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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
3 août 2017 (03.08.2017)

WIPO | PCT

(10) Numéro de publication internationale
WO 2017/129887 A1

(51) Classification internationale des brevets :
G06F 21/35 (2013.01) *G06F 21/81* (2013.01)
G06F 21/79 (2013.01) *G06F 21/88* (2013.01)

(21) Numéro de la demande internationale :
PCT/FR2017/050139

(22) Date de dépôt international :
24 janvier 2017 (24.01.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1650570 25 janvier 2016 (25.01.2016) FR

(72) Inventeur; et
(71) Déposant : **GASCUEL, Jacques, Claude, Guy** [FR/AD]; Edifici Santa Maria de Coll de Caldes, Escala A - Planta Cinquena, Crta d'Engolasters, Escaldes-Engordany, AD700 (AD).

(74) Mandataire : **GEVERS & ORES**; 9 rue Saint Antoine du T, 31000 Toulouse (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

[Suite sur la page suivante]

(54) **Title** : ACCESS CONTROL SYSTEM

(54) **Titre** : SYSTÈME DE CONTRÔLE D'ACCÈS

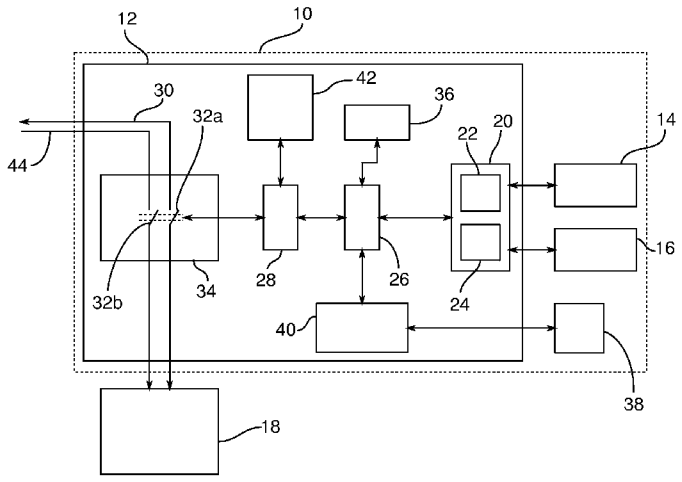

Fig. 1

(57) **Abstract** : The invention relates to a system (10) for controlling access to a device (18) protected by at least one pre-parametrised authentication factor, including an access control unit (12) including: a short-range wireless communication device (20), a key reception module (24), a module (26) for verifying the authentication factors, at least one access path (30), and at least one controllable switch (32a) configured to open or close the access path (30) to the protected device in the event that access authorisation coming from the verification module (26) is received. The system also includes an administration unit (14), suitable for making it possible to pre-parametrise each authentication factor, and a user unit (16) configured to send at least one key to the key reception module (24).

(57) **Abrégé** :

[Suite sur la page suivante]

WO 2017/129887 A1

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

L'invention concerne un système (10) de contrôle d'accès à un dispositif (18) protégé par au moins un facteur d'authentification pré-paramétré, comprenant une unité (12) de contrôle d'accès comprenant un dispositif (20) de communication sans-fil courte portée, un module (24) de réception de clés, un module (26) de vérification des facteurs d'authentification, au moins un chemin (30) d'accès, et au moins un commutateur (32a) pilotable configuré pour ouvrir ou fermer le chemin (30) d'accès au dispositif protégé en cas de réception d'une autorisation d'accès provenant du module (26) de vérification. Le système comprend en outre une unité (14) d'administration, adaptée pour permettre de pré-paramétrer chaque facteur d'authentification et une unité (16) utilisateur, configurée pour transmettre au moins une clé au module (24) de réception de clés.

SYSTÈME DE CONTRÔLE D'ACCÈS

1. Domaine technique de l'invention

L'invention concerne un système de contrôle d'accès. En particulier, l'invention concerne un système de contrôle d'accès à un dispositif protégé, par exemple l'accès à une ou plusieurs mémoires protégées d'un composant électronique.

2. Arrière-plan technologique

Les systèmes de contrôle d'accès permettent de restreindre l'accès à un dispositif protégé uniquement aux personnes qui disposent des autorisations nécessaires pour accéder au dispositif protégé. Ce dispositif protégé peut être par exemple une mémoire contenant des données numériques dont on veut restreindre l'accès, ou un équipement physique verrouillé dont l'utilisation est soumise à une autorisation d'accès.

Les systèmes de contrôle d'accès actuels mettent en œuvre généralement un ou plusieurs facteurs d'authentification avant de délivrer une autorisation d'accès. Chaque facteur d'authentification définit un ou plusieurs critères de validité d'une clé qui lui est présentée, une clé valide permettant de placer le facteur d'authentification dans un état dit déverrouillé. Lorsque l'ensemble des facteurs d'authentification est déverrouillé, l'accès est autorisé. Il peut par exemple s'agir d'un mot de passe qui est comparé avec une liste de mots de passe autorisés.

La vérification de la correspondance des facteurs d'authentification avec au moins une clé et le paramétrage des facteurs d'authentification sont souvent effectués par le biais d'une connexion à un serveur externe, notamment via Internet. Cette solution présente des risques d'interception de données à la volée par un opérateur malveillant permettant d'obtenir des informations soit sur le facteur d'authentification mis en œuvre, soit sur la clé soumise au facteur d'authentification.

En outre, les systèmes de contrôles d'accès actuels sont peu modulables, et les facteurs d'authentification sont facilement identifiables par toute personne malveillante souhaitant accéder au dispositif protégé sans autorisation. Les attaques destinées à obtenir l'accès sont donc focalisées sur ces facteurs.

3. Objectifs de l'invention

L'invention vise à pallier au moins certains des inconvénients des systèmes de contrôle d'accès connus.

En particulier, l'invention vise à fournir, dans au moins un mode de réalisation de l'invention, un système de contrôle d'accès autonome, ne nécessitant pas de connexion avec un serveur externe.

L'invention vise aussi à fournir, dans au moins un mode de réalisation, un système de contrôle d'accès permettant un paramétrage personnalisable des facteurs d'authentification.

