(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 071 641**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **17 59002**

(51) Int Cl[8] : ***G 06 F 8/71*** *(2018.01), G 06 F 21/57, G 06 K 19/067*

(12) BREVET D'INVENTION B1

(54) PROCEDE DE CONFIGURATION D'UN ELEMENT SECURISE TEL QU'UNE CARTE ELECTRONIQUE.

(22) **Date de dépôt :** 28.09.17.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 29.03.19 Bulletin 19/13.

(45) **Date de la mise à disposition du public du brevet d'invention :** 27.09.19 Bulletin 19/39.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

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

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *IDEMIA IDENTITY & SECURITY FRANCE Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** GESLAIN RAPHAEL, PEPIN CYRILLE et FROMAGER SYLVAIN, JEROME.

(73) **Titulaire(s) :** IDEMIA IDENTITY & SECURITY FRANCE Société par actions simplifiée.

(74) **Mandataire(s) :** REGIMBEAU.

FR 3 071 641 - B1

DOMAINE TECHNIQUE GENERAL

La présente invention concerne le domaine des éléments sécurisés tels que les cartes à puce. Et l'invention concerne plus particulièrement la configuration d'une application stockée sur un élément sécurisé.

ETAT DE LA TECHNIQUE

Un élément sécurisé (en anglais « *Secure Element* », (SE)) comprend classiquement un processeur configuré pour exécuter un système d'exploitation et un ou plusieurs programmes applicatifs (appelée applications) qui coopèrent avec le système d'exploitation.

L'élément sécurisé comprend une mémoire à laquelle le processeur a accès.

Pour chaque application, sont mémorisées dans la mémoire le programme lui-même (sous forme de code compilé ou interprété) et d'autre part des données écrites et/ou lues dans la mémoire par le programme au cours de son exécution par le processeur.

Ces données sont, notamment des données de personnalisation ou configuration associées à l'utilisation de l'élément sécurisé. Par exemple, dans le cas d'une carte bancaire une donnée de personnalisation peut être un plafond de paiement.

Habituellement un industriel développe l'élément sécurisé avec une ou plusieurs applications qui correspondent à l'utilisation finale proposée par un fournisseur de service à ses clients. Ces applications ont des spécifications qui sont, par exemple, issues d'un éditeur. Parfois, les spécifications sont directement fournies par l'industriel (on parle alors d'application propriétaire). L'industriel développe par exemple des cartes bancaires à destination d'une enseigne bancaire qui procède à la personnalisation des applications en fonction de l'utilisation finale pour ses clients.

Aussi, pour ce faire, le fournisseur de services dispose d'outils de personnalisation qui permettent de personnaliser une ou plusieurs application(s) à un instant donné.

Un problème survient lorsque l'éditeur fait évoluer les applications (aussi bien pour les applications que pour la personnalisation de ces applications). Le fournisseur dispose alors d'éléments sécurisés avec les différentes évolutions mais n'a pas forcément les outils de personnalisation en phase avec les évolutions.

PRESENTATION DE L'INVENTION

Un but de l'invention est d'avoir un élément sécurisé sur lequel sont stockées plusieurs programmes différents lesquels sont configurables à partir de données de configuration et ce quelle que soit la version du programme.

L'invention propose de pallier au moins un de ces inconvénients.

A cet effet, l'invention propose un procédé de configuration d'un programme destiné à être exécuté par un élément sécurisé, le procédé comprenant des étapes mises en œuvre dans l'élément sécurisé :

- réception par un élément sécurisé de données de configuration d'un programme, lesdites données comprenant une version d'un programme ;
- comparaison d'une version du programme à configurer avec la version indiquée dans les données de configuration reçues, et si les versions comparées sont différentes ;
- traitement des données de configuration reçues afin qu'elles soient compatibles avec la version du programme à configurer.

