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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
11 juin 2009 (11.06.2009)

(10) Numéro de publication internationale
WO 2009/071819 A1

(51) Classification internationale des brevets :
G06F 21/00 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2008/052106

(22) Date de dépôt international :
21 novembre 2008 (21.11.2008)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
07 08242 26 novembre 2007 (26.11.2007) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **SAGEM SECURITE** [FR/FR]; 27 rue Leblanc, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **PELLETIER, Hervé** [FR/FR]; SAGEM SECURITE, Le Ponant de Paris, 27 rue Leblanc, F-75015 Paris (FR). **DUMAS, Pascal** [FR/FR]; SAGEM SECURITE, Le Ponant de Paris, 27 rue Leblanc, F-75015 Paris (FR).

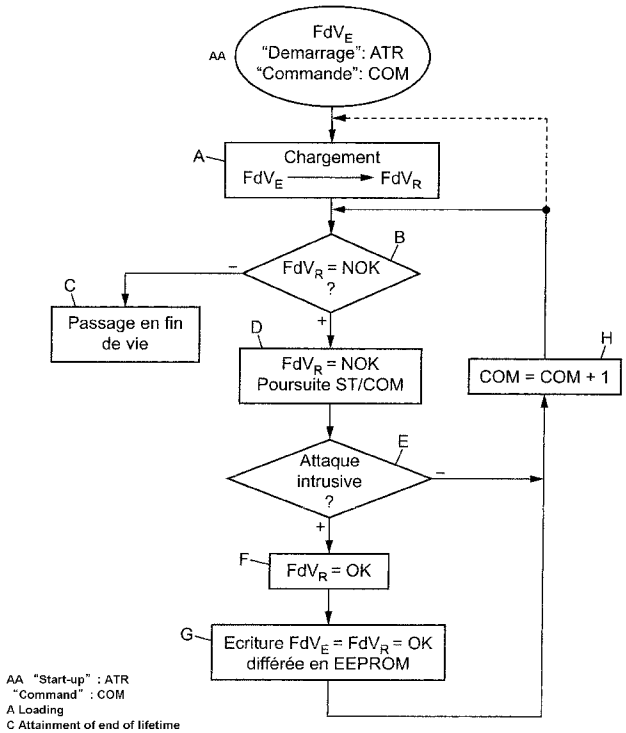
(74) Mandataire : **Cabinet Plasseraud**; 52 rue de la Victoire, F-75440 Paris Cedex 09 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW,

[Suite sur la page suivante]

(54) **Title:** METHOD OF MASKING ATTAINMENT OF END OF LIFETIME OF AN ELECTRONIC DEVICE AND DEVICE COMPRISING A CORRESPONDING CONTROL MODULE

(54) **Titre :** PROCEDE DE MASQUAGE DE PASSAGE EN FIN DE VIE D'UN DISPOSITIF ELECTRONIQUE ET DISPOSITIF COMPORTANT UN MODULE DE CONTROLE CORRESPONDANT



AA "Start-up" : ATR
"Command" : COM
A Loading
C Attainment of end of lifetime
D Continue ST/COM
E Intrusive attack?
G FdV$_E$=FdV$_R$=OK deferred in EEPROM

nothing else to translate

FIG. 1a

(57) Abstract: A method of masking attainment of the end of lifetime of an electronic microprocessor device comprising a reprogrammable non-volatile memory containing an end-of-lifetime state variable (FdV$_E$). On start-up (ATR), the value of the variable (FdV$_E$) is loaded (A) into random access memory. Before the execution of any current command (COM), the value of the variable (FdV$_R$) in random access memory is checked (B) to verify whether it has the value not true. Attainment of end of lifetime is executed (C) upon a negative response. Otherwise, the initialization or the execution of the command (COM) is continued (D). On detection (E) of an intrusive attack, the end-of-lifetime state variable (FdV$_R$) is instantiated (F) to the value true by writing to the sole random access memory, and then the writing of the variable (FdV$_E$) is deferred (G) to the value true in the non-volatile memory until the next writing operation. Application to any electronic device, microprocessor card or the like.

[Suite sur la page suivante]

WO 2009/071819 A1

MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* **:** ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

(57) Abrégé : Un procédé de masquage de passage en fin de vie d'un dispositif électronique à microprocesseur comportant une mémoire non volatile reprogrammable contenant une variable d'état de fin de vie (FdV_E). Au démarrage (ATR) on charge (A) en mémoire vive la valeur de la variable (FdV_E). Avant l'exécution de toute commande courante (COM), on vérifie (B) la valeur de la variable (FdV_R) en mémoire vive à la valeur non vraie. On exécute (C) le passage en fin de vie sur réponse négative. Sinon, on poursuit (D) l'initialisation ou l'exécution de la commande (COM). Sur détection (E) d'une attaque intrusive on instancie (F) par écriture dans la seule mémoire vive la variable d'état de fin de vie (FdV_R) à la valeur vraie puis on diffère (G) l'écriture de la variable (FdV_E) à la valeur vraie dans la mémoire non volatile jusqu'à la prochaine opération d'écriture. Application à tout dispositif électronique, carte à microprocesseur ou autre.

Procédé de masquage de passage en fin de vie d'un dispositif électronique et dispositif comportant un module de contrôle correspondant

L'invention concerne un procédé de masquage de passage en fin de vie d'un dispositif électronique, comprenant un port d'entrée-sortie, un microprocesseur, une mémoire vive, une mémoire morte et une mémoire non volatile reprogrammable contenant une variable d'état de fin de vie du dispositif électronique gérée par un module de contrôle.

De tels dispositifs électroniques correspondent, de manière non exclusive, aux cartes électroniques, ou à tout dispositif électronique comportant au moins ou entrant en relation avec, une carte électronique, telle que, notamment, une carte à microprocesseur, pour laquelle une bonne résistance sécuritaire est requise, vis-à-vis de toute intrusion externe.

Pour assurer une bonne résistance sécuritaire des cartes précitées, un mécanisme de passage en fin de vie est activé, sur détection d'un certain nombre d'erreurs critiques.

