(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 081 663**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **18 54322**

(51) Int Cl[8] : ***H 04 W 12/08*** *(2018.01), E 05 B 47/00, G 06 F 21/33, G 07 C 9/00, H 04 L 9/28, H 04 W 12/04*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 23.05.18.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 29.11.19 Bulletin 19/48.

(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 :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *ORANGE Société anonyme* — FR.

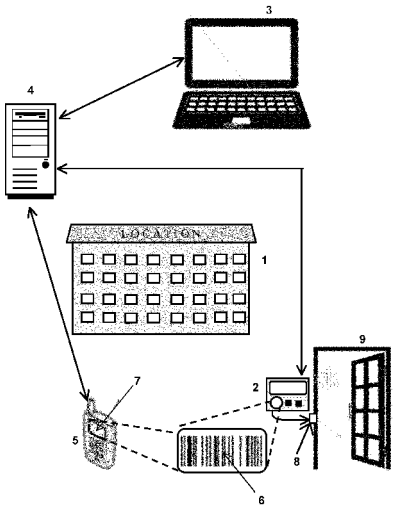
(72) **Inventeur(s) :** GRIMAULT JEAN-LUC et BOUDIER VINCENT.

(73) **Titulaire(s) :** ORANGE Société anonyme.

(74) **Mandataire(s) :** CABINET PATRICE VIDON.

(54) PROCEDE DE GESTION A DISTANCE DE L'OUVERTURE D'UNE SERRURE ELECTRONIQUE DOTEE D'UNE INTERFACE UTILISATEUR, TERMINAL, SERRURE ET PROGRAMME D'ORDINATEUR ASSOCIES.

(57) L'invention concerne un procédé de gestion à distance de l'ouverture d'une serrure électronique (2) commandant l'accès à un local, à l'aide d'un serveur distant (4) communiquant avec un terminal portable (5). Dans un premier temps, la serrure électronique et le serveur distant s'échangent une clé secrète (3.3). Puis, un utilisateur se présente devant le local et introduit une commande sur l'interface utilisateur (24) de la serrure pour demander l'accès (3.6), déclenchant la présentation d'un premier code déterminé et son enregistrement dans le terminal portable. Une requête contenant le premier code est transmis par le terminal portable vers le serveur distant en vue de déclencher l'ouverture de la serrure (3.9). Le serveur distant génère un certificat par le chiffrement du premier code en utilisant la clé secrète (3.10), et le transmet au terminal portable où il est affiché de façon à être introduit au niveau de la serrure (3.12). La serrure (2) calcule son propre certificat et le compare avec celui que lui transmet l'utilisateur (3.14). La serrure est ouverte lorsque les valeurs des deux certificats sont identiques. Le certificat est alors enregistré dans une mémoire de la serrure pour accorder de nouveau l'accès au local lorsqu'il est de nouveau présenté.



FR 3 081 663 - A1

Procédé de gestion à distance de l'ouverture d'une serrure électronique dotée d'une interface utilisateur, terminal, serrure et programme d'ordinateur associés.

1. Domaine de l'invention

L'invention concerne le domaine du contrôle à distance d'une serrure électronique commandant l'accès à un lieu en utilisant un code présenté par un terminal portable. L'invention s'applique plus particulièrement lorsque la serrure électronique dispose de moyens cryptographiques et d'un moyen limité de communication avec un réseau.

2. Art antérieur

De nos jours, il existe de nombreuses manières de contrôler l'entrée dans un lieu sécurisé ou un local dont l'accès est conditionné par un paiement. Ces locaux sont par exemple, un gîte de vacances, une chambre d'hôtel, une maison particulière, etc. L'accès à de tels locaux est accordé si l'utilisateur dispose d'un moyen d'accès matériel ou immatériel. Dans la catégorie des moyens d'accès immatériel, on trouve le code secret que l'utilisateur introduit sur le clavier numérique d'un digicode par exemple. La valeur introduite est comparée au sein d'une serrure électronique à une donnée de référence enregistrée dans une mémoire et en cas d'égalité, l'accès est accordé. Ce type d'accès présente l'autre inconvénient d'être basé sur un code secret mémorisé en dur dans la serrure électronique : si ce code est découvert, n'importe qui peut pénétrer dans le local. De plus, la sécurité impose de changer de code pour chaque nouvel arrivant dans le local, ce qui oblige le propriétaire ou l'administrateur à le changer localement au niveau de la serrure, ce qui peut être contraignant.

Il est également possible d'accéder à un local en présentant une caractéristique physique de la personne autorisée, on parle alors d'identification biométrique. Dans ce mode de réalisation, la donnée particulière permettant d'accorder l'accès dépend de chaque personne autorisée à pénétrer dans le local. Ce mode d'accès nécessite des moyens de reconnaissance biométrique, une plus grande puissance de calcul et une mémoire de taille plus importante.

Selon un autre mode de réalisation, l'accès à un local est autorisé en utilisant les services d'un serveur connecté à la serrure électronique par un réseau informatique. Un utilisateur désireux d'entrer dans le local se connecte préalablement à ce serveur et

introduit un identifiant du local ou de la serrure à ouvrir. Après le paiement éventuel des droits d'accès, le serveur communique l'identifiant de l'utilisateur ou un code d'accès à la serrure qui l'enregistre dans sa mémoire. Ensuite, lorsque l'utilisateur se présente physiquement devant la porte du local, il s'identifie en introduisant une valeur sur un clavier et la serrure électronique vérifie que cet identifiant ou ce code est bien enregistré dans sa mémoire et donc que cet utilisateur est autorisé à pénétrer dans le local.

Ce mode de réalisation permet de personnaliser les codes d'accès en fonction des utilisateurs et accroît la sécurité du système. Il nécessite cependant une liaison informatique entre la serrure et le serveur distant, ce qui complexifie les équipements et les rendent plus coûteux.

On constate donc que les techniques connues permettant d'accorder l'accès à des locaux sont mal adaptées lorsqu'un niveau important de sécurité est requis et que la serrure électronique contrôlant l'accès à ces locaux ne dispose pas de moyens de communication avec un réseau, ou que ceux-ci ont des capacités limitées. Il existe donc un besoin pour une nouvelle solution permettant de commander une serrure électronique ne présentant pas ces inconvénients de l'art antérieur.

4. Exposé de l'invention

Un objet de la présente invention est de proposer une solution pour gérer à distance le fonctionnement d'une serrure électronique.

Pour cela, il est proposé un procédé de gestion à distance de l'ouverture d'une serrure électronique commandant l'accès à un local et dotée d'une interface utilisateur, ledit procédé comportant notamment les étapes suivantes mises en œuvre au niveau de la serrure électronique :

- échange entre la serrure électronique et un serveur distant d'une clé secrète associée à l'accès dudit local,

- acquisition d'une commande sur l'interface utilisateur de la serrure électronique pour demander l'accès au local, l'acquisition de ladite commande déclenchant la génération d'un premier code,

- affichage sur l'interface utilisateur de la serrure électronique dudit premier code,

- fourniture à la serrure électronique par son interface utilisateur de la serrure électronique d'un certificat, ledit certificat étant calculé par le serveur distant par le

chiffrement du premier code en utilisant la clé secrète,

- calcul du certificat par la serrure électronique en utilisant le premier code et sa propre clé secrète,

- ouverture de la serrure électronique lorsque les valeurs des deux certificats sont identiques.

De cette manière, la transmission du code ne nécessite pas de liaison entre la serrure et un serveur, de plus, il est ainsi possible d'accorder l'accès au local sans intervention humaine que celle de l'occupant du lieu.

Selon un mode particulier de réalisation, le procédé comporte une étape d'incorporation dans le calcul du certificat en plus du premier code, d'une valeur représentative de la durée d'accès, et une étape de réception par l'interface utilisateur de ladite valeur en clair, la première égalité entre la valeur du certificat reçu par l'interface utilisateur et la valeur du certificat calculée par la serrure électronique déclenchant la mise en marche d'une horloge incorporée dans la serrure électronique pour décompter ladite durée d'accès, une nouvelle fourniture du certificat après l'expiration de la durée d'accès ne déclenchant pas l'ouverture de la serrure électronique.

