(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 809 847**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 07248**

(51) Int Cl[7] : **G 06 K 19/07,** G 06 F 9/06

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 06.06.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 07.12.01 Bulletin 01/49.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *GEMPLUS Société en commandite par actions* — FR.

(72) **Inventeur(s) :** CHEW GARY et SPORCIC TIM.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

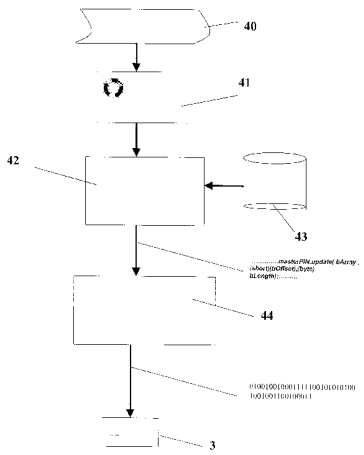
(54) PROCEDE DE PERSONNALISATION ELECTRIQUE DE CARTE A PUCE.

(57) L'invention concerne un procédé de personnalisation électrique de cartes à puce, consistant à mémoriser des données personnalisées dans chaque puce de carte à puce (3). Le procédé comprend l'étape suivante:

- écriture d'un programme applicatif en code source (40) dans un langage évolué.

Il se caractérise en ce qu'il comprend les étapes de:

- substitution (42) de variables à personnaliser dans le programme applicatif en code source par des données de personnalisation propres à ladite chaque carte, en un programme applicatif en code source personnalisé;
- compilation (44) du programme applicatif en code source personnalisé;
- chargement dans la carte à puce (3) du programme applicatif en code source personnalisé préalablement compilé.



FR 2 809 847 - A1

2809847

PROCEDE DE PERSONALISATION ELECTRIQUE DE CARTE A PUCE

La présente invention concerne de manière générale les cartes à puce. Plus précisément, l'invention concerne un procédé de personnalisation électrique d'une carte à puce, et s'applique en particulier à la personnalisation des cartes à puce de plate-forme ouverte. Une carte à puce est du type défini par les Recommandations ISO- 7816.

La personnalisation d'une carte à puce peut typiquement être réalisée sous deux formes, ou bien par « personnalisation physique » ou bien par « personnalisation électrique ».

La personnalisation physique consiste, à titre d'exemple, ou bien à inscrire sur le corps de la carte, typiquement par technique laser, les données d'identification de l'usager, un numéro d'identification bancaire, une date limite de validité de la carte bancaire, ou bien à imprimer sur le corps de la carte par technique offset ou jet d'encre un motif ou dessin particulier.

La personnalisation électrique consiste, pour sa part, à mémoriser dans la puce de la carte des données particulières propres à un usager ou un groupe d'usagers donné, telles que la valeur d'unités initiales pour une application de porte-monnaie électronique, un code secret propre à l'usager, etc...

Une puce d'une carte à puce est un composant électronique comprenant au moins une zone de mémoire et une unité de traitement, ces zone de mémoire et une unité de traitement formant partie des ressources matérielles de la puce.

La puce mémorise avantageusement, en outre, un système d'exploitation. Ce système d'exploitation est défini comme un logiciel, ou une interface logicielle, d'accès aux et de gestion des ressources matérielle (mémoires, unité d'entrée/sortie, interruptions, etc....) de la puce. Les ressources physiques sont en quelque sorte traduites par le système d'exploitation sous la forme de « ressources logiques », telles que des commandes élémentaires. Lorsqu'un programme applicatif déterminé est exécuté par la puce de la carte, le système d'exploitation est mis à contribution.

