NORME INTERNATIONALE

ISO 10202-6

Première édition
1994-12-15

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

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

Part 6: Cardholder verification

Numéro de référence
ISO 10202-6:1994(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 10202-6 a été élaborée par le comité technique ISO/TC 68, *Banque et services financiers liés aux opérations bancaires*, sous-comité SC 6, *Cartes de transactions financières, supports et opérations relatifs à celles-ci.*

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 de chiffrement*

— *Partie 4: Modules applicatifs de sécurité*

— *Partie 5: Utilisation des algorithmes*

— *Partie 6: Vérification du porteur de carte*

— *Partie 7: Gestion de clé*

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

Organisation internationale de normalisation
Case Postale 56 • CH-1211 Genève 20 • Suisse
Imprimé en Suisse

L'annexe A fait partie intégrante de la présente partie de l'ISO 10202. Les annexes B et C 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 6:
Vérification du porteur de carte

1 Domaine d'application

La présente partie de l'ISO 10202 prescrit les mesures de sécurité associées à la vérification du porteur de carte à circuit intégré (ICC), munie ou non de pistes magnétiques, à l'aide d'un identificateur de titulaire de carte (CIV) discret, tel qu'un numéro personnel d'identification (PIN). L'objectif de la vérification du porteur de carte est de déterminer que le porteur de la carte en est bien le titulaire. L'ISO 9564-1 est applicable, sauf en ce qui concerne les articles de la présente partie de l'ISO 10202 portant sur les particularités de l'utilisation d'une carte à circuit intégré.

Les dispositions de la présente partie de l'ISO 10202 ne constituent en rien une protection contre l'utilisation de dispositifs d'acceptation de carte (CAD) frauduleux.

La présente partie de l'ISO 10202 est applicable à toute organisation responsable de la mise en œuvre de procédures de sécurité pour l'utilisation d'identificateurs de titulaire de carte avec les cartes à circuit intégré.

Elle traite de la sécurité entourant la mise en relation d'un objet que le titulaire possède — sa carte à circuit intégré — avec une information qu'il détient, c'est-à-dire un CIV, tel qu'un numéro personnel d'identification. Elle porte également sur les principales mesures de sécurité associées aux cartes à circuit intégré et aux dispositifs d'acceptation de carte. Ces cartes et ces dispositifs peuvent faire appel soit uniquement à la technologie des circuits intégrés, soit à la fois à la technologie des circuits intégrés et à celle des pistes magnétiques. Seuls les systèmes à circuit intégré sont ici traités.

NOTE 1 L'expression circuit intégré sous-entend un circuit intégré encarté sur une carte à circuit intégré.

La vérification du porteur de carte peut se faire soit au niveau du fichier de données communes (CDF), soit au niveau du fichier de données d'application (ADF).

NOTE 2 Les termes émetteur de la carte et prestataire s'étendent aux agents agréés par l'un ou par l'autre.

2 Références normatives

Les normes suivantes 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. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente partie de l'ISO 10202 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO 9564-1:1991, *Banque — Gestion et sécurité du numéro personnel d'identification — Partie 1: Principes et techniques de protection du PIN.*

ISO 10202-2:—[1], *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré — Partie 2: Processus de transaction.*

ISO 10202-5:—[1], *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré — Partie 5: Utilisation des algorithmes.*

3 Définitions

Pour les besoins de la présente partie de l'ISO 10202, les définitions données dans l'ISO 10202-1 et les définitions suivantes s'appliquent.

3.1 vérification biométrique: Texte de vérification du porteur de carte obtenu par comparaison d'une caractéristique biologique observée à une valeur de référence.

3.2 titulaire de carte: Client auquel est associé le numéro de compte primaire (PAN) et qui demande la transaction auprès de l'accepteur de carte.

3.3 identificateur du titulaire de carte (CIV): Valeur servant à vérifier l'identité du porteur de carte.

NOTE 3 L'identificateur discret n'est connu que du titulaire (PIN ou mot de passe, par exemple). L'identificateur biométrique est la représentation d'une caractéristique biologique du titulaire.