Selon un mode particulier de réalisation, le procédé comporte une étape d'incorporation dans le calcul du certificat en plus du premier code, d'une valeur représentative d'au moins un moment au cours duquel l'accès au local est autorisé, et une étape de réception par l'interface utilisateur de la serrure électronique dudit moment, la serrure électronique disposant d'une horloge, l'accès au local étant accordé en fournissant le certificat à la serrure lorsqu'au moins un des moments spécifiés correspond au moment courant indiqué par l'horloge.

Selon un mode particulier de réalisation, le procédé comporte une étape d'incorporation dans le calcul du certificat en plus du premier code, d'une valeur représentative d'au moins une fenêtre périodique au cours de laquelle l'accès au local est autorisé, et une étape de réception d'au moins une fenêtre périodique par l'interface utilisateur de la serrure électronique, la serrure électronique disposant d'une horloge, l'accès au local étant accordé en fournissant le certificat à la serrure lorsque le moment courant indiqué par l'horloge se situe pendant au moins une des fenêtres périodiques spécifiées.

Selon un mode particulier de réalisation, le procédé comporte une étape de réduction de la taille des données après le calcul du certificat exécutée par la serrure électronique avant la comparaison des deux certificats.

Selon un mode particulier de réalisation, les calculs de certificats s'effectuent à l'aide d'une clé cryptographique symétrique.

Selon un mode particulier de réalisation, le procédé comporte une étape de génération de la valeur de clé secrète dans la serrure électronique, et une étape de transmission de ladite valeur au serveur distant.

Selon un mode particulier de réalisation, le procédé comporte une étape d'enregistrement du certificat dans la mémoire de la serrure électronique pour accorder de nouveau l'accès au local lors d'une nouvelle fourniture de ce certificat.

Selon un mode particulier de réalisation, la réception consécutive d'un nombre déterminé de valeurs erronées de certificats déclenchent l'effacement du certificat de la mémoire et un état de blocage qui s'interrompt lors d'une nouvelle étape d'acquisition d'une commande sur l'interface utilisateur de la serrure électronique et d'une nouvelle réception par l'interface utilisateur d'un certificat dont la valeur est égale à celle calculée par la serrure électronique en utilisant le premier code et sa propre clé secrète.

Selon un mode particulier de réalisation, l'acquisition consécutive d'un nombre déterminé de commandes d'accès du fait de la réception consécutive d'un nombre déterminé de valeurs erronées de certificats déclenchent l'effacement du certificat de la mémoire et un état de blocage provoquant la mise en marche d'une horloge incorporée dans la serrure électronique pour décompter une durée déterminée au cours de laquelle toute nouvelle acquisition de commande d'accès aboutit à un échec.

Selon un autre aspect, il est proposé un procédé de gestion à distance de l'ouverture d'une serrure électronique commandant l'accès à un local à l'aide d'un certificat calculé par un serveur distant en utilisant une clé secrète connue de la serrure électronique et dudit serveur distant, ledit procédé comportant notamment les étapes suivantes mises en œuvre au niveau d'un terminal :

- acquisition d'un premier code fourni par ladite serrure électronique,
- transmission vers le serveur distant du premier code,

- réception en provenance du serveur distant d'un certificat calculé par le serveur distant par le chiffrement du premier code en utilisant la clé secrète,

- fourniture du certificat reçu du serveur distant pour être fourni à la serrure électronique afin d'ouvrir la serrure en cas d'égalité entre le certificat reçu du serveur et un certificat calculé par la serrure électronique en utilisant le premier code et sa propre clé secrète.

Selon un autre aspect, il est également proposé une serrure électronique commandant l'accès à un local et dotée d'une interface utilisateur et d'une mémoire contenant au moins une clé secrète dont la valeur est partagée avec un serveur distant, la serrure électronique étant également dotée d'un moyen de génération d'un premier code déclenché par l'acquisition sur l'interface utilisateur d'une commande pour demander l'accès au local et présenté sur l'interface utilisateur pour être transmise au serveur distant, d'un moyen de calcul d'un certificat utilisant ledit premier code et la clé secrète, d'un moyen de réception d'un certificat calculé par le serveur distant par le chiffrement du premier code en utilisant la clé secrète, et d'un moyen de comparaison entre les deux valeurs de certificats reçues et calculées en interne, la serrure électronique déclenchant en cas d'égalité l'ouverture d'un verrou donnant l'accès au local.

Selon un autre aspect, il est également proposé un terminal portable destiné à permettre l'ouverture d'une serrure électronique commandant l'accès à un local en utilisant un certificat calculé par un serveur distant en utilisant une clé secrète connue de la serrure électronique et dudit serveur distant, ledit terminal portable comportant un moyen d'acquisition d'un premier code fourni par la serrure électronique, et un moyen de communication avec le serveur distant pour transmettre vers le serveur distant ledit premier code et pour recevoir le certificat calculé par le serveur distant par le chiffrement du premier code transmis en utilisant la clé secrète, et une interface utilisateur capable de communiquer avec une serrure électronique, ladite interface transmettant le certificat reçu du serveur distant pour être fourni à la serrure électronique afin de donner accès au local en cas d'égalité entre le certificat reçu du serveur et un certificat calculé par la serrure électronique en utilisant le premier code et sa propre clé secrète.

Selon un autre aspect, il est également proposé un système de gestion à distance de l'accès à un local comprenant une serrure électronique commandant l'accès à ce local et

dotée d'une interface utilisateur, un serveur distant et un terminal portable, la serrure électronique et le serveur distant disposant d'une clé secrète associée à l'accès dudit local, la serrure électronique comportant une interface utilisateur pour acquérir une commande d'accès au local et un moyen de génération et d'acquisition d'un premier code, ledit terminal portable comportant un moyen d'acquisition du premier code présenté par la serrure électronique, et un moyen de communication avec le serveur distant pour transmettre ledit premier code, le serveur distant comportant un moyen de calcul d'un certificat calculé par le chiffrement du premier code en utilisant la clé secrète, et un moyen de transmission dudit certificat au terminal portable, ledit terminal portable comportant en outre un moyen de réception dudit premier code et une interface utilisateur pour transmettre le certificat reçu à la serrure électronique, la serrure électronique comportant en outre un moyen de calcul d'un certificat en utilisant le premier code et sa propre clé secrète et un moyen de comparaison entre les deux valeurs de certificats reçues et calculées en interne, la serrure électronique déclenchant en cas d'égalité l'ouverture d'un verrou donnant accès au local.

Un autre aspect concerne un ou plusieurs programmes d'ordinateur comportant des instructions pour la mise en œuvre d'un procédé de gestion à distance de l'ouverture d'une serrure électronique commandant l'accès à un local et dotée d'une interface utilisateur tel(s) que décrit(s) ci-dessus lorsque ce ou ces programmes sont exécutés par au moins un processeur.

Selon encore un autre aspect, il est proposé un ou plusieurs supports d'enregistrement non transitoire lisibles par un ordinateur, et comportant des instructions d'un ou plusieurs programmes d'ordinateur comprenant des instructions pour la mise en œuvre d'un procédé de gestion à distance de l'ouverture d'une serrure électronique commandant l'accès à un local et dotée d'une interface utilisateur.

4. Liste des figures

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation particulier, donné à titre de simple exemple illustratif et non-limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 présente les principaux dispositifs pour mettre en œuvre le procédé de gestion à distance de l'ouverture d'une serrure électronique, selon un exemple de

réalisation ;

- La Fig. 2 présente un exemple de schéma des différents composants électroniques d'une serrure électronique conçue pour être gérée à distance selon le procédé,
- la figure 3 est un exemple d'ordinogramme présentant des étapes pour un mode particulier de réalisation de l'invention ;
- la figure 4 présente les principales étapes cryptographiques mises en œuvre pour commander à distance l'ouverture d'une serrure électronique selon un mode de réalisation.