Le processus de passage en fin de vie de ce type de dispositif, notamment en ce qui concerne les cartes à microprocesseur, apparaît cependant problématique, car un tel processus s'appuie, globalement, sur un processus d'écriture en mémoire reprogrammable non volatile, généralement mémoire EEPROM, ce processus d'écriture

ayant pour objet l'effacement des données et le blocage des applications.

Un tel processus apparaît toutefois vulnérable, car il est détectable en dehors de la carte, en raison notamment du fort appel de courant engendré par le processus d'écriture en mémoire reprogrammable et demande en outre un certain temps pour l'exécuter.

Un tiers indélicat dispose donc de tout loisir d'empêcher l'exécution d'un tel processus, en coupant l'alimentation électrique du dispositif ou de la carte.

La présente invention a en conséquence pour objet de rendre le processus de passage en fin de vie d'un tel dispositif électronique totalement certain dans un délai aléatoire après l'évènement, erreur critique, à l'origine du déclenchement de passage en fin de vie, en masquant, notamment à tout tiers, l'opération d'écriture en mémoire non volatile correspondant au passage en fin de vie, ce qui interdit en pratique toute attaque par canal caché.

Selon un aspect remarquable, l'invention a pour objet le masquage de toute écriture d'une variable d'état de passage en fin de vie en mémoire non volatile d'un dispositif électronique, par dilution de cette opération d'écriture dans le déroulement normal du programme d'application exécuté par le dispositif électronique.

Le procédé de masquage de passage en fin de vie d'un dispositif électronique, objet de l'invention, s'applique à tout dispositif électronique comprenant un

microprocesseur, une mémoire vive, une mémoire morte, une mémoire non volatile reprogrammable contenant une variable d'état de fin de vie gérée par un module de contrôle et un port d'entrée/sortie.

Il est remarquable en ce que, lors du démarrage du dispositif électronique, il consiste à charger en mémoire vive, à partir de la mémoire non volatile, la valeur de la variable d'état de fin de vie, et, préalablement à l'exécution de toute commande courante par le microprocesseur, vérifier la valeur de cette variable d'état de fin de vie mémorisée en mémoire vive à la valeur non vraie, et, sur réponse négative à cette vérification, exécuter les opérations de passage en fin de vie du dispositif électronique ; sinon, la variable d'état de fin de vie mémorisée en mémoire vive étant à la valeur non vraie, poursuivre l'initialisation ou l'exécution de la commande courante par le microprocesseur du dispositif électronique, et, sur détection d'une attaque intrusive, instancier par écriture, dans la seule mémoire vive, la variable d'état de fin de vie du dispositif électronique à la valeur vraie et poursuivre l'initialisation et/ou l'exécution de la commande courante, et, différer l'écriture de la variable d'état de fin de vie à la valeur vraie dans la mémoire non volatile pour l'effectuer en lieu et place de la prochaine opération d'écriture en mémoire non volatile, ce qui permet de masquer l'inscription de la variable d'état de fin de vie.

Le procédé objet de l'invention est également remarquable en ce qu'il consiste en outre, préalablement à

l'exécution de chaque commande par le microprocesseur, à charger en mémoire vive, à partir de la mémoire non volatile, la valeur de la variable d'état de fin de vie.

Le procédé, objet de l'invention, est également remarquable en ce que, pour un ensemble de commandes exécutées par le microprocesseur du dispositif électronique incluant des commandes comprenant une inscription systématique en mémoire non volatile et des commandes ne comprenant pas d'inscription en mémoire non volatile, il consiste en outre, indépendamment de la détection ou de la non détection d'une attaque intrusive, à exécuter l'écriture en mémoire non volatile d'un octet factice, ce qui permet de masquer toute écriture éventuellement de la variable d'état de fin de vie du dispositif électronique en mémoire non volatile.

De préférence, l'opération d'écriture en mémoire non volatile de cet octet factice est exécutée dans la même page mémoire que celle de la variable d'état de fin de vie.

En outre, selon un autre aspect remarquable du procédé objet de l'invention, l'opération d'écriture en mémoire non volatile de cet octet factice est exécutée préalablement à toute exécution d'opération de transmission de données sur la ligne du port d'entrée/sortie du dispositif électronique.

Selon un autre aspect remarquable, le procédé, objet de l'invention, inclut en outre, consécutivement à toute étape d'écriture en mémoire volatile de la variable

d'état de fin de vie, une étape consistant à vérifier à la valeur vraie la valeur de la variable d'état de fin de vie, et, sur vérification à cette valeur vraie, une étape d'exécution des opérations de passage en fin de vie du dispositif électronique.

Selon un autre aspect, le procédé objet de l'invention est en outre remarquable en ce que, sur vérification de la valeur de cette variable d'état de fin de vie à la valeur vraie, à l'opération d'écriture en mémoire non volatile de cet octet factice est substituée l'opération d'écriture en mémoire non volatile de la valeur de la variable d'état de fin de vie.

Le dispositif électronique, objet de l'invention, comprend un microprocesseur, une mémoire vive, une mémoire morte, une mémoire non volatile reprogrammable contenant une variable d'état de fin de vie du dispositif électronique gérée par un module de contrôle et un port d'entrée/sortie (I/O). Il est remarquable en ce que ce module de contrôle inclut un module de programme d'ordinateur d'exécution des étapes du procédé objet de l'invention précédemment citées.

Le procédé de masquage de passage en fin de vie d'un dispositif électronique et le dispositif électronique incluant un module de contrôle correspondant, objets de l'invention, trouvent application à tout type de dispositif électronique, mais, de manière préférentielle non limitative, à des dispositifs électroniques tels que les cartes à microprocesseur traitant et/ou stockant des données personnelles, privées ou secrètes.

Ils seront mieux compris à la lecture de la description et à l'observation des figures ci-après, dans lesquelles :

- la figure 1a représente, à titre purement illustratif, un organigramme des étapes essentielles de mise en œuvre du procédé objet de l'invention ;
- La figure 1b représente, à titre purement illustratif un chronogramme des différentes étapes exécutées au cours de la mise en œuvre du procédé objet de l'invention illustré en figure 1a ;
- Les figures 1c à 1f représentent des détails de mise en œuvre des étapes de procédé illustré en figure 1a ;
- La figure 2 représente, à titre purement illustratif, sous forme de schéma fonctionnel, l'architecture d'un dispositif électronique muni d'un module de contrôle de passage en fin de vie conforme à l'objet de la présente invention.

