(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
13 décembre 2001 (13.12.2001)

PCT

(10) Numéro de publication internationale
WO 01/95274 A1

(51) Classification internationale des brevets[7] : G07F 7/10

(21) Numéro de la demande internationale :
PCT/FR01/01774

(22) Date de dépôt international : 8 juin 2001 (08.06.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/07319 8 juin 2000 (08.06.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **BULL CP8** [FR/FR]; 68, route de Versailles, Boîte postale 45, F-78430 Louveciennes (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **FOUGEROUX, Nicolas** [FR/FR]; 6, square Bainville, F-78150 Le Chesnay (FR). **BOLE, Benoît** [FR/FR]; 24, rue de l'Orangeraie, F-78000 Versailles (FR). **HAMEAU, Patrice** [FR/FR]; 18, rue Belle Feuille, F-92100 Boulogne Billancourt (FR).

(74) Mandataire : **CORLU, Bernard**; Bull CP8, PC 62A24, 68, route de Versailles, Boîte Postale 45, F-78434 Louveciennes Cedex (FR).

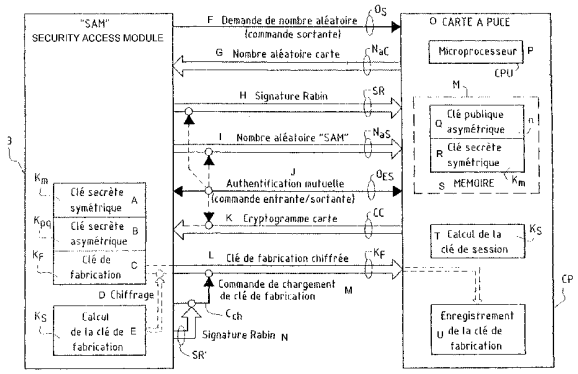
(81) États désignés *(national)* : CN, JP, KR, US.

(84) États désignés *(régional)* : brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Suite sur la page suivante]

(54) Title: METHOD FOR MAKING SECURE THE PRE-INITIALISING PHASE OF A SILICON CHIP INTEGRATED SYSTEM, IN PARTICULAR A SMART CARD AND INTEGRATED SYSTEM THEREFOR

(54) Titre : PROCEDE DE SECURISATION DE LA PHASE DE PRE-INITIALISATION D'UN SYSTEME EMBARQUE A PUCE ELECTRONIQUE, NOTAMMENT D'UNE CARTE A PUCE, ET SYSTEME EMBARQUE METTANT EN OEUVRE LE PROCEDE



A...SYMMETRIC KEY
B...ASYMMETRIC KEY
C...DEDICATED KEY
D...ENCRYPTRON
E...CALCULATING THE DEDICATED KEY
F...REQUEST FOR RANDOM NUMBER (OUTGOING COMMAND)
G...CARD RANDOM NUMBER
H,N... RABIN SIGNATURE
I... "SAM" RANDOM NUMBER
J...MUTUAL AUTHENTICATION (INCOMING/OUTGOING COMMAND)
L...ENCRYPTED DEDICATED KEY
M...COMMAND TO LOAD DEDICATED KEY
O...SMART CARD
P...MICROPROCESSOR
Q...ASYMMETRIC PUBLIC KEY
R...SYMMETRIC SECRET KEY
S...STORAGE UNIT
T...CALCULATING SESSION KEY
K...CARD CRYPTOGRAM
U...RECORDING DEDICATED KEY

(57) **Abstract:** The invention concerns a method for making secure the pre-initialising phase of a smart card (<I>CP</I>) with mutual authentication of said card (<I>CP</I>), recording a symmetric secret key (<I>K_M</I>) and an asymmetric public key (*n*), and a security device (3) storing the same secret key (<I>K_M</I>) and the asymmetric public key (K_{pq}) corresponding to the public key (n). The card (<I>CP</I>) and the device (3) supply random numbers (N_{aC}). The device (3) authenticates itself by transmitting to the card (<I>CP</I>) a cryptogram (<I>SR</I>) derived from two random numbers, using an asymmetric algorithm. The card (<I>CP</I>) authenticates itself by calculating a session secret key derived from the random number (N_{aC}), using a symmetric algorithm and the secret key (<I>K_M</I>), and in transmitting to the device (3) a cryptogram (<I>CC</I>) derived from the second random number, using the symmetric algorithm and the session key. The dedicated key (<I>K_F</I>) is transmitted to the card, encrypted by the session key (K_s).

[Suite sur la page suivante]

WO 01/95274 A1

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne la sécurisation de la phase de pré-initialisation d'une carte à puce (CP) avec authentification mutuelle de cette carte (CP), enregistrant une clé secrète symétrique (K_M) et une clé publique asymétrique (n), et d'un dispositif de sécurité (3) emmagasinant la même clé secrète (K_M) et la clé secrète asymétrique (K_{pq}) correspondant à la clé publique (n). La carte (CP) et le dispositif (3) fournissent des nombres aléatoires (N_{aC}). Le dispositif (3) s'authentifie en transmettant à la carte (CP) un cryptogramme (SR) dérivé des deux nombres aléatoires, par usage d'un algorithme asymétrique. La carte (CP) s'authentifie en calculant une clé secrète de session dérivée du nombre aléatoire (N_{aC}), à l'aide d'un algorithme symétrique et de la clé secrète (K_M), et en transmettant au dispositif (3) un cryptogramme (CC) dérivé du second nombre aléatoire, à l'aide de l'algorithme symétrique et de la clé de session. La clé dédiée (K_F) est transmise à la carte, chiffrée par la clé de session (K_S).

PROCÉDÉ DE SÉCURISATION DE LA PHASE DE PRÉ-INITIALISATION D'UN SYSTÈME EMBARQUÉ À PUCE ÉLECTRONIQUE, NOTAMMENT D'UNE CARTE À PUCE, ET SYSTÈME EMBARQUÉ METTANT EN ŒUVRE LE PROCÉDÉ

L'invention concerne un procédé de sécurisation d'une opération prédéterminée, notamment de la phase de pré-initialisation d'un système embarqué à puce électronique, par le chargement sécurisé d'une clé de chiffrement à usage dédié.

Elle s'applique plus particulièrement à une carte à puce.

L'invention concerne encore un système embarqué pour la mise en œuvre du procédé.

Dans le cadre de l'invention, le terme "pré-initialisation" s'entend dans un sens général. Il est notamment relatif à la phase de fabrication d'une carte à puce traditionnelle ou à la phase précédant la phase d'initialisation d'une carte à puce dite ouverte.

De même, le terme "système embarqué" vise des systèmes ou dispositifs divers ayant en commun le fait de disposer d'une puce électronique comprenant des moyens de mémoire et de traitement de données, généralement constitués par un microprocesseur ou un microcontrôleur. Un tel système embarqué peut être constitué notamment par une carte à puce.

Pour fixer les idées, on se placera dans ce qui suit dans le cas de l'application préférée de l'invention, à savoir celui de la pré-initialisation d'une carte à puce.

Dans la plupart des applications à base de carte à puce, il est dévolu à ces dernières des fonctions relatives à la sécurité. Ce terme recouvre d'ailleurs lui-même divers concepts : confidentialité, authentification, etc.

Pour ce faire, on inscrit, dans une partie non volatile des moyens de mémoire précités de la puce électronique, de façon définitive (utilisation de

mémoires fixes du type dit "ROM", pour "Read Only Memory" ou mémoire à lecture seule), ou semi-fixe (mémoire re-programmable du type "EEPROM", pour "Electrically Erasable Programmable Read Only Memory" ou mémoire effaçable programmable par voie électrique à lecture seule, etc.), des données dites secrètes nécessaires à ces fonctions : algorithmes de chiffrage, clés secrètes de chiffrage, données d'identification, etc.

Parmi ces données, il existe une clé dite de fabrication permettant traditionnellement de sécuriser toutes les étapes de pré-initialisation de la carte à puce.

De façon habituelle, la fabrication d'une carte à puce s'effectue en deux grandes phases. Pendant la première phase, une puce électronique est fabriquée par une première entité, que l'on appellera ci-après "fondeur". Pendant une seconde phase cette puce électronique est mise en module puis intégrée dans un support, à savoir une pièce de plastique sensiblement rectangulaire, constituant la carte à puce proprement dite. Cette opération est réalisée généralement par une seconde entité, distincte de la première, que l'on appellera ci-après "encarteur".

Une troisième entité, que l'on appellera ci-après "pré-personnalisateur", réalise l'opération de pré-initialisation précitée.