Selon une première technique connue selon la technique antérieure, la personnalisation électrique est mise en œuvre de la manière suivante. Comme montré dans la Figure 1, elle fait appel à deux étapes successives de chargement

de l'application 1 dans la carte à puce 3, puis de personnalisation 2 à proprement parté. Pour donner plus de détails, la personnalisation est réalisée de la manière suivante :

- **1** - Un logiciel applicatif, par exemple de type porte-monnaie électronique, est développé dans un langage donné, ce logiciel définira les fonctions élémentaires du porte-monnaie électronique (crédit, débit, accès sécurisé, etc...) .
- **2** - Des données de personnalisation sont définies et créées. Cela comprend la préparation des données, leur formatage dans un format approprié. Ces données sont par exemple, la valeur initiale d'unités élémentaires ayant valeur financière du porte-monnaie électronique, un code secret, un nombre limite de saisi par l'usager d'un code secret avant rejet de l'opération, etc...
- **3** – Le logiciel de personnalisation est également créé. Il prend en compte le format des données de personnalisation créées selon le point 2. Ce logiciel de personnalisation est destiné à opérer après son chargement dans une machine de personnalisation . Cette machine assure la mise en contact électrique de bornes de connexion de la puce et de bornes d'alimentation et de communication de la machine.
- **4** – Une fois la carte correctement positionnée dans la machine, elle se trouve alimentée et ses bornes d'échanges de données sont mises en contact avec des bornes d'échanges de données de la machine. La carte est réinitialisée. Une étape d'authentification prend place entre la machine commandée par le logiciel de personnalisation et la carte à puce. Une session de d'échange de données est ensuite établie entre la carte et la machine . La carte et la machine communique alors selon un protocole prédéterminée. Le logiciel de personnalisation télécharge alors le logiciel applicatif dans la carte. Puis, ce même logiciel de personnalisation télécharge les données de personnalisation propres à la carte en cours de personnalisation.

L'inconvénient principal de cette solution selon la technique antérieure est de faire appel à deux étapes : une étape de téléchargement d'un logiciel applicatif identique pour toutes les cartes, puis une étape de téléchargement de données personnalisées dans la carte. Cela induit une durée relativement longue du procédé de personnalisation. En outre, deux étapes successives d'échange de

données entre la carte et la machine étant nécessaires, il y'a un risque de téléchargement d'informations erronées.

Une solution connue de la technique antérieure, illustrée schématiquement dans la Figure 2, remédie à ce problème en prévoyant une seule étape d'échange de données entre la machine de personnalisation et la carte. Dans ce cas, les étapes suivantes sont prévues.

- **1** - Un logiciel applicatif, est développée dans un langage donné, en donnant aux variables (exemple : x, y ,z) de données personnalisées des valeurs particulières identifiables (exemple : 10101010, 11111111, 00000000).
- **2** – Ce logiciel applicatif est compilé. Il comprend alors, comme montré dans la Figure 2, un portion de logiciel en code objet et des chaînes de valeurs binaires, chaque chaîne correspondant à une valeur particulière identifiable dans le logiciel applicatif.
- **3** – Un traitement de personnalisation du logiciel applicatif compilé est alors mis en œuvre. Ce traitement comprend la reconnaissance des chaînes de valeurs binaires particulières (exemple : 10101010, 11111111, 00000000), puis pour chaque carte à personnaliser, le remplacement de ces chaîne de valeurs binaires particulières par les données de personnalisation propres à la carte en cours de personnalisation.
- **4** - La carte est réinitialisée. Une étape d'authentification prend place entre la machine commandée par un logiciel de téléchargement et la carte à puce. Une session d'échange de données est ensuite établie entre la carte et la machine . La carte et la machine communique alors selon un protocole prédéterminé. Le logiciel de téléchargement télécharge dans la carte le logiciel applicatif compilé qui a été préalablement personnalisé selon le point 3 précité.

La solution décrite ci-dessus présente l'inconvénient d'une longue mise au point pour s'assurer que les chaînes de valeurs binaires (10101010, 11111111, 00000000) seront parfaitement reconnues de façon non ambiguë dans le logiciel applicatif compilé, et garantir ainsi que les données de personnalisation les remplaçant seront bien inscrites à la position exacte qui leur est réservée dans le logiciel applicatif compilé.

L'invention vise donc à remédier aux inconvénients précités en fournissant un procédé de personnalisation électrique de carte à puce.

