

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 11.12.08.

30 Priorité :

43 Date de mise à la disposition du public de la
demande : 18.06.10 Bulletin 10/24.

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

60 Références à d'autres documents nationaux
apparentés :

71 Demandeur(s) : OBERTHUR TECHNOLOGIES
Société anonyme — FR.

72 Inventeur(s) : JAYET STEPHANE.

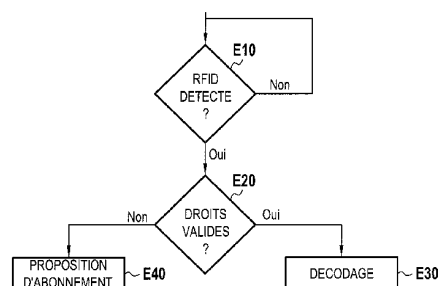
73 Titulaire(s) : OBERTHUR TECHNOLOGIES Société
anonyme.

74 Mandataire(s) : CABINET BEAU DE LOMENIE.

54 PROCÉDE DE PROTECTION D'UNE CLEF USB SECURISEE.

57 Ce procédé de protection d'une clef USB sécurisée
comporte:

- une étape d'obtention d'au moins un paramètre d'usage d'une fonction apte à s'exécuter sur la clef;
- une étape (E20) de détection d'au moins une condition de blocage dépendante de ce paramètre, et, le cas échéant, une première étape (E20) de contrôle apte à empêcher l'exécution de ladite fonction;
- une étape (E10) de détection d'au moins un événement déterminé indépendant de ladite fonction;
- une deuxième étape de contrôle (E10) apte à autoriser l'exécution de la première étape (E20) de contrôle uniquement en cas de détection dudit événement déterminé, cette deuxième étape de contrôle (E10) étant active même lorsque la condition de blocage n'est pas remplie.



Arrière-plan de l'invention

5 L'invention se situe dans le domaine de la protection des clefs USB.

Plus précisément, elle vise à protéger une fonction qui s'exécute sur une clef USB contre une attaque malveillante venant de la station hôte à laquelle la clef est connectée.

10 Dans cette demande de brevet, la fonction protégée peut être de type quelconque. Il peut notamment s'agir d'une fonction d'accès en lecture ou en écriture à une mémoire de masse comprise dans la clef USB, ou d'une fonction d'authentification.

Un type d'attaque pouvant viser les clefs USB est connu de l'homme du métier sous le nom de « déni de service ». D'une façon générale, ces attaques consistent à envoyer des données erronées à la clef USB pour stimuler l'exécution de la fonction embarquée sur la clef dans un but malveillant.

On connaît par exemple, des clefs USB (appelées aussi « dongle » ou verrous matériels) utilisées pour authentifier l'utilisateur d'une application logicielle s'exécutant sur la station hôte à laquelle elle est connectée, et éventuellement bloquer l'exécution de cette application en cas d'échec de l'authentification. L'authentification peut par exemple consister à comparer un code saisi par l'utilisateur au niveau de la station hôte avec une valeur mémorisée par la clef USB. Dans ce premier exemple, une attaque par déni de service peut consister à envoyer des codes erronés successifs à la clef USB, jusqu'à entraîner le blocage de l'application logicielle.

On connaît également des clefs USB aptes à crypter un message reçu de la station hôte en utilisant une clef secrète. Dans ce deuxième exemple, une attaque par déni de service peut consister à envoyer à une clef USB des messages en nombre élevé et/ou en fréquence élevée, à savoir en nombre ou en fréquence supérieur(e) aux conditions d'utilisation normales.

35 Une solution connue sous le nom de « Captcha » pour lutter contre les attaques par déni de service (notamment pour lutter contre les

« spams » ou pourriel) consiste à vérifier que les données envoyées par un ordinateur sont effectivement saisies par un utilisateur humain et non pas générées automatiquement par un robot logiciel s'exécutant sur cet ordinateur.

- 5 Malheureusement, ces solutions ne sont pas parfaites, des robots logiciels de plus en plus perfectionnés réussissent à reconnaître les lettres déformées avec un bon taux de réussite.

Objet et résumé de l'invention

- 10 L'invention concerne une clef USB sécurisée comportant :
- des moyens d'obtention d'au moins un paramètre d'usage d'une fonction apte à s'exécuter sur la clef ;
 - des premiers moyens de contrôle aptes à empêcher l'exécution de ladite fonction sur détection d'au moins une condition de blocage dépendante de
- 15 ce paramètre;
- des deuxièmes moyens de contrôle aptes à activer les premiers moyens de contrôle uniquement sur détection d'au moins un événement déterminé indépendant de la fonction précitée, ces deuxièmes moyens de contrôle étant actifs même lorsque la condition de blocage n'est pas remplie.

