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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
30 décembre 2015 (30.12.2015)

WIPO IPCT

(10) Numéro de publication internationale
WO 2015/197930 A1

(51) Classification internationale des brevets :
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2015/051415

(22) Date de dépôt international :
28 mai 2015 (28.05.2015)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1455854 24 juin 2014 (24.06.2014) FR

(71) Déposant : **OUTSCALE** [FR/FR]; 1 Rue Royale 319 Bureaux de la Colline, 92210 Saint Cloud (FR).

(72) Inventeurs : **SEROR, Laurent;** 10 rue du Maréchal Foch, 78570 Andresy (FR). **JUTTEAU, Jérôme;** 16 Parc de Béarn, 92210 Saint Cloud (FR).

(74) Mandataire : **NOVAGRAAF TECHNOLOGIES;** 2 Rue Sarah Bernhardt, CS90017, 92665 Asnieres sur Seine Cedex (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,

[Suite sur la page suivante]

(54) Title : METHOD OF SHARING DIGITAL FILES BETWEEN SEVERAL COMPUTERS, AND COMPUTER, DATA STORAGE ASSEMBLY AND DIGITAL FILE SHARING SYSTEM ASSOCIATED THEREWITH

(54) Titre : PROCÉDÉ DE PARTAGE DE FICHIERS NUMÉRIQUES ENTRE PLUSIEURS ORDINATEURS, ET ORDINATEUR, ENSEMBLE DE STOCKAGE DE DONNÉES ET SYSTÈME DE PARTAGE DE FICHIERS NUMÉRIQUES ASSOCIÉS

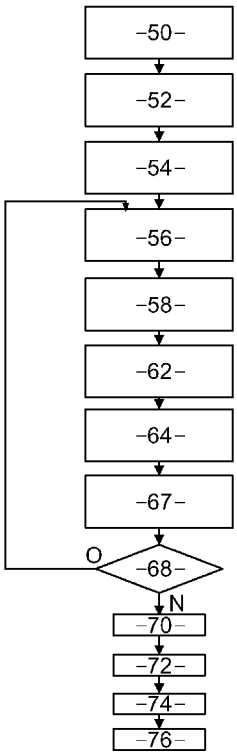

Fig. 2

(57) Abstract : The présent invention relates to a method of sharing digital files between several computers. The method comprises: · a step (50) of generating a public cryptographie key and a private cryptographie key, · a step (52) of transmitting said public cryptographie key, · a step (54) of storing said private cryptographie key, · a step (56) of generating a third cryptographie key, · a step (58) of applying a symmetric encryption algorithm, an encrypted digital file being obtained on completion of this application step, · a step (62) of downloading at least one public cryptographie key, · a step (64) of applying an asymmetric encryption algorithm to the third cryptographie key, a set of encrypted data being obtained on completion of this application step, · a step (67) of transmitting the encrypted digital file and the encrypted data set. The method also comprises répétition of the steps of generating a third cryptographie key, of applying a symmetric encryption algorithm, of applying an asymmetric encryption algorithm and of transmitting the encrypted digital file and the encrypted data set after each modification of the file.

(57) Abrégé : La présente invention concerne un procédé de partage de fichiers numériques entre plusieurs ordinateurs. Le procédé comprend : · une étape

[Suite sur la page suivante]

WO 2015/197930 A1

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))*

(50) de génération d'une clef cryptographique publique et d'une clef cryptographique privée, · une étape (52) de transmission de ladite clef cryptographique publique, · une étape (54) de stockage de ladite clef cryptographique privée, · une étape (56) de génération d'une troisième clef cryptographique, · une étape (58) d'application d'un algorithme de chiffrement symétrique, un fichier numérique chiffré étant obtenu à l'issue de cette étape d'application, · une étape (62) de téléchargement d'au moins une clef cryptographique publique, · une étape (64) d'application d'un algorithme de chiffrement asymétrique sur la troisième clef cryptographique, un ensemble de données chiffrées étant obtenu à l'issue de cette étape d'application, · une étape (67) de transmission du fichier numérique chiffré et de l'ensemble de données chiffrées. Le procédé comprend également une répétition des étapes de génération d'une troisième clef cryptographique, d'application d'un algorithme de chiffrement symétrique, d'application d'un algorithme de chiffrement asymétrique et de transmission du fichier numérique chiffré et de l'ensemble de données chiffrées après chaque modification du fichier.

PROCÉDÉ DE PARTAGE DE FICHIERS NUMÉRIQUES ENTRE PLUSIEURS ORDINATEURS, ET ORDINATEUR, ENSEMBLE DE STOCKAGE DE DONNÉES ET SYSTEME DE PARTAGE DE FICHIERS NUMÉRIQUES ASSOCIÉS

Domaine technique de l'invention

[01] La présente invention concerne les procédés et systèmes de partage de fichiers numériques entre plusieurs ordinateurs reliés via un réseau de communication. La présente invention trouve une application particulière dans les procédés et systèmes de partage de données confidentielles, telles que par exemple des données médicales de patients ou encore des données juridiques confidentielles.

Etat de la technique antérieure

[02] Il est connu des procédés de partage de fichiers numériques entre plusieurs ordinateurs reliés via un réseau de communication, typiquement via un réseau de communication offrant un accès internet. Chaque ordinateur est associé à un utilisateur, et au moins un fichier numérique destiné à être partagé est stocké sur l'ordinateur d'un premier utilisateur.

[03] Un procédé de ce type connu est par exemple le procédé fourni par la société Dropbox Inc. permettant de synchroniser des données informatiques et de les partager entre utilisateurs. Les données présentes sur l'ordinateur d'un premier utilisateur sont copiées puis envoyées avec l'assistance d'un logiciel dans un service de stockage permettant ensuite de les synchroniser et de les partager avec d'autres utilisateurs, autorisés par le premier utilisateur. Toutefois, les données synchronisées et partagées via un tel procédé sont potentiellement accessibles par un tiers dans les cas suivants:

- en cas de défaillance de sécurité du fournisseur du service de stockage, ou

- en cas de défaillance des méthodes de sécurisation du transport de la donnée entre l'utilisateur et le service de stockage, ou
- dans le cas où une autorité du pays où est stockée la donnée a le droit d'accéder à la donnée.

[04] Ceci introduit un risque quant à la sécurité du partage des données, en particulier un risque d'accès, par un utilisateur non autorisé, aux données partagées.

[05] Un autre procédé connu est le procédé proposé par le service internet MEGA permettant de partager un fichier via une application web dans le navigateur internet d'un premier utilisateur. Un lien de téléchargement vers ce fichier est alors mis à disposition de plusieurs autres utilisateurs. Dans le cadre de ce service, la donnée envoyée est chiffrée par l'application web coté client et empêche le fournisseur de service de stockage ou tout autre intermédiaire d'avoir accès aux données envoyées par l'utilisateur. En revanche, ce type de service ne permet pas la synchronisation des données entre utilisateurs.

[06] Il existe donc un réel besoin d'un procédé de partage de fichiers numériques palliant ces défauts, inconvénients et obstacles de l'art antérieur, en particulier d'un procédé permettant d'assurer de manière simple et fiable le partage et la synchronisation de données numériques, tout en améliorant le niveau de confidentialité des données partagées.

