



(43) Date de la publication internationale
8 décembre 2016 (08.12.2016)

WIPO | PCT

(10) Numéro de publication internationale
WO 2016/193590 A1

- (51) Classification internationale des brevets :
H04W 12/02 (2009.01) H04W 12/08 (2009.01)
- (21) Numéro de la demande internationale :
PCT/FR2016/051264
- (22) Date de dépôt international :
27 mai 2016 (27.05.2016)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
1554875 29 mai 2015 (29.05.2015) FR
- (71) Déposant : ORANGE [FR/FR]; 78 rue Olivier de Serres,
75015 Paris (FR).
- (72) Inventeurs : SCHILTZ, André; 14 chemin de la Rousse,
38190 Bernin (FR). COUTANT, Stéphane; 5 avenue des
Pampres, 38700 Corenc (FR).
- (74) Mandataire : ORANGE/IPL; MILET Isabelle, 38-40 rue
du Général Leclerc, 92794 Issy Moulineaux Cedex 9 (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, 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, KN, KP, KR,
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).

Publiée :

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

(54) Title : TELECOMMUNICATIONS TERMINAL AND METHOD FOR CONTROLLING ACCESS TO DATA IN SUCH A TERMINAL

(54) Titre : TERMINAL DE TÉLÉCOMMUNICATIONS ET PROCÉDÉ DE GESTION D'ACCÈS DE DONNÉES DANS UN TEL TERMINAL

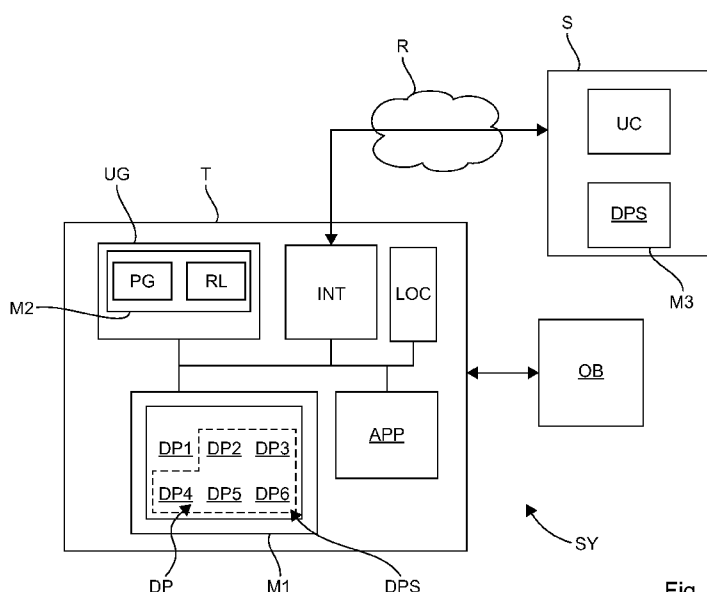


Fig. 2

(57) Abstract : The invention relates to a tele-communications terminal (T) comprising a first memory (M1), an application (APP) capable of accessing sensitive personal data (DP2-DP6) stored in the first memory (M1) and an access control unit (UG) to execute a processing such that the application (APP) is prevented from accessing the sensitive personal data (DPS) in the first memory (M1), the processing comprising the transfer of the sensitive personal data (DP2-DP6) to a second memory (S) and the deletion of the sensitive personal data (DP2-DP6) from the first memory (M1). The access control unit (UG) is capable of accessing the sensitive personal data stored in the second memory (S). The invention further relates to a method for controlling access to sensitive personal data (DP2-DP6) in such a telecommunications terminal (T).

(57) Abrégé : L'invention concerne un terminal de télécommunications (T) comprenant une première mémoire

[Suite sur la page suivante]



(M1), une application (APP) apte à accéder à une donnée personnelle sensible (DP2- DP6) stockée dans la première mémoire (M1) et une unité de gestion d'accès (UG) pour réaliser un traitement de façon à empêcher l'application (APP) d'accéder à la donnée personnelle sensible (DPS) dans la première mémoire (M1), le traitement comprenant le transfert de la donnée personnelle sensible (DP2-DP6) vers une deuxième mémoire (S) et la suppression de la donnée personnelle sensible (DP2-DP6) dans la première mémoire (M1). L'unité de gestion d'accès (UG) est apte à accéder à la donnée personnelle sensible stockée dans la deuxième mémoire (S). L'invention concerne en outre un procédé de gestion d'accès à une donnée personnelle sensible (DP2-DP6) dans un tel terminal de télécommunications (T).

Terminal de télécommunications et procédé de gestion d'accès de données dans un tel terminal

5 1. Domaine de l'invention

La présente invention concerne la protection de données personnelles dans un terminal de télécommunications et porte plus particulièrement sur la protection de données personnelles stockées en mémoire dans un terminal de télécommunication vis-à-vis d'une application installée dans ledit terminal.

10 2. Art antérieur

De façon connue, il est généralement possible d'installer diverses applications dans des terminaux de télécommunications tels que des téléphones mobiles, tablettes ou équivalents. Typiquement, un utilisateur peut télécharger des applications gratuites ou payantes depuis une plateforme de téléchargement sur son téléphone mobile. Lorsque l'on télécharge une telle application depuis Internet par exemple, il est en général obligatoire d'autoriser l'accès de cette application à un certain nombre de données personnelles dans le téléphone mobile. Faute d'autoriser l'accès de l'application à ces données personnelles, le téléchargement et l'installation de l'application dans le téléphone mobile sont généralement impossibles.

La **figure 1** représente schématiquement un téléphone mobile 2 comprenant des données personnelles 4 stockées en mémoire ainsi qu'une application 6 installée dans le téléphone mobile 2. Dans cet exemple, l'application a au préalable été téléchargée par l'utilisateur via Internet 10 depuis un fournisseur de services 8. Une fois installée, l'application 6 peut être mise en œuvre et ainsi accéder aux données personnelles 4 stockées dans la mémoire du téléphone mobile 2.

S'il est vrai que certaines des données personnelles de l'utilisateur sont utiles, voire indispensables, pour exécuter l'application dans le téléphone mobile, l'accès à d'autres données personnelles par l'application n'est souvent pas justifié et ne vise en réalité qu'à permettre des analyses comportementales de l'utilisateur au détriment de la confidentialité de ses données personnelles.

Les données personnelles réellement utiles pour l'exécution d'une application dépendent de la nature même de l'application en question. Ainsi, selon le cas, une application peut, par exemple, nécessiter l'accès à des données de localisation du terminal de télécommunications, à des données d'achats (s'il s'agit par exemple d'une application avec option d'achat), des paramètres de données cellulaires, etc.

Il est en revanche courant pour une application d'exiger l'accès dans un terminal de télécommunications à des données personnelles qui ne sont pas réellement utiles pour

l'exécution de l'application. Ces données personnelles superflues présentent une valeur économique indéniable pour le gestionnaire de l'application puisque, une fois extraites, ces données personnelles permettent en particulier de déduire les usages et comportements de l'utilisateur. Selon le cas, ces données personnelles superflues concernent, par exemple, l'identité numérique de l'utilisateur, les contacts de l'utilisateur, l'agenda de l'utilisateur, les SMS, les contenus multimédias stockés dans le terminal de télécommunications, etc. Ainsi, le gestionnaire d'une application peut vendre à des commerçants des données personnelles (numéro du téléphone, identité de l'utilisateur etc.) permettant de déterminer les habitudes de consommation des utilisateurs. Les gestionnaires d'application sont également en mesure de proposer aux utilisateurs des contenus publicitaires ciblés en fonction du contenu de leurs données personnelles.

Ces applications exécutées sur les terminaux de télécommunications présentent donc un problème de non-respect de la confidentialité des données personnelles des utilisateurs. Ce problème est d'autant plus critique lorsqu'il s'agit de données personnelles sensibles portant par exemple sur la santé ou la vie privée de l'utilisateur, voire de celles des contacts de l'utilisateur en question.

