NORME INTERNATIONALE

ISO 10202-4

Première édition
1996-02-01

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

Partie 4: Modules applicatifs de sécurité

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

Part 4: Secure application modules

Numéro de référence
ISO 10202-4:1996(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 10202-4 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 entre les clés cryptographiques (DIS distribué en version anglaise seulement)*

— *Partie 4: Modules applicatifs de sécurité*

— *Partie 5: Utilisation des algorithmes*

— *Partie 6: Vérification du porteur de carte*

— *Partie 7: Gestion des clés*

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

— *Partie 8: Principes généraux et vue d'ensemble (DIS distribué en version anglaise seulement)*

L'annexe A fait partie intégrante de la présente partie de l'ISO 10202. L'annexe B est donnée uniquement à titre d'information.

Page blanche

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

Partie 4:
Modules applicatifs de sécurité

1 Domaine d'application

La présente partie de l'ISO 10202 prescrit les mesures de sécurité minimales relatives au cycle de vie d'un module applicatif de sécurité (SAM) qui peut être ajouté à un dispositif d'acceptation de carte (CAD). Un SAM fournit des informations liées à la cryptographie de sécurité et associées à une application pour le traitement d'une transaction financière. Chaque fournisseur d'application peut avoir un SAM. Les émetteurs de cartes et/ou les fournisseurs d'application peuvent s'entendre pour utiliser un seul SAM pour leurs applications. La présente partie de l'ISO 10202 est applicable à tout organisme intervenant dans l'émission de SAM pour une utilisation dans les CAD. Un SAM peut prendre en charge un seul CAD ou une grappe de CAD interconnectés.

La présente partie de l'ISO 10202 permet qu'une interaction entre une carte à circuit intégré (ICC) et un SAM soit fonctionnellement transparente pour un dispositif d'acceptation de carte (CAD). Cela autorise l'utilisation de différentes techniques et niveaux de structure de commandes ainsi que de formats de messages.

Une description de l'audit de sécurité et des champs de données associées à la sécurité, mémorisés par un SAM, est donnée dans l'annexe A. Des mises en œuvre suggérées de fonctions de SAM sont données dans l'annexe B.

Un SAM peut être utilisé pour assurer, lors d'une transaction, une relation sécurisée entre l'ICC, le fournisseur d'application, l'acquéreur et le CAD. Cela pourrait inclure l'authentification du SAM par le fournisseur du SAM. Un CAD peut contenir un ou plusieurs SAM.

La relation qui existe entre le SAM et le système hôte du fournisseur de SAM sortent du cadre de la présente partie de l'ISO 10202.

NOTE 1 Dans la présente partie de l'ISO 10202, toute référence au fournisseur du SAM, à l'émetteur de la carte, au fournisseur d'application ou à l'acquéreur inclut aussi leurs agents.

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/CEI 7812-1:1993, *Cartes d'identification — Identification des émetteurs — Partie 1: Système de numérotation.*

ISO/CEI 7812-2:1993, *Cartes d'identification — Identification des émetteurs — Partie 2: Procédures de demande d'enregistrement.*

ISO 7816-1:1987, *Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 1: Caractéristiques physiques.*

ISO 7816-2:1988, *Cartes d'identification — Carte à circuit(s) intégrés à contacts — Partie 2: Dimensions et emplacements des contacts.*

ISO/CEI 7816-3:1989, *Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 3: Signaux électroniques et protocoles de transmission.*

ISO/CEI 7816-4:1995, *Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 4: Commandes intersectorielles pour les échanges.*

ISO/CEI 7816-5:1994, *Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 5: Système de numérotation et procédure d'enregistrement d'identificateurs d'applications.*

ISO 10202-1:1991, *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:—[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 10202-3:—[1], *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré — Partie 3: Relations entre les clés cryptographiques (DIS distribué en version anglaise seulement).*

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.*

ISO 10202-7:—[1], *Cartes de transactions financières — Architecture de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré — Partie 7: Gestion des clés.*

3 Définitions

Pour les besoins de la présente partie de l'ISO 10202, les définitions données dans les parties précédentes de l'ISO 10202 ainsi que les définitions suivantes s'appliquent.