Dans l'état actuel de la technique, de manière quasi systématique, la clé de fabrication sécurisant toutes les étapes de pré-initialisation d'une carte à puce est écrite en clair et sans authentification préalable par l'encarteur. Ce mode opératoire pose plusieurs problèmes :

- si des cartes sont subtilisées lors de leur transport du fondeur vers l'encarteur, aucune sécurité logicielle ("software") n'est assurée : les cartes peuvent être frauduleusement pré-initialisées et utilisées de façon malveillante par la suite ;
- un fraudeur réalisant une carte en tout point clonée peut l'insérer dans la chaîne d'encartage sans être repéré ; et
- un simple espionnage de ligne permet d'obtenir la clé de fabrication transmise en clair.

Une solution serait de faire écrire la clé de fabrication par le fondeur lors d'une opération dite "sous pointe", mais cette solution est très onéreuse, car les données secrètes doivent être diversifiées pour chaque carte (données non fixes), ce qui de plus est mal adapté aux cadences de fabrication du fondeur. Ce procédé onéreux n'est donc pas réaliste et, de ce fait, pratiquement jamais mis en œuvre.

L'invention vise à pallier les inconvénients des dispositifs de l'art connu, et dont certains viennent d'être rappelés.

Pour ce faire, selon une première caractéristique avantageuse de l'invention, l'écriture de la clé de fabrication est protégée par une authentification mutuelle entre un organe connu sous le sigle anglo-saxon "SAM" (pour "Security Access Module" ou "Module d'Accès Sécurisé") et la carte à puce, de manière à se prévaloir de l'utilisation d'un faux module "SAM" ou d'une carte à puce clonée ou encore ayant une mémoire non volatile, "ROM" ou autre", falsifiée. Ci-après, par mesure de simplification, ce module sera appelé "SAM". Celui-ci peut être hébergé dans un micro-ordinateur ou une carte à puce, par exemple. De façon générale, on peut définir le "SAM" comme étant un organe "porteur de clé". Celui-ci emmagasine en effet une clé secrète qui n'est jamais divulguée, dans le sens où elle n'est pas communiquée au monde extérieur. Elle sert à calculer d'autres clés permettant l'authentification mutuelle précitée.

L'authentification du "SAM" par la carte à puce utilise un algorithme de chiffrage de type asymétrique. Il peut s'agir, par exemple, de l'algorithme très utilisé dans le domaine des applications bancaires et connu sous le sigle "RSA" (pour "Rivest, Shamir et Adleman", inventeurs désignés dans le brevet US 4 405 829 A). Cependant, une carte à puce n'étant pourvue que de ressources informatiques limitées, on préférera utiliser, pour ce faire, l'algorithme dit de "Rabin". En effet, dans ce dernier cas, la puissance de calcul nécessaire est moindre, ce qui convient mieux aux caractéristiques propres à un dispositif du type carte à puce ou similaire. Aussi, on considérera ci-après, sans que cela limite en quoi que ce soit la portée de

l'invention, que l'algorithme de type asymétrique utilisé est l'algorithme de "Rabin".

En ce qui concerne l'authentification de la carte à puce par le module "SAM", celle-ci est basée avantageusement sur un algorithme symétrique, préférentiellement du type dit "triple DES" (pour "Data Encryption System").

En utilisant l'algorithme de Rabin pour l'authentification du "SAM" par la carte à puce et l'algorithme "triple DES" pour l'authentification de la carte à puce par le "SAM", le recours à un cryptoprocesseur n'est pas nécessaire pour mettre en œuvre le mécanisme de sécurisation, ce qui est avantageux également dans le cadre des applications visées par l'invention.

Le procédé selon l'invention permet ensuite au "SAM" authentifié de charger la clé de fabrication de manière sécurisée vers la carte à puce elle-même authentifiée.

L'invention a donc pour objet principal un procédé de chargement sécurisé d'une clé dédiée à la sécurisation d'une opération prédéterminée dans des moyens de mémoire d'une puce électronique d'un système embarqué, ladite clé dédiée étant contenue dans un dispositif de sécurité comportant des moyens de communication bidirectionnels avec ladite puce électronique, caractérisé en ce que, lesdits moyens de mémoire de ladite puce électronique emmagasinant une clé de chiffrement secrète symétrique et une clé publique asymétrique et ledit dispositif de sécurité emmagasinant la même clé de chiffrement secrète symétrique et la clé secrète asymétrique correspondant à la clé publique de ladite puce électronique, il comprend :

- une première phase consistant en l'authentification dudit dispositif de sécurité par ladite puce électronique et comprenant les étapes de génération par la puce électronique d'un premier nombre aléatoire et sa transmission au dispositif de sécurité, la génération par celui-ci d'un deuxième nombre aléatoire et d'un premier cryptogramme, à partir desdits premier et deuxième nombres aléatoires, par l'application d'un algorithme de signature de type asymétrique, à l'aide de ladite clé secrète

asymétrique, et sa transmission à ladite puce électronique de manière à y réaliser ladite authentification par vérification à l'aide de ladite clé publique ;

- une deuxième phase consistant en l'authentification de ladite puce électronique et comprenant les étapes de génération, par la puce électronique et ledit dispositif de sécurité d'une clé secrète dite de session à partir dudit premier nombre aléatoire, par l'application d'un algorithme de chiffrement de type symétrique, à l'aide de ladite clé de chiffrement secrète, suivi de la génération d'un deuxième cryptogramme par l'application d'un algorithme de chiffrement de type symétrique, à l'aide de ladite clé secrète de session et sa transmission au dit dispositif de sécurité de manière à y réaliser ladite authentification par vérification à l'aide de ladite clé de session ; et

- une phase de transfert dans lesdits moyens de mémoire de ladite puce électronique de ladite clé dédiée, chiffrée par ladite clé secrète de session.

L'invention a encore pour objet un système embarqué à puce électronique pour la mise en œuvre du procédé.

L'invention va maintenant être décrite de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

- la figure 1 illustre schématiquement un exemple de configuration de la mémoire d'une carte à puce selon un aspect de l'invention, pour l'enregistrement d'une clé publique ;
- la figure 2 illustre schématiquement les principaux échanges d'informations pour l'authentification mutuelle d'un module dit "SAM", porteur de clé, et d'une carte à puce, selon le procédé de l'invention ;
- la figure 3 illustre un exemple de données concaténées servant au calcul d'une signature Rabin sur des nombres aléatoires générés respectivement par la carte à puce et le module "SAM", selon un aspect du procédé de l'invention ;

- la figure 4 illustre, sur un exemple, la génération d'une clé de session dans la carte à puce, selon un aspect de l'invention ;
- la figure 5 illustre, sur un exemple, la génération d'un cryptogramme dans la carte à puce, à l'aide de la clé de session, selon un aspect de l'invention ; et
- la figure 6 illustre un exemple de données concaténées servant au calcul d'une signature Rabin, calculée par le "SAM", sur la commande de chargement de la clé de fabrication devant être transférée chiffrée dans la carte à puce.

Dans ce qui suit, sans en limiter en quoi que ce soit la portée, on se placera ci-après dans le cadre de l'application préférée de l'invention, sauf mention contraire, c'est-à-dire dans le cas de la sécurisation de la phase de pré-initialisation d'une carte à puce.

Le procédé selon l'invention nécessite, du point de vue de la carte à puce et du module "SAM", une clé secrète symétrique, que l'on appellera ci-après clé maître K_M. Cette clé K_M doit être présente dès que la puce électronique ou "chip" sort de l'entité qui a été appelé "fondeur".

Le stockage de cette clé K_M est effectué dans une partie non volatile de la mémoire dont est munie la puce électronique : mémoire fixe de type "ROM" ou semi-fixe de type "EEPROM" ou similaire.

Dans une variante de réalisation préférée de l'invention, et selon une première caractéristique, la clé K_M est écrite "sous pointe" en "EEPROM" par le fondeur. Les octets composant la clé K_M sont des données extrêmement sensibles et doivent être traités comme des octets de sécurité. Le stockage en "EEPROM" permet une éventuelle diversification de cette clé K_M pour plusieurs lots de cartes.

Le procédé selon l'invention nécessite également, du point de vue de la carte à puce, une clé publique asymétrique, que l'on appellera ci-après clé publique asymétrique n. Cette clé n, fixe pour toutes les cartes, doit être présente dès que la puce électronique ou "chip" sort de l'entité qui a été appelé "fondeur".

Le stockage de cette clé *n* est effectué dans une partie non volatile de la mémoire dont est munie la puce électronique : mémoire fixe de type "ROM" et/ou semi-fixe de type "EEPROM" ou similaire

Dans une variante de réalisation préférée de l'invention, et selon une deuxième caractéristique, la mémoire non volatile de la puce électronique présente une configuration hybride, physique et logique, particulière. On prévoit une partie fixe, de type "ROM" et une partie semi-fixe re-programmable, par exemple de type "EEPROM". On répartit les octets de la clé publique précitée entre ces deux zones de mémoire de la façon particulière explicitée ci-après. Les octets doivent être présents dès que la puce sort de chez le fondeur.

