PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/10	A1	(11) Numéro de publication internationale: **WO 99/10848**
		(43) Date de publication internationale: 4 mars 1999 (04.03.99)

(21) Numéro de la demande internationale: PCT/FR98/01820

(22) Date de dépôt international: 19 août 1998 (19.08.98)

(30) Données relatives à la priorité:
97/10548 21 août 1997 (21.08.97) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: ACTIVCARD [FR/FR]; 24–28, avenue du Général de Gaulle, F–92156 Suresnes Cedex (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: AUDEBERT, Yves, Louis, Gabriel [FR/FR]; 2, allée Jehan–le–Jeune, F–78290 Croissy–sur–Seine (FR).

(74) Mandataire: CABINET DE BOISSE ET COLAS; 37, avenue Franklin D. Roosevelt, F–75008 Paris (FR).

(81) Etats désignés: AU, CA, CN, JP, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

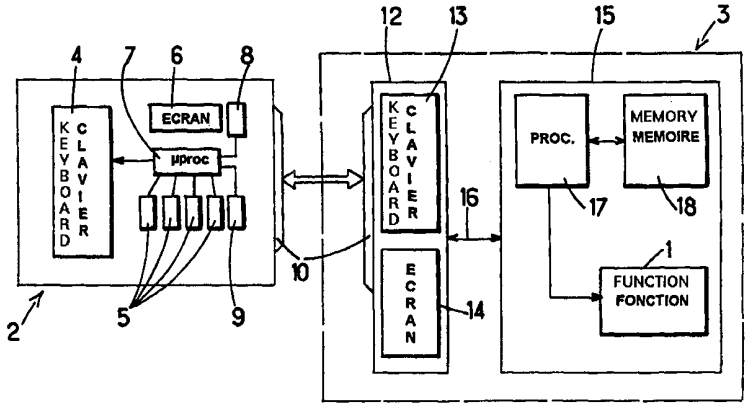
Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: PORTABLE ELECTRONIC DEVICE FOR SAFE COMMUNICATION SYSTEM, AND METHOD FOR INITIALISING ITS PARAMETERS

(54) Titre: DISPOSITIF PORTABLE ELECTRONIQUE POUR SYSTEME DE COMMUNICATION SECURISEE, ET PROCEDE D'INITIALISATION DE SES PARAMETRES

(57) Abstract

The invention concerns a portable electronic device for safe communication with at least one electronic unit comprising means for data storage (8, 9), means (10) interfacing with at least an external tool for loading data in said storage means, and means for data processing (7) including initialisation means for enabling, in response to the application of a secret personalization access code, to modify said access code and personalization data loading into said storage means. Said device comprises a plurality of functions and particular re–programmable secret access codes different from one another (K_{PERX}, K_{PERY}) and each assigned to personalizing a particular function (X, Y...) of said device, and inhibiting means (7; 222) adapted for authorising said processing means access to loading and/or reading personalization data particular to a function only in response to the application of the access code assigned to said function.



6,14... DISPLAY
7... MICROPROCESSOR
15... PROCESSOR

(57) Abrégé

Ce dispositif portable électronique sécurisé de communication avec au moins une unité électronique comprend des moyens de mémorisation de données (8, 9), des moyens (10) d'interface avec au moins un outil extérieur pour charger des données dans lesdits moyens de mémorisation, et des moyens de traitement de données (7) comprenant des moyens d'initialisation pour permettre, en réponse à l'application d'un code secret d'accès en personnalisation, la modification dudit code d'accès et le chargement de données de personnalisation dans lesdits moyens de mémorisation. Ce dispositif comprend une pluralité de fonctions et de codes secrets d'accès particuliers reprogrammables différents les uns des autres (K_{PERX}, K_{PERY}) et affectés chacun à la personnalisation d'une fonction particulière (X, Y, ...) dudit dispositif, et des moyens d'inhibition (7; 222) adaptés pour n'autoriser l'accès desdits moyens de traitement au chargement et/ou à la lecture de données de personnalisation particulières à une fonction qu'en réponse à l'application du code d'accès particulier affecté à ladite fonction.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

Dispositif portable électronique pour système de communication sécurisée, et procédé d'initialisation de ses paramètres.

La présente invention est relative d'une manière générale aux systèmes de communication électronique sécurisée et, plus particulièrement, à de tels systèmes dans lesquels des dispositifs portables électroniques sécurisés permettent d'établir une communication avec et/ou d'accéder à une autre unité électronique.

De nombreux systèmes de communication électronique nécessitent de contrôler l'accès des utilisateurs à des applications déterminées, ce contrôle impliquant généralement d'authentifier des personnes et/ou des messages. Tel est le cas notamment lorsqu'il s'agit de contrôler l'accès à un ordinateur ou plus généralement à un réseau informatique dont l'utilisation est réservée à des personnes s'étant dûment légitimées. De tels réseaux peuvent servir, par exemple, à assurer toutes sortes de services impliquant une transaction, le plus souvent à contrepartie économique, tels que le télé-achat, la télévision à péage, la banque à domicile, les jeux télévisés interactifs, etc....

Des systèmes de contrôle d'accès sont notamment décrits dans les documents US-A-3 806 874, US-A-4 601 011, US-A-4 720 860, US-A-4 800 590 et US-A-5 060 263. Les systèmes décrits dans ces documents font appel à un dispositif portable électronique sécurisé qui génère un mot de passe par chiffrement d'une variable. Une unité de vérification effectue le même calcul ou un calcul similaire sur la même ou approximativement la même variable et autorise l'accès à l'application demandée s'il y a concordance entre les mots de passe générés dans le dispositif portable et l'unité de vérification. La variable peut être un nombre aléatoire ou pseudo-aléatoire, ci-après appelé aléa, transmis de l'unité de vérification au dispositif portable, ou bien elle peut être générée indépendamment dans

le dispositif portable et l'unité de vérification au moyen, par exemple, d'une horloge et/ou d'un compteur d'événements.

Lorsque le chiffrement mis en œuvre dans le dispositif portable et l'unité de vérification fait appel à un algorithme symétrique et une clé secrète, par exemple l'algorithme DES (Data Encryption Standard), la sécurité du système repose sur la préservation du caractère secret de la clé stockée à la fois dans le dispositif portable et l'unité de vérification.

Dans certains cas, la clé peut être statique, c'est-à-dire qu'elle conserve la même valeur pendant toute la durée de vie du dispositif portable.

Dans d'autres cas, la clé peut être dynamique, c'est-à-dire qu'elle évolue avec le temps en fonction, par exemple, du contenu d'un compteur incrémenté par un signal d'horloge et/ou d'un compteur d'événements.

Que la clé soit statique ou dynamique, elle doit présenter initialement, c'est-à-dire lors de la personnalisation du dispositif, une valeur déterminée qui est stockée à la fois dans le dispositif portable électronique et dans une base de données associée à l'unité de vérification. Lorsqu'un utilisateur effectue une demande d'accès, il doit d'une manière ou d'une autre, par exemple au moyen d'un numéro d'identification public ou d'un numéro d'identification personnelle (PIN), s'identifier auprès de l'unité de vérification qui obtient de la base de données la clé statique ou, s'il s'agit d'une clé dynamique, les informations éventuellement nécessaires pour calculer la clé en cours.

Les problèmes de sécurité se posent dans les mêmes termes dans les systèmes de communication électronique sécurisée à dispositifs portables électroniques et unité(s) de vérification qui font appel à un chiffrement et au déchiffrement par algorithme asymétrique à clé(s) publique(s) et clé(s) privée(s). Suivant les mécanismes mis en œuvre au moyen d'un tel algorithme (authentification, signature, etc.....) le caractère secret d'une ou plusieurs des clés stockées dans les dispositifs et/ou les unités de vérification doit en effet être conservé.

Lors du processus de personnalisation cette ou ces clés et d'autres données de personnalisation secrètes sont chargées en mémoire dans le dispositif par l'entité qui livre le dispositif à l'utilisateur final. Afin de protéger ces données de personnalisation, il est connu, notamment par le document WO 93/10509, de permettre au fournisseur d'une carte à mémoire de substituer une nouvelle clé maître d'accès aux données de personnalisation à la clé initiale qui a été implantée par le fabricant de la carte.

Par ailleurs, le grand développement que connaissent les systèmes de communication électronique sécurisée conduit à concevoir des produits permettant la mise en œuvre de plusieurs applications différentes et présentant plusieurs niveaux de sécurité pour une même application. Le problème qui se pose alors est de garantir l'indépendance des applications et des niveaux de sécurité associés, c'est-à-dire des différentes fonctions mises en œuvre par le dispositif.

L'invention a entre autres buts de fournir un dispositif portable électronique sécurisé de communication avec une autre unité électronique qui permette d'assurer une telle indépendance des fonctions.

A cet effet l'invention concerne un tel dispositif comprenant des moyens de mémorisation de données, des moyens d'interface avec au moins un outil extérieur pour charger des données dans lesdits moyens de mémorisation, des moyens de traitement de données comprenant des moyens d'initialisation pour permettre, en réponse à l'application d'un code secret d'accès en personnalisation, la modification dudit code d'accès et le chargement de données de personnalisation dans lesdits moyens de mémorisation, caractérisé en ce que ledit dispositif est adapté à la mise en œuvre d'une pluralité de fonctions et comporte des moyens de chargement d'une pluralité de données secrètes particulières représentatives respectivement de codes secrets d'accès particuliers différents les uns des autres et affectés chacun à la personnalisation d'une fonction particulière dudit dispositif, et des moyens d'inhibition adaptés pour n'autoriser l'accès

desdits moyens de traitement au chargement et/ou à la lecture de données de personnalisation particulières à une fonction qu'en réponse à l'application du code d'accès particulier affecté à ladite fonction.

Suivant une caractéristique de l'invention, lesdits moyens d'inhibition sont adaptés pour interdire l'accès en lecture à l'une quelconque desdites données secrètes.

Suivant une autre caractéristique de l'invention, lesdits moyens de chargement comprennent au moins une donnée secrète spécifique reprogrammable représentative d'un code secret spécifique commun à l'ensemble desdites fonctions et lesdits moyens d'inhibition sont adaptés pour interdire l'accès desdits moyens de traitement auxdites données de personnalisation particulières par l'intermédiaire dudit code secret spécifique.

Suivant une autre caractéristique de l'invention, lesdits moyens de traitement de données sont adaptés pour autoriser une modification d'une donnée secrète représentative d'un code d'accès particulier à une fonction et chargée dans lesdits moyens de mémorisation via ledit code secret d'accès spécifique, en réponse à l'application dudit code d'accès particulier.

Suivant une autre caractéristique de l'invention, lesdits moyens de chargement sont adaptés pour autoriser, au moyen de ladite donnée secrète spécifique reprogrammable, l'effacement de données secrètes particulières et de données de personnalisation particulières préalablement chargées et le chargement de nouvelles données secrètes particulières.

De préférence, ledit code secret spécifique est un code d'accès à la personnalisation de données de personnalisation communes à l'ensemble desdites fonctions du dispositif.

Selon encore d'autres caractéristiques de l'invention considérées seules ou en combinaison :

- lesdits moyens de mémorisation comprennent au moins une mémoire permanente dans laquelle est stockée une clé secrète de base,

lesdits moyens d'initialisation comprenant des premiers moyens pour calculer une valeur initiale de ladite donnée secrète spécifique en fonction de ladite clé secrète de base et d'un paramètre secret initial ;

- lesdits moyens d'inhibition sont adaptés pour effacer desdits moyens de mémorisation l'une desdites données secrètes représentatives d'un code d'accès en réponse au chargement, au moyen dudit code d'accès, d'une nouvelle donnée secrète représentative d'un nouveau code d'accès ;

- ladite donnée secrète est une clé secrète de calcul d'un code de vérification du code d'accès dont ladite donnée est représentative ;

- lesdits moyens de traitement comprennent des seconds moyens pour calculer ledit code de vérification par chiffrement d'une variable au moyen de ladite clé secrète de calcul ;

- lesdites données de personnalisation comprennent au moins une pluralité de clés secrètes d'authentification différentes les unes des autres et affectées chacune à l'une desdites fonctions et en ce que lesdits moyens de traitement comprennent des troisièmes moyens pour calculer un code d'authentification vis-à-vis d'une unité de vérification en fonction de l'une desdites clés secrètes d'authentification.