1) À publier.

3.1 module applicatif de sécurité (SAM): Module destiné à contenir le ou les algorithmes, les clés associées, les informations et les procédures de sécurité nécessaires pour protéger une application de manière à rendre impossible tout accès illicite. Pour ce faire, le module doit faire l'objet d'une protection physique, électrique et logique.

3.2 initialiseur de SAM: Entité qui charge dans le SAM ses paramètres de sécurité et de fonctionnement.

3.3 fournisseur de SAM: Entité qui fournit un SAM à un accepteur de carte (habituellement le fournisseur d'application).

4 Principes généraux de sécurité

Les règles de sécurité fournies dans la présente partie de l'ISO 10202 s'appuient sur les principes suivants.

a) Aucune opération effectuée par un SAM ou aucune donnée qu'on peut en obtenir ne doit compromettre la sécurité d'aucun autre système ou combinaison de systèmes utilisant des SAM.

b) Le fournisseur du SAM est responsable du cycle de vie du SAM.

c) La gestion des clés cryptographiques utilisées dans des SAM doivent être gérées de façon à ne pas nuire à la sécurité d'aucun système utilisant des ICC.

d) Les logiciels d'application des CAD ne doivent pas pouvoir compromettre les fonctions de sécurité du SAM.

5 Cycle de vie du SAM

Le présent article prescrit les règles minimales de sécurité propres aux différentes étapes du cycle de vie du SAM:

Fabrication du SAM

Préparation du SAM

Initialisation du SAM

Activation du SAM

Emploi du SAM

Utilisation du SAM

Désactivation du SAM

Réactivation du SAM

Fin

Démantèlement d'utilisation du SAM

5.1 Fabrication du SAM

Le processus de fabrication du SAM comprend la conception matérielle et logicielle du SAM, ainsi que l'assemblage et la présentation pour aboutir à un SAM.

Préalablement à l'étape du processus de chargement des données spécifiques dans le SAM, la sécurité des procédures de fabrication doit être conforme au niveau exigé par le fournisseur du SAM.

Les procédures de sécurité suivantes doivent être appliquées, une fois franchie l'étape du chargement dans le SAM des données spécifiques (par exemple, un algorithme cryptographique, une clé ou des données secrètes).

a) Toutes les opérations doivent se dérouler dans un environnement dont l'accès est contrôlé et où la confidentialité des données spécifiques est assurée;

b) L'accès aux zones protégées du SAM doit se faire exclusivement par le biais d'une clé cryptographique (à savoir une Clé de production) conformément à l'ISO 10202-3;

c) Les SAM doivent être physiquement et/ou cryptographiquement protégés au cours de leur stockage et de leur transport.

La conception et la fabrication des SAM doivent se dérouler de telle manière qu'il soit impossible, sans recourir à des procédés généralement non disponibles (par exemple, des attaques physiques ou logiques), de leur porter préjudice et voir ainsi des données secrètes dévoilées.

Les données d'analyse d'audit doivent être mémorisées dans le SAM de la façon suivante (voir annexe A).

Identificateur du fournisseur de SAM

Identificateur du fabricant

Identificateur du type de SAM

Le processus de fabrication doit inclure une vérification (par exemple, par examen d'un échantillon statistique) de l'intégrité des fonctionnalités du SAM aux spécifications de référence.

5.2 Préparation du SAM

Cette préparation se décompose en deux étapes suivantes.

— Initialisation du SAM

— Activation du SAM

5.2.1 Initialisation du SAM

Le fournisseur d'application ou le fournisseur du SAM doit être responsable de la fourniture des données et des processus de sécurité relatifs à l'initialisation.