Les octets écrits "sous pointe" dans la partie "EEPROM" de la mémoire doivent être considérés comme extrêmement sensibles, et, à ce titre, être traités comme des octets de sécurité.

Par exemple, pour fixer les idées, on va considérer une clé publique de longueur 768 bits (soit 96 octets). Celle-ci réside totalement en mémoire "ROM". Cependant, selon un mode de réalisation préféré du procédé selon l'invention, on enregistre un octet par bloc de douze de façon intentionnellement erronée dans la zone de mémoire de type "ROM", cette valeur erronée ayant été volontairement écrite dans le code enregistré dans cette partie de la mémoire de type "ROM". Pour sa part, la valeur correcte de l'octet en question est enregistrée dans la partie de type "EEPROM". Dans cet exemple, huit octets (c'est-à-dire 96/12=8) doivent donc être programmés dans la partie de type "EEPROM" de la mémoire. Ces données sont fixes, car une clé publique ne se diversifie pas.

En outre, il est réalisé une opération connue sous le terme "hachage" ("hash") sur 160 bits de la clé publique *n*. Le résultat est stocké en mémoire "ROM", de façon à pouvoir être vérifié à chaque utilisation de la clé *n*. Pour ce faire, il est utilisé avantageusement un algorithme du type connu sous le sigle "SHA-1". Cet algorithme particulier doit donc être implanté dans la carte à puce.

Associé au stockage particulier de la clé publique *n*, le "hash" permet de garantir simultanément l'intégrité des deux parties de type "ROM" et "EEPROM" de la mémoire.

La figure 1 illustre schématiquement une telle configuration de mémoire d'une carte à puce *CP*. Dans l'exemple décrit, les moyens de mémoire *M* comprennent notamment une partie de mémoire 1, de type "ROM", et une partie de mémoire 2, de type "EEPROM". Toujours dans l'exemple décrit, on enregistre, dans la mémoire "ROM" 1, huit blocs de douze octets de données numériques, B_1 à B_8, représentant la clé publique précitée *n*. Dans chacun de ces huit blocs, B_1 à B_8, il existe un octet intentionnellement erroné, arbitrairement les octets, O_1 à O_8. On enregistre, dans la mémoire "EEPROM" 2, huit octets corrects, O'_1 à O'_8, correspondant à ces octets erronés O_1 à O_8.

On va maintenant décrire les étapes permettant le chargement sécurisé d'une clé dite de fabrication dans la carte à puce.

La première phase du procédé selon l'invention consiste en l'authentification du "SAM" vis-à-vis de la carte à puce *CP*.

Cette phase comprend notamment une étape de calcul par le "SAM" d'un cryptogramme en faisant usage d'une clé secrète asymétrique correspondant à la clé publique asymétrique *n* contenue dans la carte. Dans la pratique, la clé est composée de deux nombres premiers, que l'on appellera arbitrairement *p* et *q*. On appellera arbitrairement K_{pq} la clé secrète asymétrique du "SAM. En d'autres termes, le "SAM" s'identifie vis-à-vis de la carte à puce *CP* et celle-ci reconnaît son interlocuteur avec la clé publique *n*.

Comme le montre la figure 2, au moyen d'un ordre sortant O_S, le "SAM" 3 récupère de la carte à puce *CP* un nombre aléatoire N_{ac} sur seize octets. Le nombre N_{ac} sera appelé ci-après "nombre aléatoire carte" et peut être généré, par exemple, par les moyens de calcul de la carte à puce *CP*, dans l'exemple illustré, un microprocesseur *CPU*. Le "SAM" 3 génère

également un nombre aléatoire de seize octets que l'on appellera "nombre aléatoire SAM" N_{aS}.

Une signature Rabin, que l'on dénommera ci-après *SR*, est calculée, par le "SAM" 3sur quatre vingt seize octets de données, référencées *DSR*. Ces données *DSR* peuvent être conformes à la concaténation illustrée par la figure 3, de façon à atteindre les quatre vingt seize octets précités :

- une suite de cinquante neuf octets de remplissage, DSR_1, ayant par exemple la configuration fixe suivante : 01, FF, ... FF, en hexadécimal ;
- une suite de cinq octets, DSR_2, dits d'en-tête de la commande d'authentification mutuelle ; et
- trente deux octets, DSR_3, constitués par la concaténation des nombres N_{aS} et N_{aC} précités.

La suite de cinq octets d'en-tête de la commande d'authentification mutuelle, DSR_2, peut être constituée avantageusement par le contenu d'une commande d'un type dit "APDU", si la carte à puce *CP* est lue par un lecteur de carte à puce selon un protocole conforme aux normes "ISO 7816-1" à "ISO 7816-4". De façon plus précise, il peut s'agir du code associé à une instruction de chargement.

Si on se réfère de nouveau à la figure 2, la signature Rabin *SR* et le nombre aléatoire N_{aS} sont envoyés à la carte à puce *CP*, au moyen d'un ordre entrant-sortant O_{ES}, indiquant une authentification mutuelle. Le "SAM" 3 est seul capable de générer cette signature *SR*, puisque la clé secrète qu'il emmagasine n'est jamais divulguée. La carte à puce *CP* vérifie la signature Rabin à l'aide de la clé publique asymétrique *n* qu'elle stocke, ce qui permet d'authentifier le "SAM" 3.

La deuxième phase du procédé consiste en l'authentification de la carte à puce *CP* vis-à-vis du "SAM" 3, de façon à compléter l'authentification mutuelle des deux entités.

A partir de la clé secrète maître K_M et du nombre aléatoire précité de seize octets, N_{aC}, la carte à puce *CP* génère une clé symétrique secrète

dite de session, K_S, de seize octets, permettant de calculer un cryptogramme propre à la carte à puce *CP*.

De façon préférentielle, cette clé secrète de session, K_S, dite d'authentification, s'obtient en effectuant un chiffrement par un algorithme de type triple "DES" sur les deux parties, N_{aC1} et N_{aC2}, du nombre aléatoire carte N_{aC},

De façon plus précise, le processus de calcul de la clé secrète de session, K_S, s'effectue comme illustré par le diagramme de la figure 4.

Comme il bien connu, un chiffrement par un algorithme de type triple "DES" comporte, en cascade, un premier chiffrement, à l'aide d'une clé (en l'occurrence la clé secrète maître K_M), par un "DES" direct, un deuxième "DES" de type inverse et un troisième "DES", direct également.

Sur la partie "poids faible" de huit octets, N_{aC1}, du nombre aléatoire carte à puce, N_{aC}, le triple "DES" s'effectue directement à l'aide de trois modules en cascade, référencés D_{11}, D_{21} et D_{31}. Les modules D_{11} et D_{31} reçoivent, sur leurs entrées de clé, une même valeur de clé, en l'occurrence la partie "poids fort" de huit octets, K_{M1}, de la clé K_M, alors que le module D_{21} reçoit, sur son entrée de clé, la partie "poids faible", K_{M2}, toujours sur huit octets. En sortie du module D_{31}, on obtient la partie "poids fort" sur huit octets, K_{S1}, de la clé secrète de session K_S. Ce mot de huit octets, K_{S1}, peut être stocké temporairement dans un registre de mémoire ou dans une partie de la mémoire vive dont est habituellement munie la carte à puce *CP*.

La partie K_{S1} est ré-injectée sur une première entrée d'un circuit logique de type "OU-exclusif" référencé *XOR*. Celui-ci reçoit, sur une seconde entrée, la partie "poids fort" de huit octets, N_{aC2}, du nombre aléatoire carte à puce, N_{aC}. La sortie de ce circuit logique *XOR* est transmise à l'entrée d'une chaîne de chiffrage en triple "DES". Ce triple "DES" s'effectue à l'aide de trois modules en cascade, référencés D_{12}, D_{22} et D_{32}. Comme précédemment, les modules D_{12} et D_{32} reçoivent, sur leurs entrées de clé, une même valeur de clé, en l'occurrence la partie "poids fort" de huit octets, K_{M1}, de la clé K_M, alors que le module D_{22} reçoit, sur son entrée clé,

la partie "poids faible", K_{M2}, toujours sur huit octets. En sortie du module D_{32}, on obtient la partie "poids faible" sur huit octets, K_{S2}, de la clé secrète de session K_S. Ce mot de huit octets, K_{S2}, peut lui aussi être stocké temporairement dans un registre de mémoire ou dans une partie de la mémoire vive.

La clé secrète K_M peut être présente en "ROM", ou écrite "sous pointe" en "EEPROM", comme il a été rappelé précédemment.

Il va de soit que l'opération logique "OU-exclusif" peut être réalisée de manière logicielle, au lieu d'utiliser un circuit logique spécifique *XOR*, ce en faisant appel à une routine enregistrée en mémoire "ROM" 1 par exemple, sous la commande du microprocesseur *CPU*. De même, les opérations de chiffrage "DES" ou "DES^{-1}" sont généralement réalisées à l'aide d'algorithmes enregistrés en mémoire "ROM" 1, toujours sous la commande du microprocesseur *CPU*. Les résultats intermédiaires sont stockés dans des registres ou en mémoire vive.