L'invention a également pour objet un procédé d'initialisation d'un dispositif tel que défini ci-dessus, caractérisé en ce qu'il comprend :

- un premier stade d'initialisation consistant à définir et à stocker dans lesdits moyens de mémorisation une clé de personnalisation spécifique audit dispositif,

- un deuxième stade de personnalisation consistant à charger dans lesdits moyens de mémorisation, au moyen d'un code d'accès spécifique fonction de ladite clé de personnalisation spécifique, des données de personnalisation communes auxdites fonctions et des clés secrètes de calcul desdits codes secrets d'accès particuliers affectés chacun au chargement de données de personnalisation relatives à l'une desdites fonctions, et

- un troisième stade de personnalisation consistant, pour chacune desdites fonctions, à charger dans lesdits moyens de mémorisation, au

moyen du code secret d'accès particulier correspondant, les données de personnalisation relatives à ladite fonction.

De préférence, ledit troisième stade comprend l'étape consistant, lors du chargement des données de personnalisation relatives à au moins l'une desdites fonctions, à modifier ladite clé secrète de calcul dudit code secret d'accès particulier affecté à ladite fonction.

Suivant une caractéristique de l'invention, le premier stade d'initialisation du procédé défini ci-dessus comprend :

- au moins une première phase d'initialisation consistant à définir au moins une donnée secrète commune à un ensemble de dispositifs destinés à une même entité,
- au moins une deuxième phase d'initialisation comprenant les étapes consistant, pour chaque dispositif dudit ensemble, à :

a) lire une donnée d'identification spécifique portée par ledit dispositif,

b) calculer une première clé de personnalisation spécifique en fonction de ladite donnée secrète commune, et de ladite donnée d'identification,

c) stocker ladite donnée d'identification et ladite première clé de personnalisation spécifique dans lesdits moyens de mémorisation, et

- au moins une troisième phase d'initialisation comprenant les étapes consistant, pour chaque dispositif dudit ensemble, à :

d) extraire ladite donnée d'identification spécifique dudit dispositif,

e) calculer dans un premier outil extérieur ladite première clé de personnalisation spécifique en fonction de ladite donnée secrète commune et de ladite donnée d'identification spécifique,

f) calculer dans ledit outil extérieur un premier code d'accès en fonction de ladite première clé de personnalisation spécifique et d'un aléa transmis par ledit dispositif,

g) transmettre dudit premier outil audit dispositif ledit premier code d'accès avec des paramètres de personnalisation comprenant une deuxième clé de personnalisation différente de ladite première clé de personnalisation,

h) calculer dans ledit dispositif un code de vérification dudit premier code d'accès en fonction de ladite première clé de personnalisation spécifique et dudit aléa,

i) comparer dans ledit dispositif ledit premier code d'accès et ledit code de vérification et, en réponse à une cohérence desdits codes,

j) stocker lesdits paramètres de personnalisation dans lesdits moyens de mémorisation, et

k) substituer ladite deuxième clé de personnalisation à ladite première clé de personnalisation dans lesdits moyens de mémorisation.

Selon une forme de mise en œuvre, ledit procédé est caractérisé en ce qu'il comprend une quatrième phase consistant à stocker initialement une clé secrète de base commune dans une mémoire permanente desdits moyens de mémorisation et en ce que les étapes a) et b) consistent à :

- appliquer ladite donnée secrète et ladite clé de base à un deuxième outil extérieur,
- lire ladite donnée d'identification au moyen dudit deuxième outil,
- calculer ladite clé de personnalisation spécifique au moyen dudit deuxième outil,
- chiffrer dans ledit deuxième outil extérieur ladite clé de personnalisation spécifique au moyen de ladite clé de base commune,
- transmettre dudit deuxième outil audit dispositif le résultat dudit chiffrement, et
- déchiffrer ledit résultat dans ledit dispositif au moyen de ladite clé de base pour restituer ladite clé de personnalisation spécifique.

Selon une autre forme de mise en œuvre, ledit procédé est caractérisé en ce qu'il comprend une quatrième phase consistant à stocker

initialement une clé de base commune dans une mémoire permanente desdits moyens de mémorisation, en ce que ladite première phase consiste également à chiffrer ladite donnée secrète commune au moyen de ladite clé de base commune et à appliquer le résultat dudit chiffrement à un deuxième outil extérieur, et en ce que ladite deuxième phase consiste également à :

a) lire ladite donnée d'identification spécifique au moyen dudit deuxième outil et transmettre ladite donnée d'identification et le résultat dudit chiffrement audit dispositif,

b) déchiffrer ledit résultat dans ledit dispositif au moyen de ladite clé de base pour restituer ladite donnée secrète commune puis calculer ensuite ladite clé de personnalisation spécifique.

L'invention a encore pour objet un système de communication sécurisée comprenant un ensemble de dispositifs tels que définis ci-dessus et au moins un outil d'initialisation de paramètres de personnalisation pour la mise en oeuvre de la troisième phase du procédé défini ci-dessus.

Selon une caractéristique de l'invention, ledit système comprend en outre un outil d'initialisation de paramètres de production pour la mise en œuvre de la deuxième phase du procédé défini ci-dessus.

Enfin, l'invention a pour objet un système de communication sécurisée comprenant un ensemble de dispositifs comportant des moyens tels que définis ci-dessus pour la mise en oeuvre de mécanismes d'authentification et au moins une unité de vérification.

D'autres caractéristiques et avantages de l'invention résulteront de la description qui va suivre de modes de réalisation donnés à titre d'exemple et illustrés par les dessins annexés sur lesquels :

la figure 1 est un schéma général d'un système de communication sécurisée selon l'invention appliqué au contrôle d'accès ;

la figure 2 est un diagramme illustrant les mécanismes d'initialisation en production des paramètres du dispositif portable électronique faisant partie du système de la figure 1 ;

la figure 3 est un diagramme illustrant une variante des mécanismes d'initialisation en production des paramètres du dispositif portable électronique faisant partie du système de la figure 1 ;

la figure 4 est un diagramme illustrant les mécanismes d'initialisation des paramètres de personnalisation du dispositif portable d'électronique faisant partie du système de la figure 1 ; et

la figure 5 est un organigramme général illustrant sous forme synthétique les différentes phases d'initialisation du dispositif portable électronique faisant partie du système de la figure 1.

Le système de contrôle d'accès représenté à la figure 1 est supposé donner un accès conditionnel à une application qui est symbolisée par le rectangle 1. Le terme "application" doit être pris dans une acception très large. Il désigne toute application à laquelle l'accès est conditionné par une autorisation faisant intervenir une authentification impliquant une vérification du dispositif (carte) à l'aide duquel la demande est formulée, et de préférence également une identification de la personne demandant l'accès à l'application pour savoir si sa demande est légitime.

L'application peut être de toute nature, par exemple le contrôle d'accès à un local, à un réseau informatique ou à un ordinateur, la mise en œuvre d'une transaction pécuniaire ou autre (télé-achat, banque à domicile, jeux télévisés inter-actifs, télévision à péage), etc... Par ailleurs, l'authentification de personnes et/ou de messages (signature électronique) tombe expressément dans la portée de la présente invention.

Selon l'exemple de réalisation illustré à la figure 1, le système de contrôle d'accès comprend une première unité ou dispositif portable 2 également appelé ci-après "carte" et au moins une seconde unité de vérification 3. Le système de contrôle d'accès selon l'invention peut comporter un grande nombre de cartes 2 et une ou plusieurs unités de vérification 3, mais en tout cas en un nombre généralement plus faible. Les nombres des cartes 2 et des unités 3 ne sont nullement limitatifs de l'invention.

La carte 2 se présente par exemple sous la forme d'une calculette ou d'une carte de crédit et elle comporte un clavier 4 destiné à permettre l'introduction d'informations, telles que par exemple un numéro d'identification personnel PIN, ainsi que diverses touches de fonction 5. Elle comporte également un écran d'affichage 6, par exemple à cristaux liquides, et est dotée d'un circuit électronique intégré comportant un microcontrôleur programmé 7 ainsi qu'une mémoire morte permanente 8 de type ROM et une mémoire reprogrammable 9 constituée par de la mémoire RAM et éventuellement de la mémoire EEPROM. La mémoire permanente 8 et la mémoire reprogrammable 9 sont inaccessibles de l'extérieur de la carte et les bus de données et d'adresses du microcontrôleur 7 sont également inaccessibles de l'extérieur de manière à rendre impossible une lecture ou une modification frauduleuse, depuis l'extérieur, des informations contenues dans les mémoires 8 et 9.

La zone mémoire permanente 8 (ROM) comprend une zone programme et une zone donnée.

La zone programme comprend des instructions de programme relatives à la mise en œuvre des mécanismes suivants :

1. les mécanismes de sécurité
   - identification du porteur
   - authentification du porteur vis-à-vis de l'unité de vérification
   - authentification de l'unité de vérification et de l'unité de personnalisation
   - authentification de message
   - chiffrement/déchiffrement
   - éventuellement signature électronique
   - .....
2. les mécanismes de personnalisation
   - lors de la fabrication
   - lors des différentes personnalisations chez le ou les clients
3. les mécanismes relatifs à la ou aux applications de la carte

4. les mécanismes de communication

- communication avec l'utilisateur : affichage, clavier,
- communication avec l'unité de vérification ou de personnalisation
  * infrarouge
  * DTMF
  * communication avec un lecteur
- communication avec une carte à puce
- etc.....

La zone donnée comprend les données communes à un masque de fabrication :

1. clé ROM (K_{ROM})
2. le numéro de version du logiciel
3. etc.....

La zone mémoire reprogrammable 9 de type RAM et éventuellement EEPROM stocke les informations décrits ci-après :

1. Les données introduites lors des différentes phases d'initialisation des paramètres de production et des paramètres de personnalisation :

Ces données sont structurées selon les niveaux de sécurité et selon les applications, la modification d'une zone de données est conditionnée par l'authentification de l'entité demandeur de la personnalisation : code d'accès fonction d'un aléa généré par la carte, signature, ...

Ces données peuvent être secrètes (clés secrètes) ou être consultables mais non modifiables, il s'agit de :

* clés secrètes de personnalisation
* clés secrètes relatives aux mécanismes de sécurité : authentification d'entité, authentification de message, génération d'aléas,
* données relatives à l'application : contenu des messages, types de mécanismes de sécurité requis,.....
* données relatives à l'exploitation de la carte dans une application donnée : longueur exigée pour le numéro d'identification personnel (PIN), longueur de l'aléa, format du code d'accès,.....

* données communes à toutes les applications : valeur du PIN, valeur de l'horloge, valeur des compteurs, contenu des messages standards.

2. Les données de travail

La carte 2 comporte également un dispositif de communication 10 permettant de communiquer avec l'unité de vérification 3, ou bien avec un outil de fabrication ou un outil de personnalisation comme cela sera décrit dans la suite, soit directement, soit par une liaison de transmission à plus ou moins longue distance. Ce dispositif de communication 10 peut se présenter sous de nombreux aspects, par exemple une liaison câblée bidirectionnelle, une liaison téléphonique bidirectionnelle en DTMF, une liaison bidirectionnelle par rayons infrarouges, une liaison bidirectionnelle dite "en mode connecté" dans lequel la carte est insérée dans un lecteur approprié, des moyens de réception optique associés, dans l'unité 3, à des moyens de lecture d'informations affichées sur l'écran 6 comme décrit par exemple dans le document EP-A-0 399 897, ou tout autre dispositif de transmission bien connu dans la technique.

Enfin, une source d'énergie électrique (non représentée), par exemple une pile électrique de dimensions réduites, est prévue pour alimenter les divers circuits de la carte 2 et permettre son fonctionnement autonome.

L'unité 3 englobe tout d'abord des moyens d'interface permettant d'assurer la communication avec la carte 2 au moyen du dispositif de communication 10. Ces moyens d'interface, symbolisés par un rectangle 12, peuvent se présenter sous de nombreuses formes. Il peut s'agir par exemple d'un lecteur dédié, mais il peut s'agir également d'un terminal d'ordinateur, d'un ordinateur personnel inséré par exemple dans un réseau, etc... La particularité de ces moyens d'interface 12 est qu'ils permettent d'assurer la communication avec la ou les cartes 2 qui leur sont associées via le dispositif de communication 10.

