9796: 1991, *Information technology — Security techniques — Digital signature scheme giving message recovery*.

ISO/IEC 9797: 1993, *Information technology — Security techniques — Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm*.

ISO/IEC 9979: 1991, *Cryptographic techniques — Procedures for the registration of cryptographic algorithms*.

ISO/IEC 10116: 1991, *Information technology — Information technology — Security techniques — Modes of operation of an n-bit block cipher algorithm*.

ISO/IEC 10118-1: 1994, *Information technology — Security techniques — Hash functions — Part 1: General*.

ISO/IEC 10118-2: 1994, *Information technology — Security techniques — Hash functions — Part 2: Hash functions using an n-bit block cipher algorithm*.

3 Definitions

For the purpose of this part of ISO/IEC 7816, the following definitions apply.

3.1 Answer-to-Reset file: Elementary file which indicates operating characteristics of the card.

3.2 command-response pair: Set of two messages: a command followed by a response.

3.3 data unit: The smallest set of bits which can be unambiguously referenced.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.