4. Exposé de l'invention

Pour ce faire, l'invention concerne un système de contrôle d'accès à un dispositif protégé par au moins un facteur d'authentification pré-paramétré, chaque facteur d'authentification définissant au moins un critère de validité d'une clé et étant dans un état dit déverrouillé si une clé qui lui est présentée répond aux critères de validité, et un état dit verrouillé si aucune clé qui lui est présentée ne répond aux critères de validité, comprenant :

- une unité de contrôle d'accès comprenant :
  - un dispositif de communication sans-fil courte portée, comprenant un module de transmission sans-fil de données et un module de récolte d'énergie électrique,
  - un module de réception de clés, adapté pour recevoir au moins une clé,
  - un module de vérification des facteurs, adapté pour vérifier la validité de chaque facteur d'authentification pré-paramétré avec au moins une clé reçue par le module de réception de clé et fournir une autorisation d'accès si l'ensemble des facteurs d'authentification sont dans l'état déverrouillé,
  - au moins un chemin d'accès, adapté pour permettre l'accès au dispositif protégé,
  - au moins un commutateur pilotable, configuré pour ouvrir ou fermer le chemin d'accès au dispositif protégé, le chemin d'accès

étant par défaut fermé et étant ouvert en cas de réception d'une autorisation d'accès provenant du module de vérification,

- une unité d'administration, adaptée pour permettre de pré-paramétrer chaque facteur d'authentification par interaction avec le module de transmission sans-fil de données du dispositif de connexion de l'unité de contrôle d'accès,
- une unité utilisateur, configurée pour transmettre au moins une clé au module de réception de clés, via le module de transmission sans-fil de données.

Un système de contrôle d'accès selon l'invention permet donc de gérer l'accès à un dispositif protégé de façon autonome, sans connexion à un serveur externe, le paramétrage des facteurs d'utilisation et la vérification des facteurs d'utilisation sont effectués uniquement dans l'unité de contrôle d'accès ou à proximité, les interactions avec l'unité de contrôle d'accès se faisant uniquement via une connexion sans-fil courte portée (inférieure à 100m). Le système d'accès est donc plus résistant aux attaques par interception de trames, car les interactions critiques (notamment pré-paramétrage des facteurs d'authentification par l'administrateur grâce à l'unité d'administration et tentative d'accès par un utilisateur grâce à une unité utilisateur) sont effectuées uniquement en local à courte portée.

De plus, les facteurs d'authentification sont entièrement paramétrables au préalable par un administrateur humain, via l'unité d'administration.

L'unité d'administration et l'unité utilisateur sont des équipements permettant la transmission de données sans-fil et chacun contrôlés par un opérateur humain, appelés respectivement administrateur et utilisateur. L'unité d'administration et l'unité utilisateur sont donc distinctes, c'est-à-dire qu'ils sont des équipements distincts utilisés par des opérateurs humains distincts. L'équipement est par exemple un terminal de communication tel qu'un ordiphone (communément appelé *smartphone* en anglais). L'administrateur définit les facteurs d'authentification grâce à l'unité d'administration et l'utilisateur tente de déverrouiller l'accès au dispositif protégé avec l'unité utilisateur. Des clés peuvent être fournies manuellement par l'administrateur à l'utilisateur, par exemple par validation sur une application ou un logiciel installé sur l'unité

d'administration et transmission à l'unité utilisateur.

Le système est en outre autonome grâce à la récolte d'énergie effectuée par le module de récolte d'énergie électrique. Cette récolte d'énergie est par exemple une récolte d'énergie photovoltaïque, cinétique, thermoélectrique, etc., et est choisie en fonction du dispositif à protéger, de son emplacement, de sa fonction, etc. La récolte d'énergie permet au système de ne pas être uniquement tributaire d'une batterie, laquelle a une durée de vie limitée. Le système peut toutefois comprendre un dispositif de stockage d'énergie, rechargé grâce à la récolte d'énergie (permettant par exemple de stocker l'énergie photovoltaïque le jour pour une utilisation du système la nuit).

Le dispositif protégé, dont l'accès et/ou l'utilisation sont contrôlés par le système, peut être de différents types, par exemple un moyen de stockage lisible par ordinateur (mémoire de type clé USB, disque dur externe ou interne, etc.), un véhicule (voiture, vélo ou trottinette en libre-service protégés, etc.), une porte d'accès, etc.

Le chemin d'accès permettant l'accès au dispositif protégé est par exemple un bus de transmission de données. Le commutateur pilotable permet de contrôler physiquement ce bus de transmission. Le chemin d'accès est ouvert (c'est-à-dire que l'on peut accéder au dispositif protégé) lorsque le commutateur est électriquement fermé et inversement, le chemin d'accès est fermé lorsque le commutateur est électriquement ouvert.

Ainsi, par exemple lorsque le dispositif protégé est un support de stockage, si le support de stockage est branché à un ordinateur et que le chemin d'accès est fermé, la présence du support de stockage n'est pas détectée par l'ordinateur, et est donc non détectable par un opérateur malveillant non autorisé.

Avantageusement et selon l'invention, chaque facteur d'authentification définit au moins un critère de validité d'une clé choisie dans le groupe comprenant les clés suivantes :

- mot de passe,
- clé transmise par l'unité d'administration,
- données de géolocalisation du dispositif protégé et/ou de l'unité utilisateur,

- valeurs mesurées par un ou plusieurs capteurs électroniques,
- données temporelles,
- clé provenant d'une balise de proximité.

Selon cet aspect de l'invention, les facteurs d'authentification peuvent être de différentes sortes et peuvent être combinés afin d'offrir la meilleure sécurité possible, en fonction du contexte d'utilisation du dispositif protégé.

Un dispositif protégé par le système de contrôle est ainsi accessible uniquement si l'ensemble des facteurs d'authentification sont déverrouillés : par exemple, l'accès d'un utilisateur à un disque dur contenant des informations à caractère professionnel peut être autorisé uniquement si le disque dur se trouve dans les locaux professionnels (facteur géolocalisation ou balise de proximité), aux heures de travail autorisées (facteur temporel), si l'utilisateur a son téléphone avec lui et si l'utilisateur a entré son mot de passe.

Avantageusement et selon l'invention, le dispositif de communication sans-fil courte portée est un dispositif de communication sans-fil en champ proche, et l'unité d'administration et l'unité utilisateur sont adaptées pour fournir une énergie électrique au module de récolte d'énergie électrique du dispositif de communication sans-fil en champ proche pour alimenter l'unité de contrôle d'accès.