5. Description d'un mode de réalisation

5.1 Principe général

Le principe général de l'invention décrit un procédé de gestion à distance de l'ouverture d'une serrure électronique commandant l'accès à un local, à l'aide d'un serveur distant communiquant avec un terminal portable. Dans un premier temps, la serrure électronique et le serveur distant s'échangent une clé secrète. Puis, un utilisateur se présente devant le local et introduit une commande sur l'interface utilisateur de la serrure pour demander l'accès, déclenchant la présentation par la serrure d'un premier code déterminé et son acquisition dans le terminal portable. Une requête contenant le premier code est transmis par le terminal portable vers le serveur distant en vue de demander l'ouverture de la serrure. Le serveur distant génère un certificat par le chiffrement du premier code en utilisant la clé secrète, et le transmet au terminal portable où il est affiché. De cette façon, l'utilisateur peut l'introduire au niveau de la serrure. La serrure calcule son propre certificat et le compare avec celui que lui transmet l'utilisateur. La serrure est ouverte lorsque les valeurs des deux certificats sont identiques.

5.2 Description des principaux dispositifs mis en œuvre dans le procédé

La **Fig.1** présente les principaux dispositifs pour mettre en œuvre le procédé de gestion à distance de l'ouverture d'une serrure électronique, selon un exemple de réalisation.

Un propriétaire dispose d'un local 1 fermé par une serrure électronique 2. Ce local est par exemple, un gîte de vacances, une chambre d'hôtel, une maison particulière, etc. Le propriétaire décide d'accorder l'accès à des utilisateurs sous certaines conditions, de cette façon des utilisateurs peuvent disposer d'un service de location de locaux pendant une

durée déterminée. Pour cela, il utilise un ordinateur personnel 3 du type : téléphone portable, ordiphone, ordinateur, tablette, pour télécharger une application de gestion à distance de l'accès à un local, cette application est sous la gestion d'un serveur distant 4. Le serveur 4 dispose classiquement d'une unité centrale, de moyens de communication via un réseau informatique (Internet par exemple) et d'une mémoire pour enregistrer les informations associées aux différents propriétaires et aux locaux proposés ainsi que les informations associées aux différents utilisateurs. Le serveur exécute un programme dédié aux services ainsi offerts aux propriétaires et aux utilisateurs. Ce service permet à ces derniers de choisir un local en fonction de critères géographiques et temporels et d'effectuer des réservations du local à des moments et des durées déterminés.

Les utilisateurs disposent d'au moins un terminal portable 5 leur permettant de faire des réservations et ensuite de donner l'accès au local lorsqu'ils se présentent devant la serrure 2. L'accès au local est accordé en présentant un code 6 qui s'affiche sur l'écran 7 du terminal portable. Ce code est transmis à la serrure via son interface utilisateur et contrôlé par une unité de contrôle. Si la valeur du code transmis est égale à celle calculée par la serrure et enregistrée dans une mémoire, le verrou 8 commandant la porte 9 du local est déverrouillé.

La **Fig. 2** présente un exemple de schéma des différents composants électroniques d'une serrure électronique conçue pour être gérée à distance selon le procédé. Selon cet exemple de réalisation, la serrure 2 comporte les éléments suivants :

- une Unité de Contrôle 20, typiquement un microprocesseur et sa mémoire programme associée 21,

- une mémoire de données non volatile 22,

- une interface utilisateur éventuellement déportée 23, comportant un moyen d'acquisition de commandes 24 (clavier spécialisé, touches dédiées à certaines fonctions, microphone associé à un système de reconnaissance vocale, ...) et des moyens d'affichage de données 25 (écran, afficheur électroluminescent, ...). Selon une variante, la serrure est équipée d'un écran tactile,

- un port de sortie 26 pour commander un verrou électrique 8 afin d'accorder l'accès au local en déverrouillant la porte 9,

- une batterie 27, ou une pile, ou tout autre moyen pour fournir une alimentation

électrique.

Selon un mode de réalisation, la serrure est dotée d'une horloge 28 capable de fournir la date et l'heure courante, ou tout du moins de gérer une temporisation. Dans certains modes de réalisation, la serrure peut également comporter :

- une caméra 29 capable de capter l'image d'un objet placé devant la serrure, et d'en déterminer certaines caractéristiques. La caméra et son programme de gestion sont notamment capables d'analyser un graphisme (un code à barre par exemple) placé à 10 ou 20 centimètres devant l'objectif et d'en déduire une donnée. La caméra peut aussi traiter l'image d'un QR code qui est un type de code-barre en deux dimensions constitué de modules noirs disposés dans un carré à fond blanc. On trouve différents codes comprenant des nombres différents de points noirs ou blancs allant de 21 par 21 points, 25 par 25, 29 par 29 jusqu'à 177 par 177. Les QR Codes sont particulièrement utilisés en cryptographie car ils possèdent des Codes Correcteurs d'Erreurs permettent de corriger des erreurs de lecture.

- Un moyen de communication 30 à très courte portée (Bluetooth, Zigbee, Wifi, ...) permettant notamment de communiquer avec un terminal portable 5. La communication peut être déclenchée en approchant simplement le terminal portable 5 à proximité immédiate de la serrure 2, ou en appuyant sur un bouton.

Après avoir détaillé les principaux dispositifs permettant de mettre en œuvre le procédé, nous allons maintenant expliquer comment ceux-ci coopèrent.

5.3 Description des étapes du procédé

La **FIG.3** présente un ordinogramme d'un premier mode de réalisation d'un procédé de gestion à distance d'une serrure électronique permettant de donner l'accès à un local sécurisé pour un utilisateur.

Le déroulement des étapes s'effectue en deux temps, le premier temps consiste à générer et enregistrer la clé secrète de la serrure et fait intervenir le propriétaire du local, et le second temps permet à un utilisateur d'entrer dans ce local en mettant en œuvre un procédé qui utilise ladite clé, à la fois coté serveur et côté serrure.

5.2 Enregistrement de la clé secrète

Prenons un propriétaire qui désire autoriser l'accès de son local 1 à au moins un utilisateur ; dans un premier temps, il utilise son ordinateur personnel 3 (téléphone

portable, ordiphone, ordinateur, tablette, ...) pour se connecter à un serveur distant 4. A l 'étape 3.1, le propriétaire télécharge dans son ordinateur l'application lui permettant de s'enregistrer et introduit son nom, son adresse informatique, la localisation du local et des caractéristiques liées à ce local permettant à un utilisateur de le choisir selon certains critères. Le serveur enregistre toutes ces informations, et génère une clé secrète dite « Clé_Propriétaire» (étape 3.2) selon un mode de réalisation. Cette clé cryptographique est de préférence de type symétrique et utilisable par exemple avec l'algorithme de cryptage A.E.S. (pour « Advanced Encryption Standard »).

Puis, la serrure électronique 2 et le serveur distant 4 s'échangent la clé secrète Clé_Propriétaire associée à l'accès de ce local 1. Cet échange peut s'effectuer de multiples façons. Selon un premier mode de réalisation, le serveur distant 4 calcule la valeur de Clé_Propriétaire et la transmet à un appareil détenu par le propriétaire. La clé est affichée en clair sur l'écran de l'ordinateur 3 du propriétaire, ou sur une tablette ou sur un téléphone portable. Quel que soit le moyen d'affichage, le propriétaire peut ainsi prendre connaissance de la valeur de la clé et l'introduire manuellement sur les touches du clavier numérique de la serrure. Selon une variante, la serrure dispose d'une caméra capable de scanner l'écran de l'ordinateur, dans ce cas la clé Clé_Propriétaire est avantageusement affichée sus la forme d'un QR code. Selon une autre variante, la serrure 2 dispose d'un moyen de communication à très courte portée (Bluetooth, Zigbee, wifi, ...) et communique par ce moyen avec l'ordinateur du propriétaire pour recevoir la valeur de clé Clé_Propriétaire. Selon une autre variante, la valeur « Clé_Propriétaire » est transmise au propriétaire par des moyens postaux, et la serrure scanne le QR Code qui est imprimé sur le courrier.

Selon une variante de réalisation, le serveur reçoit la valeur de clé secrète et la serrure dispose d'un moyen de la générer. Ce moyen peut consister à placer la serrure dans un mode spécial d'initialisation dans lequel la valeur de la clef secrète est affichée par le moyen d'affichage 25 sous forme d'une chaîne de caractères. Le propriétaire peut ainsi prendre connaissance de la valeur de la clé et la saisir par un menu applicatif s'exécutant sur un appareil communiquant avec le serveur 4. La saisie de la valeur de la clé peut aussi s'effectuer à l'aide d'une caméra faisant l'acquisition de la valeur affichée sous la forme d'un QR code. Dans ce cas, l'appareil 3 du propriétaire (par exemple une tablette ou

téléphone intelligent) dispose d'une caméra et d'un logiciel capable de traiter les QR codes et d'en extraire les informations.