Le "SAM" 3 est en mesure de calculer la même clé de session secrète K_S, de la façon qui vient d'être décrite, car ce dernier stocke également la clé secrète maître K_M.

Dans une étape supplémentaire, la carte à puce *CP* génère une suite d'octets qui va être appelée ci-après "cryptogramme carte" *CC*. Ce dernier est obtenu en chiffrant le nombre aléatoire "SAM" transmis à la carte à puce *CP* à l'aide de la clé secrète de session K_S qui vient d'être calculée.

La figure 5 illustre le processus. Ce dernier est similaire à celui qui a permis de calculer la clé secrète de session K_S. Il a notamment recours à des fonctions "OU-exclusif" et à chiffrage selon l'algorithme triple "DES". Aussi, les éléments communs aux figures précédentes portent les mêmes références et ne seront re-décrits qu'en tant que de besoin.

Le nombre aléatoire "SAM", N_{aS}, a été reçu du "SAM" 3 et est stocké provisoirement dans un emplacement de mémoire, registre ou autre. La partie poids fort sur huit octets, N_{aS1}, de ce nombre aléatoire, N_{aS}, est soumise à un triple "DES" par la chaîne D_{11} à D_{31}. Cependant elle subit

d'abord une opération logique "OU-exclusif" avec une valeur de chaînage initiale de huit octets, N_i, de valeur hexadécimale "00", à l'aide d'un premier circuit XOR_1 (ou par un processus logiciel). C'est la sortie de ce circuit XOR_1 qui est transmise à la chaîne précitée. La clé de chiffrage est la clé de session secrète K_S calculée à l'étape précédente. De façon plus précise, les entrées de clé des "DES" D_{11} et D_{31} reçoivent les huit octets de plus fort poids, K_{S1}, de cette clé K_S, et l'entrée de clé du " DES " D_{21}, les huit octets de plus faible poids, K_{S2}.

Ce processus permet de calculer les huit octets de plus fort poids, CC_1, du cryptogramme CC. Ces octets CC_1 sont ré-injectés en entrée de la chaîne de chiffrage triple "DES", D_{12} à D_{32}, pour les octets de plus faible poids, N_{aS2}, du nombre aléatoire "SAM" N_{aS}, plus exactement sur une des entrées d'un deuxième circuit "OU-exclusif" XOR_2, la première entrée recevant les huit octets de plus faible poids du nombre aléatoire N_{aS}. C'est la sortie de ce circuit XOR_2 qui est transmise à la chaîne précitée. Les entrées de clé des "DES" D_{12} et D_{32} reçoivent les huit octets de plus fort poids, K_{S1}, de cette clé K_S, et l'entrée de clé du " DES " D_{22}, les huit octets de plus faible poids, K_{S2}. La sortie du "DES" D_{32} génère les huit octets de poids faible CC_2 du cryptogramme carte CC.

Ce cryptogramme est transmis au "SAM" 3, au moyen de l'ordre d'entrée-sortie *OES* (figure 2) d'authentification mutuelle. A l'issue de cette étape, le "SAM" 3 peut authentifier la carte à puce *CP* à partir du cryptogramme carte *CC*, puisqu'il a également calculé la clé de session K_S, comme rappelé ci-dessus.

La dernière étape consiste à charger la clé dite de fabrication K_F dans la mémoire de la carte à puce *CP*., à l'aide d'une commande de chargement C_{ch}. Cette clé K_F est sécurisée par chiffrage à l'aide de la clé secrète de session K_S, en mode dit "CBC" (pour "Concatened Blocks Ciphering" ou Blocs Concaténés Chiffrés).

Si la commande de chargement échoue, la clé de session K_S est perdue et une nouvelle authentification mutuelle est nécessaire, avec calcul d'une nouvelle clé de session.

La commande de chargement est signée à l'aide d'une signature Rabin par le "SAM" 3. La figure 6 illustre schématiquement les données *DSR'* servant à calculer une signature Rabin *SR'*.

Au total, *DSR'* comprend quatre vingt seize octets. *DSR'* comprend, dans l'exemple trois parties :

- une en-tête DSR'_3, avantageusement une commande "APDU" comme dans le cas de la figure 2 ;
- des données chiffrées, DSR'_2, soit Do_1 à Do_n, représentant la clé de fabrication *KF* (avec *n* le nombre d'octets total de la clé de fabrication *KF*) ; et
- des données fixes de remplissage, DSR'_1, soit *x* octets, par exemple de configuration : 01, FF ... FF, en hexadécimal (la valeur de x est choisie pour que le nombre total d'octets de *DSR'* soit égal à quatre vingt seize).

A la lecture de ce qui précède, on constate aisément que l'invention atteint bien les buts qu'elle s'est fixés.

Notamment, le chargement de la clé de fabrication utilisée ultérieurement pour la sécurisation des étapes de pré-initialisation de la carte à puce *CP* s'effectue avec un niveau de sécurité très élevé. Le procédé permet de charger dans chaque carte à puce *CP* sa propre clé, ou en d'autres termes une clé différente des autres cartes à puce.

Cependant, bien qu'il permette cette diversification de clé, le procédé n'oblige pas pour autant à avoir recours à des opérations longues et coûteuses, du type signalé dit d'écriture "sous pointe du fondeur".

Il doit être clair cependant que l'invention n'est pas limitée aux seuls exemples de réalisations explicitement décrits, notamment en relation avec les figures 1 à 6.

Comme il a été indiqué, bien que l'algorithme de Rabin soit particulièrement avantageux, car peu gourmand en ressources informatiques, cet algorithme pourrait être remplacé par d'autres types d'algorithmes asymétriques, tel le "RSA". Il en est de même de l'algorithme du type triple "DES". D'autres algorithmes à clés symétriques sont utilisables sans quitter le domaine de l'invention. Ceci ne constitue qu'un choix technologique, en soi à la portée de l'Homme de Métier, et dépendant notamment de l'application précise envisagée.

De même, les valeurs numériques précises, nombre d'octets ou autres, n'ont été indiquées que dans un but de fixer les idées et ne sauraient limiter en quoi que ce soit la portée de l'invention. Notamment, comme il est bien connu, la longueur des clés de chiffrement dépend du degré de sécurité que l'on escompte atteindre et peut résulter de choix technologiques, liés par exemple à des standards de fait et/ou aux types d'algorithmes choisis.

Enfin, comme il a été indiqué, l'invention n'est pas limitée aux seules applications à base de cartes à puce. Elle peut trouver application dans le cadre de tout système embarqué comprenant une puce électronique ou un organe similaire, dans lequel il est nécessaire de charger une clé pour la sécurisation d'opérations prédéterminées.

Les opérations en question peuvent être des opérations de pré-initialisation, comme il a été décrit de façon détaillée, mais aussi d'autres types opérations.

A titre d'exemple, il est possible de soumettre des commandes sensibles d'une carte à puce dite ouverte, telles le chargement de librairies du type dit "API" ("Application Program Interface") ou de codes divers, dans la partie "EEPROM", à une authentification mutuelle entre le dispositif de chargement et la carte à puce, le processus d'authentification mutuelle se déroulant de façon conforme au procédé de l'invention.

De façon générale, Il est possible d'affecter du point de vue de la carte à puce une clé publique et une clé secrète symétrique à chaque type d'opération à sécuriser. La clé de session dérivée lors du mécanisme

d'authentification peut être utilisée par la suite afin de sécuriser le chargement d'une autre clé à usage dédié, comme la protection de librairies de type "API" précité ou de "patches", c'est-à-dire l'application de données binaires en remplacement de tout ou partie d'un programme existant.

