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

Part 8:
General principles and overview

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

Partie 8: Principes généraux et vue d'ensemble



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 10202-8 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail 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 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 to C of this part of ISO 10202 are for information only.

© ISO 1998

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
Internet iso@iso.ch

Printed in Switzerland

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

Part 8:

General principles and overview

1. SCOPE

ISO 10202 defines the security architecture of financial transaction systems using integrated circuit cards. This part introduces general security principles, presents an overview of security requirements for financial transaction systems using integrated circuit cards, and introduces parts 1 to 7 of ISO 10202. The mandatory and optional data elements used in ISO 10202 are summarised in this part.

There are three annexes to this International Standard, namely annex A (informative) which provides a quick guide to this International Standard, annex B (informative) which portrays a logical architecture of the ICC, and annex C (informative) for a logical architecture of the SAM.

2. NORMATIVE REFERENCES

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 10202. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 10202 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 3166	Codes for the representation of names of countries
ISO 4909	Bank cards - Magnetic stripe data contents for track 3
ISO 7810	Identification cards - Physical characteristics
ISO 7812	Identification cards - Numbering system and registration procedure for issuer identifiers
ISO 7813	Identification cards - Financial transaction cards
ISO/IEC 7816-1	Identification cards - Integrated circuit(s) cards with contacts - Physical characteristics
ISO/IEC 7816-2	Identification cards - Integrated circuit(s) cards with contacts - Dimensions and locations of the contacts
ISO/IEC 7816-3	Identification cards - Integrated circuit(s) cards with contacts - Electronic signals and transmission protocols
ISO/IEC 7816-4	Identification cards - Integrated circuit(s) cards with contacts - Interindustry commands for interchange
ISO/IEC 7816-5	Identification cards - Integrated circuit(s) cards with contacts - Number system and registration procedure for application identifiers

ISO/IEC 7816-6	Identification cards - Integrated circuit(s) cards with contacts - Interindustry data elements
ISO 8583	Financial transaction card originated messages - Interchange message specifications
ISO 8732	Banking - Key management (wholesale)
ISO 8908	Banking and related financial services - Vocabulary and data elements
ISO 9564-1	Banking - Personal identification number Management and security - PIN protection principles and techniques
ISO 9796	Information technology - Security techniques - Digital signature scheme giving message recovery
ISO 9807	Banking and related financial services - Requirements for message authentication (retail)
ISO 9992-1	Financial transaction cards - Messages between the integrated circuit card and the card accepting device - Concepts and structures
ISO 9992-2	Financial transaction cards - Messages between the integrated circuit card and the card accepting device - Functions, messages (commands and responses), data elements and structures
ISO 10202-1	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Card Life Cycle
ISO 10202-2	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Transaction Process
ISO 10202-3	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Cryptographic Key Relationships
ISO 10202-4	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Secure Application Modules
ISO 10202-5	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Use of Algorithms
ISO 10202-6	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Cardholder Verification
ISO 10202-7	Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Key Management

ISO 11568 Banking - Key management (retail)

ISO 13491 Banking - Secure Cryptographic Devices (retail)

STANDARDSISO.COM : Click to view the full PDF of ISO 10202-8:1998

3. DEFINITIONS

The following definitions apply to ISO 10202. For terms not defined within this International Standard refer to ISO 8908

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

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

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

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

Asymmetric algorithm: An algorithm in which the encipherment and decipherment keys are different and which it is computationally infeasible to deduce one from the other.

Authentication: A process used to ensure data integrity and data origin authentication.

Biometric verification: A form of cardholder verification involving the comparison of an observed biological characteristic against a reference value.

Card accepting device (CAD): The device used to interface with the ICC during a session.

Card acceptor: The party accepting the card for the provision of goods and services.

Card Issuer: The institution (or its agent) which issues the financial transaction ICC to the cardholder.

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

Cardholder Identification Value (CIV): A value which is used for the verification of cardholder identity. A discrete CIV is known to the cardholder (ie a PIN or password). A biometric CIV is a representation of an observed biological characteristic of the cardholder.