3.4 système à circuit intégré seulement: Système de carte ne reposant que sur la technologie des circuits intégrés et sur l'équipement d'interface correspondant.

3.5 CAD mixte: Dispositif d'acceptation de carte pouvant lire à la fois les cartes à circuit intégré et les cartes à piste magnétique.

3.6 système mixte: Système alliant la technologie des circuits intégrés à celle des pistes magnétiques.

3.7 mot de passe: Identificateur secret alphanumérique dont chaque caractère est représenté de façon unique.

3.8 identificateur de référence: Identificateur utilisé pour vérifier l'identificateur de transaction.

3.9 identificateur de transaction: Identificateur fourni par le porteur de la carte au moment de la transaction.

1) À publier.

4 Vérification par valeurs discrètes

Le présent article définit les prescriptions minimales de sécurité associées à l'utilisation d'un identificateur discret avec une carte à circuit intégré. Ces identificateurs discrets peuvent être des numéros discrets personnels d'identification, décrit dans l'ISO 9564-1, ou des mots de passe (voir annexe B).

4.1 Principes généraux de sécurité

Les procédures de sécurité indiquées dans la présente partie de l'ISO 10202 doivent s'appuyer sur les principes suivants.

a) Les principes fondamentaux de gestion des numéros personnels d'identification prescrits dans l'ISO 9564-1.

b) Les prescriptions de vérification du porteur de carte doivent être fixées par l'émetteur de la carte lorsque la vérification a lieu au niveau du fichier de données communes (CDF), et par le prestataire lorsque la vérification a lieu au niveau du fichier de données d'application (ADF).

c) L'enregistrement d'un identificateur discret de référence dans le circuit intégré doit se faire d'une manière sécurisée et contrôlée.

d) La mémorisation d'un identificateur discret de référence dans le circuit intégré doit se faire de manière à en empêcher la lecture externe.

e) Lorsque la vérification a lieu au niveau du CDF, les procédures d'enregistrement, de réenregistrement et de modification de l'identificateur secret de référence doivent être réalisées sous le contrôle de l'émetteur de la carte.

f) Le processus de vérification de l'identificateur au niveau du CDF doit être disponible à partir de toute application de la carte.

g) Lorsque la vérification a lieu au niveau de l'ADF, les procédures d'enregistrement, de réenregistrement et de modification de l'identificateur secret de référence doivent être réalisées sous le contrôle du prestataire.

h) Le processus de vérification du porteur de carte dans un système de carte à circuit intégré doit se faire de manière à ne pas compromettre ce sys-

tème ou tout autre système de carte à circuit intégré ou à piste magnétique.

i) Le processus de vérification du porteur de carte dans un système de carte à circuit intégré doit se faire de telle sorte que la compromission d'un circuit intégré n'entraîne pas la compromission d'un autre circuit intégré.

j) Le processus de vérification de l'identificateur discret doit se faire dans le circuit intégré.

k) En cas de vérification d'un identificateur discret de transaction, le circuit intégré doit empêcher une recherche exhaustive de l'identificateur de référence.

4.2 Numéro personnel d'identification (PIN)

L'utilisation d'un PIN dans un système faisant appel à la technologie des cartes à circuit intégré est régie par l'ISO 9564-1 et assujettie aux dispositions indiquées dans la présente partie de l'ISO 10202.

4.2.1 Enregistrement et réenregistrement du PIN

L'enregistrement d'un PIN de référence initial dans un circuit intégré ou le réenregistrement d'un PIN de référence (si, par exemple, le titulaire l'oublie) doit se faire dans un environnement physiquement sûr ou avec une protection cryptographique utilisant les clés de chiffrement adéquates qui seront indiquées dans une future partie de l'ISO 10202.

4.2.2 Modification du PIN

Le titulaire de la carte peut modifier lui-même le PIN de référence au niveau du CDF ou de l'ADF, mais il doit le faire selon une procédure déterminée respectivement par l'émetteur de carte ou le prestataire, la procédure comprenant la vérification du PIN actuel.

