(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 028 335***

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

(21) **N° d'enregistrement national :** **14 60907**

(51) Int Cl[8] : ***G 06 F 21/60*** *(2016.01), H 04 L 29/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 12.11.14.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 13.05.16 Bulletin 16/19.

(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 :** Polynésie-Fr

(71) **Demandeur(s) :** *GHAVAMIAN CHARLES SHAHROKH* — FR.

(72) **Inventeur(s) :** GHAVAMIAN CHARLES SHAHROKH.

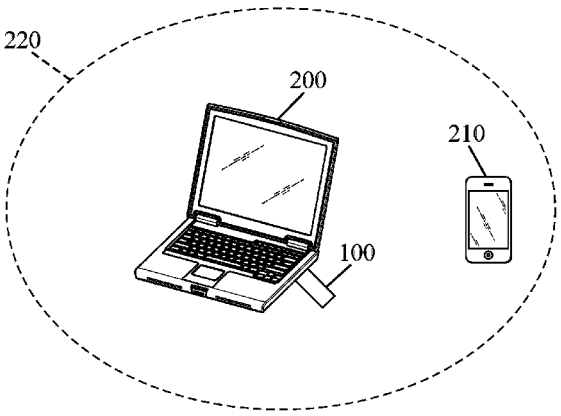
(73) **Titulaire(s) :** GHAVAMIAN CHARLES SHAHROKH.

(74) **Mandataire(s) :** CABINET PLASSERAUD.

(54) PERIPHERIQUE DE STOCKAGE DE DONNEES AVEC GESTION D'ACCES SECURISE ET PROCEDE DE GESTION D'ACCES ASSOCIE.

(57) L'invention concerne un procédé et un périphérique de stockage de données dont l'accès est contrôlé de manière sécurisée, le périphérique (100) comportant au moins :

- une interface de connexion (110) apte à être connectée à un système informatique (200) ;
- une mémoire (112) configurée pour stocker des données ;
- un module de communication (114) sans-fil apte à communiquer avec au moins un équipement électronique (210) ;
- un module de gestion (116) configuré pour autoriser l'accès du système informatique à au moins une partie des données stockées dans la mémoire uniquement lorsqu'une communication est établie entre le module de communication et l'équipement électronique.



FR 3 028 335 - A1

Périphérique de stockage de données avec gestion d'accès sécurisé et procédé de gestion d'accès associé.

[001] Domaine technique

[002] L'invention concerne le domaine de l'accès sécurisé à des données numériques stockées dans un périphérique, et notamment celui du contrôle d'accès à de telles données en fonction de la présence ou non de l'utilisateur à proximité du périphérique.

[003] Etat de la technique

[004] Les périphériques de stockage de données sont des supports physiques très populaires pour conserver, transporter et transférer des données numériques. Ces périphériques peuvent être par exemple :

- une clé USB ;
- une carte mémoire de type carte SD ;
- un disque dur externe.

[005] Ces moyens de stockage ont pour avantages d'être amovibles, facilement transportables par leur utilisateur et lisibles par les nombreux systèmes informatiques qui disposent de ports de connexion adaptés (comme un port USB ou un lecteur de carte mémoire par exemple). Il est ainsi possible à un utilisateur d'enregistrer des données sur son périphérique de stockage en vue de pouvoir y accéder ultérieurement sur un autre poste informatique (lors d'une réunion à l'extérieur typiquement).

[006] Les données qui sont enregistrées dans le périphérique peuvent être privées, voire hautement confidentielles. Dans ce cas de figure, il n'est évidemment pas souhaitable que ces données sensibles puissent être consultées par des tiers sans autorisation de l'utilisateur.

[007] Or, lorsque l'utilisateur n'est pas physiquement à proximité de son périphérique, il ne peut pas s'assurer des personnes qui l'utilisent. De fait, des personnes peuvent consulter les données sensibles en question, et ce à l'insu de l'utilisateur. De telles situations ne sont pas souhaitables et peuvent pourtant se

présenter régulièrement, par exemple lorsque l'utilisateur prête son périphérique de stockage à un tiers, ou en cas d'oubli, de perte voire de vol du périphérique.

[008] Les données enregistrées sur un périphérique de stockage sont donc vulnérables. Il existe donc un besoin de sécuriser les données stockées sur ce type de périphérique, et tout particulièrement les données sensibles, lorsque l'utilisateur n'est pas en mesure de s'assurer des personnes qui utilisent son périphérique.

[009] L'invention vient améliorer la situation en ce sens.

[010] Résumé de l'invention

[011] L'objet de l'invention est de remédier aux inconvénients précités en proposant notamment de contrôler l'accès aux données que contient un périphérique de stockage en fonction de la présence d'un équipement électronique personnel de l'utilisateur à proximité du périphérique.

[012] A cet effet, un premier aspect de l'invention concerne un périphérique de stockage de données comportant au moins :

- une interface de connexion apte à être connectée à un système informatique ;
- une mémoire configurée pour stocker des données ;
- un module de communication sans-fil apte à communiquer avec au moins un équipement électronique ;
- un module de gestion configuré pour autoriser l'accès du système informatique à au moins une partie des données stockées dans la mémoire uniquement lorsqu'une communication est établie entre le module de communication et l'équipement électronique.

[013] L'au moins un équipement électronique peut plus particulièrement être un équipement mobile et personnel de l'utilisateur du périphérique de stockage, comme son téléphone portable (de type Smartphone par exemple), une montre connectée, une tablette numérique, ou autre. Ce type d'équipement est porté ou transporté par l'utilisateur. Leur localisation habituelle est donc sensiblement la même que celle de l'utilisateur.

[014] En outre, ces équipements sont aptes à communiquer via des protocoles de communication sans-fil. Préférentiellement, les protocoles de communication utilisés sont des protocoles qui permettent des échanges de données seulement à une courte distance. On entend par courte distance une distance entre l'équipement électronique et le périphérique inférieure ou égale à 100 mètres par exemple. Les protocoles de communication utilisés peuvent notamment être de type Bluetooth, infrarouge (IrDa, pour « *Infrared Data Association* » en langue anglaise), Wi-Fi, en champ proche (en anglais « *Near Field Communication* », NFC), ou autre. A titre purement illustratif, la communication entre l'équipement et le informatique peut être établie pour une distance allant jusqu'à :

- 100 mètres lorsque le protocole de communication utilisé est de type Bluetooth,
- 50 mètres lorsque le protocole de communication utilisé est de type Wi-Fi,
- 10 centimètres lorsque le protocole de communication utilisé est de type en champ proche.

[015] Aussi, quand le module de communication du périphérique est en communication avec l'équipement électronique, cet équipement est à proximité du périphérique (i.e. à la portée d'émission radiofréquence du module de communication), et donc de l'utilisateur qui porte ou transporte l'équipement.