Selon cet aspect de l'invention, la communication sans-fil entre l'unité d'administration et le dispositif de communication sans-fil ou entre l'unité utilisateur et le dispositif de communication sans-fil sont des communications en champ proche, de type NFC (pour *Near Field Communication* en anglais). Les communications en champ proche permettent d'augmenter la sécurité du système de contrôle d'accès, le pré-paramétrage par l'unité d'administration et la tentative de connexion par l'unité utilisateur devant se faire à proximité directe, inférieure à 20cm. En outre, l'unité d'administration et l'unité utilisateur apportent l'énergie électrique nécessaire pour alimenter l'unité de contrôle d'accès lorsqu'elles sont utilisées. Ainsi, l'unité de contrôle peut ne pas être alimentée lorsqu'elle n'est pas utilisée, la rendant notamment invisible en termes de rayonnements électromagnétiques. L'unité de contrôle peut ainsi être

dissimulée et donc moins facilement détectable aux utilisateurs non informés de sa localisation.

Avantageusement et selon l'invention, l'unité de contrôle d'accès comprend au moins un commutateur pilotable configuré pour ouvrir ou fermer une alimentation électrique du dispositif protégé, indépendante de l'unité de contrôle, l'alimentation étant par défaut fermée et étant ouverte en cas de réception d'une autorisation d'accès provenant du module de vérification.

Selon cet aspect de l'invention, l'alimentation en énergie électrique du dispositif protégé est aussi contrôlée par le système de contrôle d'accès. Si l'accès n'est pas autorisé, l'alimentation est fermée et le dispositif protégé est ainsi moins visible et l'accès au contenu du dispositif sans autorisation est plus difficile.

Avantageusement, un système selon l'invention comprend une balise de proximité, externe à l'unité de contrôle, comprenant un générateur aléatoire de clé adapté pour générer périodiquement une clé de proximité et transmettre la clé de proximité à l'unité de contrôle par un protocole de communication sans-fil, ladite balise de proximité et ladite unité de contrôle étant préalablement appairées par l'unité d'administration.

Selon cet aspect de l'invention, la balise de proximité permet de savoir si le dispositif protégé est localisé dans une zone précise (dans la portée de la balise de proximité) ou en dehors de cette zone (hors de portée de la balise de proximité). La localisation du dispositif protégé par la balise de proximité permet de ne pas être tributaire d'informations de géolocalisation fournies par un utilisateur, qui peuvent être truquées. La balise de proximité peut en outre être dissimulée, l'accès au dispositif protégé étant ainsi tributaire de la balise de proximité, mais sans que l'utilisateur ne soit au courant de la nécessité de cette balise de proximité.

La clé de proximité transmise à l'unité de contrôle d'accès fait partie des clés dont on vérifie les critères de validité. La présence (ou l'absence) de cette clé de proximité peut alors être un facteur d'authentification vérifié par le module de vérification des facteurs de l'unité de contrôle d'accès.

L'invention concerne également un support de stockage de données, comprenant au moins deux mémoires protégées distinctes, caractérisé en ce que l'accès à chaque mémoire protégée est contrôlé par un système de contrôle d'accès selon l'invention.

Un support de stockage selon l'invention permet de faire cohabiter des mémoires indépendantes dans un même équipement et de leur appliquer des facteurs d'authentification différents, permettant ainsi de disposer de mémoires pouvant contenir des informations n'ayant pas vocation à être utilisées simultanément, ou ne pouvant être utilisées qu'à certaines conditions.

L'invention concerne également un procédé de contrôle d'accès à un dispositif protégé par un système de contrôle d'accès selon l'invention, caractérisé en ce qu'il comprend :

- une étape de pré-paramétrage des facteurs d'authentification par un administrateur à l'aide de l'unité d'administration,
- une étape de transmission d'au moins une clé par un utilisateur à l'aide de l'unité utilisateur,
- une étape d'ouverture du chemin d'accès au dispositif protégé si l'ensemble des facteurs d'authentification sont déverrouillés.

Avantageusement, un procédé selon l'invention comprend :

- une étape d'envoi d'une requête par l'utilisateur via l'unité utilisateur, vers l'unité d'administration,
- une étape de validation manuelle par l'administrateur de la requête via l'unité d'administration,
- une étape de transmission d'une clé de validation par l'unité d'administration à l'unité utilisateur, si la requête est validée par l'administrateur.

Selon cet aspect de l'invention, l'administrateur effectue une validation manuelle de la requête de l'utilisateur, sans traitement automatique, permettant

d'accentuer la sécurité du système en autorisant uniquement les utilisateurs approuvés par l'administrateur à accéder au dispositif protégé.

L'invention concerne également un système de contrôle d'accès, un support de stockage et un procédé de contrôle d'accès caractérisé en combinaison par tout ou partie des caractéristiques mentionnées ci-dessus ou ci-après.

5. Liste des figures

D'autres buts, caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante donnée à titre uniquement non limitatif et qui se réfère aux figures annexées dans lesquelles :

- la figure 1 est une vue schématique d'un système de contrôle d'accès à un dispositif protégé selon un mode de réalisation de l'invention,
- la figure 2 est une vue schématique d'un support de stockage protégé par un système de contrôle d'accès selon un mode de réalisation de l'invention.

6. Description détaillée d'un mode de réalisation de l'invention

Les réalisations suivantes sont des exemples. Bien que la description se réfère à un ou plusieurs modes de réalisation, ceci ne signifie pas nécessairement que chaque référence concerne le même mode de réalisation, ou que les caractéristiques s'appliquent seulement à un seul mode de réalisation. De simples caractéristiques de différents modes de réalisation peuvent également être combinées pour fournir d'autres réalisations. Sur les figures, les échelles et les proportions ne sont pas strictement respectées et ce, à des fins d'illustration et de clarté.

La figure 1 représente schématiquement un système 10 de contrôle d'accès selon un mode de réalisation de l'invention.

Le système 10 de contrôle comprend une unité 12 de contrôle d'accès, une unité 14 d'administration et une unité 16 utilisateur.

L'objectif du système de contrôle d'accès est de contrôler l'accès à un dispositif 18 protégé, par exemple un support de stockage, une mémoire d'un support de stockage, un véhicule en libre-service moyennant autorisation préalable, une porte d'accès, etc.

Le dispositif 18 est protégé par au moins un facteur d'authentification pré-paramétré. Le système 10 permet de contrôler la validité de clés qui lui sont présentées en fonction de chaque facteur d'authentification : un facteur d'authentification est dans un état déverrouillé si une clé qui lui est présentée répond aux critères de validité, et dans un état dit verrouillé si aucune clé qui lui est présentée ne répond aux critères de validité. Par exemple, un facteur d'authentification peut être qu'un mot de passe présenté corresponde à un mot de passe défini. Si le mot de passe présenté est identique au mot de passe défini, le facteur d'authentification est dans l'état déverrouillé.