REVENDICATIONS

1. Procédé de chargement sécurisé d'une clé dédiée à la sécurisation d'une opération prédéterminée dans des moyens de mémoire d'une puce électronique d'un système embarqué, ladite clé dédiée étant contenue dans un dispositif de sécurité comportant des moyens de communication bidirectionnels avec ladite puce électronique, caractérisé en ce que, lesdits moyens de mémoire (*M*) de ladite puce électronique emmagasinant une clé de chiffrement secrète symétrique (K_M) et une clé publique asymétrique (*n*) et ledit dispositif de sécurité (3) emmagasinant la même clé de chiffrement secrète symétrique (K_M) et une clé secrète asymétrique (K_{pq}) correspondant à ladite clé publique *n* de ladite puce électronique, il comprend :

- une première phase consistant en l'authentification dudit dispositif de sécurité (3) par ladite puce électronique (*CP*) et comprenant les étapes de génération par la puce électronique (*CP*) d'un premier nombre aléatoire (N_{aC}) et sa transmission au dispositif de sécurité (3), la génération par celui-ci d'un deuxième nombre aléatoire (N_{aS}) et d'un premier cryptogramme (*SR*), à partir desdits premier (N_{aC}) et deuxième (N_{aS}) nombres aléatoires, par l'application d'un algorithme de signature de type asymétrique, à l'aide de ladite clé secrète (K_{pq}), et sa transmission à ladite puce électronique (*CP*), de manière à y réaliser ladite authentification par vérification à l'aide de ladite clé publique (*n*);

- une deuxième phase consistant en l'authentification de ladite puce électronique (*CP*) et comprenant les étapes de génération, par la puce électronique (*CP*) et ledit dispositif de sécurité (3), d'une clé secrète dite de session (K_S) à partir dudit premier nombre aléatoire

(N_{aC}), par l'application d'un algorithme de chiffrement de type symétrique, à l'aide de ladite clé secrète (K_M), suivi de la génération d'un deuxième cryptogramme (CC) par l'application d'un algorithme de chiffrement de type symétrique, à l'aide de ladite clé secrète de session (K_S) et sa transmission au dit dispositif de sécurité (3) de manière à y réaliser ladite authentification par vérification à l'aide de ladite clé de session (K_S) ; et

- une phase de transfert dans lesdits moyens de mémoire (M) de ladite puce électronique (CP) de ladite clé dédiée (K_F), chiffrée par ladite clé de session (K_S).

2. Procédé selon la revendication 1, caractérisé en ce que ladite phase de transfert de ladite clé dédiée (K_F) est déclenchée par une commande de chargement de clé (C_{ch}) est signée (SR') par l'application d'un algorithme de signature de type asymétrique.

3. Procédé selon la revendication 1, caractérisé en ce que ledit algorithme asymétrique est l'algorithme dit de Rabin.

4. Procédé selon la revendication 3, caractérisé en ce que lesdits premier (N_{aC}) et deuxième (N_{aS}) nombres aléatoires ont une longueur de seize octets et en ce que ledit premier cryptogramme (SR) est obtenu par application dudit algorithme de Rabin sur la concaténation desdits premier (N_{aC}) et deuxième (N_{aS}) nombres aléatoires (DSR_3), d'un premier nombre déterminé d'octets formant un en-tête (DSR_2), et d'un deuxième nombre déterminé d'octets (DSR_1), dits de remplissage, de manière à ce que la longueur totale de ladite concaténation (DSR) soit de quatre vingt seize octets, équivalente à la longueur de ladite clé publique (n).

5. Procédé selon la revendication 3, caractérisé en ce que ladite clé dédiée (K_F) est chiffrée (DSR'_2) par ladite clé secrète de session (K_S) et est concaténée avec un troisième nombre déterminé d'octets (DSR'_3),

formant un en-tête, et un quatrième nombre déterminé d'octets (DSR'_1), dits de remplissage, de manière à ce que la longueur totale de ladite concaténation (DSR') soit de quatre vingt seize octets, et en ce que ladite concaténation (DSR') soit signée par application dudit algorithme de Rabin, avant ledit transfert vers ladite puce électronique (CP).

6. Procédé selon la revendication 1, caractérisé en ce que ledit algorithme symétrique est l'algorithme est du type dit triple "DES".

7. Procédé selon la revendication 6, caractérisé en ce que lesdits premier nombre aléatoire (N_{aC}) et la dite clé secrète (K_M) ayant une longueur de seize octets, ladite étape de génération de ladite clé secrète de session comprend :

- l'application dudit triple "DES" sur les huit octets de plus faible poids (N_{aC1}) dudit premier nombre aléatoire (N_{aC}), avec en cascade un "DES" direct (D_{11}), avec pour clé de chiffrement les huit octets de plus fort poids de ladite clé secrète (K_{M1}), un "DES" inverse (D_{21}), avec pour clé de chiffrement les huit octets de plus faible poids de ladite clé secrète (K_{M2}), et de nouveau un "DES" direct (D_{31}), avec pour clé de chiffrement les huit octets de plus fort poids de ladite clé secrète (K_{M1}), de manière à générer huit octets de plus fort poids de ladite clé secrète de session (K_{S1}) ;

- l'application d'une opération logique "OU-exclusif" (XOR) entre ces huit octets de plus fort poids (K_{S1}) et les huit octets de plus fort poids (N_{aC2}) dudit premier nombre aléatoire (N_{aC}) ; et

- l'application sur le résultat de ladite opération logique dudit triple "DES", avec en cascade un "DES" direct (D_{12}), avec pour clé de chiffrement les huit octets de plus fort poids de ladite clé secrète (K_{M1}), un "DES" inverse (D_{22}), avec pour clé de chiffrement les huit octets de plus faible poids de ladite clé secrète (K_{M2}), et de nouveau

un "DES" direct (D_{32}), avec pour clé de chiffrement les huit octets de plus fort poids de ladite clé secrète (K_{M1}), de manière à générer huit octets de plus faible poids (K_{S2}) de ladite clé secrète de session (K_S), lesdits octets de plus fort poids (K_{S1}) et de plus faible poids (K_{S2}) formant ensemble ladite clé secrète de session (K_S).

8. Procédé selon la revendication 6, caractérisé en ce que ledit deuxième nombre aléatoire (N_{aS}) et ladite clé secrète de session (K_S) ayant une longueur de seize octets, ladite étape de génération dudit cryptogramme de la carte comprend :

- l'application d'une opération logique "OU-exclusif" (XOR_1) entre les huit octets de plus fort poids (N_{aS1}) dudit deuxième nombre aléatoire (N_{aS}) et huit octets fixes à la valeur hexadécimale 00 ;

- l'application dudit triple "DES" sur le résultat de ladite opération logique, avec en cascade un "DES" direct (D_{11}), avec pour clé de chiffrement les huit octets de plus fort poids de ladite clé secrète de session (K_{S1}), un "DES" inverse (D_{21}), avec pour clé de chiffrement les huit octets de plus faible poids de ladite clé secrète de session (K_{S2}), et de nouveau un "DES" direct (D_{31}), avec pour clé de chiffrement les huit octets de plus fort poids de ladite clé secrète de session (K_{S1}), de manière à générer huit octets de plus fort poids (CC_1) dudit deuxième cryptogramme (CC) ;

- l'application d'une opération logique "OU-exclusif" (XOR_2) entre ces huit octets de plus fort poids (CC_1) et les huit octets de plus faible poids (N_{aS2}) dudit deuxième nombre aléatoire (N_{aS}) ; et

- l'application sur le résultat de ladite opération logique dudit triple "DES", avec en cascade un "DES" direct (D_{12}), avec pour clé de chiffrement les huit octets de plus fort poids de ladite clé secrète de session (K_{S1}), un "DES" inverse (D_{22}), avec pour clé de chiffrement

les huit octets de plus faible poids de ladite clé secrète de session (K_{S2}), et de nouveau un "DES" direct (D_{32}), avec pour clé de chiffrement les huit octets de plus fort poids de ladite clé secrète de session (K_{S1}), de manière à générer huit octets de plus faible poids (CC_2) dudit deuxième cryptogramme (CC), lesdits octets de plus fort poids (CC_1) et de plus faible poids (CC_2) formant ensemble ledit deuxième cryptogramme (CC).

9. Procédé selon la revendication 1, caractérisé en ce que, ledit système embarqué à puce électronique étant une carte à puce (CP), ladite clé dédiée est une clé dite de fabrication (K_F) servant à sécuriser les opérations de pré-initialisation de la carte à puce.

10. Système embarqué à puce électronique comprenant des moyens de traitement et de mémorisation de données, destiné à coopérer avec un dispositif de sécurité via des moyens de communication bidirectionnels, de manière à recevoir une clé dédiée à la sécurisation d'opérations prédéterminées, caractérisé en ce que lesdits moyens de mémorisation de données (M) emmagasinant une clé de chiffrement secrète symétrique (K_M) et une clé publique asymétrique (n) et ledit dispositif de sécurité (3) enregistrant la même clé de chiffrement secrète symétrique (K_M) et la clé secrète asymétrique (K_{pq}) correspondant à ladite clé publique (n), ladite puce électronique comprend des moyens pour générer un premier nombre aléatoire (N_{aC}) destiné à être transmis au dit dispositif de sécurité (3), des moyens pour recevoir de celui-ci un deuxième nombre aléatoire (N_{aS}) et un premier cryptogramme d'authentification (SR), généré à partir desdits premier (N_{aC}) et deuxième (N_{aS}) nombres aléatoires, par application d'un algorithme du type asymétrique et l'utilisation de ladite clé secrète (K_{pq}),des moyens (XOR, D_{11} – D_{32}) pour générer une clé secrète dite de session (K_S), à partir dudit premier nombre aléatoire (N_{aC}), par application d'un algorithme du type symétrique et l'utilisation de ladite clé secrète (K_M), des moyens pour générer un deuxième cryptogramme

(*CC*), à partir dudit deuxième nombre aléatoire (N_{aS}) reçu dudit dispositif de sécurité (3), par application d'un algorithme du type symétrique et l'utilisation de ladite clé secrète de session (K_S), et des moyens pour recevoir dudit dispositif de sécurité (3) ladite clé dédiée (K_F) chiffrée (DSR'_2) à l'aide de ladite clé de session (K_S) et pour l'enregistrer dans lesdits moyens de mémoire (*M*).

