

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 910 839 B1

(12)

FASCICULE DE BREVET EUROPEEN

(45) Date de publication et mention
de la délivrance du brevet:

22.10.2003 Bulletin 2003/43

(21) Numéro de dépôt: **97926064.3**

(22) Date de dépôt: **30.05.1997**

(51) Int Cl.7: **G07F 7/08**

(86) Numéro de dépôt international:
PCT/FR97/00947

(87) Numéro de publication internationale:
WO 97/045815 (04.12.1997 Gazette 1997/52)

(54) **PROCEDE DE STOCKAGE DES UNITES DE VALEUR DANS UNE CARTE A PUCE DE FACON
SECURISEE ET SYSTEME DE TRANSACTION MONETAIRE AVEC DE TELLES CARTES**

VERFAHREN ZUM GESICHERTEN SPEICHERN VON WERTEINHEITEN IN EINER CHIPKARTE
UND GELDÜBERWEISUNGSSYSTEM ZUR DESSEN VERWENDUNG

METHOD FOR SAFELY STORING CREDIT UNITS IN A SMART CARD AND MONETARY
TRANSACTION SYSTEM USING SAME

(84) Etats contractants désignés:
BE DE DK ES FI FR GB IT NL PT SE

(30) Priorité: **31.05.1996 FR 9606705**

(43) Date de publication de la demande:
28.04.1999 Bulletin 1999/17

(73) Titulaire: **GEMPLUS**
13881 Gémenos Cédex (FR)

(72) Inventeur: **KIRIK, Jean-Paul**
F-13010 Marseille (FR)

(56) Documents cités:
EP-A- 0 299 826 EP-A- 0 423 035
EP-A- 0 621 570 FR-A- 2 689 662

EP 0 910 839 B1

Il est rappelé que: Dans un délai de neuf mois à compter de la date de publication de la mention de la délivrance du brevet européen, toute personne peut faire opposition au brevet européen délivré, auprès de l'Office européen des brevets. L'opposition doit être formée par écrit et motivée. Elle n'est réputée formée qu'après paiement de la taxe d'opposition. (Art. 99(1) Convention sur le brevet européen).

Description

[0001] La présente invention se rapporte aux procédés qui permettent de stocker de façon sécurisée des unités de valeur dans une carte à puce et aux systèmes de transaction monétaire utilisant ces cartes. L'invention s'applique plus particulièrement à des cartes à puces comportant une zone mémoire de type EEPROM non protégée.

[0002] En effet, une zone EEPROM non protégée d'une carte est accessible par tout individu disposant d'un simple lecteur de carte et de commandes de lecture et écriture en mémoire. Ce type de zone mémoire ne permet pas d'enregistrer des données sensibles puisque n'importe qui peut les lire et les modifier.

[0003] Le procédé s'applique également à des cartes à puce à mémoire protégée afin d'en élever le niveau de sécurité.

[0004] Les cartes à microprocesseurs sont capables de contenir des unités de valeur et d'en interdire l'accès. Seul le système d'exploitation de la carte peut accéder à ces unités et en augmenter ou en diminuer le nombre. Des commandes sécurisées et gérées par le système d'exploitation permettent donc la gestion de la zone contenant les unités de valeur, permettant l'utilisation de ces unités de valeur ainsi que leur rechargement en toute sécurité.

[0005] Une carte à mémoire ne comporte ni microprocesseur, ni a fortiori de système d'exploitation mais simplement quelques commandes permettant l'accès aux zones mémoire de la carte. Néanmoins, certaines zones de la carte peuvent avoir des caractéristiques permettant le stockage sécurisé d'unités de valeur. C'est le cas de certaines cartes à mémoire possédant une zone protégée par un code secret. Seul un terminal de paiement possédant ce code secret pourra accéder à la zone contenant les unités de valeur et pourra modifier le nombre d'unités avec des commandes d'écriture en mémoire. Par définition, un fraudeur ne connaît pas le code secret, il n'est donc pas capable de recharger une carte en unités de valeur. D'autres caractéristiques liées à la carte peuvent permettre un stockage sécurisé d'unités de valeur.

[0006] Dans l'état de la technique connu, les mécanismes de base existant sont l'utilisation d'un certificat d'intégrité, d'un compteur de transaction ainsi que d'une zone de copie. Ces mécanismes vont être détaillés dans la suite. Dans le cas des cartes à microprocesseur, ces mécanismes de base peuvent être inclus dans les systèmes d'exploitation.

[0007] Ces mécanismes peuvent également être appliqués sous forme de note d'application ou de recommandation d'application aux cartes à microprocesseur et à certaines cartes à mémoire de type synchrone.

[0008] Une note d'application ou de recommandation décrit les mécanismes à mettre en oeuvre au niveau de la carte et du terminal et définit la façon dont le terminal doit utiliser la carte.

[0009] On entend plus précisément par note d'application, une définition particulière de l'état de la mémoire dans la carte et dans le terminal, appelée "mapping" en terminologie anglo-saxonne, ce mapping étant obtenu par un logiciel informatique tenant compte de la note d'application. Le mécanisme à mettre en oeuvre consiste à inclure dans le calcul de ce certificat une donnée variant à chaque transaction. On entend par transaction une modification du nombre d'unités de valeur d'une carte.

Mécanisme 1 :

[0010] Un premier mécanisme en oeuvre est l'utilisation d'un certificat associé au nombre d'unités. Ce certificat garantit l'intégrité des informations auxquelles il se rapporte. Un terminal d'une application de paiement peut lire le nombre d'unités de valeur présentes dans une carte à puce. Le certificat présent dans la carte et associé au nombre d'unités de valeur stockées doit être lu et vérifié. Ce certificat est calculé à l'aide d'une fonction mathématique. Il se calcule à partir du nombre d'unités présentes dans la carte, de données identifiant la carte et avec un secret seulement connu par le terminal. Le terminal est donc capable de vérifier ou de calculer un tel certificat. Une autre solution consiste à partager le secret entre les cartes et un serveur central. Les terminaux de l'application devront donc se connecter au serveur pour toute vérification.

[0011] Si le certificat est correct, le nombre d'unités de valeur présentes dans la carte est considéré comme valide.

Mécanisme 2 :

[0012] Ce mécanisme consiste à inclure dans le calcul de ce certificat une donnée variant à chaque transaction. L'introduction de cette donnée qui peut être un compteur de transaction permet de garantir que l'on a un certificat différent à chaque fois. Une carte possède un nombre d'unités de valeur à un instant t donné. A l'instant $t+n$, c'est-à-dire après un certain nombre n de transactions, si cette carte contient de nouveau le même nombre d'unités de valeur qu'à l'instant t , le certificat associé sera malgré tout différent. Il faut bien sûr que la valeur du compteur de transaction soit modifiée à chaque transaction.

Mécanisme 3 :

[0013] Ce mécanisme consiste à dupliquer les informations sensibles avant le déroulement d'une transaction. Les données dupliquées sont stockées dans la carte, dans la mémoire EEPROM non protégée.

[0014] La mémoire EEPROM non protégée est donc divisée en deux zones que nous appellerons dans toute la suite zone active et zone de copie. Ces deux zones comportent un nombre d'unités de valeur et le certificat

correspondant.

[0015] En cas d'arrachement de la carte, si les données en cours de modification dans la zone active sont corrompues ou altérées, les données dupliquées dans la zone de copie seront récupérées et transférées dans la zone active. La carte demeure ainsi dans un état stable. En cas d'arrachement de carte, le certificat présent dans la zone de copie doit correspondre à la valeur du compteur de transaction de la carte. Ceci permet de vérifier l'authenticité du certificat de la zone de copie et donc l'intégrité du nombre d'unités de valeur de la zone de copie. C'est pourquoi, le compteur de transaction de la carte doit être modifié en fin de transaction.

[0016] Toutes ces sécurités n'empêchent pas malheureusement certaines fraudes que l'on va expliciter dans ce qui suit :

1er cas de fraude :

[0017] Dans le cas d'unités de valeur présentes dans une zone mémoire non protégée par la puce de la carte, la fraude consiste à modifier le nombre d'unités présentes dans la carte et à essayer différentes valeurs de certificat.

