(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
28 septembre 2017 (28.09.2017)

WIPO | PCT

(10) Numéro de publication internationale
WO 2017/162995 A1

(51) Classification internationale des brevets :
H04L 29/06 (2006.01) *G06F 21/40* (2013.01)

(21) Numéro de la demande internationale :
PCT/FR2017/050694

(22) Date de dépôt international :
24 mars 2017 (24.03.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1652650 25 mars 2016 (25.03.2016) FR

(71) Déposant : **ARCANSECURITY** [FR/FR]; 589, Chemin du Vallon Vert, 06600 Antibes (FR).

(72) Inventeur : **PRADINES, Florian**; Chez M et MMe F. Pradines, Bât C, Place Stanislas Fabre, 13780 Cuges-Les-Pins (FR).

(74) Mandataire : **ROMAN, Alexis**; 30064, Cabinet Roman, 35, Rue Paradis, 13484 Marseille Cedex 20 (FR).

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

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

Publiée :

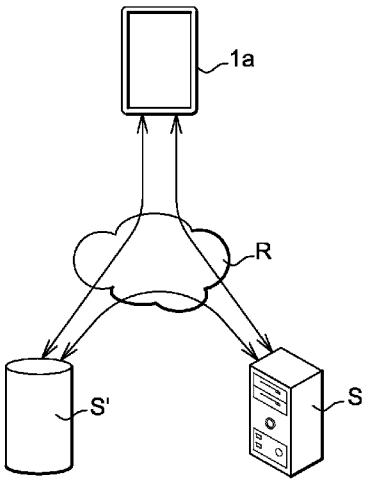
— *avec rapport de recherche internationale (Art. 21(3))*

WO 2017/162995 A1

(54) Title : AUTHENTICATION METHOD FOR AUTHORISING ACCESS TO A WEBSITE

(54) Titre : PROCEDE D'AUTHENTIFICATION POUR AUTORISER L'ACCES A UN SITE WEB

Fig. 1



(57) Abstract : The invention relates to an authentication method for authorising access to an Internet site from the computing device of a user or access to encrypted data stored in said computer device, wherein a prior phase of parameter setting comprises the following steps : o creating a list of authentication parameters, which parameters are divided: into a first group consisting of at least one item of geolocation data of the computer device and/or a time range of operation of said device, and a second group consisting of at least one other item of data other than a password, a login, an item of geolocation data of the computing device and a time range of the operation of said device; selecting, from a graphic interface of the electronic device, at least one authentication parameter of the first group and at least one authentication parameter of the second group; defining, from the graphic interface, at least one authentication condition by selecting one or more logic operators belonging to the following list: logical AND, logical OR and logical NOT; and combining the logical operator or operators selected with the chosen authentication parameters.

(57) Abrégé :

[Suite sur la page suivante]

L'invention concerne un procédé d'authentification pour autoriser l'accès à un site internet depuis l'appareil informatique d'un utilisateur ou l'accès à des données chiffrées stockées dans ledit appareil informatique, dans lequel, une phase préalable de paramétrage comprend les étapes suivantes : o créer une liste de paramètres d'authentification, lesquels paramètres sont répartis : dans un premier groupe consistant en au moins une donnée de géo-localisation de l'appareil informatique et/ou une plage horaire de fonctionnement dudit appareil, et dans un second groupe consistant en au moins une autre donnée autre qu'un mot de passe, qu'un login, qu'une donnée de géo-localisation de l'appareil informatique et qu'une plage horaire de fonctionnement dudit appareil, sélectionner, depuis une interface graphique de l'appareil électronique, au moins un paramètre d'authentification du premier groupe et au moins un paramètre d'authentification du second groupe, définir, depuis l'interface graphique, au moins une condition d'authentification en sélectionnant un ou plusieurs opérateurs logiques appartenant à la liste suivante : ET logique, OU logique, NON logique, et combiner le ou les opérateurs logiques sélectionnés aux paramètres d'authentification choisis.