11. Système selon la revendication 9, caractérisé en ce qu'il est constitué par une carte à puce (*CP*) et en ce que ladite clé dédiée est une clé dite de fabrication (K_F), et en ce que lesdites opérations à sécuriser sont des opérations de pré-initialisation de ladite carte à puce (*CP*).

FIG.1

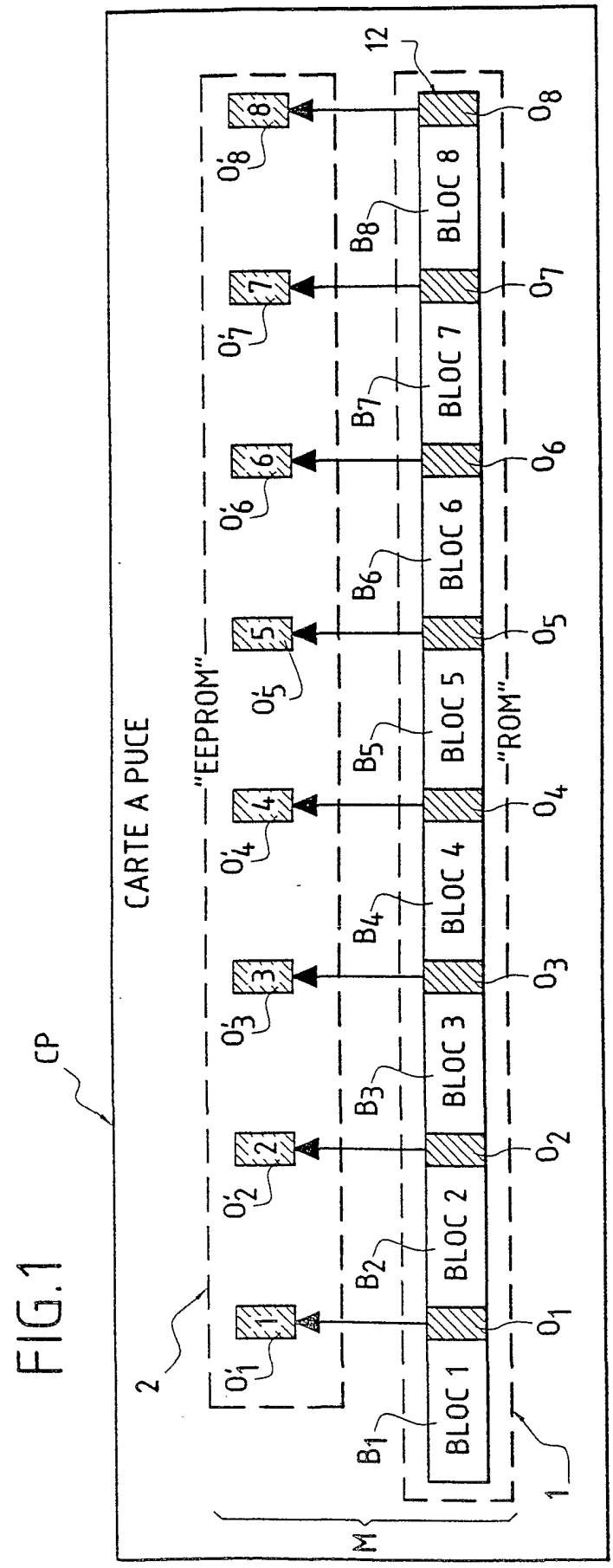
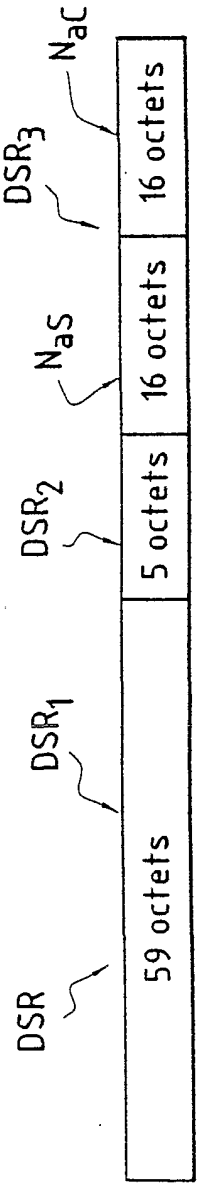


FIG.3



Signature "Rabin" (96 octets)

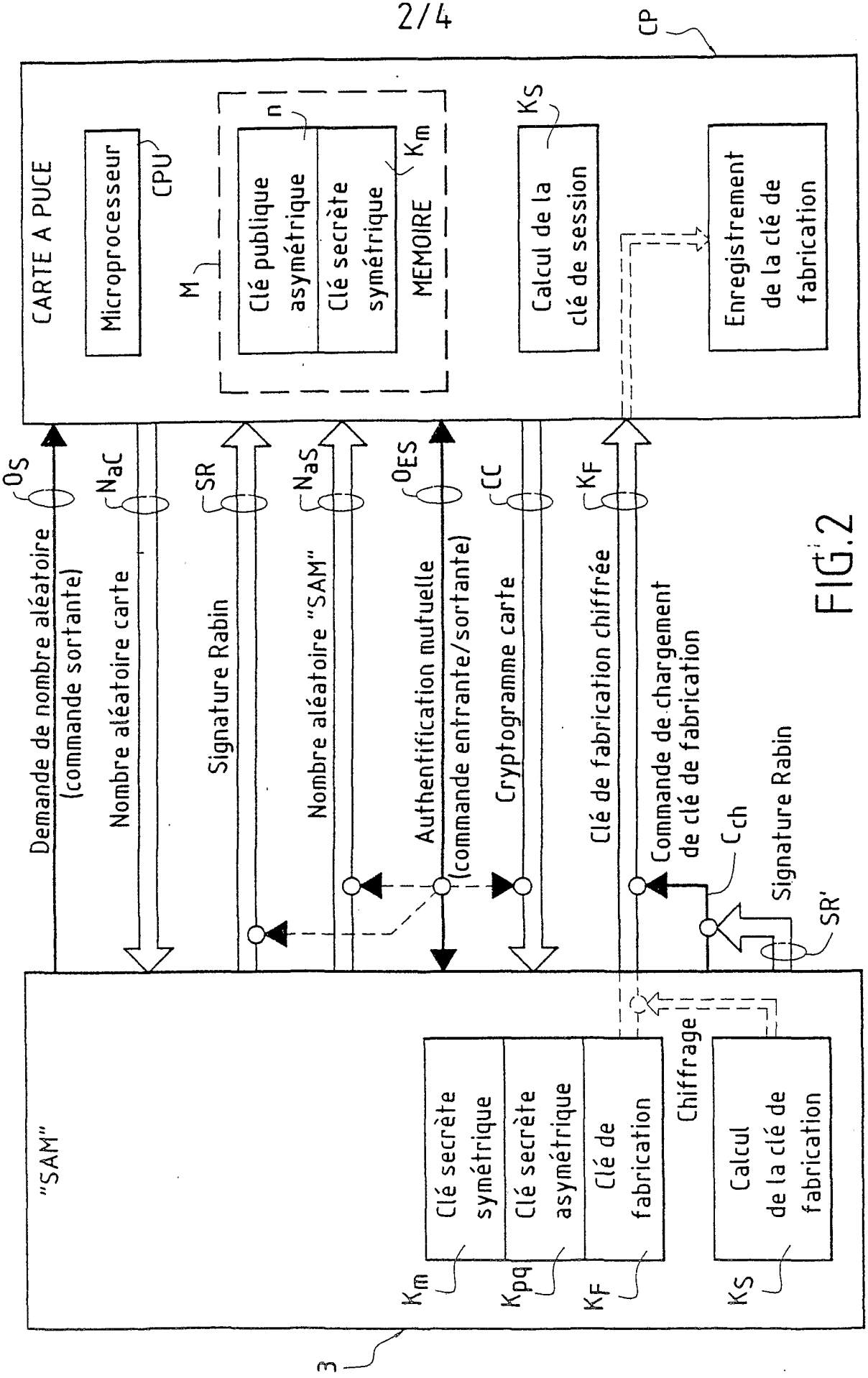

CP
CARTE A PUCE
Microprocesseur
CPU
M
n
Clé publique asymétrique
Clé secrète symétrique
K_m
MEMOIRE
K_S
Calcul de la clé de session
Enregistrement de la clé de fabrication
O_S
Demande de nombre aléatoire (commande sortante)
N_{aC}
Nombre aléatoire carte
SR
Signature Rabin
N_{aS}
Nombre aléatoire "SAM"
O_{ES}
Authentification mutuelle (commande entrante/sortante)
CC
Cryptogramme carte
K_F
Clé de fabrication chiffrée
Commande de chargement de clé de fabrication
C_{ch}
Signature Rabin
SR'
"SAM"
Clé secrète symétrique
Clé secrète asymétrique
Clé de fabrication
Chiffrage
Calcul de la clé de fabrication
K_m
K_{pq}
K_F
K_S
3