Certificate: See transaction certification code and public key certificate.

Certificate identifier: Certificate information which enables proper verification of a key certificate.

Certification authority: An authority trusted by all users to create and assign certificates.

Ciphertext: Enciphered plaintext.

Collision resistant: A function is called collision resistant if any two different input values produce different output results.

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.

Counter: An increasing count used between two parties.

Credentials: The set of data items assigned to each entity and used to authenticate that entity.

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

Cryptographic function: A process performed (eg. encryption, authentication, certification) using a cryptographic algorithm.

Cryptographic key (key): A parameter used in conjunction with a cryptographic algorithm for executing cryptographic transformations.

Cryptographic link: Two logical entities (nodes) who have previously agreed to exchange data and who have a cryptographic key-relationship.

Cryptographic node: One of the logical entities (nodes) in a cryptographic link.

Cryptoperiod: A defined period of time which a cryptographic key is authorized for use, or during which time the cryptographic keys for a given system may remain in effect.

Data key: A cryptographic key used for the encipherment, decipherment or authentication of data.

Decipherment: The process of transforming ciphertext into plaintext.

Derivation key: A key used to generate a derived key.

Derived key: A symmetric key generated from a derivation key and non-secret variable data. The derivation key is used to generate a large number of keys (derived keys).

Digital signature: The result of a cryptographic transformation, executed by the initiator using his secret key with an asymmetric algorithm, providing non repudiation of the source and integrity of the signed data.

Distinguishing name: A name which uniquely identifies an entity in a process.

Diversified key: See derived key.

Dual control: A process of utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information whereby no single entity is able to access or utilise the materials eg. cryptographic keys.

Elementary file: A file which may contain data and/or file control information.

Encipherment: The process of transforming plaintext into ciphertext.

Entity authentication: Corroboration that the identity of an entity (node) is the one claimed.

Embedder: The entity which performs IC embedding.

Hash function: A one-way function mapping a variable length input to a fixed length output, such that it is computationally infeasible to obtain the same output from two different intelligible inputs; a hash function shall be collision resistant.

Host/SAM derivation key: A derivation key used to derive ICC or SAM keys.

Host security module: A physically secure device used to support cryptographic functions and perform SAM functionality on a host system.

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

IC assembler: The entity which performs IC assembling.

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

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

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

IC only system: A card system which relies solely on IC technology and corresponding interface equipment.

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

ICC derivation key: An ICC (CDF or ADF) derivation key used to derive unique message data keys.

Initiator: The node or entity that initiates a process.

Key enciphering key: A key used to encipher another key.

Key generation module: A type of cryptographic equipment used for generating and deriving cryptographic keys.

Key identifier: Key information which enable the recipient to determine the appropriate key(s) associated with a transaction.

Key loading module: An electronic, self contained unit which is capable of storing at least one cryptographic key and transferring that cryptographic key, upon request, into a cryptographic device such as an ICC or a SAM.

Key synchronization: The ability of two nodes to determine the identical data key.

Keying material: The data necessary to establish and maintained a keying relationship.

Master derivation key: A derivation key used by a bank card company or another organisation to derive unique issuer or application supplier keys.

Message authentication: Process providing cryptographic proof that a message has not been altered or destroyed in an unauthorised manner.

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.

Mixed CAD: A CAD which accepts IC cards and magnetic stripe cards.

Mixed system: A system which accepts a combination of IC and magnetic stripe card technology.

Non-repudiation: Security service providing permanent cryptographic proof of the integrity and origin of data - both in an unforgeable relationship - which can be verified by any third party at any time.

One-way function: A mathematical function which maps input values into output values in an irreversible manner.

Password: An alphanumeric discrete CIV where each character has a unique representation.

Plaintext: Intelligible data that has a meaning and can be read or acted upon without the application of a transformation.

Public key: That part of an asymmetric key set which is known to other parties than the generator of the key set.

Public key certificate: A set consisting of user credentials (including the public key) together with the trusted third party's digital signature of these credentials.