- 20 Selon un principe connu, les premiers moyens de contrôle sont aptes à empêcher l'exécution de la fonction sur détection d'une condition de blocage dépendante d'un paramètre d'usage de la fonction.

- Ces moyens peuvent par exemple utiliser une condition de blocage dépendant d'un compteur d'usage, d'une fréquence d'usage, ou
- 25 d'une date d'usage de la fonction.

- Mais dans l'art antérieur, les premiers moyens de contrôle sont toujours actifs, du moins tant que la fonction n'est pas bloquée. Il a été démontré que de tels moyens étaient très fragiles face aux attaques par déni de service.

- 30 Conformément à l'invention, ces premiers moyens de contrôle sont eux-mêmes sous le contrôle de deuxièmes moyens de contrôle mis en œuvre par la clef USB sécurisée elle-même.

- Plus précisément, les deuxièmes moyens de contrôle n'autorisent l'exécution des premiers moyens de contrôle que lorsqu'un
- 35 événement déterminé, indépendant cette fois de la fonction, est détecté.

Dans un mode particulier de réalisation, les deuxièmes moyens de contrôle activent les premiers moyens de contrôle uniquement pendant une durée déterminée comptée à partir de la détection de l'événement déterminé.

5 Dans un mode particulier de réalisation, cette durée est configurable.

Nous allons maintenant donner quatre exemples d'un tel événement :

Selon un premier mode de réalisation, les deuxièmes moyens de
10 contrôle comportent un capteur et sont aptes à activer ou non les premiers moyens de contrôle en fonction de l'état du capteur.

Préférentiellement, le capteur permet de s'assurer que l'utilisateur est physiquement à proximité de la clef USB. Par exemple, le capteur est un bouton-poussoir et les premiers moyens de contrôle ne
15 sont mis en œuvre que lorsqu'un utilisateur presse ce bouton.

Dans un deuxième mode de réalisation de l'invention, la clef USB comporte un afficheur d'un premier message et des moyens pour recevoir un deuxième message émis par la station hôte, les deuxièmes
20 moyens de contrôle étant aptes à comparer ces messages et à activer les premiers moyens de contrôle lorsque ces messages sont identiques.

Dans un troisième mode de réalisation, la clef USB comporte une table associant au moins un premier message à au moins un deuxième message, des moyens de présentation d'un de ces premiers messages à l'utilisateur et des moyens de réception d'un message émis
25 par la station hôte, lesdits deuxièmes moyens de contrôle étant aptes à activer lesdits premiers moyens de contrôle si le message reçu de la station hôte est associé avec le message à la station hôte dans la table.

Typiquement, le premier message peut consister en une question posée à l'utilisateur de la station hôte et les deuxièmes messages
30 des réponses possibles à cette question.

Là encore, l'envoi de réponses erronées par la station hôte n'entraîne pas le blocage de l'application, mais seulement l'inhibition des premiers moyens de contrôle.

Dans un quatrième mode de réalisation, la clef USB comporte
35 des moyens de communication aptes à échanger des informations d'authentification avec un dispositif externe, les deuxièmes moyens de

contrôle activant ou non les premiers moyens de contrôle en fonction de ces informations d'authentification.

Le dispositif externe peut par exemple être constitué par une carte à puce sans contact et les informations d'authentification peuvent être des informations d'authentification de cette carte à puce auprès de la clef USB sécurisée.

L'invention est particulièrement bien adaptée à protéger les clefs USB qui utilisent une valeur secrète protégée par les premiers moyens de contrôle : clef cryptographique, numéro d'identification personnel (code PIN), ...

En effet, si la fonction protégée de la clef USB est une fonction d'authentification par comparaison d'un code PIN, des codes PIN erronés émis par la station hôte seront ignorés à moins qu'un utilisateur ait saisi au niveau de la station hôte, un message affiché sur la clef USB, ce message n'étant pas transmis à la station hôte.

En variante, des informations de contrôle peuvent se limiter à un identifiant du dispositif externe, cet identifiant étant vérifié par les moyens d'inhibition de la clef USB.

Corrélativement, l'invention concerne un procédé de protection d'une clef USB sécurisée comportant :

- une étape d'obtention d'au moins un paramètre d'usage d'une fonction apte à s'exécuter sur la clef ;
- une étape de détection d'au moins une condition de blocage dépendante de ce paramètre, et, le cas échéant, une première étape de contrôle apte à empêcher l'exécution de ladite fonction ;
- une étape de détection d'au moins un événement déterminé indépendant de la fonction ;
- une deuxième étape de contrôle apte à autoriser l'exécution de ladite première étape de contrôle uniquement en cas de détection de l'événement déterminé, cette deuxième étape de contrôle étant active même lorsque la condition de blocage n'est pas remplie.

Conformément à l'invention, la première étape de contrôle est apte à autoriser l'exécution de la fonction seulement lorsque l'événement est détecté et lorsque la condition de blocage n'est pas remplie.