Les moyens d'interface 12 peuvent comprendre également un clavier 13 et un écran d'affichage 14 pour permettre à un utilisateur d'introduire

des informations à communiquer à une partie 15 de l'unité 3, telles que par exemple des mots de passe ou des données à authentifier relatives à l'application 1. Toutefois, l'introduction de ces données peut être réalisée d'autres manières, notamment automatiquement sans intervention manuelle de l'utilisateur, par exemple par la simple introduction de la carte 2 dans l'interface 12 ou par émission de rayons infrarouges modulés commandée au moyen de l'une des touches de fonction 5.

L'interface 12 communique avec la partie 15 de l'unité 3 que l'on appellera "serveur". Cette communication symbolisée par la connexion 16 peut se faire à courte ou à longue distance par tout moyen approprié. Les informations circulant sur cette connexion sont notamment le mot de passe à contrôler dans le serveur 15 et éventuellement des données à authentifier et à exploiter dans le serveur.

Le serveur 15 comporte en particulier un processeur 17 et une mémoire 18. Le processeur 17 est capable de libérer conditionnellement les applications 1, visées par les demandes d'accès formulées par les cartes 2.

Le microcontrôleur 7 de la carte 2 est programmé pour assurer, en liaison avec l'unité de vérification 3, la sécurité de communications au sens large, par exemple l'authentification d'un utilisateur muni de la carte 2, la certification de messages, la sécurisation de transactions, etc... Ces mécanismes d'authentification, de certification, etc... sont bien connus des spécialistes de la technique et ils ne seront pas décrits en détail dans la présente demande. Ces mécanismes font appel au chiffrement et/ou au déchiffrement dans la carte 2 et/ou dans l'unité 3 d'une ou plusieurs informations par un algorithme à clé publique et clé privée ou d'un algorithme à clé secrète, clés qui sont stockées dans la mémoire programmable 9 associée au microcontrôleur 7 et/ou dans la mémoire 18 du "serveur" 15.

Dans la description qui va suivre, l'invention met en œuvre des algorithmes à clé secrète, mais il doit être compris qu'elle n'est nullement limitée à ce type d'algorithme.

C'est ainsi, par exemple, qu'une procédure d'authentification au moyen d'un algorithme à clé secrète consiste, après que l'utilisateur se soit identifié auprès de l'unité de vérification, à chiffrer une variable parallèlement dans la carte 2 et dans l'unité de vérification 3 au moyen de cet algorithme et d'une clé secrète partagée K_{SEA} et à comparer ensuite, généralement dans l'unité de vérification 3, les deux mots de passe A_{SEA} résultant du chiffrement de cette variable. Dans les systèmes dits asynchrones, cette variable est un nombre aléatoire généré par l'unité de vérification 3 et transmis à la carte 2. Dans les systèmes dits synchrones, cette variable est dynamique, c'est-à-dire qu'il s'agit d'un nombre qui, dans la carte 2 et l'unité 3, évolue dans le temps en fonction du contenu d'un compteur d'horloge et/ou d'un compteur d'événements. Les systèmes synchrones supposent, à certaines tolérances près, une concordance entre les contenus des compteurs d'horloge et/ou d'événements de la carte 2 et le contenu, à l'adresse associée à la carte 2, d'une base de données faisant partie de l'unité de vérification 3 ou à laquelle celle-ci a accès pour la mise en œuvre du processus d'authentification. Des exemples détaillés de ces mécanismes d'authentification sont donnés, par exemple, dans le document EP-A-0 338 936 et dans la demande de brevet français No. 96 04797 déposée le 17 Avril 1996 auxquels on pourra se reporter.

Comme indiqué précédemment, la ou les clés secrètes de chiffrement et/ou de déchiffrement mémorisées dans la carte 2 et le serveur 15 peuvent être statiques, c'est-à-dire qu'elles conservent la même valeur pendant toute la durée du produit, ou dynamiques, c'est-à-dire que leur valeur évolue avec le temps. La valeur des clés dynamiques peut elle-même être une fonction du contenu de compteurs d'horloge et/ou d'événements comme décrit par exemple dans la demande de brevet français No. 96 04798 déposée le 17 Avril 1996.

Qu'il s'agisse d'une clé statique ou d'une clé dynamique, il est nécessaire lors de la phase d'initialisation des paramètres de production ou des paramètres de personnalisation de la carte 2 de charger dans la

mémoire programmable 9 de celle-ci une valeur initiale qui constituera la clé statique, la clé dynamique initiale ou une racine permettant de calculer la clé dynamique initiale. Dans un système comportant un grand nombre de cartes, par exemple plusieurs milliers à plusieurs dizaines de milliers, la gestion d'une ou plusieurs clés secrètes propre à chaque carte et différentes chacune de celles de toutes les autres cartes pose des problèmes de sécurité. Il est en effet souhaitable que l'utilisateur final de la carte soit assuré que la sécurité offerte par celle-ci ne risque pas d'être mise en cause par suite des opérations de programmation mises en oeuvre en amont par la ou les entités chargées de l'initialisation des paramètres de production et/ou des paramètres de personnalisation de la carte.

Ces problèmes de sécurité sont encore accentués par les développements actuels des systèmes de communication sécurisée qui doivent être en mesure de répondre aux besoins liés à la multiplicité des applications et à la multiplicité des niveaux de sécurité pour une application. C'est ainsi, par exemple, que pour un système de sécurité de configuration donnée, c'est-à-dire un ensemble de cartes et les logiciels associés implantés dans les cartes 2 et les unités de vérification 3 en vue d'assurer des fonctionnalités déterminées, une même carte peut être utilisée pour différentes applications, par exemple l'authentification auprès d'un réseau informatique ou similaire pour accéder à une ou plusieurs ressources de ce réseau (l'accès à chaque ressource pouvant nécessiter une authentification distincte), le télé-achat, etc... De plus, pour une même application, il peut être prévu plusieurs niveaux de sécurité, par exemple suivant des catégories d'utilisateurs, de sorte que les cartes devront être personnalisées en fonction des utilisateurs finaux de celles-ci.

La multiplicité des applications pour un même système de sécurité et des niveaux de sécurité pour une même application, combinée aux différentes phases de vie que connaît le système entre sa fabrication et sa livraison à l'utilisateur final, font qu'il peut y avoir pour un même système,

simultanément ou non, plusieurs gestionnaires ou administrateurs responsables de la gestion des problèmes de sécurité.

Si l'on considère un cas simple où le système de sécurité ne comporte qu'une seule application, une carte peut, durant son cycle de vie, circuler entre un certain nombre d'entités, à savoir :

- le fabricant ou le fournisseur qui vend le système de sécurité au client ;

- un administrateur général, qui peut être le responsable sécurité du client, lequel peut avoir plusieurs sites géographiques, chaque site possédant sa propre organisation de gestion du système de sécurité qui est indépendante de celle des autres sites ;

- des administrateurs locaux responsables chacun de l'organisation du système de sécurité de l'entreprise au niveau d'un site géographique ; et

- les utilisateurs finaux qui seront chacun détenteur d'une carte 2 et qui utiliseront celle-ci au niveau d'un ou plusieurs sites géographiques déterminés.

La gestion d'un tel système de sécurité suppose, une fois qu'un lot de cartes a été vendu à un client par le fournisseur ou le fabricant, que seul l'administrateur général puisse utiliser ce lot de cartes et qu'un autre client ne puisse pas les utiliser. Il faut donc :

- d'une part que le fabricant ou le fournisseur initialise en production un certain nombre de paramètres communs à un lot de cartes destiné à un client donné qui seul pourra initialiser ses paramètres de personnalisation dans les cartes ;

- d'autre part assurer le caractère irréversible de l'opération de personnalisation par le client : une fois que l'administrateur général a personnalisé les cartes, ces dernières ne doivent plus pouvoir être utilisées par le fournisseur ou le fabricant.

Une fois en possession du lot de cartes, l'administrateur général va initialiser dans les cartes tous les paramètres de personnalisation communs à tous les sites. Les cartes seront ensuite réparties sur plusieurs

sites sur chacun desquels un administrateur local initialisera les paramètres de personnalisation propres au site concerné. Si des cartes doivent pouvoir être utilisées et reconnues sur plusieurs sites, elles seront données à un premier administrateur local pour être initialisées des paramètres de personnalisation du premier site, puis à un deuxième administrateur local pour être initialisées des paramètres de personnalisation du deuxième site, etc... Dans ce contexte, il sera nécessaire d'assurer l'indépendance des moyens de gestion c'est-à-dire que:

- un administrateur local X ne pourra initialiser que les paramètres de personnalisation du site X : le fait de pouvoir initialiser les paramètres de personnalisation du site X n'entraîne pas la possibilité d'initialiser les paramètres de personnalisation du site Y, ni de connaître les paramètres de personnalisation du site Y ;

- le fait d'être administrateur général n'entraîne pas la connaissance des paramètres de personnalisation des différents sites, ceci afin d'assurer l'indépendance de la gestion au niveau de chaque site.

Ces différentes fonctionnalités sont mises en œuvre au moyen de mécanismes d'initialisation des paramètres de production et des paramètres de personnalisation qui seront maintenant décrits en se reportant aux figures 2 à 4.

La figure 2 est un diagramme illustrant les mécanismes d'initialisation en production des données ou paramètres, ci-après appelés paramètres de production, qui sont communs à un lot de cartes destiné à un client donné. Sur cette figure, la colonne de gauche montre les opérations effectuées par le fournisseur de la carte, c'est-à-dire l'entité qui est responsable de la fourniture du système de sécurité au client. La colonne du milieu illustre les opérations qui sont mises en œuvre par un outil 20 de fabrication des cartes 2, le fabricant pouvant ou non être la même entité que le fournisseur. Enfin, la colonne de droite illustre les opérations qui sont mises en œuvre dans la carte 2. L'outil de fabrication 20 utilisé par le fabricant comprend des moyens matériels et logiciels

conventionnels qu'il n'y a pas lieu de décrire ici et qui permettent, entre autres, d'élaborer un certain nombre de données et de les transmettre aux cartes 2 pour en programmer la mémoire programmable 9.

Dans la colonne de gauche de la figure 2 apparaissent un certain nombre de clés secrètes K_{ROM}, K_{PEM}, K_{ALE} et K_{MES} qui sont communes à un lot de cartes destinées à un client donné.

La clé K_{ROM} est définie par le fournisseur et elle est connue de lui seul. Cette clé K_{ROM} est implantée dans la mémoire morte permanente 8 des cartes lors du masquage des circuits intégrés, mais elle n'est pas connue du fabricant des cartes 2 si celui-ci n'est pas la même entité que le fournisseur. A cet effet, elle peut par exemple être noyée sous forme chiffrée dans le logiciel de pilotage de l'outil de fabrication des cartes.

Les clés K_{PEM}, K_{ALE} et K_{MES} sont également choisies par le fournisseur et introduites sous forme chiffrée par celui-ci dans le logiciel de pilotage de l'outil de fabrication. Les valeurs de ces trois clés sont communiquées confidentiellement au client, de préférence séparément du lot de cartes qui lui est destiné. La clé K_{PEM} est une clé maître de personnalisation qui, comme cela sera décrit dans la suite, permet de générer une clé de personnalisation propre à chaque carte en fonction de son numéro de série. La clé K_{ALE} est une clé permettant aux cartes de générer des aléas et la clé K_{MES} est une clé qui permet de charger un alphabet et des messages dans les cartes.

Comme représenté sur la colonne centrale de la figure 2, le numéro de série NS associé à une carte donnée est lu par l'outil de fabrication 20 et ce numéro NS est soumis par un algorithme à une opération de chiffrement E à l'aide de la clé maître de personnalisation K_{PEM} (bloc 100). Le résultat de ce chiffrement est une clé de personnalisation spécifique propre à la carte, K_{PER} qui est soumise en 101 au moyen d'un algorithme et de la clé K_{ROM} à une opération inverse E-1 pour produire une donnée $E(K_{PER})$. La clé K_{PER} est utilisée en 102 et 103 pour générer des données $E(K_{MES})$ et $E(_{KALE})$, à partir des clés K_{MES} et K_{ALE} respectivement, grâce à

l'opération inverse E-1. Dans ce qui précède et ce qui suit, si B = E[K_X](A) est le résultat du chiffrement E d'une donnée A à l'aide d'une clé K_X, E-1 représente l'opération inverse A = E - 1[K_X](B) permettant, au moyen de la clé K_X, d'obtenir en sortie la donnée A en appliquant à l'entrée de l'algorithme de chiffrement la donnée B.