Une description plus détaillée du procédé de masquage de passage en fin de vie d'un dispositif électronique, conforme à l'objet de la présente invention, sera maintenant donnée en liaison avec les figures 1a à 1f.

D'une manière générale, on indique que le procédé de masquage de passage en fin de vie d'une carte électronique, objet de la présente invention, s'applique à tout dispositif électroniques comprenant un

microprocesseur, une mémoire vive, une mémoire morte et une mémoire non volatile reprogrammable contenant une variable d'état de fin de vie du dispositif électronique, gérée par un module de contrôle. De manière plus particulière, le dispositif électronique peut comporter également un port d'entrée/sortie permettant l'échange de données soit avec un appareil hôte ou même en réseau, par exemple. La notion de mémoire non volatile reprogrammable couvre les mémoires reprogrammables électriquement, mémoires EEPROM, les mémoires flash, par exemple.

L'appareil électronique précité, lors de son fonctionnement, exécute une phase de démarrage, notée ATR (Answer To Reset en anglais), puis des commandes courantes successives, notées COM.

On comprend, en particulier, que le dispositif électronique correspondant peut avantageusement être constitué par toute carte à microprocesseur, par exemple.

En référence à la figure 1a, le procédé de masquage de passage en fin de vie d'un dispositif électronique, objet de l'invention, comprend une étape A consistant à charger en mémoire vive du dispositif électronique, à partir de la mémoire non volatile de ce dernier, la valeur notée FdV_E de la variable de fin de vie mémorisée en mémoire non volatile.

L'opération correspondante à l'étape A est notée :

$FdV_E \longrightarrow FdV_R$.

Dans la relation précédente, FdV_R désigne la valeur de la variable d'état de fin de vie du dispositif électronique chargée en mémoire vive.

Suite à l'étape A de la figure 1a, et préalablement à l'exécution de toute commande courante COM par le microprocesseur, le procédé objet de l'invention consiste ensuite, en une étape B, à vérifier la valeur de la variable d'état de fin de vie mémorisée en mémoire vive à la valeur non vraie. À l'étape B de la figure 1a, la vérification est représentée par une étape de test :

FdV_R = NOK ?

Dans cette relation NOK représente la valeur non vraie de la variable d'état de fin de vie du dispositif électronique mémorisée en mémoire vive.

Sur réponse négative au test de l'étape B, le procédé objet de l'invention consiste à exécuter C les opérations de passage en fin de vie du dispositif électronique.

Au contraire sur réponse positive au test exécuté à l'étape B, la variable d'état de fin de vie mémorisée en mémoire vive FdVR étant à la valeur non vraie NOK, le procédé objet de l'invention consiste à poursuivre l'initialisation ou l'exécution de la commande courante COM par le microprocesseur du dispositif électronique. On indique que l'exécution de la commande courante correspond à toute commande d'une application exécutée par le dispositif électronique.

Au cours de cette exécution et sur détection, à une étape

E, d'une attaque intrusive, le procédé objet de l'invention consiste, en une étape F, à instancier par écriture dans la seule mémoire vive la variable d'état de fin de vie du dispositif électronique, la variable FdV_R, à la valeur vraie et à poursuivre l'initialisation et/ou l'exécution de la commande courante COM.

A l'étape F de la figure 1a l'opération d'instanciation est notée par la relation :

FdV_R = OK.

Dans la relation précédente, on indique que la valeur OK désigne la valeur vraie de la variable d'état de fin de vie mémorisée en mémoire vive.

Enfin l'étape d'instanciation F précitée est suivie d'une étape G consistant à différer l'écriture de la variable d'état de fin de vie FdV_E à la valeur vraie dans la mémoire non volatile, pour l'effectuer en lieu et place de la prochaine opération d'écriture en mémoire non volatile. Ceci permet de masquer l'inscription de la variable d'état de fin de vie.

On comprend bien entendu que l'étape G précitée est suivie d'un retour à l'exécution de la commande courante suivante par l'intermédiaire de l'étape H. À l'étape précitée, COM+1 désigne la commande suivante.

Ainsi que représenté sur la figure 1a, le retour est effectué à L'Étape B pour la simple exécution de la commande suivante.

Toutefois, selon une autre possibilité de mise en œuvre du procédé objet de l'invention, le retour peut être effectué, ainsi que représenté en pointillé au dessin de la figure 1a, en amont du chargement exécuté à l'étape A, pour renouvellement du processus de chargement en mémoire vive de la valeur de la variable d'état de fin de vie FdV_E de manière systématique. Un tel processus n'est toutefois pas indispensable mais peut être mis en œuvre en variante.

Sur la figure 1b, on a représenté un chronogramme des opérations d'exécution des étapes de la figure 1a.

En particulier, l'étape A peut être exécutée au démarrage ATR ou préalablement à l'exécution de chaque commande COM, ainsi que mentionné précédemment.

Le test de l'étape B est exécuté préalablement à la poursuite du démarrage ou de l'exécution de la commande courante représentée en hachures à gauche sur la figure 1a. On rappelle que la réponse négative au test de l'étape B amène automatiquement le passage en fin de vie du dispositif électronique à l'étape C.

La poursuite du démarrage ou de l'initialisation ou encore de l'exécution de la commande courante à l'étape D correspond en fait à la mise en œuvre de processus algorithmiques manipulant des secrets pour le dispositif électronique, lorsque ce dernier est constitué par une carte à microprocesseur par exemple.

Le test de l'étape E correspondant à un test de détection

d'attaque intrusive peut être mis en œuvre de manière classique soit par l'exécution de mécanismes anti-DFA (Differential Fault Analysis en anglais, procédé d'attaque consistant à introduire une erreur dans un traitement pour en déduire des informations sur les données traitées) soit par des processus de vérification de l'intégrité des données par exemple.

L'étape d'instanciation de la variable d'état de fin de vie du dispositif électronique par écriture dans la seule mémoire vive, étape F, est exécutée par le module de contrôle du passage en fin de vie du dispositif électronique et opère par écriture de cette variable d'état à la valeur vraie selon la relation précédemment mentionnée :

FdV_R = OK.

