NORME INTERNATIONALE

ISO 10202-7

Première édition
1998-07-15

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

Partie 7: Gestion de clé

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

Part 7: Key management

Numéro de référence
ISO 10202-7:1998(F)

Sommaire

Page

Organisation internationale de normalisation
Case postale 56 • CH-1211 Genève 20 • Suisse
Internet iso@ iso.ch

Version française tirée en 1999

Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 10202-7 a été élaborée par le comité technique ISO/TC 68, *Banque, valeurs mobilières et autres services financiers*, sous comité SC 6, *Services financiers liés à la clientèle*.

L'ISO 10202 comprend les parties suivantes, présentées sous le titre général *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*

— *Partie 2: Processus de transaction*

— *Partie 3: Relations avec les clés cryptographiques*

— *Partie 4: Modules applicatifs de sécurité*

— *Partie 5: Emploi des algorithmes*

— *Partie 6: Vérification du porteur de carte*

— *Partie 7: Gestion de clé*

— *Partie 8: Principes généraux et vue d'ensemble*

Les annexes A à E de la présente partie de l'ISO 10202 sont données uniquement à titre d'information.

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

Partie 7:
Gestion de clé

1 Domaine d'application

La présente partie de l'ISO 10202 spécifie les exigences de gestion de clé requises pour les systèmes de transactions financières utilisant des cartes à circuit intégré. Elle définit les procédures et processus de gestion sécurisés des clés cryptographiques utilisées pendant le cycle de vie de la carte, ainsi que le traitement des transactions dans un environnement de carte à circuit intégré. Les schémas de gestion de clés symétriques et asymétriques sont abordés. Des exigences de gestion minimale des clés sont spécifiées.

La gestion des clés est le procédé par lequel des clés cryptographiques sont fournies en vue de leur utilisation par des entités accréditées communiquant entre elles, et par lequel des clés cryptographiques sont soumises à des procédures de sécurité jusqu'à ce qu'elles soient détruites. La sécurité des données chiffrées consiste à éviter toute divulgation ainsi que toute modification, substitution, insertion ou suppression illicite de clés. Ainsi, la gestion des clés est en relation avec les procédures de génération, de stockage, de distribution, d'utilisation et de destruction des clés. De même, la formalisation de ces procédures permet la mise en œuvre de mécanismes de traçabilité.

La présente partie de l'ISO 10202 s'applique entre l'ICC et le SAM, tant dans des environnements de traitement des transactions en ligne ou hors ligne, ainsi qu'entre l'ICC et le SAM ou le module de sécurité d'un ordinateur distant dans un environnement en ligne (de bout-en-bout).

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui par suite de la référence qui en est faite, constituent des dispositions valables pour la présente partie de l'ISO 10202. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente partie de l'ISO 10202 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO 7812 (toutes les parties), *Cartes d'identification — Identification des émetteurs.*

ISO 7816-3, *Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts – Partie 3: Signaux électroniques et protocoles de transmission.*

ISO 7816-4, *Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 4: Commandes intersectorielles pour les échanges.*

ISO 7816-5, *Cartes à circuit(s) intégré(s) à contacts — Partie 5: Système de numérotation et procédure d'enregistrement d'identificateurs d'applications.*

ISO 8732, *Banque — Gestion de clés (services aux entreprises).*

ISO 8908, *Banque et services financiers connexes — Vocabulaire et éléments de données.*

ISO 9796, *Technologies de l'information — Techniques de sécurité — Schéma de signature numérique rétablissant le message.*

ISO 9992-1, *Cartes de transactions financières — Messages entre la carte à circuit intégré et le dispositif d'acceptation des cartes — Partie 1: Concepts et structures.*

ISO 9992-2, *Cartes de transactions financières — Messages entre la carte à circuit intégré et le dispositif d'acceptation des cartes — Partie 2: Fonctions, messages (commandes et réponses), éléments de données et structures.*

ISO 10202-1, *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré — Partie 1: Concepts et structures.*

ISO 10202-2, *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré — Partie 2: Processus de transaction.*

ISO 10202-3, *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.*

ISO 10202-4, *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré — Partie 4: Modules applicatifs de sécurité.*

ISO 10202-5, *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré — Partie 5: Utilisation des algorithmes.*

ISO 10202-6, *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.*

ISO 10202-8, *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*

ISO 11568 (toutes les parties), *Banque — Gestion de clés (services aux particuliers).*

ISO 13491 (toutes les parties), *Banque — Dispositifs cryptographiques de sécurité (service aux particuliers).*

3 Définitions et termes abrégés

3.1 Définitions

Pour les besoins de la présente partie de l'ISO 10202, les définitions suivantes s'appliquent.