Un autre moyen consiste en ce que la serrure électronique dispose d'une valeur secrète enregistrée par le fabriquant, le propriétaire introduit au moyen de l'interface utilisateur un diversifiant de cette valeur pour générer la clé secrète au niveau de la serrure 2. Cette variante présente l'avantage que le propriétaire peut à tout moment changer la valeur de la clé, sans devoir garder secrète la valeur de ce diversifiant.

A l'issue de l'étape 3.3, le serveur distant et la serrure se sont échangés la clé secrète et ainsi ils disposent de la même valeur de Clé_Propriétaire. Il est maintenant possible d'autoriser un utilisateur à accéder à ce local.

5.5 élaboration d'une requête d'accès au local

A un certain moment, un utilisateur cherche une location et se connecte au serveur 4 en téléchargeant l'application sur un équipement informatique, de préférence son terminal portable 5. A l'étape 3.4, il s'identifie en tant qu'utilisateur et recherche un local qui correspond à ses critères aussi bien géographiques que temporels. Il peut éventuellement créer un compte auprès du serveur de façon à obtenir ensuite des facilités de paiement ou pour enregistrer un profil utilisateur. A l'issue de l'étape 3.4, le local 1 est sélectionné et l'utilisateur émet une requête d'accès en spécifiant la date et l'heure de début de location. De façon optionnelle, l'utilisateur introduit un mot de passe pour verrouiller sa requête d'accès et la rendre inaccessible à toute autre personne.

A l'étape 3.5, le serveur 4 vérifie les conditions d'accès pour cet utilisateur (paiement de la location, vérification des autorisations, ...) et génère un code de réservation qui est transmis à l'équipement de l'utilisateur. Le code de réservation est affiché sur l'équipement de façon que l'utilisateur en ait connaissance, et peut aussi être enregistré dans la mémoire si c'est cet équipement qui est utilisé lors de l'accès au local 1. A ce moment, le local 1 est effectivement réservé et n'apparaît plus disponible sur le site de l'application pendant toute la durée spécifiée par cet utilisateur.

Au moment défini dans la requête d'accès, l'utilisateur se présente devant la serrure pour accéder au local 1 qu'il a réservé.

5.6 Accès au local

Devant la serrure 2 commandant l'accès au local 1, l'utilisateur dispose d'un terminal

portable 5 qui peut être le même que celui avec lequel il a fait sa réservation ou un autre appareil. Dans tous les cas, ce terminal portable 5 doit lui permettre de communiquer avec le serveur 4.

A l'étape 3.6, l'utilisateur introduit une commande sur l'interface utilisateur 24 de la serrure 2 pour initialiser une autorisation d'accès au local. En réponse à cette commande, la serrure électronique produit un code dit « CODE_5chiffres », et l'affiche sur son écran (étape 3.7). La valeur « CODE_5chiffres » est générée de façon aléatoire et constitue une valeur de challenge utilisable pendant une durée courte, par exemple 5 minutes.

L'utilisateur lance l'application qui lui a permis auparavant de réserver ce local 1 et introduit le code de réservation qui a été généré par le serveur à l'étape 3.5 ou bien il choisit dans la liste des réservations, celle qui correspond au local devant lequel il se trouve. L'accès à l'application peut être conditionné par un mot de passe à introduire à ce moment. L'utilisateur introduit alors le CODE_5chiffres sur son terminal portable 5 au moyen du clavier (étape 3.8). Si le terminal portable de l'utilisateur dispose d'une caméra, alors celle-ci peut scanner l'afficheur de la serrure et ainsi faire l'acquisition de la valeur affichée. Selon une variante, la serrure transmet par radio à courte portée la valeur « CODE_5chiffres ».

A l'étape 3.9, le terminal portable 5 transmet au serveur 4 le code de réservation et la valeur « CODE_5chiffres ». Dès réception, le serveur recherche les éléments de la réservation en utilisant le code et récupère les informations associées au local 1 concerné ainsi qu'à sa serrure. Le serveur exécute un calcul cryptographique pour produire un certificat en combinant les valeurs « CODE_5chiffres » et Clé_Propriétaire (étape 3.10). Le calcul cryptographique est par exemple le chiffrement de « CODE_5chiffres » par la valeur de clé symétrique Clé_Propriétaire. A l'étape 3.11, le serveur 4 transmet au terminal portable 5 la valeur du certificat généré qui est affichée de façon que l'utilisateur en prenne connaissance.

L'utilisateur transmet la valeur du certificat à la serrure 2, soit de façon manuelle, soit par un scan de l'écran de son termina portable 5 (notamment si le certificat apparaît sous la forme d'un QR code), ou par liaison radio à très courte portée (étape 3.12). Dès réception du certificat, à l'étape 3.13, la serrure électronique 2 contrôle son authenticité en effectuant le même calcul que celui réalisé par le serveur, c'est à dire le même algorithme

cryptographique pour produire un certificat en combinant les valeurs « CODE_5chiffres » et « Clé_Propriétaire ». A l'étape 3.14, la serrure compare ensuite le résultat du calcul avec la valeur de certificat reçu. Si les deux valeurs sont égales, alors la serrure 2 émet un signal de déverrouillage autorisant ainsi l'accès au local 1 (étape 3.16). Dans le cas contraire, le verrou ne s'ouvre pas.

Au terme d'un nombre limité d'essais de saisie du certificat (manuel ou par lecture de code graphique), l'utilisateur doit de nouveau introduire une commande sur l'interface de la serrure pour demander une autorisation d'accès au local, tel que cela est décrit à l'étape 3.6. On peut prévoir qu'au bout de trois essais consécutifs et infructueux, la serrure se bloque pendant une durée déterminée, une demi-heure par exemple. Dans le cas où la valeur du certificat présenté est égal à celle calculé à l'étape 3.13, cette valeur est mémorisée par la serrure et permet, lors d'une nouvelle introduction du certificat de donner l'accès au local sans avoir à communiquer avec le serveur 4. L'introduction du certificat s'effectue de préférence au moyen d'une autre commande (un autre bouton ou une autre icône affichée par exemple) que celle utilisée lors de l'étape 3.6. Si un autre utilisateur se présente devant la serrure et demande une autorisation d'accès, le nouveau certificat généré efface le précédent.

Selon un perfectionnement, si l'utilisateur introduit consécutivement plusieurs valeurs erronées de certificat, on peut suspecter une mauvaise introduction de valeur ou une tentative de fraude visant à découvrir la véritable valeur. Dans ce cas, le certificat est effacé dans la mémoire de la serrure au bout d'un certain nombre de présentation, 10 par exemple. De cette manière, tout nouvel accès à ce local 1 passe par une requête vers le serveur 4 pour recevoir un nouveau certificat.

Selon un autre perfectionnement, l'introduction consécutive d'un certain nombre de commandes d'accès, 3 par exemple, qui aboutissent à l'effacement du certificat en mémoire à cause du fait que les valeurs introduites sont erronées, peut constituer une tentative de découvrir la clé secrète. Dans un tel cas, la serrure se met dans un état de blocage dans lequel le certificat est effacé de la mémoire 22 et pour lequel il faut attendre une durée déterminée, une demi-heure par exemple, avant tout nouvel essai de demande d'accès. Cette durée est décomptée par l'horloge 28 incorporée dans la serrure électronique 2.

Dans un mode plus automatisé comme la lecture du QR code, une seule capture de certificat par la serrure avec une valeur erronée suffit pour devoir repartir de l'étape 3.6.

Selon un perfectionnement, les étapes 3.6 à 3.13 doivent être effectuées au cours d'une durée limitée dans le temps, 5 minutes par exemple. Si ce temps est dépassé (étape 3.15), alors la serrure émet un signal lumineux et/ou sonore indiquant à l'utilisateur qu'il doit de nouveau introduire une commande, comme cela est décrit à l'étape 3.6.