Les avantages et caractéristiques particuliers du procédé de protection sont les mêmes que ceux de la clef USB mentionnés précédemment.

En particulier, l'étape de détection d'au moins un événement déterminé indépendant de ladite fonction peut consister à :

- détecter l'état d'un capteur de ladite clef USB ;
- vérifier qu'un message reçu de la station hôte est identique à un message affiché sur un afficheur de la clef USB;
- vérifier qu'un message reçu de la station hôte est associé, dans une table de la clef USB avec un message présenté à l'utilisateur ;
- vérifier des informations d'authentification échangées avec un dispositif externe.

Dans un mode particulier de réalisation, les différentes étapes du procédé de protection sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans une clef USB sécurisée, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de protection tel que décrit ci-dessus.

Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations lisible par une clef USB, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

5

Brève description des dessins

D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple de réalisation dépourvu de tout caractère limitatif. Sur les figures :

10

- les figures 1 à 4 représentent quatre clefs USB conformes à l'invention dans des modes particuliers de réalisation ; et
- la figure 5 représente, sous forme d'organigramme, les principales étapes d'un procédé de protection conforme à l'invention.

15

Description détaillée de plusieurs modes de réalisation

La **figure 1** représente une clef USB 10 sécurisée conforme à l'invention dans un premier mode de réalisation.

Cette clef USB 10 comporte un processeur 11, une mémoire vive de type RAM 12, une mémoire morte de type ROM 13 et une mémoire non volatile réinscriptible de type flash 16 et des moyens 14 de communication avec une station hôte 100 sur laquelle s'exécute une application logicielle 110.

La mémoire morte 13 constitue un support d'enregistrement conforme à l'invention, sur lequel est enregistré un programme d'ordinateur PG conforme à l'invention, ce programme comportant des instructions pour exécuter les étapes d'un procédé de protection conforme à l'invention, ces étapes étant représentées sous forme d'organigramme à la figure 5 qui sera décrite ultérieurement.

Dans l'exemple de réalisation décrit ici, la clef USB est utilisée comme mémoire de masse externe à la station hôte 100, les accès à cette mémoire étant autorisés uniquement lorsqu'un code saisi au clavier de la station hôte 100 et reçu par les moyens 14 de communication de la clef USB correspond à un code PIN mémorisé dans la mémoire flash 16.

La comparaison d'un code émis par la station hôte avec le code PIN est un premier contrôle au sens de l'invention. Plus précisément, ce

premier contrôle, effectué par exécution du programme d'ordinateur PG comporte les opérations suivantes :

- réception d'un code émis par la station hôte et comparaison avec le code PIN mémorisé dans la mémoire flash 16 ;
- 5 - si le code émis par la station hôte 100 est valide, le processeur 11 retourne à la station hôte un message OK et positionne un drapeau (en anglais « flag ») dans la mémoire flash 16 pour autoriser l'accès à la mémoire de masse ;
- si le code est invalide, le processeur 11 retourne un message
- 10 NG à la station hôte 100 ; et
- si le nombre de codes invalides reçus par la clef USB est supérieur à un nombre déterminé, le processeur 11 positionne un drapeau (en anglais « flag ») dans la mémoire flash 16 pour interdire tout futur accès à la mémoire de masse et toute comparaison d'un code
- 15 éventuellement reçu avec le code PIN.

Conformément à l'invention, la clef USB 10 comporte des deuxièmes moyens de contrôle pour activer ou non les premiers moyens de contrôle.

20 Dans le mode de réalisation de la figure 1, la clef USB comporte à cet effet un bouton-poussoir associé à un capteur 15, la comparaison étant effectuée uniquement lorsqu'un utilisateur presse le bouton-poussoir.

Ainsi, si le bouton-poussoir est relâché, l'envoi de codes invalides par l'application 110 de la station hôte 100 est sans effet.

25 La **figure 2** représente une clef USB conforme à l'invention dans un deuxième mode de réalisation.

Dans ce mode de réalisation, la clef USB 10 comporte une horloge 21 et un afficheur 17 sur lequel peut s'afficher un message MSG1 généré aléatoirement.

30 Cet afficheur invite l'utilisateur à saisir le message MSG1 au clavier de la station hôte et à actionner un bouton logiciel pour que le message saisi soit envoyé à la clef USB.

 Dans ce mode de réalisation de l'invention, le processeur 11 compare le message MSG2 émis par la station hôte 110 avec celui MSG1

35 affiché sur l'afficheur 17 et active, lorsque ces messages sont identiques, la fonction de comparaison d'un code reçu avec le code PIN pendant une

durée T_OUT déterminée mémorisée dans la mémoire non volatile 16, cette durée étant mesurée par l'horloge 21.

La **figure 3** représente un troisième mode de réalisation de l'invention.

