NORME INTERNATIONALE

ISO 10202-3

Première édition
1998-07-01

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

Partie 3: Relations avec les clés cryptographiques

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/026f4be7-9084-4861-81fe-39ee020577bc/iso-10202-3-1998

Part 3: Cryptographic key relationships

Numéro de référence
ISO 10202-3:1998(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 10202-3 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 et B font partie intégrante de la présente partie de l'ISO 10202. Les annexes C et D sont données uniquement à titre d'information.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/026f4be7-9084-4861-81fe-39ee020577bc/iso-10202-3-1998

© ISO 1998

Droits de reproduction réservés. Sauf prescription différente, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

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 3:
Relations avec les clés cryptographiques

1 Domaine d'application

iTeh STANDARD PREVIEW
(standards.iteh.ai)

La présente partie de l'ISO 10202 spécifie les conditions minimales requises pour les relations avec les clés cryptographiques dans les architectures de sécurité des systèmes de transactions financières utilisant des cartes à circuit intégré; elle propose différentes options, parmi lesquelles l'émetteur de la carte ou le fournisseur d'application pourra choisir les relations avec les clés cryptographiques adaptées à son application.

ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/026f48e7-9084-4861-81fe-39ee020577bc/iso-10202-3-1998

Les relations avec les clés cryptographiques peuvent être établies durant le cycle de vie de la carte et du SAM entre les parties chargées de la fabrication et de la préparation de l'ICC et du SAM, ainsi que du processus de transaction.

Chaque fois qu'il est fait référence dans ce document à une relation avec clés cryptographiques, cette relation est obtenue en établissant une clé mutuelle secrète pour un algorithme symétrique, ou une clé appropriée issue d'une paire de clés publique/secrète pour un algorithme asymétrique.

NOTE Toute référence faite dans cette Norme internationale à l'émetteur de la carte ou au fournisseur d'applications, englobe également les agents mandatés par ces derniers.

Les relations avec les clés cryptographiques abordées dans la présente partie de l'ISO 10202 sont présentées à la Figure 1 (fabrication et préparation de l'ICC et du SAM) ainsi qu'à la Figure 2 (processus de transaction). Le dispositif d'acceptation de carte (CAD) de la Figure 2 se compose d'une partie agissant comme agent de l'acquéreur (aspect non abordé dans cette Norme internationale) ainsi que, le cas échéant, d'une autre partie agissant comme agent du fournisseur d'application: un module applicatif de sécurité (SAM). Un SAM est

— un dispositif physique fourni par le fournisseur de SAM ou

— une fonction logique au sein du module de sécurité du CAD.

Le SAM est sous la responsabilité du fournisseur d'application.

Deux annexes normatives sont jointes à la présente partie de l'ISO 10202. Il s'agit des annexes A et B, qui présentent les tableaux de relations avec les clés. Deux annexes informatives sont également rattachées: l'Annexe C, qui fournit un exemple de structure hiérarchique des clés dans une carte à circuit intégré (ICC), et l'Annexe D, qui donne un exemple d'utilisation des clés cryptographiques.

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 9807:1991, *Banque et services financiers liés aux opérations bancaires — Spécifications liées à l'authentification des messages (service au particuliers).*

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/020f48e7-9084-4861-81fe-39ee020577bc/iso-10202-3-1998

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 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.*

3 Termes et définitions

3.1 Pour les besoins de la présente Norme internationale, les définitions suivantes s'appliquent.

3.1.1
texte chiffré
texte en clair chiffré

3.1.2
clé cryptographique
paramètre utilisé avec un algorithme cryptographique pour procéder à des conversions cryptographiques

3.1.3
déchiffrement
processus consistant à convertir du texte chiffré en texte en clair

3.1.4
chiffrement
processus consistant à convertir du texte en clair en texte chiffré à des fins de confidentialité

3.1.5
clé
(voir clé cryptographique)

3.1.6
module applicatif de sécurité (SAM)
module physique (ou fonction logique du CAD) contenant un ou plusieurs algorithmes, des clés associées, ainsi que des procédures et informations de sécurité destinées à protéger une application contre tout accès illicite. Pour cela, le module doit être protégé physiquement et logiquement

3.1.7
acquéreur de transaction
organisme qui reçoit du dispositif d'acceptation de carte, les données relatives à une transaction financière à des fins de règlement

3.2 Pour une définition des abréviations utilisées dans la présente partie de l'ISO 10202, telles que CDF, ADF, ICC, voir l'ISO 10202-1 (1991).