Un utilisateur n'est pas aujourd'hui en capacité de protéger convenablement l'accès à ses données personnelles vis-à-vis d'applications installées dans un terminal de télécommunications, tels qu'un téléphone mobile, tablette ou ordinateur par exemple.

3. Objet et résumé de l'invention

Un des buts de l'invention est donc de remédier aux inconvénients de l'état de la technique. En particulier, un des buts de l'invention est d'empêcher une application installée dans un terminal de télécommunications d'accéder à certaines données personnelles dites sensibles de l'utilisateur et ce, tout en permettant l'exécution de cette application sur le terminal de télécommunications en question.

A cet effet, la présente invention concerne un terminal de télécommunications selon la revendication 1.

Le terminal de communication comprend notamment :

- une première mémoire ;
- une application installée dans le terminal de télécommunications et apte à accéder à au moins une donnée personnelle sensible stockée dans la première mémoire, ladite au moins une donnée personnelle sensible étant associée au terminal ou à un utilisateur du terminal.

Le terminal de télécommunications comprend également une unité de gestion d'accès apte à réaliser un traitement de façon à empêcher l'application d'accéder à ladite au moins une donnée personnelle sensible dans la première mémoire, le traitement comprenant :

- 5 a) le transfert de ladite au moins une donnée personnelle sensible vers une deuxième mémoire ; et
- b) la suppression de ladite au moins une donnée personnelle sensible dans la première mémoire ;

10 l'unité de gestion d'accès étant apte à accéder à ladite au moins une donnée personnelle sensible stockée dans la deuxième mémoire.

La combinaison à la fois du stockage dans une deuxième mémoire des données personnelles sensibles et de la suppression de ces données personnelles sensibles dans la première mémoire du terminal de télécommunications permet avantageusement de protéger l'accès aux données personnelles sensibles de l'utilisateur vis-à-vis d'une application malveillante ou considérée

15 comme trop curieuse.

La deuxième mémoire est une mémoire du terminal, typiquement une zone mémoire non accessible par ladite application ou une mémoire d'un serveur distant accessible par ledit terminal via un réseau de télécommunications.

20 Selon un mode de réalisation particulier, ladite au moins une donnée sensible comprend au moins l'une parmi :

- une donnée de contact d'utilisateur,
- une donnée d'agenda électronique,
- un favori d'un navigateur Internet,
- une donnée d'historique d'un navigateur Internet,
- 25 - une donnée de géolocalisation du terminal de télécommunications,
- une donnée électronique fournie par un objet connecté au terminal de télécommunications.

Selon un mode de réalisation particulier, l'unité de gestion d'accès est configurée pour déclencher le traitement sur détection qu'au moins une condition prédéterminée est remplie. Il

30 est ainsi possible de paramétrer l'unité de gestion d'accès de sorte à ce que le traitement se déclenche automatiquement de façon appropriée.

Selon un mode de réalisation particulier, ladite au moins une condition prédéterminée définit au moins l'une parmi :

- une quantité de données personnelles d'un type prédéterminé stockée dans la première mémoire ; et
- une condition de temps indiquant quand ledit traitement doit être initié.

Selon un mode de réalisation particulier, l'unité de gestion d'accès est configurée pour
5 maintenir dans la première mémoire au moins une donnée personnelle prédéterminée dite « non sensible » lorsque ladite suppression est réalisée. Il est ainsi possible de paramétrer l'unité de gestion d'accès afin de définir de façon optimisée quelles données personnelles doivent faire l'objet dudit traitement.

Selon un mode de réalisation particulier, lors dudit traitement, l'unité de gestion d'accès est
10 configurée pour remplacer, dans la première mémoire, ladite au moins une donnée personnelle sensible par au moins une donnée fictive différente de ladite au moins une donnée personnelle sensible.

Ainsi, l'unité de gestion d'accès permet à l'application de fonctionner normalement malgré la suppression dans le terminal de données personnelles qui peuvent être utiles voire indispensables
15 à la mise en œuvre de l'application. L'application peut accéder dans la première mémoire du terminal de télécommunications à chaque donnée fictive tandis que la ou les données personnelles réelles correspondantes sont stockées dans la deuxième mémoire. Il est ainsi possible de masquer si besoin certaines données personnelles de l'utilisateur vis-à-vis d'une application sans que cette dernière puisse s'en rendre compte.

Selon un mode de réalisation particulier, le terminal de télécommunications comprend une
20 unité de géolocalisation apte, dans un mode normal, à déterminer des coordonnées de géolocalisation représentatives de la localisation dudit terminal,

l'unité de gestion d'accès étant apte à commander la commutation de l'unité de géolocalisation du mode normal vers un mode secret dans lequel l'unité de géolocalisation est
25 configurée pour générer des données de géolocalisation fictives non représentatives de la localisation du terminal de télécommunications.

Selon un mode de réalisation particulier, ladite au moins une donnée personnelle sensible comprend des données de géolocalisation générées en mode normal par l'unité de géolocalisation,

l'unité de gestion d'accès étant configurée, lors du traitement, pour remplacer dans la
30 mémoire les données de géolocalisation par des données de géolocalisation fictives générées en mode secret par l'unité de géolocalisation.

De façon avantageuse, il est ainsi possible de masquer, si nécessaire, la localisation du terminal de télécommunications.

Selon un mode de réalisation particulier, la deuxième mémoire est une mémoire d'un serveur distant, accessible par le terminal via un réseau de télécommunications, et, suite au traitement, l'unité de gestion d'accès est apte à envoyer au serveur distant une requête comprenant un identifiant d'au moins une donnée personnelle sensible stockée par le serveur distant et pour recevoir, en réponse à la requête, au moins une donnée personnelle sensible correspondant à l'identifiant.

De manière avantageuse, l'utilisateur peut ainsi commander le rapatriement sélectif vers son terminal de télécommunications d'une ou plusieurs données personnelles sensibles stockées à distance par le serveur.

La présente invention concerne également un système comprenant un terminal de télécommunications tel que défini ci-avant, et un serveur distant apte à recevoir et à stocker ladite au moins une donnée personnelle sensible transférée par l'unité de gestion d'accès du terminal de télécommunications.

Corrélativement, l'invention concerne un procédé de gestion d'accès mis en œuvre dans un terminal de télécommunications comprenant une première mémoire dans laquelle est stockée au moins une donnée personnelle sensible, ladite au moins une donnée personnelle sensible étant associée au terminal ou à un utilisateur du terminal,

une application, apte à accéder à ladite au moins une donnée personnelle sensible dans la première mémoire, étant installée dans le terminal de télécommunications,

le procédé comprenant un traitement réalisé par une unité de gestion d'accès du terminal de télécommunications de façon à empêcher ladite application d'accéder à ladite au moins une donnée personnelle sensible dans ladite première mémoire, le traitement comprenant :

a) transfert de ladite au moins une donnée personnelle sensible vers une deuxième mémoire ; et

b) suppression de ladite au moins une donnée personnelle sensible dans la première mémoire.

Dans un mode de réalisation particulier, le procédé comprend, ultérieurement au traitement, l'accès par l'unité de gestion d'accès, à ladite au moins une donnée personnelle sensible stockée dans la deuxième mémoire.

Dans un mode de réalisation particulier, cet accès nécessite un accord préalable de l'utilisateur.

A noter que les divers modes de réalisation mentionnés ci-avant en relation avec le terminal de télécommunications de l'invention s'appliquent de façon analogue au procédé de gestion d'accès de l'invention.

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

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations (ou support d'enregistrement), ce programme étant susceptible d'être mis en œuvre dans un terminal de télécommunications ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de gestion d'accès tel que défini ci-dessus.