Le dispositif 18 est protégé généralement par une pluralité de facteurs d'authentification pré-paramétrés, et l'accès au dispositif 18 protégé n'est permis qu'en cas de déverrouillage de l'ensemble des facteurs d'authentification.

Pour ce faire, l'unité 12 de contrôle d'accès comprend :

- un dispositif 20 de communication sans-fil courte portée, comprenant un module 22 de transmission sans-fil de données et un module 24 de récolte d'énergie électrique,
- un module 26 de réception de clés,
- un module 28 de vérification des facteurs,
- au moins un chemin 30 d'accès au dispositif protégé,
- au moins un commutateur pilotable, ici un premier commutateur 32a pilotable et un deuxième commutateur 32b pilotable, réunis dans un module 34 de commutation.

Dans tout le texte, on désigne par module, un élément logiciel, un sous-ensemble d'un programme logiciel, pouvant être compilé séparément, soit pour une utilisation indépendante, soit pour être assemblé avec d'autres modules d'un programme, ou un élément matériel, ou une combinaison d'un élément matériel et d'un sous-programme logiciel. Un tel élément matériel peut comprendre un circuit intégré propre à une application (plus connue sous l'acronyme ASIC pour la dénomination anglaise *Application-Specific Integrated Circuit*) ou un circuit logique programmable (plus connu sous l'acronyme FPGA pour la dénomination anglaise *Field-Programmable Gate Array)* ou un circuit de microprocesseurs spécialisés (plus connu sous l'acronyme

DSP pour la dénomination anglaise *Digital Signal Processor*) ou tout matériel équivalent. D'une manière générale, un module est donc un élément (logiciel et/ou matériel) qui permet d'assurer une fonction.

Le module 26 de réception de clés permet la réception d'une clé ou plusieurs clés transmises par différents éléments, par exemple l'unité 16 utilisateur, un ou plusieurs capteurs 36 externes, une balise 38 de proximité via un module 40 de réception sans-fil, etc.

L'ensemble des clés reçues sont transmises au module 28 de vérification des facteurs, qui vérifie la validité de chaque facteur d'authentification, c'est-à-dire vérifie si au moins une clé transmise valide les critères de chaque facteur d'authentification. Pour cette vérification, le module 28 de vérification a accès à une mémoire 42 sécurisée comprenant les facteurs d'authentification pré-paramétrés et les critères associés.

Les transmissions des clés jusqu'au module 28 de vérification des facteurs s'effectuent de manière chiffrée, le déchiffrement des clés se faisant uniquement au module 28 de vérification des clés (par un microprogramme de déchiffrement), pour davantage de sécurité. Le module 28 de vérification des clés et la mémoire 42 sécurisée sont de préférence réunis dans un même composant sécurisé, afin que les clés déchiffrées ne soient pas accessibles en dehors de ce composant.

Si l'ensemble des facteurs d'authentification sont déverrouillés suite à leur vérification, le module 28 de vérification de clé fournit une autorisation d'accès, transmise au module 34 de commutation.

L'autorisation d'accès au dispositif 18 protégé entraine la commutation des commutateurs liés au dispositif 18 protégé : le premier commutateur 32a pilotable est électriquement fermé de façon à ouvrir le chemin 30 d'accès au dispositif 18 protégé en cas de réception d'une autorisation d'accès, ou électriquement ouvert de façon à fermer le chemin 30 d'accès si aucune autorisation n'est reçue (donc par défaut). En outre, le deuxième commutateur 32b pilotable peut aussi être activé en même temps que le premier commutateur 32a pilotable, ce deuxième commutateur 32b étant relié à une alimentation 44 électrique du dispositif 18 protégé : de façon analogue, le deuxième commutateur 32b est électriquement fermé de façon à alimenter le dispositif 18 protégé en cas de réception d'une autorisation d'accès, ou électriquement ouvert de

façon à bloquer l'alimentation 44 du dispositif 18 protégé si aucune autorisation d'accès n'est reçue.

Ainsi, sans autorisation d'accès, le dispositif 18 protégé n'est ni accessible, ni alimenté. Si ce dispositif 18 protégé est une mémoire, il est impossible d'échanger des données avec cette mémoire, ni d'accéder aux données, et la mémoire n'est pas visible.

L'accès au dispositif 18 protégé est réglementé par un administrateur, permettant de déterminer qui a accès au dispositif 18 protégé et sous quelles conditions. L'utilisateur souhaite accéder au dispositif 18 protégé, et doit donc remplir les conditions fixées par l'administrateur.

L'administrateur pré-paramètre les facteurs d'authentification du dispositif 18 protégé grâce à l'unité 14 d'administration. L'unité 14 d'administration est par exemple un smartphone comprenant un logiciel (ou application) permettant le choix des facteurs d'authentification et le pré-paramétrage de ces facteurs. L'unité 14 d'administration permet la transmission des facteurs d'authentification choisis dans la mémoire sécurisée, via le dispositif 20 de communication sans-fil courte portée. Les données contenant les facteurs d'authentifications (transmises sous forme chiffrée) sont transmises via le module 22 de transmission sans-fil.

Le dispositif 20 de communication sans-fil comprend aussi un module 24 de récolte d'énergie, permettant de récolter de l'énergie de différentes sources (photovoltaïques, cinétiques, thermoélectrique), notamment provenant de l'unité 14 d'administration (par induction électromagnétique). Le module 24 de récolte d'énergie permet d'alimenter l'unité 12 de contrôle d'accès, en particulier tous les modules de l'unité 12 de contrôle d'accès.

Dans ce mode de réalisation, le dispositif 20 de communication sans-fil est un dispositif de communication sans-fil en champ proche, de type NFC. Le module 24 de récolte d'énergie est ainsi adapté pour récolter de l'énergie de l'unité 14 d'administration, afin d'alimenter l'unité 12 de contrôle le temps d'effectuer le pré-paramétrage des facteurs d'authentification.

Une fois les facteurs pré-paramétrés, le dispositif 18 est protégé par les facteurs d'authentification. Notamment, le chemin 30 d'accès au dispositif 18 protégé est fermé

par défaut (et éventuellement le dispositif 18 protégé n'est pas alimenté électriquement).