Le SAM doit contenir les clés cryptographiques nécessaires, décrites dans l'ISO 10202-3.

Le processus d'initialisation doit se dérouler conformément à l'ISO 10202-3, en particulier en ce qui concerne le chargement de clés cryptographiques et autres données de sécurité.

Il convient qu'un identificateur de l'initialiseur du SAM soit mémorisé dans le SAM à des fins d'audit. Cet identificateur doit avoir la spécification détaillée dans l'annexe A.

5.2.2 Activation du SAM

L'activation du SAM rend celui-ci opérationnel pour les transactions financières réalisées par un CAD. Ce processus doit se dérouler sous le contrôle de l'acquéreur pour le compte du fournisseur du SAM ou de son agent.

Le processus d'activation doit être développé conformément à l'ISO 10202-3. À la suite de cette opération, le SAM doit contenir toutes les données nécessaires à l'identification du CAD ou de l'accepteur de carte.

Il convient que l'identificateur de l'activateur du SAM et la date d'activation soient mémorisés dans le SAM à des fins d'audit de sécurité (voir annexe A pour des prescriptions détaillées).

Le complet déroulement du processus d'activation doit se traduire par un passage du SAM à l'état activé.

5.3 Emploi du SAM

5.3.1 Utilisation du SAM

Un SAM ne doit pas être diffusé avant d'avoir été initialisé et ne doit pas être utilisable pour une transaction financière sans avoir été activé.

Le SAM doit pouvoir prendre en charge les fonctions de transactions contenues dans l'ISO 10202-2 et répondre de façon adéquate aux prescriptions de sécurité formulées par l'émetteur de carte ou le fournisseur d'application. Les fonctions de transactions qui s'effectuent entre l'ICC et le SAM doivent être conformes aux prescriptions de l'ISO 10202-2.

Le SAM doit être accessible au CAD tout au long des transactions qui activent des fonctions prises en charge par le SAM.

5.3.2 Désactivation du SAM

Seuls le fournisseur de SAM ou son agent sont habilités à désactiver un SAM. Le SAM ne doit alors plus accepter aucune transaction financière. Il est toutefois possible d'effectuer la réactivation du SAM.

La désactivation du SAM doit se traduire par un passage à l'état désactivé de l'identificateur d'activation du SAM (voir annexe A).

S'il est nécessaire de se prémunir contre une désactivation du SAM non autorisée, alors le processus doit inclure un échange cryptographique utilisant la clé cryptographique prescrite dans l'ISO 10202-3.

5.3.3 Réactivation du SAM

Le processus de réactivation du SAM, qui permet au SAM d'être de nouveau utilisable pour les transactions financières, doit être lancé sous le contrôle de l'acquéreur pour le compte du fournisseur de SAM ou de son agent.

La réactivation du SAM doit se traduire par la mise à l'état «activé» de l'identificateur d'activation du SAM (voir annexe A).

S'il est nécessaire de se prémunir contre une réactivation du SAM non autorisée, alors le processus doit inclure un échange cryptographique, utilisant la clé cryptographique *k*ActI prescrite dans l'ISO 10202-3.

5.4 Fin à usage

Le processus consistant à désactiver de façon définitive un SAM est au bon vouloir de l'acquéreur pour le compte du fournisseur du SAM ou de son agent, et doit rendre le SAM inutilisable.

L'identificateur d'activation du SAM doit être mis à l'état de désactivation définitive (voir annexe A).

S'il est nécessaire de se prémunir contre une fin d'usage du SAM non autorisée, alors le processus doit inclure un échange cryptographique utilisant la clé cryptographique *k*ActI prescrite dans l'ISO 10202-3.

6 Interfaces SAM-CAD

6.1 Caractéristiques physiques

Les caractéristiques physiques du SAM doivent être conformes aux prescriptions de l'ISO/CEI 7816-1 et de l'ISO/CEI 7816-2.