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

L'invention vise aussi un support d'informations (ou support d'enregistrement) lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

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

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

4. Brève description des dessins

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

- la figure 1 déjà décrite représente, de manière schématique, un terminal de télécommunications conventionnel dans lequel est exécutée une application ;
- la figure 2 représente schématiquement un système comprenant un terminal de télécommunication conforme à un mode de réalisation particulier de l'invention ;
- la figure 3 est un organigramme représentant un procédé de gestion d'accès conformément à un mode de réalisation particulier de l'invention ; et

- la figure 4 représente, sous forme d'un organigramme, la récupération, par le terminal de télécommunications illustré en figure 2, de données personnelles stockées à distance.

5. Description détaillée de plusieurs modes de réalisation

La présente invention concerne la protection de données personnelles dans un terminal de télécommunications et porte plus particulièrement sur la protection de données personnelles stockées en mémoire dans un terminal de télécommunication vis-à-vis d'une application installée dans ledit terminal.

Dans le présent exposé, sont décrits des exemples de mise en œuvre de l'invention portant sur la sécurisation de données personnelles dites sensibles dans un téléphone mobile. On comprendra que la mise en œuvre de l'invention ne se limite pas aux téléphones mobiles et s'applique plus généralement à la sécurisation de quelconques données personnelles dans un terminal de télécommunications (tablette, ordinateur etc.).

Comme expliqué précédemment, lorsqu'il souhaite télécharger et installer une application dans son téléphone mobile, l'utilisateur est généralement contraint d'accepter les conditions imposées par le fournisseur de l'application, notamment en ce qui concerne l'accès de l'application à certaines données personnelles de l'utilisateur, faute de quoi l'installation (ou du moins l'exécution) de l'application n'est pas possible sur le téléphone mobile en question.

La déposante a par conséquent mis au point une solution permettant d'autoriser les requêtes d'accès du fournisseur de services aux données personnelles de l'utilisateur, tout en protégeant les données personnelles dites sensibles de l'utilisateur.

A cet effet, la présente invention prévoit dans un mode de réalisation particulier un procédé de gestion d'accès mis en œuvre dans un terminal de télécommunications, ce procédé comprenant :

- a) le transfert, via un réseau de télécommunications, d'au moins une donnée personnelle sensible du terminal de télécommunications vers un serveur distant ; et
- b) la suppression de ladite au moins une donnée personnelle sensible dans la mémoire du terminal de télécommunications.

La combinaison à la fois du stockage à distance des données personnelles sensibles et de la suppression de ces données personnelles sensibles dans la mémoire du terminal de télécommunications permet avantageusement de protéger l'accès aux données personnelles sensibles de l'utilisateur vis-à-vis d'une application malveillante ou considérée comme trop curieuse.

Sauf indications contraires, les éléments communs ou analogues à plusieurs figures portent les mêmes numéros de références et présentent des caractéristiques identiques ou analogues, de sorte que ces éléments communs ne sont généralement pas à nouveau décrits par souci de simplicité.

5 La **figure 2** représente, de manière schématique, la structure d'un système SY comprenant un terminal de télécommunications T (un téléphone mobile dans cet exemple) conforme à un mode de réalisation particulier de l'invention.

Le terminal de télécommunications T (appelé ci-après « terminal ») comprend une mémoire M1, une unité de gestion d'accès UG, une interface de communication INT, une application APP
10 installée dans le terminal T, et une unité de géolocalisation LOC.

Plus précisément, la mémoire M1 est par exemple une mémoire non volatile réinscriptible (de type EEPROM par exemple) ou une mémoire non volatile réinscriptible. On suppose ici dans un premier temps qu'au moins une donnée personnelle DP est stockée dans la mémoire M1 du terminal T. Chaque donnée personnelle DP est associée au terminal T et/ou à un utilisateur du
15 terminal T.

Dans l'exemple considéré ci, les données personnelles DP comprennent :

- une donnée personnelle DP1 dite « non sensible » ; et
- des données personnelles DP2 à DP6 dites « sensibles » (notées collectivement DPS).

Ces données personnelles DP1 à DP6 ne sont naturellement proposées ici qu'à titre
20 d'exemple non limitatif.

On comprend ici par donnée personnelle « sensible » le fait que l'on souhaite protéger cette donnée personnelle vis-à-vis d'une ou de multiples applications exécutées dans le terminal T, en particulier vis-à-vis de l'application APP dans cet exemple.

Dans un cas particulier, la ou les données personnelles sensibles DPS stockées en mémoire
25 dans le terminal T comprennent au moins l'une parmi :

- une donnée de contact d'utilisateur,
- une donnée d'agenda électronique,
- un favori d'un navigateur Internet,
- une donnée d'historique d'un navigateur Internet,
- 30 - une donnée de géolocalisation du terminal T, et
- une donnée électronique fournie par un objet connecté OB (décrit ultérieurement).

D'autres types de données personnelles peuvent toutefois être envisagés dans le cadre de l'invention.

A la demande de l'utilisateur, l'application APP a dans cet exemple été téléchargée depuis un fournisseur d'applications (non représenté) via le réseau de télécommunications R (Internet dans cet exemple), puis installée dans une mémoire du terminal T. L'application APP peut ensuite être exécutée par un processeur (non représenté) du terminal T. Cette application peut être une
5 quelconque application pouvant être téléchargée puis exécutée dans le terminal T (application d'achat, application d'aide à la localisation et/ou à la navigation, utilitaire quelconque...).

De façon connue, l'application APP mise en œuvre dans le terminal T est apte à accéder aux données personnelles DP lorsque ces dernières sont stockées dans la mémoire M1 (comme représentées en **figure 2**).

10 L'interface INT permet ici au terminal T de communiquer via le réseau de télécommunications R (Internet dans cet exemple) avec un serveur distant S. Le serveur distant S comprend ici une mémoire M3 et une unité de contrôle UC apte notamment à contrôler l'accès au contenu de la mémoire M3. Comme indiqué ci-après, la mémoire M3 est apte à stocker des données personnelles de l'utilisateur du terminal T.

15 La mémoire M3 représente une deuxième mémoire au sens de l'invention.

Le serveur S constitue par exemple tout ou partie d'un service informatique de stockage de données à distance (appelé communément « Cloud ») accessible par le terminal T par l'intermédiaire du réseau R. Dans un exemple particulier, l'accès au serveur S, et plus particulièrement au contenu de la mémoire M3, est sécurisé. Une identification et/ou une
20 authentification sont nécessaires pour accéder aux données personnelles sensibles DPS pouvant être stockées à distance dans la mémoire M3 du serveur S.

A noter que le serveur S peut également former tout ou partie d'un service de stockage de données domestiques (dit aussi « Cloud personnel »), c'est-à-dire situé dans l'environnement domestique de l'utilisateur. Il peut s'agir par exemple d'un serveur S externe au terminal T mais
25 inclus dans un même réseau résidentiel que le terminal T.

Comme déjà indiqué, le terminal T comprend par ailleurs une unité de gestion d'accès UG conforme à un mode de réalisation particulier de l'invention, cette unité UG étant apte à protéger l'accès aux données personnelles sensibles DPS de l'utilisateur. Pour ce faire, l'unité de gestion d'accès UG est configurée pour réaliser un traitement TR (cf. S4 décrite ci-après en référence à la
30 **figure 3**) de façon à empêcher l'application APP d'accéder à au moins une donnée personnelle sensible DPS dans la mémoire M1 du terminal T.

L'unité de gestion d'accès UG comprend dans une mémoire M2 un programme d'ordinateur PG et au moins une règle prédéterminée RL. Dans l'exemple considéré ici, l'unité de gestion d'accès UG est configurée pour déclencher le traitement TR mentionné ci-dessus sur détection
35 qu'au moins une condition prédéterminée (définie dans une règle RL) est remplie. Un exemple de

mise en œuvre d'une telle règle RL sera décrit plus en détail ultérieurement en référence à la **figure 3**.