Selon une première variante de l'invention relative à un programme applicatif compilable, le procédé de personnalisation électrique de cartes à puce, consistant à mémoriser des données personnalisées dans chaque puce de carte à puce, comprend l'étape suivante :

- écriture d'un programme applicatif en code source dans un langage évolué.

Il se caractérise en ce qu'il comprend les étapes de :

- substitution de variables à personnaliser dans le programme applicatif en code source par des données de personnalisation propres à ladite chaque carte, en un programme applicatif en code source personnalisé ;
- compilation du programme applicatif en code source personnalisé ;
- chargement dans la carte à puce du programme applicatif en code source personnalisé et préalablement compilé.

Selon une seconde variante de l'invention relative à un programme applicatif interprétable, de type Javacard, le procédé de personnalisation électrique de cartes à puce, consiste à mémoriser des données personnalisées dans chaque puce de carte à puce. Il comprend l'étape suivante :

- écriture d'un programme applicatif en code source dans un langage interprétable;

Il se caractérise en ce qu'il comprend les étapes de :

- reconnaissance de caractères particuliers dans le programme applicatif en code source;
- substitution de variables à personnaliser dans le programme applicatif en code source par des données de personnalisation propres à ladite chaque carte, en un programme applicatif en code source personnalisé ;
- chargement dans la carte à puce du programme applicatif en code source personnalisé.

La reconnaissance de caractères particuliers étant réalisée selon l'invention dans le programme applicatif en code source, tous les inconvénients relatifs à la

reconnaissance des chaînes de valeurs binaires particulières sont supprimés, la reconnaissance étant réalisée sur des caractères particuliers de type caractères ASCII. Il en résulte alors une réduction extrêmement importante des risques d'erreurs et de mise au point, le nombre de caractères ASCII étant très supérieur au nombre de caractères binaires qui est lui limité à deux caractères (ou bien « 0 » ou bien « 1 »).

Ainsi, la reconnaissance de caractères particuliers étant réalisée selon l'invention dans le programme applicatif en code source, tous les inconvénients relatifs à la reconnaissance des chaînes de valeurs binaires particulières sont supprimés, la reconnaissance étant réalisée sur des caractères particuliers de type caractères ASCII. Il en résulte alors une réduction extrêmement importante des risques d'erreurs et de mise au point, le nombre de caractères ASCII étant très supérieur au nombre de caractères binaires qui est limité en nombre à deux (ou bien « 0 » ou bien « 1 »).

Avantageusement, l'étape de substitution est précédée par une étape de reconnaissance de caractères identifiant des zones délimitant lesdites variables dans le programme applicatif en code source.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description qui suit, en référence aux dessins annexés correspondants dans lesquels :

- la Figure 1, déjà commentée, est une représentation schématique d'un premier procédé de personnalisation de carte à puce selon la technique antérieure ;
- la Figure 2, également déjà commentée, est une représentation schématique d'un premier procédé de personnalisation de carte à puce selon la technique antérieure ;
- la Figure 3 est un bloc-diagramme schématique d'un procédé de personnalisation de carte à puce selon l'invention ; et
- la Figure 4 montre un extrait d'un programme applicatif ainsi qu'un enregistrement élémentaire d'une base de données de personnalisation, pour expliquer la mise en œuvre de la présente invention.

En référence aux Figures 3 et 4, un procédé de personnalisation de cartes à puce selon l'invention met en œuvre les étapes suivantes.

Initialement, un programme applicatif en code source **40** est écrit dans un langage évolué. Ce langage évolué se caractérise par des instructions compactes assimilables par l'Homme. Il peut être un langage évolué à proprement parlé ou un langage dit interprétable.

Un extrait de langage évolué donné seulement à titre d'exemple est montré dans la partie gauche de la Figure 4. Ce langage évolué est traité par une unité de reconnaissance de caractères **41**, cette unité de reconnaissance étant typiquement réalisée sous forme logicielle. Cette unité de reconnaissance **41** a pour fonction d'identifier des caractères particuliers, ici notés « **<** » et « **>** » (voir Figure 4) dans le programme applicatif en code source **40**. Comme cela est représentées par les zones grises de l'extrait de langage montré dans la partie gauche de la Figure 4, l'unité de reconnaissance identifie les zones délimitées par un caractère « **<** » d'une part et par un caractère « **>** » d'autre part, ces zones délimitant des définitions de variables dans le programme applicatif en code source **40**.