Exposé de l'invention

[07] Pour pallier à au moins un des inconvénients cités précédemment, l'invention a pour objet un procédé de partage de fichiers numériques entre plusieurs ordinateurs reliés via un réseau de communication, chaque ordinateur étant associé à un utilisateur et étant relié, via le réseau de communication, à un dispositif de stockage de clefs cryptographiques et à un ensemble de stockage de données, au moins un fichier numérique destiné à être partagé étant stocké sur un premier ordinateur d'un premier utilisateur, le procédé comprenant :

- une étape de génération, par le premier ordinateur et par au moins un ordinateur de chaque utilisateur distinct du premier utilisateur, d'une première clef cryptographique publique et d'une deuxième clef cryptographique privée associée à la clef cryptographique publique dans un algorithme de chiffrement asymétrique, la clef cryptographique publique étant associée à l'utilisateur dudit ordinateur,
- une étape de transmission au dispositif de stockage de clefs cryptographiques, par chaque ordinateur ayant généré une clef cryptographique publique, de ladite clef cryptographique publique,
- une étape de stockage, par chaque ordinateur ayant généré une clef cryptographique privée, de ladite clef cryptographique privée,
- une étape de génération, par le premier ordinateur, d'une troisième clef cryptographique unique et aléatoire,
- une étape d'application, par le premier ordinateur, sur au moins une donnée du fichier numérique destiné à être partagé, d'un algorithme de chiffrement symétrique ayant pour paramètre la troisième clef cryptographique, un fichier numérique chiffré comprenant ladite au moins une donnée étant obtenu à l'issue de cette étape d'application,
- une étape de téléchargement, depuis le dispositif de stockage, par le premier ordinateur, d'au moins une clef cryptographique publique associée à un deuxième utilisateur distinct du premier utilisateur,
- une étape d'application, par le premier ordinateur, sur la troisième clef cryptographique, d'un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique associée au premier utilisateur et d'un algorithme de chiffrement asymétrique ayant pour paramètre ladite au moins une clef cryptographique publique associée à un deuxième utilisateur, un ensemble comprenant au moins deux données chiffrées étant obtenu à l'issue de cette étape d'application,

- une étape de transmission à l'ensemble de stockage de données, par le premier ordinateur, du fichier numérique chiffré et de l'ensemble de données chiffrées ;

dans lequel l'étape de génération d'une troisième clef cryptographique unique et aléatoire, l'étape d'application d'un algorithme de chiffrement symétrique, l'étape d'application d'un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique associée au premier utilisateur et d'un algorithme de chiffrement asymétrique ayant pour paramètre ladite au moins une clef cryptographique publique associée à un deuxième utilisateur et l'étape de transmission du fichier numérique chiffré et de l'ensemble de données chiffrées sont ré-effectuées par le premier ordinateur après chaque nouvelle modification du fichier destiné à être partagé ou d'une partie de ce fichier.

[08] Grâce au fait que la troisième clef cryptographique est une clef unique, combiné à la caractéristique selon laquelle l'étape de génération d'une troisième clef cryptographique unique et aléatoire, l'étape d'application d'un algorithme de chiffrement symétrique, l'étape d'application d'un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique associée au premier utilisateur et d'un algorithme de chiffrement asymétrique ayant pour paramètre ladite au moins une clef cryptographique publique associée à un deuxième utilisateur et l'étape de transmission du fichier numérique chiffré et de l'ensemble de données chiffrées sont ré-effectuées par le premier ordinateur après chaque nouvelle modification du fichier destiné à être partagé ou d'une partie de ce fichier, l'accès aux données du fichier par un intermédiaire ou tiers non autorisé est empêché de manière simple et automatique. En particulier, en cas de modifications ultérieures de ces données, un tiers non autorisé est avantageusement empêché d'accéder au fichier chiffré en utilisant une clef symétrique forgée par lui même.

[09] En outre, grâce au fait que chaque clef cryptographique privée, permettant le déchiffrement des données, est une clef gardée secrète par l'ordinateur l'ayant générée, combiné à l'application, sur la troisième clef cryptographique ayant servi au chiffrement symétrique du fichier à partager, d'un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique associée au premier utilisateur et d'un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique associée à un deuxième utilisateur, le niveau de confidentialité des données partagées est encore amélioré. En particulier, même le fournisseur du service de stockage de données ne peut avoir accès aux données du fichier partagé.

[10] Dans une réalisation particulière de l'invention, le fichier destiné à être partagé comprend au moins une métadonnée, et l'algorithme de chiffrement symétrique est en outre appliqué sur ladite métadonnée lors de l'étape d'application, par le premier ordinateur, d'un algorithme de chiffrement symétrique sur au moins une donnée du fichier numérique destiné à être partagé.

[11] Cette caractéristique permet de réduire le risque lié à un déchiffrement, par un tiers non autorisé, des données partagées, par exemple par une attaque de type attaque par similitude. Ceci permet ainsi d'augmenter le niveau de confidentialité des données partagées.

[12] Selon une caractéristique technique particulière de l'invention, la clef cryptographique privée est stockée dans un support d'enregistrement amovible connecté à une unité centrale de l'ordinateur, et l'accès au support d'enregistrement amovible est protégé par un mot de passe.

[13] Une telle caractéristique permet de réduire le risque de piratage d'une mémoire interne de l'ordinateur afin d'accéder à la clef cryptographique privée, et permet ainsi d'augmenter le niveau de confidentialité des données partagées.

[14] Avantageusement, le support d'enregistrement amovible comprend un composant de chiffrement cryptographique de données, et la clef

cryptographique privée est chiffrée par le composant de chiffrement lors de l'étape de stockage au sein du support d'enregistrement.

[15] Cette caractéristique permet d'augmenter le niveau de confidentialité des données partagées.

[16] Selon une caractéristique technique particulière de l'invention, l'étape d'application d'un algorithme de chiffrement symétrique comprend en outre l'adjonction d'une signature numérique à la ou chaque donnée chiffrée du fichier numérique chiffré, la signature numérique étant associée à ladite donnée.

[17] L'adjonction d'une telle signature permet à un utilisateur déchiffrant le fichier chiffré de vérifier, lors du déchiffrement, l'identité de l'utilisateur associé au fichier chiffré, et/ou de vérifier l'intégrité des données chiffrées. L'utilisateur peut ainsi s'assurer que les données chiffrées n'ont pas été altérées pendant leur transport ou pendant leur stockage au sein de l'ensemble de stockage de données.

[18] Dans une réalisation particulière de l'invention, au cours de l'étape d'application d'un algorithme de chiffrement symétrique, l'algorithme de chiffrement symétrique est également appliqué sur la signature numérique.

[19] Cette caractéristique permet d'augmenter encore le niveau de confidentialité des données partagées.

[20] Selon une caractéristique technique particulière de l'invention, le procédé comprend en outre une étape de téléchargement, depuis l'ensemble de stockage, par le premier ordinateur, de la donnée chiffrée associée au premier utilisateur; et une étape de détection, par le premier ordinateur, si des différences existent entre des données ou métadonnées du fichier numérique stocké sur le premier ordinateur et des données et métadonnées du fichier numérique chiffré stocké dans l'ensemble de stockage, et de détermination des dates de modification respectives du fichier numérique et du fichier numérique chiffré.

[21] Cette caractéristique permet de procéder à une synchronisation des données du fichier entre le premier ordinateur et l'ensemble de stockage.

[22] Selon un autre aspect, l'invention a aussi pour objet un ordinateur muni de moyens de génération de clefs cryptographiques, de moyens d'application d'un algorithme de chiffrement symétrique et d'un algorithme de chiffrement asymétrique sur des données informatiques, d'au moins une mémoire adaptée pour stocker au moins un fichier numérique destiné à être partagé et d'au moins une mémoire adaptée pour stocker au moins une clef cryptographique, l'ordinateur étant propre à mettre en œuvre le procédé de partage de fichiers numériques tel que défini ci-dessus, l'ordinateur étant le premier ordinateur du procédé.

[23] Dans une réalisation particulière de l'invention, l'ordinateur comprend en outre au moins un processeur, et la mémoire comprend une application, l'application étant propre, lorsqu'elle est exécutée par ledit au moins un processeur, à mettre en œuvre le procédé de partage de fichiers numériques tel que défini ci-dessus, l'application comprenant les moyens de génération de clefs cryptographiques et les moyens d'application d'un algorithme de chiffrement symétrique et d'un algorithme de chiffrement asymétrique sur des données informatiques.

[24] Selon un autre aspect, l'invention a aussi pour objet un ensemble de stockage de données propre à être relié à plusieurs ordinateurs via un réseau de communication, pour le partage de fichiers numériques entre les ordinateurs, chaque ordinateur étant associé à un utilisateur, au moins un des ordinateurs étant tel que défini ci-dessus, l'ensemble de stockage étant propre à stocker des données chiffrées et des fichiers numériques chiffrés destinés à être partagés entre les ordinateurs.

[25] Selon un autre aspect, l'invention a aussi pour objet un système de partage de fichiers numériques, comprenant :

- une pluralité d'ordinateurs reliés via un réseau de communication, chaque ordinateur étant associé à un utilisateur, au moins un des ordinateurs étant tel que défini ci-dessus,
- un dispositif de stockage de clefs cryptographiques, relié à chaque ordinateur via le réseau de communication,

- un ensemble de stockage de données, relié à chaque ordinateur via le réseau de communication, l'ensemble de stockage étant tel que défini ci-dessus.

[26] Selon un autre aspect, l'invention a également pour objet un produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou enregistré sur un support lisible par ordinateur et/ou exécutable par un processeur, comprenant des instructions de programme adaptées pour mettre en œuvre le procédé tel que défini ci-dessus lorsque le produit programme est exécuté sur un ordinateur.