PROCEDE D'AUTHENTIFICATION POUR AUTORISER L'ACCES A UN SITE WEB

Description

Domaine technique de l'invention.

L'invention a pour objet un procédé d'authentification pour autoriser l'accès à un site web.

Elle concerne le domaine du traitement de données numériques et plus particulièrement celui des techniques de sécurité pour protéger ces données contre une activité non autorisée.

État de la technique.

Il est courant d'autoriser l'accès à un site web ou à des données chiffrées au moyen d'une authentification par identifiant et mot de passe. Cette authentification permet à un utilisateur de prouver son identité lorsqu'il désire accéder à une ressource (notamment informatique) ou à un service proposé sur un site internet (par exemple des comptes bancaires en ligne) dont l'accès est limité et protégé.

Des techniques d'authentification qui ne sont pas basées sur les traditionnels identifiant et mot de passe existent.

Le document brevet EP 2.804.136 (ORANGE) concerne par exemple la gestion d'accès à un réseau social. La demande d'accès à ce réseau social est gérée par un serveur distant. Ce dernier autorise l'accès en fonction d'une position géographique et d'un laps de temps associé à la demande d'accès. La position géographique correspond par exemple à un centre de conférences et le laps de temps à une plage horaire d'un jour déterminé (qui coïncide typiquement avec une conférence qui à lieu dans le centre de conférences). Ainsi, seules les personnes qui demandent à se joindre au réseau social et qui sont situées dans le centre de conférences pendant le laps de temps prédéfini, seront inscrites au réseau social dédié à la conférence se déroulant ce même jour, au centre de conférence. Les personnes souhaitant s'inscrire au réseau social ne peuvent toutefois pas choisir les paramètres d'authentification, ces derniers leur étant imposés.

Le document brevet US 2014/0230022 (YUASA) concerne un dispositif de traitement d'informations permettant d'accéder à un contenu. Ce dispositif permet à une personne (propriétaire) qui dirige un groupe, d'autoriser l'accès à ce groupe à des participants. Les conditions d'accès au groupe sont définies par le propriétaire et

consistent en une combinaison d'un emplacement, d'une plage horaire et d'un thème. Les participants ne peuvent pas choisir les paramètres d'authentification leur permettant d'accéder au groupe. Ces paramètres leur sont en effet imposés par le propriétaire.

Le document brevet WO2012/000107 (ABSOLUTE SOFTWARE CORPORATION) décrit un dispositif permettant de définir automatiquement le réglage d'un géo-repérage d'un appareil informatique tel que ordinateur, téléphone, etc. L'utilisateur définit préalablement une zone de géo-repérage autour d'un point de géo-localisation de l'appareil. Si l'appareil est situé dans la zone de géo-repérage, l'appareil fonctionne (l'utilisateur peut donc avoir accès aux données contenues dans son appareil). Si l'appareil n'est pas situé dans la zone de géo-repérage, l'appareil ne fonctionne plus (l'utilisateur n'a donc plus accès aux données contenues dans son appareil). La position de l'appareil peut être vérifiée pour voir s'il est situé dans la zone de géo-repérage. Si l'appareil est en dehors de la zone de géo-repérage, le dispositif invite l'utilisateur à saisir un mot de passe pour ajuster ladite zone de géo-repérage de manière à y inclure le nouvel emplacement dudit appareil. L'intérêt de cette méthode d'authentification est limité dans la mesure où l'utilisateur ne peut choisir qu'un seul paramètre d'authentification (autre que le mot de passe) qui est l'étendue de la zone de géo-repérage.

Le document brevet US2013/0036462 (QUALCOMM) décrit un procédé d'authentification pour autoriser un appareil informatique à avoir accès à des informations sensibles. Outre le fait que ce document ne traite pas de l'accès à un site internet, ia gestion de l'authentification est dévolue à l'appareil informatique de sorte que le niveau de sécurité n'est pas optimum. Une situation similaire apparaît dans les documents brevets US2013/262873 (READ) et US2015/0281279 (SMITH).