L'étape G consistant en la mise à jour de la variable d'état de fin de vie FdV_E en mémoire non volatile, c'est-à-dire le plus souvent en mémoire EEPROM, est alors exécutée de manière différée, c'est-à-dire en lieu et place de la prochaine écriture à effectuer dans la commande.

Sur la figure 1b, cette opération est représentée par un pic en hachures à droite illustrant l'augmentation de l'intensité de courant consommé par la mémoire précitée en raison de l'opération d'inscription dans la mémoire précitée.

L'étape E est alors suivie d'une étape de retour soit à l'étape B, soit à l'étape A, ainsi que décrit

précédemment en liaison avec la figure 1a.

D'une manière plus spécifique, on indique que la valeur non vraie, notée NOK, de la variable d'état de fin de vie du dispositif électronique a une valeur numérique arbitraire. La valeur vraie OK de la variable d'état de fin de vie est au contraire toute valeur numérique distincte de la valeur numérique arbitraire précitée.

Ainsi qu'on l'a en outre représenté en figure 1c, on considère tout ensemble de commandes exécutées par le microprocesseur du dispositif électronique incluant des commandes (COM_W) comprenant une inscription systématique en mémoire non volatile et des commandes ($\overline{COM_W}$) ne comprenant pas d'inscription en mémoire non volatile. Dans cette hypothèse, le procédé objet de l'invention consiste, indépendamment de la détection ou de la non détection d'une attaque intrusive, à exécuter l'écriture D_2 en mémoire non volatile d'un octet factice, lequel est noté OF. Ceci permet de masquer toute écriture éventuelle de la variable d'état de fin de vie du dispositif électronique en mémoire non volatile.

De préférence, l'écriture de l'octet factice OF est exécutée dans la même page mémoire que celle de la variable d'état de fin de vie.

À l'étape D_2 représentée en figure 1c l'opération d'écriture dans la même page mémoire est représentée par la relation :

WAP(OF) = WAP(FdVE).

Dans la relation précédente WAP désigne l'adresse de la page mémoire d'écriture.

L'étape D2 est suivie de l'appel de l'étape E de la figure 1a.

En outre, ainsi que représenté sur la même figure 1c, l'opération d'écriture en mémoire non volatile de l'octet factice est exécutée préalablement à toute opération de transmission de données sur la ligne du port d'entrée/sortie du dispositif électronique. Sur la figure 1c l'opération correspondante est représentée de manière symbolique par la détection de toute opération d'entrée/sortie par la relation :

COM = I/O ?

La détection d'une telle opération provoque alors l'écriture systématique et immédiate de l'octet factice, ainsi que décrit précédemment dans la description.

Enfin, ainsi que représenté en figure 1 d, le procédé objet de l'invention inclut avantageusement, consécutivement à toute étape d'écriture en mémoire non volatile de la variable d'état de fin de vie telle que représentée à l'étape G1, une étape notée G2 consistant à vérifier à la valeur vraie la valeur de la variable d'état de fin de vie FdV_R mémorisée en mémoire vive. L'opération correspondante à l'étape précitée est notée selon la relation :

FdV_R = OK.

Sur vérification à la valeur vraie de la variable d'état de fin de vie, une étape d'exécution des opérations de passage en fin de vie du dispositif électronique est effectuée par appel de l'étape C représentée en figure 1a.

Au contraire, en l'absence de vérification à la valeur vraie de la variable d'état de fin de vie, un retour à l'étape H est effectué.

En outre, ainsi qu'on l'a également représenté en figure 1e, sur vérification à l'étape D_{21} de la valeur de la variable d'état de fin de vie FdV_R à la valeur vraie, soit sur réponse positive au test D_{21} précité, à l'opération d'écriture en mémoire non volatile de l'octet factice OF, représentée à l'étape D_{22} de la figure 1e, est substituée l'écriture en mémoire EEPROM de la valeur de la variable d'état de fin de vie FdVE par appel de l'étape G de la figure 1a.

Le procédé objet de l'invention permet en outre la mise en œuvre d'un compteur d'erreur.

D'une manière générale, la mise à jour d'un compteur d'erreur est soumise à la même restriction que l'écriture d'une variable de fin de vie.

En raison du fait qu'il s'agit d'une écriture en mémoire non volatile, de type EEPROM, une telle écriture est normalement détectable en raison de la surintensité

consommée par cette dernière au cours de l'opération d'écriture.

Le procédé objet de l'invention peut donc permettre de manière avantageuse, dans le cas de détection d'erreurs ne justifiant pas un passage direct en fin de vie, l'implémentation d'un compteur avant d'effectuer l'écriture normale. La valeur de ce compteur est ensuite régulièrement vérifiée et le dépassement d'une valeur de seuil permet de déclencher alors un passage en fin de vie.

Un tel mode opératoire est représenté en figure 1f, de la manière suivante :

-- sur détection I_1 d'une erreur d'exécution temporaire d'une instruction, distincte d'une attaque intrusive et ne justifiant pas d'un passage en fin de vie du dispositif électronique, la détection de l'erreur temporaire étant désignée ∃ TE ? , où TE désigne l'erreur d'exécution temporaire précitée, la réponse positive au test I_1 appelle une étape I_2 de mise à jour par implémentation d'un compteur d'erreur en mémoire vive.
La valeur mise à jour à l'étape I_2 représentée par la relation :
TE = TE + 1 est alors suivie d'une étape de comparaison I_3 de la valeur de comptage des valeurs mises à jour à une valeur de seuil, notée STE.
À l'étape de test I_3 l'opération de comparaison est notée:
TE > STE ?

Sur dépassement de la valeur de seuil par la valeur de

comptage d'erreur actualisée, c'est-à-dire sur réponse positive au test I_3, l'écriture de la valeur de la variable d'état de fin de vie du dispositif électronique à la valeur vraie et le passage en fin de vie sont effectués par appel de l'étape F puis G, ainsi que représenté en figure 1f.

Un dispositif électronique comportant un microprocesseur noté 1_1, une mémoire vive notée 1_2, une mémoire non volatile de type EEPROM par exemple, notée 1_3, et une mémoire morte notée 1_4 est maintenant décrit en liaison avec la figure 2. En outre, ainsi que représenté sur la figure précitée, le dispositif comprend un port d'entrée sortie noté I/O.