Lorsqu'un utilisateur souhaite accéder au dispositif 18 protégé, il doit ouvrir le chemin 30 d'accès (et éventuellement l'alimentation 44 électrique) du dispositif 18 protégé. Pour cela, il doit remplir les critères définis par l'ensemble des facteurs d'authentification. Des clés sont reçues par le module 26 de réception de clé, transmises au module 28 de vérification de clés et vérifiées, comme expliqué précédemment. L'utilisateur utilise l'unité 16 utilisateur pour accéder au dispositif 18 protégé. L'unité 16 utilisateur est par exemple un smartphone comprenant un logiciel (ou application) permettant une tentative d'accès au dispositif 18 protégé, et la transmission d'au moins une clé. L'unité 16 utilisateur communique avec le module 22 de transmissions sans-fil du dispositif 20 de communication sans-fil courte portée par un protocole de communication sans-fil courte portée tel que par exemple IEEE 802.15.1 (notamment Bluetooth), IEEE 802.15.11 (notamment Wi-Fi), etc. De manière préférentielle, la communication se fait en champ proche (distance généralement inférieure à 20cm, de préférence inférieure à 10cm) via une technologie telle que le NFC.

Comme l'unité 14 d'administration, l'unité 16 utilisateur peut apporter l'énergie électrique nécessaire au fonctionnement de l'unité 12 de contrôle par induction électromagnétique. Dans certains modes de réalisation, l'unité 12 de contrôle peut n'être fonctionnelle que lorsque qu'une unité 14 d'administration ou une unité 16 utilisateur fournit de l'énergie, et être éteinte le reste du temps, de façon à dissimuler sa présence en réduisant les émissions électromagnétiques.

Au moins une clé reçue est transmise par l'unité 16 utilisateur. Cette clé peut-être une clé vérifiant un facteur simple, par exemple uniquement le fait que l'unité 16 utilisateur est présente et qu'un utilisateur souhaite accéder au dispositif 18 protégé, ou bien un facteur plus complexe, tel qu'un mot de passe entré par l'utilisateur dans l'application de l'unité 16 utilisateur. L'unité 16 utilisateur peut aussi transmettre plusieurs clés, dont certaines indépendamment d'une volonté de l'utilisateur, pour déverrouiller ou verrouiller certains facteurs d'authentification : par exemple, des clés peuvent être des valeurs enregistrées par des capteurs de l'unité 16 utilisateur (capteur de température, gyroscope, géolocalisation, horloge, etc.), ou un numéro

d'identification du téléphone. Par exemple, l'accès au dispositif 18 protégé peut n'être autorisé que si l'utilisateur utilise un téléphone autorisé, que si le téléphone est disposé dans une certaine configuration (posé sur un meuble donc horizontalement par exemple), si la température est comprise dans une certaine plage, etc.

De même, lors d'une tentative d'accès au dispositif 18 protégé par un utilisateur, le module 26 de réception de clé peut recevoir des clés provenant des capteurs 36 externes. Les clés peuvent être des valeurs enregistrées par les capteurs 36 externes (capteur de température, gyroscope, géolocalisation, horloge, capteur de fumées, capteur chimique, etc.). Par exemple, l'accès au dispositif 18 protégé peut être interdit en dehors de plages horaires prédéterminées, si l'utilisateur a dépassé un temps maximum de connexion, si le dispositif 18 protégé n'est pas dans une disposition particulière ; une porte d'accès peut ne pas être déverrouillée si un capteur chimique détecte une présence anormale d'un composant chimique dans la salle à laquelle la porte donne accès, etc.

Une clé fournie par l'unité 16 utilisateur peut aussi être fournie par un administrateur, via l'unité 14 d'administration. Pour obtenir cette clé, l'utilisateur envoie une requête via l'unité 16 utilisateur, vers l'unité 14 d'administration. Cette requête est par exemple envoyée par SMS (pour *Short Messaging Service* en anglais) depuis l'application de l'unité 16 utilisateur. L'administrateur reçoit la requête sur l'unité 14 d'administration, et valide manuellement (ou ne valide pas) la requête. Les critères de validation sont choisis par l'administrateur : par exemple, si un identifiant de l'unité 16 utilisateur (son numéro de téléphone par exemple) appartient à une liste approuvée par l'administrateur, il peut choisir de valider la requête. Si l'administrateur manque d'informations sur l'utilisateur, il peut l'appeler par liaison téléphonique entre l'unité 14 d'administration et l'unité 16 utilisateur avant de décider de valider ou non la requête. Une fois la requête validée par l'administrateur, l'unité 14 d'administration envoie une clé à l'unité 16 utilisateur, lui permettant de déverrouiller au moins un facteur d'authentification. La clé peut être paramétrée, par exemple valable uniquement pendant un intervalle de temps spécifique ou selon la géolocalisation de l'unité 16 utilisateur ou du dispositif 18 protégé.

Dans ce mode de réalisation, le module de réception de clé peut aussi recevoir

des clés d'une balise 38 de proximité, via le module 40 de réception sans-fil de l'unité 12 de contrôle. Cette balise 38 de proximité envoie en permanence une clé générée aléatoirement (et chiffrée), dite clé de proximité. Lors du pré-paramétrage, l'unité 14 administrateur peut appairer l'unité 12 de contrôle et la balise 38 de proximité, de sorte que l'unité 12 de contrôle considère la réception de la clé de proximité provenant de la balise 38 de proximité comme un des facteurs d'authentification.

La balise 38 de proximité communique via un protocole de communication sans-fil courte portée, qui peut être identique ou différent du protocole de communication entre l'unité 16 utilisateur et le dispositif 20 de communication sans-fil. Si les deux protocoles de communication sont différents, l'interception de la ou des clés fournies par l'utilisateur et de la clé de proximité émise par la balise 38 de proximité est complexifiée, car il faut récupérer des trames de deux protocoles différents.

En outre, la balise 38 de proximité est généralement cachée de l'utilisateur, et permet de s'assurer de la présence de l'utilisateur à proximité de cette balise 38 (dans la distance permise par la communication sans-fil courte portée). Par exemple, une balise 38 de proximité dissimulée dans un local professionnel permet de s'assurer que l'accès au dispositif 18 protégé, par exemple un support de stockage, n'est possible que lorsque le support de stockage est à proximité de la balise 38 de proximité, et donc dans le local professionnel. L'utilisateur peut ne pas savoir que sa proximité avec la balise 38 de proximité est une condition du déverrouillage du support de stockage, ce qui permet d'accroitre la protection aux intrusions.