L'invention vise à remédier à cet état des choses. En particulier, un objectif de l'invention est d'améliorer la technique d'authentification autre que par identifiant et mot de passe.

Un autre objectif de l'invention est de permettre à un utilisateur d'accéder de manière plus sécurisée à un site web dont l'accès lui est réservé.

Un autre objectif de l'invention est de proposer une solution technique d'authentification qui soit peu onéreuse, facile à installer, et dont l'utilisation est aisée.

Divulgation de l'invention.

La solution proposée par l'invention est un procédé d'authentification pour autoriser la connexion à un site internet depuis un appareil informatique d'un utilisateur.

Une phase préalable de paramétrage comprend les étapes suivantes :

- créer une liste de paramètres d'authentification, lesquels paramètres sont répartis :
  - dans un premier groupe consistant en au moins une donnée de géo-localisation de l'appareil informatique et/ou une plage horaire de fonctionnement dudit appareil,
  - et dans un second groupe consistant en au moins une autre donnée autre qu'un mot de passe, qu'un login, qu'une donnée de géo-localisation de l'appareil informatique et qu'une plage horaire de fonctionnement dudit appareil,
- sélectionner au moins un paramètre d'authentification du premier groupe et au moins un paramètre d'authentification du second groupe,
- définir au moins une condition d'authentification en sélectionnant un ou plusieurs opérateurs logiques appartenant à la liste suivante : ET logique, OU logique, NON logique, et combiner le ou les opérateurs logiques sélectionnés aux paramètres d'authentification choisis,
- enregistrer, dans un serveur informatique, cette condition d'authentification, lequel serveur informatique est adapté pour gérer la connexion au site internet ou l'accès aux données chiffrées.

Une phase ultérieure d'accès au site internet comprend les étapes suivantes :

- l'appareil informatique se connecte au site internet dont l'accès est protégé,
- la connexion de l'appareil informatique au site internet déclenche la mise en œuvre d'un processus qui entraine la connexion automatique dudit appareil au serveur informatique,
- l'appareil informatique transmet au serveur informatique des paramètres d'authentification,
- le serveur informatique analyse les paramètres d'authentification transmis par l'appareil informatique et les confronte à la condition d'authentification,
- le serveur informatique génère une instruction d'autorisation d'accès au site internet, cette instruction n'étant générée que si les paramètres d'authentification transmis respectent la condition d'authentification,
- le serveur informatique transfert l'instruction d'autorisation au site internet,
- en réponse à la réception de l'instruction d'autorisation, le site internet autorise son accès à l'appareil informatique.

C'est donc maintenant l'utilisateur qui paramètre lui-même sa propre condition d'authentification. Cette dernière ne lui est pas imposée par un tiers contrairement aux techniques précitées connues de l'art antérieur. En outre, la condition d'authentification étant maintenant constituée par la combinaison d'au moins deux paramètres (autres qu'un mot de passe ou qu'un identifiant) auxquels sont associés des opérateurs logiques, le niveau de sécurité est amélioré. Et le fait de déléguer à un serveur informatique disant (indépendant de l'appareil informatique de l'utilisateur ou du site web) la gestion de l'authentification, et donc la gestion de l'accès au site internet, permet d'accroître davantage le niveau de sécurité.