3.1.1
fichier de données d'application
fichier supportant un ou plusieurs services

3.1.2
algorithme asymétrique
algorithme dont les clés de chiffrement et de déchiffrement sont différentes, et qu'aucun calcul ne permet de déduire l'une de l'autre

3.1.3
authentification
processus utilisé pour assurer l'intégrité des données et l'authentification de leur origine

3.1.4
certificat
(voir code de certification de transaction et certificat de clé publique.)

3.1.5
identificateur de certificat
information de certificat permettant de vérifier le certificat d'une clé

3.1.6
autorité de certification
entité habilitée par tous les utilisateurs à créer et à attribuer des certificats

3.1.7
fichier de données communes (CDF)
fichier obligatoire contenant les éléments de données communes à plusieurs applications. Ces données sont utilisées pour identifier la carte, ainsi que le porteur et l'émetteur de la carte

3.1.8
fonction cryptographique
processus (tel que le chiffrement, l'authentification ou la certification) assuré par un algorithme cryptographique

3.1.9
clé de cryptographique (clé)
paramètre utilisé conjointement avec un algorithme cryptographique pour l'exécution de conversions cryptographiques

3.1.10
période de validité
période de temps durant laquelle l'utilisation d'une clé cryptographique est autorisée, ou de maintien en vigueur des clés de chiffrement d'un système donné

3.1.11
clé de données
clé de chiffrement utilisée pour le chiffrement, le déchiffrement ou l'authentification des données

3.1.12
déchiffrement
processus visant à convertir un texte chiffré en un texte en clair

3.1.13
clé de dérivation
clé utilisée pour générer une clé dérivée

3.1.14
clé dérivée
clé symétrique générée à partir d'une clé de dérivation et de données variables non secrètes

NOTE La clé de dérivation permet de générer un grand nombre de clés (clés dérivées).

3.1.15
clé diversifiée
(voir clé dérivée.)

3.1.16
contrôle partagé
processus faisant appel à deux entités distinctes ou plus (généralement des personnes), intervenant de concert, pour protéger des fonctions ou informations sensibles. Aucune entité ne peut accéder seule à des éléments (tels que des clés cryptographiques) ou les utiliser

3.1.17
fichier élémentaire
fichier pouvant contenir des données et/ou des informations de contrôle

3.1.18
identificateur explicite de clé
(voir identificateur de clé.)

3.1.19
chiffrement
processus visant à convertir un texte en clair en un texte chiffré

3.1.20
clé de dérivation SAM/ordinateur distant
clé de dérivation permettant de dériver des clés d'ICC ou de SAM

3.1.21
module de sécurité d'ordinateur distant
dispositif physiquement sécurisé assurant des fonctions cryptographiques et exécutant les fonctionnalités d'un SAM sur un système central

3.1.22
clé de dérivation ICC
clé de dérivation de carte à circuit intégré (CDF ou ADF) utilisée pour obtenir des clés de données de message uniques

3.1.23
clé de chiffrement de clé
clé utilisée pour chiffrer une autre clé

3.1.24
module de génération de clés
équipement cryptographique permettant de générer et de dériver des clés cryptographiques

3.1.25
identificateur de clé
information spécifiant les exigences de sécurité de base de l'ICC

3.1.26
module de chargement de clé
module électronique autonome permettant d'enregistrer au moins une clé cryptographique et de la transférer, à la demande, vers un dispositif cryptographique tel qu'une ICC ou un SAM

3.1.27
synchronisation de clés
processus par lequel deux nœuds vérifient qu'ils utilisent une clé identique pour communiquer entre eux

3.1.28
éléments de mise à la clé
données nécessaires à l'établissement et au maintien d'une relation basée sur des clés

3.1.29
clé de dérivation maîtresse
clé de dérivation utilisée par un institut bancaire ou tout autre organisme pour dériver des clés uniques d'émetteur ou de fournisseur d'application

3.1.30
dispositif physiquement sécurisé
(voir l'ISO 13491.)