5 Dans ce mode de réalisation, la clef USB 10 est une clef apte à crypter un message MSG reçu de la station hôte 100 par ses moyens de communication 14 avec une clef secrète KS mémorisée dans sa mémoire flash 16 et à renvoyer le message crypté MSGK à la station hôte 100.

10 Dans l'exemple de réalisation décrit ici, la clef USB 10 comporte une table 18 dans laquelle des premiers messages M1 (respectivement M2) sont associés à au moins un deuxième message M11, M12 (respectivement M21, M22).

15 Dans ce mode de réalisation, le processeur 11, mettant en œuvre le programme d'ordinateur PG, envoie à la station hôte un message choisi aléatoirement parmi la liste des premiers messages M1, M2 et se place en attente d'une réponse d'un message de réponse émis par la station hôte 100.

20 Dans ce mode de réalisation, la clef USB comporte des premiers moyens de contrôle aptes à mémoriser le nombre NB_USE d'utilisation de la fonction de cryptage et à interdire l'usage de cette fonction si ce nombre dépasse un seuil NB_MAX, ces valeurs étant mémorisées dans la mémoire flash 16.

25 Dans ce mode de réalisation, les premiers moyens de contrôle sont activés si le message M11 émis par la station hôte 100 est associé, dans la table 18, au message M1 émis vers cette station hôte.

La **figure 4**, représente un quatrième mode de réalisation de l'invention.

30 Dans ce mode de réalisation, la clef USB 10 mesure la fréquence FQ_USE d'utilisation de la fonction de cryptage, cette fréquence étant mémorisée dans la mémoire flash 16 et des premiers moyens de contrôle aptes à désactiver la fonction de cryptage si la fréquence d'usage FQ_USE de cette fonction dépasse une valeur seuil.

Dans ce mode de réalisation, la clef USB 10 comporte des moyens de communication avec un dispositif externe 20.

35 Dans le mode de réalisation décrit ici, le dispositif externe 20 est une carte à puce sans contact et les moyens de communication 19 sont

adaptés à communiquer avec cette carte à puce par une communication en champ proche, d'une portée de quelques centimètres, pour s'échanger des informations d'authentification.

5 Dans un mode de réalisation particulier, ces informations sont des informations d'authentification de la carte à puce sans contact 20 auprès de la clef USB 10.

Quoi qu'il en soit, dans ce quatrième mode de réalisation de l'invention, les premiers moyens de contrôle sont activés, pendant une durée T_OUT déterminée mesurée par une horloge 21, si le dispositif 10 externe 20 est effectivement authentifié.

La **figure 5** représente les principales étapes d'un procédé d'authentification conforme à l'invention.

Ce procédé est mis en œuvre par une clef USB 10 telle que décrite précédemment en référence aux figures 1 à 4.

15 Nous supposons dans cet exemple que la clef USB met en œuvre une fonction de décodage de télévision numérique terrestre, cette clef pouvant être connectée à un décodeur numérique relié à un téléviseur.

20 Au cours d'une étape E10, la clef USB 10 vérifie si un événement déterminé indépendant de cette fonction de décodage se produit. Dans l'exemple de réalisation décrit ici, cette étape consiste à authentifier une étiquette électronique RFID incorporée dans le décodeur.

Dans le mode de réalisation décrit ici, le programme de protection boucle sur cette étape E10 si l'événement n'est pas détecté.

25 Si l'événement est détecté, l'étape E10 est suivie par une étape E20 au cours de laquelle la clef USB vérifie si une condition de blocage dépendante d'un paramètre d'usage de la fonction de décodage est remplie. Il peut s'agir par exemple de vérifier, en fonction de la date courante DC, si l'abonnement de l'utilisateur est toujours valable ou s'il a 30 expiré.

Dans le mode de réalisation décrit ici, on décode le programme de télévision numérique si les droits de l'utilisateur sont valables (étape E30) et, on lui propose (étape E40), lorsque la condition de blocage se produit, de renouveler son abonnement en validant une offre proposée à 35 l'écran du téléviseur par le décodeur.

