

INTERNATIONAL STANDARD

**ISO
10202-2**

First edition
1996-02-01

ANSI Internat Doc Sec

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

Part 2:

Transaction process

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

Partie 2: Processus de transaction



Reference number
Documents
ISO 10202-2:1996(E)
AVA Document Sharing Hub

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 10202-2 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

Annexes A, B, C and D of this part of ISO 10202 are for information only.

© ISO 1996

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 the publisher

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 2: Transaction process

1 Scope

This part of ISO 10202 specifies the minimum level of security required for interchange and provides security options from which the card issuer or application supplier can select different levels of security in accordance with application and risk control policy.

NOTE 1 Whenever the card issuer or application supplier is referred to in this part of ISO 10202, these terms encompass agents appointed by either

The relationships to which this part of ISO 10202 applies are indicated in figure 1 and explained in ISO 10202-3.

Messages which are not authenticated or coded by the ICC are not within the scope of this part of ISO 10202.

The relationships displayed by dotted lines fall outside the scope of this part of ISO 10202.

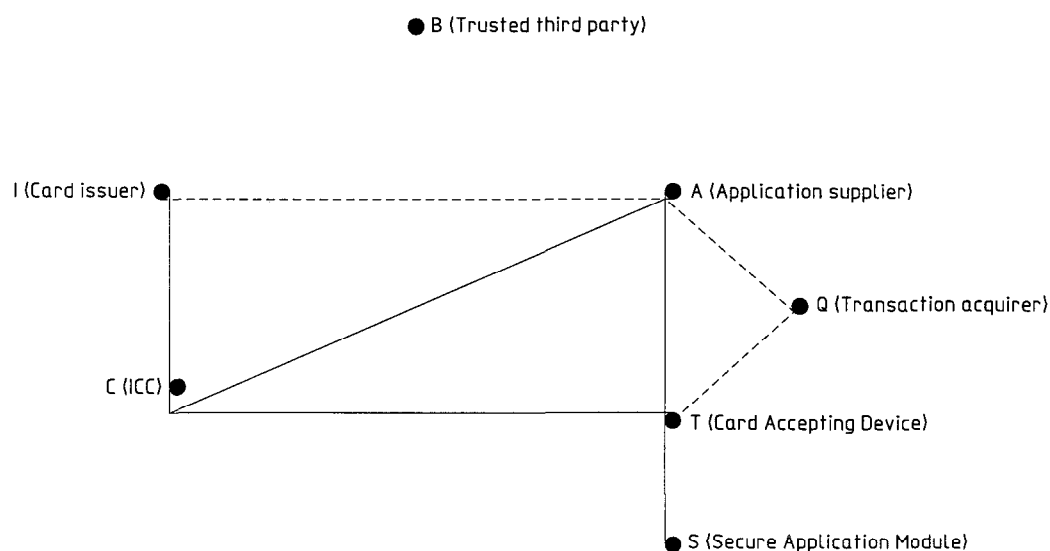


Figure 1 — Transaction process relationships

This part of ISO 10202 is specifically designed for use by systems deploying ICCs for general financial applications, for example point of service, telepayment and remote banking. The system may involve on-line or off-line applications using a financial transaction card. An application in an ICC may not require the use of a Secure Application Module (SAM).

Annex A provides an example of transaction functions, annex B provides examples of when an on-line link should be established for a financial transaction, and annex C provides the relationships for each transaction process function.

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/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 10202-3:—¹⁾, *Financial transaction cards — Security architecture of financial transaction systems*

using integrated circuit cards — Part 3: Cryptographic key relationships.

ISO 10202-4:—¹⁾, *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 4: Secure application modules*.

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

ISO 10202-6:1994, *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 6: Cardholder verification*.

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 purposes of this part of ISO 10202, the definitions given in ISO 10202-1 and the following definitions apply.

3.1 card acceptor: Party accepting the card for the provision of goods or services.

3.2 transaction certification: Process of providing cryptographic proof of the origin and integrity of transaction data which can be verified by a third party

3.3 cryptographic exchange: A method of providing protection of information passing between two parties.

3.4 Message Authentication Code (MAC): A data field, the contents of which can be used to verify the integrity of a message, or selected message elements.

3.5 Personal Identification Number (PIN): The code or password the cardholder uses for verification of his identity.

3.6 Secure Application Module (SAM): A module 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 is physically and logically protected.