[0018] Un fraudeur ayant un petit nombre d'unités présentes dans la carte va donc le remplacer par le nombre maximum d'unités que peut contenir sa carte. Dans ce cas précis, aucun mécanisme n'empêche de modifier le contenu de la zone mémoire de la carte, la carte ne possédant pas de zone protégée. Puis le fraudeur va inscrire dans la carte, en lieu et place du précédent certificat une valeur aléatoire. Étant donné les faibles capacités mémoire des composants utilisés, les certificats sont enregistrés sur quelques bits.

[0019] La probabilité de trouver par hasard le certificat correspondant au nombre d'unités de la carte est élevée. La carte ne peut être considérée d'un point de vue cryptographique comme un porte-unités de valeur sécurisée. Cette fraude permet de recharger illégalement une carte en unités de valeur.

2ième cas de fraude :

[0020] Dans le cas d'un débit d'unités de valeur dans la carte, et en cas d'arrachement, la carte se retrouve avec une zone active éventuellement corrompue et une zone de copie contenant un certain nombre d'unités de valeur. De plus, la zone de copie contient le nombre d'unités de valeur précédant le débit.

[0021] Puisqu'il s'agit d'une interruption de transaction, le compteur de transaction peut ne pas avoir encore été modifié. La zone mémoire contenant les unités de valeur n'étant pas protégée contre les modifications, un fraudeur peut transférer le contenu de la zone de copie dans la zone active. Le contenu de la zone de copie est valide puisque son certificat correspond toujours à la valeur du compteur de transaction. Cette fraude permet de récupérer des unités de valeur utilisées.

3ième cas de fraude :

[0022] Un fraudeur peut également lire le contenu de sa carte avant une transaction. Il inscrit le contenu de la zone active sur une feuille de papier sans même en comprendre la signification. Puis il exécute une transaction. En cas d'arrachement de carte, la transaction ne sera pas achevée. La valeur du compteur de transaction de la carte ne sera pas modifiée. Le fraudeur pourra simplement réécrire dans la zone active de sa carte les données inscrites sur sa feuille de papier. Cette fraude permet également de récupérer des unités de valeur utilisées.

[0023] La présente invention permet de remédier à ces problèmes.

La présente invention a pour objet un procédé de stockage d'unités de valeur dans une carte à puce pour la réalisation de transactions à partir d'un terminal selon la revendication 1.

[0024] La présente invention concerne aussi un terminal tel que défini par la revendication 9.

[0025] Selon une autre caractéristique les opérations de chiffrement sont réalisées au moyen d'un algorithme de chiffrement E_K et d'une clé secrète K par le terminal de transaction.

[0026] Selon une autre caractéristique, le procédé consiste globalement à calculer un certificat destiné à la zone active en utilisant une première fonction, et à calculer le certificat destiné à la zone de copie, en utilisant une autre fonction. Ainsi, dans le cas où le certificat de la zone de copie serait copié dans la zone active, il ne serait plus valide.

[0027] Plus précisément, le procédé consiste à :

- calculer à partir d'une première fonction mathématique FA, un premier certificat CA stocké dans la zone active et garantissant l'intégrité des points de cette zone;
- calculer à partir d'une seconde fonction mathématique FB, un second certificat CB stocké dans la zone de copie et garantissant l'intégrité de cette zone.

[0028] Afin d'éviter que le contenu de la zone active ne puisse être utilisé en cas d'arrachement, selon une autre caractéristique de l'invention, le calcul du certificat destiné à la zone de copie est réalisé à partir du nombre d'unités de valeur, mais aussi de la valeur d'un compteur de transaction. Dans la phase d'initialisation d'une transaction, on calcule le certificat à partir du nombre d'unités de valeur présent dans la zone active et d'une valeur du compteur de transaction incrémentée à sa prochaine valeur, la donnée obtenue est chiffrée et enregistrée en zone de copie, le compteur de transaction est ensuite incrémenté à cette nouvelle valeur de sorte qu'à cet instant, le certificat de la zone active n'est plus en accord avec la valeur du compteur, seule la donnée de sauvegarde étant correcte. De cette façon, le terminal marque dans la carte le début d'une transaction.

[0029] Selon une caractéristique de l'invention on distingue une carte arrachée accidentellement d'une carte arrachée frauduleusement en vérifiant la parité du compteur de transaction dans la phase d'initialisation de la transaction. En effet, si par convention on choisit qu'une valeur du compteur de transaction impaire indique que la carte a été arrachée avant la fin de la transaction. Alors dans la phase d'initialisation d'une nouvelle transaction, le terminal vérifie la parité du compteur de transaction. Une valeur impaire du compteur de transaction lui indique donc que la carte a été arrachée. Le terminal ne vérifie pas l'intégrité de la zone active et vérifie directement l'intégrité de la zone de copie. Le fraudeur n'a plus de moyen de tester les valeurs aléatoires qu'il écrit dans la zone active.

[0030] Ainsi selon le procédé la parité de la valeur du compteur de transaction utilisé dans le calcul des certificats est identique en début et en fin de transaction, et la valeur du compteur de transaction est incrémentée deux fois durant la transaction, chaque incrémentant étant d'une seule unité.

[0031] Dans la phase d'initialisation d'une transaction, on lit la valeur du compteur de transaction de la carte. Si la valeur lue est paire, on lit les informations de la zone active (ZA), on vérifie l'intégrité des informations de la zone active, l'intégrité des informations de la zone active est vérifiée, on procède au stockage d'unités de valeur dans la carte à puce.

[0032] Dans la phase d'initialisation d'une transaction, on lit la valeur du compteur de transaction de la carte. Si la valeur lue est impaire, on lit les informations de la zone de copie (ZC), on vérifie l'intégrité des informations de la zone de copie, l'intégrité des informations de la zone de copie est vérifiée, on calcule un certificat à partir du nombre d'unités de valeur présent dans la zone de copie (ZC) et de la valeur du compteur de transaction incrémentée à sa prochaine valeur paire, la donnée obtenue est chiffrée et enregistrée en zone active (ZA), le compteur est ensuite incrémenté à cette nouvelle valeur de sorte qu'à cet instant, le certificat de la zone de copie (ZC) n'est plus en accord avec la valeur du compteur, seule la donnée de la zone active étant correcte.

[0033] D'autres avantages et caractéristiques de l'invention apparaîtront à la lecture de la description suivante qui est faite à titre illustratif et non limitatif et en regard des dessins sur lesquels :

- la figure 1, représente le schéma d'un système de transaction,
- la figure 2, représente une structure des données de la mémoire 103 de carte à puce selon un exemple de réalisation,
- la figure 3, représente les étapes relatives à une transaction mises en oeuvre par un terminal,
- la figure 4, représente les étapes mises en oeuvre lors de la vérification de l'intégrité des données de la zone active ou de la zone de copie,

- la figure 5, représente les étapes préalables à une transaction décrite en figure 3,
- la figure 6, représente les étapes de mise à jour du solde lors d'une transaction et la fin de la transaction.

[0034] Ainsi, selon une première caractéristique de l'invention, on chiffre le contenu des zone active ZA et zone de copie ZC de la mémoire EEPROM non protégée 103 représentée sur la figure 1.

[0035] Ce chiffrement est réalisé par un terminal 100 de l'application utilisant les cartes, à l'aide d'un algorithme de chiffrement E_K et d'une clef du terminal K. Cette clef de chiffrement est connue par les terminaux acceptant les cartes de l'application. Un terminal sachant chiffrer saura également déchiffrer le contenu de la carte à partir d'un algorithme de déchiffrement D_K .

[0036] Un fraudeur connaissant les principes de l'invention détaillés dans la suite et qui tente d'augmenter le nombre d'unités de valeur d'une carte ne sera plus capable de fixer le nombre maximum d'unités de valeur. Il ne pourra qu'essayer de recharger aléatoirement sa carte. Il inscrira donc des données aléatoires dans la zone active de sa carte. Il existe une probabilité pour qu'en déchiffrant la zone active d'une carte modifiée aléatoirement, un terminal obtienne un nombre d'unités de valeur et le certificat correspondant. Mais le nombre d'unités de valeur obtenu peut être inférieur au nombre d'unités de valeur contenu précédemment dans la carte. La probabilité d'obtenir un nombre d'unités de valeur supérieur au nombre d'unités de valeur initialement présent dans la carte est d'autant plus faible que ce nombre d'unités de valeur initial est grand.