Pour une carte donnée 2, les paramètres de production (bloc 104) comprennent le numéro de série NS, les données de sortie des blocs 101, 102 et 103, et l'état d'un compteur d'horloge interne de l'outil de fabrication permettant d'initialiser un compteur d'horloge de la carte 2, en particulier si le système met en oeuvre des variables et/ou des clés dynamiques.

Après mise à zéro des paramètres et initialisation des paramètres internes de la carte concernée 2, celle-ci est mise dans un état d'attente de réception d'une trame de fabrication (bloc 105). A l'étape 106, la carte 2 reçoit la trame de fabrication constituée des données énumérés précédemment (bloc 104). Au moyen du logiciel qui lui a été programmé, le microcontrôleur 7 calcule ensuite en 107 par l'opération E la clé K_{PER} à partir de la donnée E(K_{PER}) et de la clé K_{ROM}. Il calcule également par l'opération E, en 108 la clé K_{MES} à partir de la donnée E(K_{MES}) et de la clé K_{PER}, et en 109 la clé K_{ALE} à partir de la donnée E(K_{ALE}) et de la clé K_{PER}.

A l'étape 110, le numéro de série NS et les clés K_{PER}, K_{ALE} et K_{MES}, sont stockées en mémoire et la carte est prête à être transmise à un client en vue de sa personnalisation.

Dans le processus décrit ci-dessus, il suffit de connaître le format de la trame de fabrication (bloc 104) pour charger des paramètres dans une carte puisque cette opération ne fait pas appel à un code d'accès. Mais un pirate qui connaîtrait le format de cette trame de fabrication serait néanmoins dans l'impossibilité de personnaliser et d'exploiter cette carte car il ne connaîtrait pas la clé K_{ROM}.

La figure 3 décrit une variante de réalisation du processus d'initialisation des paramètres de production qui a pour avantage de ne pas introduire la clé K_{ROM} et la clé K_{PEM} dans le logiciel d'initialisation des

paramètres de production de l'outil de fabrication 20. A cet effet, au moyen d'un logiciel qui lui est propre, le fournisseur (colonne de gauche) calcule les données $E(K_{PER})$, $E(K_{MES})$ et $E(K_{ALE})$ à partir, respectivement, des données K_{PER}, K_{MES} et K_{ALE}, et de la clé K_{ROM}. Après le calcul de ces données en 111, 112 et 113 par une opération E-1, celles-ci sont introduites par le fournisseur dans le logiciel d'initialisation des paramètres de production de l'outil de fabrication (étape 114).

Après lecture du numéro de série de la carte concernée par l'outil 20 en 115, et après mise à zéro des paramètres et initialisation des paramètres internes de la carte en 116, l'outil de fabrication 20 transmet les paramètres de production à la carte (étape 117) : il s'agit du numéro de série NS, des données $E\text{-}1(K_{PER})$, $E\text{-}1(K_{MES})$ et $E\text{-}1(K_{ALE})$, ainsi que de l'état du compteur d'horloge interne. Après réception de la trame correspondante (étape 118), le microcontrôleur 6 calcule par l'opération E la clé K_{PEM} à l'aide de la donnée $E(K_{PEM})$ et de la clé K_{ROM} (étape 119). Il calcule ensuite la clé de personnalisation propre à la carte, K_{PER}, par l'opération E au moyen de la donnée NS et de la clé maître de personnalisation K_{PEM} (étape 120). Enfin, le microcontrôleur 7 calcule en 121 et 122 par l'opération E les clés K_{ALE} et K_{MES} à partir des données $E(K_{ALE})$ et $E(K_{MES})$ respectivement et de la clé K_{ROM} stockée dans la mémoire permanente 8 de la carte. A l'étape 123, les données NS, K_{PER}, K_{ALE} et K_{MES} sont stockées dans la mémoire programmable 9 de la carte 2. Ces données sont les mêmes que celles obtenues par le processus d'initialisation des paramètres de production décrits en regard de la figure 2.

Lorsque les paramètres de production d'un lot de cartes destinées à un client donné ont ainsi été initialisés, celles-ci sont livrées au client. Les clés communes à ce lot, à savoir la clé maître de personnalisation K_{PEM}, la clé permettant de générer des aléas K_{ALE} et la clé permettant de charger l'alphabet et des messages, à savoir K_{MES}, sont communiquées confidentiellement au client. Chaque carte contient en mémoire les clés

K_{ALE} et K_{MES} qui sont communes à ce lot de cartes, ainsi que la clé K_{PER} et le numéro de série NS qui lui sont propres.

En outre, chaque carte 2 contient en mémoire un code ou numéro permettant d'identifier la version du logiciel qui a été implantée, lors de leur masquage, dans les circuits intégrés de cette carte. En effet, d'un lot de cartes à un autre, la version de logiciel implantée peut être différente et, à l'intérieur d'un même lot de carte destiné à un client, il peut éventuellement y avoir plusieurs groupes de cartes équipées de versions différentes de logiciel en fonction des besoins exprimés par le client quant à l'utilisation de ces cartes. Le code ou numéro de chaque version du logiciel implanté dans les cartes qui lui sont livrées est fourni par le fournisseur au client. Ce dernier dispose également du ou des logiciels nécessaires à la personnalisation de ses cartes en fonction de la version du logiciel implanté dans celles-ci.

Le processus de personnalisation des cartes 2 par le client est illustré à la figure 4 sur laquelle la colonne de gauche représente les opérations mises en œuvre par un outil de personnalisation 30 et la colonne de droite les opérations mises en œuvre dans les cartes 2. L'outil de personnalisation 30 présente une structure similaire à celui de l'unité de vérification 3, c'est-à-dire qu'il comporte des moyens de communication avec les cartes 2, un processeur de traitement d'informations, des mémoires contenant notamment le ou les logiciels nécessaires à la personnalisation des cartes en fonction de la version du logiciel implanté dans celles-ci, et une base de données contenant les valeurs des clés K_{PEM}, K_{ALE} et K_{MES} et les paramètres de personnalisation à charger dans les cartes 2 en fonction de la version du logiciel implanté dans celles-ci.

Sur la figure 4, à l'étape 200, la carte est dans un état d'attente d'une trame d'ouverture de communication en provenance de l'outil de personnalisation. A l'étape 201, l'outil de personnalisation ouvre la communication avec la carte à personnaliser et émet la trame d'ouverture de communication INIT-MAT. A l'étape 202, la carte reçoit la trame

d'ouverture de communication INIT-MAT et émet vers l'outil de personnalisation une trame d'identification IDENT-MAT incluant le code ou numéro de la version du logiciel qu'elle contient. A l'étape 203, l'outil de personnalisation 30 reçoit la trame d'identification IDENT-MAT et le numéro de version de logiciel est appliqué à la base de données pour y lire, entre autres, les paramètres de personnalisation à charger dans la carte. A l'étape 204, l'outil de personnalisation 30 émet une trame d'initialisation logicielle INIT-LOG reçue en 205 par la carte, qui passe alors à l'étape 206.

A l'étape 206, la carte calcule par l'opération E un aléa au moyen de la clé K_{ALE} (bloc 207), puis la donnée E(NS) par chiffrement du numéro de série NS de la carte au moyen d'une clé qui est elle-même le résultat du chiffrement par une fonction logique F du numéro de version du logiciel NL au moyen de l'aléa calculé en 207. Après ces opérations de chiffrement 208 et 209, la carte émet en 210 une trame d'identification IDENT-LOG contenant l'aléa et E(NS). Cette trame est reçue en 211 par l'outil de personnalisation 30 qui, par une opération F en 212 sur le numéro NL au moyen de l'aléa transmis depuis la carte et une opération E-1 en 213 sur E(NS) au moyen du résultat de l'opération effectuée en 212, génère le numéro de série NS de la carte. Le numéro de série NS de la carte en cours de personnalisation est appliqué à la base de données afin de permettre au client de garder une table des données de personnalisation de chaque carte. En 214, l'outil de personnalisation calcule la clé K_{PER} propre à la carte par une opération de chiffrement E du numéro de série NS au moyen de la clé maître de personnalisation K_{PEM} qui est fournie par la base de données de l'outil 30. L'outil calcule ensuite en 215 un mot de passe d'authentification A_{PO} (qui constitue le code d'accès à la personnalisation de la carte) par chiffrement F de l'aléa au moyen de la clé K_{PER} : $A_{PO} = F\ [K_{PER}]$ (Aléa).

A l'étape 216, l'outil de personnalisation construit les données de personnalisation communes de la carte à partir du mot de passe calculé en 215 et des paramètres de personnalisation reçus de la base de données. Ces données de personnalisation communes comprennent des codes de

commande de personnalisation, le mot de passe A_{PO} d'authentification de l'outil de personnalisation, une nouvelle clé secrète de personnalisation propre à la carte NK_{PER} destinée à être substituée à la clé de personnalisation initiale K_{PER} et les différents paramètres de personnalisation comprenant, par exemple, une ou des clés secrètes K_{SEA} de calcul du mot de passe d'authentification A_{SEA} vis-à-vis de l'unité de vérification 3 (A_{PEA} = E [K_{SEA}] (Aléa)), ainsi que des clés secrètes secondaires ou particulières de personnalisation K_{PERX}, K_{PERY}, etc... propres à chaque site X, Y, etc.. pour lequel la carte devra être personnalisée.

A l'étape 217, ces données de personnalisation sont transmises à la carte sous forme de plusieurs trames.

A l'étape 218, la carte reçoit les trames de personnalisation, vérifie les codes de commande de personnalisation, stocke les données reçues et envoie un accusé de réception à l'outil de personnalisation.

A l'étape 219, la carte calcule un code ou mot de passe A_{PC} de vérification du mot de passe d'authentification A_{PO} par chiffrement de l'aléa selon la fonction logique F au moyen de la clé de personnalisation spécifique K_{PER} stockée dans sa mémoire en 110 ou 123 : A_{PC} = F [K_{PER}] (Aléa).

A l'étape 220, la carte vérifie que le mot de passe d'authentification A_{PO} reçu de l'outil de personnalisation 30 est cohérent avec le mot de passe de vérification A_{PC} calculé par la carte et, dans l'affirmative, mémorise les données de personnalisation en 221 : cette cohérence peut consister, par exemple, en ce que les deux mots de passe sont identiques comme représenté à la figure 4, mais elle peut également résider dans le fait que ces deux mots de passe sont liés par une autre relation prédéterminée.

Enfin, à l'étape 222 la carte substitue la nouvelle clé de personnalisation NK_{PER} reçue de l'outil de personnalisation à l'ancienne clé K_{PER}. Cette nouvelle clé NK_{PER} n'est pas connue du fournisseur à qui il sera désormais impossible d'accéder aux données de personnalisation du client. L'accès en lecture et/ou en écriture à ces données de personnalisation

nécessitera la fourniture à la carte, par l'outil de personnalisation, d'un nouveau mot de passe d'authentification $NA_{PO} = F[NK_{PER}]$ (Aléa) cohérent avec le mot de passe de vérification NA_{PC} calculé dans la carte comme indiqué en 219, NA_{PO} et NA_{PC} étant calculés sur la base d'un nouvel aléa généré dans la carte et transmis à l'outil de personnalisation.

Cependant, la connaissance de la clé secrète de personnalisation commune NK_{PER} ne permettra pas de lire les clés secrètes de personnalisation secondaires K_{PERX}, K_{PERY}, etc... chargées dans la carte à l'étape 221, ni aucune autre clé secrète.

En effet, les clés secrètes ne peuvent pas être lues car le programme du microcontrôleur 7 ne comporte aucune commande de lecture de ces paramètres.