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

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.

Reference CIV: The CIV used to verify the transaction CIV.

Reflection attack: An attack by a false respondent whereby the initiator is challenged in a separate session with the same random value it has transmitted in a concurrent session to authenticate the respondent.

Respondent: The node or entity that responds to the initiator of a process.

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

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

Secure 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.

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 unauthorised access is not possible. In order to achieve this the module shall be physically and logically protected.

Symmetric algorithm: A cryptographic method using the same secret cryptographic key for encipherment and decipherment.

Timeliness: A method to prevent a valid message from being replayed at a later time by using a probe of information as a challenge requesting a proper and timely response.

Token: A set of data items formed for each data exchange sent by one entity to another.

Transaction acquirer: Institution which collects the data relating to a financial transaction from the card acceptor for settlement purposes.

Transaction certification code: Result of the transformation certification process producing an electronic signature, which could be either a MAC (based on a symmetric algorithm) or a digital signature (based on an asymmetric algorithm).

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

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

Trusted third party: A generally accessible entity being known and trusted by the communicating entities.

4. ICC SECURITY ARCHITECTURE OVERVIEW

The integrated circuit card (ICC) used in financial transaction systems contains an integrated circuit (IC) which performs processing and memory functions. The ICC, issued by a card issuer, supports one or more applications. The applications may be independent, and may belong to different parties, called application suppliers. The card issuer may be an application supplier.

ISO 10202 defines minimum security requirements and optional security functionality for financial transaction systems using ICCs. These security requirements are applicable during the entire life of the ICC, called the card life cycle. The card life cycle covers the IC and ICC from their manufacture, through their use and to their eventual termination, and is described in ISO 10202-1. The card issuer is responsible for the security procedures during the life cycle of the ICC.

The card issuer may enter into business relationships with application suppliers to add applications to the ICC. ICC transactions may be processed on-line or off-line, and may involve the participation of a card acceptor, the party accepting the card for the provision of goods or services. The security requirements during the transaction process are described in ISO 10202-2. Contractual agreements are necessary, for example, when the ICC is used as a pre-paid instrument, to provide for the use or refund of unused prepaid value. The ability to activate and deactivate any of the ICC applications improves control over the ICC as a financial instrument.

Common data which identifies the card, the card issuer and the cardholder are stored in the ICC by the card issuer in the ICC common data file (CDF). Specific application supplier data stored in the ICC are located in an application data file (ADF). ICC related data which may be stored in ICCs, including ISO 10202 security data, are defined in ISO 7816-6, and ISO 9992-2 for financial transaction systems. Annex B (informative) shows a logical architecture of the ICC.

The security of ICC systems relies on security processes, and the physical and logical characteristics of the ICC and optional secure application modules (SAMs) in card accepting devices (CADs). The security processes involve the use of cryptographic keys and are described in ISO 10202-3. ISO 10202-4 specifies the minimum security requirements for the life cycle of the SAM. Annex C (informative) shows a logical architecture of the ICC.

For the transaction process, the ICC enables the implementation of cryptographic authentication techniques described in ISO 10202-2 and ISO 10202-5. Cardholder identification values such as personal identification numbers (PINs) enable cardholder verification in the ICC (ISO 10202-6). The security functions available in the ICC may be restricted in use to a subset of the ICC applications. Security functions which may be implemented in ICCs and SAMs are described in ISO 10202-5.

During their entire life cycles, the ICC and SAM rely on the use of cryptographic keys and algorithms to protect their integrity and, when required, provide logical separation between applications in the ICC. Cryptographic keys and algorithms also permit the secure movement of data between an application in the ICC and the optional SAM or host system. ISO 10202-3 describes the cryptographic key relationships which may exist between parties which share cryptographic keys. ISO 10202-7 specifies the key management alternatives, and the procedures and processes necessary for the secure management of cryptographic keys.

Figure 1 and 2 show the components that may be part of the security architecture of financial transaction systems using integrated circuit cards.