[0037] Afin de rendre encore plus difficile la fraude consistant à trouver aléatoirement un certificat correspondant à un nombre important d'unités de valeur, on prévoit selon le procédé d'augmenter la taille du certificat. Plus la taille du certificat est grande, plus il est difficile de trouver la bonne valeur. Or, comme les tailles mémoires sont relativement faibles dans une carte à puce, il n'est pas possible d'avoir à la fois un grand nombre d'unités et un grand certificat.

[0038] Pour résoudre ce problème on propose selon une caractéristique de l'invention, que le nombre d'unités de valeur enregistré dans la carte ne corresponde pas au nombre d'unités de valeur pour l'application, mais au nombre d'unités de valeur qui ont fait l'objet d'une transaction (zéro pour une carte pleine d'unités).

[0039] Ce nombre est donc nul tant qu'aucune transaction n'a eu lieu. Ainsi, un nombre nul d'unités de valeur dans la carte correspond à la valeur maximale d'unités de valeur pour l'application. Et inversement, la valeur maximale d'unités de valeur dans la carte correspond à une valeur nulle d'unités de valeur pour l'application.

[0040] Un terminal de l'application lisant le contenu d'une carte obtient le nombre d'unités de valeur en soustrayant au nombre d'unités de valeur maximal de l'ap-

plication le nombre d'unités de valeur contenu dans la carte.

[0041] De cette façon, lorsque la carte contiendra un zéro, cela correspondra à la valeur maximale. Un zéro dans la carte se code sur un seul bit. Ainsi, les bits restants de la zone de codage du nombre d'unités de valeur peuvent être utilisés pour contenir le certificat.

[0042] Plus le nombre d'unités de valeur est grand, plus la valeur codée dans la carte est faible, donc plus la taille mémoire allouée au certificat est importante.

[0043] Il est nécessaire d'indiquer aux terminaux la taille mémoire allouée au certificat pour chaque carte. Pour cela, cette taille est indiquée dans la zone mémoire EEPROM non protégée de la carte, avec le nombre d'unités de valeur et le certificat. Cette indication est présente dans la zone active et dans la zone de copie.

[0044] Selon une autre caractéristique de l'invention le calcul du certificat de la zone active est réalisé de manière différente du calcul du certificat de la zone de copie.

[0045] Il n'est alors plus possible de transférer le contenu de la zone active dans la zone de copie. Un terminal vérifiant une carte dont le contenu de la zone de copie a été transféré dans la zone active sera capable de constater la fraude. Le certificat que le terminal lira dans la zone active ne correspondra pas au calcul opéré dans le cas de la zone active, et correspondra au calcul opéré pour la zone de copie.

[0046] Selon une autre caractéristique de l'invention, pour que le contenu de la zone active d'une carte ne puisse être réutilisé en cas d'arrachement de carte, le compteur de transaction de la carte est également modifié en tout début de transaction. La zone de copie est initialisée avec le nombre d'unités de valeur contenu dans la zone active et avec un certificat tenant compte de la prochaine valeur du compteur de transaction. Puis, le compteur de transaction est modifié à cette nouvelle valeur. A cet instant précis, le contenu de la zone active n'est plus réutilisable, le compteur de transaction ne correspond plus à son certificat. Par contre, la zone de copie est valide.

[0047] Le compteur de transaction est de nouveau modifié en fin de transaction pour éviter que cette transaction ne puisse être refaite, comme indiqué précédemment.

[0048] Le procédé peut concerner également la vérification de la parité de la donnée variant à chaque transaction. Cette donnée qui peut être un compteur de transaction est incrémentée deux fois durant une transaction complète, d'une unité à chaque fois. La parité de la valeur du compteur de transaction est donc identique en début de transaction et en fin de transaction. Si la première valeur du compteur de transaction est paire, la valeur du compteur de transaction est paire en début et en fin de transaction.

[0049] La parité du compteur de transaction doit être vérifiée en début de transaction, la valeur du compteur de transaction doit être paire. Dans le cas où la valeur

du compteur de transaction est impaire en début de transaction, l'intégrité des informations de la zone de copie de la carte doit être directement vérifiée. Si la vérification est réussie, le terminal transfère les données de la zone de copie dans la zone active.

[0050] L'invention va maintenant être décrite dans le cas de l'application à un système de transaction monétaire, le terminal 100 étant un terminal monétaire et la carte 103, une carte porte-monnaie électronique.

[0051] Selon un exemple préféré de réalisation, la structure de données de la mémoire 103 est telle que représentée sur la figure 2. Cette structure ou organisation est bien sûr donnée à titre d'exemple. D'autres organisations peuvent être adaptées.

[0052] La mémoire comporte des données d'identification comprenant :

- une valeur d'identification du circuit (circuit silicium) dans la zone Id circuit,
- un code client dans la zone de référence émetteur de carte (organisme bancaire),
- une donnée d'identification de l'application dans la zone Id Card (donnée par l'émetteur),
- un numéro de série CSN de la carte (donné par exemple par le fabricant).

[0053] La mémoire comporte une zone de compteurs comportant les champs suivants :

- un compteur de fraude incrémenté à chaque vérification d'un certificat s'avérant mauvais.

[0054] Ce compteur est formé de 3 bits selon la réalisation pratique qui a été faite.

- un compteur de transaction CTC.

[0055] Dans un exemple de réalisation, ce compteur CTC est divisé en 5 sous-compteurs de 8 bits (cinq étages de comptage) avec un fonctionnement type boulier tel que décrit par exemple dans le brevet FR 93 10477 publié le 10 mars 1995 sous le N° 2 709 582. Les cinq sous-compteurs sont référencés C1, C8, C64, C512, C4096. Les cellules mémoire de l'étage de comptage C1 ont un poids de 1, ... et celles de l'étage C4096 ont un poids de $4096 = 8^4$.

[0056] Les quatre premiers étages sont du type effaçables, c'est-à-dire que l'on peut effacer des bits qui y sont inscrits et ensuite ré-écrire aux mêmes emplacements. Le cinquième étage C4096 est par contre à écriture uniquement. Seuls 4 bits de ce dernier étage sont utilisés pour le comptage. Parmi les 4 bits restants, 1 bit est utilisé comme fusible et les trois autres bits comme compteur de fraude.

[0057] Deux bits sont grillés par transaction.

[0058] Ainsi, ce type de compteur va permettre de compter 10239 transactions $[7+7 \times 8+7 \times 8^2+7 \times 8^3+4 \times 8^4]/2$.

[0059] La mémoire comporte en outre

- une zone certificat.

[0060] Cette zone ne peut être effacée et sert à l'enregistrement de certification CER permettant l'authentification de la carte. Le certificat d'authentification est enregistré après la configuration du circuit pour l'utilisateur final et est vérifié par le terminal à chaque utilisation de la carte.

[0061] Il est calculé par exemple à partir d'une donnée d'identification ID, d'une fonction à sens unique f_{OP} et d'une clé secrète suivant la formule :

$$CER = f_{OP}(ID, K)$$

[0062] ID est par exemple le contenu des zones d'identification de carte, identification de circuit ou de référence d'émetteur.

- une zone utilisateur.

[0063] Il s'agit de la zone active porte-monnaie électronique et de la zone de copie pour les sauvegardes.

[0064] La zone active contient selon une caractéristique de l'invention une donnée chiffrée du solde Bal et du certificat correspondant Cert. L'information du solde d'unités de valeur correspond à un codage sur un premier nombre constant de bits, et l'information représentative du certificat est codée sur un second nombre constant de bits.

[0065] La donnée chiffrée correspondant à une des deux zones du porte-unités peut s'écrire de la façon suivante :

$$\langle \text{Bal}, \text{Cert} \rangle = E_K(\text{Bal}, \text{Cert})$$

Bal étant le nombre d'unités de valeur et
Cert le certificat correspondant
K étant la clé secrète du terminal
<donnée> la valeur chiffrée
(donnée) la valeur non chiffrée
 E_K l'algorithme de chiffrement.

[0066] Le calcul du certificat permet d'assurer l'intégrité des données du porte-monnaie électronique.