D'autres caractéristiques avantageuses de l'invention sont listées ci-dessous. Chacune de ces caractéristiques peut être considérée seule ou en combinaison avec les caractéristiques remarquables définies ci-dessus, et faire l'objet, le cas échéant, d'une ou plusieurs demandes de brevet divisionnaires :

- Préférentiellement, durant la phase préalable de paramétrage, les paramètres d'authentification sont sélectionnés de manière à ce que durant la phase ultérieure d'accès au site internet, l'appareil informatique puisse détecter automatiquement tous ces paramètres d'authentification sans action volontaire sur ledit appareil.
- La condition d'authentification est une condition statique, la sélection d'un paramètre n'influençant pas les autres paramètres sélectionnés.
- préférentiellement, le second groupe consiste en au moins une donnée choisie dans la liste suivante : identifiant intégré dans une carte SIM de l'appareil informatique ; identifiant associé à l'appareil informatique ; SSID d'un réseau wifi ; détection d'une connexion Bluetooth entre l'appareil informatique et un autre appareil électronique ; identifiant enregistré dans un tag NFC ou RFID ; empreinte digitale ; scan rétinien ; reconnaissance d'iris ; détection d'une connexion entre l'appareil informatique et un serveur proxy ; détection d'une connexion entre l'appareil informatique et un serveur VPN ; adresse IP attribuée à l'appareil informatique lors de sa connexion à un réseau de télécommunication ; détection d'une connexion de l'appareil informatique à un réseau social ; détection d'une connexion de l'appareil informatique à la page d'un ami spécifique ou d'une personne spécifique suivie sur un réseau social ; adresse MAC d'une passerelle réseau.
- La donnée de géo-localisation de l'appareil informatique peut être sélectionnée par l'utilisateur depuis une carte interactive affichée sur une interface graphique dudit appareil.

- La plage horaire de fonctionnement de l'appareil informatique peut consister en un ou plusieurs jours de la semaine et un laps de temps.

- Avantageusement, la phase préalable de paramétrage comprend en outre les étapes suivantes : - afficher, depuis un menu accessible depuis une interface graphique de l'appareil informatique, l'ensemble des paramètres d'authentification ; - sélectionner, dans le menu, des paramètres d'authentification parmi l'ensemble des paramètres d'authentification affichés. Les opérateurs logiques peuvent également être affichés dans ce menu avec l'ensemble des paramètres d'authentification.

- Le procédé comprend avantageusement une étape consistant à chiffrer la condition d'authentification avec un algorithme de cryptographie.

- Dans ce cas, on chiffre préférentiellement la condition d'authentification avec une clé AES générée par l'appareil informatique.

- Cette clé AES peut être chiffrée avec une clé RSA publique générée par le serveur informatique.

- Cette clé RSA publique peut être générée par le serveur informatique en réponse à une requête transmise par le site internet.

Un autre aspect de l'invention non couvert par les revendications concerne un procédé d'authentification pour autoriser le déchiffrement de données chiffrées stockées dans un appareil informatique d'un utilisateur,

- dans lequel, une phase préalable de paramétrage comprend les étapes suivantes :
  - o créer une liste de paramètres d'authentification, lesquels paramètres sont répartis :
    - dans un premier groupe consistant en au moins une donnée de géo-localisation de l'appareil informatique et/ou une plage horaire de fonctionnement dudit appareil,
    - et dans un second groupe consistant en au moins une donnée autre qu'un mot de passe, qu'un login, qu'une donnée de géo-localisation de l'appareil informatique et qu'une plage horaire de fonctionnement dudit appareil,
  - o sélectionner, depuis une interface graphique de l'appareil électronique, au moins un paramètre d'authentification du premier groupe et au moins un paramètre d'authentification du second groupe,

- définir, depuis l'interface graphique, au moins une condition d'authentification en sélectionnant un ou plusieurs opérateurs logiques appartenant à la liste suivante : ET logique, OU logique, NON logique, et combiner le ou les opérateurs logiques sélectionnés aux paramètres d'authentification choisis,
- enregistrer, dans un serveur informatique, cette condition d'authentification, lequel serveur informatique est adapté pour gérer l'accès aux données chiffrées,