Après l'étape 222, l'administrateur général peut transmettre les cartes aux administrateurs locaux des sites X, Y, etc... qui, chacun au moyen des clés secondaires respectives K_{PERX}, K_{PERY}, etc..., seront en mesure, par un processus similaire à celui de la figure 4 qu'il n'y a pas lieu de décrire à nouveau en détail, de charger dans la carte les paramètres de personnalisation propres au site dont ils sont responsables. A cet effet, la clé secondaire propre à la personnalisation de la carte pour chaque site aura été communiquée de manière confidentielle par l'administrateur général à l'administrateur local concerné.

Au moyen de la clé secondaire qui lui aura été communiquée, l'administrateur local chargera dans la carte les données de personnalisation propres au site concerné, par exemple une clé d'authentification pour le calcul d'un mot de passe d'authentification vis-à-vis d'une unité de vérification de ce site. C'est ainsi que l'administrateur local du site X pourra charger une clé d'authentification K_{SEAX}, l'administrateur local du site Y une clé d'authentification K_{SEAY}, etc... Au cours du processus de personnalisation de la carte pour un site donné X, l'administrateur local aura, dans la carte, la possibilité de substituer à la clé secondaire de personnalisation K_{PERX} reçue de l'administrateur général

pour le site concerné une nouvelle clé secondaire de personnalisation NK_{PERX}, comme décrit à la figure 4. Ceci interdira à l'administrateur général d'avoir accès à la lecture et/ou à la modification des paramètres de personnalisation des cartes dont la clé secondaire de personnalisation aura été modifiée. La modification des clés secondaires permet d'assurer également l'étanchéité entre les différents segments ou fonctions de la carte. En modifiant les clés secondaires K_{PERX}, K_{PERY}, etc... (remplacées par NK_{PERX}, NK_{PERY}, etc...), on se protège contre une attaque visant à écrire d'autres données secrètes dans les segments. Ce type d'attaque est limité, car il ne sera pas possible de lire ces données secrètes même si on possède la clé secrète secondaire de personnalisation correspondante. Mais on garantit ainsi l'accès exclusif à la personnalisation de chaque segment, comme on garantit l'accès exclusif aux données de personnalisation communes avec la clé K_{PER}, NK_{PER}.

De préférence, la clé K_{PER}, NK_{PER} spécifique à la carte permet, après personnalisation des segments au moyen des clés secondaires K_{PERX}, K_{PERY}, NK_{PERX}, NK_{PERY}, d'écraser ces dernières afin d'effectuer, si nécessaire, un nouveau processus d'initialisation de l'ensemble des paramètres de personnalisation de la carte. Cette possibilité peut être utile, en cas d'anomalie, pour éviter que le dispositif soit définitivement rendu inutilisable.

Cependant, en variante, il peut être prévu d'interdire cette possibilité.

L'organigramme général de la figure 5 illustre les phases principales du programme qui se déroule dans une carte 2 pourvue de plusieurs segments qui, après une initialisation des paramètres de personnalisation communs, doivent être initialisés avec des paramètres de personnalisation qui leur sont propres en vue de la mise en œuvre, au moyen de la carte, de fonctions propres à chaque segment.

Le programme débute en 300 et en 301 un test est effectué pour déterminer s'il s'agit de la première mise en route de la carte après remise à zéro ("RESET").

Dans l'affirmative, la mémoire est remise à zéro en 302, puis on passe à un test 303 pour déterminer si un drapeau représentatif de l'initialisation des paramètres en production (paramètres initialisés par le fabricant) est actif. Si la réponse au test 301 est négative, on passe directement au test 303.

Si la réponse au test 303 est négative, le programme se met dans un état d'attente d'initialisation des paramètres de production (étape 304). L'étape suivante 305 correspond à l'initialisation dans la carte 2 des paramètres de production comme décrit en regard des figures 2 ou 3. Lorsque cette initialisation est achevée, un drapeau est activé à l'étape 306 et le programme revient à l'entrée du test 303.

Lorsque la réponse au test 303 est positive, c'est-à-dire que les paramètres de production ont été initialisés, le programme passe à un test 307 pour déterminer si un drapeau représentatif de l'initialisation par le client des paramètres de personnalisation communs est actif. Si la réponse est négative, le programme se met dans un état d'attente d'initialisation des paramètres de personnalisation communs (étape 308). L'étape suivante 309 correspond à l'initialisation dans la carte 2 des paramètres de personnalisation communs comme décrit en regard de la figure 4. Ces paramètres de personnalisation communs comprennent entre autres les clés de personnalisation reprogrammables K_{PERX}, K_{PERY} particulières à chaque segment ou fonction. Lorsque cette initialisation est achevée, un drapeau est activé à l'étape 310 et le programme revient à l'entrée du test 307.

Lorsque la réponse au test 307 est positive, le programme passe au test 311 pour déterminer si un drapeau représentatif de l'initialisation des paramètres de personnalisation propres ou particuliers aux différents segments de la carte est actif. Si la réponse est négative, le programme se

met dans un état d'attente d'initialisation des paramètres de personnalisation particuliers aux segments (étape 312). L'étape 313 correspond à l'initialisation dans la carte 2 des paramètres de personnalisation particuliers aux segments. Cette initialisation est subordonnée, pour chaque segment, à la fourniture à la carte d'un code d'accès correct A_{PX}, A_{PY}, fonction de la clé K_{PERX}, K_{PEY} affecté à ce segment et d'un aléa fourni par la carte à l'outil de personnalisation comme décrit en regard de la figure 4. Suivant les cas, cette initialisation peut être effectuée par l'administrateur général ou par des administrateurs locaux au niveau de différents sites géographiques, comme décrit précédemment. Au cours de ce processus d'initialisation des paramètres de personnalisation particuliers, l'administrateur responsable peut substituer une nouvelle clé de personnalisation particulière NK_{PERX}, NK_{PERY} à la clé de personnalisation initiale K_{PERX}, K_{PERY} qui, pour le segment considéré, avait été chargée à l'étape 309. Seul le détenteur de cette nouvelle clé NK_{PERX}, NK_{PERY} pourra générer le nouveau code d'accès NA_{PX}, NA_{PY} et accéder ultérieurement (en lecture et/ou en écriture selon la programmation des moyens de traitement) aux données de personnalisation particulières au segment correspondant, et le détenteur de la clé de personnalisation spécifique K_{PER} (ou NK_{PER} si celle-ci a été modifiée), n'y aura pas accès s'il ne connaît pas la nouvelle clé de personnalisation particulière.

Lorsque l'initialisation des paramètres de personnalisation de tous les segments est achevée, un drapeau est activé à l'étape 314, la réponse au test 311 est positive et le programme passe à l'étape 315 qui représente l'accès, pour l'utilisateur final, aux différentes fonctions de la carte mises en œuvre par le programme de celle-ci.

Comme indiqué précédemment, l'invention n'est pas limitée à la mise en œuvre d'algorithmes symétriques à clé secrète, et elle s'applique également dans le cas où les mécanismes d'initialisation des paramètres de la carte font appel à des algorithmes asymétriques à clé publique et clé

privée. Dans ce cas, la clé publique est stockée dans la carte ou dispositif 2, l'aléa est toujours généré dans le dispositif 2 et la clé privée est stockée dans un outil de personnalisation ou dans une carte à puce utilisée par l'outil de personnalisation.

L'utilisation d'algorithmes asymétriques ne permet cependant pas de mettre en œuvre une dérivation des clés, car le concept de clé mère n'existe pas dans ce type d'algorithme.

Il va d'ailleurs de soi que les modes de réalisation décrits ne sont que des exemples et l'on pourrait les modifier, notamment par substitution d'équivalents techniques, sans sortir pour cela du cadre de l'invention.

REVENDICATIONS

1. Dispositif portable électronique sécurisé de communication avec au moins une unité électronique, pour la mise en œuvre d'au moins une fonction, comprenant :

* des moyens de mémorisation de données,

* des moyens d'interface avec au moins un outil extérieur pour charger des données dans lesdits moyens de mémorisation,

* des moyens de traitement de données comprenant des moyens d'initialisation pour permettre, en réponse à l'application d'un code secret d'accès en personnalisation, la modification dudit code d'accès et le chargement de données de personnalisation dans lesdits moyens de mémorisation, caractérisé en ce que ledit dispositif est adapté à la mise en œuvre d'une pluralité de fonctions (X, Y, ...) et comporte

* des moyens (K_{PER} ; NK_{PER}) de chargement d'une pluralité de données secrètes particulières (K_{PERX}, K_{PERY}, ...) représentatives respectivement de codes secrets d'accès particuliers différents les uns des autres (A_{PX}, A_{PY},.....) et affectés chacun à la personnalisation d'une fonction particulière (X, Y,.....) dudit dispositif, et

* des moyens d'inhibition (7 ; 222) adaptés pour n'autoriser l'accès desdits moyens de traitement au chargement et/ou à la lecture de données de personnalisation particulières à une fonction qu'en réponse à l'application du code d'accès particulier affecté à ladite fonction.

2. Dispositif selon la revendication 1, caractérisé en ce que lesdits moyens d'inhibition (7) sont adaptés pour interdire l'accès en lecture à l'une quelconque desdites données secrètes (K_{PER}, K_{PERX}, K_{PERY}.....) .

3. Dispositif selon l'une quelconque des revendications 1 et 2, caractérisé en ce que lesdits moyens de chargement comprennent au moins une donnée secrète spécifique reprogrammable (K_{PER}) représentative d'un code secret spécifique (A_{PO}) commun à l'ensemble desdites fonctions et en ce que lesdits moyens d'inhibition sont adaptés pour interdire l'accès

desdits moyens de traitement (7) auxdites données de personnalisation particulières par l'intermédiaire dudit code secret spécifique (A_{PO}).

4. Dispositif selon la revendication 3, caractérisé en ce que lesdits moyens de traitement de données (7) sont adaptés pour autoriser une modification d'une donnée secrète (K_{PERX}, K_{PERY}) représentative d'un code d'accès particulier à une fonction (X, Y, ...) et chargée dans lesdits moyens de mémorisation via ledit code secret d'accès spécifique (A_{PO}), en réponse à l'application dudit code d'accès particulier (A_{PX}, A_{PY}).

5. Dispositif selon la revendication 4, caractérisé en ce que lesdits moyens de chargement sont adaptés pour autoriser, au moyen de ladite donnée secrète spécifique reprogrammable (K_{PER}, NK_{PER}), l'effacement de données secrètes particulières (K_{PERX}, K_{PERY}, ...) et de données de personnalisation particulières (K_{SEAX}, K_{SEAY}, ...) préalablement chargées et le chargement de nouvelles données secrètes particulières.

6. Dispositif selon l'une quelconque des revendications 3 à 5, caractérisé en ce que ledit code secret spécifique (A_{PO}) est un code d'accès à la personnalisation de données de personnalisation communes à l'ensemble desdites fonctions du dispositif.

7. Dispositif selon l'une quelconque des revendications 3 à 6, caractérisé en que les lesdits moyens de mémorisation comprennent au moins une mémoire permanente (8) dans laquelle est stockée une clé secrète de base (K_{ROM}), lesdits moyens d'initialisation (7) comprenant des premiers moyens (7, 107) pour calculer une valeur initiale de ladite donnée secrète spécifique (K_{PER}) en fonction de ladite clé secrète de base (K_{ROM}) et d'un paramètre secret initial ($E(K_{PER})$; $E(K_{PEM})$).

8. Dispositif selon l'une quelconque des revendications 1 à 7, caractérisé en ce que lesdits moyens d'inhibition (7, 222) sont adaptés pour effacer desdits moyens de mémorisation (9) l'une desdites données secrètes (K_{PER}, K_{PERX}, K_{PERY}) représentatives d'un code d'accès en réponse au chargement, au moyen dudit code d'accès (A_{PO}, A_{PX}, A_{PY}), d'une nouvelle

donnée secrète (NK_{PER}, NK_{PERX}, NK_{PERY}) représentative d'un nouveau code d'accès (NA_{PO}, NA_{PX}, NA_{PY}).

9. Dispositif selon l'une quelconque des revendications 1 à 8, caractérisé en ce que ladite donnée secrète (K_{PER}, NK_{PER}) est une clé secrète de calcul d'un code (A_{PC} ; NA_{PC}) de vérification du code d'accès (A_{PO}; NA_{PO}) dont ladite donnée est représentative.

