NORME INTERNATIONALE

ISO 10202-8

Première édition
1998-07-15

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

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

Part 8: General principles and overview

Numéro de référence
ISO 10202-8:1998(F)

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 10202-8 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 C de la présente partie de l'ISO 10202 sont données uniquement à titre d'information.

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

Version française tirée en 1999

Imprimé en Suisse

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

1 Domaine d'application

L'ISO 10202 définit l'architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré. La présente partie présente les principes de sécurité généraux ainsi qu'une vue d'ensemble des exigences de sécurité requises pour les systèmes de transactions financières utilisant des cartes à circuit intégré, et introduit les parties 1 à 7 de l'ISO 10202. Elle résume les éléments de données obligatoires et facultatifs utilisés dans l'ISO 10202.

Cette Norme internationale comporte trois annexes: l'annexe A (informative) qui présente de manière succincte la Norme internationale en question, l'annexe B (informative) qui décrit l'architecture logique de l'ICC (carte à circuit intégré), et l'annexe C (informative) présentant l'architecture logique du SAM.

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 3166, *Codes pour la représentation des noms de pays et de leurs subdivisions.*

ISO 4909, *Cartes bancaires — Zone magnétique — Contenu en données de la piste 3.*

ISO 7810, *Cartes d'identification — Caractéristiques physiques.*

ISO 7812, *Cartes d'identification — Système de numération et procédure d'enregistrement pour les identificateurs d'émetteur.*

ISO 7813, *Cartes d'identification — Cartes de transactions financières.*

ISO/CEI 7816-1, *Cartes d'identification — Cartes à circuit(s) intégré(s) à contact — Partie 1: Caractéristiques physiques.*

ISO/CEI 7816-2, *Cartes d'identification — Cartes à circuit(s) intégré(s) à contact — Partie 2: Dimensions et emplacements des contacts.*

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

ISO/CEI 7816-6, *Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 6: Eléments de données intersectoriels.*

ISO 8583, *Messages initiés par carte de transaction financière — Spécifications d'échange de messages.*

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

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

ISO 9564-1, *Banque — Gestion et sécurité du numéro personnel d'identification — Partie 1: Principes et techniques de protection du PIN.*

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

ISO 9807, *Banque et services financiers liés aux opérations bancaires — Spécifications liées à l'authentification des messages (service au particuliers).*

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: Cycle de vie de la carte.*

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 10202-7, *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré — Partie 7: Gestion de clé.*

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

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

3 Termes et définitions

Les définitions suivantes s'appliquent à l'ISO 10202. En ce qui concerne les termes non définis dans cette Norme internationale, consulter l'ISO 8908.

3.1
fichier de données d'application (ADF)
fichier du circuit intégré gérant un ou plusieurs services

3.2
allocation d'ADF
mise à disposition d'un espace sécurisé dans l'IC en vue de son utilisation ultérieure par un fournisseur d'application

3.3
personnaliseur d'ADF
entité assurant le chargement initial des paramètres de sécurité et de fonctionnement associés dans l'espace alloué à un ADF dans l'IC

3.4
fournisseur d'application
entité responsable d'un ADF après son allocation

3.5
algorithme asymétrique
algorithme dont les clés de chiffrement et de déchiffrement sont différentes et ne peuvent être déduites par calcul

3.6
authentification
processus utilisé pour garantir l'intégrité des données et l'authentification de leur origine

3.7
vérification biométrique
mode de vérification du porteur de la carte reposant sur une comparaison entre une caractéristique biologique observée et une valeur de référence

3.8
dispositif d'acceptation de carte (CAD)
dispositif assurant l'interface avec la carte à circuit intégré lors d'une session

3.9
accepteur de carte
entité acceptant la carte en échange de la fourniture de biens et services

3.10
émetteur de carte
organisme financier (ou son agent) fournissant la carte ICC de transactions financières au porteur de la carte

3.11
porteur de la carte
personne à laquelle la carte ICC de transactions financières a été délivrée

3.12
identificateur du titulaire de carte (CIV)
valeur utilisée pour vérifier l'identité du porteur de la carte. Un CIV est communiqué, au porteur de la carte (par exemple un PIN ou un mot de passe). Un CIV biométrique est la représentation d'une caractéristique biologique observée chez le porteur de la carte

3.13
certificat
(voir code de certification de transaction et certificat de clé publique)

3.14
identificateur de certificat
information permettant la vérification correcte d'un certificat de clé

3.15
autorité de certification
entité habilitée par tous les utilisateurs à créer et à attribuer des certificats

3.16
texte chiffré
texte en clair ayant été converti par un procédé cryptographique

3.17
bi-univoque
une fonction est appelée bi-univoque lorsque deux valeurs d'entrée différentes produisent des résultats de sortie différents

3.18
fichier à données communes (CDF)
fichier obligatoire contenant les éléments de données communes à plusieurs applications, utilisé pour identifier la carte, le porteur et l'émetteur de la carte

3.19
compteur
compte incrémenté utilisé entre deux parties

3.20
habilitations
ensemble d'éléments de données affecté à chaque entité afin de les authentifier