[0067] Les données suivantes sont utilisées dans le calcul :

- la valeur du solde, ce qui rend le certificat unique pour un solde donné,
- des données permanentes de la carte, à savoir les données d'identification (carte et émetteur),
- le compteur de transaction CTC. A chaque transaction deux bits sont grillés dans ce compteur CTC et le compteur peut uniquement être incrémenté ou

uniquement décrémenté. Un bit est grillé au début d'une transaction, un deuxième bit est grillé à la fin de la transaction.

[0068] Selon une des caractéristiques de l'invention, les certificats correspondant à un solde sont calculés par le terminal de la façon suivante :

$$\text{Cert A} = F_A(\text{Bal}, \text{CSN}, \text{CTC})$$

pour la zone active du porte-monnaie
et

$$\text{Cert B} = F_B(\text{Bal}, \text{CSN}, \text{CTC})$$

pour la zone de copie du porte-monnaie.

[0069] F_A et F_B étant des fonctions différentes détenues par le terminal. On pourra par exemple prendre comme fonction un algorithme DES utilisant une clé secrète k détenue par le terminal.

[0070] Lors d'une transaction, l'enregistrement des informations relatives au solde et au certificat dans la zone de copie et dans la zone active se fait suivant le déroulement suivant :

- enregistrement du solde et de son certificat (présents dans la zone active) dans la zone de copie,
- effacement de la zone active,
- écriture du nouveau solde dans la zone active et de son certificat,
- effacement de la zone de copie (effacement de la donnée de sauvegarde).

[0071] Cet enchaînement permet d'éviter toute perte d'information en cas d'arrachement de la carte ou de coupure de courant.

[0072] Les différentes étapes mises en oeuvre par le terminal lors d'une transaction sont représentées par les blocs fonctionnels de la figure 3:

[0073] Le procédé comporte une phase d'initialisation de la transaction et une phase correspondant à la transaction elle-même.

[0074] La phase d'initialisation comporte une vérification de la zone de fraude correspondant aux étapes 50, 51, 52 détaillée dans la suite.

[0075] Cette phase d'initialisation comporte en outre une vérification de la parité de la donnée variant à chaque transaction correspondant sur le schéma de la figure 3 aux étapes 400, 401, 203A, 204A, 205A, 207A.

[0076] Si la première valeur du compteur de transaction est paire, la valeur du compteur de transaction est paire en début et en fin de transaction.

[0077] La parité du compteur de transaction est vérifiée en début de transaction étapes 400, 401, la valeur du compteur de transaction doit être paire.

[0078] Dans le cas où la valeur du compteur de transaction est impaire en début de transaction, l'intégrité des informations de la zone de copie de la carte doit être directement vérifiée 204 A en opérant les étapes 20, 21

et 22 de la figure 4.

[0079] Si la vérification est réussie, le terminal transfère les données de la zone de copie dans la zone active étape 205A. Puis le terminal marque le début d'une transaction dans la carte en incrémentant le compteur CTC. A la suite de cela le terminal repasse à l'étape 401.

[0080] Si la vérification de l'intégrité est négative, le terminal exécute l'étape 206 à savoir incrémentation du compteur de fraude de la carte et éjection de la carte.

[0081] Après la vérification de la parité le terminal lit le contenu de la zone active de la carte (porte-monnaie électronique PM) 150, laquelle comporte la donnée <Bal1, Cert1A>. Bal est le nombre d'unités de valeur initialement stockées dans la carte, et Cert1A est le certificat initialement stocké dans la carte.

[0082] Le terminal vérifie l'intégrité de ces données, étape 200. Pour cela, il déchiffre cette donnée suivant les étapes 20 à 22 détaillées à la figure 4. Si le certificat qu'il a calculé correspond au certificat de la carte, alors la vérification a réussi. La transaction se poursuit 201, 202, 300.

[0083] Le terminal met à jour le solde dans la carte et calcule une nouvelle donnée chiffrée 301 et 302. La mise à jour est réalisée suivant les étapes 30 à 35 illustrées sur la figure 6.

[0084] Dans le cas où l'intégrité des données de la zone active n'est pas vérifiée, le terminal lit la zone de copie qui contient <Bal1, Cert1B> 203.

[0085] Le terminal vérifie l'intégrité des données de sauvegarde 204 par déchiffrement de ces données en opérant les étapes 20, 21 et 22 de la figure 4 sur ces données.

[0086] Si le certificat calculé est égal au certificat de cette zone Cert1B==Cert1b, alors les données sont intègres, le terminal restaure cette donnée de sauvegarde dans la zone active qui ne contenait rien ou une donnée erronée 205.

[0087] Dans le cas où les données contenues dans la zone de copie ne sont pas intègres, alors le terminal inscrit un bit dans la zone de fraude 206.

[0088] Selon l'application, une ou plusieurs tentatives de fraude peuvent être acceptées avant de refuser définitivement la carte.

[0089] Lorsque la zone de fraude est pleine, la carte est avalée. Le contrôle de la zone de fraude se fait lors d'une étape préalable à la transaction au tout début de l'initialisation de la transaction 50, 51, 52.

[0090] La figure 5, illustre les étapes préalables 200, 201 et 202 à la mise en oeuvre d'une transaction. On pourra préférentiellement utiliser des fonctions différentes FA et FB pour le calcul des certificats.

[0091] A l'étape 200 (ou 204 ou 204A), le terminal effectue les opérations développées sur la figure 4.

[0092] Le terminal opère le déchiffrement du contenu de la zone active (ou de copie). (20)

[0093] Dans le cas de l'étape 200,

[0094] Il calcule ensuite le certificat Cert1A correspondant au solde (Bal1) de cette zone. (21)

[0095] Il opère la vérification d'intégrité. (22)

[0096] A l'étape 201 :

- le terminal calcule le certificat (Cert1B) pour la zone de sauvegarde; (23)
- il chiffre la donnée (Bal1, Cert1B); (24)
- il sauvegarde dans la zone de copie de la carte la valeur chiffrée. (25)

[0097] A l'étape 202 :

- le terminal incrémente le compteur CTC; (26)
- il efface le contenu de la zone active. (27)

[0098] Dans le cas des étapes 204 ou 204A, le terminal calcule ensuite le certificat Cert 1B correspondant au solde Bal de cette zone (21). Il opère la vérification d'intégrité (22). Le terminal calcule le certificat Cert 1A pour la zone active (23), il chiffre la donnée Bal, Cert 1A (24), il sauvegarde dans la zone active de la carte la valeur chiffrée (25). Puis le terminal incrémente le compteur CTC (26) et efface le contenu de la zone de copie (27).

[0099] La figure 6, illustre les étapes de mise à jour du solde (301) lors d'une transaction et la fin de la transaction (302).

[0100] L'ancien solde Bal est modifié d'une valeur x (en plus ou en moins selon la transaction opérée) pour donner le nouveau solde Bal2 tel que :

[0101] $Bal2 = Bal1 \pm x$ (30), x étant la valeur de la transaction.

[0102] Le terminal calcule un nouveau certificat tenant compte de ce nouveau solde, et de la nouvelle valeur du compteur de transaction CTC+1 :

$$Cert2_A = F_A(Bal2, Card Id, CTC+1) \quad (31)$$

[0103] Le terminal effectue le chiffrement de ces nouvelles données :

$$\langle Bal2, Cert2_A \rangle = E_K(Bal2, Cert2_A) \quad (32)$$

[0104] Le terminal enregistre dans la zone active de la carte cette nouvelle donnée chiffrée. (33)

[0105] La zone de copie de la carte contient l'ancienne donnée, c'est-à-dire <Bal1, Cert1B>. Le terminal incrémente le compteur de transaction CTC de la carte en grillant un second bit pour valider la transaction. (34)

[0106] Le terminal efface la zone de copie (35) et commande l'éjection de la carte.