6.2 Caractéristiques électriques et types de protocoles

Les caractéristiques électriques et types de protocoles doivent être conformes à l'ISO/CEI 7816-3.

6.3 Commandes

Les commandes utilisées par le SAM doivent être conformes à l'ISO/CEI 7816-4.

6.4 Identificateurs

Les identificateurs utilisés par le SAM doivent être conformes à l'ISO/CEI 7816-5.

7 Fonctions de sécurité du SAM

L'ensemble minimal de fonctions de sécurité que doit pouvoir accomplir un SAM comprend l'authentification d'un ADF ou d'une ICC. D'autres fonctions additionnelles peuvent être disponibles, telles que l'authentification d'un SAM par l'ICC et, si nécessaire, par l'ordinateur hôte du fournisseur du SAM, le chargement/remplacement des clés du SAM, la certification de transaction par le SAM et le chargement/remplacement de données du SAM (l'annexe B fournit des exemples de mise en œuvre). Dans tous les cas, le SAM effectue ses tâches relatives à la sécurité, sous la coordination du logiciel d'application du CAD.

Toutes les fonctions doivent être indépendantes du type de protocole de transmission. Le SAM et l'ICC peuvent utiliser différents protocoles conformes à l'ISO/CEI 7816-3.

Au cours de l'initialisation de la session SAM, le CAD doit recevoir toutes les informations nécessaires en ce qui concerne les prérogatives du SAM relatives à la validité, au système de paiement, aux algorithmes et aux clés. Le CAD doit fournir, comme faisant partie du processus cryptographique de la session ICC, les informations attendues par le SAM pour la sélection des clés et de l'algorithme.

Les algorithmes et clés sélectionnés restent actifs jusqu'à ce qu'une autre sélection soit réalisée ou que la transaction ou la session ICC s'achève.

Pour les messages (commandes et réponses) de sélection, de transmission et d'exécution des fonctions, voir l'ISO/CEI 7816-4 et l'ISO 9992-2.

7.1 Authentification dynamique d'un CDF ou d'un ADF

Le but de cette fonction est de donner la possibilité au SAM de vérifier l'authenticité d'un CDF ou d'un ADF, et de s'assurer ainsi qu'ils ont été fournis par l'autorité habilitée.

Il est recommandé que l'authentification dynamique d'un CDF ou d'un ADF comprenne la transmission d'un nombre pseudo-aléatoire, ou d'une variable temporelle (par exemple, un compteur), au CDF ou à l'ADF, à partir du SAM. L'identité de l'algorithme et de la clé cryptographique à utiliser par le processus d'authentification peut être définie implicitement ou explicitement en utilisant un identificateur de clé (voir ISO 10202-7). Le nombre pseudo-aléatoire doit ensuite être traité dans le CDF ou l'ADF, par un algorithme, avec la clé cryptographique *k*Iaut ou *k*Aaut prescrite dans l'ISO 10202-3. Le résultat de ce processus, le paramètre d'authentification, doit être renvoyé au SAM pour contrôle.

NOTE 2 La procédure décrite correspond au processus 2, authentification d'entité, décrit dans l'ISO 10202-5.

7.2 Authentification dynamique d'un SAM

Le but de cette fonction est de permettre à une ICC de vérifier l'authenticité du SAM, et de s'assurer ainsi qu'il a été fourni par l'autorité habilitée (par exemple, le fournisseur d'application).

Il est recommandé que l'authentification dynamique d'un SAM comprenne la transmission d'un nombre pseudo-aléatoire, ou d'une variable temporelle (par exemple, un compteur), au SAM, à partir d'une ICC. L'identité de l'algorithme et de la clé cryptographique à utiliser par le processus d'authentification peut être définie implicitement ou explicitement en utilisant un identificateur de clé (voir ISO 10202-7). Le nombre pseudo-aléatoire doit ensuite être traité dans le SAM par un algorithme, avec la clé cryptographique *k*Iaut ou *k*Aaut prescrite dans l'ISO 10202-3. Le résultat de ce processus, le paramètre d'authentification, doit être renvoyé à l'ICC pour contrôle.

