INTERNATIONAL STANDARD

ISO 10202-3

First edition
1998-07-01

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

Part 3:
Cryptographic key relationships

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

Partie 3: Relations avec les clés de chiffrement

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 10202-3 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 and B form an integral part of this part of ISO 10202. Annexes C and D are for information only.

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 3:
Cryptographic key relationships

1 SCOPE

This part of ISO 10202 specifies the minimum cryptographic key relationship requirements for security architectures of financial transaction systems using ICCs and, in addition, 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 this document 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.

NOTE: Whenever the card issuer or application supplier is referred to in this International Standard these terms encompass agents appointed by either.

The key relationships which are covered by this part of ISO 10202 are given in figure 1 (for the ICC and SAM manufacture and preparation) and figure 2 (for the transaction process). The Card Accepting Device (CAD) of figure 2 consists of one part that acts as an agent for the acquirer (outside the scope of this International Standard) and, optionally, one part that acts as an agent for the application supplier: a Secure Application Module (SAM). A SAM is either

- a physical device supplied by the SAM provider or
- a logical functionality in the CAD security module.

It is assumed that the SAM is the responsibility of the application supplier.

Two normative annexes are attached to this part of ISO 10202, namely annex A and B, tables of key relationships. Two informative annexes are attached; namely, annex C, an example of key layered structure in an ICC, and annex D, an example of how to use cryptographic keys.

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 9807 (1991) **Banking and related financial services - Requirements for message authentication (retail)**

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 (1991) **Financial Transaction Cards - Security architecture of financial transaction system using Integrated Circuit Cards - Card Life Cycle.**

ISO 10202 -2 **Financial Transaction Cards - Security architecture of financial transaction system using Integrated Circuit Cards - Transaction Process.**

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 10202 -8	**Financial Transaction Cards - Security architecture of financial transaction systems using Integrated Circuit Cards - General Principles and Overview.**

3 DEFINITIONS AND ABBREVIATIONS

3.1 For the purpose of the International Standard the following definitions apply.

ciphertext
Enciphered plaintext.

cryptographic key
A parameter used in conjunction with a cryptographic algorithm for executing cryptographic transformations.

decipherment
The process of transforming ciphertext into plaintext.

encipherment
The process of transforming plaintext into ciphertext for confidentiality.

key
(see cryptographic key)

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.

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

3.2 For abbreviations used in this part of 10202 such as CDF, ADF, ICC, see ISO 10202 - 1 (1991).

The following letters are used as abbreviations in the text which follows:

A: application supplier
B: trusted third party for public key certification
C: ICC
D: designer
E: embedder/IC assembler
H: cardholder
I : card issuer
K: secret key used with a symmetric algorithm
M: manufacturer
N: SAM initialiser
P: public key used with an asymmetric algorithm
Q: transaction acquirer
R: card personaliser
S: secret key used with an asymmetric algorithm
T: CAD
U: SAM
VA: ADF activator
VC: CDF activator
W: SAM activator

4 GENERAL SECURITY PRINCIPLES

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

a)Those principles applicable to the ICC, see 10202 -2
b)Those principles applicable to the SAM, see 10202 -4
c)The information obtainable by any means from one ICC shall not compromise the security of any other ICC or SAM system or the combination of such systems.
d)Access to a CDF or an ADF shall always be subject to the logical access controls of the CDF or ADF.
e)While processing in one given ADF, the memory belonging to other ADF's can neither be read nor written.
f)Knowledge of a cryptographic key at one layer of the cryptographic key layered structured shall not compromise any other cryptographic key at that layer or at a higher layer. (see section 7)
g)Cryptographic key separation shall ensure that after an ADF is activated the card issuer shall have no control over the functioning of that ADF unless the application supplier is either the card issuer or makes the card issuer his agent.

5 NOTATION FOR KEY RELATIONSHIPS AND ASSOCIATED KEYS

Two entities X and Y have established a keying relationship *k* when:

-they have exchanged or are sharing a common secret symmetric key K, or

-the public asymmetric key P of either X or Y has been exchanged and its certificate verified, or

-the public asymmetric key P of X and the public asymmetric key P of Y have been exchanged and their certificates verified.