Selon un autre perfectionnement, la serrure prend en compte la durée de la réservation et dispose pour cela d'une horloge 28 permettant de comptabiliser le temps de l'accès pour un utilisateur donné. Selon ce perfectionnement, le serveur 4 enregistre la durée de la réservation « DUR » prévue pour la réservation de ce local par l'utilisateur, en nombre de jours par exemple et concatène « DUR » avec « CODE_5chiffres » pour obtenir la valeur utilisée pour le calcul cryptographique décrit à l'étape 3.9. Par exemple, le champ concaténé s'exprime en 7 digits décimaux ou hexadécimaux, 2 pour la durée DUR et 5 pour la valeur CODE_5chiffres. Le certificat est transmis au terminal portable 5 de l'utilisateur avec la valeur « DUR » en clair. La serrure électronique 2 contrôle l'authenticité du certificat en exécutant le même calcul que celui du serveur 4 (même fonction mathématique et mêmes valeurs) et en comparant les résultats. En cas d'égalité détectée lors de l'étape 3.14, la serrure 2 autorise l'accès au local et programme son horloge 28 avec la valeur DUR.

L'accès au local est autorisé en utilisant cette valeur de certificat pendant la durée DUR. Lorsque le temps est écoulé, le certificat est effacé de la mémoire 22 de la serrure et l'accès au local en utilisant cette valeur n'est plus possible. A partir de ce moment, l'utilisateur devra introduire une nouvelle commande sur l'interface utilisateur 24 de la serrure 2, déclenchant la génération d'une autre valeur de CODE_5chiffres et la production d'un autre certificat.

Selon un autre perfectionnement, la serrure 2 prend en compte des plages horaires pour accéder dans la journée au local, par exemple de 7 heures du matin jusqu'à 23 heures. Ces plages horaires participent au calcul cryptographique de l'étape 3.10 et sont transmises en clair à la serrure. La serrure qui dispose d'une horloge 28 contrôle que la demande d'accès au local 1 par un utilisateur s'effectue au cours des plages horaires spécifiées.

Selon un autre perfectionnement, le serveur 4 transmet l'heure et la date spécifiées par l'utilisateur lors de l'étape 3.4 à la serrure 2 via le terminal portable 5. Ces valeurs

déterminent le moment où l'utilisateur est effectivement autorisé à accéder au local. Selon ce perfectionnement, plusieurs dates et heures peuvent être spécifiées dans la demande de réservation formulée par l'utilisateur, le même certificat permettant d'accéder au local 1 lors de ces différents moments. La serrure qui dispose d'une horloge 28 contrôle que l'introduction du certificat pour accéder au local telle que décrit à l'étape 3.12, intervient lors d'un de ces moments.

La **Fig.4** présente les principales étapes cryptographiques mises en œuvre pour commander à distance l'ouverture d'une serrure électronique selon un mode de réalisation. La **Fig.4** est séparée en deux par une ligne verticale afin de distinguer les calculs effectués par le serveur 4 (à gauche) et par la serrure 2 (à droite).

Selon ce mode de réalisation, la serrure génère la valeur CODE5chiffres et le serveur dispose de la valeur DUR qui a été définie par le propriétaire. Lors de l'initialisation d'une autorisation d'accès au local, la serrure transmet la valeur CODE5chiffres au serveur qui émet en retour le certificat et la valeur DUR (cette valeur ayant également participé au calcul du certificat). CODE5chiffres possède préférentiellement 5 digits numériques ou hexadécimal et DUR : deux digits, les nombres 2 et 5 ne sont donnés qu'à titre d'exemple de réalisation et peuvent être modifiés. Les deux valeurs concaténées constituent le paramètre d'entrée d'une fonction mathématique notée « Algo » utilisant Clé_Propriétaire en tant que clé cryptographique. La fonction Algo est de préférence un algorithme de chiffrement symétrique, les valeurs chiffrées ayant le même nombre de digits que les valeurs en clair, 7 digits dans le cas présent.

Selon ce mode de réalisation, le champ de 7 digits est réduit à 5 digits à l'aide d'une fonction de hachage, notée « H ». De cette façon, la taille du certificat est limitée, ce qui simplifie son introduction au niveau de la serrure. Un certificat sur 5 digits est produit par la fonction de hachage. Les calculs cryptographiques qui viennent d'être décrits plus haut s'exécutent à l'identique coté serveur 4 et coté serrure 2, de sorte que, si les paramètres d'entrées sont identiques (CODE5chiffres, DUR, Clé_Propriétaire), les certificats le sont également. La serrure électronique 2 contrôle l'authenticité du certificat en comparant la valeur reçue du serveur avec la valeur calculée. En cas d'égalité, la serrure accorde l'accès au local en ouvrant le verrou 8.

En fonction du mode de réalisation choisi, certains actes, actions, évènements ou

fonctions de chacun des procédés décrits dans le présent document peuvent être effectués ou se produire selon un ordre différent de celui dans lequel ils ont été décrits, ou peuvent être ajoutés, fusionnés ou bien ne pas être effectués ou ne pas se produire, selon le cas. En outre, dans certains modes de réalisation, certains actes, actions ou évènements sont effectués ou se produisent concurremment et non pas successivement.

Dans le cas où la serrure dispose d'une caméra 29 capable de lire des codes graphiques tels que des code-barres ou des QR codes, la fonction de hachage peut produire un haché plus long, car il n'y a pas la contrainte de la saisie des digits du certificat manuellement sur la serrure.

Dans le cas où l'algorithme de chiffrement produit un résultat contenant davantage de digits (ou caractères hexadécimaux) que ceux en entrée, la fonction de hachage peut compenser en donnant un nombre de digits compatible avec une introduction au niveau de l'interface 24 de la serrure, c'est à dire que le nombre de digits est plus faible si l'introduction est manuelle et le nombre de digits est plus important si l'introduction s'effectue en scannant un code par la caméra 29.

Bien que décrits à travers un certain nombre d'exemples de réalisation détaillés, les procédés proposés et les dispositifs correspondants comprennent différentes variantes, modifications et perfectionnements qui apparaîtront de façon évidente à l'homme de l'art, étant entendu que ces différentes variantes, modifications et perfectionnements font partie de la portée de l'invention, telle que définie par les revendications qui suivent. De plus, différents aspects et caractéristiques décrits ci-dessus peuvent être mis en œuvre ensemble, ou séparément, ou bien substitués les uns aux autres, et l'ensemble des différentes combinaisons et sous combinaisons des aspects et caractéristiques font partie de la portée de l'invention. En outre, il se peut que certains dispositifs décrits ci-dessus n'incorporent pas la totalité des modules et fonctions décrits pour les modes de réalisation préférés.

REVENDICATIONS

1. Procédé de gestion à distance de l'ouverture d'une serrure électronique (2) commandant l'accès à un local (1) et dotée d'une interface utilisateur (24,25), ledit procédé comportant notamment les étapes suivantes mises en œuvre au niveau de la serrure électronique :
   - échange (3.3) entre la serrure électronique et un serveur distant d'une clé secrète associée à l'accès audit local,
   - acquisition d'une commande (3.6) sur l'interface utilisateur (24) de la serrure électronique pour demander l'accès au local, l'acquisition de ladite commande déclenchant la génération d'un premier code,
   - affichage (3.7) sur l'interface utilisateur (24) de la serrure électronique dudit premier code,
   - fourniture (3.12) à la serrure électronique par son interface utilisateur (24) d'un certificat, ledit certificat étant calculé par le serveur distant par le chiffrement du premier code en utilisant la clé secrète,
   - calcul du certificat (3.13) par la serrure électronique en utilisant le premier code et sa propre clé secrète,
   - ouverture (3.16) de la serrure électronique lorsque les valeurs des deux certificats sont identiques.

2. Procédé selon la revendication 1, dans lequel il comporte une étape d'incorporation dans le calcul du certificat (3.10) en plus du premier code, d'une valeur représentative de la durée d'accès, et une étape de réception (3.12) par l'interface utilisateur (24) de ladite valeur en clair, la première égalité entre la valeur du certificat reçu par l'interface utilisateur (24) et la valeur du certificat calculé par la serrure électronique déclenchant la mise en marche d'une horloge (28) incorporée dans la serrure électronique (2) pour décompter ladite durée d'accès, une nouvelle fourniture du certificat après l'expiration de la durée d'accès ne déclenchant pas l'ouverture de la serrure électronique (2).