[016] Il est ainsi possible d'autoriser l'accès à des données du périphérique seulement lorsque l'utilisateur est à proximité du périphérique et qu'il peut s'assurer de l'usage qui est fait des données stockées.

[017] Le système informatique peut être un ordinateur portable ou tout autre système informatique adapté pour lire/écrire des données stockées sur un périphérique de stockage : poste informatique fixe, tablette numérique, écran de télévision, lecteur DVD, chaine Hi-Fi ou autre.

[018] Les données auxquelles le module de gestion autorise l'accès peuvent être :

- l'intégralité des données stockées dans la mémoire du périphérique ;

- une partie seulement des données, par exemple une partition de données sélectionnée par l'utilisateur (des fichiers confidentielles notamment) ;
- des données déterminées comme étant sensibles, personnelles ou confidentielles.

[019] Avantageusement, la mémoire du périphérique peut contenir une liste d'identifiants d'équipements électroniques autorisés à communiquer avec le module de communication, le module de communication étant configuré pour ne communiquer qu'avec des équipements électroniques dont l'identifiant est compris dans ladite liste.

[020] Cette liste d'identifiants d'équipements électroniques permet d'établir une communication seulement avec des équipements personnels de l'utilisateur qui ont été configurés et/ou authentifiés auprès du périphérique par l'utilisateur (par exemple via une procédure d'appairage effectuée au préalable entre l'équipement et le périphérique).

[021] Selon une réalisation avantageuse, la mémoire du périphérique peut contenir en outre une clé de chiffrement, le module de gestion étant configuré pour chiffrer selon ladite clé de chiffrement l'au moins une partie des données à laquelle le module de gestion autorise l'accès.

[022] Ainsi, les données sensibles, la partition de données à protéger, voire l'intégralité des données du périphérique peuvent être protégées. Si le module de gestion ne fournit pas la clé de chiffrement à un système informatique, ou ne déchiffre pas les données selon cette clé, le système informatique ne peut pas lire les données stockées dans la mémoire. Cette réalisation permet donc d'empêcher la lecture des données à des tiers malveillants sans autorisation du module de gestion.

[023] Selon une réalisation avantageuse, le périphérique peut comprendre en outre un module de sécurité apte à détecter une tentative d'accès non-autorisé aux données stockées dans la mémoire, le module de gestion étant configuré pour détruire l'au moins une partie des données stockées dans la mémoire lorsque ladite tentative est détectée par le module de sécurité.

[024] Le module de sécurité peut en l'occurrence être configuré pour détecter une tentative d'attaque malveillante par voie électronique, par exemple en cas de détection

d'activité anormale au niveau de l'interface de connexion. Le module de sécurité peut aussi être adapté pour détecter une atteinte à l'intégrité physique du périphérique comme par exemple une tentative d'ouverture de son enveloppe. Ainsi, en cas de tentative d'accès non-autorisé à l'intégrité des données stockées dans le périphérique, celles-ci sont détruites pour éviter qu'un tiers malveillant ne puisse les consulter, et ce quelles que soient les actions malintentionnées qu'il entreprend.

[025] Avantageusement, le périphérique de stockage de données peut comprendre en outre une batterie, le module de gestion étant configuré pour détruire au moins une partie des données stockées dans la mémoire lorsque le niveau de charge de la batterie est inférieur à un seuil prédéterminé.

[026] En l'occurrence, le seuil prédéterminé peut correspondre à un niveau de batterie faible. De cette manière, lorsque la batterie arrive à un faible niveau de charge, les données dans la mémoire sont rendues inaccessibles (notamment parce que les modules de sécurité et de gestion ne peuvent bientôt plus assurer correctement les mesures de sécurité mises en œuvre quand ils sont convenablement alimentés). Ainsi, un tiers malveillant ne peut consulter les données stockées alors que le périphérique n'a plus de batterie, par exemple si le périphérique est resté longtemps inutilisé.

[027] Cette batterie peut toutefois être rechargée via une alimentation électrique fournie par un système informatique auquel le périphérique est connecté. Cette alimentation peut notamment être fournie via le port de connexion du système informatique auquel le périphérique est connecté.

[028] Typiquement, l'interface de connexion du périphérique peut être un connecteur universel de type USB.

[029] Un deuxième aspect de l'invention concerne un système de gestion d'accès à des données stockées sur le périphérique de stockage précité, dans lequel l'au moins un équipement électronique est configuré pour émettre une alerte à destination d'un utilisateur lorsque la communication établie entre le module de communication et l'équipement électronique est interrompue.

[030] Ainsi, lorsque l'utilisateur n'est plus à proximité de son périphérique, il peut tout de suite être averti par l'équipement qu'il porte ou transporte. Il peut ainsi rapidement récupérer son périphérique en cas d'oubli.

[031] Un troisième aspect de l'invention concerne un procédé de gestion d'accès à des données stockées dans une mémoire d'un périphérique de stockage de données. Le procédé comprend au moins les étapes suivantes, exécutées dans le périphérique de stockage de données :

- vérification qu'une communication sans-fil établie entre un module de communication dudit périphérique et un équipement électronique ;
- autorisation d'accès d'un système informatique à au moins une partie des données stockées dans la mémoire, uniquement lorsque ladite vérification de communication établie est positive.

[032] Le procédé de gestion d'accès peut comprendre en outre les étapes de :

- réception d'un identifiant de l'équipement électronique ;
- comparaison de l'identifiant reçu avec une liste d'identifiants d'équipements électroniques autorisés à communiquer avec le module de communication ;
- mise en communication du module de communication et de l'équipement électronique lorsque l'identifiant reçu est compris dans ladite liste.

[033] Selon une réalisation avantageuse, le procédé peut comprendre aussi une étape de chiffrement de l'au moins une partie des données stockées dans la mémoire du périphérique.

[034] Avantageusement, le procédé peut comprendre en outre une destruction de l'au moins une partie des données stockées dans la mémoire du périphérique lorsqu'une tentative d'accès non-autorisé aux données est détectée.

[035] De manière avantageuse, le procédé peut comprendre la destruction de l'au moins une partie des données stockées dans la mémoire du périphérique lorsque le niveau de charge d'une batterie du périphérique est inférieur à un seuil prédéterminé.

[036] Avantageusement, le procédé peut comprendre en outre une étape d'authentification d'un utilisateur avant d'autoriser l'accès du système informatique à l'au moins une partie des données stockées dans la mémoire.

[037] En complément, lors de l'autorisation d'accès, les données peuvent être rendues accessibles en fonction des droits d'accès associés à l'utilisateur authentifié.