Le facteur d'authentification peut aussi être exclusif, c'est-à-dire que l'accès au dispositif est autorisé si une clé n'est pas dans une valeur précise ou si une clé n'est pas reçue. Notamment, dans l'exemple de la balise 38 de proximité dans un local professionnel, l'accès à un dispositif 18 protégé, par exemple un support de stockage comprenant des données personnelles, peut être verrouillé si le dispositif 18 protégé est à proximité de la balise 38 de proximité et donc dans le local professionnel. Le critère ainsi défini par le facteur d'authentification est la non-réception d'une clé provenant de la balise 38 de proximité.

Une application de cet exemple est présentée plus en détail en référence avec la figure 2, représentant schématiquement un support 45 de stockage protégé par un

système de contrôle d'accès selon un mode de réalisation de l'invention.

En particulier, le support 45 de stockage comprend deux mémoires protégées, distinctes, indépendantes et séparées (dans des composants différents), une première mémoire 46a protégée et une deuxième mémoire 46b protégée.

Le support 45 de stockage comprend un connecteur, ici un connecteur 48 USB (pour *Universal Serial Bus* en anglais), permettant, grâce à une pluralité de broches (non représentées), de transmettre des données via un bus 50 de transmission de données et d'alimenter le support 45 de stockage avec une alimentation 44 électrique. Le support 45 de stockage peut être par exemple une clé USB ou un disque dur externe, branchée sur un ordinateur grâce au connecteur 48 USB. Le support 45 de stockage peut aussi être un disque dur interne d'un ordinateur, branché directement à l'intérieur de l'ordinateur via un connecteur spécifique.

Le support 45 de stockage comprend une unité 12 de contrôle du système de contrôle d'accès, telle que décrite précédemment en référence avec la figure 1. Les interactions avec l'unité 12 de contrôle s'effectuent, comme décrit précédemment, grâce à une unité 14 d'administration (pour le pré-paramétrage) et une unité 16 utilisateur (pour la tentative d'accès).

L'unité 12 de contrôle permet de contrôler l'accès aux deux mémoires protégées et leur alimentation. Chaque mémoire protégée peut être considérée comme un dispositif protégé par le système de contrôle d'accès. L'accès à chaque mémoire protégée contrôlée est régi par un ensemble de facteurs d'authentification propre à chaque mémoire protégée. Pour ce faire, l'unité 12 de contrôle comprend des commutateurs pilotables réunis dans un module 34 de commutation, ici :

- un premier commutateur 32a pilotable et un deuxième commutateur 32b pilotable, permettant d'ouvrir/fermer respectivement l'accès aux données de la première mémoire 46a protégée et l'alimentation de la première mémoire 46a protégée,
- un troisième commutateur 32c pilotable et un quatrième commutateur 32d pilotable, permettant d'ouvrir/fermer respectivement l'accès aux données de la deuxième mémoire 46b protégée et l'alimentation de la deuxième mémoire 46b protégée.

Les commutateurs pilotables sont pilotés en fonction de la réception ou non d'une autorisation d'accès, comme décrit précédemment.

Un tel support 45 de stockage est particulièrement adapté pour une application professionnelle et personnelle, ou pour de la dissimulation de données.

Dans l'application professionnelle et personnelle, la première mémoire 46a protégée est par exemple une mémoire dédiée à des données personnelles, et la deuxième mémoire 46b protégée est dédiée à des données professionnelles. Lorsque l'utilisateur est en dehors des locaux professionnels, il est autorisé à accéder uniquement à la première mémoire 46a protégée. Lorsque l'utilisateur est dans les locaux professionnels, une balise 38 de proximité telle que décrite précédemment permet d'autoriser l'accès de la deuxième mémoire 46b protégée et de bloquer l'accès à la première mémoire 46a protégée, permettant ainsi de s'assurer que des données personnelles ne sont jamais accessibles dans le milieu professionnel et que les données professionnelles ne sont jamais accessibles dans le milieu personnel. Si les mémoires protégées comprennent chacune un système d'exploitation, il est possible d'utiliser deux systèmes d'exploitation différents et totalement séparés (un système n'ayant pas accès aux données de l'autre système), ce qui est particulièrement utile pour les pratiques dites de BYOD (*Bring Your Own Device* en anglais, soit « apportez votre appareil personnel ») ou COPE (*Corporate Owned, Personally Enabled* en anglais, soit « appartient à l'entreprise, autorisé en privé ») dans lesquels la même machine peut ainsi être utilisée pour des raisons personnelles ou professionnelles sans risques accrus de sécurité.

Dans l'application de dissimulation de données, une première mémoire 46a protégée peut comprendre des données quelconques et être accessible par défaut. Une deuxième mémoire 46b protégée comprend des données confidentielles, et n'est accessible et visible qu'en validant les critères des facteurs d'authentification. Ainsi, si le support de stockage est branché à un ordinateur pour en vérifier le contenu, seule la première mémoire 46a protégée sera accessible et visible, ce qui attire moins l'attention que si aucune mémoire n'était accessible ou visible. La deuxième mémoire 46b protégée n'est donc pas vérifiée car non visible.

REVENDICATIONS

1. Système de contrôle d'accès à un dispositif (18) protégé par au moins un facteur d'authentification pré-paramétré, chaque facteur d'authentification définissant au moins un critère de validité d'une clé et étant dans un état dit déverrouillé si une clé qui lui est présentée répond aux critères de validité, et un état dit verrouillé si aucune clé qui lui est présentée ne répond aux critères de validité, comprenant :

- une unité (12) de contrôle d'accès comprenant :
  - un dispositif (20) de communication sans-fil courte portée, comprenant un module (22) de transmission sans-fil de données et un module (24) de récolte d'énergie électrique,
  - un module (26) de réception de clés, adapté pour recevoir au moins une clé,
  - un module (28) de vérification des facteurs, adapté pour vérifier la validité de chaque facteur d'authentification pré-paramétré avec au moins une clé reçue par le module (26) de réception de clé et fournir une autorisation d'accès si l'ensemble des facteurs d'authentification sont dans l'état déverrouillé,
  - au moins un chemin (30) d'accès, adapté pour permettre l'accès au dispositif (18) protégé,
  - au moins un commutateur (32a, 32c) pilotable, configuré pour ouvrir ou fermer le chemin (30) d'accès au dispositif (18) protégé, le chemin (30) d'accès étant par défaut fermé et étant ouvert en cas de réception d'une autorisation d'accès provenant du module (28) de vérification,
- une unité (14) d'administration, adaptée pour permettre de pré-paramétrer chaque facteur d'authentification par interaction avec le module (22) de transmission sans-fil de données du dispositif (20) de communication de l'unité (12) de contrôle d'accès,
- une unité (16) utilisateur, configurée pour transmettre au moins une clé au module (26) de réception de clés, via le module (22) de transmission

sans-fil de données.