3. Procédé selon la revendication 1, dans lequel il comporte une étape d'incorporation dans le calcul du certificat (3.10) en plus du premier code, d'une valeur

représentative d'au moins un moment au cours duquel l'accès au local est autorisé, et une étape de réception (3.12) par l'interface utilisateur (24) de la serrure électronique dudit moment, la serrure électronique (2) disposant d'une horloge (28), l'accès au local étant accordé en fournissant le certificat à la serrure lorsqu'au moins un des moments spécifiés correspond au moment courant indiqué par l'horloge.

4. Procédé selon la revendication 1, dans lequel il comporte une étape d'incorporation dans le calcul du certificat (3.10) en plus du premier code, d'une valeur représentative d'au moins une fenêtre périodique au cours de laquelle l'accès au local est autorisé, et une étape de réception (3.12) d'au moins une fenêtre périodique par l'interface utilisateur (24) de la serrure électronique (2), la serrure électronique (2) disposant d'une horloge (28), l'accès au local étant accordé en fournissant le certificat à la serrure lorsque le moment courant indiqué par l'horloge se situe pendant au moins une des fenêtres périodiques spécifiées.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel il comporte une étape de réduction de la taille des données pour le calcul du certificat exécutée par la serrure électronique (2) avant la comparaison des deux certificats.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel les calculs de certificats s'effectuent à l'aide d'une clé cryptographique symétrique.

7. Procédé selon l'une quelconque des revendications précédentes, comportant une étape de génération de la valeur de clé secrète dans la serrure électronique, et une étape de transmission de ladite valeur au serveur distant (4).

8. Procédé selon l'une quelconque des revendications précédentes, comportant une étape d'enregistrement du certificat dans la mémoire (22) de la serrure électronique (2) pour accorder de nouveau l'accès au local lors d'une nouvelle fourniture de ce certificat.

9. Procédé selon la revendication 8, dans lequel la réception (3.12) consécutive d'un nombre déterminé de valeurs erronées de certificats déclenchent l'effacement du certificat de la mémoire (22) et un état de blocage qui s'interrompt lors d'une nouvelle étape d'acquisition (3.6) d'une commande sur l'interface utilisateur de la serrure électronique et d'une nouvelle réception (3.12) par l'interface utilisateur (24) d'un certificat dont la valeur est égale à celle calculée par la serrure électronique en utilisant le premier code et sa propre clé secrète.

10. Procédé selon la revendication 9, dans lequel l'acquisition consécutive d'un nombre déterminé de commandes d'accès (3.6) du fait de la réception (3.12) consécutive d'un nombre déterminé de valeurs erronées de certificats déclenchent l'effacement du certificat de la mémoire (22) et un état de blocage provoquant la mise en marche d'une horloge (28) incorporée dans la serrure électronique (2) pour décompter une durée déterminée au cours de laquelle toute nouvelle acquisition de commande d'accès aboutit à un échec.

11. Procédé de gestion à distance de l'ouverture d'une serrure électronique (2) commandant l'accès à un local (1) à l'aide d'un certificat calculé par un serveur distant (4) en utilisant une clé secrète connue de la serrure électronique et dudit serveur distant, ledit procédé comportant notamment les étapes suivantes mises en œuvre au niveau d'un terminal (5) :
- acquisition (3.8) d'un premier code fourni par ladite serrure électronique (2),
- transmission (3.9) vers le serveur distant du premier code,
- réception (3.11) en provenance du serveur distant d'un certificat calculé par le serveur distant par le chiffrement du premier code en utilisant la clé secrète,
- fourniture (3.12) à la serrure électronique du certificat reçu du serveur distant (4) pour être fourni à la serrure électronique (2) afin d'ouvrir la serrure en cas d'égalité entre le certificat reçu du serveur et un certificat calculé par la serrure électronique en utilisant le premier code et sa propre clé secrète.

12. Serrure électronique (2) commandant l'accès à un local (1) et dotée d'une interface utilisateur (24,25) et d'une mémoire (22) contenant au moins une clé secrète dont la valeur est partagée avec un serveur distant (4), la serrure électronique (2) étant

également dotée d'un moyen de génération d'un premier code déclenché par l'acquisition sur l'interface utilisateur (24,25) d'une commande pour demander l'accès au local et présenté sur l'interface utilisateur pour être transmise au serveur distant, d'un moyen de calcul d'un certificat utilisant ledit premier code et la clé secrète, d'un moyen de réception d'un certificat calculé par le serveur distant par le chiffrement du premier code en utilisant la clé secrète, et d'un moyen de comparaison entre les deux valeurs de certificats reçues et calculées en interne, la serrure électronique déclenchant en cas d'égalité l'ouverture d'un verrou donnant l'accès au local.

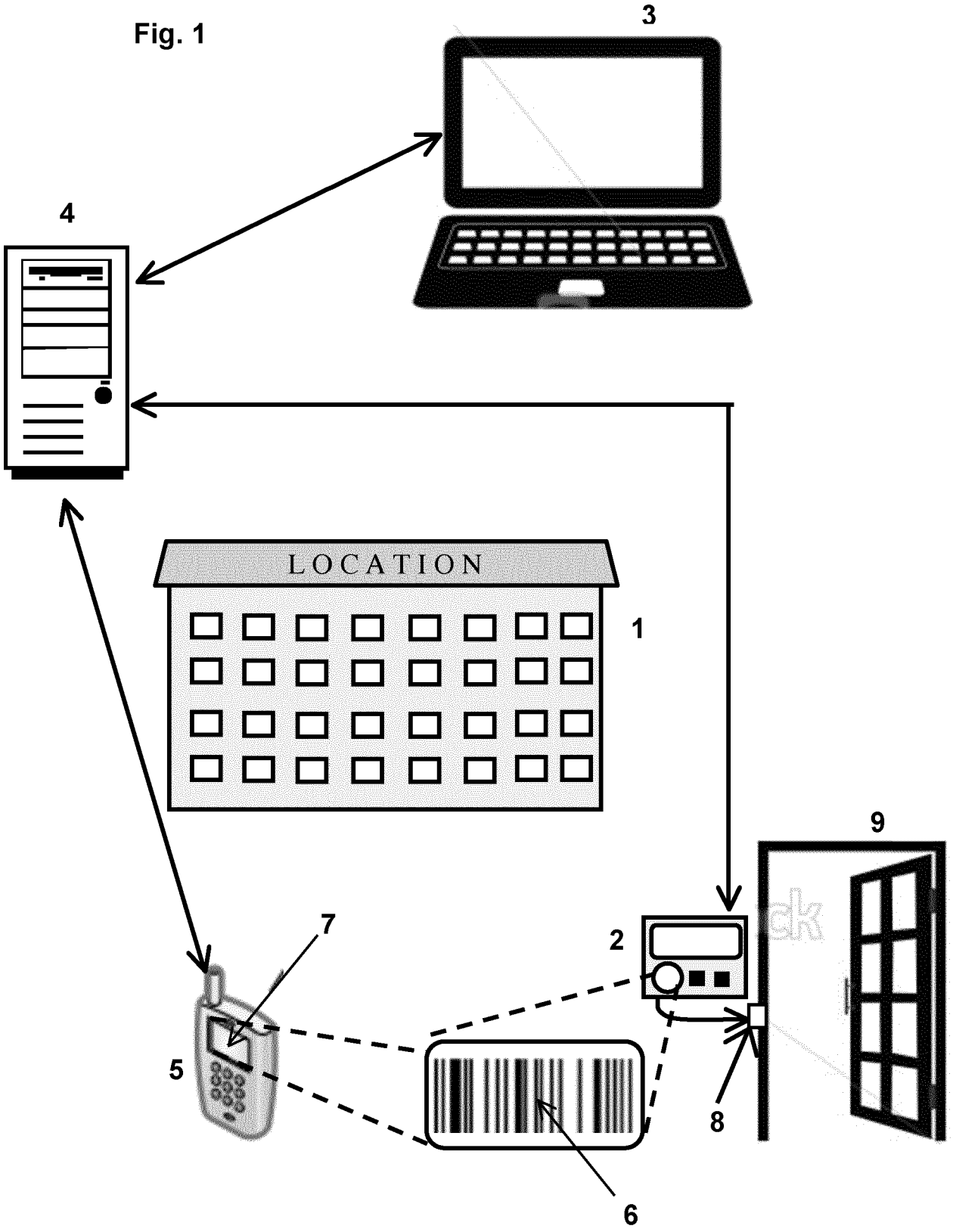
13. Terminal portable (5) destiné à permettre l'ouverture d'une serrure électronique (2) commandant l'accès à un local (1) en utilisant un certificat calculé par un serveur distant (4) en utilisant une clé secrète connue de la serrure électronique et dudit serveur distant, ledit terminal portable (5) comportant un moyen d'acquisition d'un premier code fourni par la serrure électronique (2), et un moyen de communication avec le serveur distant (4) pour transmettre vers le serveur distant ledit premier code et pour recevoir le certificat calculé par le serveur distant par le chiffrement du premier code transmis en utilisant la clé secrète, et une interface utilisateur (7) capable de communiquer avec une serrure électronique, ladite interface transmettant le certificat reçu du serveur distant (4) pour être fourni à la serrure électronique (2) afin de donner accès au local (1) en cas d'égalité entre le certificat reçu du serveur et un certificat calculé par la serrure électronique en utilisant le premier code et sa propre clé secrète.