The public asymmetric key P of entity X, and the public asymmetric key P of entity Y shall both be exchanged when two way encipherment, authentication and certification functions are required.
Entities which share a key are denoted by two letters separated by a hyphen, for example (X-Y).

The nomenclature used to denote a key - as provided in Table 1 - shall be $kl\,(i,j)\,f_{X\text{-}Y}$ where:
-*l* denotes who is responsible for loading the key.

-*k* is a generic notation for a key (K,P or S) which can be either a key for a symmetric or an asymmetric algorithm

-f denotes the function of the key.

-the index i denotes a specific ADF and its related set of keys

-the index j denotes a specific key of a set of keys related to one ADF and having the same function.

NOTE: j is the key set number defined in 10202-7 and 10202-8

TABLE 1 - Key Nomenclature

Key (k)	Responsible for loading keys (*l*)	Function of Key (f)	Entities which share the use of a key (X-Y)
K S P	A E I M N R	aut (entity authentication) cer (certification) ctl (control) enc (encipherment) kex (key exchange) mac(message authentication) prd (production)	A C E I M N R U

As an example for symmetric algorithms, KA (i,j) $aut_{C\text{-}A}$ is the application supplier Authentication Key j for ADF (i) shared by the ICC and the application supplier. An example for asymmetric algorithm, SA (i,j)aut is the application supplier Authentication Key j for ADF (i) known only by the application supplier.

The key relationships are established in different phases of the card of SAM life cycle - manufacture of the IC, ICC or SAM; ICC or SAM preparation; ADF preparation; card or SAM usage; and termination of use (see 10202-1).

A cryptographic key relationship is defined for every CDF, ADF and SAM related security function. For some of these functions, namely the mandatory control functions, the cryptographic key shall be different for each ICC [see annex A (normative)]. For other functions it is recommended [see annex A (normative)] that with the exception of the mandatory keys, it is the responsibility of the application supplier, card issuer and acquirer to determine which keys are needed, which keys may be omitted and which keys may be shared in several ICCs for their applications. The values defined for the references of keys are contained in 10202-7.

6 KEY RELATIONSHIPS

6.1 DURING MANUFACTURE AND PREPARATION

Figure 1 shows the ICC key relationships and the SAM key relationships during the manufacture and preparation of the ICC and SAM