Les lettres suivantes sont utilisées comme abréviations dans le texte qui suit:

A fournisseur d'application;

B tierce partie de confiance pour la certification de clé publique;

C ICC;

D concepteur;

E encarteur/assembleur d'IC;

H porteur de carte;

I émetteur de la carte;

K clé secrète employée avec un algorithme symétrique;

M fabricant;

N initialiseur de SAM;

P clé publique employée avec un algorithme asymétrique;

Q acquéreur de transaction;

R personnalisateur de carte;

S clé secrète employée avec un algorithme asymétrique;

T CAD;

U SAM;

VA activateur d'ADF;

VC activateur de CDF;

W activateur de SAM.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/026f4be7-9084-4861-81fe-39ee020577bc/iso-10202-3-1998

4 Principes généraux de sécurité

Les procédures de sécurité présentées dans cette partie de l'ISO 10202 sont régies par les principes suivants:

a) principes applicables à l'ICC, voir 10202-2;

b) principes applicables au SAM, voir 10202-4;

c) les informations obtenues par quelque moyen que ce soit d'une ICC ne doivent pas compromettre la sécurité d'une autre ICC ou d'un autre SAM ou de ces systèmes combinés entre eux;

d) l'accès à un CDF ou à un ADF doit toujours faire l'objet des contrôles d'accès logiques du CDF ou de l'ADF;

e) lors d'un traitement dans un ADF donné, la mémoire allouée à d'autres ADF ne peut faire l'objet d'aucune opération de lecture ou d'écriture;

f) la connaissance d'une clé cryptographique à un niveau de la structure hiérarchique des clés cryptographiques ne doit compromettre aucune autre clé cryptographique à ce niveau ou à un niveau supérieur de la structure ou (voir section 7);

g) du fait du principe de la séparation des clés cryptographiques, lors de l'activation d'un ADF, l'émetteur de la carte ne peut contrôler le fonctionnement de cet ADF que s'il est également fournisseur de l'application ou agent de ce dernier.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5 Notation pour les relations avec les clés et les clés associées

Deux entités, X et Y, ont établi une relation avec les clés cryptographiques *k* dans les cas suivants:

ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/026f4be7-9084-4861-81fe-39ee020577bc/iso-10202-3-1998

— en échangeant ou en partageant une clé symétrique secrète commune K, ou

— en échangeant la clé asymétrique publique P de X ou Y et en vérifiant son certificat, ou

— en échangeant la clé asymétrique publique P de X et la clé asymétrique publique P de Y et en vérifiant leur certificat.

La clé asymétrique publique P de l'entité X et la clé asymétrique publique P de l'entité Y seront toutes deux échangées si les fonctions de chiffrement, d'authentification et de certification bidirectionnelles sont requises.

Les entités partageant une clé sont identifiées par deux lettres séparées par un trait d'union, X-Y, par exemple.

La nomenclature employée pour faire référence à une clé, telle que celle employée dans le Tableau 1, doit être *kl* (i,j)f_{X-Y}, où

— *l* correspond à l'entité responsable du chargement de la clé;

— *k* est la notation générique d'une clé (K, P ou S) d'algorithme symétrique ou asymétrique;

— f correspond à la fonction de la clé;

— l'index i correspond à un ADF spécifique et à son jeu de clés correspondant;

— l'index j correspond à une clé spécifique d'un jeu de clés associé à un ADF et ayant la même fonction.