Brève description des figures

[27] L'invention sera mieux comprise à la lecture de la description qui suit, faite uniquement à titre d'exemple, et en référence aux figures en annexe dans lesquelles :

- la figure 1 est une représentation schématique d'un réseau de communication destiné à transporter des fichiers numériques entre plusieurs ordinateurs, auquel est connecté un système de partage des fichiers numériques selon un mode de réalisation de l'invention, le système comprenant deux ordinateurs ;
- la figure 2 est un organigramme représentant le fonctionnement du système de partage de fichiers numériques de la figure 1, et comprenant un procédé de partage de fichiers numériques selon un mode de réalisation de l'invention, mis en œuvre par les ordinateurs de la figure 1 ;
- la figure 3 représente schématiquement et fonctionnellement un des ordinateurs de la figure 1, mettant en œuvre, via une application dédiée, le procédé de partage de fichiers numériques selon un mode de réalisation de l'invention ;
- la figure 4 représente schématiquement et fonctionnellement l'autre ordinateur de la figure 1, mettant en œuvre, via une application dédiée, un procédé de récupération de fichiers numériques selon un mode

de réalisation de l'invention, ledit procédé correspondant à certaines étapes de l'organigramme de la figure 2.

Description détaillée d'un mode de réalisation

[28] Dans la suite, il est divulgué en particulier un procédé de partage de fichiers numériques 2 entre plusieurs ordinateurs.

[29] Dans la suite de la description, on entend par « clef cryptographique » une clef de chiffrement cryptographique, c'est-à-dire un paramètre utilisé en entrée d'une opération cryptographique.

[30] On entend en outre par « modification d'un fichier numérique » toute altération partielle ou totale de celui-ci. Par exemple, dans le cas d'une suppression d'un fichier numérique, la modification considérée est une altération totale du fichier.

[31] On entend également par « ordinateur » tout dispositif électronique muni de moyens de calcul de données et de moyens de stockage de données, tel que par exemple un ordinateur de bureau, un ordinateur portable, un appareil de communication sans fil tel qu'un smartphone, ou encore une tablette numérique, sans que cette liste ne soit exhaustive.

[32] Un réseau de communication 4 destiné à transporter les fichiers numériques 2 est représenté schématiquement sur la figure 1. Un système 6 de partage des fichiers numériques 2 est connecté au réseau de communication 4.

[33] Le réseau de communication 4 est muni d'une infrastructure de communication privée ou étendue permettant la connexion, ou l'accès, à des équipements de communication de type serveurs et/ou bases de données. De manière classique, l'infrastructure de communication forme un réseau sans fil, ou un réseau filaire, ou encore un réseau comprenant une portion sans fil et une portion filaire. Dans un mode de réalisation particulier, le réseau de communication 4 est conçu comme un réseau de type internet.

[34] Le système de partage 6 comprend plusieurs ordinateurs 8A, 8B, un dispositif 10 de stockage de clefs cryptographiques et un ensemble 12 de stockage de données, tous reliés au réseau de communication 4. Dans l'exemple de réalisation de la figure 1, le système de partage 6 comprend un premier ordinateur 8A et un second ordinateur 8B.

[35] Chaque ordinateur 8A, 8B est associé à un utilisateur. Dans l'exemple de réalisation de la figure 1, le premier ordinateur 8A est associé à un premier utilisateur et le second ordinateur 8B est associé à un second utilisateur, distinct du premier utilisateur. En variante non représentée, plusieurs ordinateurs peuvent être associés à un même utilisateur. En d'autres termes, chaque utilisateur peut être associé à un ou plusieurs des ordinateurs du système de partage 6.

[36] Au moins un ordinateur de chaque utilisateur comprend des moyens 16 de génération de clefs cryptographiques et des moyens 21 d'application d'un algorithme de chiffrement symétrique et d'un algorithme de chiffrement asymétrique sur des données informatiques, comme représenté sur la figure 3. Dans l'exemple de réalisation de la figure 1, le premier ordinateur 8A et le second ordinateur 8B comprennent chacun des moyens 16 de génération de clefs cryptographiques et des moyens 21 d'application d'un algorithme de chiffrement symétrique et d'un algorithme de chiffrement asymétrique sur des données informatiques. Chaque ordinateur 8A, 8B est muni également d'une unité centrale 18 comprenant au moins un processeur 19, et d'au moins une mémoire 20 adaptée pour stocker au moins une clef cryptographique. Dans l'exemple de réalisation de la figure 1, chaque ordinateur 8A, 8B est muni d'un processeur 19 et d'une mémoire 20. Chaque ordinateur 8A, 8B comporte en outre un périphérique d'entrée utilisateur et des moyens d'émission et de réception de données connectés au réseau de communication 4, ces éléments n'étant pas représentés sur la figure 1 pour des raisons de clarté.

[37] Le premier ordinateur 8A comprend en outre au moins une mémoire 22 adaptée pour stocker au moins un fichier numérique 2 destiné à être

partagé. Dans l'exemple de réalisation de la figure 1, le premier ordinateur 8A comprend une mémoire 22 agencée dans l'unité centrale 18.

[38] Comme illustré sur la figure 3, les moyens de génération 16 sont propres à générer, par mise en œuvre d'un algorithme de chiffrement asymétrique, un jeu de clefs asymétriques comprenant une première clef cryptographique publique 25 et une deuxième clef cryptographique privée 26. En particulier, les moyens de génération 16 du premier ordinateur 8A sont propres à générer un jeu de clefs asymétriques comprenant une première clef cryptographique publique 25A et une deuxième clef cryptographique privée 26A, et les moyens de génération 16 du second ordinateur 8B sont propres à générer un jeu de clefs asymétriques comprenant une première clef cryptographique publique 25B et une deuxième clef cryptographique privée 26B.

[39] Ainsi, la clef cryptographique publique 25A, 25B est associée à l'utilisateur de l'ordinateur 8A, 8B l'ayant générée respectivement. La clef cryptographique privée 26A, respectivement 26B est associée à la clef cryptographique publique 25A, respectivement 25B dans l'algorithme de chiffrement asymétrique. L'algorithme de chiffrement asymétrique est par exemple un algorithme de type RSA (Rivest Shamir Adleman), connu en soi, et les clefs publique et privée 25A, 25B, 26A, 26B sont, par exemple, des clefs asymétriques RSA 4096 bits.

[40] En outre, comme représenté sur la figure 3, les moyens de génération 16 du premier ordinateur 8A sont propres également à générer une troisième clef cryptographique 27 unique et aléatoire.

[41] La troisième clef cryptographique 27 est une chaîne de caractères aléatoire de longueur donnée. Dans un exemple de réalisation particulier, la troisième clef cryptographique 27 est une clef symétrique, par exemple une clef symétrique AES (de l'anglais Advanced Encryption Standard) 256 bits.

[42] Comme représenté sur les figures 3 et 4, les moyens d'application 21 comportent un composant 28A d'application d'un algorithme de chiffrement

symétrique, et un composant 28B d'application d'un algorithme de chiffrement asymétrique. Les moyens d'application 21 du premier ordinateur 8A sont adaptés pour appliquer, sur au moins une donnée du fichier numérique 2 destiné à être partagé, un algorithme de chiffrement symétrique ayant pour paramètre la troisième clef cryptographique 27. Les moyens d'application 21 du premier ordinateur 8A sont propres en outre à appliquer, sur la troisième clef cryptographique 27, un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique 25A associée au premier utilisateur. Ils sont propres également à appliquer, sur la troisième clef cryptographique 27, un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique 25B associée au deuxième utilisateur.

[43] L'algorithme de chiffrement symétrique est par exemple un algorithme de type AES, ou encore un algorithme de type Blowfish, connu en soi.

[44] Le ou chaque algorithme de chiffrement asymétrique est par exemple un algorithme de type RSA.

[45] De manière préférentielle, les moyens d'application 21 du premier ordinateur 8A sont propres en outre à adjoindre une signature numérique à la ou chaque donnée informatique chiffrée du fichier numérique chiffré. La signature numérique est par exemple une signature numérique de type SHA (Secure Hash Algorithm). Dans un mode de réalisation particulier, les moyens d'application 21 du premier ordinateur 8A sont en outre adaptés pour appliquer, sur la signature numérique, l'algorithme de chiffrement symétrique ayant pour paramètre la troisième clef cryptographique 27.