REVENDICATIONS

1. Clef USB sécurisée (10) comportant :
- 5 - des moyens d'obtention d'un moins un paramètre d'usage d'une fonction apte à s'exécuter sur ladite clef (100) ;
- des premiers moyens de contrôle aptes à empêcher l'exécution de ladite fonction sur détection d'au moins une condition de blocage dépendante dudit paramètre ;
- 10 ladite clef étant caractérisée en ce qu'elle comporte :
- des deuxièmes moyens de contrôle aptes à activer lesdits premiers moyens de contrôle uniquement sur détection d'au moins un événement déterminé indépendant de ladite fonction, lesdits deuxièmes moyens de contrôle étant actifs même lorsque ladite condition de blocage n'est pas
- 15 remplie ; et en ce que :
- lesdits premiers moyens de contrôle sont adaptés à autoriser l'exécution de ladite fonction seulement lorsque ledit événement est détecté et lorsque ladite condition de blocage n'est pas remplie.
- 20 2. Clef USB sécurisée (10) selon la revendication 1, dans laquelle ladite fonction utilise une valeur secrète protégée par lesdits premiers moyens de contrôle.
3. Clef USB sécurisée (10) selon la revendication 2, dans
- 25 laquelle ladite valeur secrète est une clef cryptographique.
4. Clef USB sécurisée (10) selon la revendication 2, dans laquelle ladite valeur secrète est un numéro d'identification personnel.
- 30 5. Clef USB sécurisée (10) selon l'une quelconque des revendications 1 à 4, dans laquelle ladite condition de blocage dépend au moins d'une valeur choisie parmi :
- un compteur (NB_USE) d'usage de ladite fonction ;
- une fréquence (FQ_USE) d'usage de ladite fonction ; ou
- 35 - une date (DC) d'usage de ladite fonction.

6. Clef USB selon l'une quelconque des revendications 1 à 5 dans laquelle lesdits deuxièmes moyens de contrôle comportent un capteur (15) et sont aptes à activer ou non lesdits premiers moyens de contrôle en fonction de l'état dudit capteur.

5

7. Clef USB selon l'une quelconque des revendications 1 à 6 comportant un afficheur (17) d'un premier message (MSG1) et des moyens (14) de réception d'un deuxième message (MSG2) émis par ladite station hôte (100), lesdits deuxièmes moyens de contrôle étant aptes à
10 comparer lesdits messages (MSG1, MSG2) et à activer lesdits premiers moyens de contrôle lorsque lesdits messages sont identiques.

8. Clef USB selon l'une quelconque des revendications 1 à 7 comportant une table (18) associant au moins un premier message (M1) à
15 au moins un deuxième message (M11, M12), des moyens de présentation d'un desdits premiers messages (M1) à l'utilisateur et des moyens (14) de réception d'un message (M11) émis par ladite station hôte, lesdits deuxièmes moyens de contrôle étant aptes à activer lesdits premiers moyens de contrôle si le message (M11) reçu de ladite station hôte est
20 associé avec le message (M1) envoyé à la station hôte dans ladite table (18).

9. Clef USB selon l'une quelconque des revendications 1 à 8 comportant des moyens de communication (19) aptes à échanger des
25 informations d'authentification avec un dispositif externe (20), et dans laquelle lesdits deuxièmes moyens de contrôle activent lesdits premiers moyens de contrôle en fonction desdites informations d'authentification.

10. Clef USB selon l'une quelconque des revendications 1 à 9,
30 dans laquelle lesdits deuxièmes moyens de contrôle activent lesdits premiers moyens de contrôle uniquement pendant une durée (T_OUT) déterminée comptée à partir de la détection de l'événement déterminé.