NOTE j est le numéro du jeu de clés défini dans l'ISO 10202-7 et l'ISO 10202-8.

Tableau 1 — Nomenclature des clés

Clé (*k*)	**Entité responsable du chargement des clés** (*l*)	**Fonctions de la clé** (f)	**Entités partageant l'emploi d'une clé** (X-Y)
K	A	aut (authentification d'entité)	A
S	E	cer (certification)	C
P	I	ctl (contrôle)	E
	M	enc (chiffrement)	I
	N	kex (échange de clés)	M
	R	mac (authentification du message)	N
		prd (production)	R
			U

Pour prendre un exemple d'algorithmes symétriques, KA (i,j)$aut_{C\text{-}A}$ est la clé d'authentification j du fournisseur d'application pour l'ADF (i), partagée par l'ICC et le fournisseur d'application. Si l'on prend un exemple d'algorithme asymétrique, SA (i,j)aut est la clé d'authentification j du fournisseur d'application pour l'ADF (i), connue uniquement du fournisseur d'application.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Les relations avec les clés sont établies à différentes phases du cycle de vie de la carte ou du SAM: fabrication de l'IC, de l'ICC ou du SAM, préparation de l'ICC ou du SAM, préparation de l'ADF, utilisation de la carte ou du SAM, et invalidation (voir 10202-1).

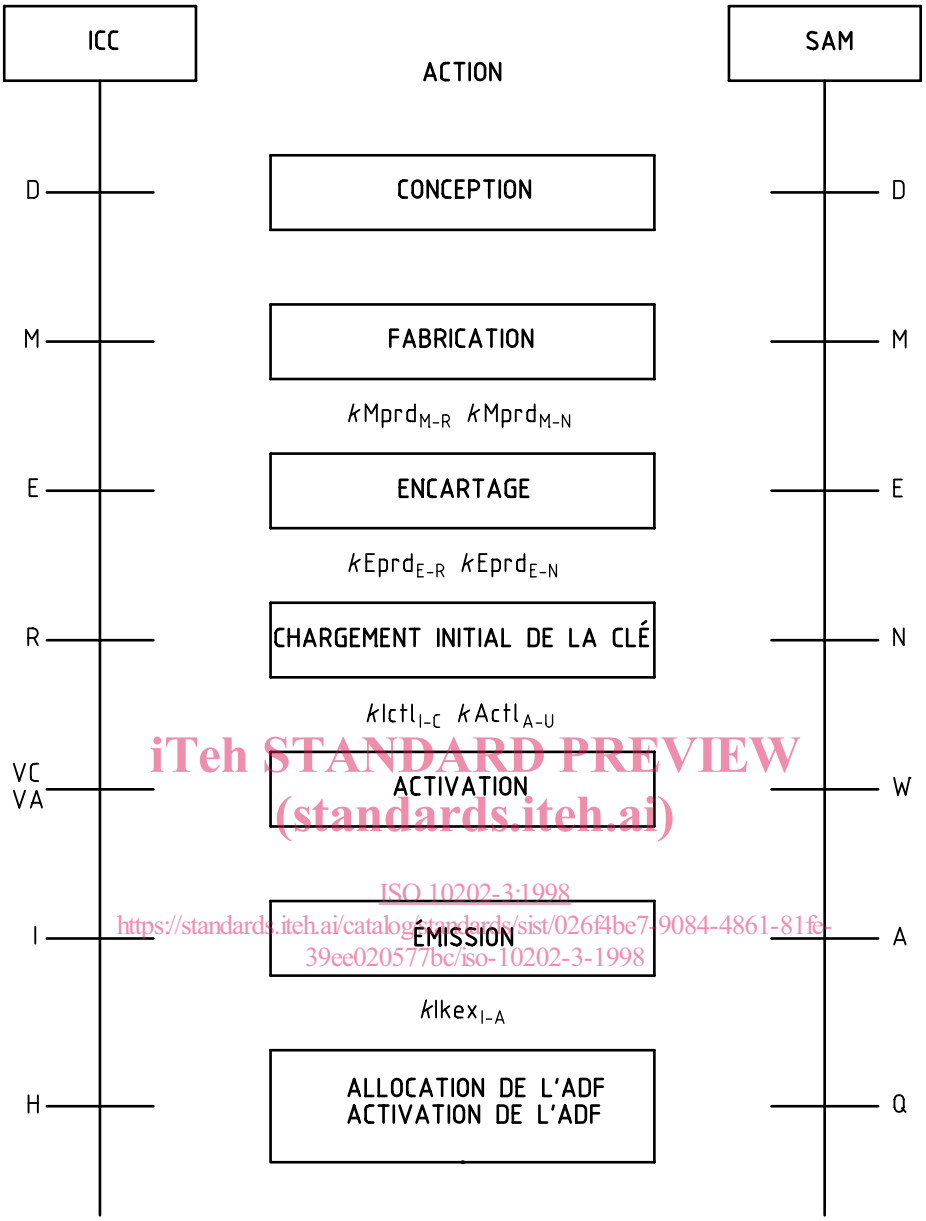
ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/...

