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.

1) To be published.

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.

Prior to the stage of the process when proprietary data is loaded into the SAM, the security of the manufacturing procedures shall be in accordance with the level of security required by the SAM provider.

From the stage when proprietary data (e.g. a cryptographic algorithm, a key or secret data) are stored in the SAM, the following security procedures shall apply:

a) all processes shall be conducted in a secure environment where access is controlled and confidentiality of proprietary data is maintained;

b) access to controlled areas of the SAM shall only be through the use of a cryptographic key (i.e. Production Key) in accordance with ISO 10202-3;

c) during storage and transport of SAMs, they shall be physically and/or cryptographically protected.

In order to protect secret data the SAM shall be designed and manufactured in such a manner that it will not be possible without the use of tools that are not generally available to compromise the SAM, e.g. by physical or logical attacks.

Audit trail data shall be recorded in the SAM as follows (see annex A).

SAM provider identifier

Manufacturer identifier

SAM-type identifier

As part of the manufacturing process the integrity of the functionality of the SAM should be verified (for example, by examining a statistical sample) to confirm that it corresponds to the agreed reference specifications.

5.2 SAM preparation

SAM preparation consists of the following two steps:

— SAM initialization

— SAM activation

5.2.1 SAM initialization

The application supplier or the SAM provider shall be responsible for providing the secure data for use by, and security for, the initialization process.

The SAM shall contain the required cryptographic keys, described in ISO 10202-3.

The initialization process shall be conducted in accordance with ISO 10202-3, in particular with regard to the loading of cryptographic keys and other secure data.

A SAM initializer identifier should be recorded in the SAM for audit purposes. This identifier shall have the specification detailed in annex A.

5.2.2 SAM activation

The SAM activation process renders the SAM usable for financial transactions in a CAD. It shall be carried out under the control of the acquirer on behalf of the SAM provider or his agent.

The activation process shall be conducted in accordance with ISO 10202-3. Following this process the SAM shall contain the data necessary to identify the CAD or card acceptor.

The SAM activator identifier and date of activation should be recorded in the SAM for security audit purposes (see annex A for detailed specifications).

The completion of the activation process shall be denoted by the SAM entering the activated status.

5.3 SAM usage

5.3.1 SAM use

A SAM shall not be issued unless it has been initialized and it shall not be usable for a financial transaction unless it has been activated.

The SAM shall support the transaction functions contained in ISO 10202-2 which require the use of a SAM according to the card issuer or application supplier security requirements. The transaction functions which are used between the ICC and SAM shall be conducted in accordance with the requirements of ISO 10202-2.

If a transaction is performed which requires functions supported by the SAM, then the SAM shall be accessible by the CAD throughout the transaction process.

5.3.2 SAM deactivation

Only the SAM provider or his agent shall be able to deactivate a SAM. In this state the SAM shall not act upon any financial transaction. However, reactivation may still be performed.

SAM deactivation shall be denoted by setting the SAM activation status to a deactivated state (see annex A).

If protection against unauthorized deactivation of the SAM is required then the process to deactivate the SAM shall involve a cryptographic exchange using the appropriate cryptographic key specified in ISO 10202-3.

5.3.3 SAM reactivation

The process of reactivating a SAM so that it may again be used for financial transactions shall be conducted under the control of the acquirer on behalf of the SAM provider or his agent.

SAM reactivation shall be achieved by setting the SAM activation status to an activated state (see annex A).

If protection against unauthorized reactivation of the SAM is required then the process to reactivate the SAM shall involve a cryptographic exchange using the cryptographic key *k*Actl specified in ISO 10202-3.

5.4 Termination of use

The process of permanently disabling a SAM from use is at the discretion of the acquirer on behalf of the SAM provider or his agent and shall render the SAM unusable.

The SAM activation status shall be set to the final deactivation state (see annex A).

If protection against unauthorized termination of use of the SAM is required then the process to deactivate the SAM shall involve a cryptographic exchange using the cryptographic key *k*Actl specified in ISO 10202-3.

6 SAM interfaces to the CAD

6.1 Physical characteristics

The physical characteristic requirements for the SAM shall be in accordance with the requirements of ISO 7816-1 and ISO 7816-2.

6.2 Electrical characteristics and protocol types

The electrical characteristics and protocol types shall be in accordance with ISO/IEC 7816-3.

6.3 Commands

The commands used by the SAM shall be in accordance with ISO/IEC 7816-4.

6.4 Identifiers

The identifiers used by the SAM shall be in accordance with ISO/IEC 7816-5.

