INTERNATIONAL STANDARD

ISO 10202-4

First edition
1996-02-01

Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards —

Part 4:
Secure application modules

Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré —

Partie 4: Modules applicatifs de sécurité

Reference number
ISO 10202-4:1996(E)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 10202-4 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Subcommittee SC 6, *Financial transaction cards, related media and operations.*

ISO 10202 consists of the following parts, under the general title *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards*:

— *Part 1: Card life cycle*

— *Part 2: Transaction process*

— *Part 3: Cryptographic key relationships*

— *Part 4: Secure application modules*

— *Part 5: Use of algorithms*

— *Part 6: Cardholder verification*

— *Part 7: Key management*

— *Part 8: General principles and overview*

Annex A forms an integral part of this part of ISO 10202. Annex B is for information only.

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards —

Part 4:
Secure application modules

1 Scope

This part of ISO 10202 specifies the minimum security requirements of the life cycle for a Secure Application Module (SAM) which can be added to a Card Accepting Device (CAD). A SAM provides application-related and cryptographic security information for the processing of a financial transaction. Each application supplier may have a SAM. Card issuers and/or application supplier(s) may agree to combine the use of one SAM for their applications. This part of ISO 10202 is applicable to any organization involved in issuing SAMs for use in CADs. A SAM may service one CAD or a cluster of attached CADs.

This part of ISO 10202 allows interaction between an Integrated Circuit Card (ICC) and a SAM in a way which may be functionally transparent to the Card Accepting Device (CAD). This permits the use of different techniques and levels of command structure and message formats.

A description of security audit and security related data fields recorded in a SAM is given in annex A. Suggested implementations of SAM functions are provided in annex B.

A SAM may be used to establish a secure transaction relationship between the ICC, application supplier, acquirer and CAD. This could include SAM authentication by the SAM provider. A CAD may contain one or more SAMs.

The relationship between the host of the SAM provider and the SAM is outside the scope of this part of ISO 10202.

NOTE 1 Whenever the SAM provider, card issuer, application supplier or acquirer is referred to in this part of ISO 10202, these terms also encompass their agents.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 10202. 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 10202 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/IEC 7812-1:1993, *Identification cards — Identification of issuers — Part 1: Numbering system.*

ISO/IEC 7812-2:1993, *Identification cards — Identification of issuers — Part 2: Application and registration procedures.*

ISO 7816-1:1987, *Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics.*

ISO 7816-2:1988, *Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts.*

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

ISO/IEC 7816-4:1995, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange.*

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

ISO 10202-1:1991, *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 1: Card life cycle.*

ISO 10202-2:—[1], *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 2: Transaction process.*

ISO 10202-3:—[1], *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 3: Cryptographic key relationships.*

ISO 10202-5:—[1], *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 5: Use of algorithms.*

ISO 10202-7:—[1], *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 7: Key management.*

3 Definitions

For the purpose of this part of ISO 10202, the definitions given in ISO 10202-1, together with the following apply.

3.1 Secure Application Module (SAM): A physical module (or a logical functionality in the CAD) intended to contain algorithm(s), related keys, security procedures and information to protect an application in such a way that unauthorized access is not possible. In order to achieve this, the module must be physically and logically protected.

3.2 SAM initializer: The entity which loads security and related operational parameters in the SAM.

3.3 SAM provider: The entity that provides a SAM to a card acceptor (usually the application supplier).

4 General security principles

The security provided in this part of ISO 10202 is governed by the following principles.

a) Any aspect in the operation of a SAM or data obtainable from that SAM shall not compromise the security of any other system or combination of systems using SAMs.

b) The SAM provider shall be responsible for the SAM life cycle.

c) Cryptographic keys used in SAMs shall be managed in such a way that the security of any system using ICCs is not compromised.

d) The CAD application software shall not be able to compromise the security functions of the SAM.

5 SAM life cycle

This clause specifies the minimum security requirements in respect of the following stages of the SAM life cycle:

Manufacture of the SAM

SAM preparation

SAM initialization

SAM activation

SAM usage

SAM use

SAM deactivation

SAM reactivation

Termination of use

SAM termination

5.1 Manufacture of the SAM

The manufacturing process includes hardware and software design, assembly and the packaging to form a SAM.

1) To be published.