2. Système de contrôle selon la revendication 1, caractérisé en ce que chaque facteur d'authentification définit au moins un critère de validité d'une clé choisie dans le groupe comprenant les clés suivantes :

- mot de passe,
- clé transmise par l'unité (14) d'administration,
- données de géolocalisation du dispositif (18) protégé et/ou de l'unité (16) utilisateur,
- valeurs mesurées par un ou plusieurs capteurs électroniques,
- données temporelles,
- clé provenant d'une balise (38) de proximité.

3. Système de contrôle selon l'une des revendications 1 ou 2, caractérisé en ce que le dispositif (20) de communication sans-fil courte portée est un dispositif de communication sans-fil en champ proche, et en ce que l'unité (14) d'administration et l'unité (16) utilisateur sont adaptées pour fournir une énergie électrique au module (24) de récolte d'énergie électrique du dispositif (20) de communication sans-fil en champ proche pour alimenter l'unité (12) de contrôle d'accès.

4. Système de contrôle selon l'une des revendications 1 à 3, caractérisé en ce que l'unité (12) de contrôle d'accès comprend au moins un commutateur (32b, 32d) pilotable configuré pour ouvrir ou fermer une alimentation (44, 44a, 44b) électrique du dispositif (18) protégé, indépendante de l'unité (12) de contrôle, l'alimentation (44, 44a, 44b) étant par défaut fermée et étant ouverte en cas de réception d'une autorisation d'accès provenant du module (28) de vérification.

5. Système de contrôle selon l'une des revendications 1 à 4, caractérisé en ce qu'il comprend une balise (38) de proximité, externe à l'unité (12) de contrôle, comprenant un générateur aléatoire de clé adapté pour générer périodiquement une clé de proximité et transmettre la clé de proximité à l'unité (12) de contrôle par un protocole

de communication sans-fil, ladite balise (38) de proximité et ladite unité (12) de contrôle étant préalablement appairées par l'unité (14) d'administration.

6. Support de stockage de données, comprenant au moins deux mémoires (46a, 46b) protégées distinctes, caractérisé en ce que l'accès à chaque mémoire (46a, 46b) protégée est contrôlé par un système (10) de contrôle d'accès selon l'une des revendications 1 à 5.

7. Procédé de contrôle d'accès à un dispositif (18) protégé par un système (10) de contrôle d'accès selon l'une des revendications 1 à 5, caractérisé en ce qu'il comprend :

- une étape de pré-paramétrage des facteurs d'authentification par un administrateur à l'aide de l'unité (14) d'administration,
- une étape de transmission d'au moins une clé par un utilisateur à l'aide de l'unité (16) utilisateur,
- une étape d'ouverture du chemin (30) d'accès au dispositif (18) protégé si l'ensemble des facteurs d'authentification sont déverrouillés.

8. Procédé de contrôle d'accès selon la revendication 7, caractérisé en ce qu'il comprend :

- une étape d'envoi d'une requête par l'utilisateur via l'unité (16) utilisateur, vers l'unité (14) d'administration,
- une étape de validation manuelle par l'administrateur de la requête via l'unité (14) d'administration,
- une étape de transmission d'une clé de validation par l'unité (14) d'administration à l'unité (16) utilisateur, si la requête est validée par l'administrateur.

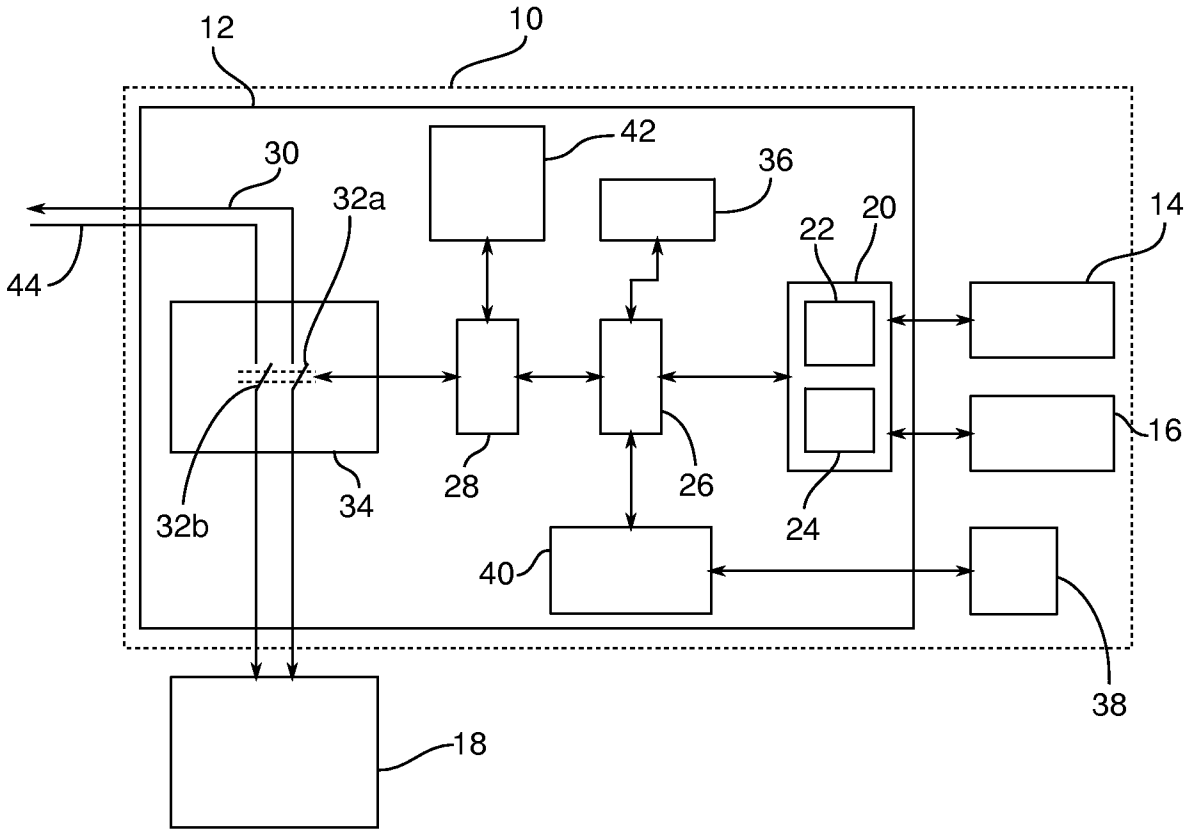
12
10
42
30
36
32a
20
14
22
44
32b
34
28
26
24
16
40
38
18