Une relation avec clés cryptographiques est définie pour chaque fonction liée à la sécurité du CDF, de l'ADF et du SAM. Pour certaines de ces fonctions, en l'occurrence les fonctions de contrôle obligatoires, la clé cryptographique doit être différente pour chaque ICC [voir l'annexe A (normative)]. En ce qui concerne les autres fonctions, il est conseillé [voir l'annexe A (normative)] de confier au fournisseur d'applications, à l'émetteur de la carte et à l'acquéreur le soin de déterminer les clés nécessaires, les clés pouvant être omises, ainsi que celles pouvant être partagées dans plusieurs ICC pour leur application; ceci ne concerne pas les clés obligatoires. Les valeurs définies pour les références de clés sont présentées dans l'ISO 10202-7.

6 Relations avec les clés cryptographiques

6.1 Fabrication et préparation

La Figure 1 illustre les relations avec les clés cryptographiques de l'ICC et du SAM lors de la fabrication et de la préparation de la carte à circuit intégré (ICC) et du module applicatif de sécurité (SAM).



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/026f4be7-9084-4861-81fe-39ee020577bc/iso-10202-3-1998

Figure 1 — Phases de préparation de l'ICC et du SAM et clés employées lors de ce processus

Durant le cycle de vie de l'ICC et du SAM, l'émetteur et le fournisseur d'application sont chargés de vérifier l'authenticité de l'ICC et du SAM avant le chargement initial de la clé.

Le personnalisateur d'ICC et l'initialiseur de SAM agissent en tant qu'agents de l'émetteur et du fournisseur d'application. Ils doivent s'assurer que les fabricants de l'IC et du SAM n'ont aucun contrôle sur l'ICC et le SAM lors de la phase de «chargement initial de la clé». Cela est possible en faisant de *k*Mprd une clé temporaire non associée à la structure hiérarchique des clés de l'ICC (figure 3) et du SAM (figure 4) à l'issue des phases de personnalisation et d'initialisation.

L'encartage ne doit pas être nécessairement assuré par une entité distincte. Le fabricant ou le personnalisateur/initialiseur de SAM peut s'en charger.

6.2 Processus de transaction

Les relations avec les clés doivent être établies pour le processus de transaction comme indiqué dans la Figure 2 ci-dessous.