3.1.31
environnement physiquement sécurisé
(voir l'ISO 11568.)

3.1.32
clé publique
la partie d'un ensemble de clés asymétriques, connue par d'autres entités que l'entité ayant généré l'ensemble de clés en question

3.1.33
certificat de clé publique
ensemble constitué des habilitations d'utilisateur (incluant la clé publique) portant la signature numérique de la partie tierce accréditée

3.1.34
dispositif cryptographique sécurisé
dispositif assurant le stockage sécurisé d'informations secrètes, telles que les clés, et offrant des services de sécurité reposant sur ces informations secrètes

3.1.35
module applicatif de sécurité (SAM)
module physique (ou fonction logique du CAD) destiné à contenir un ou plusieurs algorithmes, des clés associées, ainsi que des procédures et informations relatives à la sécurité pour protéger une application en rendant impossible tout accès illicite

NOTE Pour cela, le module doit être protégé d'un point de vue physique et logique.

3.1.36
algorithme symétrique
méthode cryptographique utilisant la même clé de chiffrement secrète pour le chiffrement et le déchiffrement

3.1.37
résistance à l'altération
protection physique de données sensibles contre des attaques éventuelles

3.1.38
code de certification de transaction
résultat d'un processus de certification générant une signature électronique qui peut être un code d'authentification de message (MAC) basé sur un algorithme symétrique, ou une signature numérique basée sur un algorithme asymétrique

3.2 Termes abrégés

ADF Fichier de données d'application

CAD Dispositif d'acceptation de carte

CDF	Fichier de données communes
CID	Identificateur de certificat
e(..)	Chiffrement
EF	Fichier élémentaire
IC	Circuit intégré
ICC	Carte à circuit intégré
KCD	Clé de dérivation ICC (CDF ou ADF)
KD	Clé de données
Kx	x prend les valeurs I ou A
KEK	Clé de chiffrement de clé
KHD	Clé de dérivation SAM/ordinateur distant
KID	Identificateur de clé
KMD	Clé de dérivation maîtresse
KSN	Numéro de séquence de clé
KVC	Code de vérification de clé
S(..)	Signe
SAM	Module applicatif de sécurité

4 Principes généraux de sécurité

La gestion des clés dans les systèmes de transactions financières utilisant des cartes à circuit intégré doit être conforme aux principes de base suivants:

a) la gestion des clés adoptée pour un système ICC, pouvant inclure des SAM, ne doit pas compromettre la sécurité d'autres systèmes similaires;

b) la gestion des clés adoptée pour une application d'un ADF ne doit pas compromettre la sécurité d'autres applications d'un autre ADF;

c) l'ICC et le SAM doivent assurer une résistance à l'altération conforme aux principes décrits dans l'ISO 10202-2 et l'ISO 10202-4;

d) la relation basée sur des clés doit être conforme à l'ISO 10202-3;

e) l'emploi d'algorithmes cryptographiques pour effectuer des fonctions cryptographiques doit être conforme à l'ISO 10202-5;

f) des contrôles et audits doivent être instaurés pour la gestion des clés dans les ICC, les SAM, les modules de génération et de chargement de clés, les modules de sécurité d'un ordinateur distant, ainsi que tout autre dispositif cryptographique employé dans les systèmes de transactions financières utilisant des cartes à circuit intégré.

L'annexe A (informative) fournit un exemple de gestion de clé pendant le cycle de vie de la carte.

Les annexes B et C (informatives) fournissent des exemples de techniques de gestion de clés symétriques pour le traitement des transactions.

Les annexes D et E (informatives) fournissent des exemples de gestion de clés asymétriques.