INTERNATIONAL STANDARD ISO 10202-1:1991
TECHNICAL CORRIGENDUM 1

Published 1999-12-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

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

Part 1:

Card life cycle

TECHNICAL CORRIGENDUM 1

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

Partie 1: Cycle de vie de la carte

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to International Standard ISO 10202-1:1991 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial service.*

This part of ISO 10202 contains data elements related to dates where the *year* is formatted in *less than four digits*. The format of these data elements will be considered, and, if appropriate, amended on the occasion of the next revision. Meanwhile, it is recommended that users consider, within the context of their implementation of this part of ISO 10202, any requirements for amendment in relation to the year 2000 and their business environment.

ICS 35.240.15

Ref. No. ISO 10202-1:1991/Cor.1:1999(E)

Printed in Switzerland

INTERNATIONAL STANDARD

ISO 10202-1

First edition
1991-09-15

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

Part 1:
Card life cycle

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

Partie 1: Cycle de vie de la carte

Reference number
ISO 10202-1:1991(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 10202-1 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services.*

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 6: Cardholder verification*

Further parts of ISO 10202 will consist of part 4: *Security application modules,* and part 5: *Use of algorithms.*

Annex A forms an integral part of this part of ISO 10202. Annexes B and C are 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 1: Card life cycle

1 Scope

This part of ISO 10202 specifies the principles for the protection of the Integrated Circuits (ICs) in financial transaction cards from their manufacture and issue, through use to their termination.

It is applicable to any organization which is responsible for implementing security procedures for protecting the IC and the Integrated Circuit Cards (ICC) during their life cycle.

This part of ISO 10202 covers those features of the life cycle of the ICC which are additional to those addressed in International Standards relating to bank cards with magnetic stripes. This part of ISO 10202 covers the security techniques to be used by organizations involved in the IC and ICC manufacture, issue, use of the IC and termination processes.

NOTES

1 The risks addressed by these procedures and the measures to counteract these risks are provided in annex B. A description of security audit and security related data fields recorded in the IC is given in annex A.

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

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 3166:1988, *Codes for the representation of names of countries.*

ISO 7812:1987, *Identification cards — Numbering system and registration procedure for issuer identifiers.*

ISO 7813:1990, *Identification cards — Financial transaction cards.*

3 Definitions

For the purposes of this part of ISO 10202, the following definitions apply.

3.1 Application Data File (ADF): A file in the IC that supports one or more services.

3.2 application supplier: An entity which is responsible for an ADF after its allocation.

3.3 ADF personalizer: The entity which initially loads security and related operational parameters in the space allocated in the IC for an ADF.

3.4 ADF allocation: The secure provision of space in the IC for subsequent use by an application supplier.

3.5 Card Accepting Device (CAD): A device used to interface with the ICC during a session.

3.6 card issuer: The institution (or its agent) which issues the financial transaction ICC to the cardholder.

3.7 cardholder: The person to whom the financial transaction ICC has been issued.

3.8 Common Data File (CDF): A mandatory file that contains the common data elements stored in the ICC and used to identify the card, the card issuer and the cardholder.

3.9 embedder: The entity which performs IC embedding.

3.10 Integrated Circuit (IC): Electronic component(s) which are embedded in an ICC in the form of microcircuits to perform processing and memory functions.

3.11 Integrated Circuit Card (ICC): A card into which has been inserted one or more ICs.

3.12 IC assembler: The entity which performs IC assembling.

3.13 IC assembling: The process of combining one or more ICs with elements enabling external communication to a module suitable for IC embedding.

3.14 IC assembly: A module containing one or more ICs and external communication elements suitable for IC embedding.

3.15 IC embedding: The process of inserting an IC assembly into a card to form an ICC.

3.16 Primary Account Number (PAN): The assigned number that identifies the card issuer and cardholder. This number is composed of an issuer identification number, individual account identification, and an accompanying check digit, as defined in ISO 7812.

3.17 security audit trail: The historic data and information which are available for examination in order to prove the correctness and integrity with which the agreed security procedures have been followed and which allows breaches in security to be detected.

4 General security principles

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

a) The manufacture, preparation, usage and termination of ICCs shall be performed in such a way that compromising one ICC implementation shall not compromise any other ICC implementation.

b) The card issuer shall be responsible for the card life cycle, allocation of the CDF and data in the CDF and for the allocation of ADFs; once allocated an ADF shall be controlled by the application supplier who may be the card issuer. A card issuer or an application supplier may delegate functions to agents within the scope of the security principles.

c) The data stored in an ADF and/or the actions performed in respect of an ADF shall not compromise the ADFs of another application supplier.

d) Security audit trail records shall be kept during the ICC's life cycle.

5 Protection during the card life cycle

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

Manufacture of the IC and ICC (see 5.1)

Card preparation (see 5.2)

Card personalization

CDF activation

Application Data File (ADF) preparation (see 5.3)

ADF allocation

ADF personalization

ADF activation

Card usage (see 5.4)

Card use

ADF deactivation

CDF deactivation

CDF reactivation

ADF reactivation

Termination of use (see 5.5)

ADF termination

CDF termination

Key termination

These requirements allow for the management of the card life cycle and form the basis for more detailed commercial agreements between those who manufacture, supply, issue and use ICCs.