La mémoire M2 constitue dans cet exemple un support d'enregistrement conforme à un mode de réalisation particulier de l'invention, lisible par l'unité de gestion d'accès UG (et plus généralement par le terminal T), et sur lequel est enregistré le programme d'ordinateur PG conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG comporte des instructions pour l'exécution des étapes d'un procédé de gestion d'accès selon un mode de réalisation particulier de l'invention. Les étapes S2 à S10 de ce procédé sont représentées, dans un mode particulier de réalisation de l'invention, sur la **figure 3** décrite ultérieurement.

La mémoire M2 est par exemple une mémoire non volatile réinscriptible ou une mémoire morte ROM. Dans un cas particulier, les mémoires M1 et M2 forment une seule et même mémoire dans le terminal T.

Dans cet exemple, le terminal T comprend également une unité de géolocalisation LOC qui permet de mettre en œuvre une fonction de géolocalisation du terminal T. L'inclusion notamment de cette unité de géolocalisation LOC dans le terminal T n'est toutefois pas indispensable pour mettre en œuvre la présente invention.

Dans le mode de réalisation considéré ici, l'unité de géolocalisation LOC est apte à fonctionner soit dans un mode normal, soit dans un mode secret. En mode normal, l'unité de géolocalisation LOC est apte à déterminer des coordonnées de géolocalisation représentatives de la localisation du terminal T. En mode secret, l'unité de géolocalisation LOC est configurée pour générer des données de géolocalisation fictives qui ne sont pas représentatives de la localisation du terminal T.

Dans l'exemple considéré ici, l'unité de géolocalisation LOC est apte à commuter entre le mode normal et le mode secret sous le contrôle de l'unité de gestion d'accès UG, comme expliqué plus en détail ultérieurement.

Toujours dans cet exemple, un dispositif électronique OB (dit « objet connecté ») est apte, lorsqu'il est connecté au terminal T, à coopérer avec ce dernier afin notamment de lui transmettre des données personnelles. Cet objet connecté OB peut comprendre par exemple un brassard électronique ou encore une montre. La connexion, et plus généralement l'usage, d'un tel objet connecté OB ne sont toutefois pas obligatoires pour mettre en œuvre la présente invention.

Un mode de réalisation particulier de l'invention est à présent décrit en référence aux **figures 2 et 3**. Pour ce faire, le terminal T (et plus précisément l'unité de gestion d'accès UG) met en œuvre un procédé de gestion d'accès en exécutant le programme PG.

On considère ici le cas particulier où les données personnelles DP1-DP6 stockées dans la mémoire M1 du terminal T sont définies comme suit :

- les données personnelles DP1 et DP2 sont des données de contact d'utilisateur (chacune de ces données DP1 et DP2 comprenant par exemple un numéro de téléphone) ;
- la donnée personnelle DP3 est une donnée d'agenda électronique (comprenant par exemple un événement associé à une date particulière) ;
- la donnée personnelle DP4 est une donnée de géolocalisation représentative de la localisation du terminal T à un instant donné ;
- la donnée personnelle DP5 comprend au moins l'une parmi une donnée d'historique d'un navigateur Internet et un favori Internet (ou « bookmark » en anglais) ; et
- la donnée personnelle DP6 est une donnée fournie par l'objet connecté OB lors d'une connexion établie entre le terminal T et l'objet connecté OB.

Comme déjà indiqué, l'unité de gestion d'accès UG est apte dans cet exemple à empêcher l'application APP d'accéder aux données personnelles sensibles DPS (à savoir DP2 à DP6) dans la mémoire M1 du terminal T.

On comprendra que la nature et la quantité des données personnelles (et en particulier des données personnelles dites sensibles) stockées dans la mémoire du terminal T peuvent varier selon le cas et que les données personnelles DP détaillées ci-dessus ne constituent qu'un exemple non limitatif de réalisation de l'invention.

Au cours d'une étape S2, l'unité de gestion d'accès UG détermine si au moins une condition prédéterminée définie dans une règle RL est satisfaite. Sur détection qu'une telle condition prédéterminée est satisfaite, l'unité de gestion d'accès UG procède à l'étape S4.

A l'étape S4, l'unité de gestion d'accès UG réalise un traitement TR comme déjà mentionné précédemment de façon à empêcher l'application APP d'accéder aux données personnelles sensibles DPS dans la mémoire M1 du terminal T.

Au cours de ce traitement TR, l'unité de gestion d'accès UG transfère (S6), via le réseau de télécommunications R, les données personnelles sensibles DPS (DP2 à DP6) du terminal T vers le serveur distant S.

De plus, toujours au cours de ce traitement TR, l'unité de gestion d'accès UG supprime (S8) les données personnelles sensibles DPS dans la mémoire M1 du terminal.

A l'issue du traitement TR réalisé en S4, les données personnelles sensibles DPS sont donc présentes dans la mémoire M3 mais plus dans la mémoire M1. Seule la donnée personnelle DP1 (non sensible) est ici maintenue par l'unité de gestion d'accès UG dans la mémoire M1 du terminal T. Bien que cela ne soit pas obligatoire, l'unité de gestion d'accès UG peut en outre être

configurée pour réaliser les étapes de transfert (S6) et de suppression (S8) pour la donnée personnelle non sensible DP1.

Le traitement TR ainsi réalisé par l'unité de gestion d'accès UG est avantageux en ce qu'il permet d'interdire l'accès par l'application APP aux données personnelles sensibles DPS. La
5 déposante a constaté qu'il est souvent difficile d'empêcher une telle application APP d'accéder à certaines données personnelles dans le terminal T. En stockant à distance les données personnelles sensibles DPS, et en supprimant celles-ci dans la mémoire M1 du terminal T, il n'est plus possible pour l'application APP de récupérer ces données DPS.

De cette manière, on peut protéger efficacement des données personnelles telles que des
10 données d'agenda, des contacts d'utilisateur, des données de géolocalisation ou encore des favoris Internet ou données d'historique.

De façon avantageuse, le terminal T (et plus précisément l'unité de gestion d'accès UG) est en outre apte à accéder, via le réseau de télécommunications R, à chaque donnée personnelle sensible DPS stockée à distance par le serveur distant S.

Divers mesures de sécurité (identification, authentification, cryptage...) peuvent par
15 ailleurs être mises en place au niveau du serveur S afin de contrôler (et bloquer si nécessaire) l'accès aux données personnelles sensibles stockées à distance par le serveur S.

Par ailleurs, il est possible de conserver en permanence certaines données personnelles dites non sensibles (ici DP1) dans la mémoire M1 du terminal T, en particulier lorsque l'utilisateur
20 souhaite pouvoir accéder rapidement à ces données, même en l'absence d'une connexion via le réseau de télécommunications R entre le terminal T et le serveur distant S. La donnée personnelle DP1 peut par exemple comprendre des données de contact (appels d'urgence...) auxquelles l'utilisateur souhaite pouvoir accéder à tout moment sans qu'il soit nécessaire de consulter le serveur distant S. En revanche, il convient de noter que la donnée personnelle DP1 n'est pas
25 protégée au sens de l'invention vis-à-vis de l'application APP puisqu'elle demeure dans la mémoire M1 du terminal T.

Dans un mode de réalisation particulier, si au moins une copie des données personnelles sensibles DPS faisant l'objet du traitement TR (S4) sont stockées dans une ou des mémoires du terminal T autres que M1, l'unité de gestion d'accès UG supprime chaque copie existante dans le
30 terminal T lors de l'étape de suppression S8.

Par ailleurs, le traitement TR est avantageux en ce qu'il peut est configuré pour permettre à l'application APP de fonctionner normalement dans le terminal T malgré la suppression des données personnelles sensibles DPS dans la mémoire M1.