4.2.3 Mémorisation du PIN

Un PIN de référence mémorisé dans un circuit intégré doit être protégé contre la lecture externe. Un PIN de référence peut être mémorisé en clair si la carte à circuit intégré répond aux conditions suivantes.

a) La recherche non autorisée d'un PIN de référence mémorisé dans un circuit intégré doit endommager ce dernier de façon à rendre impossible sa remise en service. De plus, les procédures de détermination du PIN de référence d'un circuit intégré doivent nécessiter des instruments et qualifications spécialisés qui ne sont pas facilement accessibles.

b) La violation du contenu d'une carte à circuit intégré ne doit pas permettre de déduire le PIN de référence de toute autre carte.

Dans un système à circuit intégré seul, la vérification du PIN a lieu dans le circuit intégré. En outre, l'émetteur de carte ou le prestataire ne doit pas conserver ni pouvoir reproduire le PIN de référence; il convient que ce dernier ne soit mémorisé que dans le circuit intégré.

4.2.4 Transmission du PIN

Le PIN de transaction associé à une carte à circuit intégré doit être transmis à ce circuit. Le PIN de référence, lui, ne doit jamais sortir du circuit intégré.

Dans le cas d'un CAD mixte, le PIN de transaction doit être envoyé du clavier d'entrée avec une protection cryptographique, mais si la connexion entre le clavier et le lecteur du circuit intégré est physiquement sûre, le PIN peut être reçu en clair par le circuit intégré. (Voir l'ISO 10202-5 pour plus de détails sur la protection cryptographique.)

NOTE 4 La meilleure solution est l'intégration physique du clavier d'entrée du PIN et du lecteur de carte à circuit intégré.

Dans le cas d'un système à circuit intégré seul, lorsque la carte ne comporte pas de piste magnétique pouvant être utilisée conjointement avec le même PIN, la transmission cryptographique du PIN entre le clavier et le lecteur n'est pas obligatoire.

4.2.5 Vérification du PIN

Le PIN de transaction doit être comparé au PIN de référence dans le circuit intégré. La réponse du circuit intégré à cette vérification ne doit pas nécessairement être transmise avec une protection cryptographique. (Voir l'ISO 10202-2.)

La carte à circuit intégré doit empêcher une recherche exhaustive d'un PIN de référence en limitant le nombre consécutif de tentatives non réussies pouvant être traitées. Ce nombre, s'appliquant à la vérification du PIN au niveau du CDF ou de l'ADF, de même que les mesures subséquentes, est déterminé par l'émetteur de carte ou par le prestataire, selon le cas.

Le circuit intégré ne doit fournir aucune information sur le résultat de la vérification du porteur de carte avant d'avoir enregistré ce résultat ou d'avoir garanti son enregistrement.

Annexe A
(normative)

Présentation du CIV

Un CIV, lorsqu'il est constitué par une suite de 4 à 12 chiffres présentée en clair, doit pouvoir être présenté à la carte à circuit intégré selon le format du bloc PIN défini dans l'ISO 9564-1:1991, paragraphe 8.3.1.1 (Zone du PIN en clair), et la zone de contrôle C doit être 2 (c'est-à-dire 0010).

Annexe B
(informative)

Mot de passe et méthodes biométriques

B.1 Mot de passe

Il est possible d'utiliser un mot de passe, comptant généralement entre 6 et 12 caractères, avec une carte à circuit intégré. Si l'utilisation de mots de passe avec une carte à circuit intégré dans les échanges internationaux s'avère réalisable, son inclusion dans la présente partie de l'ISO 10202 sera envisagée.

B.2 Méthodes biométriques

Les cartes à circuit intégré permettent l'utilisation de méthodes biométriques. Si un comité membre de l'ISO propose une méthode biométrique de vérification du porteur d'une carte pouvant être utilisée dans les échanges internationaux, l'inclusion de cette méthode dans la présente partie de l'ISO 10202 sera envisagée.