L'invention est avantageusement complétée par les caractéristiques suivantes, prises seules ou en une quelconque de leur combinaison techniquement possible :

- l'étape de traitement (300) comprend la sous-étape d'extraction (301), parmi les données de configuration reçues lesquelles sont indépendantes des versions ;
- l'étape de traitement (300) comprend les sous-étapes de : extraction (302), parmi les données de configuration lesquelles sont utilisées dans les deux versions mais de différentes manières fonctions de chacune des versions ; modification (303) des données de configuration afin que des données extraites fonctionnent avec le programme à configurer ;
- l'étape de traitement (300) comprend les sous-étapes de : extraction (304), parmi les données de configuration lesquelles sont utilisées selon plusieurs types d'utilisation dans le programme à configurer ; duplication (305) des données de configuration extraites ;
- l'étape de traitement (300) comprend les sous-étapes de : extraction (306), parmi les données de configuration lesquelles ne sont pas utilisées par le programme à configurer ; suppression (307) des données ainsi extraites ;
- l'étape de traitement (300) comprend les sous-étapes de : vérification (308) que les données de configuration attendues par le programme à configurer sont

présentes dans les données reçues, et si des données de configuration attendues ne sont pas présentes dans les données de configuration reçues ; création (309) de données de configuration ayant une valeur par défaut ;

- le procédé comprend une étape (400) de stockage des données traitées au sein de l'élément sécurisé.

L'invention concerne également un produit programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes du procédé selon l'invention, lorsque ce programme est exécuté par un processeur (2).

L'invention concerne aussi un élément sécurisé de type carte électronique comprenant : au moins un processeur (2) ; une mémoire (3) configurée pour stockée un programme ayant une version donnée et des données de configurations dudit programme ; la carte électronique étant caractérisée en ce que le processeur est configuré pour mettre en œuvre un procédé selon l'invention.

De manière complémentaire, la mémoire de l'élément sécurisé est de type flash.

Les avantages de l'invention sont multiples.

L'invention permet la modification de données de personnalisation à la volée afin :

- De conserver les mécanismes de personnalisation d'une application à l'autre,
- De rendre la mise sur le marché de certains produits plus rapide.

Ainsi, un industriel développant des éléments sécurités peut proposer à ses clients (fournisseurs de services) des solutions embarquant plusieurs applications différentes, et propose à ses clients la possibilité de pouvoir conserver leurs fichiers de configuration et de personnalisation d'une application à l'autre, même lorsque les normes applicatives sont amenées à être modifiées.

L'invention permet de configurer l'élément sécurisé contenant certaines applications avec des données d'une autre application.

L'invention permet également une mise sur le marché plus rapide de l'élément sécurisé embarquant des applications différentes de celles utilisées habituellement. En effet, le fournisseur de service peut conserver son écosystème de configuration malgré les nouvelles applications présentes, et effectuer la migration de son système de configuration à son propre rythme.

PRESENTATION DES FIGURES

D'autres caractéristiques, buts et avantages de l'invention ressortiront de la description qui suit, qui est purement illustrative et non limitative, et qui doit être lue en regard des dessins annexés sur lesquels :

- la figure 1 illustre schématiquement un élément sécurisé selon un mode de réalisation de l'invention ;

- la figure 2 illustre un organigramme d'étapes d'un procédé de configuration d'un élément sécurisé selon un mode de réalisation de l'invention.

Sur l'ensemble des figures les éléments similaires portent des références identiques.

DESCRIPTION DETAILLEE DE L'INVENTION

En référence à la **figure 1**, un élément sécurisé 1 comprend une mémoire 3 au moins un processeur 2 et une interface 4 de communication.

Un élément sécurisé 1 est par exemple une carte bancaire d'un utilisateur, un téléphone mobile ou tout élément possédant un tel élément sécurisé.

La mémoire 3 est par exemple une unité mémoire de type « flash ».

Le processeur 2 est adapté pour exécuter des instructions de code de programmes et notamment accéder en lecture et en écriture au contenu de la mémoire.