Ainsi qu'on l'a représenté sur la figure 2, le dispositif électronique en fonctionnement comporte une variable d'état de fin de vie de ce dispositif électronique, notée FdV_E, gérée par un module de contrôle CM lequel peut par exemple être un module logiciel implanté en mémoire morte 1_4.

Le module de contrôle CM inclut un module de programmes d'ordinateur SCM permettant bien entendu l'exécution des étapes du procédé de masquage de passage en fin de vie d'un dispositif électronique, ainsi que précédemment décrits en liaison avec les figures 1a à 1f.

Bien entendu, le module de programme d'ordinateur SCM peut être implanté en mémoire non volatile de type EEPROM, laquelle constitue un support de mémorisation. Ce module de programme d'ordinateur inclut une suite

d'instructions exécutables par le microprocesseur du dispositif électronique et, lors de l'exécution des instructions précitées, exécute les étapes de mise en œuvre du procédé, tel que décrit précédemment en liaison avec les figures 1a à 1f.

Le procédé de masquage de passage en fin de vie d'un dispositif électronique, objet de l'invention, a été mis en œuvre sur des cartes électroniques. Des tests très poussés exécutés sur ces cartes électroniques par des entités de confiance indépendantes n'ont pas permis d'empêcher le passage en fin de vie de ces cartes électroniques, contrairement aux cartes électroniques munies de processus de passage en fin de vie classique, pour lesquelles il est possible de répéter des attaques intrusives jusqu'à la mise en évidence d'une faille exploitable. En conséquence, il apparaît que le procédé objet de l'invention ne permet plus de différencier à temps le cas où une attaque a été détectée et va donc entraîner un passage en fin de vie du dispositif électronique du cas où l'attaque n'a pas été détectée ou n'a produit aucun effet.

REVENDICATIONS

1. Procédé de masquage de passage en fin de vie d'un dispositif électronique comprenant un microprocesseur, une mémoire vive, une mémoire morte, une mémoire non volatile reprogrammable contenant une variable d'état de fin de vie du dispositif électronique gérée par un module de contrôle et un port d'entrée/sortie, caractérisé en ce que ledit procédé consiste au moins, lors du démarrage (ATR) du dispositif électronique, à :

- charger (A) en mémoire vive, à partir de ladite mémoire non volatile, la valeur (FdV_E) de ladite variable d'état de fin de vie ; et, préalablement à l'exécution de toute commande courante par ledit microprocesseur ;

- vérifier (B) la valeur de ladite variable d'état de fin de vie mémorisée en mémoire vive (FdV_R) à la valeur non vraie ; et, sur réponse négative à cette vérification ;

- exécuter (C) les opérations de passage en fin de vie du dispositif électronique ; sinon, ladite variable d'état de fin de vie mémorisée en mémoire vive (FdV_R) étant à la valeur non vraie,

- poursuivre (D) l'initialisation ou l'exécution de la commande courante (COM) par le microprocesseur du dispositif électronique ; et, sur détection (E) d'une attaque intrusive,

- instancier (F) par écriture, dans la seule mémoire vive, ladite variable d'état de fin de vie du dispositif électronique (FdV_R) à la valeur vraie et

poursuivre l'initialisation et/ou l'exécution de la commande courante ; et

- différer (G) l'écriture de la variable d'état de fin de vie (FdV_E) à la valeur vraie dans ladite mémoire non volatile pour l'effectuer en lieu et place de la prochaine opération d'écriture en mémoire non volatile dans la commande, ce qui permet de masquer l'inscription de ladite variable d'état de fin de vie.

2. Procédé selon la revendication 1, caractérisé en ce que la valeur non vraie (FdV_R=NOK) de ladite variable d'état de fin de vie du dispositif électronique est une valeur numérique arbitraire et en ce que la valeur vraie (FdV_R = OK) de ladite variable d'état de fin de vie du dispositif électronique est toute valeur numérique distincte de ladite valeur numérique arbitraire.

3. Procédé selon l'une des revendications précédentes, caractérisé en ce que pour un ensemble de commandes exécutées par le microprocesseur du dispositif électronique ($COM \in \{COM_W, \overline{COM_W}\}$) incluant des commandes (COM_w) comprenant une inscription systématique en mémoire non volatile et des commandes ($\overline{COM_W}$) ne comprenant pas d'inscription en mémoire non volatile, ledit procédé consiste en outre, indépendamment de la détection ou de la non détection d'une attaque intrusive, à exécuter l'écriture en mémoire non volatile d'un octet factice, ce qui permet de masquer toute écriture éventuelle de la variable d'état de fin de vie du dispositif électronique en mémoire non volatile.

4. Procédé selon la revendication 3, caractérisé en ce que celui-ci consiste à exécuter l'écriture dudit

octet factice dans la même page mémoire que celle de ladite variable d'état de fin de vie.

5. Procédé selon l'une des revendications 3 ou 4, caractérisé en ce que, ladite opération d'écriture en mémoire non volatile dudit octet factice est exécutée préalablement à toute exécution d'opération de transmission de données sur la ligne du port d'entrée/sortie du dispositif électronique à microprocesseur.

6. Procédé selon la revendication 5, caractérisé en ce que, sur vérification de la valeur de ladite variable d'état de fin de vie (FdV_R) à la valeur vraie, à ladite opération d'écriture en mémoire non volatile dudit octet factice est substituée l'opération d'écriture en mémoire non volatile de la valeur de la variable d'état de fin de vie (FdV_E) :

7. Procédé selon l'une des revendications 3 à 6, caractérisé en ce que celui-ci inclut en outre, consécutivement à toute étape d'écriture en mémoire non volatile de la variable d'état de fin de vie (FdV_E) une étape consistant à vérifier à la valeur vraie, la valeur de ladite variable d'état de fin de vie, mémorisée en mémoire vive (FdVr), et, sur vérification à la valeur vraie, une étape d'exécution des opérations de passage en fin de vie du dispositif électronique.