FIG.2

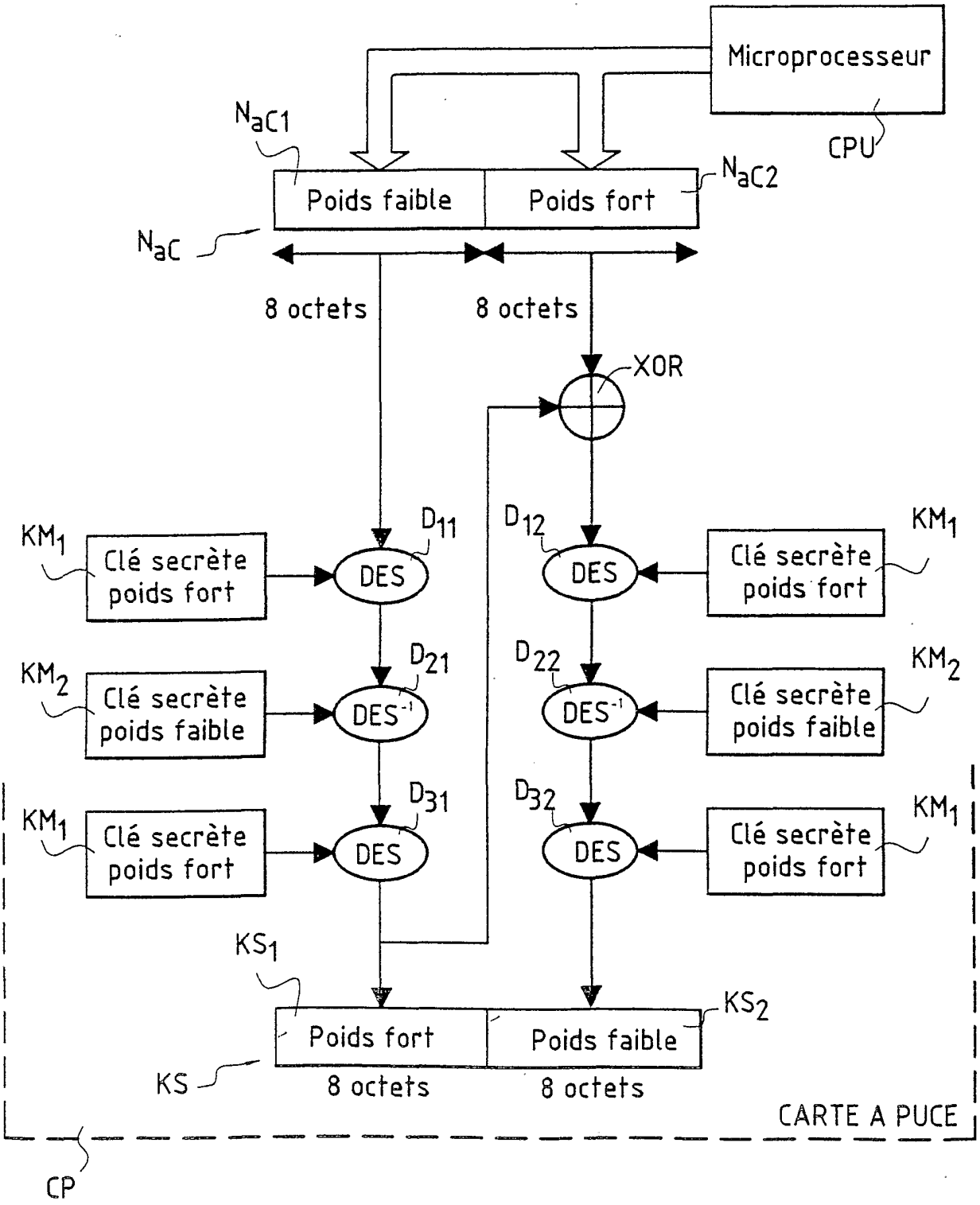

Microprocesseur
CPU
N_{aC1}
N_{aC2}
Poids faible
Poids fort
N_{aC}
8 octets
8 octets
XOR
KM_1
Clé secrète poids fort
D_{11}
DES
D_{12}
DES
KM_1
Clé secrète poids fort
KM_2
Clé secrète poids faible
D_{21}
DES^{-1}
D_{22}
DES^{-1}
KM_2
Clé secrète poids faible
KM_1
Clé secrète poids fort
D_{31}
DES
D_{32}
DES
KM_1
Clé secrète poids fort
KS_1
KS_2
Poids fort
Poids faible
KS
8 octets
8 octets
CARTE A PUCE
CP

FIG.4

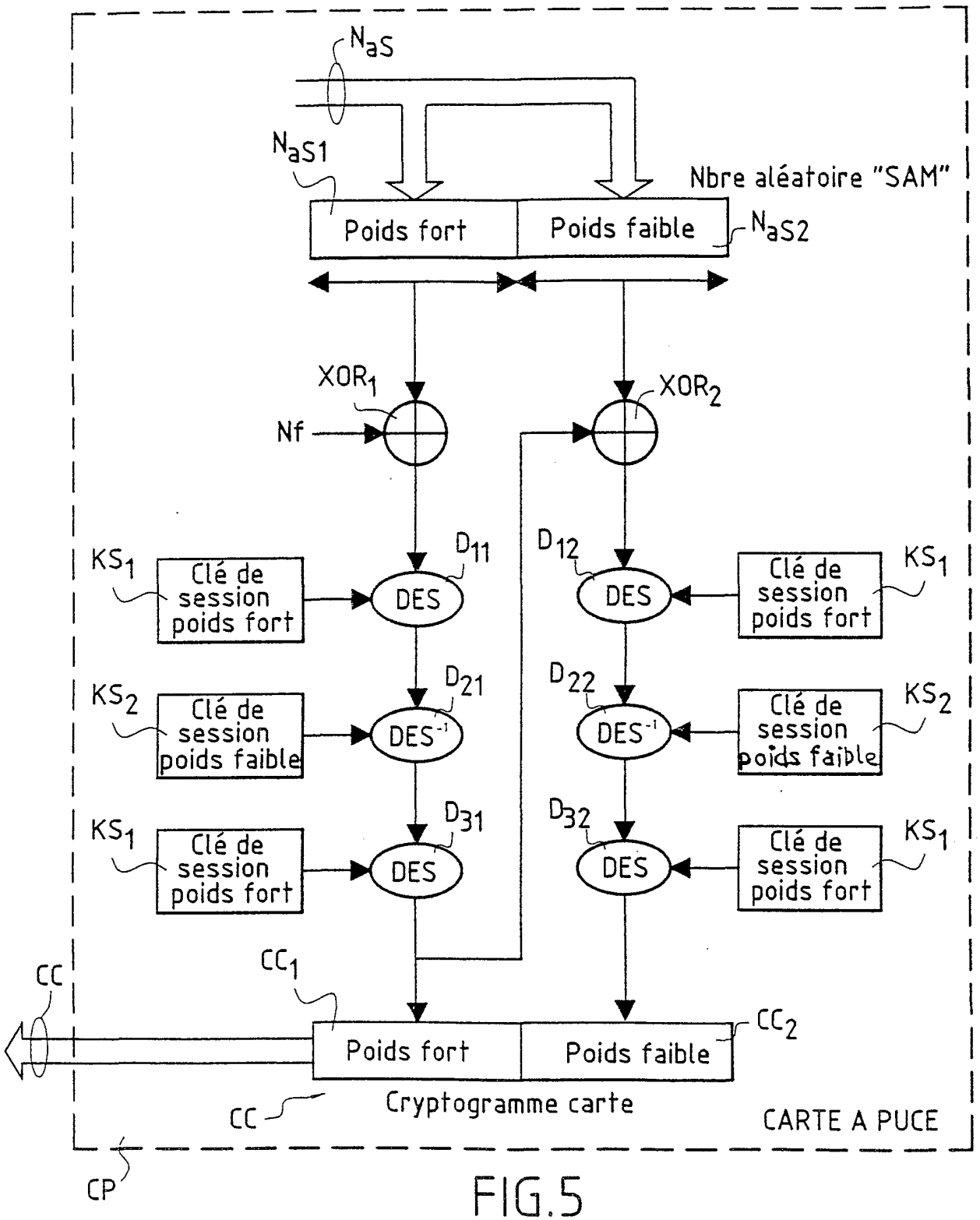
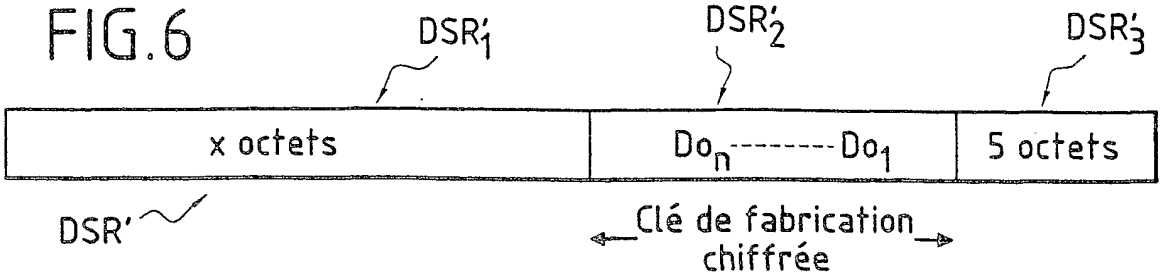