- Manufacturing and preparation of the ICC and SAM:

During the manufacturing and preparation stages of the ICC and SAM, mandatory data and cryptographic keys are written to the ICC and SAM. Security measures are used to protect the ICC until it is delivered to the application supplier, and the SAM until it is delivered to the SAM provider.

Figure 1 gives an example of secure delivery of ICCs and SAMs by loading mandatory data and cryptographic keys into the ICC and SAM.

Key loading modules may be used to transfer cryptographic keys between the parties involved in the ICC and SAM life cycle. These keys are used to authenticate the ICC or SAM before the loading of further keys.

ISO 10202 defines the protection requirements for ICCs and SAMs during manufacturing and preparation.

- Transaction process:

For the transaction process, transaction relationships are established between:

- the ICC and the CAD/SAM for off-line applications,
- the ICC and the issuer or application supplier host system for on-line processing,
- the CAD/SAM and the application supplier host system for processing off-line transactions, or
- the SAM and SAM provider for updating of SAM parameters, program and keys.

Cardholder Identification Values (CIV) and cryptographic keys may be used during the transaction process to secure the access to the ICC, and ensure the integrity and confidentiality of transactions.

Figure 2 gives an example of financial transaction system components that may be used for the financial transaction process. In this example transaction relationships may be established between the ICC and SAM, the ICC and host system, and between the SAM and host system.

ISO 10202 defines the possible transaction relationships in financial transaction systems using ICCs, mandatory security for the transaction process, and optional security that may be implemented in the ICC, CAD or SAM.