10. Dispositif selon la revendication 9, caractérisé en ce que lesdits moyens de traitement (7) comprennent des seconds moyens pour calculer ledit code de vérification (A_{PC}, NA_{PC}) par chiffrement d'une variable au moyen de ladite clé secrète de calcul (K_{PER}, K_{PERX}, K_{PERY},....).

11. Dispositif selon l'une quelconque des revendications 1 à 10, caractérisé en ce que lesdites données de personnalisation comprennent au moins une pluralité de clés secrètes d'authentification (K_{SEAX}, K_{SEAY}) différentes les unes des autres et affectées chacune à l'une desdites fonctions et en ce que lesdits moyens de traitement (7) comprennent des troisièmes moyens pour calculer un code d'authentification (A_{PEA}) vis-à-vis d'une unité de vérification (3) en fonction de l'une desdites clés secrètes d'authentification (K_{SEAX}, K_{SEAY}).

12. Procédé d'initialisation d'un dispositif selon l'une quelconque des revendications 1 à 11, caractérisé en ce qu'il comprend :

- un premier stade d'initialisation consistant à définir et à stocker dans lesdits moyens de mémorisation (9) une clé de personnalisation (NK_{PER}) spécifique audit dispositif,

- un deuxième stade de personnalisation consistant à charger dans lesdits moyens de mémorisation, au moyen d'un code d'accès spécifique (NA_{PO}) fonction de ladite clé de personnalisation spécifique (NK_{PER}), des données de personnalisation communes auxdites fonctions et des clés secrètes (K_{PERX}, K_{PERY}) de calcul desdits codes secrets d'accès particuliers (A_{PX}, A_{PY}) affectés chacun au chargement de données de personnalisation relative à l'une desdites fonctions (X, Y), et

- un troisième stade de personnalisation consistant, pour chacune desdites fonctions (X, Y), à charger dans lesdits moyens de mémorisation, au moyen du code secret d'accès particulier correspondant (A_{PX}, A_{PY}), les données de personnalisation relatives à ladite fonction.

13. Procédé selon la revendication 12, caractérisé en ce que ledit troisième stade comprend l'étape consistant, lors du chargement des données de personnalisation relatives à au moins l'une desdites fonctions (X, Y), à modifier ladite clé secrète (K_{PERX}, K_{PERY}) de calcul dudit code secret d'accès particulier (A_{PX}, A_{PY}) affecté à ladite fonction.

14. Procédé selon l'une quelconque des revendications 12 à 13, caractérisé en ce que le premier stade d'initialisation comprend :

- au moins une première phase d'initialisation consistant à définir au moins une donnée secrète (K_{PEM} ; $E(K_{PEM})$) commune à un ensemble de dispositifs destinés à une même entité,
- au moins une deuxième phase d'initialisation comprenant les étapes consistant, pour chaque dispositif dudit ensemble, à :

a) lire une donnée d'identification (NS) spécifique portée par ledit dispositif,

b) calculer une première clé de personnalisation spécifique (K_{PER}) en fonction de ladite donnée secrète commune (K_{PEM} ; $E(K_{PEM})$), et de ladite donnée d'identification (NS),

c) stocker ladite donnée d'identification (NS) et ladite première clé de personnalisation spécifique (K_{PER}) dans lesdits moyens de mémorisation (9), et

- au moins une troisième phase d'initialisation comprenant les étapes consistant, pour chaque dispositif dudit ensemble, à :

d) extraire ladite donnée d'identification spécifique (NS) dudit dispositif (2),

e) calculer dans un premier outil extérieur (30) ladite première clé de personnalisation spécifique (K_{PER}) en fonction de ladite

donnée secrète commune (K_{PEM}) et de ladite donnée d'identification spécifique (NS),

f) calculer dans ledit outil extérieur (30) un premier code d'accès (A_{PO}) en fonction de ladite première clé de personnalisation spécifique (K_{PER}) et d'un aléa transmis par ledit dispositif,

g) transmettre dudit premier outil audit dispositif (2) ledit premier code d'accès (A_{PO}) avec des paramètres de personnalisation comprenant une deuxième clé de personnalisation (NK_{PER}) différente de ladite première clé de personnalisation (K_{PER})

h) calculer dans ledit dispositif un code (A_{PC}) de vérification dudit premier code d'accès (A_{PO}) en fonction de ladite première clé de personnalisation spécifique (K_{PER}) et dudit aléa,

i) comparer dans ledit dispositif ledit premier code d'accès (A_{PO}) et ledit code de vérification (A_{PC}) et, en réponse à une cohérence desdits codes,

j) stocker lesdits paramètres de personnalisation dans lesdits moyens de mémorisation (9), et

k) substituer ladite deuxième clé de personnalisation (NK_{PER}) à ladite première clé de personnalisation (K_{PER}) dans lesdits moyens de mémorisation (9).

15. Procédé selon la revendication 14, caractérisé en ce qu'il comprend une quatrième phase consistant à stocker initialement une clé secrète de base (K_{ROM}) commune dans une mémoire permanente (8) desdits moyens de mémorisation et en ce que les étapes a) et b) consistent à :

- appliquer ladite donnée secrète (K_{PEM}) et ladite clé de base (K_{ROM}) à un deuxième outil extérieur (20),
- lire ladite donnée d'identification (NS) au moyen dudit deuxième outil,
- calculer ladite clé de personnalisation spécifique (K_{PER}) au moyen dudit deuxième outil (20),

- chiffrer (101) dans ledit deuxième outil extérieur (20) ladite clé de personnalisation spécifique (K_{PER}) au moyen de ladite clé de base commune (K_{ROM}),
- transmettre (104) dudit deuxième outil (20) audit dispositif (2) le résultat ($E(K_{PER})$) dudit chiffrement, et
- déchiffrer (107) ledit résultat ($E(K_{PER})$) dans lequel dispositif au moyen de ladite clé de base (K_{ROM}) pour restituer ladite clé de personnalisation spécifique (K_{PER}).

16. Procédé selon la revendication 14, caractérisé en ce qu'il comprend une quatrième phase consistant à stocker initialement une clé de base (K_{ROM}) commune dans une mémoire permanente (8) desdits moyens de mémorisation, en ce que ladite première phase consiste également à chiffrer ladite donnée secrète commune (K_{PEM}) au moyen de ladite clé de base commune (K_{ROM}) et à appliquer le résultat dudit chiffrement ($E(K_{PEM})$) à un deuxième outil extérieur (20), et en ce que ladite deuxième phase consiste également à :

a) lire ladite donnée d'identification spécifique (NS) au moyen dudit deuxième outil (20) et transmettre ladite donnée d'identification (NS) et le résultat dudit chiffrement ($E(K_{PEM})$) audit dispositif,

b) déchiffrer ledit résultat ($E(K_{PEM})$) dans ledit dispositif (2) au moyen de ladite clé de base (K_{ROM}) pour restituer ladite donnée secrète commune (K_{PEM}) puis calculer ensuite ladite clé de personnalisation spécifique (K_{PER}).

17. Système de communication sécurisée, caractérisé en ce qu'il comprend un ensemble de dispositifs selon l'une quelconque des revendications 1 à 11 et au moins un outil (30) d'initialisation de paramètres de personnalisation pour la mise en œuvre de ladite troisième phase du procédé selon l'une quelconque des revendications 14 à 16.

18. Système de communication sécurisée selon la revendication 17, caractérisé en ce qu'il comprend en outre un outil (20) d'initialisation de

paramètres de production pour la mise en œuvre de ladite deuxième phase du procédé selon l'une quelconque des revendications 14 à 16.

19. Système de communication sécurisée, caractérisé en ce qu'il comprend un ensemble de dispositifs selon la revendication 11 et au moins une unité de vérification (3).