8. Procédé selon l'une des revendications précédentes, caractérisé en ce que, sur détection d'une erreur d'exécution temporaire d'une instruction distincte d'une attaque intrusive ne justifiant pas d'un passage en fin de vie du dispositif électronique, ledit procédé inclut en outre,

- la mise à jour par incrémentation d'un compteur

d'erreur en mémoire vive ;

- la comparaison de la valeur de comptage d'erreur à une valeur de seuil ; et, sur dépassement de ladite valeur de seuil par ladite valeur de comptage d'erreur,

- l'écriture de la valeur de ladite variable d'état de fin de vie du dispositif électronique à la valeur vraie et le passage en fin de vie du dispositif électronique.

9. Dispositif électronique comprenant un microprocesseur, une mémoire vive, une mémoire morte, une mémoire non volatile reprogrammable, contenant une variable d'état de fin de vie du dispositif électronique (FdV_E) gérée par un module de contrôle et un port d'entrée sortie, caractérisé en ce que ledit module de contrôle inclut un module de programme d'ordinateur (SCM) d'exécution des étapes du procédé selon l'une des revendications 1 à 8 ;

10. Produit de programme d'ordinateur mémorisé sur un support de mémorisation et incluant une suite d'instructions exécutables par un ordinateur ou par le microprocesseur d'un dispositif électronique, caractérisé en ce que, lors de l'exécution desdites instructions, ledit programme exécute les étapes du procédé selon l'une des revendications 1 à 8.

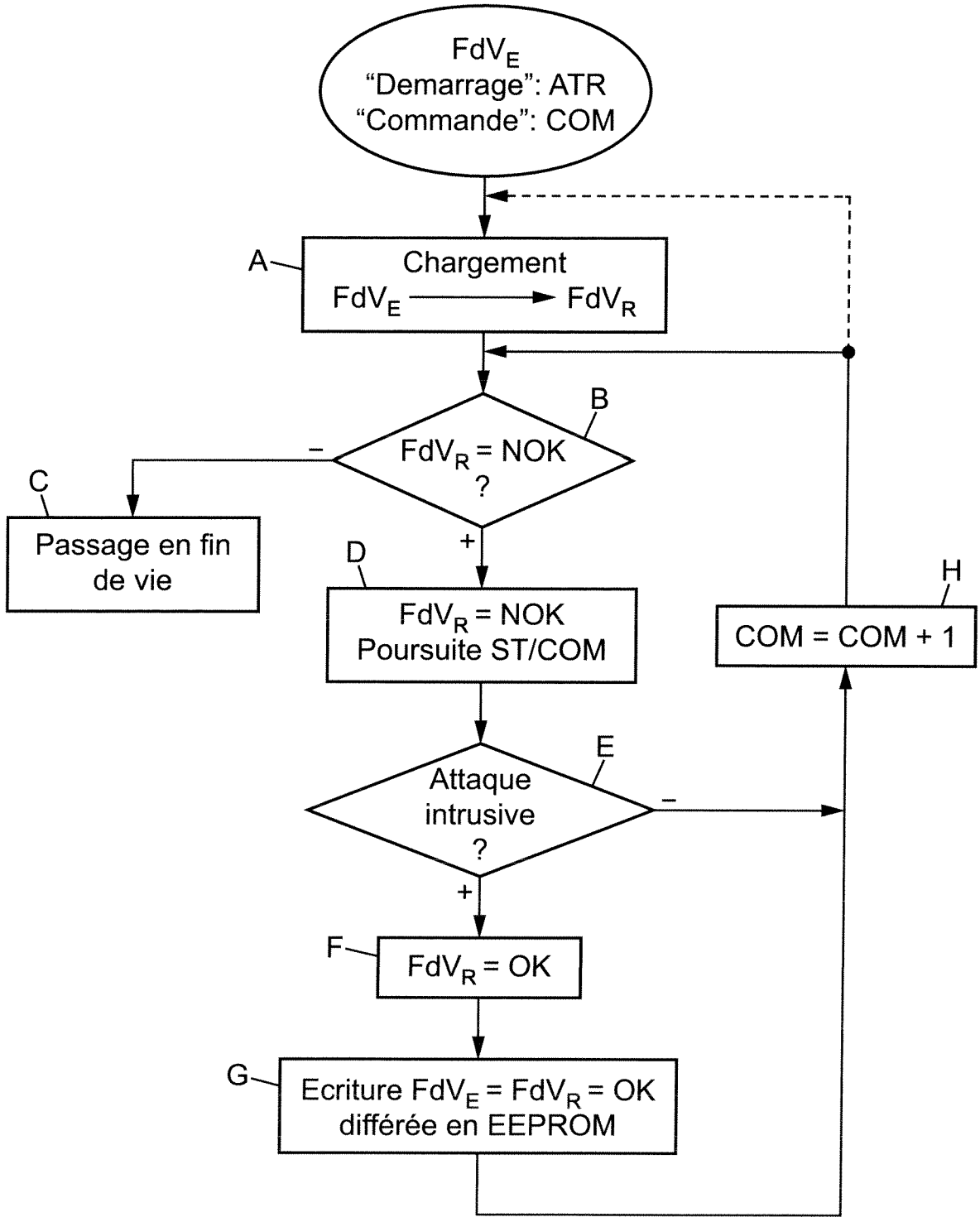

FdV_E
"Demarrage": ATR
"Commande": COM
A
Chargement
FdV_E → FdV_R
B
FdV_R = NOK
?
–
+
C
Passage en fin
de vie
D
FdV_R = NOK
Poursuite ST/COM
H
COM = COM + 1
E
Attaque
intrusive
?
–
+
F
FdV_R = OK
G
Ecriture FdV_E = FdV_R = OK
différée en EEPROM