Une base de données identifiée par la référence **43** dans la Figure 3 mémorise les données de personnalisation. Cette base de données **43** est typiquement construite, de manière connue par l'homme du métier, sur la base de définitions de champs, tels que cela apparaît dans le cercle de la partie droite de la Figure 4. Un enregistrement de la base de données est illustré dans la partie droite de la Figure 4. Pour l'application visée à titre purement indicatif dans la présente description, cet enregistrement destiné à la personnalisation d'une carte à puce donnée **3** définit la valeur maximale de chargement du porte-monnaie électronique à 2000 unités de valeur, la valeur initiale de chargement du porte-monnaie électronique à 200 unités de valeur, et le nombre maximal d'essais par l'usager de saisi de code secret à 2.

Est ensuite prévue une étape de substitution **44** de variables à personnaliser dans le programme applicatif en code source **40** par des données de personnalisation propres à chaque carte, en un programme applicatif en code source personnalisé. Ainsi, un programme applicatif en code source personnalisé est créé pour chaque carte **3.**

Ensuite selon que la carte **3** mémorise ou pas un logiciel de type Machine Virtuelle de type JavaCard ™ promu et licensié par SUN, ou Smart Card for Windows™ licensiée par MICROSOFT Corp., une étape de compilation est requise ou pas. Si la carte **3** mémorise un logiciel de type Machine Virtuelle, le programme applicatif en code source personnalisé est directement interprétable par la carte **3**. Il est dans ce cas chargé tel quel dans la carte. Dans le cas inverse, une étape de compilation **44** est nécessaire. Cette étape de compilation **44** consiste à transformer une instruction compacte écrite en langage évolué, par exemple « WRITE », en une série d'instructions en langage machine, toujours les mêmes pour cette instruction, directement exécutable par l'unité de traitement de la puce de la carte à puce. Par exemple, dans le cas de cette instruction « WRITE », la transformation par compilation aura pour objet de produire des instructions par lesquelles l'unité de traitement devra, successivement, charger, dans un registre d'échange avec la mémoire, la valeur à écrire, sélectionner par son adresse une cellule de la mémoire où cette valeur doit être écrite, provoquer l'écriture, incrémenter son compteur d'instructions pour admettre une instruction suivante du programme, etc....

REVENDICATIONS

1 – Procédé de personnalisation électrique de cartes à puce, consistant à mémoriser des données personnalisées dans chaque puce de carte à puce, comprenant l'étape suivante :

- écriture d'un programme applicatif en code source (**40**) dans un langage évolué;

caractérisé en ce qu'il comprend les étapes de :

- substitution de variables à personnaliser dans le programme applicatif en code source par des données de personnalisation propres à ladite chaque carte, en un programme applicatif en code source personnalisé ;
- compilation du programme applicatif en code source personnalisé ;
- chargement dans la carte à puce du programme applicatif en code source personnalisé et préalablement compilé.

2 – Procédé de personnalisation électrique de cartes à puce, consistant à mémoriser des données personnalisées dans chaque puce de carte à puce, comprenant l'étape suivante :

- écriture d'un programme applicatif en code source (**40**) dans un langage interprétable;

caractérisé en ce qu'il comprend les étapes de :

- reconnaissance (**41**) de caractères particuliers dans le programme applicatif en code source (**40**) ;
- substitution de variables à personnaliser dans le programme applicatif en code source par des données de personnalisation propres à ladite chaque carte, en un programme applicatif en code source personnalisé ;
- chargement dans la carte à puce du programme applicatif en code source personnalisé.