[038] La présente invention vise également un programme informatique comportant des instructions pour la mise en œuvre du procédé précédemment décrit, lorsque ce programme est exécuté par un module de gestion d'un périphérique de stockage de données, tel qu'un microprocesseur.

[039] Ce programme peut utiliser n'importe quel langage de programmation (par exemple, un langage objet ou autre), et être sous la forme d'un code source interprétable, d'un code partiellement compilé ou d'un code totalement compilé.

[040] La figure 4 décrite en détails ci-après, peut former un organigramme de l'algorithme général d'un tel programme informatique.

[041] Brève description des figures

[042] D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des figures annexées sur lesquelles :

- la **figure 1** illustre un exemple de réalisation du périphérique de stockage de données selon l'invention ;
- la **figure 2** illustre un exemple dans lequel le périphérique est connecté à un système informatique et où un équipement électronique d'un utilisateur est à proximité ;
- la **figure 3** illustre un même exemple de périphérique où cette fois l'équipement électronique de l'utilisateur n'est pas à proximité du périphérique connecté ;
- la **figure 4** représente un organigramme composé d'un exemple de succession d'étapes du procédé de gestion d'accès de l'invention.

[043] Pour des raisons de clarté, les dimensions des différents éléments représentés sur ces figures ne sont pas en proportion avec leurs dimensions réelles. Sur les figures,

des références identiques correspondent à des éléments identiques pour les différents modes de réalisation exposés.

[044] Description détaillée

[045] On se réfère tout d'abord à la **figure 1** qui illustre un exemple de réalisation du périphérique de stockage de données dans un mode de réalisation de l'invention. Dans ce mode de réalisation, le périphérique de stockage de données est réalisé sous la forme d'une clé de stockage USB.

[046] Dans ce mode de réalisation, le périphérique 100 comporte :

- une interface de connexion 110 apte à être connectée à un système informatique, l'interface de connexion étant un connecteur USB mâle typiquement ;
- une mémoire 112 configurée pour stocker :
    - des données à enregistrer durablement ;
    - des instructions permettant la mise en œuvre du procédé de gestion d'accès et
    - des données temporaires pour réaliser les différentes étapes du procédé tel que décrit précédemment et détaillé plus loin ;
- un module de communication sans-fil et de courte portée 114 apte à communiquer avec un ou plusieurs équipements électroniques en simultané, comme par exemple un module radiofréquence selon les protocoles de communication Bluetooth, Wi-Fi, IrDa, NFC ou autre ;
- un module de gestion 116 qui peut être un circuit comme par exemple :
    - un processeur ou microprocesseur apte à interpréter des instructions sous la forme de programme informatique, ou
    - une carte électronique dont les étapes du procédé de l'invention sont décrites dans le silicium, ou encore
    - une puce électronique programmable comme une puce FPGA (pour « *Field-Programmable Gate Array* » en anglais).

[047] En l'occurrence, lorsque le module de gestion 116 exécute les instructions stockées dans la mémoire 112, il est alors configuré pour autoriser l'accès du système informatique à au moins une partie des données stockées dans la mémoire uniquement lorsqu'une communication est établie entre le module de communication et l'équipement électronique.

[048] A cet effet, le module de communication comporte une antenne permettant d'établir une communication selon les protocoles précités, et ce dans un périmètre allant jusqu'à une vingtaine de mètres. Pour détecter les équipements électroniques qui sont dans ce périmètre, le module de communication 114 vérifie régulièrement si un équipement électronique autorisé est à portée d'antenne.

[049] Les données auxquelles le module de gestion 116 autorise l'accès peuvent être :

- l'intégralité des données stockées dans la mémoire 112 ;
- une partie seulement des données sélectionnée par l'utilisateur ;
- des données déterminées comme étant sensibles, personnelles ou confidentielles.

[050] En outre, la mémoire 112 contient une liste d'identifiants d'équipements électroniques autorisés à communiquer avec le module de communication. Ces identifiants d'équipements correspondent à des équipements qui ont été autorisés par l'utilisateur à s'associer avec le périphérique en vue d'établir une communication. Cette autorisation peut être mise en œuvre au cours d'une phase préalable de paramétrage du périphérique au cours de laquelle l'utilisateur défini les équipements autorisés à s'appairer avec le périphérique.

[051] La mémoire 112 peut aussi contenir une clé de chiffrement. Cette clé de chiffrement peut être utilisée par le module de gestion 116 pour chiffrer une partie des données stockées dans la mémoire, par exemple les données sensibles, voire l'intégralité des données stockées.

[052] Selon une réalisation possible, le module 116 peut fournir la clé de chiffrement à un système informatique seulement lorsque l'équipement électronique de l'utilisateur est à proximité du périphérique (i.e. en communication avec le périphérique). La clé de

chiffrement récupérée par le système informatique lui permet de déchiffrer les données stockées dans la mémoire 112. Ainsi, les données de la mémoire ne sont lisibles par le système informatique que lorsque l'utilisateur est à proximité du périphérique.

[053] Selon une autre réalisation possible, le module de gestion 116 contrôle l'accès aux données en refusant les requêtes de lecture/écriture du système 200 tant que l'équipement électronique n'est pas en communication avec le périphérique.

[054] En outre, le périphérique comprend un module de sécurité 118 apte à détecter une tentative d'accès non-autorisé aux données stockées dans la mémoire 112. Ce module peut notamment être agencé de manière à détecter une atteinte physique à l'intégrité du périphérique. Par exemple, le module 118 est prévu pour détecter une ouverture d'enveloppe de la clé USB. En complément ou en variante, le module de sécurité 118 peut détecter des attaques informatiques en fonction d'activités anormales remarquées au niveau de l'interface de connexion 110. En cas de tentative d'accès non-autorisé détectée, le module de sécurité 118 envoie un signal d'alerte au module de gestion 116 qui détruit alors les données à protéger de tout accès non-autorisé.

[055] Le périphérique comprend aussi une batterie 120 qui permet d'alimenter les composants électroniques du périphérique lorsque le périphérique ne reçoit pas d'autre alimentation électrique (par exemple via l'interface de connexion 110). La batterie permet ainsi de maintenir le périphérique dans un état de veille nécessaire à la protection des données.

[056] Lorsque l'interface de connexion 110 est un connecteur USB mâle, la batterie 120 peut être rechargée par l'alimentation électrique fournie par le port USB du système informatique. Cette alimentation peut aussi être utilisée pour alimenter directement les modules de gestion 116, de sécurité 118, de communication 118 et la mémoire 112.