Dans un mode de réalisation particulier, l'unité de gestion d'accès UG remplace (S10) en
35 outre, lors du traitement TR (S4), au moins une donnée personnelle sensible DPS, par une donnée

de remplacement différente de ladite donnée personnelle sensible. Comme expliqué plus en détail ci-après, cette donnée de remplacement peut être une donnée personnelle fictive générée ou obtenue par l'unité de gestion d'accès UG.

Comme déjà indiqué, la nature des données personnelles sensibles DPS peut varier selon le cas. Deux types de données personnelles sensibles peuvent en particulier être considérés pour une application APP donnée, à savoir :

- Type 1 : l'absence de cette donnée personnelle dans la mémoire M1 du terminal T n'empêche pas l'application APP de fonctionner normalement ;
- Type 2 : l'absence de cette donnée personnelle dans la mémoire M1 du terminal T empêche l'application APP de fonctionner normalement.

Dans certains cas, la suppression dans la mémoire M1 du terminal T d'une donnée personnelle sensible, telle qu'une donnée de géolocalisation du terminal T par exemple, peut poser problème si celle-ci est nécessaire à l'application APP pour fonctionner normalement (donnée personnelle sensible de type 2).

Dans un mode de réalisation particulier, lorsque la donnée personnelle sensible DPS stockée dans la mémoire M1 du terminal T est de type 2, l'unité de gestion d'accès UG remplace (S10) en outre lors du traitement TR (S4) cette donnée personnelle sensible DPS par une donnée personnelle fictive différente de la donnée personnelle sensible en question. Cette donnée personnelle fictive est par exemple une donnée du même type (contact, historique, donnée de géolocalisation...) que la donnée personnelle sensible supprimée et stockée à distance lors du traitement TR afin de ne pas déclencher d'erreur au niveau de l'application APP. Le terminal peut ainsi répondre à la requête de données personnelles de l'application APP (en lui fournissant une donnée fictive) sans pour autant dévoiler une donnée personnelle sensible que l'utilisateur souhaite protéger.

On considère par exemple le cas où la donnée personnelle sensible DP4 est une donnée nécessaire à l'application APP (donnée de type 2) pour fonctionner normalement. Dans ce cas, l'unité de gestion d'accès UG remplace (S10), lors du traitement TR (S4), la donnée personnelle sensible DP4 par une donnée fictive DP4F différente de la donnée DP4 en question. Cette donnée fictive DP4F est par exemple une donnée fictive de géolocalisation du terminal générée par l'unité de géolocalisation LOC en mode secret. Contrairement à la donnée DP4 générée par l'unité de géolocalisation LOC en mode normal, la donnée fictive DP4F n'est pas représentative de la localisation du terminal T.

Ainsi, l'unité de gestion d'accès UG permet à l'application APP de fonctionner normalement en accédant dans la mémoire M1 à la donnée fictive DP4F et ce, tout en protégeant la véritable donnée personnelle sensible DP4 stockée à distance dans la mémoire M3 du serveur S. Ce mode

de réalisation permet de masquer si besoin la position géographique de l'utilisateur vis-à-vis d'une application APP considérée comme malveillante ou trop curieuse.

Dans un mode de réalisation particulier, sur requête de l'utilisateur, l'unité de gestion d'accès UG commande la commutation de l'unité de géolocalisation LOC du mode normal au mode secret afin de masquer l'emplacement de l'utilisateur à l'application APP.

On comprendra que l'unité de gestion d'accès UG peut également être configurée pour remplacer une donnée personnelle sensible par une donnée fictive différente, quand bien même la donnée personnelle sensible en question est de type 1 (c.-à-d. pas nécessaire à l'application APP pour fonctionner normalement). En effet, l'application APP peut être configurée pour accéder à des données personnelles sensibles qui ne sont pas réellement utiles pour la mise en œuvre de ladite application APP, comme déjà expliqué précédemment.

Comme indiqué ci-avant, dans l'exemple considéré ici, l'unité de gestion d'accès UG déclenche en S4 le traitement TR lorsqu'au moins une condition prédéterminée est détectée comme étant satisfaite en S2. Ladite au moins une condition prédéterminée définit par exemple au moins l'une parmi :

- une quantité de données personnelles d'un type prédéterminé stockée dans la mémoire M1 ; et
- une condition de temps indiquant quand le traitement TR doit être initié.

Dans un mode de réalisation particulier, une règle RL prévoit que l'unité de gestion d'accès UG procède au traitement TR (S4) sur détection qu'un nombre maximum prédéterminé de contacts d'utilisateur stockés dans la mémoire M1 est atteint. Lorsque ce nombre maximum prédéterminé est atteint, l'unité de gestion d'accès UG réalise le traitement TR pour un certain nombre de contacts d'utilisateur présents dans la mémoire M1 de sorte à ce que le nombre de contacts d'utilisateur soit à nouveau inférieur au nombre maximum prédéterminé dans la mémoire M1. Diverses variantes de réalisation sont envisageables pour définir quelles données personnelles doivent ou non faire l'objet du traitement TR.

Selon une autre variante, conformément à une règle RL, l'unité de gestion d'accès UG est configurée pour réaliser périodiquement le traitement TR pour chaque donnée personnelle sensible DPS se trouvant dans la mémoire M1 du terminal T. Diverses variantes de réalisation sont envisageables pour adapter à quels moments le traitement TR doit être déclenché par l'unité de gestion d'accès UG.

A noter également qu'une donnée personnelle est par exemple définie ou non comme « sensible » (c.-à-d. devant faire l'objet du traitement TR) dans une règle RL. Dans un exemple particulier, une règle RL définit un ou une pluralité de types de données personnelles en tant que données personnelles sensibles à traiter par l'unité de gestion d'accès UG. Une configuration

préenregistrée de données personnelles définies ou non comme sensibles est par exemple proposée par défaut à l'utilisateur du terminal T.

Par ailleurs, dans un mode de réalisation particulier, ultérieurement au traitement TR, l'unité de gestion d'accès UG est apte à communiquer avec le serveur distant S afin de récupérer au moins une donnée personnelle sensible DPS stockée dans la mémoire M3.

Comme représenté en **figure 4**, pour accéder (S20) à une donnée personnelle sensible DPS stockée à distance, l'unité de gestion d'accès UG envoie (S22) par exemple une requête au serveur distant S.

L'envoi de cette requête est par exemple effectué après accord de l'utilisateur du terminal.

Par exemple, un code d'accès est demandé à l'utilisateur par l'unité de gestion via une interface graphique du terminal et la requête n'est transmise que si le code d'accès est valide.

En réponse à la requête transmise à l'étape S22, l'unité de gestion UG reçoit (S24) la donnée personnelle sensible DPS demandée en provenance du serveur distant S. Une fois obtenue, l'unité de gestion d'accès UG commande (S26) alors le stockage de la donnée personnelle sensible DPS ainsi récupérée dans la mémoire M1 du terminal T.

Une fois stockée dans la mémoire du terminal T, la donnée personnelle sensible DPS est alors à nouveau accessible localement par l'utilisateur mais également par l'application APP. Dans un cas particulier, afin de protéger au maximum l'accès à cette donnée personnelle sensible DPS, l'unité de gestion d'accès UG réalise dès que possible le traitement TR afin de renouveler le stockage à distance de la donnée personnelle sensible DPS en question.

Dans un mode de réalisation particulier, chaque donnée personnelle sensible DPS transférée (S6) lors du traitement TR vers le serveur distant S, est associée à un identifiant. Lors de l'étape S20, la requête envoyée au serveur distant S comprend au moins un identifiant correspondant à une donnée personnelle sensible DPS souhaitée. En réponse, l'unité de gestion d'accès UG reçoit à l'étape S24 la ou les données personnelles sensibles DPS correspondant à chaque identifiant fourni à l'étape S20.

De manière avantageuse, l'utilisateur peut ainsi commander le rapatriement sélectif vers son terminal T d'une ou plusieurs données personnelles sensibles DPS spécifiques stockées à distance par le serveur S.