Revendications

1. Procédé de stockage d'unités de valeur dans une

carte à puce pour la réalisation de transactions à partir d'un terminal, la carte comprenant une mémoire non volatile de type EEPROM (103), comportant une zone active (ZA) susceptible de contenir des informations relatives au nombre d'unités de valeur de la carte pour une application donnée et à un certificat destiné à la zone active et calculé par le terminal à partir de ce nombre, la mémoire comportant également une zone de copie (ZC) destinée à contenir des informations de sauvegarde de la zone active,

caractérisé en ce qu'il comporte les étapes suivantes :

- l'enregistrement dans la zone de copie (ZC) dans la phase d'initialisation d'une transaction de l'information relative au nombre d'unités de valeur de la carte pour une application donnée présent dans la zone active et d'une information relative à un certificat destiné à la zone de copie calculé à partir de ce nombre, les informations relatives au nombre d'unités de valeur présent dans la zone active et au certificat destiné à la zone de copie étant chiffrées et enregistrées chiffrées dans la zone de copie (ZC) ;
- l'enregistrement dans la zone active (ZA) lors de la transaction d'informations relatives à un nouveau nombre d'unités de valeur de la carte pour une application donnée et à un nouveau certificat destiné à la zone active calculé par le terminal à partir de ce nouveau nombre d'unités de valeur, les informations relatives au nouveau nombre d'unités de valeur et au nouveau certificat destiné à la zone active étant chiffrées et enregistrées chiffrées dans la zone active.

2. Procédé de stockage selon la revendication 1, **caractérisé en ce que** les opérations de chiffrement sont réalisées au moyen d'un algorithme de chiffrement Ek et d'une clé secrète K par le terminal de transaction.

3. Procédé de stockage selon l'une quelconque des revendications précédentes **caractérisé en ce que** le certificat destiné à la zone active (CertA) est calculé en utilisant une première fonction (FA), et **en ce que** le certificat destiné à la zone de copie (CertB) est calculé en utilisant une autre fonction (FB).

4. Procédé de stockage selon la revendication 3 **caractérisé en ce que** :

- dans la phase d'initialisation de la transaction, les informations relatives au nombre d'unités de valeur de la carte pour une application donnée présent dans la zone active et relatives au

certificat (CertB) destiné à la zone de copie calculé à partir de ce nombre sont chiffrées selon une première opération de chiffrement,

- lors de la transaction, les informations relatives au nouveau nombre d'unités de valeur de la carte pour une application donnée et au nouveau certificat (CertA) destiné à la zone active calculé par le terminal à partir de ce nouveau nombre d'unités de valeur sont chiffrées selon une seconde opération de chiffrement.

5. Procédé selon l'une des revendications précédentes **caractérisé en ce que** dans la phase d'initialisation de la transaction :

- on calcule le certificat destiné à la zone de copie à partir du nombre d'unités de valeur présent dans la zone active et d'une valeur d'un compteur de transaction incrémentée à sa prochaine valeur,
- le compteur de transaction est ensuite incrémenté à cette nouvelle valeur de sorte qu'après enregistrement des informations dans la zone de copie, le certificat de la zone active n'est plus en accord avec la valeur du compteur, seules les informations de sauvegarde étant correctes.

6. Procédé selon la revendication précédente selon lequel la valeur du compteur de transaction est utilisée dans le calcul des certificats, la parité de la valeur du compteur de transaction étant identique dans la phase d'initialisation et en fin de transaction et la valeur du compteur de transaction étant incrémentée deux fois durant la transaction, chaque incrémentation étant d'une seule unité.

7. Procédé selon la revendication précédente **caractérisé en ce que**, dans la phase d'initialisation de la transaction, on lit la valeur du compteur de transaction de la carte, si la valeur lue est paire, on lit les informations de la zone active (ZA), on vérifie l'intégrité des informations de la zone active, l'intégrité des informations de la zone active est vérifiée, on procède au stockage d'unités de valeur dans la carte à puce.

8. Procédé selon la revendication 6 **caractérisé en ce que**, dans la phase d'initialisation d'une transaction, on lit la valeur du compteur de transaction de la carte, si la valeur lue est impaire, on lit les informations de la zone de copie (ZC), on vérifie l'intégrité des informations de la zone de copie, l'intégrité des informations de copie est vérifiée, on calcule un certificat à partir du nombre d'unités de valeur présent dans la zone de copie (ZC) et de la valeur du compteur de transaction incrémentée à sa prochaine valeur paire, la donnée obtenue est chiffrée et enre-

gistrée en zone active (ZA), le compteur est ensuite incrémenté à cette nouvelle valeur de sorte qu'à cet instant, le certificat de la zone de copie (ZC) n'est plus en accord avec la valeur du compteur, seule la donnée de la zone active étant correcte.

9. Terminal de transaction utilisant des cartes à puce comprenant une mémoire non volatile de type EEPROM (103) comportant une zone active (ZA) susceptible de contenir des informations relatives au nombre d'unités de valeur de la carte pour une application donnée et à un certificat destiné à la zone active et calculé par le terminal à partir de ce nombre, la mémoire comportant également une zone de copie (ZC) destinée à contenir des informations de sauvegarde de la zone active, **caractérisé en ce que** le terminal comporte un moyen de chiffrement pour chiffrer dans la phase d'initialisation d'une transaction l'information relative au nombre d'unités de valeur de la carte pour une application donnée présente dans la zone active et une information relative à un certificat destiné à la zone de copie calculé à partir de ce nombre, et pour chiffrer lors de la transaction des informations relatives à un nouveau nombre d'unités de valeur de la carte pour une application donnée et à un nouveau certificat destiné à la zone active calculé par le terminal à partir de ce nouveau nombre d'unités de valeur, et un moyen pour enregistrer dans la zone de copie les données chiffrées dans la phase d'initialisation et pour enregistrer dans la zone active les informations chiffrées lors de la transaction.

Patentansprüche

1. Speicherverfahren von Wertseinheiten in einer Chipkarte zur Durchführung von Transaktionen von einem Terminal aus, wobei die Karte einen nicht flüchtigen Speicher des Typs EEPROM (103) umfasst, mit einem aktiven Bereich (ZA), der Informationen bezüglich der Anzahl von Wertseinheiten der Karte für eine bestimmte Applikation und bezüglich eines Zertifikats enthalten kann, das für den aktiven Bereich bestimmt ist und vom Terminal ab dieser Anzahl berechnet wird, wobei der Speicher ebenfalls einen Kopiebereich (ZC) umfasst, der Sicherungsinformationen des aktiven Bereichs enthalten soll, **dadurch gekennzeichnet, dass** es aus den folgenden Schritten besteht:
- Aufzeichnen in dem Kopiebereich (ZC) während der Initialisierungsphase einer Transaktion der Information bezüglich der im aktiven Bereich vorhandenen Anzahl von Wertseinheiten der Karte für eine bestimmte Applikation und einer ab dieser Anzahl berechneten Information bezüglich eines Zertifikats für den Kopiebereich

reich, wobei die Informationen bezüglich der im aktiven Bereich vorhandenen Anzahl von Wertseinheiten und bezüglich des Zertifikats für den Kopiebereich verschlüsselt und im Kopiebereich (ZC) verschlüsselt eingetragen werden;

- Aufzeichnen in dem aktiven Bereich (ZA) während der Transaktion von Informationen bezüglich einer neuen Anzahl von Wertseinheiten der Karte für eine bestimmte Applikation und bezüglich eines neuen Zertifikats für den aktiven Bereich, das vom Terminal ab dieser neuen Anzahl von Wertseinheiten berechnet wird, wobei die Informationen bezüglich der neuen Anzahl von Wertseinheiten und des neuen Zertifikats für den aktiven Bereich verschlüsselt und im aktiven Bereich verschlüsselt eingetragen werden.
2. Speicherverfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Verschlüsselungsoperationen anhand eines Verschlüsselungsalgorithmus Ek und eines Geheimschlüssels K vom Transaktionsterminal durchgeführt werden.
3. Speicherverfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** das Zertifikat für den aktiven Bereich (CertA) unter Verwendung einer ersten Funktion (FA) berechnet wird, und dass das Zertifikat für den Kopiebereich (CertB) unter Verwendung einer anderen Funktion (FB) berechnet wird.
4. Speicherverfahren nach Anspruch 3, **dadurch gekennzeichnet, dass:**
- während der Initialisierungsphase der Transaktion die Informationen bezüglich der im aktiven Bereich vorhandenen Anzahl von Wertseinheiten der Karte für eine bestimmte Applikation und bezüglich des ab dieser Anzahl berechneten Zertifikats (CertB) für den Kopiebereich gemäß einer ersten Verschlüsselungsoperation verschlüsselt werden,
 - während der Transaktion die Informationen bezüglich der neuen Anzahl von Wertseinheiten der Karte für eine bestimmte Applikation und bezüglich des neuen Zertifikats (CertA) für den aktiven Bereich, das vom Terminal ab dieser neuen Anzahl von Wertseinheiten berechnet wurde, gemäß einer zweiten Verschlüsselungsoperation verschlüsselt werden.
5. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** während der Initialisierungsphase der Transaktion:
- das Zertifikat für den Kopiebereich ab der im aktiven Bereich vorhandenen Anzahl von Wertseinheiten und ab einem Wert eines um seinen