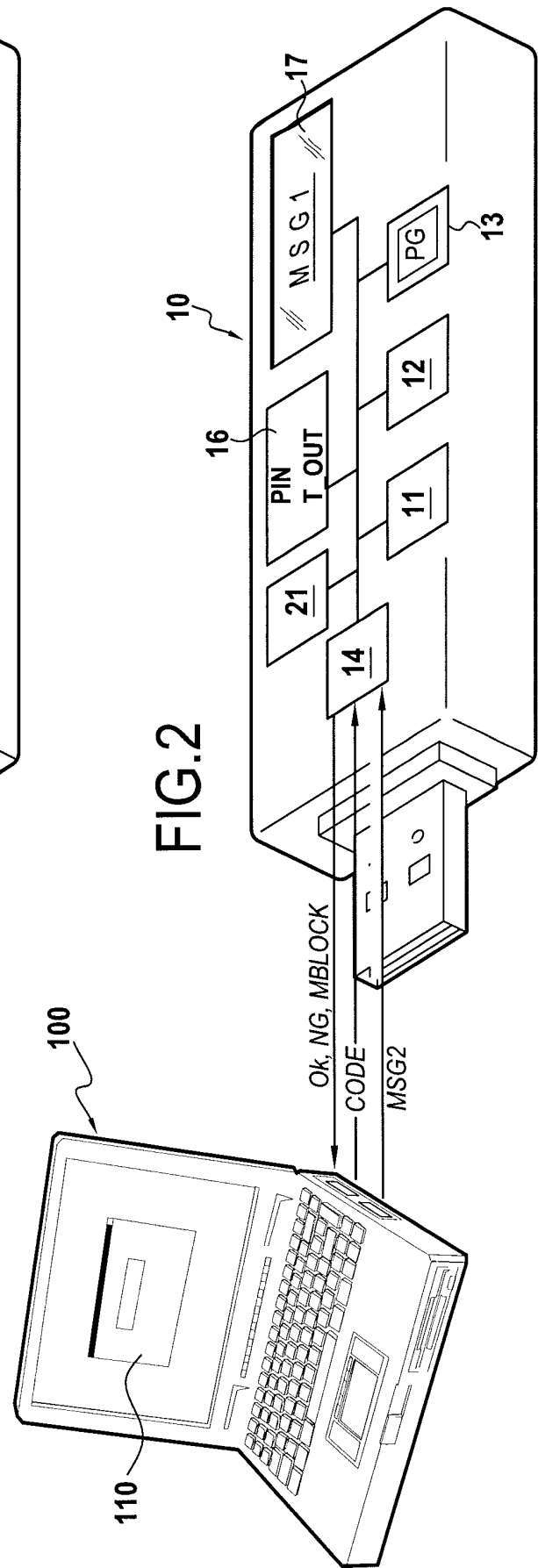
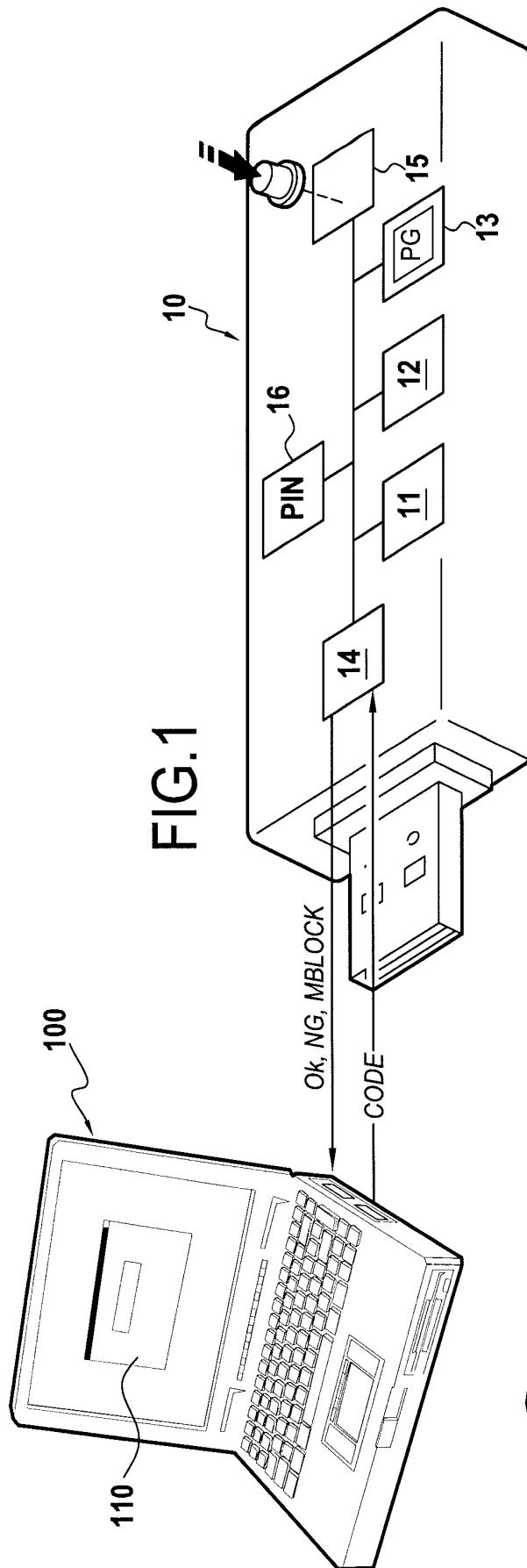
11. Procédé de protection d'une clef USB sécurisée (10)
35 comportant :