[057] Toutefois, si la batterie 120 devient faible, la sécurité des données est mise en péril car les composants électroniques tels que le module de gestion 116 et le module de sécurité 118 s'apprête à ne plus être alimenté en électricité. Le cas échéant, le module de gestion 116 est configuré pour détruire les données stockées, et ce par mesure de précaution afin d'éviter qu'un tiers malveillant puisse *in fine* accéder aux données lorsque la batterie est vide.

[058] Aussi, on comprend que le module de gestion 116 a pour principales fonctions de :

- gérer les accès aux données stockées dans la mémoire 112 ;
- réaliser des opérations de chiffrement/déchiffrement des données stockées ; et
- effacer des données stockées en cas de tentative d'accès non-autorisé (par voie électronique, ou physique avec tentative de démontage du périphérique par exemple).

[059] En outre, comme décrit plus loin, l'autorisation d'accès aux données peut être conditionnée selon au moins l'un des deux paramètres suivants :

- la proximité d'un équipement électronique personnel de l'utilisateur ;
- la saisie d'un code d'authentification lorsque le périphérique est connecté à un système informatique.

[060] Lorsque l'utilisateur est à proximité du périphérique et que son équipement s'est mis en communication avec le module de communication 114, un signal sonore peut être généré de sorte à prévenir l'utilisateur que son équipement électronique personnel est à portée d'antenne du module de communication et que l'accès aux données stockées dans le périphérique est autorisé.

[061] En complément, pour accéder aux données de la mémoire, un code d'authentification peut être demandé à l'utilisateur. Ce code d'authentification peut en outre être mis en correspondance à un niveau de sécurité. Pour ce faire, la mémoire 112 peut comprendre :

- une liste de codes d'authentification autorisés à accéder aux données du périphérique ;
- un niveau de sécurité associé à chacun des codes d'authentification ; et
- un niveau de sécurité en correspondance des données stockées dans la mémoire 112.

[062] Ainsi, lorsque l'utilisateur entre son code, le module de gestion 116 donne accès aux données qui correspondent au même niveau de sécurité que celui du code saisi.

[063] On se réfère maintenant à la **figure 2** sur laquelle est illustré le périphérique 100 connecté au système informatique 200. Cette connexion peut être établie via la connexion entre un connecteur USB femelle du système 200 et du connecteur USB mâle 110 du périphérique 100. Le système informatique 200 peut être un ordinateur portable ou tout autre système informatique adapté pour lire/écrire des données stockées sur un périphérique de stockage : poste informatique fixe, tablette numérique, écran de télévision, lecteur DVD, chaine Hi-Fi ou autre.

[064] Dans cet exemple, l'interface de connexion 110 reçoit une alimentation électrique du système 200, permettant d'alimenter les composants électroniques du périphérique et de recharger la batterie 120.

[065] Dans cet exemple, la portée d'antenne du module de communication 114 est représentée par la zone de détection 220, zone dans laquelle le module de communication 114 peut détecter la présence d'un équipement électronique 210 et établir une communication avec celui-ci si l'équipement 210 est autorisé (équipement dont l'identifiant correspond à l'un des identifiants enregistrés dans la liste d'identifiants contenue dans la mémoire 112).

[066] L'équipement électronique 210 peut notamment être un équipement mobile et personnel de l'utilisateur tel qu'une montre connectée, un téléphone portable, une tablette numérique ou autres équipements mobiles et personnel de l'utilisateur, portable ou transportable par ce dernier, et apte à établir une communication avec le périphérique selon les protocoles susmentionnés (Bluetooth, Wi-Fi, IrDa, NFC, etc.).

[067] Lorsque l'équipement 210 est dans la zone 220, le module de communication 114 détecte sa présence et établit la communication si cet équipement 210 est effectivement autorisé à s'associer avec le périphérique 100. L'utilisateur portant ou transportant l'équipement 210 peut dès lors accéder aux données (si nécessaire, après que l'utilisateur se soit authentifié via son code d'accès).

[068] Tant que le périphérique est alimenté (via l'interface 110 ou par la batterie 120), le module de gestion 116 vérifie régulièrement (par exemple à la fréquence d'une fois toutes les 15 secondes) si le module de communication 114 est toujours en communication avec l'équipement 210. Tant que la communication avec l'équipement 210 est établie (i.e. l'équipement est présent dans la zone 220), l'accès aux données est

maintenu. Dans le cas contraire, après plusieurs tentatives infructueuses de rétablissement de la communication, l'accès est bloqué.

[069] A la **figure 3**, il est illustré un exemple selon lequel l'équipement 210 n'est pas (ou n'est plus) dans la zone 220. Ce cas de figure peut notamment correspondre à :

- à l'éloignement temporaire de l'utilisateur par rapport au périphérique (par exemple parce que l'utilisateur a besoin de sortir d'une salle de présentation pour prendre un appel sur son téléphone) ;
- un oubli du périphérique (l'utilisateur quitte la salle de présentation en laissant le périphérique sur le système 200) ;
- une perte ou un vol du périphérique.

[070] Dans ces cas de figures, les données stockées sont protégées par le module de gestion 116 qui n'autorisera aucun accès aux données protégées tant qu'un équipement électronique 210 de l'utilisateur n'est pas à nouveau détecté dans la zone 220.

[071] De cette manière, les données à protéger dans la mémoire 112 ne sont rendues accessibles qu'en cas de proximité de l'équipement 210 de l'utilisateur, lorsque ce dernier revient dans la zone 220 avec cet équipement 210 qu'il porte ou transporte.

[072] Par ailleurs, une alerte peut être prévue sur l'équipement 210 afin de prévenir l'utilisateur que la communication sans-fil et de courte portée avec le périphérique 100 a été interrompue. Cette alerte permet à l'utilisateur d'être averti de l'oubli, de la perte ou du vol de son périphérique 100 dès qu'il a quitté la zone de détection 220. Il peut alors tenter de récupérer son périphérique quand c'est encore possible.

[073] On se réfère maintenant à la **figure 4** sur laquelle est représenté un organigramme composé d'un exemple de succession d'étapes du procédé de gestion d'accès de l'invention.

[074] Selon une étape 400, il est vérifié si l'interface de connexion 110 du périphérique 100 est connectée à un système informatique 200.

[075] Dans le cas d'une vérification négative (flèche N en sortie de l'étape 400), il peut ensuite être vérifié selon les étapes 401 et 402 si :

- le module de sécurité 118 a émis un signal t^{MS} indiquant qu'une tentative d'accès non-autorisé aux données a été détectée (étape 401) et si

- le niveau de charge n^{BAT} de la batterie 120 est supérieur à un niveau de charge limite n^{lim} prédéterminé (étape 402).

[076] Il convient de noter que les étapes 401 et 402 peuvent être réalisées indépendamment l'une de l'autre, successivement ou concomitamment.