- nächsten Wert inkrementierten Transaktionszählers berechnet wird,
- der Transaktionszähler dann um diesen neuen Wert inkrementiert wird, so dass nach dem Aufzeichnen der Informationen im Kopiebereich das Zertifikat des aktiven Bereichs nicht mehr mit dem Wert des Zählers übereinstimmt, wobei nur die Sicherungsinformationen richtig sind.
6. Verfahren nach dem vorangehenden Anspruch, nach dem der Wert des Transaktionszählers für die Berechnung der Zertifikate verwendet wird, wobei die Parität des Werts des Transaktionszählers während der Initialisierungsphase und am Ende der Transaktion identisch ist, und wobei der Wert des Transaktionszählers während der Transaktion zwei Mal inkrementiert wird, wobei jede Inkrementierung um eine einzige Einheit erfolgt.
7. Verfahren nach dem vorangehenden Anspruch, **dadurch gekennzeichnet, dass** man während der Initialisierungsphase der Transaktion den Wert des Transaktionszählers der Karte liest, wenn der gelesene Wert gerade ist, man die Informationen des aktiven Bereichs (ZA) liest, man die Unversehrtheit der Informationen des aktiven Bereichs überprüft, die Unversehrtheit der Informationen des aktiven Bereichs überprüft wird, man die Werteinheiten in der Chipkarte speichert.
8. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** man während der Initialisierungsphase einer Transaktion den Wert des Transaktionszählers der Karte liest, wenn der gelesene Wert ungerade ist, man die Informationen des Kopiebereichs (ZC) liest, man die Unversehrtheit der Informationen des Kopiebereichs überprüft wird, man ein Zertifikat berechnet ab der im Kopiebereich (ZC) vorhandenen Anzahl von Werteinheiten und ab dem um seinen nächsten geraden Wert inkrementierten Wert des Transaktionszählers, die erhaltene Information verschlüsselt und im aktiven Bereich (ZA) aufgezeichnet wird, der Zähler dann um diesen neuen Wert inkrementiert wird, so dass das Zertifikat des Kopiebereichs (ZC) nicht mehr mit dem Wert des Zählers übereinstimmt, wobei nur die Information des aktiven Bereichs richtig ist.
9. Transaktionsterminal, das Chipkarten benutzt, die einen nicht flüchtigen Speicher des Typs EEPROM (103) umfassen, mit einem aktiven Bereich (ZA), der Informationen bezüglich der Anzahl von Werteinheiten der Karte für eine bestimmte Applikation und bezüglich eines Zertifikats enthalten kann, das für den aktiven Bereich bestimmt ist und vom Terminal ab dieser Anzahl berechnet wird, wobei der

Speicher ebenfalls einen Kopiebereich (ZC) umfasst, der Sicherungsinformationen des aktiven Bereichs enthalten soll, **dadurch gekennzeichnet, dass** das Terminal ein Verschlüsselungsmittel umfasst, um während der Initialisierungsphase einer Transaktion die Information bezüglich der im aktiven Bereich vorhandenen Anzahl von Werteinheiten der Karte für eine bestimmte Applikation und eine Information bezüglich eines ab dieser Anzahl errechneten Zertifikats für den Kopiebereich zu verschlüsseln, und um während der Transaktion Informationen bezüglich einer neuen Anzahl von Werteinheiten der Karte für eine bestimmte Applikation und bezüglich eines neuen Zertifikats für den aktiven Bereich, das vom Terminal ab dieser neuen Anzahl von Werteinheiten berechnet wird, zu verschlüsseln, sowie ein Mittel zum Aufzeichnen im Kopiebereich der während der Initialisierungsphase verschlüsselten Daten und zum Aufzeichnen im aktiven Bereich der während der Transaktion verschlüsselten Informationen.

Claims

1. A method for storing units of value in a smart card for performing transactions using a terminal, the card comprising a non-volatile memory of the EEPROM type (103), comprising an active area (ZA) able to contain information relating to the number of units of value in the card for a given application and a certificate intended for the active area and calculated by the terminal from this number, the memory also comprising a copying area (ZC) intended to contain backup information from the active area, **characterised in that** it comprises the following steps:
 - the recording in the copying area (ZC) in the initialisation phase of a transaction on the information relating to the number of units of value in the card for a given application present in the active area and information relating to a certificate intended for the copying area calculated from this number, the information relating to the number of units of value present in the active area and to the certificate intended for the copying area being enciphered and recorded enciphered in the copying area (ZC);
 - the recording in the active area (ZA) during the transaction of information relating to a new number of units of value in the card for a given application and to a new certificate intended for the active area calculated by the terminal from this new number of units of value, the information relating to the new number of units of value and to the new certificate intended for the active

area being enciphered and recorded enciphered in the active area.

2. A storage method according to Claim 1, **characterised in that** the enciphering operations are performed by the transaction terminal by means of an enciphering algorithm Ek and a secret key K. 5
3. A storage method according to any one of the preceding claims, **characterised in that** the certificate intended for the active area (CertA) is calculated using a first function (FA), and **in that** the certificate intended for the copying area (CertB) is calculated using another function (FB). 10
4. A storage method according to Claim 3, **characterised in that:** 15
 - in the transaction initialisation phase, the information relating to the number of units of value in the card for a given application present in the active area and relating to the certificate (CertB) intended for the copying area calculated from this number is enciphered according to a first enciphering operation, 20
 - during the transaction, the information relating to the new number of units of value in the card for a given application and to the new certificate (CertA) intended for the active area calculated by the terminal from this new number of units of value is enciphered according to a second enciphering operation. 25
5. A method according to one of the preceding claims, **characterised in that**, in the transaction initialisation phase: 30
 - the certificate intended for the copying area is calculated from the number of units of value present in the active area and a value of a transaction counter incremented to its next value, and the transaction counter is then incremented to this new value so that, after recording of the information in the copying area, the certificate of the active area is no longer in agreement with the value of the counter, only the backup information being correct. 35
6. A method according to the preceding claim, according to which the value of the transaction counter is used in calculating the certificates, the parity of the value of the transaction counter being identical in the initialisation phase and at the end of the transaction and the value of the transaction counter being incremented twice during the transaction, each incrementation being by a single unit. 40
7. A method according to the preceding claim, **characterised in that**, in the transaction initialisation phase, the value of the transaction counter of the card is read, if the value read is even, the information in the active area (ZA) is read, the integrity of the information in the active area is checked, and the integrity of the information in the active area is checked, the storage of units of value in the smart card is proceeded with. 45
8. A method according to Claim 6, **characterised in that**, in the phase of initialisation of a transaction, the value of the transaction counter of the card is read and, if the value read is odd, the information in the copying area (ZC) is read, the integrity of the information in the copying area is verified, the integrity of the copying information is verified, a certificate is calculated from the number of units of value present in the copying area (ZC) and the value of the transaction counter incremented to its next even value, the data obtained is enciphered and recorded in the active area (ZA), and the counter is then incremented to this new value so that, at this moment, the certificate of the copying area (ZC) is no longer in agreement with the value of the counter, only the data of the active area being correct. 50
9. A transaction terminal using smart cards comprising a non-volatile memory of the EEPROM type (103) comprising an active area (ZA) able to contain information relating to the number of units of value in the card for a given application and to a certificate intended for the active area and calculated by the terminal from this number, the memory also comprising a copying area (ZC) intended to contain backup information from the active area, **characterised in that** the terminal comprises an enciphering means for enciphering, in the initialisation phase of a transaction, the information relating to the number of units of value in the card for a given application present in the active area and information relating to a certificate intended for the copying area calculated from this number, and for enciphering, during the transaction, information relating to a new number of units of value in the card for a given application and to a new certificate intended for the active area calculated by the terminal from this new number of units of value, and a means for recording in the copying area the data enciphered in the initialisation phase and for recording in the active area the information enciphered during the transaction. 55

