INTERNATIONAL STANDARD

ISO 10202-6

First edition
1994-12-15

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

Part 6:
Cardholder verification

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

Partie 6: Vérification du porteur de carte

Reference number
ISO 10202-6:1994(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 10202-6 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. 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 6: Cardholder verification

1 Scope

This part of ISO 10202 specifies the requirements for the security of cardholder verification when a discrete Cardholder Identification Value (CIV), for example a Personal Identification Number (PIN), is used in conjunction with an Integrated Circuit Card (ICC), which may or may not contain magnetic stripes. The purpose of cardholder verification is to determine that the card presenter is the cardholder. ISO 9564-1 applies, except for the clauses of this part of ISO 10202 which cover those aspects specific to the use of an ICC.

The provisions of this part of ISO 10202 are not intended to protect against the use of bogus Card Accepting Devices (CADs).

It is applicable to any organisation which is responsible for implementing secure procedures for the use of CIVs in conjunction with an ICC.

This part of ISO 10202 covers the security associated with the matching of something a cardholder possesses — an ICC — and something a cardholder knows, namely a CIV such as a PIN. It also addresses relevant security requirements of an ICC and CAD, where each can have an integrated circuit (IC) only or jointly magnetic stripe and IC capability. The emphasis is on an IC-only system.

NOTE 1 The term IC refers to an IC embedded in an ICC.

Cardholder verification may be performed either at the Common Data File (CDF) or Application Data File (ADF) level.

NOTE 2 The terms 'card issuer' and 'application supplier' encompass their respective 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 9564-1:1991, *Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques.*

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

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

[1] To be published.

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 biometric verification: Form of cardholder verification involving the comparison of an observed biological characteristic against a reference value.

3.2 cardholder: Customer associated with the Primary Account Number requesting the transaction from the Card Acceptor.

3.3 Cardholder Identification Value (CIV): Value which is used for the verification of cardholder identity.

NOTE 3 A discrete CIV is known to the cardholder (i.e. a PIN or password). A biometric CIV is a representation of an observed biological characteristic of the cardholder.

3.4 IC-only system: Card system which relies solely on IC technology and corresponding interface equipment.

3.5 mixed CAD: CAD which accepts IC cards and magnetic stripe cards.

3.6 mixed system: System which accepts a combination of IC and magnetic stripe card technology.

3.7 password: Alphanumeric discrete CIV where each character has a unique representation.

3.8 reference CIV: CIV used to verify the transaction CIV.

3.9 transaction CIV: CIV as provided by the card presenter during a transaction.

4 Discrete value methods

This clause specifies the minimum security requirements in the use of discrete CIVs with an ICC. These discrete values can be PINs, as defined in ISO 9564-1, or passwords (see annex B).

4.1 General security principles

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

a) Those basic principles of PIN management specified in ISO 9564-1.

b) The requirements for cardholder verification at the Common Data File (CDF) level shall be specified by the card issuer and at the Application Data File (ADF) level by the application supplier.

c) The discrete reference CIV shall be loaded securely into the IC in a controlled manner.

d) The discrete reference CIV shall be stored in the IC in a way which is protected from external reading.

e) If there is a CDF-level CIV, the procedures for loading, re-loading and changing the discrete reference CIV shall be under the control of the card issuer.

f) The process of verifying the CDF-level CIV should be available for use by any application in the card.

g) If there is an ADF-level CIV, the procedures for loading, re-loading and changing the discrete reference CIV shall be under the control of the application supplier.

h) The cardholder verification process of an ICC system shall be performed in such a manner that it shall not compromise that system or any other ICC or magnetic stripe card system.

i) The cardholder verification process shall be performed in such a way that compromise of one IC shall not lead to the compromise of any other IC.

j) The discrete CIV checking process shall be performed in the IC.

k) If a discrete transaction CIV is checked then the IC shall protect against an exhaustive search for the discrete reference CIV.