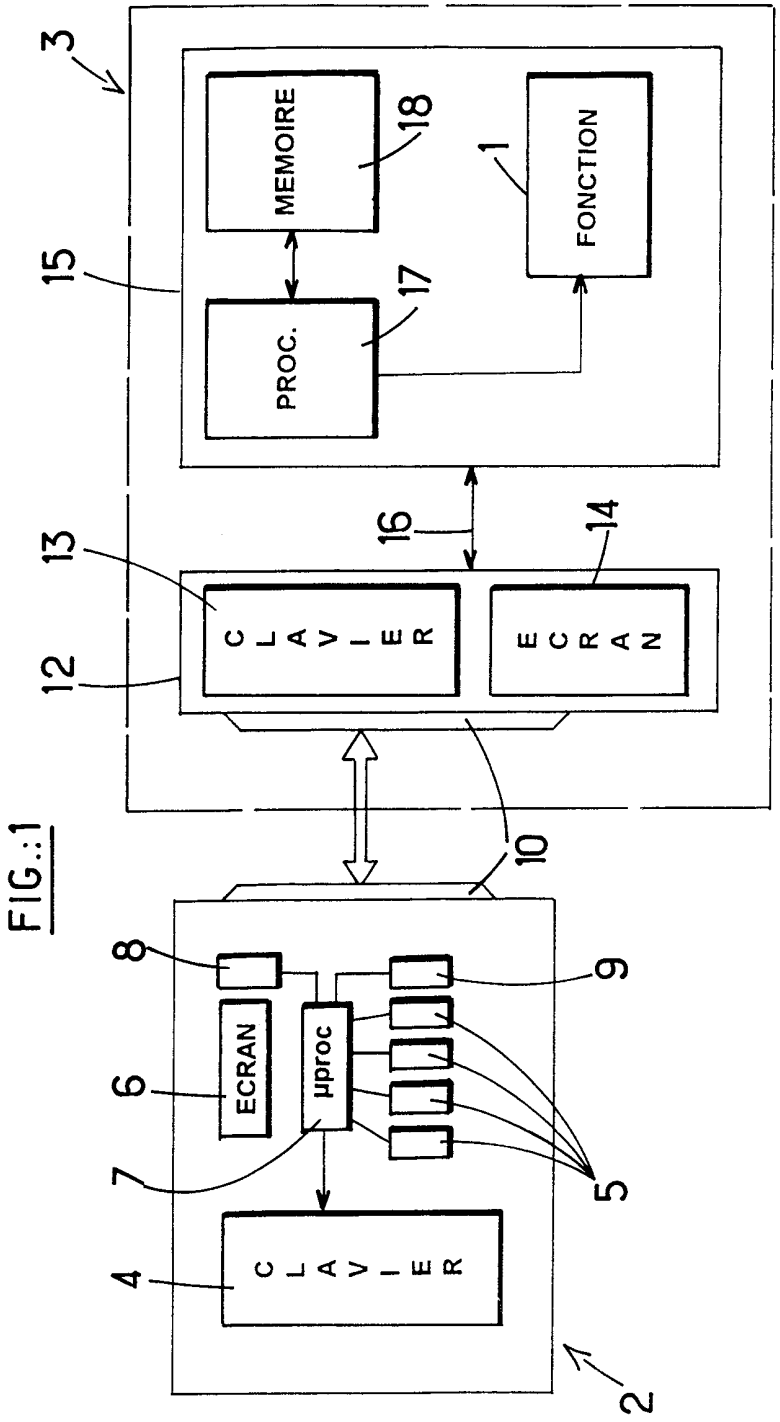

3
MEMOIRE
18
1
FONCTION
15
17
PROC.
16
14
13
CLAVIER
ECRAN
12
10
8
9
ECRAN
µproc
6
7
5
CLAVIER
4
2

FIG.:1

FIG.:2

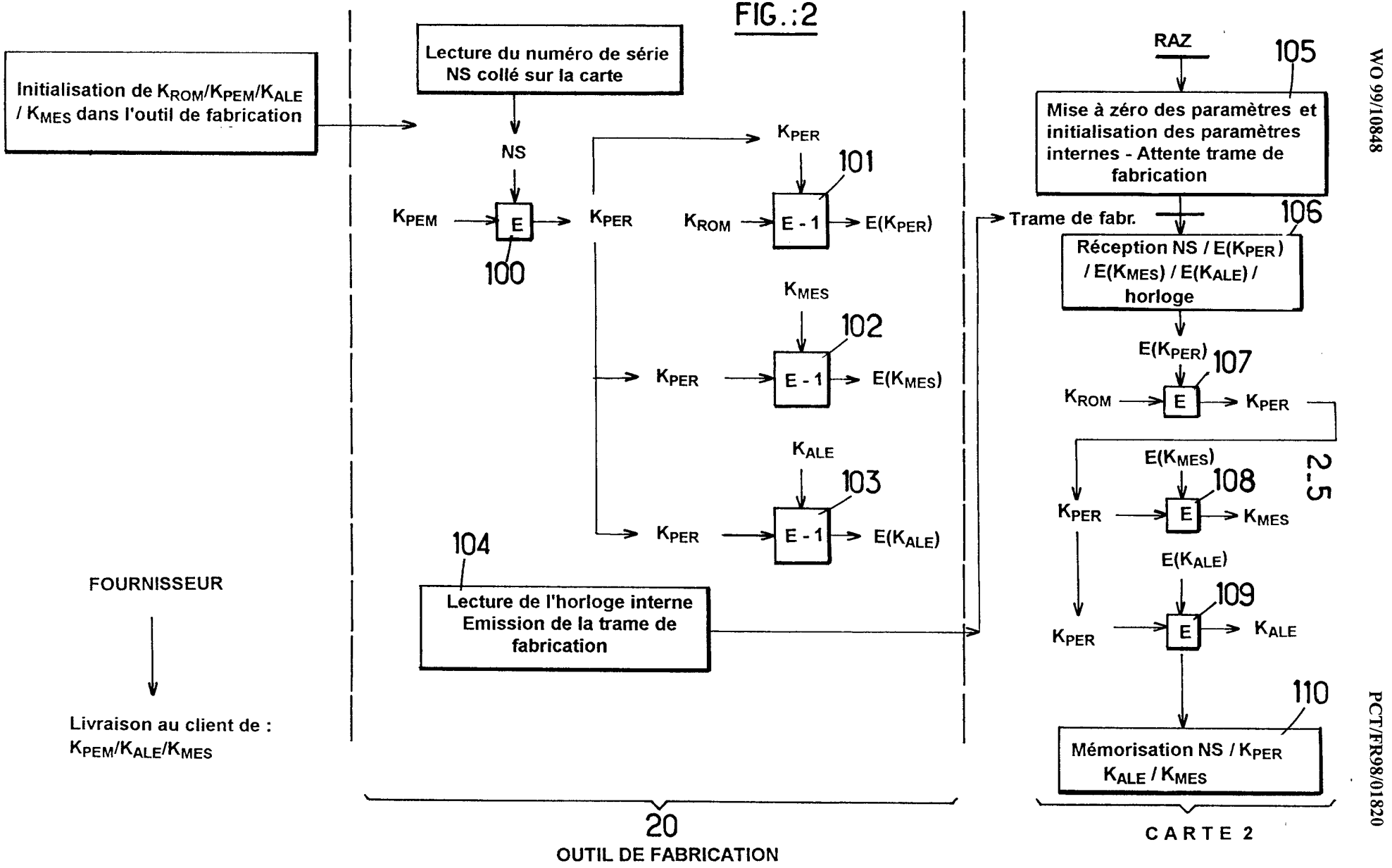
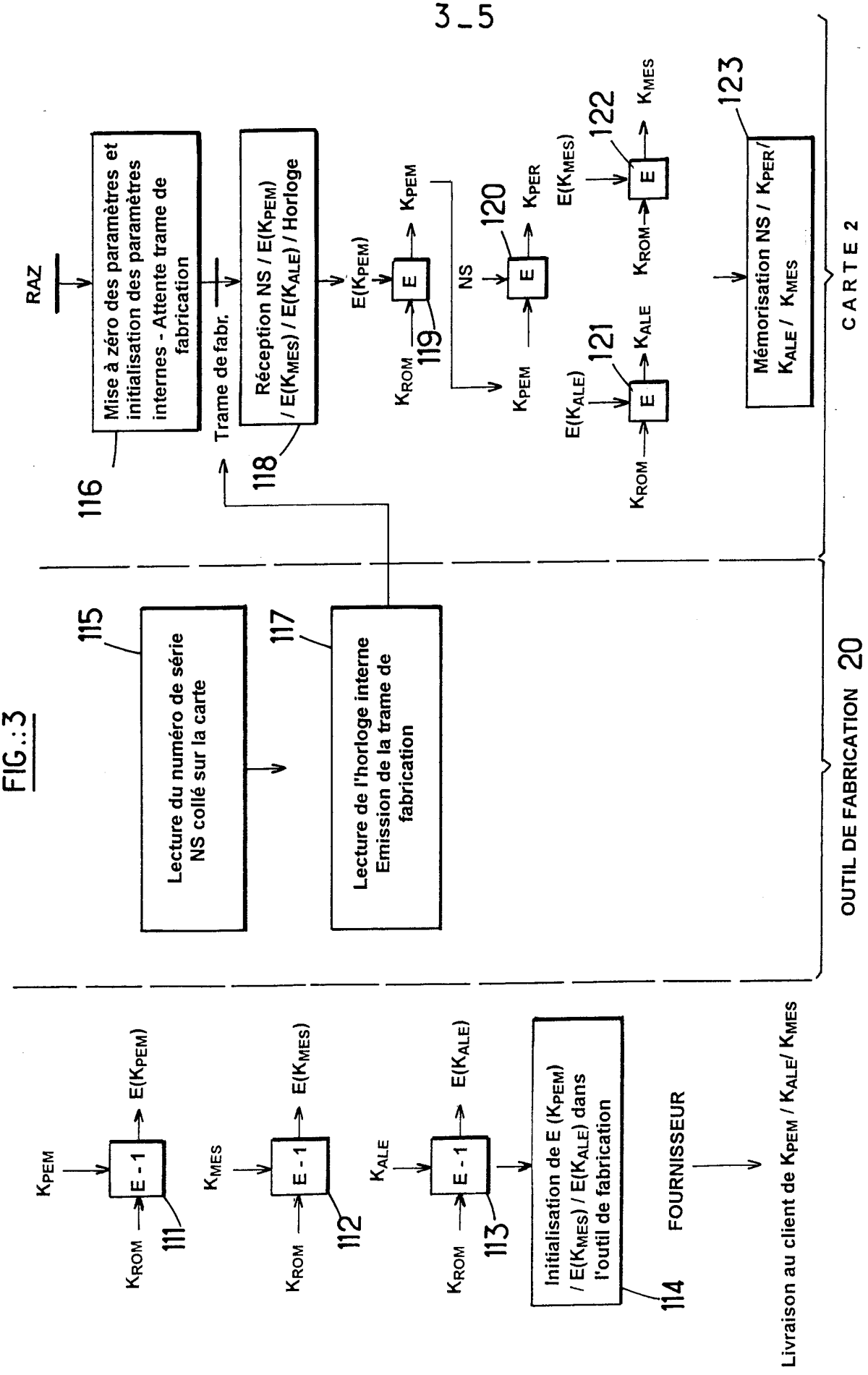

Initialisation de $K_{ROM}/K_{PEM}/K_{ALE}$ / K_{MES} dans l'outil de fabrication
Lecture du numéro de série NS collé sur la carte
NS
K_{PEM}
E
100
K_{PER}
K_{PER}
101
K_{ROM}
E - 1
$E(K_{PER})$
K_{MES}
102
K_{PER}
E - 1
$E(K_{MES})$
K_{ALE}
103
K_{PER}
E - 1
$E(K_{ALE})$
104
Lecture de l'horloge interne
Emission de la trame de fabrication
FOURNISSEUR
Livraison au client de : $K_{PEM}/K_{ALE}/K_{MES}$
20
OUTIL DE FABRICATION
RAZ
105
Mise à zéro des paramètres et initialisation des paramètres internes - Attente trame de fabrication
Trame de fabr.
106
Réception NS / $E(K_{PER})$ / $E(K_{MES})$ / $E(K_{ALE})$ / horloge
$E(K_{PER})$
107
K_{ROM}
E
K_{PER}
2.5
$E(K_{MES})$
108
K_{PER}
E
K_{MES}
$E(K_{ALE})$
109
K_{PER}
E
K_{ALE}
110
Mémorisation NS / K_{PER} K_{ALE} / K_{MES}
CARTE 2

FIG.:3


RAZ
Mise à zéro des paramètres et initialisation des paramètres internes - Attente trame de fabrication
116
Trame de fabr.
Réception NS / E(KPEM) / E(KMES) / E(KALE) / Horloge
118
E(KPEM)
E
KPEM
KROM
119
NS
120
KPER
KPEM
E(KMES)
122
KMES
KROM
E(KALE)
121
KALE
KROM
123
Mémorisation NS / KPER / KALE / KMES
CARTE 2
115
Lecture du numéro de série NS collé sur la carte
117
Lecture de l'horloge interne Emission de la trame de fabrication
OUTIL DE FABRICATION 20
KPEM
E - 1
E(KPEM)
KROM
111
KMES
E - 1
E(KMES)
KROM
112
KALE
E - 1
E(KALE)
KROM
113
Initialisation de E (KPEM) / E(KMES) / E(KALE) dans l'outil de fabrication
114
FOURNISSEUR
Livraison au client de KPEM / KALE / KMES