1) To be published

4 General security principles

The security procedures provided in this part of ISO 10202 are governed by the following basic principles.

- a) Each participant in the system shall be responsible for providing the minimum level of security as defined by the card issuer or application supplier for its part of the financial transaction process (See annex C for details of where the initiative lies.)
- b) The card issuer shall employ a security architecture for an ICC system in such a manner that it does not compromise the security of any other ICC system or the combination of such systems.
- c) The application supplier shall employ a security architecture for an Application Data File (ADF) in such a manner that it does not compromise the security of any other application supplier's ADF
- d) If the card issuer or an application supplier chooses to use a Personal Identification Number (PIN) as a means of cardholder verification then the PIN check shall be conducted by the integrated circuit (IC) in the card.

5 Transaction process security functions

In the following list of security functions, the ICC compatibility check is mandatory. The presence and sequence of additional security functions in a financial transaction process is at the discretion of the card issuer or application supplier. An example of the security functions described in this section is given in annex A

NOTE 2 A Secure Application Module (SAM), which contains application and cryptographic security information, may be used in the processing of a financial transaction

Card session initialization (see 5.1):

- ICC compatibility check (no cryptographic exchange involved)

and, if required

CDF accessing (see 5.2)

CDF-specific authentication and verification (see 5.3):

- CDF static authentication
- CDF dynamic authentication

- CAD, SAM or Host authentication

- Cardholder verification

- CDF parameters update

ADF accessing (see 5.4)

ADF-specific authentication and verification (see 5.5):

- ADF static authentication

- ADF dynamic authentication

- CAD, SAM or Host authentication

- Cardholder verification

- ADF parameters update

Transaction handling (see 5.6):

- Transaction authorization

- Determination of cardholder acceptance

- Transaction certification

- Transaction recording

Card session termination (see 5.7)

At the discretion of the card issuer or application supplier, messages may be protected against undetectable alteration by using message authentication and for confidentiality by encipherment, as described in ISO 10202-5. In this case the appropriate cryptographic keys shall be used as described in ISO 10202-3.

The card issuer may use the CDF for providing an application if no ADF is required.

5.1 Card session initialization

ICC compatibility check

The purpose of the compatibility check is to verify the basic physical and logical compatibility of the ICC with the CAD in accordance with ISO/IEC 7816-3, ISO/IEC 7816-4 and ISO/IEC 7816-5. The check shall be performed by a CAD whenever an ICC is presented.

The minimum acceptable form shall be in compliance with the card session initialization description in a future International Standard, ISO 9992-2, which will address the functions, messages (commands and responses), data elements and structures in the area of financial transactions for messages between the in-

tegrated circuit card and the card accepting device. The Primary Account Number (PAN) and the expiry date from the Common Data File (CDF) shall also be checked

5.2 CDF accessing

The purpose of this process is to perform the transaction in an application by accessing the required CDF data. This data shall not be accessed until the CDF access control conditions (held by the ICC, CAD, SAM or Host) have been met.

5.3 CDF-specific authentication and verification

5.3.1 CDF static authentication

This form of authentication offers a level of protection which does not encompass protection against replay of this authentication process. This process may be achieved by verifying data stored in the ICC. This can be achieved by the card issuer storing the same data (which includes at least the PAN) in the ICC in plain text and in a cryptographically processed form. (The preferred approach is to process the data using an asymmetric algorithm which may be completed by a redundancy check.) Both are then transferred to the CAD, SAM or Host during the verification process. The data is verified by the decipherment (using the public key) of the enciphered data which is then compared with the plain-text version.

5.3.2 CDF dynamic authentication

A high level of ICC authentication may be achieved by the use of a cryptographic exchange, which is initiated by the CAD or Host. If this function is used then the cryptographic key k_{Iaut} specified in ISO 10202-3 shall be used.

Dynamic authentication should comprise the movement from the CAD, SAM or Host of a pseudo-random number or a time variant (for example a counter). 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 the algorithm in the ICC using the cryptographic key k_{Iaut} . The outcome of this process, the authentication parameter, shall be returned to the CAD, SAM or Host for checking.