5.1 Manufacture of the IC and ICC

The manufacturing process includes

- IC semi-conductor design and software design
- IC manufacturing
- IC assembling
- IC embedding

Prior to the stage when proprietary data enters the manufacturing process of the ICC, the security of the manufacturing procedures shall be in accordance with the level of security as requested by the card issuer.

From the stage when proprietary data (e.g. a proprietary cryptographic algorithm or a cryptographic key) and/or other secret elements are combined with an IC the following security requirements 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 an IC shall only be through the use of a Production Key which will be specified in ISO 10202-3. Between each stage of manufacture there may be a different Production Key.

c) During the storage and transport, ICs and ICCs shall be physically or cryptographically protected.

The following data shall be recorded in an IC for security audit purposes (see annex A for detailed specifications):

- IC manufacturer identifier
- Manufacturer's IC type identifier
- Embedder/IC assembler identifier

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

5.2 Card preparation

Card preparation consists of two steps:

- Card personalization
- CDF activation

5.2.1 Card personalization

The card issuer shall be responsible for the card personalization process.

The personalization process shall be under the control of the appropriate cryptographic key(s) which will be specified in ISO 10202-3 and involves the loading of Common Data File (CDF) data and its IC related cryptographic keys. The CDF data shall contain, at least, the Primary Account Number (PAN) and the Expiration Date (ED) (defined in ISO 7813). The minimum data to be loaded during this process will be specified in ISO 9992-4.

A card personalizer identifier shall be recorded in an IC for security audit purposes (see annex A for detailed specifications).

If the PAN in the CDF encoded on the magnetic stripe and/or embossed on the ICC they shall all be the same.

5.2.2 CDF activation

The CDF activation process prepares the ICC for use in financial transactions by the cardholder. CDF activation is the responsibility of the card issuer. CDF activation shall be conducted by a securely controlled process. CDF activation may take place at the end of the CDF personalization process or as a separate process later.

CDF activation shall be indicated in the ICC.

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

Unique identification of the IC may be obtained by combining the CDF activator identifier with the CDF activator serial number.

5.3 ADF preparation

ADF preparation consists of three steps:

- ADF allocation
- ADF personalization
- ADF activation

5.3.1 ADF allocation

This process shall only be conducted under the control of the card issuer and involves the allocation of memory areas in an IC. For protection against unauthorized ADF allocation a cryptographic exchange using the appropriate cryptographic key which will be specified in ISO 10202-3 shall be used.

5.3.2 ADF personalization

The application supplier shall be responsible for the ADF personalization process. For protection against unauthorized personalization a cryptographic exchange using the appropriate cryptographic key which will be specified in ISO 10202-3 shall be used. This process involves the loading of ADF related keys and data.

5.3.3 ADF activation

The ADF activation process prepares an ADF for use in financial transactions by the cardholder. ADF activation is the responsibility of the application supplier.

ADF activation shall be conducted by a securely controlled process. ADF activation may take place at the end of the ADF personalization process or as a separate process later.

ADF activation shall be indicated in the ICC. An ADF can only be activated when the CDF is either in an activated or a reactivated state.

5.4 Card usage

5.4.1 Card use

An ICC shall not be issued unless the card has been personalized. The IC shall not be usable for a financial transaction unless the CDF is in an activated or a reactivated state.

Where a Personal Identification Number (PIN) is to be used in association with an ICC, the PIN shall be managed in accordance with the procedures which will be specified in ISO 10202-6.

Updating of ADF security parameters shall not be possible without approval of the application supplier. For protection against unauthorized modification a cryptographic exchange using the appropriate cryptographic key which will be specified in ISO 10202-3.

5.4.2 ADF deactivation

ADF deactivation shall be indicated in the ICC.

Only the application supplier shall be able to deactivate or define the conditions for the deactivation of the ADF. Whilst the ADF is deactivated the ADF shall not perform any financial transaction. However reading of an ADF, and ADF reactivation may still be performed under the direct control of the application supplier.

For protection against unauthorized deactivation of an ADF a cryptographic exchange using the appropriate cryptographic key which will be specified in ISO 10202-3 shall be used.

5.4.3 CDF deactivation

CDF deactivation shall be indicated in the ICC.

Only the card issuer shall be able to deactivate or define the conditions for the deactivation of the CDF. Whilst the CDF is deactivated an ICC shall not perform any financial transaction. However, reading of the CDF, or CDF reactivation may still be performed under the direct control of the card issuer.

For protection against unauthorized deactivation of the CDF a cryptographic exchange using the appropriate cryptographic key which will be specified in ISO 10202-3 shall be used.

5.4.4 CDF reactivation

CDF reactivation shall be indicated by an active status in the ICC.

The process of reactivating the CDF, so that the ICC may again be used for financial transactions, shall be conducted under the control of the card issuer. For protection against unauthorized reactivation of the CDF a cryptographic exchange using the appropriate cryptographic key which will be specified in ISO 10202-3 shall be used.

5.4.5 ADF reactivation

ADF reactivation shall be indicated by an active status in the ICC.