14. Système de gestion à distance de l'accès à un local (1) comprenant une serrure électronique (2) commandant l'accès à ce local (1) et dotée d'une interface utilisateur (24,25), un serveur distant (4) et un terminal portable (5), la serrure électronique (2) et le serveur distant (4) disposant d'une clé secrète associée à l'accès dudit local, la serrure électronique comportant une interface utilisateur (24) pour acquérir une commande d'accès au local et un moyen de génération et d'acquisition d'un premier code, ledit terminal portable (5) comportant un moyen d'acquisition du premier code présenté par la serrure électronique (2), et un moyen de communication avec le serveur distant (4) pour transmettre ledit premier code,

le serveur distant (4) comportant un moyen de calcul d'un certificat calculé par le chiffrement du premier code en utilisant la clé secrète, et un moyen de transmission dudit certificat au terminal portable, ledit terminal portable (5) comportant en outre un moyen de réception dudit premier code et une interface utilisateur (7) pour transmettre le certificat reçu à la serrure électronique (2), la serrure électronique (2) comportant en outre un moyen de calcul d'un certificat en utilisant le premier code et sa propre clé secrète et un moyen de comparaison entre les deux valeurs de certificats reçues et calculées en interne, la serrure électronique déclenchant en cas d'égalité l'ouverture d'un verrou donnant accès au local (1).

15. Programme d'ordinateur comportant des instructions pour la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 11, lorsque ce programme est exécuté par un processeur.