[46] Dans le mode de réalisation préférentiel illustré sur la figure 1, la mémoire 20 est un support d'enregistrement amovible connecté à l'unité centrale 18 de l'ordinateur 8A, 8B. En variante non représentée, la mémoire 20 est une mémoire interne de l'ordinateur 8A, 8B, par exemple une mémoire non-éphémère. En variante encore, la mémoire 20 est un support de stockage apte à être généré par l'ordinateur, à destination de

l'utilisateur de l'ordinateur. Selon cette variante, la mémoire 20 est par exemple un support papier apte à être imprimé, tel qu'un code QR ou encore un support contenant des données imprimées sous une représentation texte de type base64 par exemple. L'accès à la mémoire 20 est par exemple protégé par un mot de passe, par exemple un mot de passe de type phrase secrète.

[47] De manière préférentielle, le support d'enregistrement amovible 20 connecté à l'unité centrale 18 comporte un composant 29 apte à chiffrer cryptographiquement des données stockées sur le support d'enregistrement 20. Le support d'enregistrement amovible 20 est par exemple le dispositif TrustWay® RCI développé par la société BULL.

[48] Dans le mode de réalisation particulier illustré sur la figure 1, la mémoire 22 comprend une application 30. La mémoire 22 est par exemple une mémoire non-éphémère.

[49] L'application 30 est par exemple une application téléchargeable depuis le réseau de communication 4, via une plateforme de téléchargement non représentée sur les figures. L'application 30 comporte des instructions de programme adaptées pour mettre en œuvre le procédé de partage de fichiers numériques 2 selon l'invention, comme décrit par la suite.

[50] Comme représenté sur le mode de réalisation de la figure 3, l'application 30 comprend les moyens 16 de génération de clefs cryptographiques et les moyens 21 d'application d'un algorithme de chiffrement symétrique et d'un algorithme de chiffrement asymétrique sur des données informatiques.

[51] Selon ce mode de réalisation, les moyens de génération 16 sont formés d'un module logiciel de génération de clefs cryptographiques, et les moyens d'application 21 sont formés d'un module logiciel d'application d'un algorithme de chiffrement symétrique et d'un algorithme de chiffrement asymétrique sur des données informatiques.

[52] En variante non représentée, l'application 30 ne comporte pas les moyens 16 de génération de clefs cryptographiques et les moyens 21 d'application d'un algorithme de chiffrement symétrique et d'un algorithme de chiffrement asymétrique sur des données informatiques, et ceux-ci sont réalisés sous forme de composants matériels. En variante encore, la mémoire 22 ne comprend pas d'application 30.

[53] L'application 30 est propre, lorsqu'exécutée par le processeur 19, à déterminer si le fichier numérique 2 ou une partie du fichier numérique 2 a, ou non, été modifié(e) dans la mémoire 22 de l'ordinateur.

[54] Dans un mode de réalisation particulier, l'application 30 est propre, lorsqu'exécutée par le processeur 19, à détecter si des différences existent entre les données ou métadonnées d'un fichier numérique 2 stocké dans la mémoire 22 et les données ou métadonnées d'un fichier numérique chiffré stocké dans l'ensemble de stockage 12. Selon ce mode de réalisation particulier, l'application 30 est propre en outre, lorsqu'exécutée par le processeur 19, à déterminer une date de modification d'un fichier numérique 2 stocké dans la mémoire 22 et/ou d'un fichier numérique chiffré stocké dans l'ensemble de stockage 12.

[55] Le dispositif 10 de stockage de clefs cryptographiques est relié à chaque ordinateur 8A, 8B via le réseau de communication 4. Dans l'exemple de réalisation de la figure 1, le dispositif de stockage 10 comprend un serveur 32 relié à une base de données 34. Dans cet exemple de réalisation, le dispositif de stockage 10 est propre, par exemple, à mettre en œuvre un service de stockage en ligne de type Google Drive® (service développé par la société Google Inc.). En variante de réalisation non représentée, le dispositif de stockage 10 comprend un service web permettant l'authentification des utilisateurs, connecté à la base de données 34.

[56] La base de données 34 est propre à stocker les clefs cryptographiques publiques 25A, 25B associées aux différents utilisateurs. Dans l'exemple de réalisation de la figure 1, la base de données 34 est

propre à stocker la clef cryptographique publique 25A associée au premier utilisateur et la clef cryptographique publique 25B associée au second utilisateur.

[57] L'ensemble 12 de stockage de données est relié à chaque ordinateur 8A, 8B via le réseau de communication 4. L'ensemble de stockage 12 est propre à stocker les fichiers numériques chiffrés destinés à être partagés entre les ordinateurs 8A, 8B. L'ensemble de stockage 12 est propre en outre à stocker des données chiffrées, comme décrit plus en détail par la suite. Dans l'exemple de réalisation de la figure 1, l'ensemble de stockage 12 comprend un serveur de stockage 36.

[58] Le serveur 36 est par exemple un serveur fournissant des services de type FTP (de l'anglais File Transfer Protocol), ou encore des services de type Amazon® S3 (Amazon est une marque de la société Amazon Web Services).

[59] En variante de réalisation, l'ensemble 12 de stockage de données comprend au moins un serveur relié à au moins une base de données.

[60] Le fonctionnement du système 6 de partage de fichiers numériques 2 va maintenant être décrit en détail, en référence aux figures 2, 3 et 4. En particulier, le procédé de partage de fichiers numériques 2 selon l'invention, mis en œuvre par les ordinateurs 8A, 8B du système de partage 6, va être décrit en référence aux figures 2 et 3.

[61] On suppose qu'initialement, au moins un fichier numérique 2 destiné à être partagé est stocké dans la mémoire 22 du premier ordinateur 8A.

[62] Dans le mode de réalisation particulier des figures 1 et 3, l'application 30 est alors exécutée par le processeur 19 du premier ordinateur 8A, et les instructions de programme de l'application 30 mettent en œuvre le procédé de partage du fichier numérique 2.

[63] Au cours d'une première étape 50, le premier ordinateur 8A et au moins un ordinateur de chaque utilisateur distinct du premier utilisateur génèrent un jeu de clefs asymétriques comprenant une première clef cryptographique publique 25 et une deuxième clef cryptographique privée

26. La clef cryptographique privée 26 est associée à la clef cryptographique publique 25. Dans l'exemple de réalisation des figures 1 et 3, les moyens de génération 16 du premier et du second ordinateurs 8A, 8B génèrent chacun une clef cryptographique publique 25A, 25B respective, ainsi qu'une clef cryptographique privée 26A, 26B respective.

[64] Au cours d'une étape suivante 52, chaque ordinateur 8A, 8B ayant généré une clef cryptographique publique 25A, 25B transmet cette clef cryptographique publique 25A, 25B au dispositif de stockage 10. La base de données 34 du dispositif de stockage 10 stocke alors l'ensemble des clef cryptographiques publiques 25A, 25B transmises. Dans la variante de réalisation selon laquelle le dispositif de stockage 10 comprend un service web, l'étape de transmission 52 comprend en outre l'authentification, auprès du service web, de chaque utilisateur associé à un des ordinateurs 8A, 8B ayant généré une clef cryptographique publique 25A, 25B.

[65] Au cours d'une étape suivante 54, chaque ordinateur 8A, 8B ayant généré une clef cryptographique privée 26A, 26B stocke cette clef. Dans le mode de réalisation préférentiel illustré sur la figure 1, chaque clef cryptographique privée 26A, 26B générée est stockée, au cours de l'étape 54, dans un des supports d'enregistrement amovibles 20. De préférence, chaque clef cryptographique privée 26A, 26B est chiffrée, au cours de l'étape 54, par le composant de chiffrement 29 d'un des supports d'enregistrement amovibles 20.

[66] En variante, l'étape de stockage 54 est effectuée en parallèle de l'étape de transmission 52.

[67] Au cours d'une étape suivante 56, le premier ordinateur 8A génère une troisième clef cryptographique 27 unique et aléatoire. Plus précisément, au cours de l'étape 56, les moyens de génération 16 du premier ordinateur 8A génèrent la troisième clef cryptographique 27, comme représenté sur la figure 3.

[68] En variante, l'étape de génération 56 est effectuée en parallèle de l'étape de stockage 54 et/ou de l'étape de transmission 52 et/ou de l'étape de génération 50.