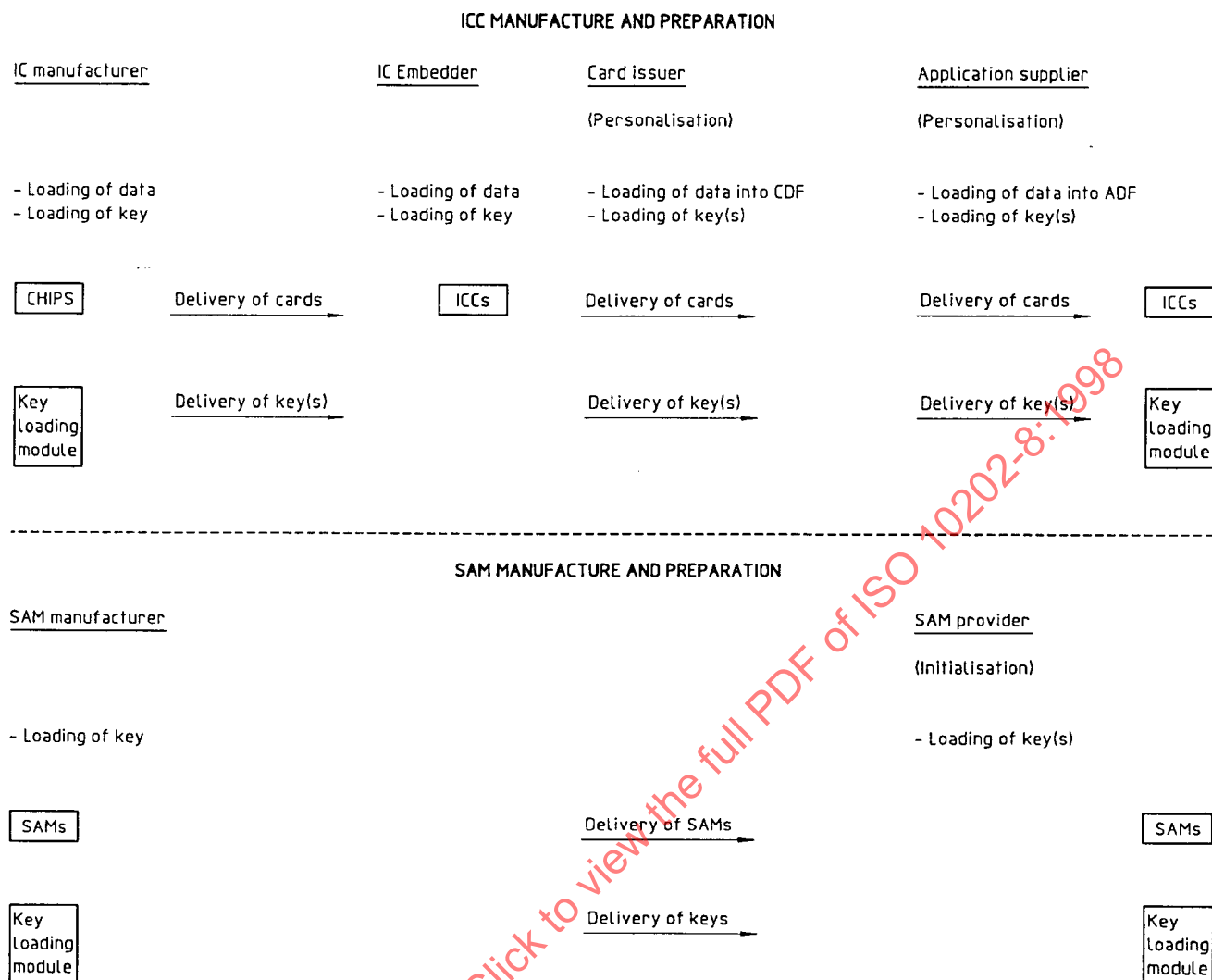


Figure 1: Example of components of the security architecture of financial transaction systems using ICCs - Manufacturing and preparation.

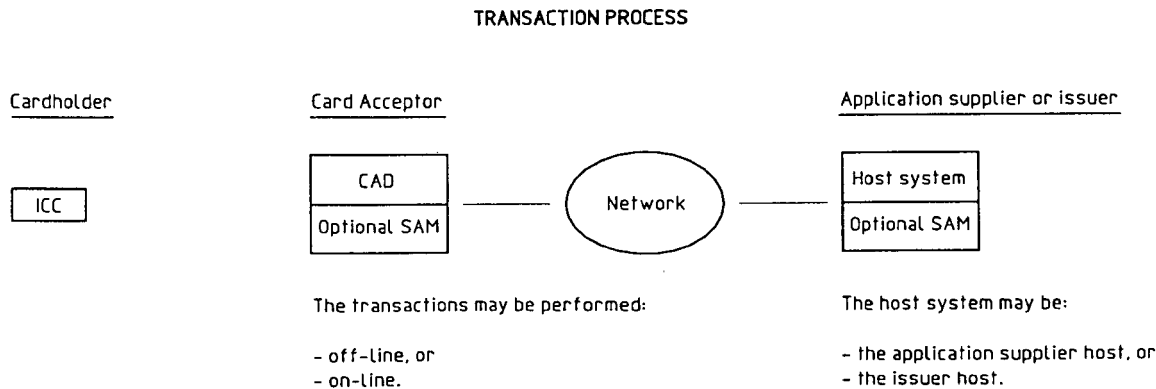


Figure 2: Example of components of the security architecture of financial transaction systems using ICCs— Transaction Process.

- Notes:

The ICC and the CAD are the only mandatory hardware components in a financial transaction system using ICCs. An optional SAM (see ISO 10202-4) may be contained in the CAD, Alternatively, the SAM functionality may be implemented in software in the CAD or be performed at the host system.

A CAD may be a stand alone component or may be integrated as part of an automated teller machine (ATM), a point of service (POS) terminal, or other terminals that may be used for financial transaction processing.

5. ICC AND SAM SECURITY REQUIREMENTS

The ICC and SAM shall support the mandatory security described in ISO 10202. Additional security, if present, shall be implemented as specified in ISO 10202 to facilitate inter-operability.

ISO 10202 does not specify the internal design of the operating system of the ICC and SAM. However, to comply to ISO 10202, the operating system of the ICC and SAM shall fulfill the following security requirements.