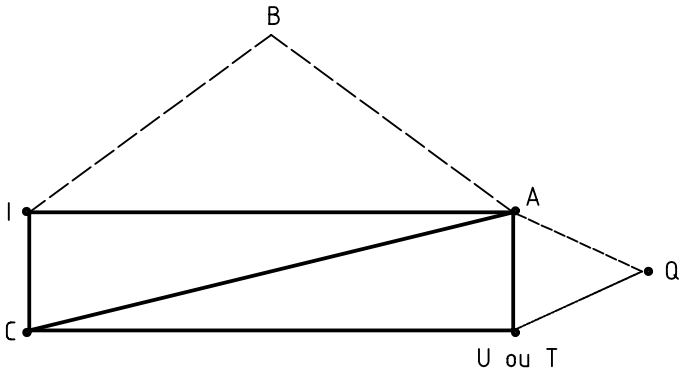


Figure 2 — Relations de transactions

Description des relations de la Figure 2

La relation T ne s'applique qu'à un algorithme asymétrique dans lequel le CAD ne possède pas de SAM.

La relation avec les clés C-T est établie entre l'ICC et le CAD pour des fonctions cryptographiques en différé. Elle est identique à la relation avec les clés C-A, à la différence toutefois que les clés publiques du fournisseur d'application sont situées dans le CAD.

La relation avec les clés I-C est utilisée pour des transactions de CDF entre l'ICC et l'émetteur de la carte.

La relation avec les clés C-A est utilisée dans des transactions en ligne entre l'ICC (agissant pour le porteur de la carte) et le fournisseur d'application. Les relations multiples avec les clés C-A peuvent être instaurées par un fournisseur d'application pour différentes fonctions telles que les fonctions de débit, de crédit ou de porte-monnaie électronique, non abordées dans cette norme.

La relation avec les clés C-U est établie entre l'ICC et le SAM pour des fonctions cryptographiques en différé. Elle est identique à la relation avec les clés C-A, à la différence toutefois que les clés du fournisseur d'application sont situées dans le SAM.

La relation avec les clés U-A est utilisée pour des mises à jour de programmes ou de clés du SAM.

La relation avec les clés I-A est une relation temporaire entre l'émetteur de la carte et le fournisseur d'application, destinée à permettre l'établissement d'un ADF et la séparation des clés.

Les relations avec les clés A-Q et U-Q ne sont pas abordées dans cette Norme internationale (elles sont identifiées par des lignes de pointillés).

Les relations avec les clés B-I et B-A sont utilisées pour la certification de clés publiques par une tierce partie de confiance B (identifiée par une ligne de tirets).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/026f4be7-9084-4861-81fe-39ee020577dc/iso-10202-3-1998

7 Relations avec les clés pour les ICC

Les clés uniques dans le présent article sont présentées en détails à l'Annexe A (normative).

Les clés utilisées pendant ou après la personnalisation de l'ICC doivent être indépendantes, d'un point de vue cryptographique, des clés établies avant la personnalisation. Les clés associées au CDF et à l'ADF doivent également être indépendantes d'un point de vue cryptographique, comme indiqué dans la structure hiérarchique de clés cryptographiques des ICC ci-après.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/026f4be7-9084-4861-81fe-39ee020577bc/iso-10202-3-1998

Figure 3 — Structure hiérarchique de clés cryptographiques des ICC

7.1 Clés établies avant la personnalisation de la carte

Si le circuit intégré contient des données privatives, l'une des clés de production appropriées doit être utilisée pour contrôler le transfert d'un IC et éviter tout risque de substitution d'un IC entre le personnalisateur de la carte et la partie qui le précède dans le cycle de vie de la carte.

NOTE S'il existe une relation avec clés entre E et R, il incombe à l'encarteur d'éviter tout risque de substitution d'un IC entre le fabricant et l'encarteur, en utilisant par exemple une clé $k\text{Mprd}_{\text{M-E}}$ fournie par E. Lorsqu'une clé $k\text{Mprd}_{\text{M-E}}$ est utilisée, une clé $k\text{Eprd}_{\text{E-R}}$ doit également être employée afin de sécuriser les informations privatives entre M et R.

Le Tableau 2 présente les clés de production possibles avant personnalisation de la carte. La responsabilité est partagée entre les deux parties utilisant une clé de production. Chacune d'elles peut utiliser sa propre clé de contrôle, non partagée par les autres parties (et non définie dans cette Norme) afin de protéger ses propres données.