[69] Au cours d'une étape suivante 58, le premier ordinateur 8A applique, sur au moins une donnée du fichier numérique 2, un algorithme de chiffrement symétrique ayant pour paramètre la troisième clef cryptographique 27. En particulier, dans l'exemple de réalisation des figures 1 et 3, le composant 28A applique, sur au moins une donnée du fichier numérique 2, l'algorithme de chiffrement symétrique ayant pour paramètre la troisième clef cryptographique 27.

[70] De préférence, l'étape d'application 58 comprend en outre l'adjonction d'une signature numérique à la ou chaque donnée chiffrée du fichier numérique chiffré. Les moyens d'application 51 associent la signature numérique à la ou chaque donnée chiffrée. Dans un mode de réalisation particulier, les moyens d'application 51 appliquent également l'algorithme de chiffrement symétrique sur la signature numérique.

[71] Selon un mode de réalisation particulier, le fichier numérique 2 destiné à être partagé comprend au moins une métadonnée, telle que par exemple le nom du fichier 2, la taille du fichier 2 et/ou la date de modification du fichier 2. Selon ce mode de réalisation, l'algorithme de chiffrement symétrique est en outre appliqué, par le premier ordinateur 8A, au cours de l'étape 58, sur la ou chaque métadonnée du fichier numérique 2.

[72] Un fichier numérique chiffré 60 comprenant la ou chaque donnée et/ou métadonnée chiffrée est obtenu à l'issue de l'étape d'application 58.

[73] Au cours d'une étape suivante 62, le premier ordinateur 8A télécharge, depuis le dispositif de stockage 10, au moins une clef cryptographique publique 25 associée à un utilisateur distinct du premier utilisateur. Dans l'exemple de réalisation des figures 1 et 3, le premier ordinateur 8A télécharge, depuis le dispositif de stockage 10, la clef cryptographique publique 25B associée au deuxième utilisateur.

[74] En variante, l'étape de téléchargement 62 est effectuée en parallèle de l'étape d'application 58 et/ou de l'étape de génération 56 et/ou de l'étape de stockage 54.

[75] Au cours d'une étape suivante 64, le premier ordinateur 8A applique, sur la troisième clef cryptographique 27, un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique 25A associée au premier utilisateur. Le premier ordinateur 8A applique en outre, sur la troisième clef cryptographique 27, au moins un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique 25 publique associée à un utilisateur distinct du premier utilisateur, autorisé par le premier utilisateur à accéder au fichier 2. Dans l'exemple de réalisation des figures 1 et 3, le composant 28B applique, sur la troisième clef cryptographique 27, un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique 25A associée au premier utilisateur et un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique 25B associée au deuxième utilisateur. L'application, sur la troisième clef cryptographique 27, d'un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique 25A associée au premier utilisateur permet d'effectuer la synchronisation des données du fichier 2 entre le premier ordinateur 8A et l'ensemble de stockage 12, comme détaillé par la suite.

[76] Un ensemble 65 comprenant au moins deux données chiffrées est obtenu à l'issue de l'étape d'application 64. Dans l'exemple de réalisation des figures 1 et 3, l'ensemble 65 comprend deux données chiffrées 66A, 66B : la première donnée 66A étant la troisième clef cryptographique 27 chiffrée par l'algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique 25A associée au premier utilisateur, et la seconde donnée 66B étant la troisième clef cryptographique 27 chiffrée par l'algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique 25B associée au deuxième utilisateur.

[77] Au cours d'une étape suivante 67, le premier ordinateur 8A transmet le fichier numérique chiffré 60 et l'ensemble 65 de données chiffrées à l'ensemble de stockage 12. Le serveur 36 de l'ensemble de stockage 12 stocke alors le fichier numérique chiffré 60 et l'ensemble 65 de données chiffrées. La troisième clef cryptographique 27 n'étant pas stockée dans l'ensemble de stockage 12, il est ainsi impossible pour le fournisseur du service de stockage de déchiffrer le fichier numérique chiffré 60 à l'aide de l'ensemble 65 de données chiffrées.

[78] Au cours d'une étape suivante 68, l'application 30 du premier ordinateur 8A détermine si le fichier numérique 2 ou une partie du fichier numérique 2 a, ou non, été modifié(e) dans la mémoire 22 de l'ordinateur.

[79] Si le fichier numérique 2 n'a pas été modifié, l'étape suivante 70 est effectuée.

[80] Si le fichier numérique 2 ou une partie du fichier numérique 2 a été modifié(e), les étapes 56, 58, 64 et 67 sont ré-effectuées par le premier ordinateur 8A. L'étape de téléchargement 62 n'est pas ré-effectuée, la ou chaque clef cryptographique publique 25 associée à un utilisateur distinct du premier utilisateur étant déjà à disposition du premier ordinateur 8A, du fait du premier téléchargement 62 effectué.

[81] On conçoit ainsi que le procédé de partage de fichiers numériques selon l'invention permet d'assurer de manière simple et fiable le partage et la synchronisation de données numériques, tout en améliorant le niveau de confidentialité des données partagées.

[82] Selon un aspect complémentaire de l'invention, un procédé de récupération de fichiers numériques 2, associé au procédé de partage de fichiers numériques 2 selon l'invention et mis en œuvre par les ordinateurs 8A, 8B du système de partage 6, va être décrit en référence aux figures 2 et 4.

[83] Au cours de l'étape 70, le ou un des ordinateur(s) de chaque utilisateur autorisé par le premier utilisateur à accéder au fichier 2 télécharge, depuis l'ensemble de stockage 12, la donnée chiffrée obtenue

par application d'un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique 25 associée audit utilisateur. Dans l'exemple de réalisation particulier des figures 1 et 4, une application du second ordinateur 8B est exécutée par le processeur 19 du second ordinateur 8B, et les instructions de programme de l'application mettent en œuvre le procédé de récupération du fichier numérique 2.

[84] Au cours de l'étape 70, le second ordinateur 8B télécharge, depuis l'ensemble de stockage 12, la seconde donnée chiffrée 66B.

[85] Au cours d'une étape suivante 72, chaque ordinateur ayant téléchargé une donnée chiffrée applique, sur ladite donnée chiffrée, un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique privée 26 stockée au sein dudit ordinateur. Dans l'exemple de réalisation des figures 1 et 4, le composant 28B du second ordinateur 8B applique, sur la donnée chiffrée 66B téléchargée par le second ordinateur 8B, un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique privée 26B stockée au sein du second ordinateur 8B. La troisième clef cryptographique 27 unique et aléatoire est ainsi récupérée à l'issue de l'étape d'application 72.

[86] Au cours d'une étape suivante 74, chaque ordinateur ayant téléchargé une donnée chiffrée télécharge, depuis l'ensemble de stockage 12, le fichier numérique chiffré 60. Dans l'exemple de réalisation des figures 1 et 4, le second ordinateur 8B télécharge, depuis l'ensemble de stockage 12, le fichier numérique chiffré 60.

[87] Au cours d'une étape finale 76, chaque ordinateur ayant téléchargé une donnée chiffrée applique, sur au moins une donnée et/ou métadonnée chiffrée du fichier numérique chiffré 60, un algorithme de chiffrement symétrique ayant pour paramètre la troisième clef cryptographique 27. Dans l'exemple de réalisation des figures 1 et 4, le composant 28A du second ordinateur 8B applique, sur au moins une donnée et/ou métadonnée chiffrée du fichier numérique chiffré 60, un algorithme de chiffrement symétrique ayant pour paramètre la troisième clef

cryptographique 27. Dans le mode de réalisation préférentiel selon lequel l'étape d'application 58 comprend en outre l'adjonction d'une signature numérique à la ou chaque donnée chiffrée du fichier numérique chiffré 60, la signature numérique est vérifiée par le second ordinateur 8B au cours de l'étape 76.

[88] Le fichier numérique initial 2 est ainsi déchiffré par le second ordinateur 8B à l'issue de l'étape d'application finale 76.

[89] En variante ou en complément des étapes 70 à 76 telles que décrites ci-dessus, l'application 30 du premier ordinateur 8A est exécutée par le processeur 19 afin de procéder à une synchronisation des données du fichier 2 entre le premier ordinateur 8A et l'ensemble de stockage 12. Au cours de l'étape 70, le premier ordinateur 8A télécharge alors, depuis l'ensemble de stockage 12, la première donnée chiffrée 66A.