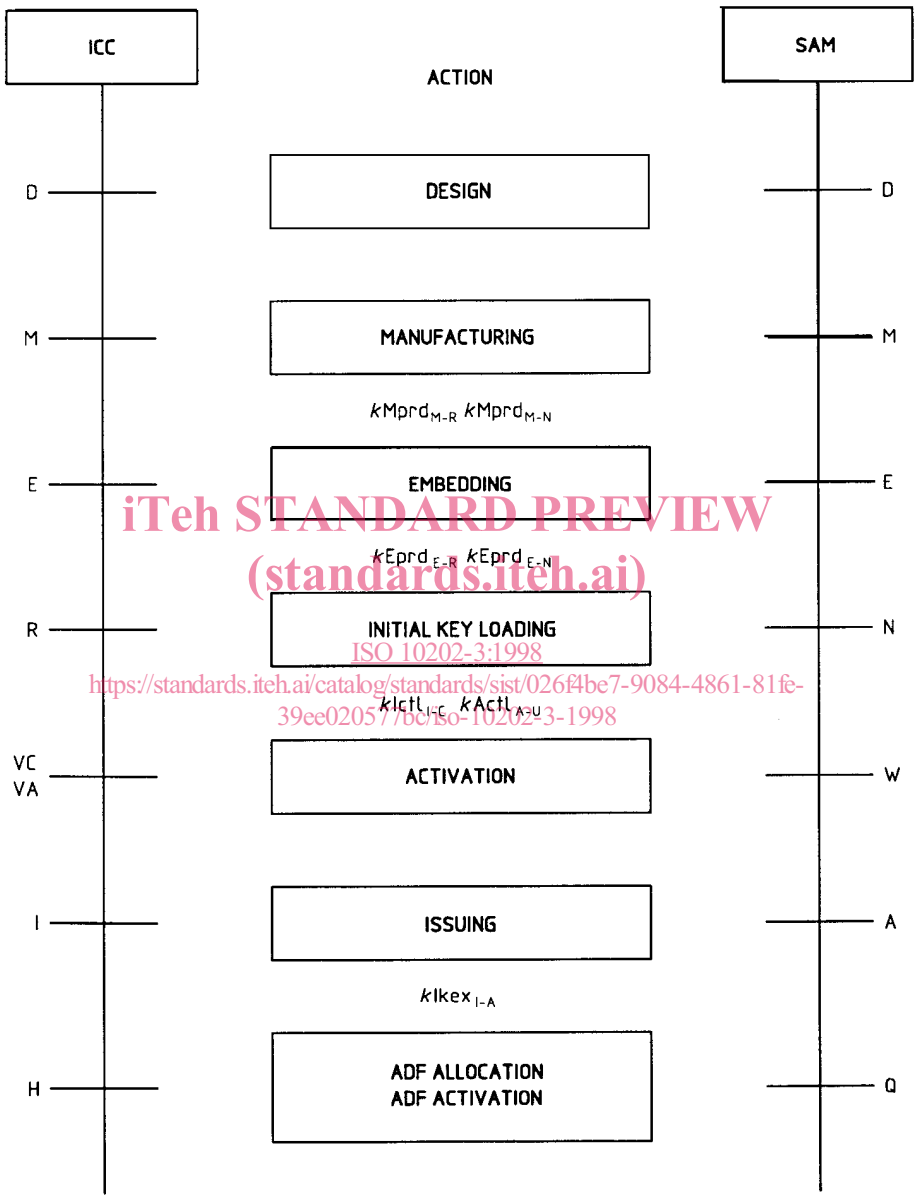

Figure 1 - Stages of the ICC or SAM preparation and keys used during that process.

In the ICC and SAM Life Cycle the issuer and application supplier are responsible for verifying the authenticity of the ICC and SAM respectively before initial key loading.

The ICC personaliser and SAM initialiser act as agents on behalf of the issuer and the application supplier and shall ensure that the IC manufacturer and SAM manufacturer have no control over or responsibility for the ICC and SAM at the stage "initial key loading". This can be accomplished by making the *k*Mprd a temporary key not related to the key hierarchy of the ICC (figure 3) and SAM (figure 4) after personalisation/initialisation.

The embedding does not necessarily have to be executed by a separate intity. This could also be done by the manufacturer or personaliser/SAM initialiser.

6.2 DURING THE TRANSACTION PROCESS

The key relationships that may be established for the transaction process are provided in figure 2.

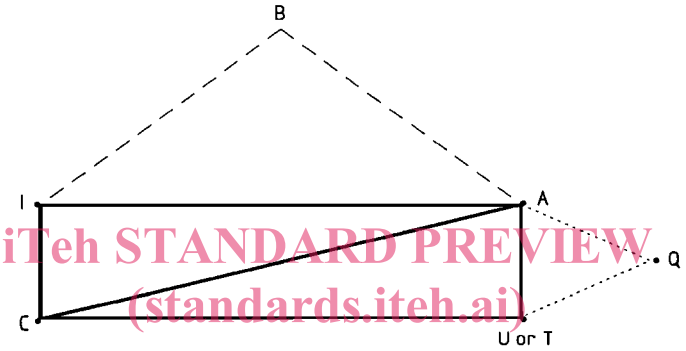

Figure 2 - Transaction relationships

Description of the relationships in figure 2

The T relationship is only for an asymmetric algorithm where the CAD does not have a SAM.

The key relationship C-T is established between the ICC and the CAD for off-line cryptographic functions. It is the same as the key relationship C-A but the application supplier public keys are located in the CAD.
The key relationship I-C is used for CDf transactions between the ICC and the card issuer.

The key relationship C-A is used for on-line transactions between the ICC (acting for the cardholder) and the application supplier. Multiple key relationships C-A may be established by an application supplier for different functions such as debit, credit or electronic purse and are outside the scope of this standard.