NOTE Il n'existe pas de relation avec clés entre R et I. Le personnalisateur de carte R est considéré comme étant l'émetteur de la carte, ou l'agent de ce dernier, auquel cas, il charge les clés fournies par l'émetteur.

Tableau 2 — Clés de production possibles avant personnalisation de la carte

Nom de la clé	Clé de production précédante pour la protection du chargement	Responsabilité partagée par	Chargée par	Fonction de la clé
kMprd$_{M\text{-}R}$	Clé de production existante	M & R	M	Contrôle du transfert d'un IC et protection contre les risques de substitution d'un IC
kEprd$_{E\text{-}R}$	Clé de production existante	E & R	E	

7.2 Clés fournies par l'émetteur de la carte et établies lors de la personnalisation de la carte (voir Tableau 3)

Lors de la personnalisation, la clé de production, si elle est utilisée, assure un contrôle cryptographique du chargement de paramètres secrets (dont kIctl$_{I\text{-}C}$) dans le circuit intégré. Les clés de production sont des clés temporaires qui ne seront plus utilisables à l'issue de la personnalisation de la carte (voir Figure 3). Si aucune clé de production n'est utilisée, le chargement de ces paramètres sera physiquement protégé d'une manière convenue par l'émetteur de la carte et le personnalisateur.

7.2.1 kIctl$_{I\text{-}C}$ — Clé de contrôle de l'émetteur

Cette clé doit être utilisée par l'émetteur de la carte pour charger et contrôler ses propres clés et paramètres cryptographiques (tels qu'un PIN) dans le circuit intégré (voir Figure 3), ainsi que pour allouer de l'espace dans l'IC.

Pour un émetteur de la carte donné, la clé kIctl$_{I\text{-}C}$ de la carte ne doit pas être volontairement identique à celle d'autres cartes.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Cette clé doit également être utilisée si une protection cryptographique est nécessaire pour l'activation, la désactivation, la réactivation, et la résiliation d'un fichier de données communes (CDF).

ISO 10202-3:1998
https://standards.iteh.ai/catalog/standards/sist/026f4be7-9084-4861-81fe-39ee02057f8c/iso-10202-3-1998

La clé kIctl$_{I\text{-}C}$ doit également être utilisée pour allouer de l'espace mémoire à des ADF si l'IC supporte l'allocation dynamique d'espace mémoire.

7.2.2 kIaut$_{I\text{-}C}$ — Clé d'authentification de l'émetteur

Cette clé doit être utilisée par l'émetteur de la carte pour l'authentification du CDF et/ou par le CDF pour l'authentification de l'émetteur de la carte, si l'une de ces fonctions est requise (voir Figure 2).

Si kIaut$_{I\text{-}C}$ et kIaut$_{C\text{-}I}$ sont identiques, il convient d'envisager les risques d'attaque par réflexion (voir 10202-5).

Tableau 3 — Relations avec les clés cryptographiques pendant la personnalisation de la carte

Nom de la clé	Chargée sous la clé	Fournie par	Chargée par	Fonction de la clé	Etat
kIctl$_{I\text{-}C}$	Clé de production existante ou protection physique	I	R	Chargement/contrôle des clés et paramètres	Voir 7.2 et 7.2.1
kIaut$_{I\text{-}C}$	kIctl$_{I\text{-}C}$	I	R	Authentification de l'émetteur de la carte / d'ICC	Voir 7.2.2
kIcer$_{I\text{-}C}$	kIctl$_{I\text{-}C}$	I	R	Certification	Voir 7.2.3
kImac$_{I\text{-}C}$	kIctl$_{I\text{-}C}$	I	R	Authentification de message	Voir 7.2.4
kIenc$_{I\text{-}C}$	kIctl$_{I\text{-}C}$	I	R	Chiffrement/déchiffrement	Voir 7.2.5