[90] Au cours d'une étape suivante, non représentée sur les figures, l'application 30 du premier ordinateur 8A détecte si des différences existent entre les données ou métadonnées du fichier numérique 2 stocké dans la mémoire 22 et les données ou métadonnées du fichier numérique chiffré 60 stocké dans l'ensemble de stockage 12. Au cours de cette même étape, l'application 30 du premier ordinateur 8A détermine les dates de modification respectives de ces deux fichiers 2, 60.

[91] Dans le cas où aucune différence n'est détectée par l'application 30, aucune action n'est réalisée et le fichier 2 est statué comme étant à jour.

[92] Dans le cas où des différences sont détectées par l'application 30 et que le fichier numérique 2 stocké dans la mémoire 22 comporte des modifications plus récentes que les dernières modifications du fichier numérique chiffré 60, les étapes 56 à 67 sont ré-effectuées par le premier ordinateur 8A sur le fichier numérique 2 ou une partie du fichier numérique 2 correspondant aux différences détectées.

[93] Dans le cas où des différences sont détectées par l'application 30 et que le fichier numérique chiffré 60 comporte des modifications plus récentes que les dernières modifications du fichier numérique 2, les étapes

72 à 76 sont effectuées par le premier ordinateur 8A sur le fichier numérique chiffré 60 ou une partie du fichier numérique chiffré 60 correspondant aux différences détectées, et sur la première donnée chiffrée 66A.

[94] L'invention est décrite dans ce qui précède à titre d'exemple. Il est entendu que l'homme du métier est à même de réaliser différentes variantes de réalisation de l'invention sans pour autant sortir du cadre de l'invention. En particulier, bien que l'invention soit décrite en référence à deux ordinateurs 8A, 8B chacun associé à un utilisateur distinct, elle s'applique plus généralement à plusieurs ordinateurs associés à plusieurs utilisateurs. Ainsi les moyens d'application 21 sont plus généralement propres à appliquer, sur la troisième clef cryptographique 27, un algorithme de chiffrement asymétrique ayant pour paramètre chaque clef cryptographique publique 25 associée à un utilisateur distinct du premier utilisateur, mais autorisé par le premier utilisateur à accéder au fichier 2 destiné à être partagé. Ainsi, la présente invention repose sur l'utilisation des clefs cryptographiques publiques 25 des utilisateurs ayant le droit d'accès aux données du fichier destiné à être partagé. Le déchiffrement de ces données est ensuite uniquement possible via l'utilisation d'une des clefs privées 26 des utilisateurs ayant eu le droit d'accès.

REVENDICATIONS

1. Procédé de partage de fichiers numériques (2) entre plusieurs ordinateurs (8A, 8B) reliés via un réseau de communication (4), chaque ordinateur (8A, 8B) étant associé à un utilisateur et étant relié, via le réseau de communication (4), à un dispositif (10) de stockage de clefs cryptographiques et à un ensemble (12) de stockage de données, au moins un fichier numérique (2) destiné à être partagé étant stocké sur un premier ordinateur (8A) d'un premier utilisateur, le procédé comprenant :

- une étape (50) de génération, par le premier ordinateur (8A) et par au moins un ordinateur (8B) de chaque utilisateur distinct du premier utilisateur, d'une première clef cryptographique publique (25A, 25B) et d'une deuxième clef cryptographique privée (26A, 26B) associée à la clef cryptographique publique (25A, 25B) dans un algorithme de chiffrement asymétrique, la clef cryptographique publique (25A, 25B) étant associée à l'utilisateur dudit ordinateur,
- une étape (52) de transmission au dispositif (10) de stockage de clefs cryptographiques, par chaque ordinateur (8A, 8B) ayant généré une clef cryptographique publique, de ladite clef cryptographique publique,
- une étape (54) de stockage, par chaque ordinateur (8A, 8B) ayant généré une clef cryptographique privée, de ladite clef cryptographique privée,
- une étape (56) de génération, par le premier ordinateur (8A), d'une troisième clef cryptographique (27) unique et aléatoire,
- une étape (58) d'application, par le premier ordinateur (8A), sur au moins une donnée du fichier numérique (2) destiné à être partagé, d'un algorithme de chiffrement symétrique ayant pour paramètre la troisième clef cryptographique (27), un fichier numérique chiffré (60) comprenant ladite au moins une donnée étant obtenu à l'issue de cette étape d'application (58),

- une étape (62) de téléchargement, depuis le dispositif de stockage (10), par le premier ordinateur (8A), d'au moins une clef cryptographique publique (25B) associée à un deuxième utilisateur distinct du premier utilisateur,
- une étape (64) d'application, par le premier ordinateur (8A), sur la troisième clef cryptographique (27), d'un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique (25A) associée au premier utilisateur et d'un algorithme de chiffrement asymétrique ayant pour paramètre ladite au moins une clef cryptographique publique (25B) associée à un deuxième utilisateur, un ensemble (65) comprenant au moins deux données chiffrées (66A, 66B) étant obtenu à l'issue de cette étape d'application (64),
- une étape (67) de transmission à l'ensemble (12) de stockage de données, par le premier ordinateur (8A), du fichier numérique chiffré (60) et de l'ensemble (65) de données chiffrées (66A, 66B),

dans lequel l'étape (56) de génération d'une troisième clef cryptographique (27) unique et aléatoire, l'étape (58) d'application d'un algorithme de chiffrement symétrique, l'étape (64) d'application d'un algorithme de chiffrement asymétrique ayant pour paramètre la clef cryptographique publique (25A) associée au premier utilisateur et d'un algorithme de chiffrement asymétrique ayant pour paramètre ladite au moins une clef cryptographique publique (25B) associée à un deuxième utilisateur et l'étape (67) de transmission du fichier numérique chiffré (60) et de l'ensemble (65) de données chiffrées (66A, 66B) sont ré-effectuées par le premier ordinateur (8A) après chaque nouvelle modification du fichier (2) destiné à être partagé ou d'une partie de ce fichier (2).

2. Procédé selon la revendication 1, caractérisé en ce que le fichier (2) destiné à être partagé comprend au moins une métadonnée, et en ce

que l'algorithme de chiffrement symétrique est en outre appliqué sur ladite métadonnée lors de l'étape (58) d'application, par le premier ordinateur (8A), d'un algorithme de chiffrement symétrique sur au moins une donnée du fichier numérique (2) destiné à être partagé.

3. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la clef cryptographique privée (26A, 26B) est stockée dans un support d'enregistrement amovible (20) connecté à une unité centrale (18) de l'ordinateur (8A, 8B), et en ce que l'accès au support d'enregistrement amovible (20) est protégé par un mot de passe.

4. Procédé selon la revendication 3, caractérisé en ce que le support d'enregistrement amovible (20) comprend un composant (29) de chiffrement cryptographique de données, et en ce que la clef cryptographique privée (26A, 26B) est chiffrée par le composant de chiffrement (29) lors de l'étape (54) de stockage au sein du support d'enregistrement (20).

5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'étape (58) d'application d'un algorithme de chiffrement symétrique comprend en outre l'adjonction d'une signature numérique à la ou chaque donnée chiffrée du fichier numérique chiffré (60), la signature numérique étant associée à ladite donnée.

6. Procédé selon la revendication 5, caractérisé en ce que, au cours de l'étape (58) d'application d'un algorithme de chiffrement symétrique, l'algorithme de chiffrement symétrique est également appliqué sur la signature numérique.

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend en outre une étape de téléchargement, depuis l'ensemble de stockage (12), par le premier ordinateur (8A), de la donnée chiffrée (66A) associée au premier utilisateur; et une étape de détection, par le premier ordinateur (8A), si des différences existent entre des données ou métadonnées du fichier numérique (2) stocké sur le premier ordinateur (8A) et des données et métadonnées du fichier numérique chiffré (60) stocké dans l'ensemble de stockage (12), et de détermination des dates de modification respectives du fichier numérique (2) et du fichier numérique chiffré (60).

8. Ordinateur (8A) muni de moyens (16) de génération de clefs cryptographiques, de moyens (21) d'application d'un algorithme de chiffrement symétrique et d'un algorithme de chiffrement asymétrique sur des données informatiques, d'au moins une mémoire (22) adaptée pour stocker au moins un fichier numérique (2) destiné à être partagé et d'au moins une mémoire (20) adaptée pour stocker au moins une clef cryptographique (26A), caractérisé en ce que l'ordinateur (8A) est propre à mettre en œuvre le procédé de partage de fichiers numériques (2) selon l'une quelconque des revendications précédentes, l'ordinateur (8A) étant le premier ordinateur du procédé.