FIG_1

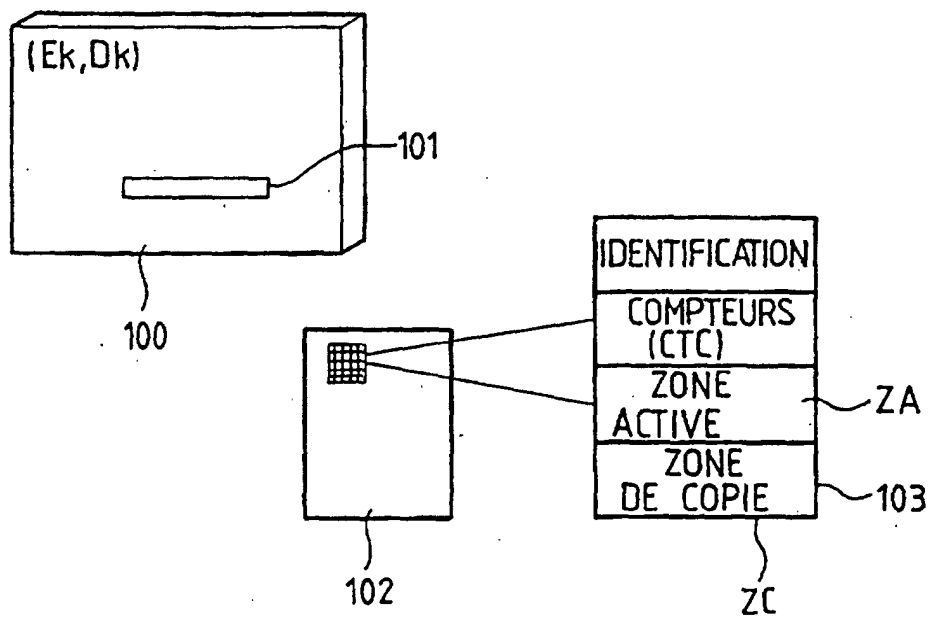


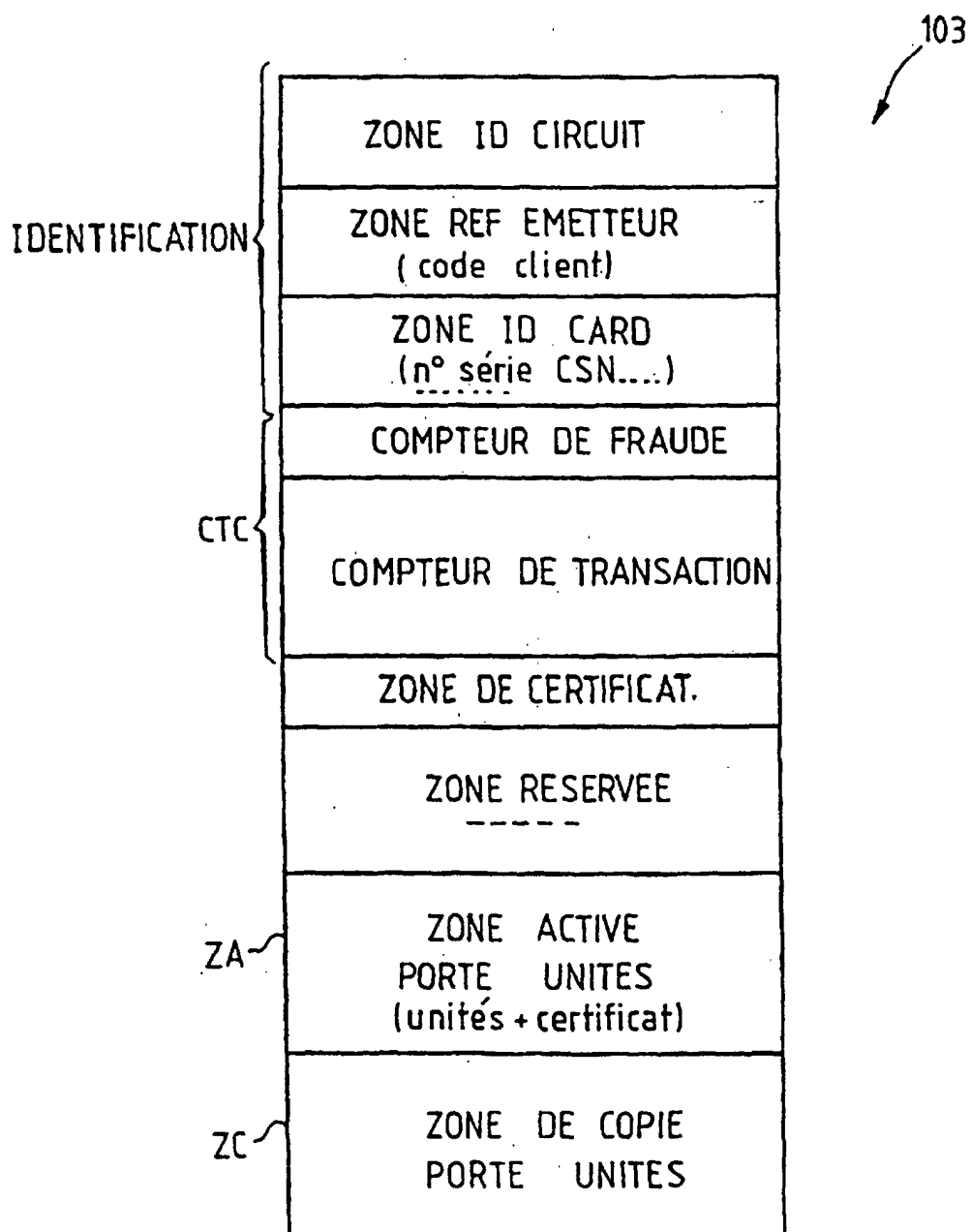
FIG. 2

FIG. 3