4.2 Personal Identification Number (PIN)

If a PIN is used in a system which employs ICC technology, the requirements of ISO 9564-1 shall apply, subject to the provisions of this part of ISO 10202.

4.2.1 PIN loading and re-loading

The loading into an IC of an initial reference PIN or the re-loading of a reference PIN (for example to replace a forgotten PIN) shall be carried out in a physically secure environment or be cryptographically protected using the appropriate cryptographic key which will be specified in ISO 10202.

4.2.2 PIN change

The changing of a CDF reference PIN or an ADF reference PIN may be performed by the cardholder, but shall employ a procedure provided by the card issuer or application supplier respectively that includes the verification of the current PIN.

4.2.3 PIN storage

A reference PIN stored in an IC shall be protected from external reading. A reference PIN in an IC may be stored as plain text provided the ICC meets the following conditions:

a) The unauthorized determination of the reference PIN stored within the IC shall cause damage to the IC so that the IC cannot be placed back in service. Furthermore, determining the reference PIN which has been or will be used within the IC shall require specialised equipment and skills which are not generally available.

b) The penetration of an ICC shall not disclose sufficient information to deduce the reference PIN associated with any other ICC.

In an IC-only system, PIN verification, when performed, shall be performed in the IC. Furthermore, the reference PIN shall not be retained or be reproduceable by the card issuer or application supplier and should be stored only in the IC.

4.2.4 PIN transmission

The ICC transaction PIN shall be transmitted to the IC and the ICC reference PIN shall never leave the IC.

In a mixed CAD, the transaction PIN shall be cryptographically protected when it leaves the PIN pad but if the connection between the IC reader and the PIN pad is physically secure, then the PIN can be transmitted in clear text into the IC. (See ISO 10202-5 for details regarding the provision of cryptographic protection.)

NOTE 4 The preferred solution is for the PIN pad and the ICC reader to be physically integrated.

In an IC-only system and where the ICC does not contain a magnetic stripe which could be used in conjunction with the same PIN, cryptographically secure PIN transmission between the PIN pad and the IC is not mandatory.

4.2.5 PIN verification

The transaction PIN shall be checked in the IC against the reference PIN. The response from the IC as to the outcome of the PIN verification need not be cryptographically protected. (See ISO 10202-2.)

The ICC shall protect against an exhaustive search for a reference PIN by limiting the number of consecutive unsuccessful PIN attempts processed. The actual number of consecutive incorrect attempts at PIN verification at the CDF level or ADF level allowed by the IC and the action which follows shall be at the discretion of the card issuer or application supplier, respectively.

The IC shall give no indication about the result of cardholder verification until the IC has recorded or can guarantee that it can record the result of the verification.

Annex A
(normative)

CIV presentation

When a CIV is a set of 4 to 12 digits to be presented in clear text, it should be presented to the ICC using the PIN-block format defined in ISO 9564-1:1991, subclause 8.3.1.1 (plain text field), and the control field C shall be 2 (i.e. 0010).

Annex B
(informative)

Password and biometric methods

B.1 Password

The use of a password of typically 6 to 12 characters with an ICC is possible. If the use of passwords with an ICC in international interchange becomes a practicable proposition then it will be considered for incorporation in this part of ISO 10202.

B.2 Biometric methods

The ICC allows for biometric methods. When a biometric method suitable for consideration for cardholder verification in international interchange using an ICC is submitted via a national member body of ISO, it will be considered for incorporation in this part of ISO 10202.

Annex C
(informative)

Bibliography

[1] ISO/IEC 7813:1995[2], *Identification cards — Financial transaction cards.*

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

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

[4] ISO 10202-4:—[3], *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 4: Secure application modules.*

[5] ISO 10202-7:—[3], *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 7: Key management.*

[2] To be published. (Revision of ISO 7813:1990).

[3] To be published.

This page intentionally left blank