Dans un mode de réalisation particulier, l'utilisateur accède à une page Internet dans un espace personnel mise à disposition par le serveur distant S. L'utilisateur peut alors chercher dans son espace personnel les données personnelles qu'il souhaite rapatrier sur son terminal T. Par exemple, lorsque l'utilisateur clique sur un contact d'utilisateur dans son espace personnel, les données du contact en question sont automatiquement transférées dans le terminal T puis le numéro du contact est composé automatiquement par le terminal T (fonction « click-to-dial »).

Dans les modes de réalisation décrits, les données personnelles sensibles sont transférées vers un serveur distant.

5 A titre d'alternative, ces données personnelles sensibles sont transférées dans une mémoire du terminal, autre que la mémoire M1. Cette mémoire dans laquelle les données personnelles sensibles sont transférées est non accessible par l'application APP. Elle représente une deuxième mémoire au sens de l'invention.

La présente invention trouve une application particulière dans la protection des données personnelles relatives à la santé de l'utilisateur qui sont susceptibles d'être stockées en mémoire dans un terminal de télécommunications.

10 Un homme du métier comprendra que les modes de réalisation et variantes décrits ci-avant ne constituent que des exemples non limitatifs de mise en œuvre de l'invention. En particulier, l'homme du métier pourra envisager une quelconque combinaison des variantes et modes de réalisation décrits ci-avant afin de répondre à un besoin bien particulier.

REVENDEICATIONS

- 5 **1.** Terminal de télécommunications (T) comprenant :
- une première mémoire (M1) ;
 - une application (APP) installée dans le terminal de télécommunications (T) et apte à accéder à au moins une donnée personnelle sensible (DP2-DP6) stockée dans la première mémoire, ladite au moins une donnée personnelle sensible étant associée
- 10 audit terminal ou à un utilisateur dudit terminal ;
- caractérisé en ce que le terminal de télécommunications comprend une unité de gestion d'accès (UG) apte à réaliser un traitement de façon à empêcher ladite application (APP) d'accéder à ladite au moins une donnée personnelle sensible (DPS) dans ladite première mémoire, ledit traitement comprenant :
- 15 a) le transfert, de ladite au moins une donnée personnelle sensible (DP2-DP6) vers deuxième mémoire ; et
- b) la suppression de ladite au moins une donnée personnelle sensible (DP2-DP6) dans la première mémoire (M1) ;
- l'unité de gestion d'accès étant apte à accéder à ladite au moins une donnée personnelle
- 20 sensible stockée dans ladite deuxième mémoire.
- 2.** Terminal selon la revendication 1, selon lequel ladite au moins une donnée sensible (DP1) comprend au moins l'une parmi :
- une donnée de contact d'utilisateur,
- 25 - une donnée d'agenda électronique,
- un favori d'un navigateur Internet,
 - une donnée d'historique d'un navigateur Internet,
 - une donnée de géolocalisation du terminal de télécommunications (T),
 - une donnée électronique fournie par un objet connecté (OB) au terminal de
- 30 télécommunications (T).
- 3.** Terminal selon la revendication 1 ou 2, dans lequel l'unité de gestion d'accès (UG) est configurée pour déclencher ledit traitement sur détection qu'au moins une condition prédéterminée (RL) est remplie.

4. Terminal selon la revendication 3, ladite au moins une condition prédéterminée (RL) définissant au moins l'une parmi :

- une quantité de données personnelles d'un type prédéterminé stockée dans la première mémoire ; et
- une condition de temps indiquant quand ledit traitement doit être initié.

5. Terminal selon l'une quelconque des revendications 1 à 4, l'unité de gestion d'accès (UG) étant configurée pour maintenir dans la première mémoire (M1) au moins une donnée personnelle prédéterminée (DP1) dite non sensible lorsque ladite suppression est réalisée.

6. Terminal selon l'une quelconque des revendications 1 à 5, dans lequel, lors dudit traitement, l'unité de gestion d'accès (UG) est configurée pour remplacer, dans ladite première mémoire (M1), ladite au moins une donnée personnelle sensible (DP4) par au moins une donnée fictive (DP4F) différente de ladite au moins une donnée personnelle sensible (DP4).

7. Terminal selon l'une quelconque des revendications 1 à 6, dans lequel le terminal de télécommunications (T) comprend une unité de géolocalisation (LOC) apte, dans un mode normal, à déterminer des coordonnées de géolocalisation représentatives de la localisation dudit terminal (T),

l'unité de gestion d'accès (UG) étant apte à commander la commutation de l'unité de géolocalisation (LOC) du mode normal vers un mode secret dans lequel l'unité de géolocalisation est configurée pour générer des données de géolocalisation fictives non représentatives de la localisation du terminal de télécommunications.

8. Terminal selon la revendication 7, dans lequel ladite au moins une donnée personnelle sensible (DP) comprend des données de géolocalisation (DP4) générées en mode normal par l'unité de géolocalisation (LOC),

l'unité de gestion d'accès étant configurée, lors du traitement, pour remplacer dans la première mémoire (M1) lesdites données de géolocalisation (DP4) par des données de géolocalisation fictives (DP4F) générées en mode secret par l'unité de géolocalisation (LOC).

9. Terminal selon l'une quelconque des revendications 1 à 8, dans lequel la deuxième mémoire est une mémoire d'un serveur distant, accessible par ledit terminal via un réseau de télécommunications et dans lequel, suite au traitement, l'unité de gestion d'accès (UG) est apte à envoyer au serveur distant une requête comprenant un identifiant d'au moins une donnée personnelle sensible (DPS) stockée par le serveur distant (S) et pour recevoir, en réponse à ladite requête, au moins une donnée personnelle sensible (DP2 – DP6) correspondant audit identifiant.

10. Système (SY) comprenant un terminal de télécommunications (T) selon l'une quelconque des revendications 1 à 9 et un serveur distant (S) apte à recevoir et à stocker ladite au moins une donnée personnelle sensible (DP2-DP6) transférée par l'unité de gestion d'accès du terminal de télécommunications.

11. Procédé de gestion d'accès mis en œuvre dans un terminal de télécommunications (T) comprenant une première mémoire (M1) dans laquelle est stockée au moins une donnée personnelle sensible (DP), ladite au moins une donnée personnelle sensible étant associée audit terminal ou à un utilisateur dudit terminal,

une application (APP), apte à accéder à ladite au moins une donnée personnelle sensible (DPS) dans la première mémoire, étant installée dans le terminal de télécommunications,

le procédé étant caractérisé en ce qu'il comprend un traitement (S4) réalisé par une unité de gestion d'accès (UG) du terminal de télécommunications (T) de façon à empêcher ladite application (APP) d'accéder à ladite au moins une donnée personnelle sensible (DPS) dans ladite première mémoire (M1), ledit traitement comprenant :

a) transfert (S6), de ladite au moins une donnée personnelle sensible (DPS) vers une deuxième mémoire ; et

b) suppression (S8) de ladite au moins une donnée personnelle sensible (DPS) dans la première mémoire (M1) ;

l'unité de gestion d'accès étant apte à accéder à ladite au moins une donnée personnelle sensible stockée dans ladite deuxième mémoire.

12. Procédé de gestion d'accès selon la revendication 11, comprenant, ultérieurement au traitement (S4), l'accès par l'unité de gestion d'accès (UG) nécessite un accord préalable de l'utilisateur.

- 13.** Programme d'ordinateur (PG) comportant des instructions pour la mise en œuvre d'un procédé de gestion d'accès selon la revendication 11 ou 12 lorsque ledit programme est exécuté par un ordinateur.
- 5 **14.** Support d'enregistrement (M1) lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur (PG) comprenant des instructions pour la mise en œuvre d'un procédé de gestion d'accès selon la revendication 11 ou 12.