9. Ordinateur (8A) selon la revendication 8, caractérisé en ce qu'il comprend en outre au moins un processeur (19), et en ce que la mémoire (22) comprend une application (30), l'application (30) étant propre, lorsqu'elle est exécutée par ledit au moins un processeur (19), à mettre en œuvre le procédé de partage de fichiers numériques (2) selon l'une quelconque des revendications 1 à 7, l'application (30) comprenant les moyens (16) de génération de clefs cryptographiques et les moyens (21) d'application d'un algorithme de chiffrement

symétrique et d'un algorithme de chiffrement asymétrique sur des données informatiques.

10. Ensemble (12) de stockage de données propre à être relié à plusieurs ordinateurs (8A, 8B) via un réseau de communication (4), pour le partage de fichiers numériques (2) entre les ordinateurs (8A, 8B), chaque ordinateur (8A, 8B) étant associé à un utilisateur, au moins un des ordinateurs étant conforme à la revendication 8 ou 9, l'ensemble de stockage (12) étant propre à stocker des données chiffrées et des fichiers numériques chiffrés (60) destinés à être partagés entre les ordinateurs (8A, 8B).

11. Système (6) de partage de fichiers numériques (2), comprenant :

- une pluralité d'ordinateurs (8A, 8B) reliés via un réseau de communication (4), chaque ordinateur (8A, 8B) étant associé à un utilisateur, au moins un des ordinateurs (8A, 8B) étant conforme à la revendication 8 ou 9,
- un dispositif (10) de stockage de clefs cryptographiques, relié à chaque ordinateur (8A, 8B) via le réseau de communication (4),
- un ensemble (12) de stockage de données, relié à chaque ordinateur (8A, 8B) via le réseau de communication (4), l'ensemble de stockage (12) étant conforme à la revendication 8.

12. Produit programme d'ordinateur (30) téléchargeable depuis un réseau de communication et/ou enregistré sur un support (22) lisible par ordinateur et/ou exécutable par un processeur (19), caractérisé en ce qu'il comprend des instructions de programme adaptées pour mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 7 lorsque le produit programme (30) est exécuté sur un ordinateur.

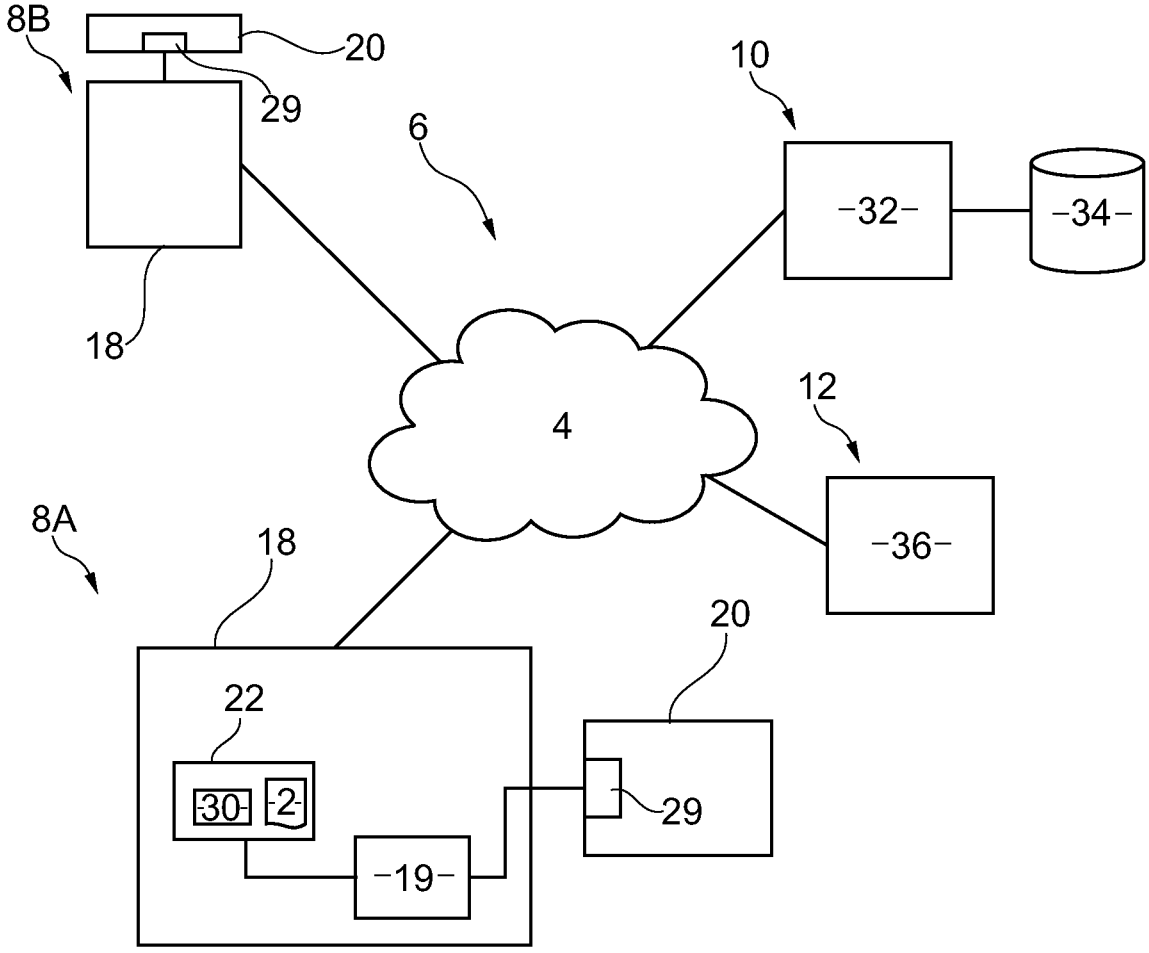
8B
20
29
10
6
-32-
-34-
18
4
12
-36-
8A
18
20
22
30
2
29
-19-

Fig. 1

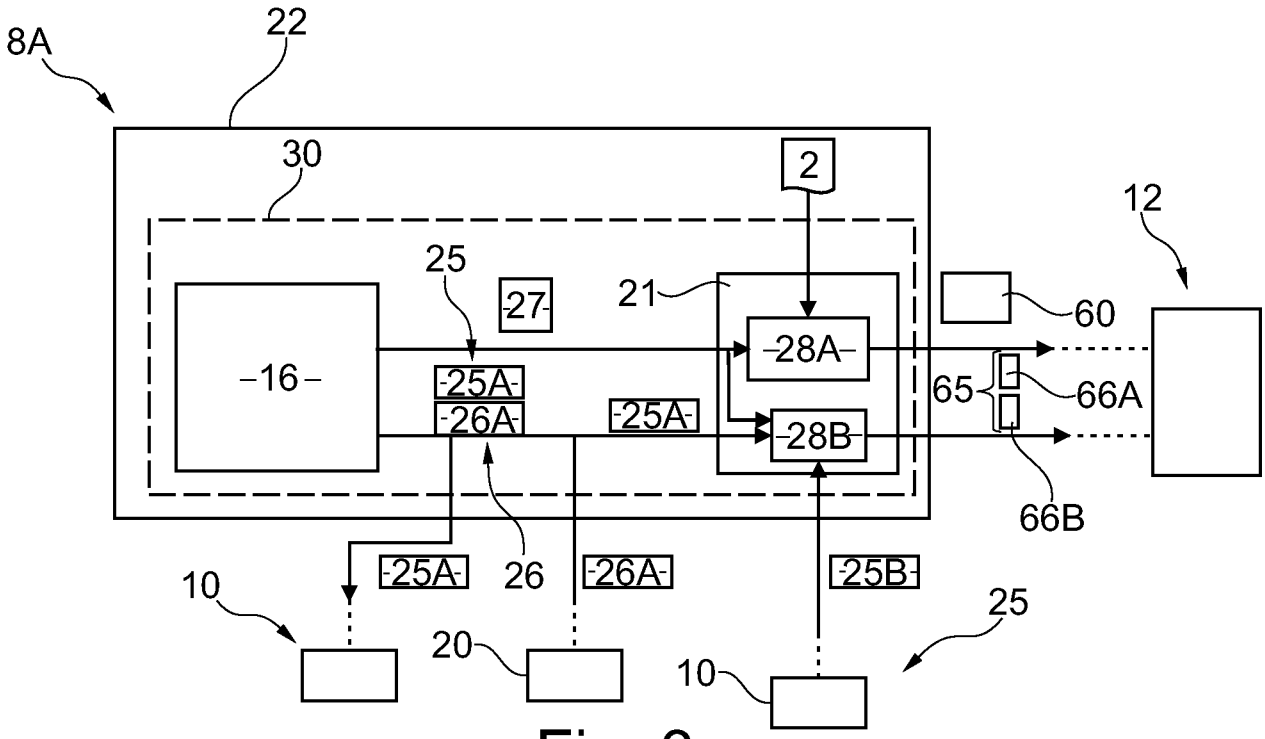
8A
22
30
2
12
25
27
21
60
-16-
-28A-
-25A-
-26A-
-25A-
-28B-
65
66A
66B
-25A-
26
-26A-
-25B-
10
20
10
25