[077] Si la vérification est positive (flèches Y en sortie des étapes 401 et 402), il peut à nouveau être vérifié si le périphérique 100 est connecté avec un système 200.

[078] Dans le cas d'une vérification négative aux étapes 401 et 402 (flèches N en sortie de 401 et 402), les données à protéger dans la mémoire 112 sont détruites selon l'étape 403 par le module de gestion 116 qui exécute l'action DEL_DAT. Les données alors détruites peuvent être :

- l'intégralité des données stockées dans la mémoire 112 ;
- la partition de données à protéger sélectionnée par l'utilisateur ;
- les données déterminées comme sensibles, personnelles ou confidentielles.

[079] Afin de rendre la récupération des données impossible, le module de gestion 116 peut par exemple remplacer les données détruites par des données aléatoires sans intérêt.

[080] A l'étape 402, le niveau de charge limite n^{lim} peut être un seuil prédéterminé correspondant à un niveau faible de la batterie 120. Néanmoins, il convient que n^{lim} corresponde à une autonomie de batterie suffisante pour que le module de gestion 116 puisse encore exécuter plusieurs instructions telles que l'action DEL_DAT. Ainsi, lorsque le périphérique reste inutilisé pendant une longue période de temps, la mémoire ne comporte plus les données sensibles.

[081] En outre, le procédé comprend une étape de chiffrement des données à protéger dans la mémoire du périphérique (étape non représentée sur la figure 4).

[082] Lorsque le périphérique 100 est effectivement connecté à un système informatique 200 (flèche Y en sortie de l'étape 400), le module de gestion 116 vérifie auprès du module de communication 114 qu'une communication est établie avec un équipement 210 autorisé (étape 404).

[083] Pour ce faire, le procédé de gestion d'accès peut comprendre en outre les étapes de :

- réception d'un identifiant de l'équipement électronique 210 ;
- comparaison de l'identifiant reçu avec la liste d'identifiants d'équipements électroniques 210 (liste qui est contenue dans la mémoire 112) autorisés à communiquer avec le module de communication 114 ;
- mise en communication du module de communication 114 et de l'équipement électronique 210 lorsque l'identifiant reçu est compris dans la liste.

[084] Si le module 114 n'est pas en communication avec un équipement 210 autorisé (flèche N en sortie de l'étape 404), l'accès des données à protéger dans la mémoire 112 n'est pas autorisé au système 200. Le module de gestion 116 exécute alors une action NO_ACC (étape 405) consistant à :

- ne pas répondre ou à bloquer une requête en lecture/écriture des données du système 200, ou
- ne pas fournir la clé de chiffrement permettant de lire les données stockées.

[085] Si la vérification de communication établie entre le module 114 et l'équipement 210 est positive (flèche Y en sortie de l'étape 404), l'utilisateur qui porte ou transporte l'équipement 210 est donc à proximité du périphérique. Il est dès lors en mesure de s'assurer des personnes voulant accéder aux données stockées dans son périphérique. Selon une réalisation possible, le module de gestion 116 exécute alors directement une action DAT_ACC à l'étape 406, action selon laquelle le contenu de la mémoire 112 est rendu accessible au système 200. Cet accès est autorisé tant que la communication entre le module 114 et l'équipement 210 reste établie. A cet effet, la clé de chiffrement nécessaire à déchiffrer les données chiffrées dans la mémoire 112 peut être fournie au système 200.

[086] De manière optionnelle, le procédé peut comprendre en outre, au préalable de l'étape 406, une étape d'authentification de l'utilisateur (étape 407) via laquelle, selon une action COD, le module de gestion 116 demande à l'utilisateur de s'authentifier via la saisi d'un code d'accès sur le système 200 auquel le périphérique est connecté.

[087] Le code d'accès saisi peut être comparé à une liste de code d'accès enregistré dans la mémoire 112, chaque code d'accès pouvant être enregistré en correspondance des niveaux de sécurité susmentionnés. Si le code est correct (code saisi compris dans la liste de codes en mémoire, flèche Y en sortie de l'étape 407), le module de gestion

autorise l'accès ou fourni la clé de déchiffrement des données correspondant au niveau de sécurité du code d'accès saisi (étape 406).

[088] Tant que le périphérique 100 est alimenté, le module de gestion 116 vérifie régulièrement que le module 114 est toujours en communication avec l'équipement 210 pour maintenir l'accès aux données (action DAT_ACC de l'étape 406). Dans le cas contraire, l'accès est bloqué (action NO_ACC de l'étape 405).

[089] Bien entendu, lorsque le code saisi par l'utilisateur à l'étape 407 n'est pas reconnu (flèche N en sortie de l'étape 407), les données de la mémoire 112 ne sont pas rendues accessibles (renvoi à l'étape 405).

[090] Ceci n'est qu'un exemple de réalisation du procédé. Toutefois, d'autres variantes peuvent être implémentées comme par exemple une réitération régulière des étapes 401 et 402 pour s'assurer en continu et presque en temps réel qu'il n'y a pas eu de tentative d'accès-non autorisé aux données (par exemple via des attaques lancées par le système 200 lorsque le périphérique est connecté), ou que le niveau de batterie est suffisant pour assurer une bonne protection des données (par exemple lorsque l'interface 110 est longtemps connectée à un port de connexion de système 200 qui ne fournit pas d'alimentation électrique au périphérique 100).

[091] En outre, une application logicielle peut être prévue du côté de l'équipement 210 pour prévenir l'utilisateur, par exemple à l'aide d'une alarme qui lui est notifiée, quand la communication entre le périphérique et son équipement est interrompue. Cette alarme le prévient de manière immédiate que le périphérique n'est plus visible et donc plus à proximité de l'utilisateur (que ce soit parce que le périphérique a été oublié, perdu ou volé.

[092] A titre purement illustratif, il est décrit ci-après un cas où l'invention est mise pratique et prend tout son sens. En l'occurrence, un utilisateur se rend à une réunion à l'extérieur pour présenter ses travaux. Pour cela, il effectue une copie de fichiers numériques (par exemple un support de la présentation qu'il doit réaliser) sur son périphérique de stockage de type clé USB. Cette présentation porte sur un sujet hautement confidentiel.

[093] A la réunion, il connecte son périphérique au poste informatique mis à sa disposition. Le périphérique s'assure alors de la présence de l'utilisateur en cherchant à

établir une communication Bluetooth avec le téléphone de l'utilisateur. Si la communication Bluetooth entre le périphérique et le téléphone a s'établit, le périphérique fait apparaitre une question à l'écran de l'ordinateur : « Entrez le code d'activation : ». En saisissant le bon code, le périphérique autorise à l'ordinateur d'accéder au contenu de la clé USB. L'utilisateur peut alors accéder au support de sa présentation et commencer la réunion.