N_{aS}
N_{aS1}
Nbre aléatoire "SAM"
Poids fort
Poids faible
N_{aS2}
XOR_1
XOR_2
Nf
KS_1
Clé de session poids fort
D_{11}
DES
D_{12}
KS_2
Clé de session poids faible
D_{21}
DES^{-1}
D_{22}
D_{31}
D_{32}
CC
CC_1
CC_2
Cryptogramme carte
CARTE A PUCE
CP

FIG.5

FIG.6


DSR'_1
DSR'_2
DSR'_3
x octets
Do_n ------- Do_1
5 octets
DSR'
Clé de fabrication chiffrée

INTERNATIONAL SEARCH REPORT

Inte nal Application No
PCT/FR 01/01774

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 759 833 A (GEMPLUS SOCIETE EN COMMANDITE PAR ACTIONS) 21 August 1998 (1998-08-21) page 1, line 1 -page 6, line 15 page 6, line 32 -page 11, line 16; figures 1,2 ---	1,10
A	FR 2 760 871 A (CP8 TRANSAC) 18 September 1998 (1998-09-18) page 2, line 1 -page 3, line 21 page 4, line 11 -page 13, line 14; figures 1-6 ---	1,10
A	EP 0 285 520 A (BULL CP8) 5 October 1988 (1988-10-05) column 4, line 14 -column 6, line 10 column 6, line 58 -column 15, line 31; figures 1-7 --- -/--	1,10

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 September 2001	10/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Rivero, C

INTERNATIONAL SEARCH REPORT

Inte ıal Application No
PCT/FR 01/01774

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 33033 A (VISA INTERNATIONAL SERVICE ASSOCIATION) 1 July 1999 (1999-07-01) page 11, line 24 -page 26, line 14; figures 3-9	1,10
A	FR 2 767 624 A (ACTIVCARD SOCIETE ANONYME) 26 February 1999 (1999-02-26) page 8, line 10 -page 22, line 25; figures 1-5	1,10
A	EP 0 440 800 A (NTT DATA COMMUNICATIONS SYSTEMS CORPORATION) 14 August 1991 (1991-08-14) column 3, line 42 -column 10, line 39; figures 1-4	1,10

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte al Application No
PCT/FR 01/01774

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2759833 A	21-08-1998	FR 2759833 A1	21-08-1998
		AU 6504298 A	09-09-1998
		WO 9837525 A1	27-08-1998
FR 2760871 A	18-09-1998	FR 2760871 A1	18-09-1998
		AU 6922898 A	29-09-1998
		BR 9804778 A	17-08-1999
		EP 0914640 A1	12-05-1999
		WO 9840853 A1	17-09-1998
		JP 11510678 T	14-09-1999
		NO 985275 A	01-12-1998
EP 285520 A	05-10-1988	FR 2613565 A1	07-10-1988
		AT 84651 T	15-01-1993
		CA 1299266 A1	21-04-1992
		DE 3877401 A1	25-02-1993
		DE 3877401 T2	06-05-1993
		DK 181888 A	04-10-1988
		EP 0285520 A1	05-10-1988
		ES 2037852 T3	01-07-1993
		FI 881540 A ,B,	04-10-1988
		HK 92195 A	16-06-1995
		JP 1173939 A	10-07-1989
		JP 2059150 C	10-06-1996
		JP 7093622 B	09-10-1995
		MX 169350 B	30-06-1993
		NO 174730 B	14-03-1994
		US 4910773 A	20-03-1990
WO 9933033 A	01-07-1999	AU 1932499 A	12-07-1999
		EP 1040456 A2	04-10-2000
		WO 9933033 A2	01-07-1999
FR 2767624 A	26-02-1999	FR 2767624 A1	26-02-1999
		AU 735885 B2	19-07-2001
		AU 9077098 A	16-03-1999
		CN 1271448 T	25-10-2000
		EP 1004100 A1	31-05-2000
		WO 9910848 A1	04-03-1999
EP 440800 A	14-08-1991	JP 2731945 B2	25-03-1998
		JP 3007399 A	14-01-1991
		EP 0440800 A1	14-08-1991
		WO 9014962 A1	13-12-1990

RAPPORT DE RECHERCHE INTERNATIONALE

De ternationale No
PCT/FR 01/01774

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, PAJ, EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FR 2 759 833 A (GEMPLUS SOCIETE EN COMMANDITE PAR ACTIONS) 21 août 1998 (1998-08-21) page 1, ligne 1 -page 6, ligne 15 page 6, ligne 32 -page 11, ligne 16; figures 1,2	1,10
A	FR 2 760 871 A (CP8 TRANSAC) 18 septembre 1998 (1998-09-18) page 2, ligne 1 -page 3, ligne 21 page 4, ligne 11 -page 13, ligne 14; figures 1-6	1,10
A	EP 0 285 520 A (BULL CP8) 5 octobre 1988 (1988-10-05) colonne 4, ligne 14 -colonne 6, ligne 10 colonne 6, ligne 58 -colonne 15, ligne 31; figures 1-7	1,10

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
28 septembre 2001	10/10/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Rivero, C

RAPPORT DE RECHERCHE INTERNATIONALE

Den Internationale No
PCT/FR 01/01774

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	WO 99 33033 A (VISA INTERNATIONAL SERVICE ASSOCIATION) 1 juillet 1999 (1999-07-01) page 11, ligne 24 -page 26, ligne 14; figures 3-9	1,10
A	FR 2 767 624 A (ACTIVCARD SOCIETE ANONYME) 26 février 1999 (1999-02-26) page 8, ligne 10 -page 22, ligne 25; figures 1-5	1,10
A	EP 0 440 800 A (NTT DATA COMMUNICATIONS SYSTEMS CORPORATION) 14 août 1991 (1991-08-14) colonne 3, ligne 42 -colonne 10, ligne 39; figures 1-4	1,10

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 01/01774

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
FR 2759833	A	21-08-1998	FR	2759833 A1	21-08-1998
			AU	6504298 A	09-09-1998
			WO	9837525 A1	27-08-1998
FR 2760871	A	18-09-1998	FR	2760871 A1	18-09-1998
			AU	6922898 A	29-09-1998
			BR	9804778 A	17-08-1999
			EP	0914640 A1	12-05-1999
			WO	9840853 A1	17-09-1998
			JP	11510678 T	14-09-1999
			NO	985275 A	01-12-1998
EP 285520	A	05-10-1988	FR	2613565 A1	07-10-1988
			AT	84651 T	15-01-1993
			CA	1299266 A1	21-04-1992
			DE	3877401 A1	25-02-1993
			DE	3877401 T2	06-05-1993
			DK	181888 A	04-10-1988
			EP	0285520 A1	05-10-1988
			ES	2037852 T3	01-07-1993
			FI	881540 A ,B,	04-10-1988
			HK	92195 A	16-06-1995
			JP	1173939 A	10-07-1989
			JP	2059150 C	10-06-1996
			JP	7093622 B	09-10-1995
			MX	169350 B	30-06-1993
			NO	174730 B	14-03-1994
			US	4910773 A	20-03-1990
WO 9933033	A	01-07-1999	AU	1932499 A	12-07-1999
			EP	1040456 A2	04-10-2000
			WO	9933033 A2	01-07-1999
FR 2767624	A	26-02-1999	FR	2767624 A1	26-02-1999
			AU	735885 B2	19-07-2001
			AU	9077098 A	16-03-1999
			CN	1271448 T	25-10-2000
			EP	1004100 A1	31-05-2000
			WO	9910848 A1	04-03-1999
EP 440800	A	14-08-1991	JP	2731945 B2	25-03-1998
			JP	3007399 A	14-01-1991
			EP	0440800 A1	14-08-1991
			WO	9014962 A1	13-12-1990