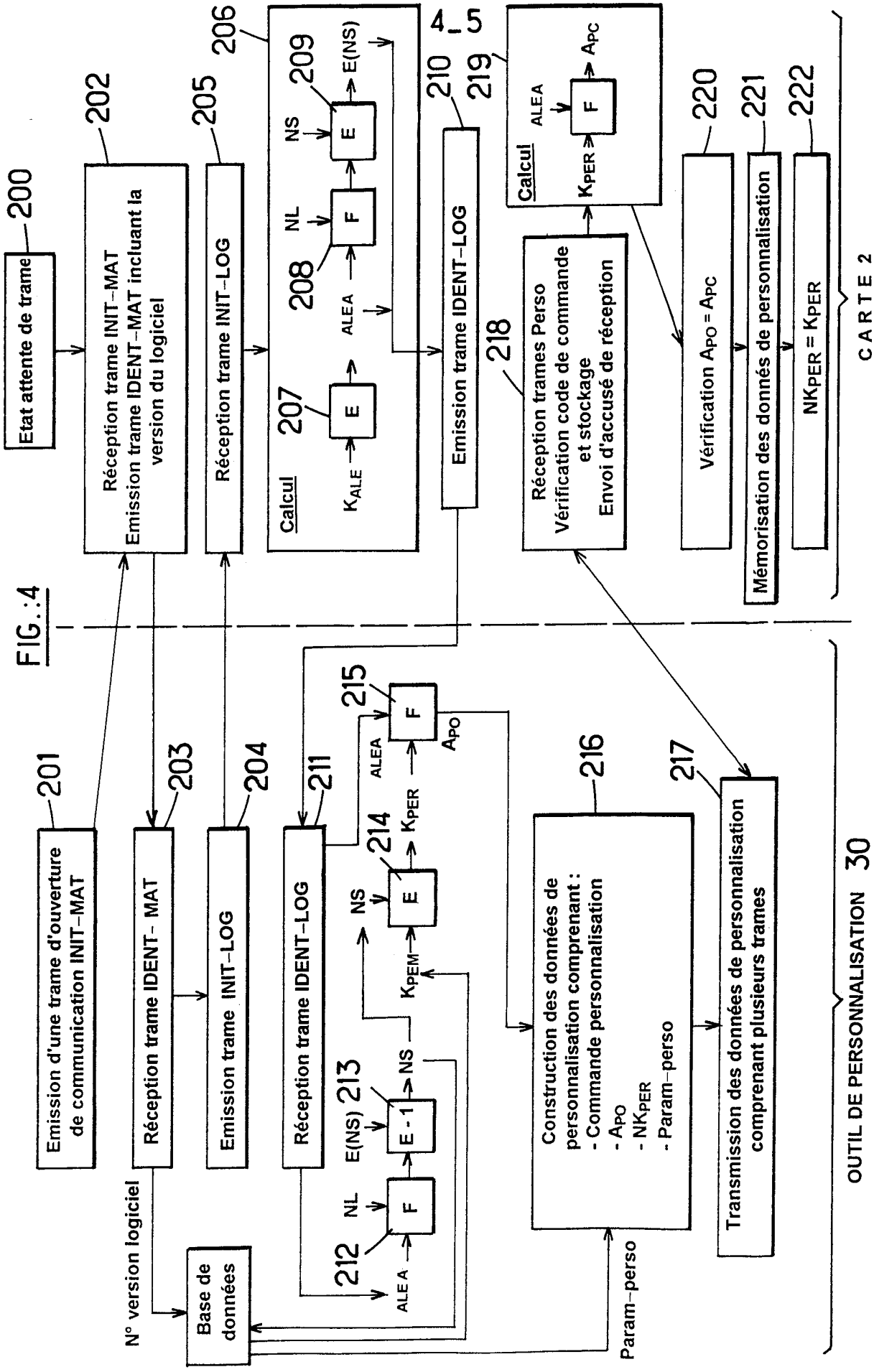
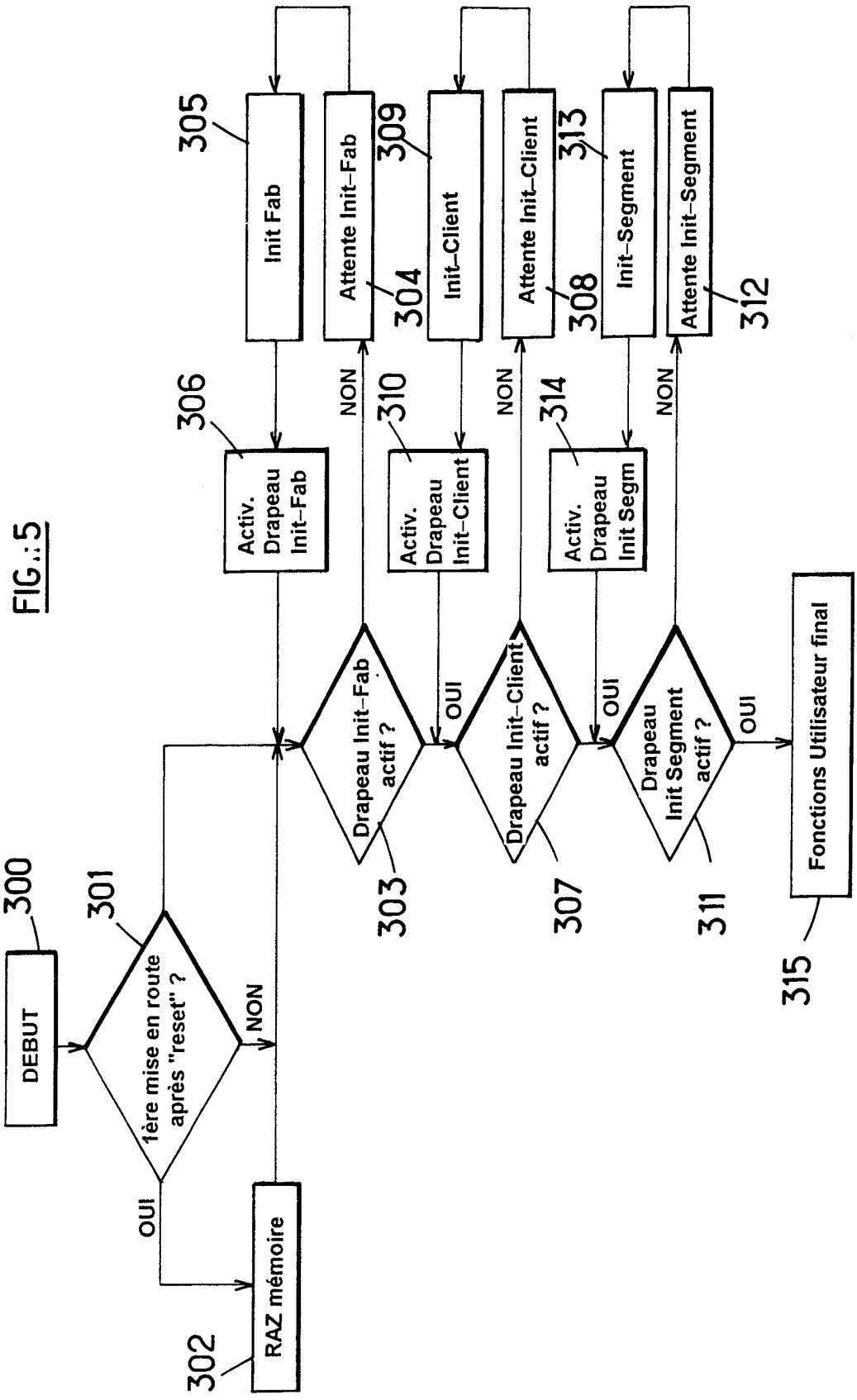

Etat attente de trame
200
Réception trame INIT-MAT
Emission trame IDENT-MAT incluant la version du logiciel
202
Réception trame INIT-LOG
205
206
Calcul
207
E
K_ALE
208
NL
F
ALEA
209
NS
E
E(NS)
4_5
210
Emission trame IDENT-LOG
219
Calcul
ALEA
F
K_PER
A_PC
Réception trames Perso
Vérification code de commande
et stockage
Envoi d'accusé de réception
218
220
Vérification A_PO = A_PC
221
Mémorisation des données de personnalisation
222
NK_PER = K_PER
CARTE 2
FIG.:4
201
Emission d'une trame d'ouverture de communication INIT-MAT
203
Réception trame IDENT- MAT
204
Emission trame INIT-LOG
211
Réception trame IDENT-LOG
215
ALEA
F
A_PO
214
NS
E
K_PER
K_PEM
213
E(NS)
E - 1
NS
212
NL
F
ALEA
216
Construction des données de personnalisation comprenant :
- Commande personnalisation
- A_PO
- NK_PER
- Param-perso
217
Transmission des données de personnalisation comprenant plusieurs trames
OUTIL DE PERSONNALISATION 30
N° version logiciel
Base de données
Param-perso

FIG.:5


DEBUT
300
1ère mise en route après "reset" ?
301
OUI
NON
RAZ mémoire
302
Drapeau Init-Fab actif ?
303
OUI
NON
Attente Init-Fab
304
Init Fab
305
Activ. Drapeau Init-Fab
306
Drapeau Init-Client actif ?
307
OUI
NON
Attente Init-Client
308
Init-Client
309
Activ. Drapeau Init-Client
310
Drapeau Init Segment actif ?
311
OUI
NON
Attente Init-Segment
312
Init-Segment
313
Activ. Drapeau Init Segm
314
Fonctions Utilisateur final
315

INTERNATIONAL SEARCH REPORT

Inter. ›nal Application No
PCT/FR 98/01820

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 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 6 G07F

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 173 103 A (CASIO COMPUTER COMPANY) 5 March 1986 see the whole document ---	1,12
A	GB 2 206 431 A (MOTOROLA INC) 5 January 1989 see the whole document ---	1
A	WO 93 10509 A (SECURITY DOMAIN PTY. LTD.) 27 May 1993 cited in the application see the whole document ---	1,12
A	DE 39 27 270 A (DEUTSCHE BUNDESPOST) 28 February 1991 see the whole document ---	1,2,12
	-/--	

[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
18 December 1998	04/01/1999

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	Meulemans, J-P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter. ›nal Application No
PCT/FR 98/01820

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 610 886 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 17 August 1994 see the whole document	1,12
A	EP 0 325 506 A (SGS-THOMPSON MICROELECTRONICS) 26 July 1989 see the whole document	1-19
A	WO 96 28796 A (SCLUMBERGER INDUSTRIES S. A.) 19 September 1996 see the whole document	1-19

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr nal Application No
PCT/FR 98/01820

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 173103 A	05-03-1986	US 4650975 A	17-03-1987
		AU 3516389 A	21-09-1989
		AU 559071 B	19-02-1987
		AU 4559685 A	06-03-1986
		AU 586715 B	20-07-1989
		AU 6562386 A	26-02-1987
		CA 1237194 A	24-05-1988
		DE 3584556 A	05-12-1991
		FR 2569885 A	07-03-1986
		GB 2164181 A,B	12-03-1986
		GB 2191881 A,B	23-12-1987
		GB 2191882 A,B	23-12-1987
		HK 47189 A	23-06-1989
		HK 47289 A	23-06-1989
		JP 1845953 C	25-05-1994
		JP 61059587 A	27-03-1986
GB 2206431 A	05-01-1989	DE 3889017 D	19-05-1994
		DE 3889017 T	20-10-1994
		EP 0297209 A	04-01-1989
		HK 4994 A	28-01-1994
		US 4841133 A	20-06-1989
WO 9310509 A	27-05-1993	AU 656245 B	27-01-1995
		EP 0722596 A	24-07-1996
		FI 942177 A	11-05-1994
		NO 941774 A	11-05-1994
		US 5534857 A	09-07-1996
DE 3927270 A	28-02-1991	NONE	
EP 610886 A	17-08-1994	JP 6236447 A	23-08-1994
		US 5506396 A	09-04-1996
EP 325506 A	26-07-1989	FR 2626095 A	21-07-1989
		JP 2005160 A	10-01-1990
		JP 2759102 B	28-05-1998
		US 5014312 A	07-05-1991
WO 9628796 A	19-09-1996	FR 2731536 A	13-09-1996
		DE 19680253 T	22-05-1997

RAPPORT DE RECHERCHE INTERNATIONALE

Dem : Internationale No
PCT/FR 98/01820

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 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 6 G07F

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)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 173 103 A (CASIO COMPUTER COMPANY) 5 mars 1986 voir le document en entier	1,12
A	GB 2 206 431 A (MOTOROLA INC) 5 janvier 1989 voir le document en entier	1
A	WO 93 10509 A (SECURITY DOMAIN PTY. LTD.) 27 mai 1993 cité dans la demande voir le document en entier	1,12
A	DE 39 27 270 A (DEUTSCHE BUNDESPOST) 28 février 1991 voir le document en entier	1,2,12

-/--

[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
18 décembre 1998	04/01/1999

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	Meulemans, J-P

1

RAPPORT DE RECHERCHE INTERNATIONALE

Dem: Internationale No
PCT/FR 98/01820

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 0 610 886 A (MITSUBISHI DENKI KABUSHIKI KAISHA) 17 août 1994 voir le document en entier	1,12
A	EP 0 325 506 A (SGS-THOMPSON MICROELECTRONICS) 26 juillet 1989 voir le document en entier	1-19
A	WO 96 28796 A (SCLUMBERGER INDUSTRIES S. A.) 19 septembre 1996 voir le document en entier	1-19

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem. e Internationale No
PCT/FR 98/01820

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 173103 A	05-03-1986	US 4650975 A	17-03-1987
		AU 3516389 A	21-09-1989
		AU 559071 B	19-02-1987
		AU 4559685 A	06-03-1986
		AU 586715 B	20-07-1989
		AU 6562386 A	26-02-1987
		CA 1237194 A	24-05-1988
		DE 3584556 A	05-12-1991
		FR 2569885 A	07-03-1986
		GB 2164181 A,B	12-03-1986
		GB 2191881 A,B	23-12-1987
		GB 2191882 A,B	23-12-1987
		HK 47189 A	23-06-1989
		HK 47289 A	23-06-1989
		JP 1845953 C	25-05-1994
		JP 61059587 A	27-03-1986
GB 2206431 A	05-01-1989	DE 3889017 D	19-05-1994
		DE 3889017 T	20-10-1994
		EP 0297209 A	04-01-1989
		HK 4994 A	28-01-1994
		US 4841133 A	20-06-1989
WO 9310509 A	27-05-1993	AU 656245 B	27-01-1995
		EP 0722596 A	24-07-1996
		FI 942177 A	11-05-1994
		NO 941774 A	11-05-1994
		US 5534857 A	09-07-1996
DE 3927270 A	28-02-1991	AUCUN	
EP 610886 A	17-08-1994	JP 6236447 A	23-08-1994
		US 5506396 A	09-04-1996
EP 325506 A	26-07-1989	FR 2626095 A	21-07-1989
		JP 2005160 A	10-01-1990
		JP 2759102 B	28-05-1998
		US 5014312 A	07-05-1991
WO 9628796 A	19-09-1996	FR 2731536 A	13-09-1996
		DE 19680253 T	22-05-1997