3.21
échange cryptographique
méthode de protection des informations échangées entre deux parties

3.22
fonction cryptographique
processus (tel que l'encryptage, l'authentification ou la certification) assuré par un algorithme cryptographique

3.23
clé cryptographique (clé)
paramètre utilisé avec un algorithme cryptographique lors de conversions cryptographiques

3.24
lien cryptographique
lien constitué par deux entités logiques (nœuds) ayant préalablement convenu d'échanger des données, et entretenant une relation basée sur des clés cryptographiques

3.25
nœud cryptographique
l'une des entités logiques (nœuds) d'un lien cryptographique

3.26
période de validité
durée d'utilisation autorisée d'une clé cryptographique, ou de maintien en vigueur des clés cryptographiques d'un système donné

3.27
clé de données
clé cryptographique utilisée pour le chiffrement, le déchiffrement ou l'authentification des données

3.28
déchiffrement
processus visant à convertir du texte chiffré en un texte en clair

3.29
clé de dérivation
clé utilisée pour générer une clé dérivée

3.30
clé dérivée
clé symétrique générée à partir d'une clé de dérivation et de données variables non secrètes. La clé de dérivation permet de générer un grand nombre de clés (dérivées)

3.31
signature numérique
résultat d'une conversion cryptographique effectuée par une entité avec sa clé secrète et un algorithme asymétrique, assurant la non-répudiation de la source et l'intégrité des données signées

3.32
nom distinctif
nom identifiant de manière unique une entité lors d'un processus

3.33
clé diversifiée
(voir clé dérivée)

3.34
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

3.35
fichier élémentaire
fichier pouvant contenir des informations de contrôle de données et/ou de fichiers

3.36
chiffrement
processus visant à convertir un texte en clair en texte chiffré

3.37
authentification d'entité
vérification de l'identité prétendue d'une entité (nœud)

3.38
encarteur
entité assurant l'intégration du circuit intégré

3.39
fonction de hachage
fonction unidirectionnelle qui mappe une entrée de longueur variable sur une sortie de longueur fixe afin qu'il ne soit pas possible d'obtenir, par calcul, un même résultat à partir de deux entrées intelligibles différentes. Cette fonction doit être bi-univoque

3.40
clé de dérivation SAM/d'ordinateur distant
clé de dérivation permettant de dériver des clés d'ICC ou de SAM

3.41
module de sécurité d'ordinateur distant
dispositif physiquement sécurisé assurant des fonctions cryptographiques et l'exploitation des fonctions de SAM sur un système central

3.42
circuit intégré (IC)
composant(s) électronique(s) intégré(s) à une carte à circuit intégré (ICC) sous la forme de micro-circuits pour assurer des fonctions de traitement et de mémoire

3.43
assembleur de circuit intégré
entité chargée de l'assemblage du circuit intégré

3.44
assemblage de circuit intégré
processus visant à combiner un ou plusieurs circuits intégrés avec des éléments permettant une communication externe avec un module adapté à l'encartage de circuits intégrés

3.45
module
module contenant un ou plusieurs circuits intégrés, ainsi que des éléments de communication externe adaptés à l'encartage de circuits intégrés

3.46
encartage d'IC
processus consistant à intégrer un module d'IC dans une carte pour former une carte à circuit intégré (ICC)

3.47
système à circuit intégré seulement
système reposant uniquement sur la technologie des circuits intégrés et les équipements d'interface correspondants

3.48
carte à circuit intégré (ICC)
carte dans laquelle ont été intégrés un ou plusieurs circuits intégrés

3.49
clé de dérivation ICC
clé de dérivation de carte à circuit intégré (CDF ou ADF) utilisée pour dériver des clés de données de message uniques

3.50
initiateur
nœud ou entité à l'origine d'un processus

3.51
clé de chiffrement de clés
clé utilisée pour chiffrer une autre clé

3.52
module de génération de clés
équipement cryptographique permettant de générer et de dériver des clés cryptographiques

3.53
identificateur de clé
informations permettant au destinataire de déterminer la ou les clés appropriées associées à une transaction

3.54
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

3.55
synchronisation de clés
aptitude de deux nœuds à déterminer la clé de données identique

3.56
éléments de calcul de clé
données nécessaires à l'établissement et au maintien d'une relation basée sur des clés

3.57
clé de dérivation principale
clé de dérivation utilisée par un institut bancaire ou tout autre organisme pour dériver des clés d'émetteur ou de fournisseur d'application uniques

3.58
authentification de message
processus apportant la preuve cryptographique qu'un message n'a été ni modifié ni détruit de manière illicite

3.59
code d'identification du message (MAC)
champ de données dont le contenu permet de vérifier l'intégrité d'un message ou des éléments sélectionnés dans un message

3.60
CAD mixte
CAD acceptant les cartes à circuit intégré et les cartes à piste magnétique

3.61
système mixte
système acceptant à la fois la technologie de circuit intégré et celle des pistes magnétiques