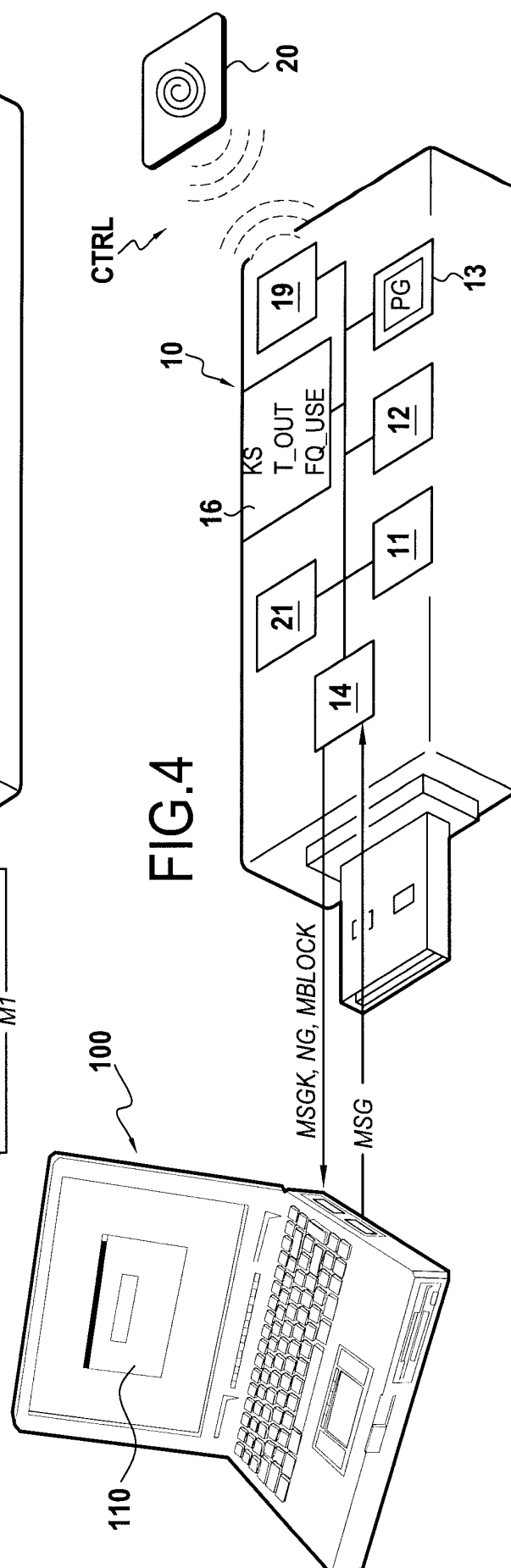
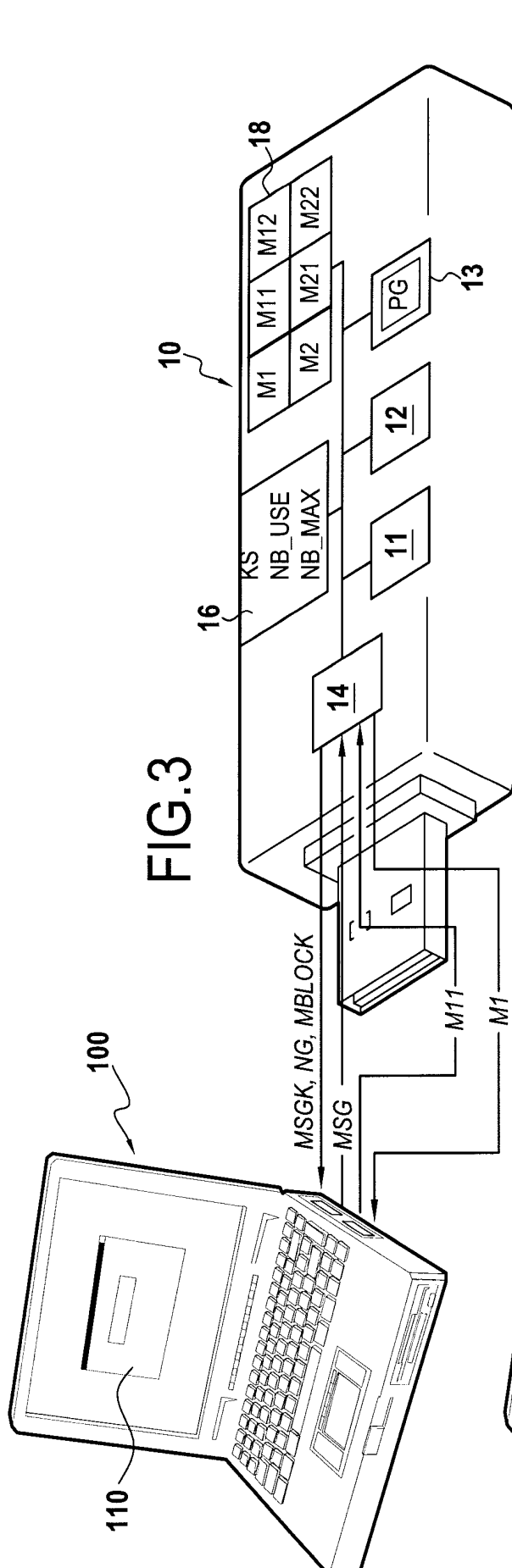
- une étape d'obtention d'au moins un paramètre d'usage d'une fonction apte à s'exécuter sur ladite clef (100) ;
 - une étape de détection d'au moins une condition de blocage dépendante dudit paramètre, et, le cas échéant, une première étape de contrôle apte à empêcher l'exécution de ladite fonction ;
- 5 ledit procédé de protection étant caractérisé en ce qu'il comporte :
- une étape de détection d'au moins un événement déterminé indépendant de ladite fonction ;
 - une deuxième étape de contrôle apte à autoriser l'exécution de ladite première étape de contrôle uniquement en cas de détection dudit événement déterminé, cette deuxième étape de contrôle étant active même lorsque ladite condition de blocage n'est pas remplie ; et en ce que :
- 10
- ladite première étape de contrôle est apte à autoriser l'exécution de ladite fonction seulement lorsque ledit événement est détecté et lorsque ladite condition de blocage n'est pas remplie.
- 15

20 12. Programme d'ordinateur (PG) comportant des instructions pour l'exécution des étapes du procédé de protection d'une clef sécurisée selon la revendication 11 lorsque ledit programme est exécuté par ladite clef USB (10).