The process of reactivating an ADF, so that it may again be used for financial transactions, shall be conducted under the control of the application supplier. For protection against unauthorized reactivation of an ADF a cryptographic exchange using the appropriate cryptographic key which will be specified in ISO 10202-3 shall be used.

5.5 Termination of use

5.5.1 ADF termination

ADF termination shall be indicated in the ICC.

ADF termination shall be the responsibility of the application supplier. In this state an ADF shall be permanently disabled (no possible reactivation) from use for a financial transaction.

Preventing the termination of an ADF shall be the responsibility of the application supplier. For protection against unauthorized termination of an ADF a cryptographic exchange using the appropriate cryptographic key which will be specified in ISO 10202-3 shall be used.

5.5.2 CDF termination

CDF termination shall be indicated in the ICC.

CDF termination shall be the responsibility of the card issuer. In this state the CDF shall be permanently disabled (no possible reactivation) from use for a financial transaction.

Preventing the termination of the CDF shall be the responsibility of the card issuer. For protection against unauthorized termination of the CDF a cryptographic exchange using the appropriate cryptographic key which will be specified in ISO 10202-3 shall be used.

5.5.3 Key termination

After ADF termination all cryptographic keys remaining in the ADF should be disabled under the control of the application supplier. This process should not preclude the subsequent reading of previously readable information (which will be specified in ISO 10202-3).

After CDF termination and the transfer of any residual values from an IC, all cryptographic keys remaining in the CDF should be disabled under the control of the card issuer. This process should not preclude the subsequent reading of the previously readable CDF information (which will be specified in ISO 10202-3).

After the termination of all the keys the cryptographic functions should be disabled in such a way that they cannot be used again.

Annex A
(normative)

Description of security audit and security related data fields

(Reference to these fields will be specified in ISO 9992-4).

IC manufacturer identifier

Status:	Mandatory
Location:	Area which is generally readable
Acces conditions:	Not changeable
Format:	1 byte
Content:	Manufacturer identifier in accordance with a register maintained by ISO.
Purpose:	To identify in a unique way the manufacturer of the IC

Manufacturer's IC type identifier

Status:	Mandatory
Location:	Area which is generally readable
Access conditions:	Not changeable
Format:	2 bytes
Content:	Manufacturer's IC type identifier
Purpose:	To identify, for a given manufacturer, each IC design and/or batch of ICs produced

Embedder/IC assembler identifier

Status:	Mandatory
Location:	Area which is generally readable
Access conditions:	Not changeable
Format:	5 bytes in the form CCEEA
Content:	CC — 2 alphabetic country code of the embedder as defined in ISO 3166 EE — 2 alphanumeric characters based on the name of the embedder. (There should be a registry at the national level.) A — 1 alphanumeric character for other purposes, e.g. to identify the IC assembler
Purpose:	To identify the organization which combines the IC assembly and the plastic card

Card personalizer identifier

Status:	Mandatory
Location:	CDF area.
Access conditions:	Not changeable
Format:	1 byte
Content:	Personalizer identifier as defined by the card issuer
Purpose:	To define the personalizer of the card

CDF activator identifier

Status:	Optional
Location:	CDF area
Access conditions:	Not changeable
Format:	10 numeric digits in the form IIIIIINNNN
Content:	IIIIII — Issuer identification as defined in ISO 7812 NNNN — Additional identification as defined by the card issuer
Purpose:	To identify in a unique way the activator of the CDF

CDF activator serial number

Status:	Optional
Location:	CDF area
Access conditions:	Not changeable
Format:	6 numeric digits
Content:	Defined by the card activator
Purpose:	To identify in a unique way, for a given card activator, the activated CDF

Date of activation of the CDF

Status:	Optional
Location:	CDF area
Access conditions:	Not changeable
Format:	6 numeric digits
Content:	YYMMDD
Purpose:	To define the date of activation

Annex B
(informative)

Card life cycle — Security/risk matrix — Measures to minimize risk

Security risk	Testing of IC	Secure environment, storage, transport	Audit trail	Key management
Functional integrity				
Accidental	×		×	
Intentional	×	×	×	
Memory integrity				
Accidental	×		×	×
Intentional	×	×	×	×
Other hardware faults			×	
Theft		×	×	
Fraudulent				
Allocation		×		×
Activation		×		×
Personalization		×		×
Deactivation				×
Reactivation				×

Annex C
(informative)

Bibliography

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

[2] ISO 9564-1:—[1], *Banking — Personal identification number management and security — Part 1: PIN protection principles and techniques.*

[3] ISO 9992-1:1990, *Financial transaction cards — Messages between the integrated circuit card and the card accepting device — Part 1: Concepts and structures.*

[4] ISO 9992-4:—[1], *Financial transaction cards — Messages between the integrated circuit card and the card accepting device — Part 4: Common data for interchange.*

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

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

[7] ISO 10202-6:—[1], *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 6: Cardholder verification.*

[1] To be published.

UDC 336.717:336.719.2:681.327.6

Descriptors: banking, identification cards, credit cards, integrated circuit cards, safety.

Price based on 9 pages