L'élément sécurisé 1 est muni d'un système d'exploitation dont l'exécution est effectuée par le processeur 2. Un tel système d'exploitation est un programme central qui contrôle l'installation, la configuration, l'exécution de programmes applicatifs ou applications.

L'interface 4 de communication est connectée au processeur 2 qui est configuré pour traiter des données reçues par l'interface.

L'interface 4 de communication est configurée pour coopérer avec une interface de communication d'un terminal 5, par exemple, une borne de transaction bancaire ou, en particulier, un terminal de configuration de l'élément sécurisé 1.

En outre, le processeur 2 est configuré pour mettre en œuvre un procédé de configuration d'un programme applicatif destiné à être exécuté par l'élément sécurisé et décrit, ci-dessous, en relation avec la **figure 2**.

Dans un état initial, un programme applicatif (ou plus simplement programme dans la suite de la description) est stocké dans la mémoire de l'élément sécurisé. Ce

programme est identifié par une version de programme afin d'identifier les évolutions du programme.

Le programme est configurable au moyen de données de configuration.

Ces données ont un certain contenu selon un certain format qui dépend de la version du programme. Ainsi, les données de configuration comprennent, notamment, la version du programme. De manière plus générale, ces données de configuration comprennent des données qui permettent à une application de fonctionner correctement une fois l'élément sécurisé dans la main de son utilisateur final.

Afin de simplifier la description ci-dessous, on considère qu'un programme ayant une version X est stocké dans la mémoire du programme et que les données de configuration qui correspondent à cette version X sont notées DX et que les données de configuration qui correspondent à la version Y du programme sont notées DY.

Dans une étape 100, l'élément sécurisé reçoit des données de configuration d'un programme.

De préférence, c'est par un terminal 5 de configuration en liaison avec l'interface 4 de communication de l'élément sécurisé 1 que l'élément sécurisé 1 reçoit les données de configuration.

Dans une étape 200, la version du programme à configurer est comparée à la version indiquée dans les données de configuration reçues.

Si les versions sont identiques (données DY reçues, programme de version Y stocké), alors les données de configuration sont stockées dans la mémoire et seront utilisées par le programme au cours de son exécution. Les données sont stockées telles quelles et ce cas-là ne sera pas plus détaillé dans la description.

Dans une étape 300, si les versions sont différentes (données DY reçues, programme de version X stocké), les données de configuration reçues sont traitées afin qu'elles soient compatibles avec la version du programme à configurer. C'est-à-dire afin qu'elles soient interprétables et utilisables.

Ce sont alors les données ainsi traitées qui, dans une étape 400, sont stockées dans la mémoire et qui seront utilisées par le programme au cours de son exécution.

On précise que l'étape de traitement 300 est faite à la volée lorsque les données de configuration sont envoyées à l'élément sécurisé.

L'étape 300 de traitement des données de configuration comprend plusieurs types de fonctionnements fonction du type de données comprises dans les données de configuration.

On décrit ci-dessous plusieurs variantes de l'étape 300 de traitement. Chacune de ces variantes peut être appelée à la volée et l'ordre de présentation de ces dernières n'est en aucun limitatif.

Variante 1

Dans une sous-étape 301, les données de configuration qui sont indépendantes des versions du programme sont extraites.

Ces données sont utilisées de la même manière par le programme à configurer et par les données de configuration qui peuvent correspondre à une version différente de celle du programme à configurer. Ces données seront directement stockées dans la mémoire sans traitement spécifique puisqu'il n'y a pas besoin de les modifier.

Variante 2

Dans une sous-étape 302, les données de configuration reçues DY qui sont utilisées à la fois par le programme à configurer de version X et par le programme de version Y qui correspond aux données reçues DY sont extraites.

Dans une étape 303 ces données sont modifiées afin qu'elles puissent fonctionner avec le programme à configurer de version X.