- a) Ensure that any application using a CDF or an ADF does not compromise the security of any other application. Any functionality supported by the ICC or SAM shall be implemented without compromising security.
- b) Only perform the functions allowed in the SAM or in the CDF or ADFs of the ICC. The operating system shall ensure that encipherment and authentication are performed when required for secure messaging to and from the ICC.
- c) Restrict access to the CDF or ADFs present in the ICC after a defined error threshold is reached. The minimum requirement is deactivation or termination of the CDF or an ADF when required by the card issuer or application supplier.
- d) Restrict access to security related data according to the protection requirements defined in ISO 10202, and implement access control mechanisms to restrict access to data which may be present in the ICC or SAM.
- e) Support a key management scheme specified in ISO 10202-7. The ICC shall have physical and logical security to protect secret cryptographic keys against disclosure. It shall not be possible to instruct the ICC or SAM to disclose a secret cryptographic key.
- f) Ensure that a cryptographic key is used only for its intended purpose. The operating system shall ensure that cryptographic keys can only be loaded into the ICC or SAM according to the requirements of ISO 10202-3 and ISO 10202-7.
- g) Ensure that any program code in an ICC or SAM does not compromise security.
- h) Ensure that access control conditions are met before accessing data contained in the SAM or in the CDF or an ADF in the ICC.
- i) Ensure that all data flow to or from the memory of the ICC or SAM is controlled by the operating system of the ICC or SAM. There shall be no other way for data transfers to or from the memory of the ICC.
- j) Ensure that after personalisation, the operating system code of the ICC or SAM cannot be changed or be otherwise accessible. The ICC issuer shall be responsible for the functionality and integrity of the operating system of the ICC.
- k) Ensure that after personalisation, the operating system code of the SAM cannot be changed or be otherwise accessible. However, changes of the operating system may be made by the SAM provider under secure cryptographic mechanisms. The SAM provider shall be responsible for the functionality and integrity of the operating system of the SAM.

NOTE: Audit records of attempted breaches or completed processes should be maintained by the ICC or SAM.

6. OVERVIEW OF ISO 10202 STANDARD

The ISO 10202 standard is an 8 part standard. This clause describes the scope of each part and summarises the mandatory and optional security.

Within ISO 10202 the CDF/ADF data file structure is an application oriented structure fully compatible with ISO 7816-4.

6.1 Card life cycle (ISO 10202-1):

All references in sub-clause 6.1 relate to ISO 10202-1: Card Life Cycle

6.1.1 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 organisation which is responsible for implementing security procedures for protecting the IC and the Integrated Circuit Card (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 organisations involved in the IC and ICC manufacture, issue, use of the IC and termination processes.

6.1.2 Mandatory security

Financial transaction systems using ICCs shall comply to the general security principles for card life cycle (sub-clause 4) and to mandatory security requirements for:

- manufacture of the IC and ICC (sub-clause 5.1),
- card preparation (sub-clause 5.2),
- ADF preparation (sub-clause 5.3), and
- card usage (sub-clause 5.4).

Mandatory security audit and security related data fields are described in Annex A.

6.1.3 Optional security

Optional ICC audit and security related data are described in Annex A.

6.2 Transaction process (ISO 10202-2):

All references in sub-clause 6.2 are related to ISO 10202-2: Transaction Process

6.2.1 Scope

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

6.2.2 Mandatory security

Financial transaction systems using ICCs shall comply to the general security principles (clause 4) for transaction process.

ICC compatibility check (sub-clause 5.1) is the only mandatory security function defined in this standard.

6.2.3 Optional security

Additional security functions may optionally be implemented at ICC level (sub-clause 5.3) and ADF level (sub-clause 5.5).

Security principles are defined for the following options:

- cardholder verification,
- CDF/ADF static authentication,
- CDF/ADF dynamic authentication,
- CAD/SAM/Host authentication, and
- CDF/ADF parameters update.

Security principles are also defined for:

- CDF accessing (sub-clause 5.2),
- ADF accessing (sub-clause 5.4),
- transaction handling (sub-clause 5.6), and
- card session termination (sub-clause 5.7).

