INTERNATIONAL STANDARD

ISO 10202-7

First edition
1998-07-15

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

Part 7:
Key management

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

Partie 7: Gestion de clé

Contents

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch

Printed in Switzerland

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 10202-7 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, SC 6, *Retail financial services*.

ISO 10202 consists of the following parts, under the general title *Financial transaction cards — Security architecture* :

— *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 E of this part of ISO 10202 are for information only.

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

Part 7:
Key management

1 Scope

This part of ISO 10202 specifies key management requirements for financial transaction systems using integrated circuit cards. It defines procedures and processes for the secure management of cryptographic keys used during the card life cycle and transaction processing in an integrated circuit card environment. Both symmetric and asymmetric key management schemes are addressed. Minimum key management requirements are specified.

Key management is the process whereby cryptographic keys are provided for use between authorized communicating parties and those keys continue to be subject to secure procedures until they are destroyed. The security of the enciphered data is dependent upon the prevention of disclosure and unauthorized modification, substitution, insertion, or deletion of keys. Thus, key management is concerned with the generation, storage, distribution, use and destruction procedures for keys. Also, by the formalization of such procedures, provision is made for audit trails to be established.

This part of ISO 10202 is applicable between the ICC and the SAM in both on-line and off-line transaction processing environments, and between the ICC and the SAM or host security module in an on-line (end-to-end) environment.

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 7812 (all parts), *Identification cards — Identification of issuers*.

ISO 7816-3, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols*.

ISO 7816-4, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange*.

ISO 7816-5, *Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers*.

ISO 8732, *Banking — Key management (wholesale)*.

ISO 8908, *Banking and related financial services — Vocabulary and data elements*.

ISO 9796, *Information technology — Security techniques — Digital signature schemes giving message recovery*.

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

ISO 9992-2, *Financial transaction cards — Messages between the Integrated Circuit Card and the Card Accepting Device — Part 2: 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 — Part 1: Card life cycle.*

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

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

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

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

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

ISO 10202-8, *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 8: General principles and overview*.

ISO 11568 (all parts), *Banking — Key management (retail)*.

ISO 13491 (all parts), *Banking — Secure cryptographic devices (retail)*.

3 Definitions and abbreviations

3.1 Definitions

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

3.1.1
application data file
a file that supports one or more services

3.1.2
asymmetric algorithm
an algorithm for which the encipherment and decipherment keys are different and where it is computationally infeasible to deduce one from the other

3.1.3
authentication
a process used to ensure data integrity and data origin authentication

3.1.4
certificate
(See transaction certification code and public key certificate.)

3.1.5
certificate identifier
certificate information which enables proper verification of a key certificate

3.1.6
certification authority
an authority trusted by all users to create and assign certificates

3.1.7
common data file
a mandatory file which contains the common data elements used to describe the card, the card issuer and the cardholder

3.1.8
cryptographic function
a process performed (e.g. encryption, authentication, certification) using a cryptographic algorithm

3.1.9
cryptographic key (key)
a parameter used in conjunction with a cryptographic algorithm for executing cryptographic transformations

3.1.10
cryptoperiod
a defined period of time within which a cryptographic key is authorized for use, or during which time the cryptographic keys for a given system may remain in effect

3.1.11
data key
a cryptographic key used for the encipherment, decipherment or authentication of data

3.1.12
decipherment
the process of transforming ciphertext into plaintext

3.1.13
derivation key
a key used to generate a derived key

3.1.14
derived key
a symmetric key generated from a derivation key and non-secret variable data

NOTE The derivation key is used to generate a large number of keys (derived keys).

3.1.15
diversified key
(See derived key.)

3.1.16
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 material (e.g. cryptographic key)

3.1.17
elementary file
a file which may contain data and/or file control information

3.1.18
explicit key identifier
(See key identifier.)

3.1.19
encipherment
the process of transforming plaintext into ciphertext

3.1.20
host/SAM derivation key
a derivation key used to derive ICC or SAM keys

3.1.21
host security module
a physically secure device used to support cryptographic functions and perform SAM functionality on a host system

3.1.22
ICC derivation key
an ICC (CDF or ADF) derivation key used to derive unique message data keys

3.1.23
key enciphering key
a key used to encipher another key

3.1.24
key generation module
a type of cryptographic equipment used for generating and deriving cryptographic keys

3.1.25
key identifier
specifies basic security requirements for the ICC

3.1.26
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

3.1.27
key synchronization
the process whereby two nodes verify that they are communicating with each other using an identical key

3.1.28
keying material
the data necessary to establish and maintain a keying relationship

3.1.29
master derivation key
a derivation key used by a bank card company or another organization to derive unique issuer or application supplier keys

3.1.30
physically secure device
(See ISO 13491.)

3.1.31
physically secure environment
(See ISO 11568.)

3.1.32
public key
that part of an asymmetric key set which is known to other parties than the generator of the key set

3.1.33
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

3.1.34
secure cryptographic device
a device that provides secure storage for secret information such as keys and provides security services based on this secret information

3.1.35
secure application module
a physical module (or 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 unauthorized access is not possible

NOTE In order to achieve this the module shall be physically and logically protected.

3.1.36
symmetric algorithm
a cryptographic method using the same secret cryptographic key for encipherment and decipherment

3.1.37
tamper resistance
provision of physical protection for sensitive data, for the purpose of preventing successful attacks

3.1.38
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)

3.2 Abbreviations

ADF Application data file

CAD Card accepting device

CDF Common data file

CID Certificate identifier

e(..) Encipherment

EF Elementary file

IC Integrated circuit

ICC Integrated circuit card

KCD ICC (CDF or ADF) derivation key

KD Data key

Kx x is either I or A

KEK Key enciphering key

KHD Host or SAM derivation key

KID Key identifier

KMD Master derivation key

KSN Key sequence number

KVC Key verification code

S(..) Sign

SAM Secure application module

4 General security principles

Key management in financial transaction systems using integrated circuit cards shall conform to the following basic principles.

a) The key management adopted for one ICC system, which may include SAMs, shall not compromise the security of any other such system.

b) The key management adopted for one application in one ADF shall not compromise the security of any other application in any other ADF.

c) The ICC and SAM shall afford tamper resistance based on the principles described in ISO 10202-2 and ISO 10202-4.

d) The keying relationship shall be in accordance with ISO 10202-3.

e) The use of cryptographic algorithms to perform cryptographic functions shall be in accordance with ISO 10202-5.

f) Controls and audits shall be in force for key management of ICC, SAM, key generation and loading modules, host security modules, and other cryptographic devices used in financial transaction systems using integrated circuit cards.

Annex A (informative) provides an example of card life cycle key management.

Annexes B and C (informative) provide examples of symmetric key management techniques for transaction processing.

Annexes D and E (informative) provide examples of asymmetric key management.

5 ICC systems key management requirements

5.1 ICC and SAM life cycle

During the life cycle of the ICC and SAM, manual and automated key management processes shall provide the ability to load, update and disable cryptographic keys under the control of the party performing these key management functions. The key management processes used shall meet the cryptographic key relationship requirements defined in ISO 10202-3.

Protection of secret cryptographic keys of symmetric and asymmetric key management schemes shall be provided during all steps of the ICC and SAM life cycle when cryptographic keys are used. The manual procedures and automated processes used to protect cryptographic keys during the card life cycle shall meet the protection requirements defined in this part of ISO 10202.