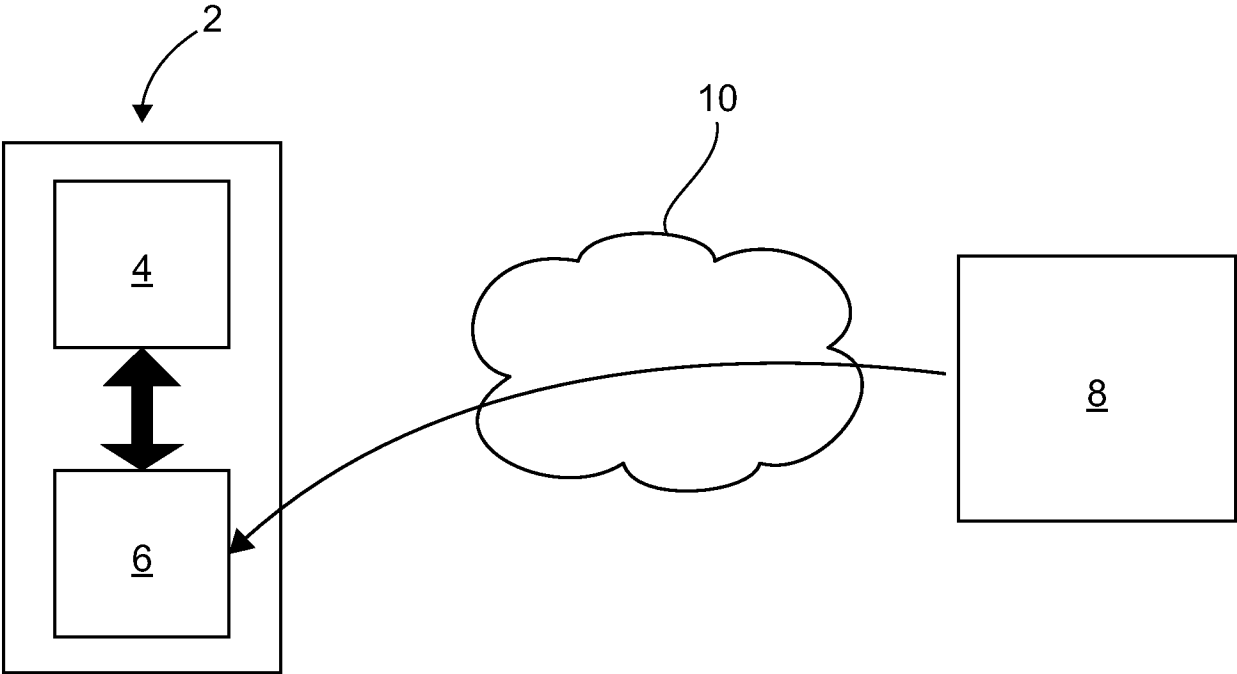


Fig. 1

ART ANTÉRIEUR

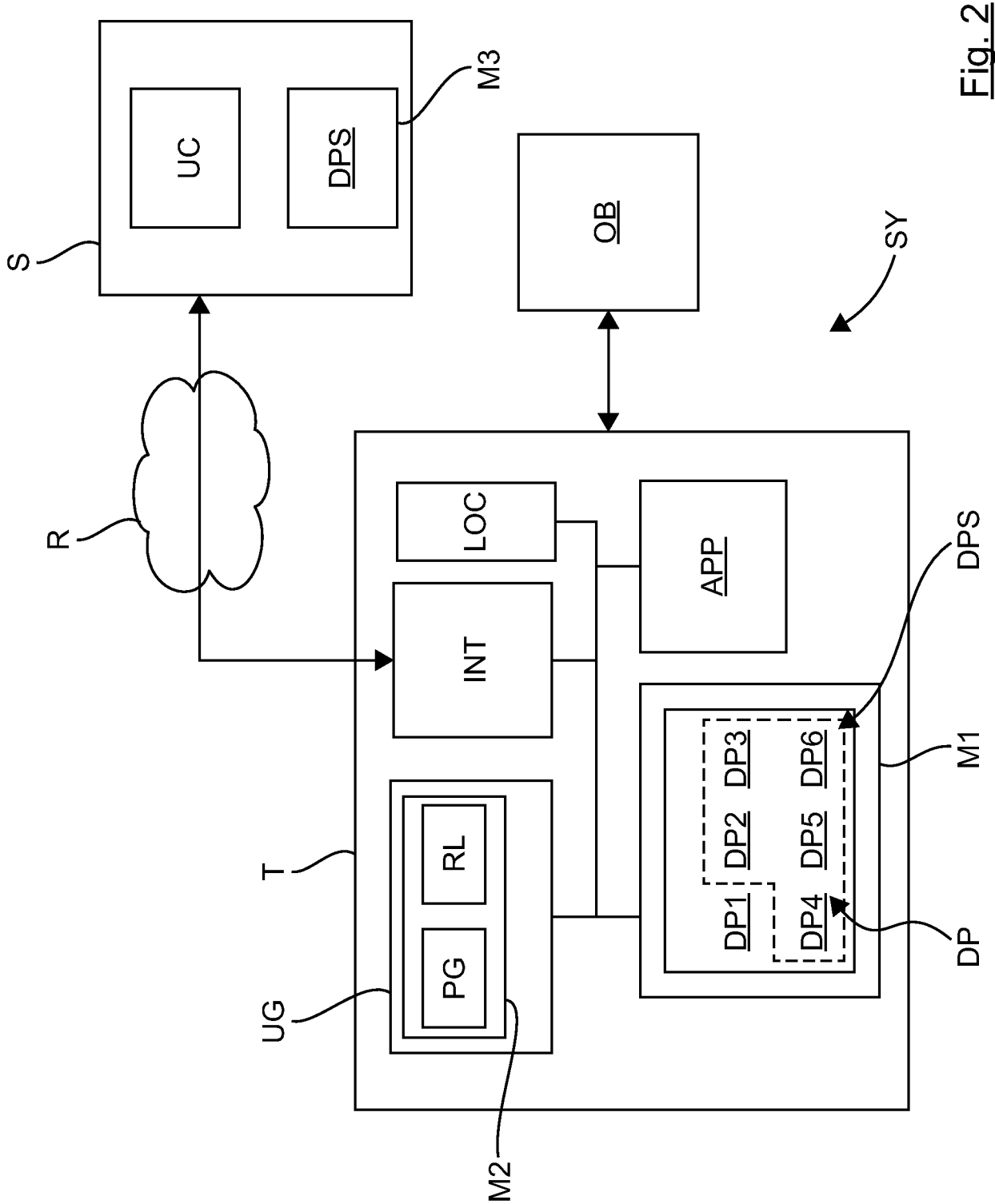


Fig. 2

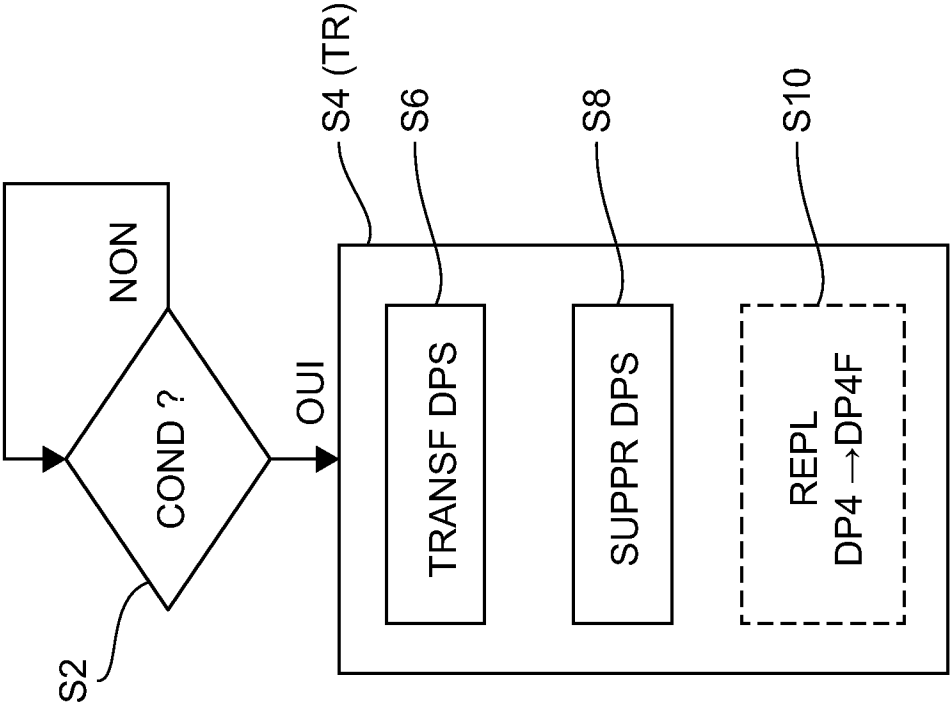


Fig. 3

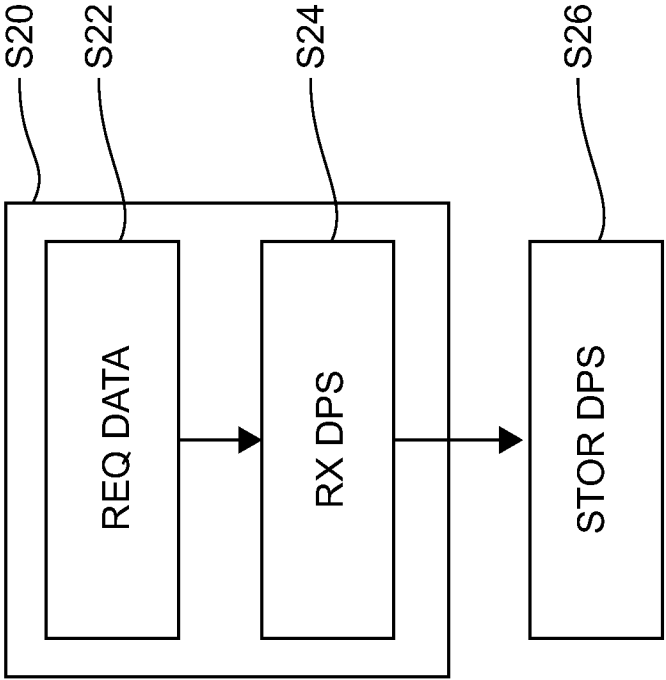


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2016/051264

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/02 H04W12/08
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)
H04W

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 2009/075630 A1 (MCLEAN IVAN H [US]) 19 March 2009 (2009-03-19) paragraphs [0002], [0004], [0033] paragraphs [0044], [0046], [0052] paragraphs [0059], [0081] -----	1-14
X	EP 2 120 431 A1 (NEC CORP [JP]) 18 November 2009 (2009-11-18) figure 1 paragraphs [0007], [0016], [0019] - [0020] paragraphs [0023] - [0025], [0035] paragraphs [0044] - [0046] -----	1-14
X	EP 2 017 767 A1 (HITACHI SOFTWARE ENG [JP]) 21 January 2009 (2009-01-21) paragraphs [0002], [0003], [0005] paragraphs [0023] - [0038] ----- -/-	1-14



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

6 September 2016

Date of mailing of the international search report

13/09/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Kufer, Léna

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2016/051264

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2 487 936 A1 (ARTILIUM UK LTD [GB]) 15 August 2012 (2012-08-15) figure 1 paragraphs [0003] - [0005], [0011] paragraphs [0015], [0017] - [0018] -----	1-14
A	WO 2015/006978 A1 (INTEL CORP [US]; PAN XIAOYONG [CN]; LIPMAN JUSTIN [CN]; HUANG YUHUAN []) 22 January 2015 (2015-01-22) figures 1,2 paragraphs [0031], [0035], [0037] paragraphs [0039], [0039], [0041] paragraph [0043] -----	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2016/051264

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009075630	A1	19-03-2009	CN 101803415 A 11-08-2010
			EP 2043396 A1 01-04-2009
			JP 2010539856 A 16-12-2010
			KR 20100072034 A 29-06-2010
			US 2009075630 A1 19-03-2009
			WO 2009039064 A1 26-03-2009

EP 2120431	A1	18-11-2009	CN 101606408 A 16-12-2009
			EP 2120431 A1 18-11-2009
			JP 5212116 B2 19-06-2013
			JP 5500222 B2 21-05-2014
			JP 2013021701 A 31-01-2013
			US 2010069038 A1 18-03-2010
			US 2012289194 A1 15-11-2012
			WO 2008096658 A1 14-08-2008

EP 2017767	A1	21-01-2009	CN 101371259 A 18-02-2009
			EP 2017767 A1 21-01-2009
			JP 4938011 B2 23-05-2012
			US 2010153716 A1 17-06-2010