[094] A la fin de cette réunion, l'utilisateur oublie malencontreusement son périphérique sur le poste informatique de la salle de réunion. Lorsque l'utilisateur s'éloigne de la salle de réunion avec son téléphone dans la poche, la communication entre le téléphone et la clé USB est interrompue. L'accès aux données est alors annulé et la clé n'est plus visible par l'ordinateur. L'utilisateur peut ensuite être prévenu via son téléphone que la communication avec le périphérique a été interrompue, l'alertant de son oubli. L'utilisateur peut ainsi retourner récupérer sa clé USB sans que, dans l'intervalle, des tiers non-autorisés par l'utilisateur n'aient pu accéder au contenu confidentiel de sa clé. Si quelqu'un tente de démonter la clé pour accéder physiquement à ses composants électroniques, la clé efface définitivement son contenu.

[095] Selon une réalisation possible (non représentée sur les figures), le périphérique peut comprendre en outre une deuxième interface de connexion apte à être connectée à un autre périphérique, et en particulier à un autre périphérique de stockage de données. Cette deuxième interface de connexion peut par exemple être un connecteur USB femelle apte à être connecté avec un connecteur USB mâle, tel qu'un connecteur USB mâle de clé de stockage USB. Le périphérique connecté à la deuxième interface de connexion du périphérique 100 peut notamment offrir un espace de stockage complémentaire à la mémoire 112 et ainsi augmenter les capacités de stockage de données.

[096] Selon cette réalisation, le module de gestion 116 du périphérique 100 peut être adapté pour :

- chiffrer les données stockées dans le périphérique connecté à la deuxième interface de connexion selon la clé de chiffrement stockée dans la mémoire 112 ;

- contrôler les données stockées dans le périphérique connecté à la deuxième interface de connexion et, si les données contrôlées sont considérées comme étant nuisibles ou à risques (données endommagées, virus informatique ou autre), ces données ne sont pas rendues visibles et/ou accessibles au système informatique 200.

[097] Ainsi, le périphérique 100 permet en outre de protéger le système informatique 200 contre des données à risques contenus dans le périphérique de stockage connecté à la deuxième interface de connexion.

[098] En complément, le module de gestion 116 peut être adapté pour formater et crypter le contenu du périphérique connecté à la deuxième interface de connexion afin qu'il ne soit accessible au système informatique 200 que par l'intermédiaire de la deuxième interface de connexion du périphérique 100.

[099] Il convient donc de noter que le périphérique de stockage proposé a pour principaux avantages d'offrir :

- un accès protégé aux données stockées ;
- un contenu qui peut être chiffré ;
- la possibilité d'un déclenchement d'alarme lors de l'oubli du périphérique ou de sa perte ;
- destruction des données en cas de vol ou d'inutilisation prolongée ;
- la possibilité d'augmenter les capacités de stockage de données tout en protégeant le système informatique de données nuisibles ou à risques.

[0100] Dans cet exemple de réalisation, le périphérique présenté est sous la forme d'une clé USB. Toutefois, d'autre réalisation de périphérique telle qu'un disque dur externe ou une carte mémoire peuvent être envisagée dans le cadre de l'invention. En outre, selon d'autres réalisations possibles, l'interface de connexion du périphérique peut être par ailleurs :

- une interface de connexion physique avec un système informatique (de type RJ45, FireWire, fibre optique, eSATA ou autre) ; ou

- une interface de connexion sans-fil avec un système informatique (utilisant par exemple un protocole de communication sans-fil tel que Bluetooth, Wi-Fi, IrDa, NFC ou autre).

[0101] L'invention a été décrite en référence à des modes de réalisations particuliers qui ne sont pas limitatifs. Bien entendu, la présente invention ne se limite pas à la forme de réalisation décrite à titre d'exemple et elle s'étend à d'autres variantes. Par exemple, pour autoriser l'accès aux données stockées sur le périphérique, il peut être requis que le module de communication soit en communication avec au moins deux équipements électroniques de l'utilisateur en simultané, permettant ainsi d'augmenter le degré de certitude que l'utilisateur est bien à proximité du périphérique.

Revendications

1. Périphérique de stockage de données (100) comportant au moins :
   - une interface de connexion (110) apte à être connectée à un système informatique (200) ;
   - une mémoire (112) configurée pour stocker des données ;
   - un module de communication (114) sans-fil apte à communiquer avec au moins un équipement électronique (210) ;
   - un module de gestion (116) configuré pour autoriser l'accès du système informatique à au moins une partie des données stockées dans la mémoire uniquement lorsqu'une communication est établie entre le module de communication et l'équipement électronique.

2. Périphérique de stockage de données selon la revendication 1, dans lequel la mémoire contient une liste d'identifiants d'équipements électroniques autorisés à communiquer avec le module de communication (114),
   le module de communication étant configuré pour ne communiquer qu'avec des équipements électroniques dont l'identifiant est compris dans ladite liste.

3. Périphérique de stockage de données selon l'une des revendications 1 et 2, dans lequel la mémoire contient en outre une clé de chiffrement,
   le module de gestion (116) étant configuré pour chiffrer selon ladite clé de chiffrement l'au moins une partie des données à laquelle le module de gestion autorise l'accès.

4. Périphérique de stockage de données selon l'une des revendications précédentes, comprenant en outre un module de sécurité (118) apte à détecter une tentative d'accès non-autorisé aux données stockées dans la mémoire (112),
   le module de gestion (116) étant configuré pour détruire l'au moins une partie des données stockées lorsque ladite tentative est détectée par le module de sécurité.

5. Périphérique de stockage de données selon l'une des revendications précédentes, comprenant en outre une batterie (120),
le module de gestion (116) étant configuré pour détruire au moins une partie des données stockées dans la mémoire (112) lorsque le niveau de charge de la batterie est inférieur à un seuil prédéterminé.

6. Système de gestion d'accès à des données stockées sur un périphérique de stockage selon l'une des revendications précédentes, dans lequel l'au moins un équipement électronique (210) est configuré pour émettre une alerte à destination d'un utilisateur lorsque la communication établie entre le module de communication (114) et l'équipement électronique (210) est interrompue.

7. Procédé de gestion d'accès à des données stockées dans une mémoire (112) d'un périphérique de stockage de données (100), le procédé comprenant au moins les étapes suivantes, exécutées dans le périphérique de stockage de données :
- vérification (404) qu'une communication sans-fil est établie entre un module de communication (114) dudit périphérique et un équipement électronique (210) ;
- autorisation d'accès (407) d'un système informatique (200) à au moins une partie des données stockées dans la mémoire, uniquement lorsque ladite vérification de communication établie est positive.