FIG. 1a

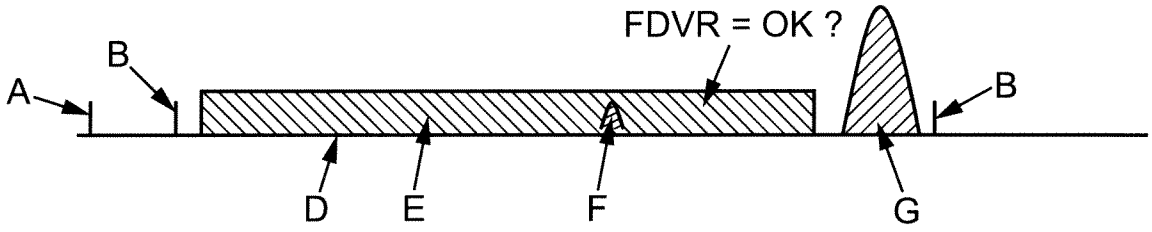

FDVR = OK ?
A
B
B
D
E
F
G

FIG. 1b

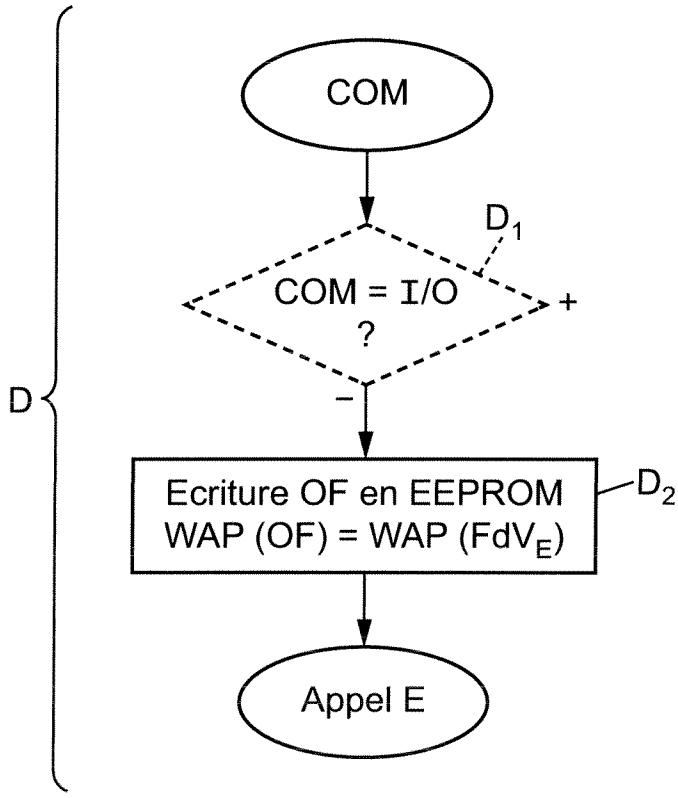

COM
D1
COM = I/O
?
+
–
D
Ecriture OF en EEPROM
WAP (OF) = WAP (FdVE)
D2
Appel E

FIG. 1c

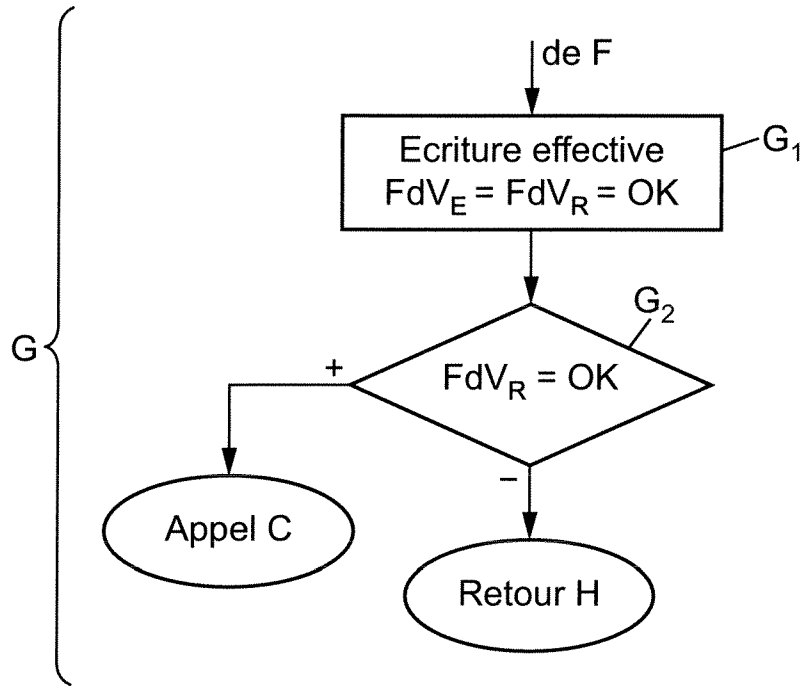

de F
Ecriture effective
FdV$_E$ = FdV$_R$ = OK
G$_1$
G$_2$
FdV$_R$ = OK
+
–
G
Appel C
Retour H

FIG. 1d

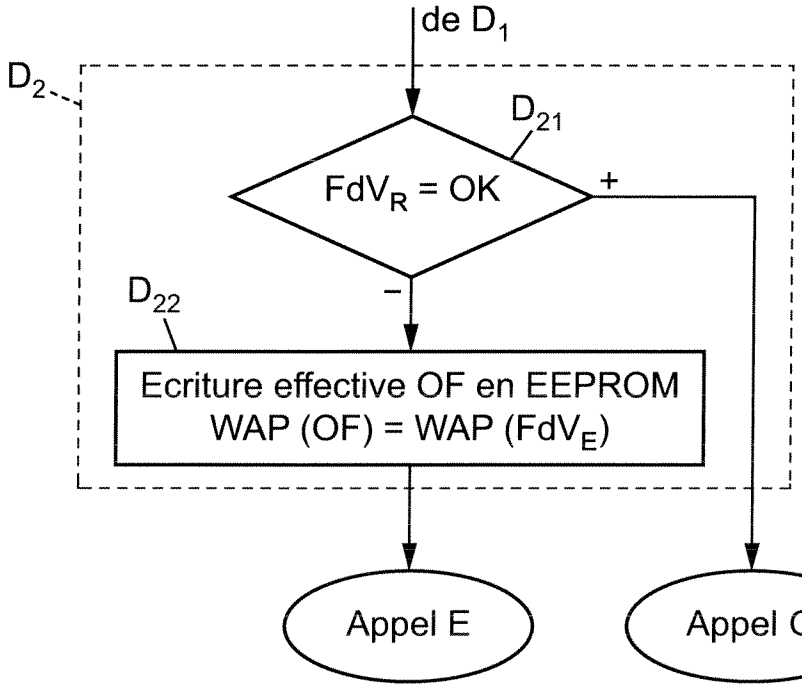

de D$_1$
D$_2$
D$_{21}$
FdV$_R$ = OK
+
–
D$_{22}$
Ecriture effective OF en EEPROM
WAP (OF) = WAP (FdV$_E$)
Appel E
Appel G