			WO 2008129701 A1 30-10-2008

EP 2487936	A1	15-08-2012	NONE

WO 2015006978	A1	22-01-2015	US 2016255497 A1 01-09-2016
			WO 2015006978 A1 22-01-2015

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2016/051264

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. H04W12/02 H04W12/08 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) H04W		
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 2009/075630 A1 (MCLEAN IVAN H [US]) 19 mars 2009 (2009-03-19) alinéas [0002], [0004], [0033] alinéas [0044], [0046], [0052] alinéas [0059], [0081] -----	1-14
X	EP 2 120 431 A1 (NEC CORP [JP]) 18 novembre 2009 (2009-11-18) figure 1 alinéas [0007], [0016], [0019] - [0020] alinéas [0023] - [0025], [0035] alinéas [0044] - [0046] -----	1-14
X	EP 2 017 767 A1 (HITACHI SOFTWARE ENG [JP]) 21 janvier 2009 (2009-01-21) alinéas [0002], [0003], [0005] alinéas [0023] - [0038] ----- -/-	1-14
☒ 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 6 septembre 2016		Date d'expédition du présent rapport de recherche internationale 13/09/2016
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Kufer, Léna

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 2 487 936 A1 (ARTILIUM UK LTD [GB]) 15 août 2012 (2012-08-15) figure 1 alinéas [0003] - [0005], [0011] alinéas [0015], [0017] - [0018] -----	1-14
A	WO 2015/006978 A1 (INTEL CORP [US]; PAN XIAOYONG [CN]; LIPMAN JUSTIN [CN]; HUANG YUHUAN []) 22 janvier 2015 (2015-01-22) figures 1,2 alinéas [0031], [0035], [0037] alinéas [0039], [0039], [0041] alinéa [0043] -----	1-14

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2016/051264

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2009075630	A1	19-03-2009	CN 101803415 A	11-08-2010
			EP 2043396 A1	01-04-2009
			JP 2010539856 A	16-12-2010
			KR 20100072034 A	29-06-2010
			US 2009075630 A1	19-03-2009
			WO 2009039064 A1	26-03-2009

EP 2120431	A1	18-11-2009	CN 101606408 A	16-12-2009
			EP 2120431 A1	18-11-2009
			JP 5212116 B2	19-06-2013
			JP 5500222 B2	21-05-2014
			JP 2013021701 A	31-01-2013
			US 2010069038 A1	18-03-2010
			US 2012289194 A1	15-11-2012
			WO 2008096658 A1	14-08-2008

EP 2017767	A1	21-01-2009	CN 101371259 A	18-02-2009
			EP 2017767 A1	21-01-2009
			JP 4938011 B2	23-05-2012
			US 2010153716 A1	17-06-2010
			WO 2008129701 A1	30-10-2008

EP 2487936	A1	15-08-2012	AUCUN	

WO 2015006978	A1	22-01-2015	US 2016255497 A1	01-09-2016
			WO 2015006978 A1	22-01-2015