Variante 3

Dans une sous-étape 304, les données de configuration reçues DY qui existent dans le programme de version Y et qui ont été dupliquées suivant plusieurs types d'utilisations différentes dans le programme de version X sont extraites et dans une sous-étape 305 sont dupliquées autant de fois que nécessaire.

Variante 4

Dans une sous-étape 306, les données de configuration reçues DY qui ne sont pas utilisées par le programme à configurer de version X sont extraites et dans une sous-étape 307 sont supprimées des données de configuration.

Variante 5

Dans une sous-étape 308, on vérifie que toutes les données attendues par le programme à configurer sont présentes dans les données de configuration reçues.

Si des données sont attendues par le programme à configurer mais qu'elles ne sont pas dans les données de configuration alors dans une sous-étape 309 des

données supplémentaires sont créés au sein de l'élément sécurisé avec une valeur par défaut et directement stockées dans une sous-étape 310 puisque ces données ne seront jamais envoyées à l'élément sécurisé au cours de la configuration.

5

REVENDICATIONS

1. Procédé de configuration d'un programme destiné à être exécuté par un élément sécurisé, le procédé comprenant des étapes mises en œuvre dans l'élément sécurisé :

- réception (100) par un élément sécurisé de données de configuration d'un programme, lesdites données comprenant une version d'un programme ;

- comparaison (200) d'une version du programme à configurer avec la version indiquée dans les données de configuration reçues, et si les versions comparées sont différentes ;

- traitement (300) des données de configuration reçues afin qu'elles soient compatibles avec la version du programme à configurer.

2. Procédé selon la revendication 1, dans lequel l'étape de traitement (300) comprend la sous-étape de :

- extraction (301), parmi les données de configuration reçues lesquelles sont indépendantes des versions.

3. Procédé selon l'une des revendications précédentes, dans lequel l'étape de traitement (300) comprend les sous-étapes de

- extraction (302), parmi les données de configuration lesquelles sont utilisées dans les deux versions mais de différentes manières fonctions de chacune des versions ;

- modification (303) des données de configuration afin que des données extraites fonctionnent avec le programme à configurer

4. Procédé selon l'une des revendications précédentes, dans lequel l'étape de traitement (300) comprend les sous-étapes de

- extraction (304), parmi les données de configuration lesquelles sont utilisées selon plusieurs types d'utilisation dans le programme à configurer ;

- duplication (305) des données de configuration extraites.

5. Procédé selon l'une des revendications précédentes, dans lequel l'étape de traitement (300) comprend les sous-étapes de

- extraction (306), parmi les données de configuration lesquelles ne sont pas utilisées par le programme à configurer ;

- suppression (307) des données ainsi extraites.

6. Procédé selon l'une des revendications précédentes, dans lequel l'étape de traitement (300) comprend les sous-étapes de

- vérification (308) que les données de configuration attendues par le programme à configurer sont présentes dans les données reçues, et si des données de configuration attendues ne sont pas présentes dans les données de configuration reçues ;

- création (309) de données de configuration ayant une valeur par défaut.

7. Procédé selon l'une des revendications précédentes, comprenant une étape (400) de stockage des données traitées au sein de l'élément sécurisé.

8. Produit programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes du procédé selon l'une des revendications précédentes, lorsque ce programme est exécuté par un processeur (2).

9. Elément sécurisé de type carte électronique comprenant

- au moins un processeur (2) ;
- une mémoire (3) configurée pour stockée un programme ayant une version donnée et des données de configurations dudit programme ;

la carte électronique étant caractérisée en ce que le processeur est configuré pour mettre en œuvre un procédé selon l'une des revendications 1 à 7.