Fig. 1



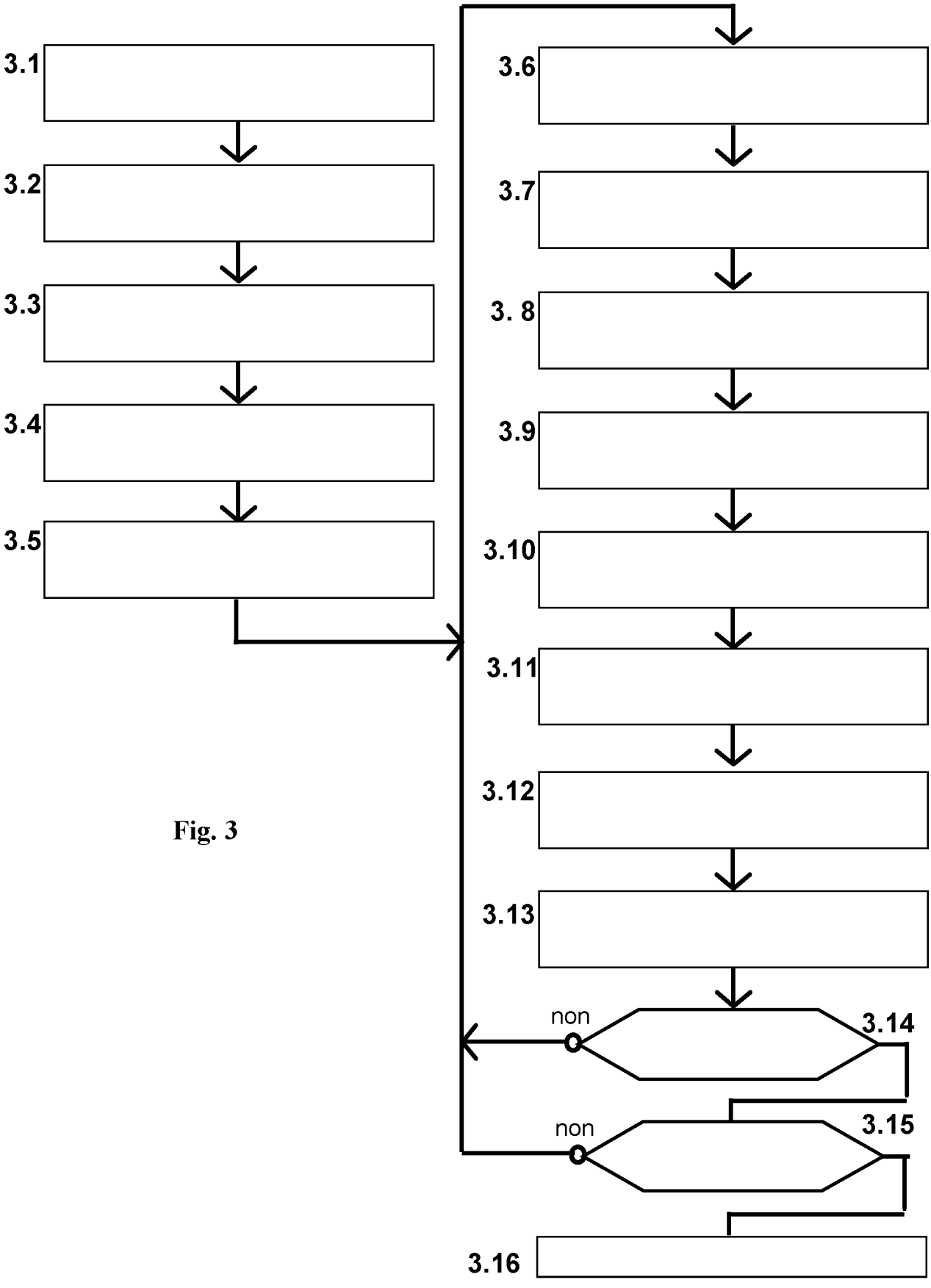


Fig. 3

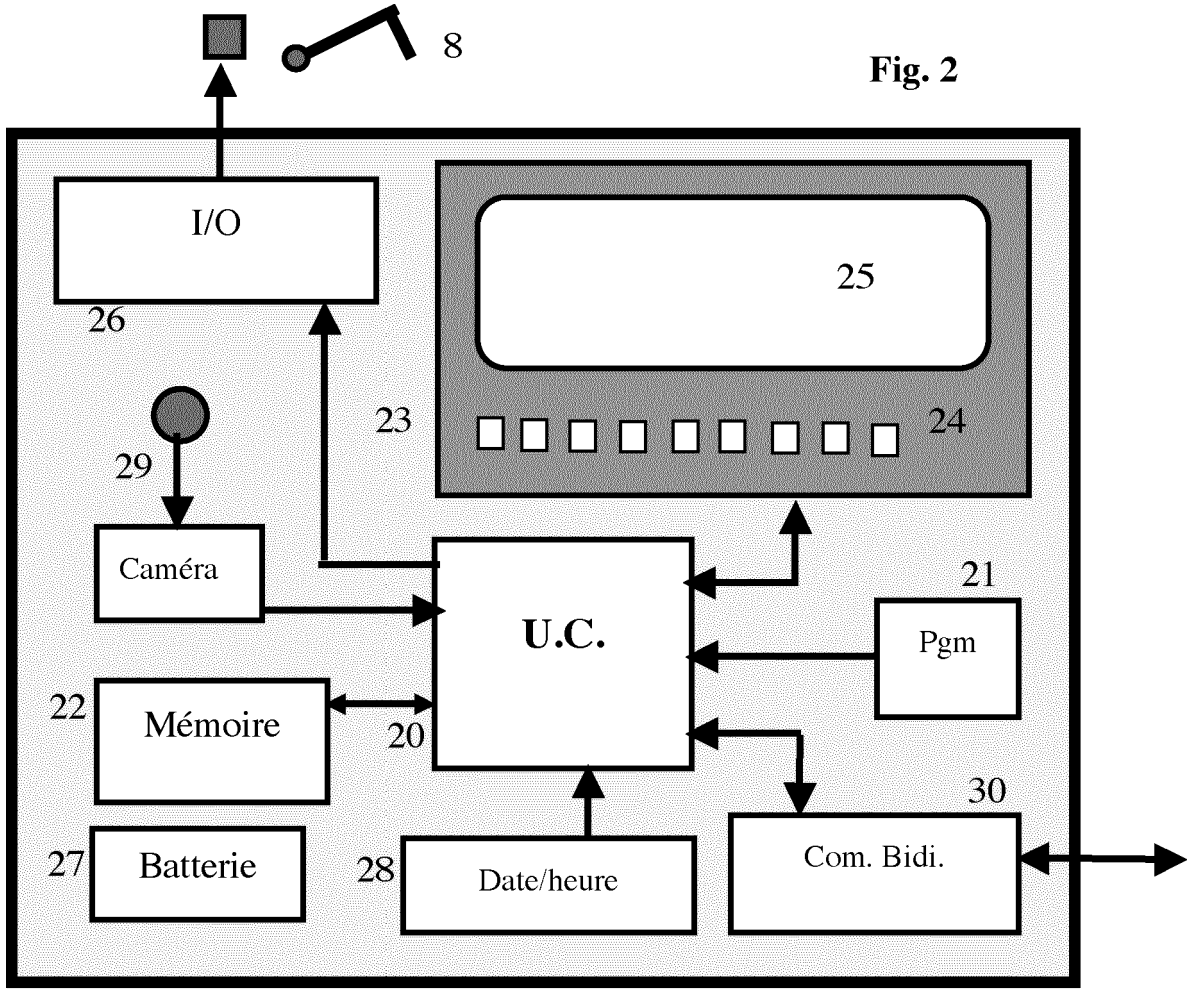

8
I/O
26
25
24
23
29
Caméra
U.C.
21
Pgm
22
Mémoire
20
30
27
Batterie
28
Date/heure
Com. Bidi.

Fig. 2

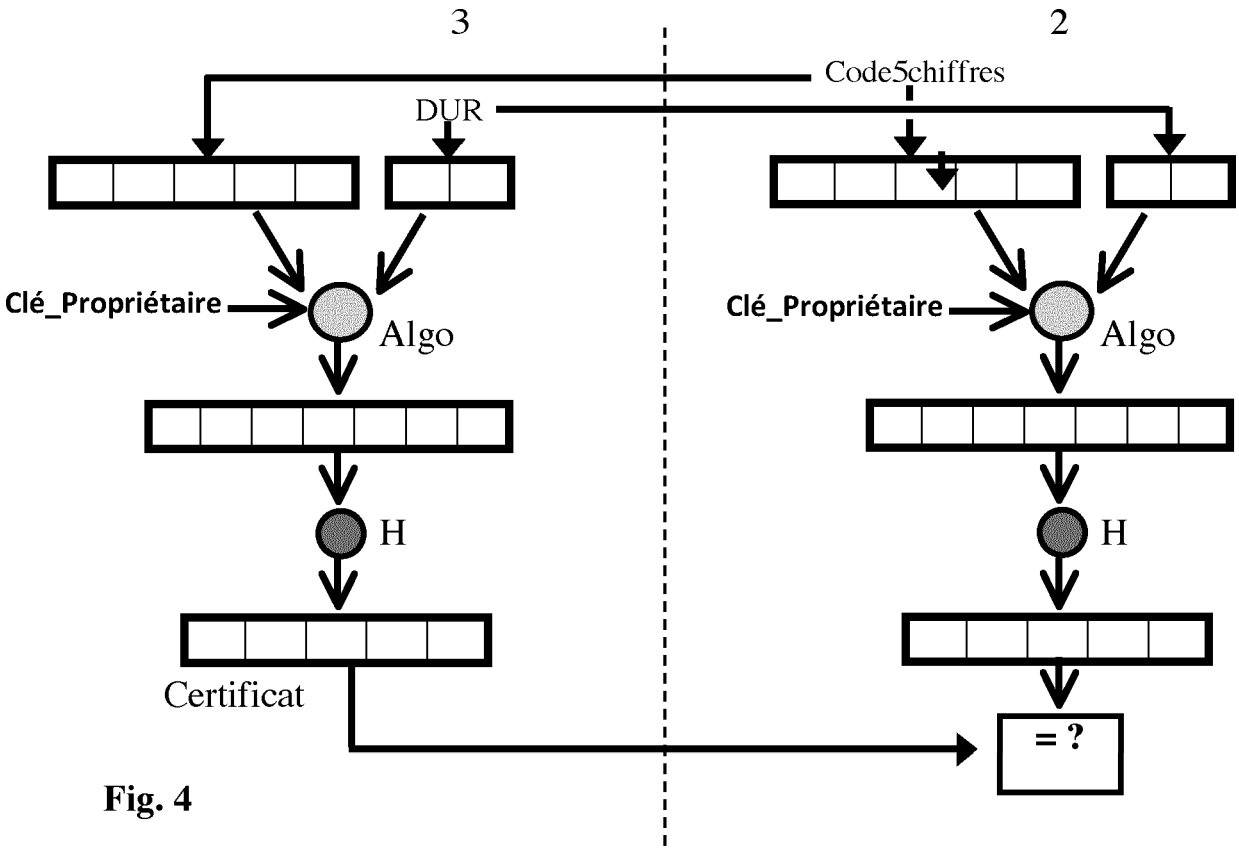

3
2
Code5chiffres
DUR
Clé_Propriétaire
Algo
H
Certificat
Clé_Propriétaire
Algo
H
= ?

Fig. 4

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 856585
FR 1854322

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 9 659 424 B2 (PARAKEET TECH INC [US]) 23 mai 2017 (2017-05-23) * colonne 17 - colonne 18 *	1-15	H04W12/08 H04W12/04 E05B47/00 H04L9/28
A	US 2012/222103 A1 (BLIDING OLLE [SE] ET AL) 30 août 2012 (2012-08-30) * alinéa [0014] - alinéa [0040]; figure 3a *	1-15	G06F21/33 G07C9/00
A	US 2016/035163 A1 (CONRAD NATHAN [US] ET AL) 4 février 2016 (2016-02-04) * figure 3 *	1-15	
A	WO 2012/047850 A2 (MASTER LOCK CO [US]; LACINA DOUGLAS E [US]) 12 avril 2012 (2012-04-12) * alinéa [0023] *	9,10	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04W G07C

Date d'achèvement de la recherche	Examinateur
28 novembre 2018	Jardak, Christine

CATÉGORIE DES DOCUMENTS CITÉS

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

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

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1854322 FA 856585

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 28-11-2018
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 9659424 B2	23-05-2017	AUCUN	
US 2012222103 A1	30-08-2012	EP 2504818 A1	03-10-2012
		SE 0950904 A1	28-05-2011
		US 2012222103 A1	30-08-2012
		US 2015310685 A1	29-10-2015
		WO 2011065892 A1	03-06-2011
US 2016035163 A1	04-02-2016	AU 2015296492 A1	16-03-2017
		AU 2017100542 A4	15-06-2017
		CA 2955797 A1	04-02-2016
		CN 107211245 A	26-09-2017
		EP 3175636 A1	07-06-2017
		JP 2017531342 A	19-10-2017
		US 2016035163 A1	04-02-2016
		US 2017236352 A1	17-08-2017
		WO 2016019065 A1	04-02-2016
WO 2012047850 A2	12-04-2012	AUCUN	

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82