25 13. Support d'enregistrement (13) lisible par une clef USB sécurisée (10) sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour l'exécution des étapes du procédé de protection selon la revendication 11.

1/3





3/3

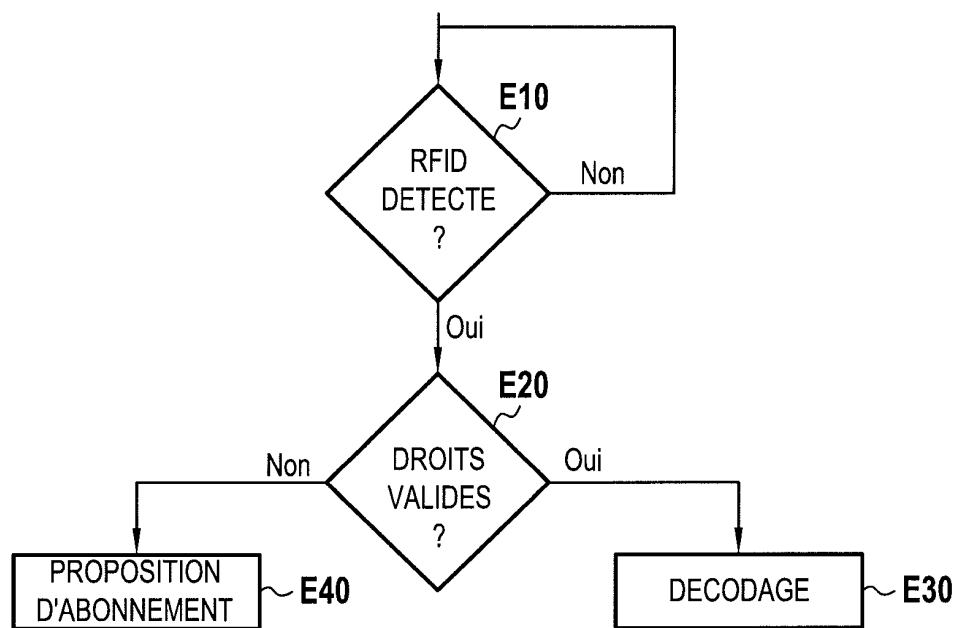


FIG.5



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 718990
FR 0858478

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2008/263364 A1 (DUNDAS ALAN H [US]; LLOYD PAUL C [US]) 23 octobre 2008 (2008-10-23)	1-4,6, 10-13	G06F21/22
Y	* alinéas [0010], [0012], [0015], [0018] - [0021]; figure 3 *	7-9	
Y	WO 2008/024644 A2 (SANDISK CORP [US]; CEDAR YORAM [US]; GONZALEZ CARLOS J [US]) 28 février 2008 (2008-02-28) * page 2, ligne 10 - page 3, ligne 10 *	7	
Y	SMITH S L: "AUTHENTICATING USERS BY WORD ASSOCIATION" COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 6, no. 6, 1 décembre 1987 (1987-12-01), pages 464-470, XP000050578 ISSN: 0167-4048 * section 4 *	8	
Y	US 2006/208853 A1 (KUNG SHAO-TSU [TW]; SHEN YI-HUNG [TW]) 21 septembre 2006 (2006-09-21) * alinéas [0007] - [0011] *	9	DOMAINES TECHNIQUES RECHERCHÉS (IPC)
Y	US 2007/120643 A1 (LEE JIUNN-CHUNG [TW]) 31 mai 2007 (2007-05-31) * abrégé * * alinéas [0018] - [0021] *	9	G06F H04L G07F
A	FR 2 910 666 A1 (OBERTHUR CARD SYST SA [FR]) 27 juin 2008 (2008-06-27) * le document en entier *	1-13	
Date d'achèvement de la recherche		Examineur	
1 septembre 2009		Veillas, Erik	
CATÉGORIE DES DOCUMENTS CITÉS		T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire			

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0858478 FA 718990**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **01-09-2009**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2008263364 A1	23-10-2008	AUCUN	

WO 2008024644 A2	28-02-2008	AUCUN	

US 2006208853 A1	21-09-2006	TW 259404 B	01-08-2006

US 2007120643 A1	31-05-2007	AUCUN	

FR 2910666 A1	27-06-2008	WO 2008096078 A2	14-08-2008