10. Elément sécurisé selon la revendication 9, dans lequel la mémoire est de type flash.

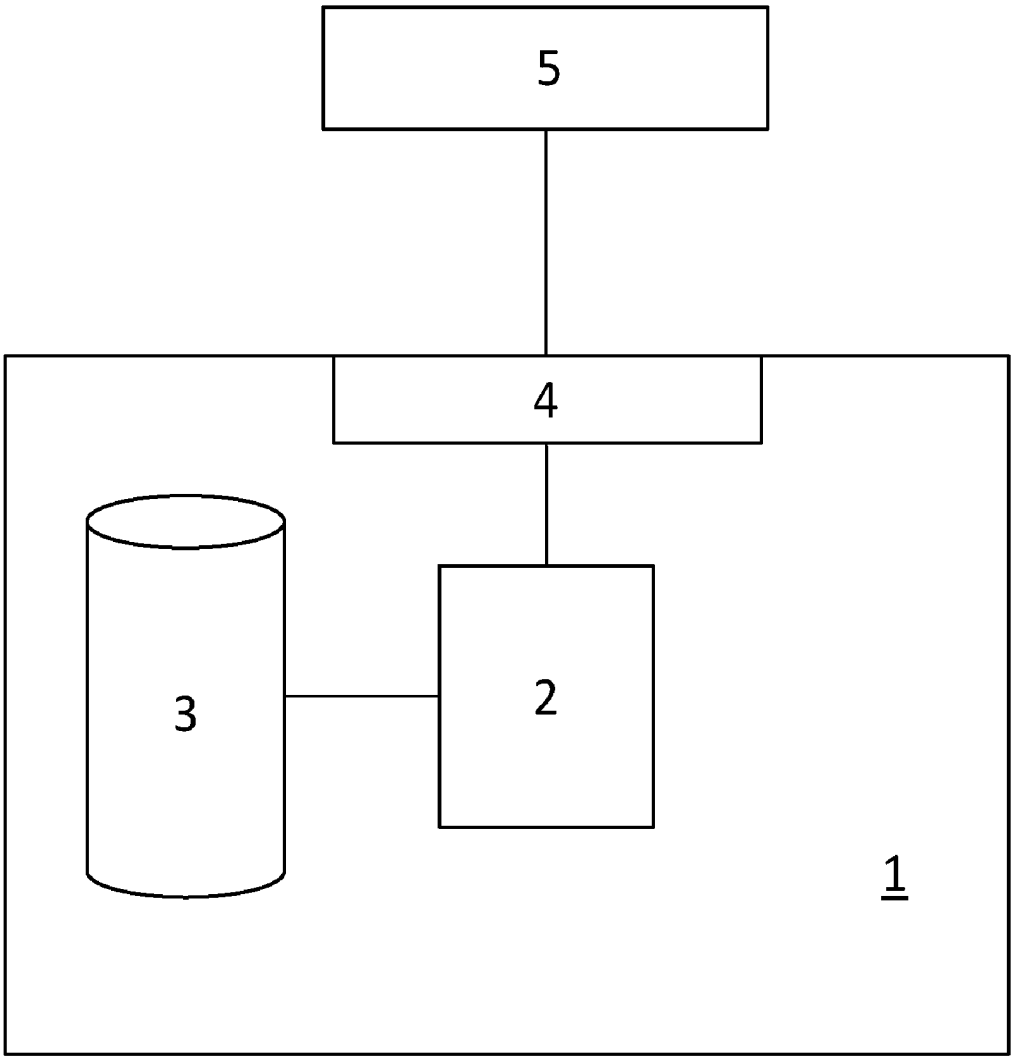

Fig. 1

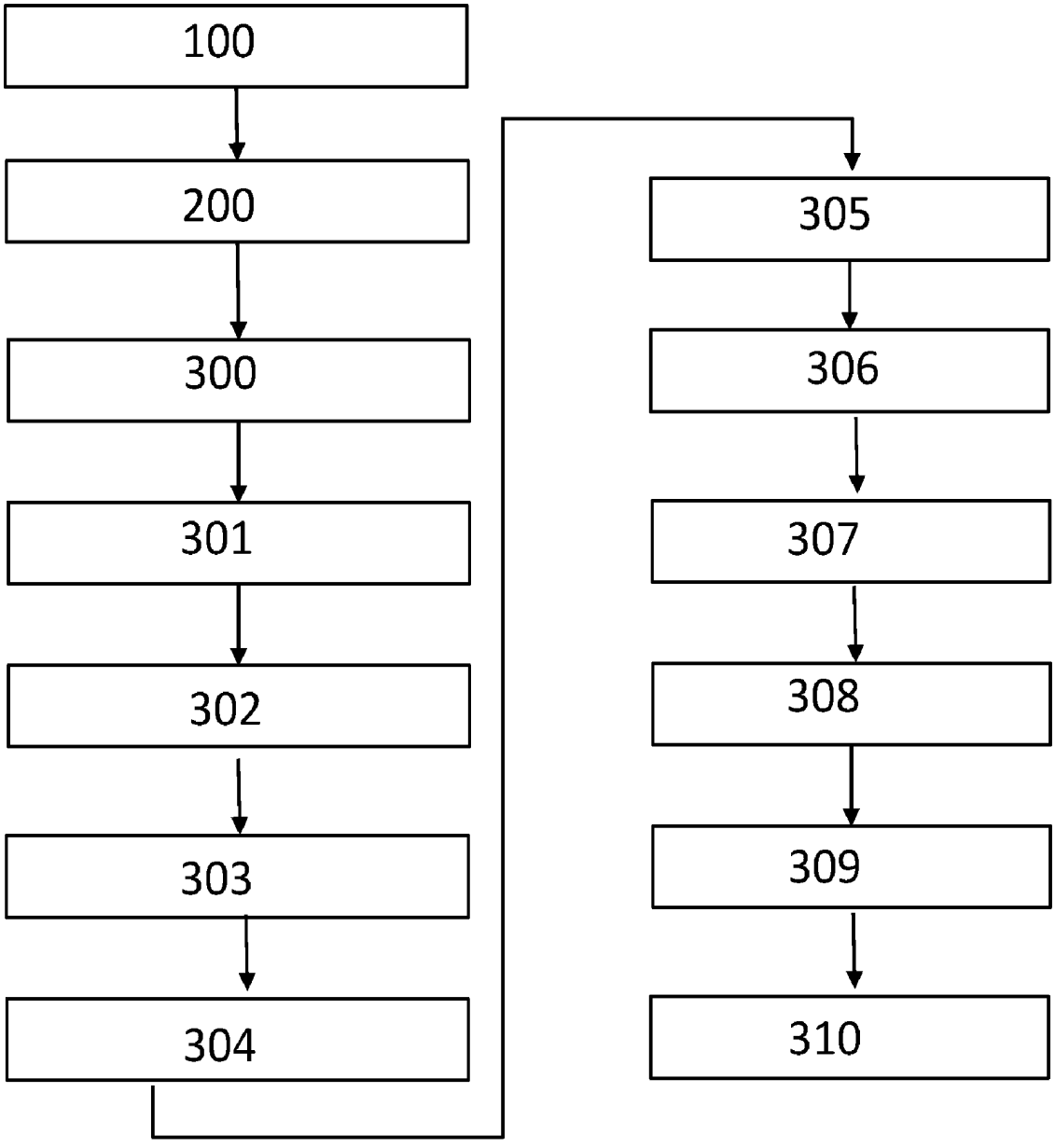

Fig. 2

RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

[x] Le demandeur a maintenu les revendications.

☐ Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

[x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

☐ Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION
WO 2010/141922 A1 (ABBOTT DIABETES CARE INC [US]; NEKOOMARAM SAEED [US]; CROUTHER NATHAN) 9 décembre 2010 (2010-12-09) CN 102 707 964 A (SHENZHEN JIAXINJIE ELECTRON CO LTD) 3 octobre 2012 (2012-10-03)
2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL
NEANT
3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES
NEANT