Fig. 3

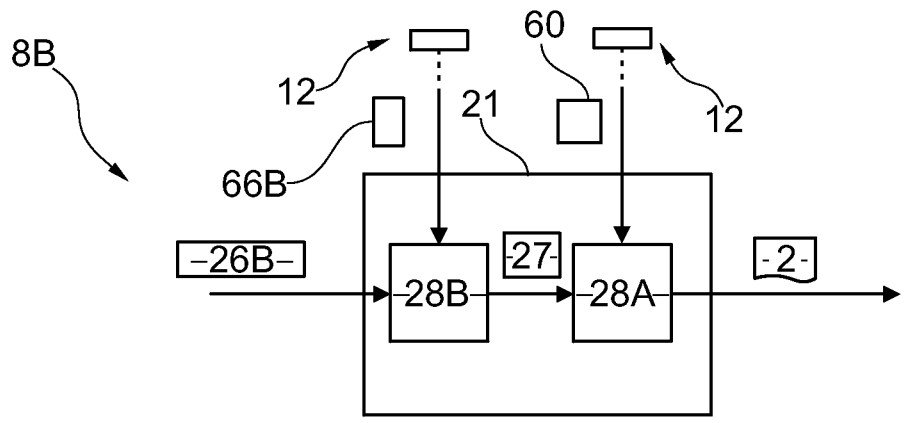
8B
12
60
12
21
66B
-26B-
28B
27
28A
-2-

Fig. 4

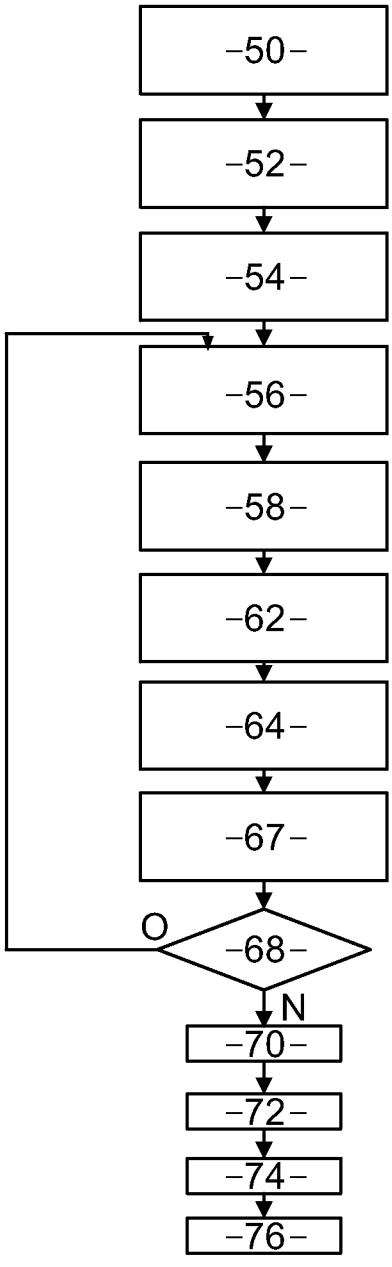
-50-
-52-
-54-
-56-
-58-
-62-
-64-
-67-
O
-68-
N
-70-
-72-
-74-
-76-

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/051415

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L9/32
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification **System** followed **by** classification **symbols)**
H04L

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 2013/013931 Al (O'HARE MARK S [US] ET AL) 10 January 2013 (2013-01-10)	1,2,5-12
Y	paragraphs [0520] , [0521] , [0524] ; figure 42B	3,4

X	FR 2 990 818 Al (MY0CEAN IT [FR]) 22 November 2013 (2013-11-22)	1,2,5-12
Y	page 8, line 8 - page 9, line 2; figure 2 page 9, line 20 - page 10, line 5; figure 3	3,4

X	EP 2 234 323 Al (0GAWA KEI K0 [JP]) 29 September 2010 (2010-09-29)	1,2,5-12
Y	paragraphs [0054] - [0061] , [0042] ; figure 3	3,4

	-/- ·	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Spécial catégories of cited documents :

"A" document defining the gênerai 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" documentwhich may throw doubts on priority claim(s) orwhich is cited to establish the publication date of another citation or other spécial 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 ortheory underlying the invention

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 August 2015	03/09/2015

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/051415

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Les : "TrustWay RCI Ressource Cryptographi que Indi vi duel l e", , 1 January 2010 (2010-01-01) , XP055171304, Retri eved from the Internet: URL: http://www.bul l . fr/pdfs/S-TrustWayRCI - fr4.pdf [retri eved on 2015-02-23] ci ted i n the appl i cati on lst col . page 2 -----	3,4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2015/051415

Patent document oited in searoh report	Publication date	Patent family member(s)	Publication date
US 2013013931 Al	10-01-2013	AU 2012225621 Al	10-10-2013
		CA 2829197 Al	13-09-2012
		CN 103636160 A	12-03-2014
		EP 2684311 Al	15-01-2014
		US 2013013931 Al	10-01-2013
		Wo 2012122175 Al	13-09-2012
FR 2990818 Al	22-11-2013	NONE	
EP 2234323 Al	29-09-2010	AU 2008344384 Al	09-07-2009
		CA 2714196 Al	09-07-2009
		CN 101919202 A	15-12-2010
		EP 2234323 Al	29-09-2010
		JP 5554066 B2	23-07-2014
		JP 2014161078 A	04-09-2014
		KR 20100103645 A	27-09-2010
		US 2010281265 Al	04-11-2010
		US 2013163754 Al	27-06-2013
		US 2014129836 Al	08-05-2014
		Wo 2009084573 Al	09-07-2009

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/051415

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L9/08 H04L9/32
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)
H04L

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 2013/013931 A1 (O'HARE MARK S [US] ET AL) 10 janvier 2013 (2013-01-10)	1,2,5-12
Y	alinéas [0520], [0521], [0524]; figure 42B	3,4

X	FR 2 990 818 A1 (MY0CEAN IT [FR]) 22 novembre 2013 (2013-11-22)	1,2,5-12
Y	page 8, ligne 8 - page 9, ligne 2; figure 2 page 9, ligne 20 - page 10, ligne 5; figure 3	3,4

X	EP 2 234 323 A1 (0GAWA KEIK0 [JP]) 29 septembre 2010 (2010-09-29)	1,2,5-12
Y	alinéas [0054] - [0061], [0042]; figure 3	3,4

	-/- .	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

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

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

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

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

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

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

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

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

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

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
25 août 2015	03/09/2015

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

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/051415

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	Les : "TrustWay RCI Ressource Cryptographi que Indi vi duel l e", , 1 janvi er 2010 (2010-01-01) , XP055171304, Extrai t de 1' Internet: URL: http://www.bul l . fr/pdfs/S-TrustWayRCI - fr4.pdf [extrai t l e 2015-02-23] ci t é dans l a demande lst col . page 2 -----	3,4

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2015/051415

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2013013931 Al	10-01-2013	AU 2012225621 Al	10-10-2013
		CA 2829197 Al	13-09-2012
		CN 103636160 A	12-03-2014
		EP 2684311 Al	15-01-2014
		US 2013013931 Al	10-01-2013
		Wo 2012122175 Al	13-09-2012
FR 2990818 Al	22-11-2013	AUCUN	
EP 2234323 Al	29-09-2010	AU 2008344384 Al	09-07-2009
		CA 2714196 Al	09-07-2009
		CN 101919202 A	15-12-2010
		EP 2234323 Al	29-09-2010
		JP 5554066 B2	23-07-2014
		JP 2014161078 A	04-09-2014
		KR 20100103645 A	27-09-2010
		US 2010281265 Al	04-11-2010
		US 2013163754 Al	27-06-2013
		US 2014129836 Al	08-05-2014
		Wo 2009084573 Al	09-07-2009