5.3.3 CAD, SAM or Host authentication

The purpose of CAD, SAM or Host authentication is for the ICC to establish that it is in communication with an authorized end-point. This may be a CAD or SAM (for example for off-line transactions) or an authorization centre, card issuer or application supplier Host. This process shall be performed whenever the card issuer or application supplier requires measures to detect the use of an unauthorized CAD, SAM or Host. If this function is used then a cryptographic exchange using the cryptographic key k_{Iaut} , specified in ISO 10202-3 shall be used.

CAD, SAM or Host authentication should comprise the movement from the ICC of a pseudo-random number or a time variant (for example a counter). 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 the algorithm in the CAD, SAM or Host using the cryptographic key k_{Iaut} . The outcome of this process, the authentication parameter, shall be returned to the ICC for checking.

5.3.4 Cardholder verification

The purpose of this process is to determine that the card presenter is the cardholder.

If a Personal Identification Number (PIN) is used, it shall be verified within the IC and protected in accordance with the requirements specified in ISO 10202-6.

5.3.5 CDF parameters update

The card issuer parameters stored in the CDF may be updated. In that case, they shall be updated using the cryptographic k_{IctI} specified in ISO 10202-3. This action shall be under the control of the card issuer.

5.4 ADF accessing

The purpose of this process is to perform the transaction in an application by accessing the required ADF data. This data shall not be accessed until the ADF access control conditions (held by the ICC, CAD, SAM or Host) have been met.

5.5 ADF-specific authentication and verification

5.5.1 ADF static authentication

This form of authentication offers a level of protection which does not encompass protection against replay of this authentication process. This process may be achieved by verifying data stored in the ADF. This can be achieved by the application supplier storing the same data (which may include the PAN) in the ADF in plain text and in a cryptographically processed form. (The preferred approach is to process the data using an asymmetric algorithm which may be completed by a redundancy check.) Both are then transferred to the CAD, SAM or Host during the verification process. The data is verified by the decipherment (using the public key) of the enciphered data which is then compared with the plain-text version.

5.5.2 ADF dynamic authentication

The application supplier may implement independent ADF authentication to gain assurance that an ADF is authentic. This process is initiated by the CAD or Host. If this function is required then the cryptographic key k_{Aaut} specified in ISO 10202-3 shall be used.

Dynamic authentication should comprise the movement from the CAD, SAM or Host of a pseudo-random number or a time variant (for example a counter). 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 the algorithm in the ADF using the cryptographic key k_{Aaut} . The outcome of this process, the authentication parameter, shall be returned to the CAD, SAM or Host for checking.

5.5.3 CAD, SAM or Host authentication

The application supplier may implement independent authentication at ADF level in a way similar to that specified in 5.3.3. If this function is required then the cryptographic key k_{Aaut} as specified in ISO 10202-3 shall be used.

CAD, SAM or Host authentication should comprise the movement from the ICC of a pseudo-random number or a time variant (for example a counter). 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 the algorithm in the CAD, SAM or Host using the cryptographic key k_{Aaut} . The outcome of this process, the authentication parameter, shall be returned to the ICC for checking.

5.5.4 Cardholder verification

The application supplier may adopt an independent cardholder verification method from that made available by the card issuer for general purpose verification. If a PIN is used, it may be verified in the CDF or ADF and protected in accordance with the requirements specified in ISO 10202-6.

5.5.5 ADF parameters update

The application supplier parameters stored in the ADF may be updated. In that case they shall be updated using the cryptographic key k_{Act1} specified in ISO 10202-3. This action shall be under the control of the application supplier.

5.6 Transaction handling

Transaction handling commences when a request for value or a request for authorization is sent to the ICC and ends with card session termination.

5.6.1 Transaction authorization

The purpose of the transaction authorization function is to approve or deny any authorization request by checking information specific to the transaction (for example available balance in the CDF or ADF, or the transaction amount requested against authorization limits).

This authorization process, which is conducted at the discretion of the card issuer or application supplier, may be performed off-line or on-line, based on parameters stored in the ICC, CAD or SAM.

When a decision is made by the ICC, CAD or SAM that an on-line authorization process is necessary then there should be no procedural difference or external evidence of this until the transaction has commenced (see annex B for further guidance).

If protection of the on-line authorization is required then a cryptographic exchange using the cryptographic key k_{Amac} specified in ISO 10202-3 shall be used.

If an on-line authorization is required by the IC, but the CAD cannot perform an on-line transaction, the card issuer or application supplier shall have determined how the transaction should proceed.