NOTE 3 La procédure décrite correspond au processus 2, authentification d'entité, décrite dans l'ISO 10202-5.

7.3 Chargement/remplacement de clés du SAM

Le but de cette fonction est de charger ou remplacer des clés cryptographiques dans un SAM après une initialisation.

Les clés cryptographiques utilisées par un SAM devraient être chargées ou remplacées sous le contrôle de la clé cryptographique *k*Actl prescrite dans l'ISO 10202-3.

NOTES

4 La procédure décrite correspond au processus 1, échange de clés, décrit dans l'ISO 10202-5.

5 On suppose qu'une clé initiale a été chargée durant le processus d'initialisation.

7.4 Certification de transaction par le SAM

Le but de cette fonction est d'apporter la preuve au fournisseur d'application (et à l'acquéreur) que le SAM a été sollicité au cours d'une transaction et que les fonctions à exécuter (par exemple, l'authentification de l'ICC) ont été réalisées.

Il est recommandé que la certification de transaction par le SAM comprenne la transmission des données de transaction au SAM. Ces données sont ensuite traitées dans le SAM par un algorithme. Le résultat de ce processus, le certificat de transaction, est alors envoyé au CAD. Ce certificat doit être constitué à l'aide de la clé cryptographique *k*Acer prescrite dans l'ISO 10202-3.

NOTE 6 La procédure décrite correspond au processus 5, certification de transaction, décrit dans l'ISO 10202-5.

7.5 Chargement/remplacement de données du SAM

Le but de cette fonction est d'assurer l'intégrité ou la confidentialité des informations soit chargées, soit mises à jour dans un SAM.

L'intégrité de ces informations doit être assurée, si nécessaire, par le biais de l'authentification de message utilisant la clé cryptographique *k*Aaut prescrite

dans l'ISO 10202-3. La confidentialité de ces informations sera, si nécessaire, éventuellement assurée au moyen d'un chiffrement utilisant la clé cryptographique *k*Aenc prescrite dans l'ISO 10202-3.

NOTE 7 Si la confidentialité n'est pas nécessaire, la procédure correspond au processus 3, authentification de message, et si la confidentialité est requise, au processus 4, chiffrement de message, décrits dans l'ISO 10202-5.

Annexe A
(normative)

Description de l'audit de sécurité et des zones de données associées

Identificateur du fabricant du SAM

Statut:	Obligatoire
Emplacement:	Zone accessible en lecture
Condition d'accès:	Non modifiable
Format:	2 octets
Contenu:	Identificateur du fabricant conformément au registre tenu par l'ISO
Objet:	Identification unique du fabricant d'un SAM

Identificateur du fournisseur du SAM

Statut:	Obligatoire
Emplacement:	Zone accessible en lecture
Condition d'accès:	Non modifiable
Format:	4 octets
Contenu:	Identificateur du fournisseur conformément au registre tenu par l'ISO
Objet:	Identification unique du fournisseur d'un SAM

Identificateur du type du SAM

Statut:	Optionnel
Emplacement:	Zone accessible en lecture
Condition d'accès:	Non modifiable
Format:	2 octets
Contenu:	L'identificateur définit le type de matériel et les caractéristiques
Objet:	Identification du type de SAM

Version du logiciel SAM

Statut:	Optionnel
Emplacement:	Zone accessible en lecture
Condition d'accès:	Non modifiable

NOTE 8 Cela n'exclut pas que le fournisseur de SAM puisse modifier l'identificateur via ses propres procédures de sécurité, par exemple en remettant à l'état initial les clés cryptographiques adéquates.

Format:	1 octet
Contenu:	Définition de la version actuelle du logiciel
Objet:	Identification de la version du logiciel utilisée dans le SAM