8. Procédé de gestion d'accès selon la revendication 7, comprenant les étapes de :
- réception d'un identifiant de l'équipement électronique (210) ;
- comparaison de l'identifiant reçu avec une liste d'identifiants d'équipements électroniques autorisés à communiquer avec le module de communication (114) ;
- mise en communication du module de communication et de l'équipement électronique lorsque l'identifiant reçu est compris dans ladite liste.

9. Procédé de gestion d'accès selon l'une des revendications 7 et 8, comprenant en outre une étape de chiffrement de l'au moins une partie des données stockées dans la mémoire du périphérique.

10. Procédé de gestion d'accès selon l'une des revendications 7 à 9, comprenant en outre une destruction (403) de l'au moins une partie des données stockées dans la mémoire du périphérique lorsqu'une tentative d'accès non-autorisé aux données est détectée.

11. Procédé de gestion d'accès selon l'une des revendications 7 à 10, comprenant en outre la destruction (403) de l'au moins une partie des données stockées dans la mémoire du périphérique lorsque le niveau de charge d'une batterie (120) du périphérique est inférieur à un seuil prédéterminé.

12. Procédé de gestion d'accès selon l'une des revendications 7 à 11, comprenant en outre une étape d'authentification (405) d'un utilisateur avant d'autoriser l'accès (407) du système informatique à l'au moins une partie des données stockées dans la mémoire.

13. Procédé de gestion d'accès selon la revendication 12, dans lequel, lors de l'autorisation d'accès (407), les données sont rendues accessibles en fonction des droits d'accès associés à l'utilisateur authentifié.

14. Programme informatique comportant des instructions pour la mise en œuvre du procédé de gestion d'accès selon l'une des revendications 7 à 13, lorsque ce programme est exécuté par un module de gestion d'un périphérique de stockage de données.