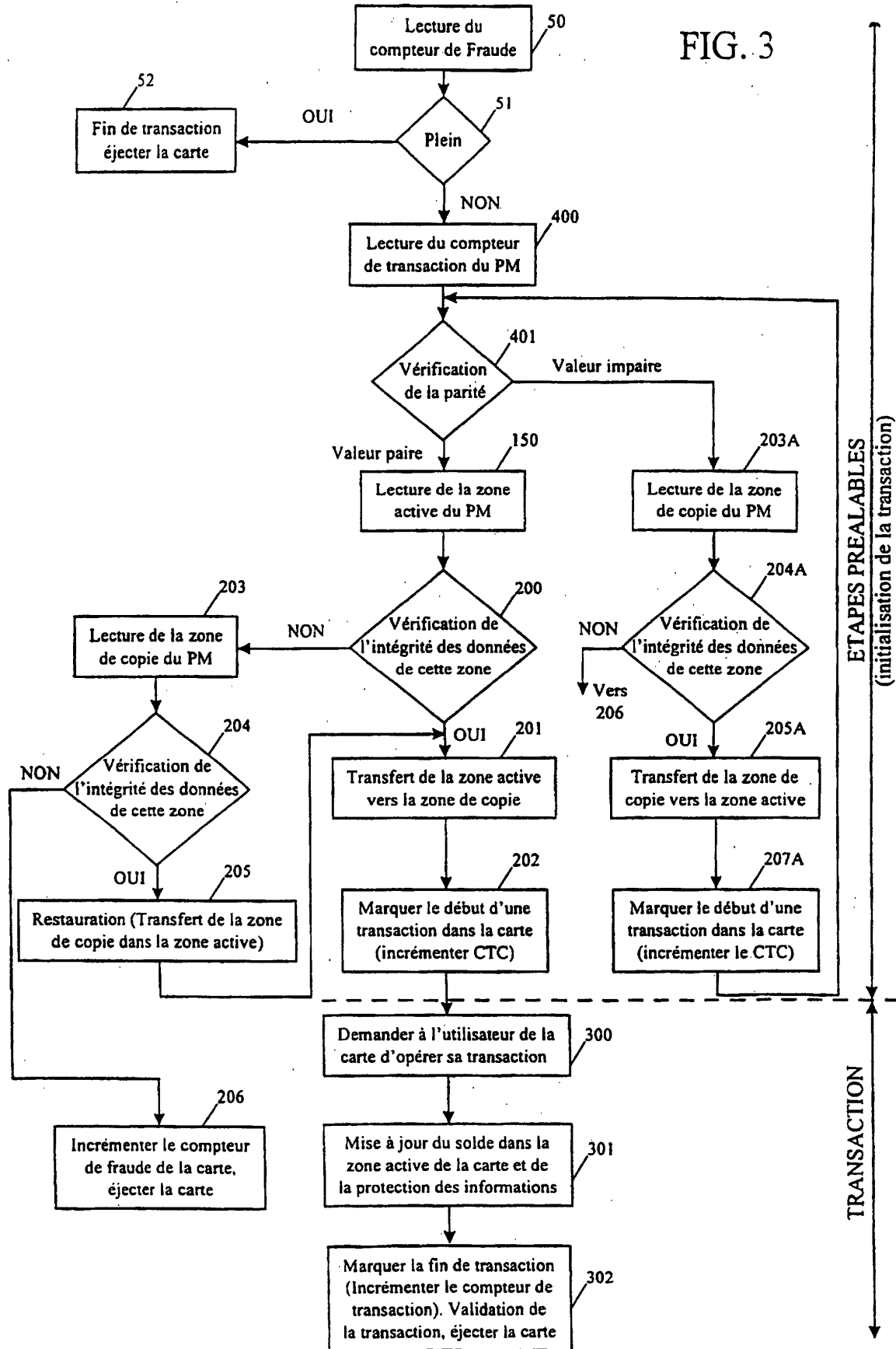


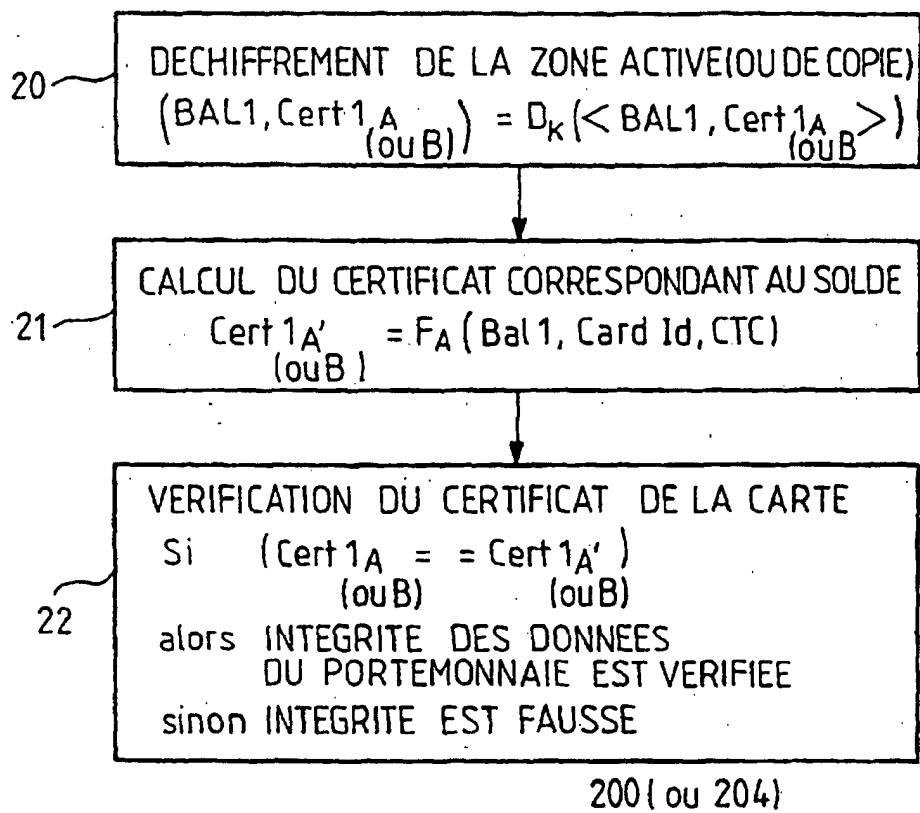
FIG_4

FIG. 5

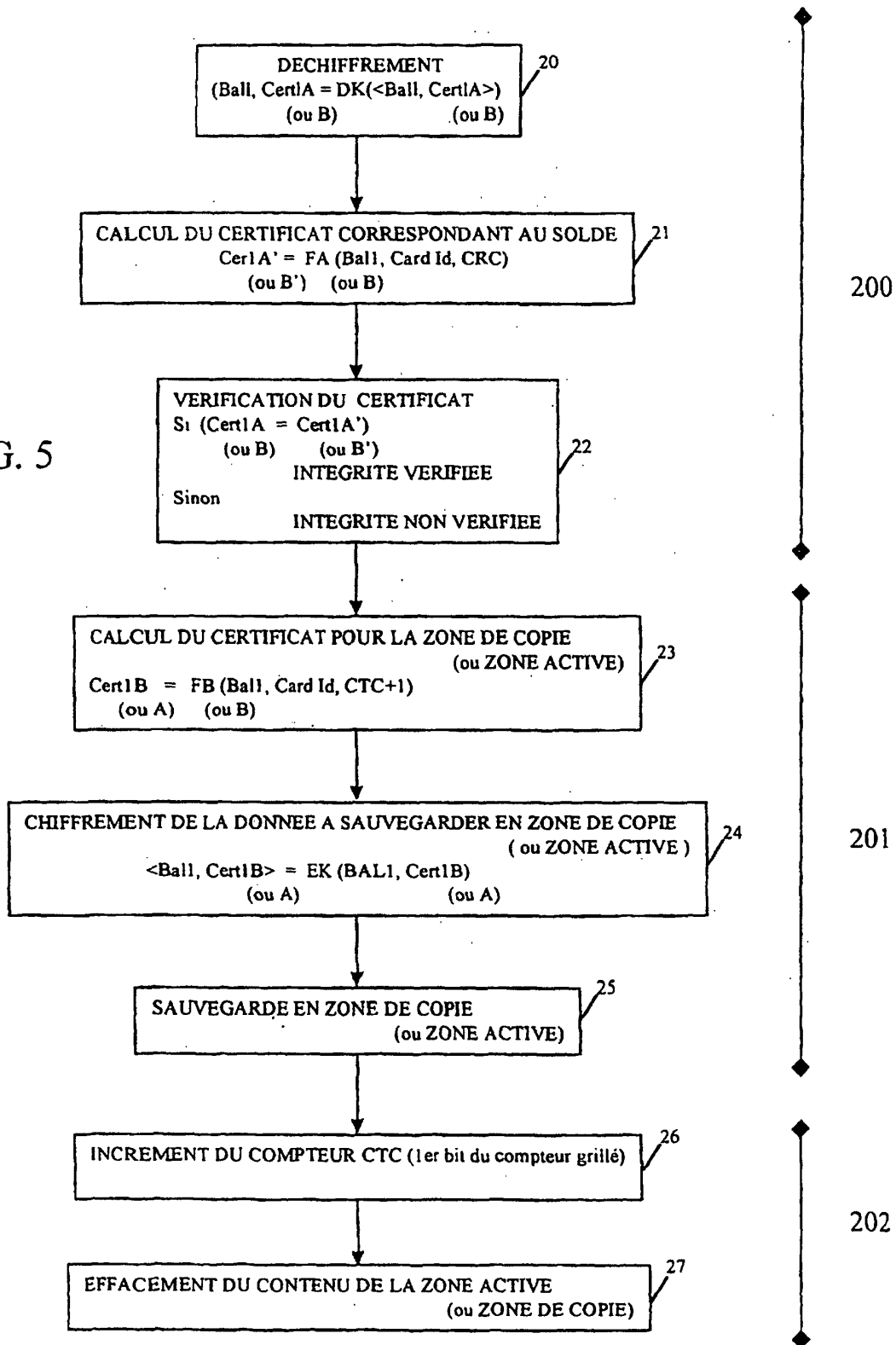


FIG_6