3 – Procédé conforme à la revendication 1 ou 2, caractérisé en ce que l'étape de substitution est précédée par une étape de reconnaissance de caractères identifiant des zones délimitant lesdites variables dans le programme applicatif en code source (**40**).

FIG. 1

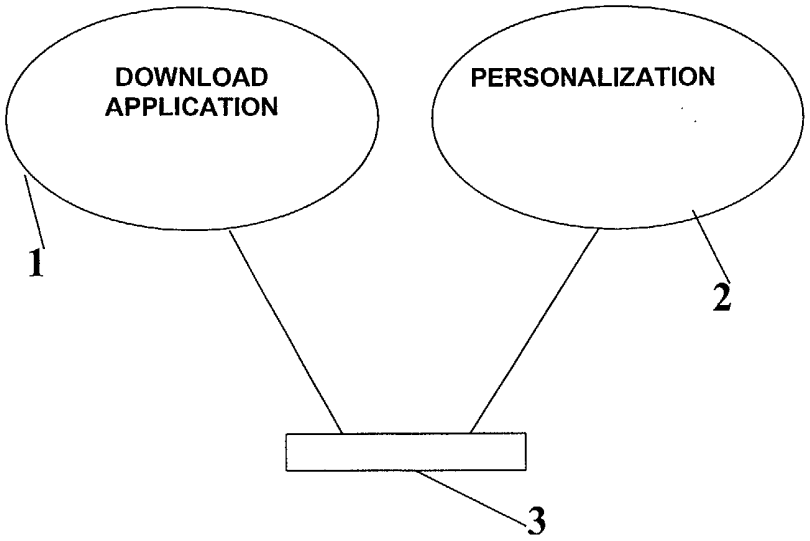

DOWNLOAD APPLICATION
PERSONALIZATION
1
2
3

FIG.2

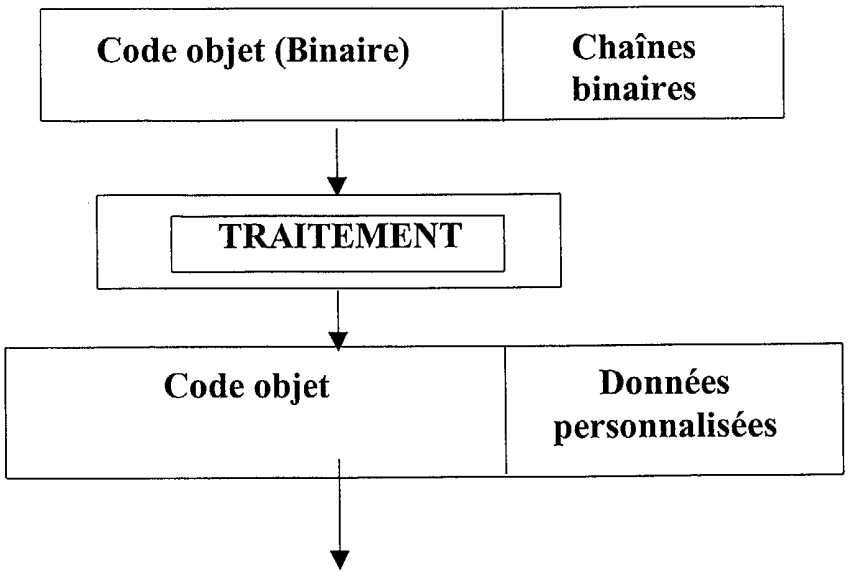

Code objet (Binaire)
Chaînes binaires
TRAITEMENT
Code objet
Données personnalisées