7 SAM security functions

The minimum set of security functions which a SAM shall be able to execute comprises ICC or ADF authentication. Additional security functions may be available such as SAM authentication by the ICC and, if necessary, by the Host of the SAM provider, load/change SAM keys, transaction certification by the SAM and load/change SAM data (for examples of an implementation see annex B). In all cases the SAM performs specific secure tasks under the coordination of the application software in the CAD.

All functions shall be independent of the transmission protocol type. Different protocol types in accordance with ISO/IEC 7816-3 may be used for the SAM and the ICC.

During the SAM session initialization the CAD shall receive all the information about the SAM's capabilities concerning validity, payment system, algorithm(s) and key(s). As part of a cryptographic process within an ICC session the CAD shall provide the expected information about the ICC to the SAM for key and algorithm selection.

The selected algorithms and keys remain selected until the next algorithm or key is selected or until the transaction or the ICC session is terminated.

For Messages (Commands and Responses) to select, transmit and perform functions, see ISO/IEC 7816-4 and ISO 9992-2.

7.1 CDF or ADF dynamic authentication

The purpose of this function is to enable a SAM to verify the authenticity of a CDF or ADF and by so doing to ensure that the CDF or ADF has been supplied by the entitled authority.

CDF or ADF dynamic authentication should comprise the movement of a pseudo-random number or a time variant (e.g. a counter) from the SAM to the CDF or ADF. The identities of the algorithm and cryptographic key to be used in the authentication process may be implicitly defined or explicitly defined using a key identifier (see ISO 10202-7). The pseudo-random

number shall then be processed by an algorithm in the ICC using the cryptographic key *k*Iaut or *k*Aaut specified in ISO 10202-3. The outcome of this process, the authentication parameter, shall be returned to the SAM for checking.

NOTE 2 The procedure described corresponds to Process 2: Entity Authentication, described in ISO 10202-5.

7.2 SAM dynamic authentication

The purpose of this function is to enable an ICC to verify the authenticity of the SAM and so doing to ensure that the SAM has been supplied by the entitled authority (e.g. the application supplier).

SAM dynamic authentication should comprise the movement of a pseudo-random number or a time variant (e.g. a counter) from an ICC to the SAM. The identities of the algorithm and the cryptographic key to be used in the authentication process may be implicitly defined or explicitly defined using a key identifier (see ISO 10202-7). The pseudo-random number shall then be processed by an algorithm in the SAM using the cryptographic key *k*Iaut or *k*Aaut specified in ISO 10202-3. The outcome of this process, the authentication parameter, shall be returned to the ICC for checking.

NOTE 3 The procedure described corresponds to Process 2: Entity Authentication described in ISO 10202-5.

7.3 Load/replace SAM keys

The purpose of this function is to load or replace cryptographic keys in a SAM subsequent to initialization.

Cryptographic keys used by a SAM should be loaded or changed under the control of the cryptographic key *k*Actl specified in ISO 10202-3.

NOTES

4 The procedure described corresponds to Process 1: Key Exchange described in ISO 10202-5.

5 It is assumed that an initial key has been loaded during the initialization process.

7.4 Transaction certification by the SAM

The purpose of this function is to prove to the application supplier (and acquirer) that the SAM has been involved in a transaction and the functions it was to perform (e.g. ICC authentication) have been accomplished.

The creation of a SAM transaction certificate should comprise the movement of transaction related data to the SAM. This data is then processed by an algorithm in the SAM. The outcome, the SAM transaction certificate, is then transmitted to the CAD. This certificate shall be generated using the cryptographic key *k*Acer specified in ISO 10202-3.

NOTE 6 The procedure described corresponds to Process 5: Transaction Certification, described in ISO 10202-5.

7.5 Load/replace SAM data

The purpose of this function is to maintain the integrity or confidentiality of data loaded into a SAM or the updating of previously loaded data.

The integrity of data either loaded or updated, if required, shall be achieved by means of message authentication using the cryptographic key *k*Aaut specified in ISO 10202-3. Confidentiality of this data, if required, shall be achieved by means of encipherment using the cryptographic key *k*Aenc specified in ISO 10202-3.

NOTE 7 If no confidentiality is required the procedure corresponds to Process 3: Message Authentication, and if condifentiality is required it corresponds to Process 4: Message Encipherment described in ISO 10202-5.