FIG. 1e

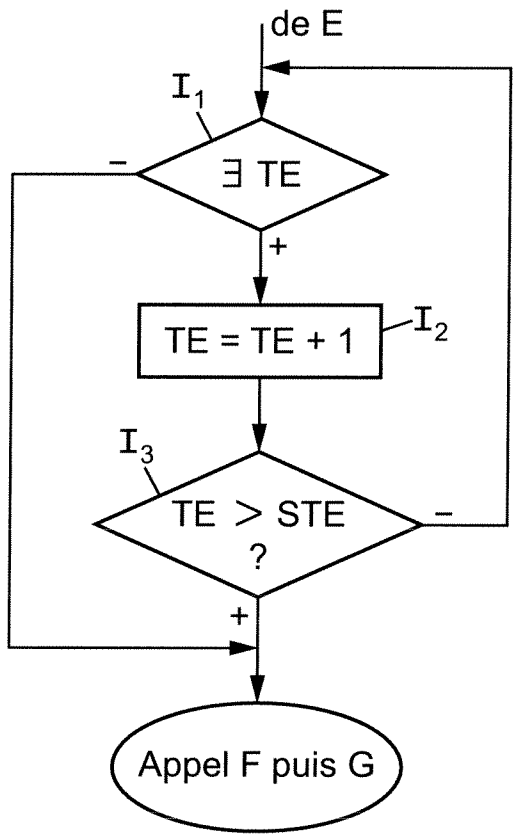

de E
I1
∃ TE
-
+
TE = TE + 1
I2
I3
TE > STE
?
-
+
Appel F puis G

FIG. 1f

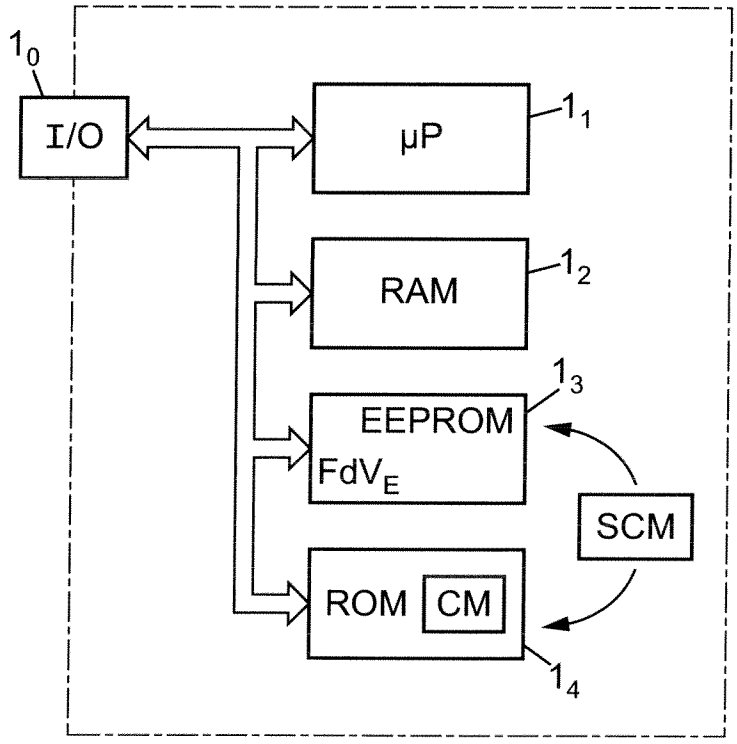

10
I/O
µP
11
RAM
12
EEPROM
FdVE
13
SCM
ROM
CM
14

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2008/052106

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

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)
G06F

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)
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 2 776 410 A (GEMPLUS CARD INT [FR]) 24 September 1999 (1999-09-24) abstract page 2, line 1 - page 3, line 13 page 6, line 6 - line 34	1-10
A	FR 2 784 763 A (GEMPLUS CARD INT [FR]) 21 April 2000 (2000-04-21) abstract page 1, line 1 - page 3, line 5 page 7, line 10 - page 8, line 36	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family 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
11 mai 2009	18/05/2009

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, Fax: (+31-70) 340-3016	Bichler, Marc

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2008/052106

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2776410 A	24-09-1999	CA 2323006 A1	30-09-1999
		CN 1288548 A	21-03-2001
		DE 69913667 D1	29-01-2004
		DE 69913667 T2	07-10-2004
		EP 1062633 A1	27-12-2000
		ES 2214012 T3	01-09-2004
		WO 9949416 A1	30-09-1999
		JP 2002508549 T	19-03-2002
		US 6698662 B1	02-03-2004
FR 2784763 A	21-04-2000	AU 6207799 A	08-05-2000
		CN 1332860 A	23-01-2002
		EP 1121629 A1	08-08-2001
		WO 0023866 A1	27-04-2000
		JP 2002528784 T	03-09-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2008/052106

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/00

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)
G06F

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 cela est réalisable, termes de recherche utilisés)
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 2 776 410 A (GEMPLUS CARD INT [FR]) 24 septembre 1999 (1999-09-24) abrégé page 2, ligne 1 - page 3, ligne 13 page 6, ligne 6 - ligne 34	1-10
A	FR 2 784 763 A (GEMPLUS CARD INT [FR]) 21 avril 2000 (2000-04-21) abrégé page 1, ligne 1 - page 3, ligne 5 page 7, ligne 10 - page 8, ligne 36	1-10

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ 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'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention 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
11 mai 2009	18/05/2009

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, Fax: (+31–70) 340–3016	Bichler, Marc

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2008/052106

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2776410 A	24-09-1999	CA 2323006 A1	30-09-1999
		CN 1288548 A	21-03-2001
		DE 69913667 D1	29-01-2004
		DE 69913667 T2	07-10-2004
		EP 1062633 A1	27-12-2000
		ES 2214012 T3	01-09-2004
		WO 9949416 A1	30-09-1999
		JP 2002508549 T	19-03-2002
		US 6698662 B1	02-03-2004
FR 2784763 A	21-04-2000	AU 6207799 A	08-05-2000
		CN 1332860 A	23-01-2002
		EP 1121629 A1	08-08-2001
		WO 0023866 A1	27-04-2000
		JP 2002528784 T	03-09-2002