3.62
non-répudiation
service de sécurité apportant une preuve cryptographique permanente de l'intégrité et de l'origine des données sous une forme infalsifiable pouvant être, à tout moment, vérifiée par une tierce partie

3.63
fonction irréversible
fonction mathématique convertissant de manière irréversible des valeurs d'entrée en des valeurs de sortie

3.64
mot de passe
CIV alphanumérique discret où chaque caractère est représenté de manière unique

3.65
données en clair
données intelligibles pouvant être lues ou exploitées sans conversion préalable

3.66
clé publique
partie d'un ensemble de clés asymétriques, connue par d'autres entités que l'entité ayant généré l'ensemble en question

3.67
certificat de clé publique
ensemble constitué des habilitations d'utilisateur (incluant la clé publique) portant la signature numérique de la partie tierce accréditée

3.68
numéro personnel d'identification (PIN)
code ou mot de passe utilisé par le porteur de la carte afin de vérifier son identité

3.69
numéro de compte primaire (PAN)
numéro identifiant l'émetteur et le porteur d'une carte. Ce numéro est composé d'un numéro d'identification de l'émetteur, d'une identification de compte individuel, et d'un chiffre de contrôle conformément à l'ISO 7812

3.70
CIV de référence
CIV utilisé pour vérifier le CIV de transaction

3.71
attaque par rejeu
attaque d'un faux répondant durant laquelle l'initiateur est confronté dans une session distincte à la même valeur aléatoire que celle transmise dans une autre session afin d'authentifier le répondant

3.72
répondant
nœud ou entité répondant à l'initiateur d'un processus

3.73
initialiseur de SAM
entité qui charge les paramètres de sécurité et d'exploitation associés dans le SAM

3.74
fournisseur de SAM
entité fournissant un SAM à un accepteur de carte (généralement le fournisseur d'application)

3.75
trace d'audit sécurisée
données et informations d'historique pouvant être examinées pour vérifier l'exactitude et l'intégrité de l'application des procédures de sécurité convenues, et permettant de détecter d'éventuelles défaillances de la sécurité

3.76
module applicatif de sécurité (SAM)
module physique (ou fonctionnalité logique du CAD) destiné à contenir des algorithmes, des clés associées, ainsi que des procédures et informations relatives à la sécurité pour protéger une application en rendant impossible tout accès illicite. Pour cela, le module doit être protégé d'un point de vue physique et logique

3.77
algorithme symétrique
méthode cryptographique utilisant la même clé cryptographique secrète pour le chiffrement et le déchiffrement

3.78
degré d'actualité des données
méthode visant à exclure le rejeu d'un message valide à un moment ultérieur en utilisant un échantillon d'informations pour demander une réponse correcte à une heure précise

3.79
jeton
ensemble d'éléments de données formé pour chaque échange de données entre deux entités

3.80
acquéreur de transactions
institution recevant de l'accepteur de carte, les données relatives à une transaction financière à des fins de règlement

3.81
code de certification de transaction
résultat du processus de certification de conversion 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

3.82
certification de transaction
processus apportant la preuve cryptographique de l'origine et de l'intégrité des données de transaction qui peuvent être vérifiées par un tiers

3.83
identificateur de transaction
CIV fourni par l'utilisateur de la carte lors d'une transaction

3.84
tierce partie de confiance
entité généralement accessible, connue et accréditée par les entités en communication

4 Vue d'ensemble de l'architecture de sécurité des systèmes utilisant des cartes à circuit intégré

Les cartes à circuit intégré (ICC) utilisées dans les systèmes de transactions financières contiennent un circuit intégré (IC) assurant les fonctions de traitement et de mémoire. L'ICC, fournie par un émetteur de carte, supporte une ou plusieurs applications. Ces applications peuvent être indépendantes et appartenir à différentes parties, appelées fournisseurs d'application. L'émetteur de la carte peut être un fournisseur d'applications.

L'ISO 10202 définit les exigences de sécurité minimales, ainsi que les fonctions de sécurité optionnelles des systèmes de transactions financières utilisant des cartes à circuit intégré. Ces exigences de sécurité s'appliquent durant toute la vie de l'ICC, appelée cycle de vie de la carte. Le cycle de vie de la carte s'applique à l'IC et à l'ICC à partir de leur fabrication, et se poursuit pendant toute leur utilisation jusqu'à leur éventuelle résiliation, comme indiqué dans l'ISO 10202-1. L'émetteur de carte est responsable des procédures de sécurité pendant tout le cycle de vie de l'ICC.

L'émetteur de carte peut instaurer des relations commerciales avec des fournisseurs d'application pour ajouter des applications à l'ICC. Les transactions par carte à circuit intégré peuvent être traitées en direct ou en différé, et entraîner la participation d'un accepteur de carte, c'est-à-dire la partie acceptant la carte en échange de la fourniture de biens ou de services. Les exigences de sécurité requises lors du processus de transaction sont décrites dans l'ISO 10202-2. Des accords contractuels sont nécessaires, par exemple, lorsque l'ICC est utilisée