Annex A
(normative)

Description of security audit and security-related data fields

SAM manufacturer identifier

Status:	Mandatory
Location:	Area which is generally readable
Access conditions:	Not changeable
Format:	2 bytes
Content:	Manufacturer identifier in accordance with a register maintained by ISO
Purpose:	To identify in a unique way the manufacturer of the SAM

SAM provider identifier

Status:	Mandatory
Location:	Area which is generally readable
Access conditions:	Not changeable
Format:	4 bytes
Content:	The SAM provider identifier in accordance with a register maintained by ISO
Purpose:	To identify in a unique way the provider of the SAM

SAM type-identifier

Status:	Optional
Location:	Area which is generally readable
Access conditions:	Not changeable
Format:	2 bytes
Content:	The identifier defines the hardware type and the characteristics
Purpose	To identify the type of SAM

SAM software release

Status:	Optional
Location:	Area which is generally readable
Access conditions:	Not changeable

NOTE 8 This does not restrict the possibility for the SAM provider to change the identifier under his own security procedures, e.g. with a resetting of the appropriate cryptographic keys.

Format:	1 byte
Content:	Defines the present version of software
Purpose:	To identify the release of software being used in the SAM

SAM initializer identifier

Status:	Mandatory
Location:	Area which is generally readable
Access conditions:	Not changeable
Format:	1 byte
Content:	Initializer identifier as defined by the SAM provider
Purpose:	To identify the initializer of the SAM

SAM activator identifier

Status:	Optional
Location:	Area which is generally readable
Access conditions:	Not changeable

NOTE 9 This does not restrict the possibility for the SAM provider to change the identifier under his own security procedures, e.g. with a resetting of the appropriate cryptographic keys.

Format:	10 numeric digits in the form IIIIIINNNN
Content:	IIIIII — Issuer identification number as defined in ISO/IEC 7812-1 and ISO/IEC 7812-2 NNNN — Additional identification as defined by the SAM provider
Purpose:	To uniquely identify the activator of the SAM

SAM activation status

Status:	Optional
Location:	Area which is generally readable
Access conditions:	Changeable under the cryptographic control of the SAM provider
Format:	1 byte
Content:	Indication as to whether the SAM is in an activated or deactivated status
Purpose:	To indicate the status of the SAM

SAM activator serial number

Status:	Optional
Location:	Area which is generally readable
Access conditions:	Not changeable
Format:	6 numeric digits
Content:	Defined by SAM activator
Purpose:	To identify in a unique way, for a given SAM activator, the activated SAM

Date of activation of the SAM

Status:	Optional
Location:	Area which is generally readable
Access conditions:	Not changeable

NOTE 10 These may be changed by the SAM provider, if, for example, a new release of software is loaded into the SAM.

Format:	6 numeric digits
Content:	YYMMDD
Purpose:	To define the date of activation

Annex B
(informative)

Examples of implementation of security functions

The annex provides an example of an implementation for each of the security functions mentioned in clause 7.

The generic names of the steps described in the functions are not to be considered as the names of the commands.

The abbreviations used in this annex are as follows:

U = Secure Application Module

A = Application Supplier

B.1 CDF or ADF authentication

B.1.1 Logical Process Flow

NOTE 11 The procedure described corresponds to Process 2: Entity Authentication, described in ISO 10202-5.

SAM task	CAD task	Associated ICC task
S.1 Generate random number R	Initialize task ←	
S.2	Transmit random number R →	
S.3 Compute AP'_{ICC}		S.1 Compute AP_{ICC}
	Transmit AP_{ICC}	S.2
	←	→
S.4 Compare AP'_{ICC} with AP_{ICC}		
S.5 Send status →	Check status Finish task	

B.1.2 SAM task

During this process the following steps are performed by the SAM:

S.1 Generate random number:

Generate a random number R

S.2 Transmit:

Transmit R to the ICC via the CAD

S.3 Compute Authentication Parameter (AP):

NOTE 12 It is assumed that KA'aut$_{A\text{-}U}$ is in the SAM.

Compute AP'$_{ICC}$ using the selected algorithm, the authentication key (kI'aut$_{I\text{-}C}$ or kA'aut$_{A\text{-}U}$) and the previously generated random number R, and retain AP'$_{ICC}$ for the next steps

S.4 Compare:

Compare AP$_{ICC}$ with AP'$_{ICC}$ which was computed in Step 3

S.5 Send Status:

Send the status of the comparison to the CAD. The status shall be retained in the SAM to be used in further functions in this session with this ICC

B.1.3 Associated ICC task

The ICC performs the following steps in conjunction with the SAM task listed previously:

S.1 Compute AP:

Compute the Authentication Parameter AP$_{ICC}$ using the selected algorithm, the authentication key (kI'aut$_{I\text{-}C}$ or kA'aut$_{A\text{-}U}$) and the random number R supplied by the SAM

S.2 Transmit:

Transmit AP$_{ICC}$ to the SAM via the CAD

B.2 SAM dynamic authentication

B.2.1 Logical Process Flow

NOTE 13 The procedure described corresponds to Process 2: Entity Authentication, described in ISO 10202-5.