FIG.3

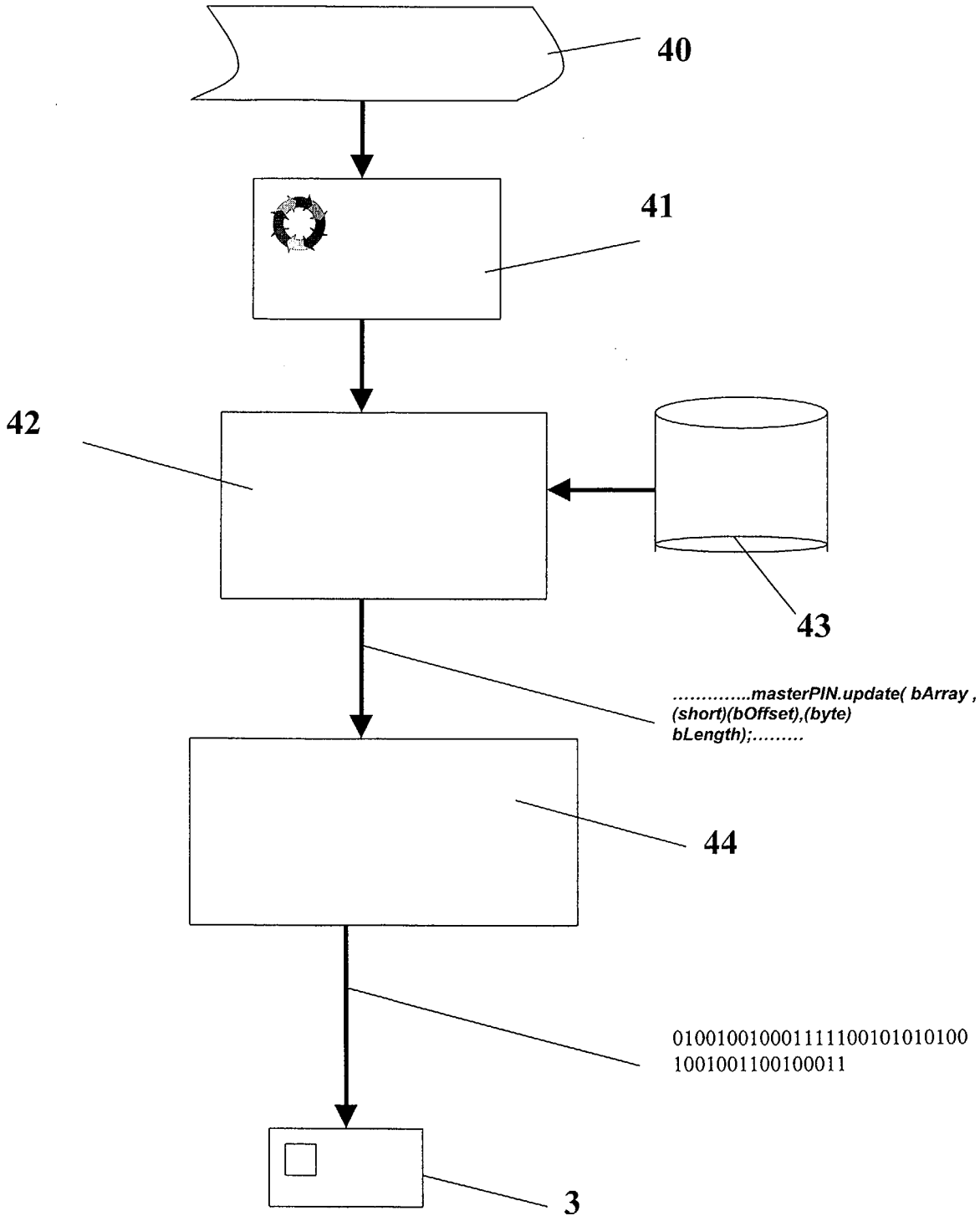
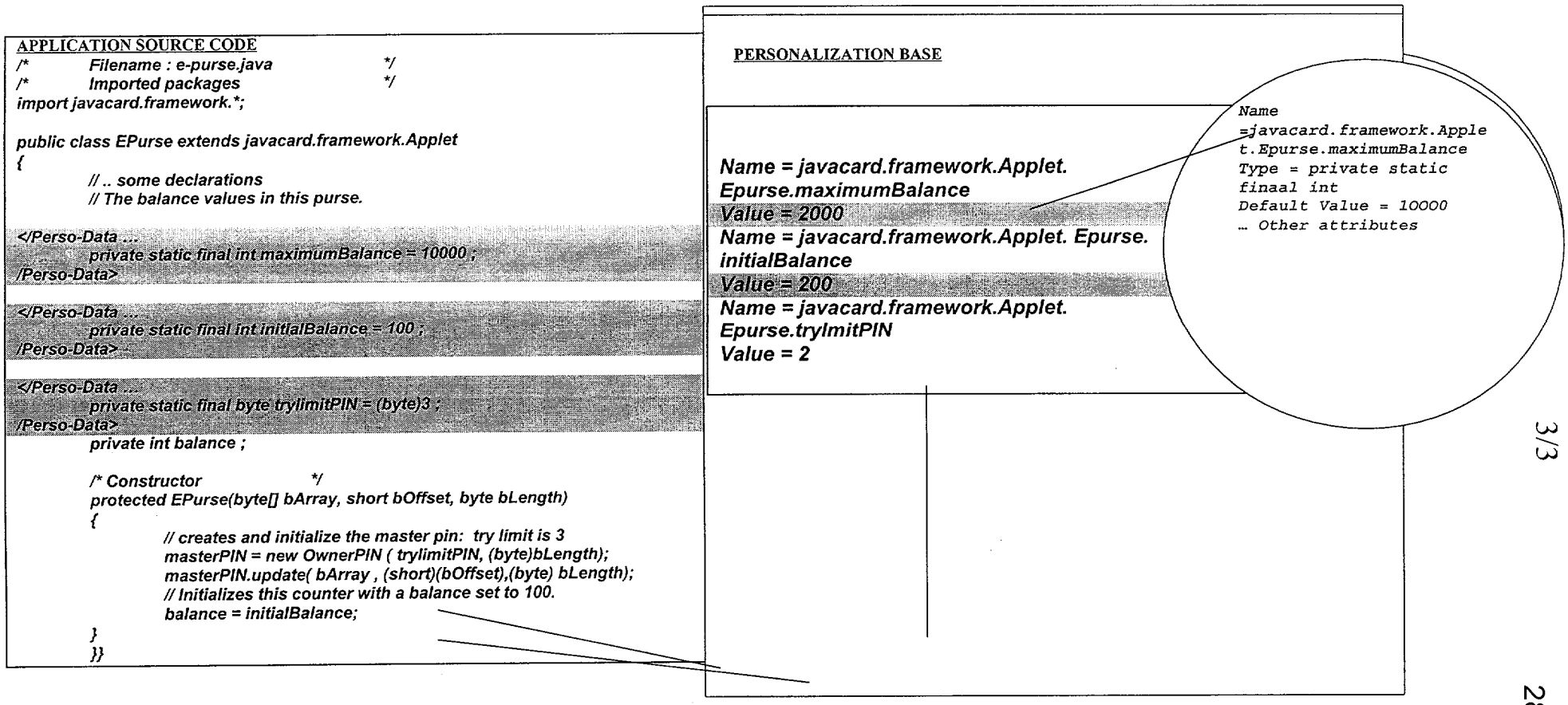

40
41
42
43
.....masterPIN.update(bArray , (short)(bOffset),(byte) bLength);.....
44
0100100100011111001010101001001001100100011
3

FIG.4



2809847

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2809847

N° d'enregistrement national

FA 590386
FR 0007248

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP 0 430 257 A (TOSHIBA) 5 juin 1991 (1991-06-05) * le document en entier * ---	1-3	G06K19/07 G06F9/06
A	WO 97 39424 A (UBIQ INCORPORATED) 23 octobre 1997 (1997-10-23) * abrégé; revendications; figures * * page 3, ligne 9 - page 6, ligne 30 * * page 24, ligne 17 - page 33, ligne 24 * ---	1-3	
A	EP 0 593 244 A (OKI ELECTRIC INDUSTRY) 20 avril 1994 (1994-04-20) * abrégé; revendications; figures * * colonne 4, ligne 40 - colonne 5, ligne 42 * -----	1-3	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			G07F

Date d'achèvement de la recherche	Examinateur
20 mars 2001	David, J

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)