Fig. 1

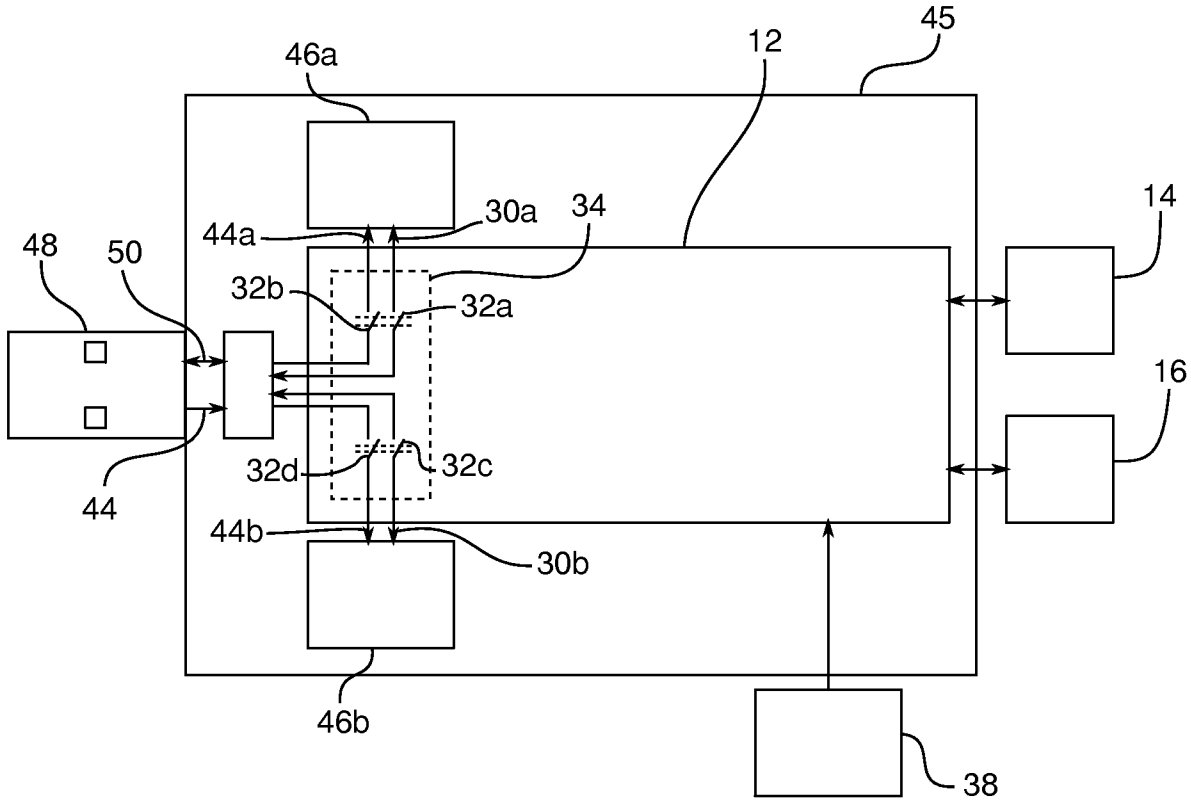
46a
12
45
14
30a
34
44a
48
50
32b
32a
16
32d
32c
44
44b
30b
46b
38

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/050139

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/35 G06F21/79 G06F21/81 G06F21/88
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/098134 A1 (VAN ACHT VICTOR MARTINUS [NL] ET AL) 24 April 2008 (2008-04-24)	1-4,6-8
Y	paragraphs [0016] - [0017], [0044] - [0046], [0048], [0051], [0052], [0058]; figures 1,2	5
Y	US 9 177 453 B2 (GILL ABRAHAM [IL] ET AL) 3 November 2015 (2015-11-03) column 7, line 49 - column 8, line 24	5
Y	US 2014/283018 A1 (DADU SAURABH [US] ET AL) 18 September 2014 (2014-09-18) paragraphs [0018], [0026] - [0029]	5

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

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 April 2017	04/05/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veillas, Erik

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2017/050139

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008098134 A1	24-04-2008	CN 101010677 A	01-08-2007
		EP 1805685 A1	11-07-2007
		JP 2008512738 A	24-04-2008
		US 2008098134 A1	24-04-2008
		WO 2006027723 A1	16-03-2006
US 9177453 B2	03-11-2015	US 2009182931 A1	16-07-2009
		US 2016055353 A1	25-02-2016
		WO 2007020650 A2	22-02-2007
US 2014283018 A1	18-09-2014	US 2014283018 A1	18-09-2014
		US 2016335438 A1	17-11-2016
		WO 2014142960 A1	18-09-2014

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2017/050139

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/35 G06F21/79 G06F21/81 G06F21/88
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2008/098134 A1 (VAN ACHT VICTOR MARTINUS [NL] ET AL) 24 avril 2008 (2008-04-24)	1-4,6-8
Y	alinéas [0016] - [0017], [0044] - [0046], [0048], [0051], [0052], [0058]; figures 1,2	5
Y	US 9 177 453 B2 (GILL ABRAHAM [IL] ET AL) 3 novembre 2015 (2015-11-03) colonne 7, ligne 49 - colonne 8, ligne 24	5
Y	US 2014/283018 A1 (DADU SAURABH [US] ET AL) 18 septembre 2014 (2014-09-18) alinéas [0018], [0026] - [0029]	5

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

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
24 avril 2017	04/05/2017

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Veillas, Erik

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2017/050139

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2008098134 A1	24-04-2008	CN 101010677 A	01-08-2007
		EP 1805685 A1	11-07-2007
		JP 2008512738 A	24-04-2008
		US 2008098134 A1	24-04-2008
		WO 2006027723 A1	16-03-2006
US 9177453 B2	03-11-2015	US 2009182931 A1	16-07-2009
		US 2016055353 A1	25-02-2016
		WO 2007020650 A2	22-02-2007
US 2014283018 A1	18-09-2014	US 2014283018 A1	18-09-2014
		US 2016335438 A1	17-11-2016
		WO 2014142960 A1	18-09-2014