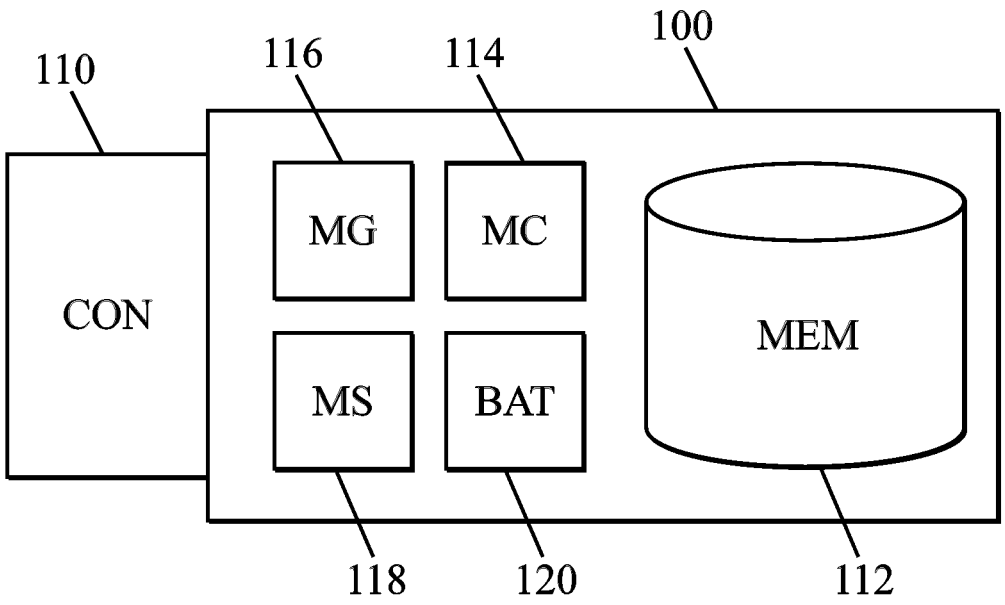


FIG. 1

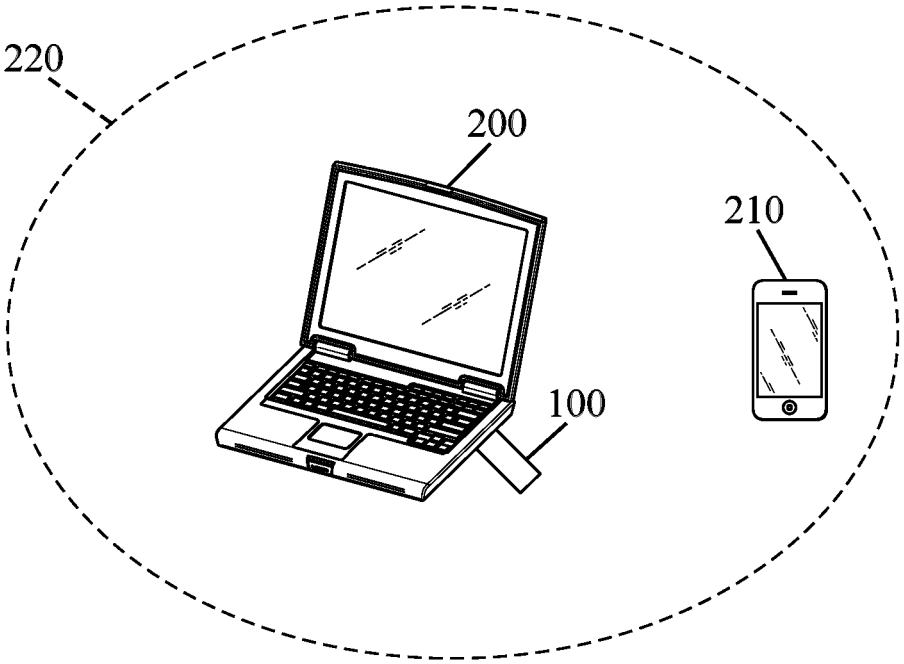


FIG. 2

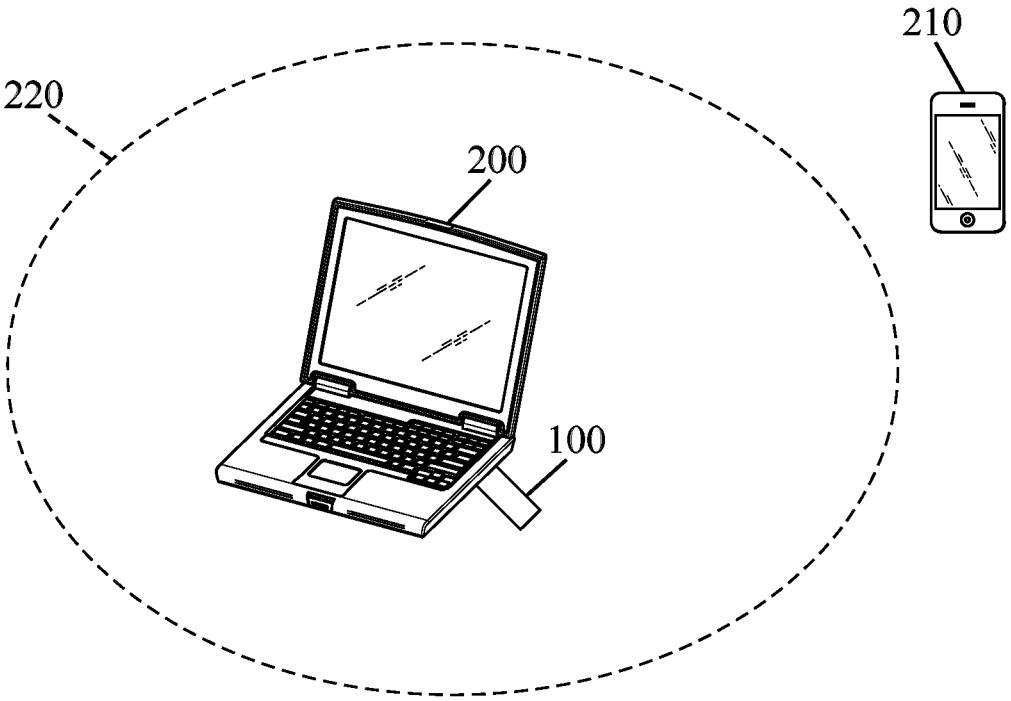


FIG. 3

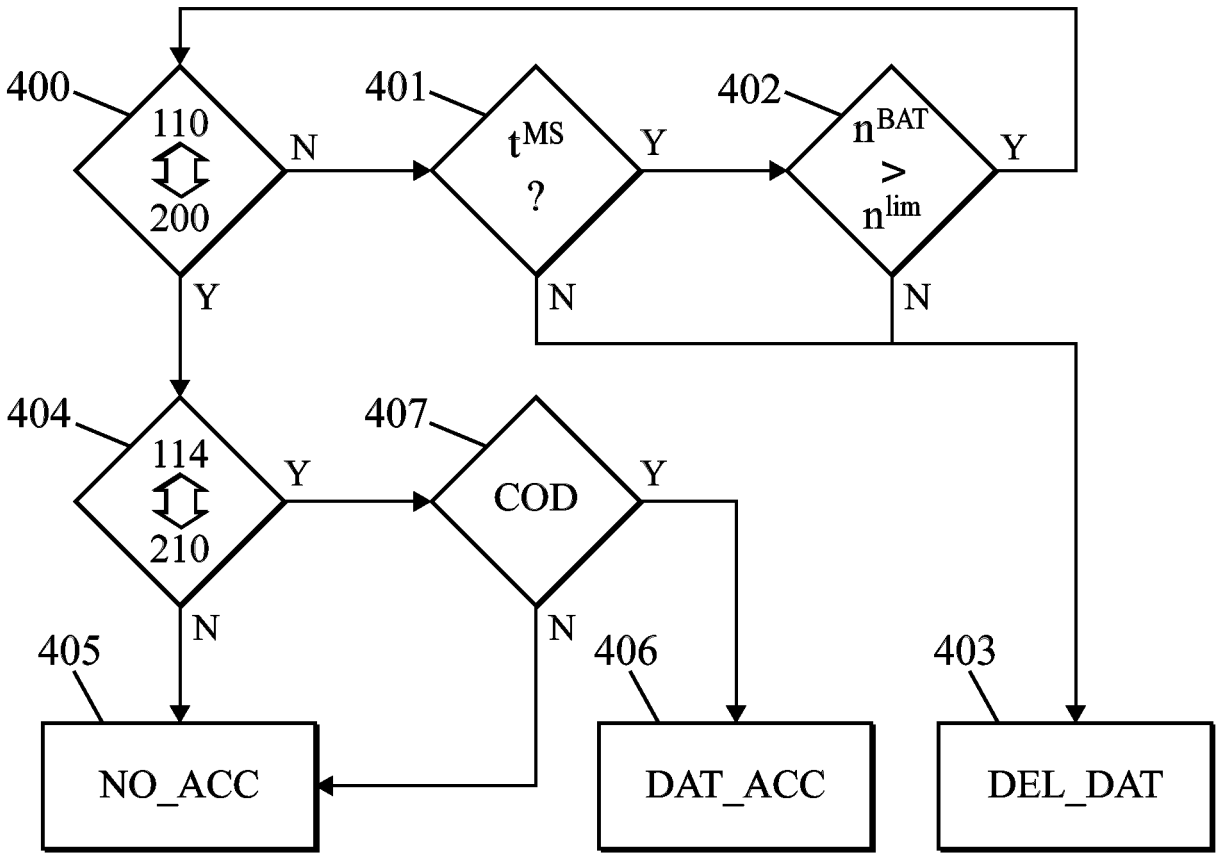

400
110
200
N
401
t^MS
?
Y
402
n^BAT
>
n^lim
Y
Y
N
N
404
114
210
Y
407
COD
Y
N
N
405
406
403
NO_ACC
DAT_ACC
DEL_DAT

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 805389
FR 1460907

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 2011/093958 A1 (DEVICTOR GILLES BRUNO MARIE [US]) 21 avril 2011 (2011-04-21)	1-4, 6-10, 12-14	G06F21/60 H04L29/06
Y	* alinéas [0007] - [0018] * * alinéas [0024] - [0031] *	5,11	
Y	US 2012/210389 A1 (BROWN MICHAEL S [CA] ET AL) 16 août 2012 (2012-08-16) * alinéas [0054] - [0055] *	5,11	
X	US 2008/303631 A1 (BEEKLEY JOHN S [US] ET AL) 11 décembre 2008 (2008-12-11) * alinéas [0015] - [0045] *	1-4, 6-10, 12-14	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

G06F

Date d'achèvement de la recherche	Examinateur
1 juillet 2015	Segura, Gustavo

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 1460907 FA 805389

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 01-07-2015
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 2011093958 A1	21-04-2011	AUCUN	
US 2012210389 A1	16-08-2012	CA 2652438 A1	29-11-2007
		EP 2021968 A1	11-02-2009
		EP 2455881 A1	23-05-2012
		US 2007298767 A1	27-12-2007
		US 2008005561 A1	03-01-2008
		US 2008009264 A1	10-01-2008
		US 2010317324 A1	16-12-2010
		US 2012210389 A1	16-08-2012
		WO 2007134448 A1	29-11-2007
US 2008303631 A1	11-12-2008	AUCUN	

EPO FORM P0465