6.3 Cryptographic key relationships (ISO 10202-3):

All references in sub-clause 6.3 refer to ISO 10202-3: Cryptographic Key Relationships.

6.3.1 Scope

This part of ISO 10202 specifies the minimum cryptographic key relationship requirements for the security architecture of financial transaction systems using ICCs and provides options from which the card issuer or application supplier can select those key relationships appropriate to their application.

Cryptographic key relationships may be established during the card life cycle and the SAM life cycle between the parties responsible for ICC and SAM manufacture and preparation, and for the transaction process.

Whenever a cryptographic key relationship is referred to in ISO 10202-3 that relationship is achieved by establishing a mutual secret key for a symmetric algorithm or an appropriate key from a public/secret key pair for an asymmetric algorithm.

6.3.2 Mandatory security

Financial transaction systems using ICCs shall comply to the general security principles for the protection of ICCs (CDF and ADFs) and SAMs (clause 4).

The issuer CDF control key is mandatory. If ADFs are used, key exchange keys and ADF control keys are mandatory.

6.3.3 Optional security

Cryptographic keys and key relationships which may be used in ICCs and SAMs are described. The use of these keys shall comply to this standard.

6.4 Secure Application Modules (ISO 10202-4):

All references in sub-clause 6.4 relate to ISO 10202-4: Secure Application Modules

6.4.1 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 in 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 organisation involved in issuing SAMs for use in CADs. A SAM may service one CAD or a cluster of attached CADs.

6.4.2 Mandatory security

Financial transactions systems using ICCs shall comply to the general security principles (clause 4) of this standard when a SAM is used.

Security requirements are defined for:

- the SAM life cycle (clause 5),
- SAM interfaces to the CAD (clause 6),

The minimum security functions (CDF and ADF dynamic authentication) that a SAM shall be able to execute are specified (sub-clause 7.1).

6.4.3 Optional security

Security requirements for additional SAM security functions such as SAM authentication by the ICC and by the host of the SAM provider, load/change SAM keys, transaction certification by the SAM, and load/change SAM data are defined (clause 7).

6.5 Use of algorithms (ISO 10202-5):

All references in sub-clause 6.5 relate to ISO 10202-5: Use of Algorithms.

6.5.1 Scope

This part of ISO 10202 applies to cryptographic exchanges where at least one node is an ICC or a SAM. Exchanges between other system nodes are outside the scope of this part of ISO 10202.

The provision of any security function is optional depending upon requirements of the system. Where a specific function is identified as being required, it shall be performed in the manner described herein.

6.5.2 Mandatory security

Security functions which are required in ICCs or SAMs shall be performed according to this standard.

6.5.3 Optional security

Cryptographic processes which may optionally be used in ICCs or SAMs are defined for both symmetric and asymmetric algorithms. They include:

- key exchange (sub-clause 6.1),
- entity authentication (sub-clause 6.2),

- message authentication (sub-clause 6.3),
- message encipherment (sub-clause 6.4),
- transaction certification (sub-clause 6.5), and
- PIN verification (sub-clause 6.6).

6.6 Cardholder verification (ISO 10202-6):

All references in sub-clause 6.6 relate to ISO 10202-6: Cardholder Verification:

6.6.1 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 ICC, which may or may not contain a magnetic stripe. The purpose of cardholder verification is to determine that the card presenter is the cardholder. The ISO 9564-1 standard shall apply except for the clauses of this International Standard (10202-6) 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).

This part of ISO 10202 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 IC only systems.

6.6.2 Mandatory security

Financial transaction systems using ICCs shall comply to the general security principles for the protection of CIVs (sub-clause 4.1) and to the PIN protection requirements (sub-clause 4.2) during PIN loading and re-loading, PIN change, PIN storage, PIN transmission, and PIN verification.

When the PIN is transmitted to the issuer or application supplier host, ISO 9564 shall apply. When the PIN is transmitted locally to the ICC, ISO 10202-6 shall apply.

6.7 Key Management (ISO 10202-7):

All references in sub-clause 6.7 relate to ISO 10202-7: Key Management