- et dans lequel, une phase ultérieure de déchiffrement des données chiffrées comprend les étapes suivantes :
  - la sélection des données chiffrées déclenche la mise en œuvre d'un processus qui entraine la connexion de l'appareil informatique au serveur informatique,
  - l'appareil informatique transmet au serveur informatique des paramètres d'authentification,
  - le serveur informatique analyse les paramètres d'authentification transmis par l'appareil informatique et les confronte à la condition d'authentification,
  - le serveur informatique génère une instruction d'autorisation d'accès aux données chiffrées, cette instruction n'étant générée que si les paramètres d'authentification transmis respectent la condition d'authentification,
  - le serveur informatique transmet à l'appareil informatique : l'instruction d'autorisation ainsi qu'une clé de déchiffrement des données chiffrées,
  - en réponse à la réception de l'instruction d'autorisation et de la clé de déchiffrement, l'appareil informatique déchiffre les données chiffrées.

- Ce procédé comprend avantageusement une étape consistant à chiffrer les données avec un algorithme de cryptographie.

- Dans ce cas, on chiffre préférentiellement les données avec une clé AES générée par le serveur informatique.

- Des données chiffrées peuvent être enregistrées dans une mémoire de l'appareil électronique ou dans une mémoire d'un second appareil électronique distinct dudit appareil

- Dans ce dernier cas, le procédé comprend avantageusement une étape consistant à transmettre une clé de déchiffrement des données au second appareil électronique, cette clé de déchiffrement étant automatiquement transmise par le serveur informatique si les paramètres d'authentification transmis par l'appareil électronique respectent la condition d'authentification.

Description des figures.

D'autres avantages et caractéristiques de l'invention apparaîtront mieux à la lecture de la description d'un mode de réalisation préféré qui va suivre, en référence aux dessins annexés, réalisés à titre d'exemples indicatifs et non limitatifs et sur lesquels :

- la figure 1 schématise un exemple de système dans lequel peut être mis en œuvre le procédé conforme à l'invention,
- la figure 2 schématise un autre exemple de système dans lequel peut être mis en œuvre le procédé conforme à l'invention,
- la figure 3 schématise encore un autre exemple de système dans lequel peut être mis en œuvre le procédé conforme à l'invention,
- la figure 4 illustre de manière simplifiée la structure d'un appareil informatique utilisé dans l'invention,
- la figure 5 illustre de manière simplifiée la structure d'un serveur informatique distant utilisé dans l'invention,
- la figure 6 illustre de manière simplifiée un exemple d'interface graphique permettant à un utilisateur de définir une condition d'authentification,
- la figure 7 est un organigramme illustrant différentes étapes mises en œuvre dans le procédé objet de l'invention, durant la phase préalable de paramétrage, pour l'accès à un site internet,
- la figure 8 est un organigramme illustrant différentes étapes mises en œuvre dans le procédé objet de l'invention, durant la phase ultérieure d'accès à un site internet,
- la figure 9 est un organigramme illustrant différentes étapes mises en œuvre dans le procédé objet de l'invention, durant la phase préalable de paramétrage, pour l'accès à des données chiffrées,
- la figure 10 est un organigramme illustrant différentes étapes mises en œuvre dans le procédé objet de l'invention, durant la phase ultérieure d'accès aux données chiffrées,
- la figure 11 est un organigramme illustrant différentes étapes mises en œuvre dans le procédé objet de l'invention, durant la phase préalable de paramétrage, pour l'accès à des données chiffrées, dans une variante de réalisation,
- la figure 12 est un organigramme illustrant différentes étapes mises en œuvre dans le procédé objet de l'invention, durant la phase ultérieure d'accès aux données chiffrées, dans une variante de réalisation.

Modes préférés de réalisation de l'invention.

Le procédé objet de l'invention consiste en une séquence cohérente d'étapes permettant d'aboutir à un résultat souhaité. Ces étapes engendrent des manipulations d'éléments physiques, notamment des signaux (électriques ou magnétiques) capables d'être stockés, transférés, combinés, comparés, etc.

Le procédé est mis en œuvre par l'intermédiaire d'applications informatiques exécutées respectivement par un ou plusieurs appareils informatiques ou par un ou plusieurs serveurs informatiques. Par souci de clarté, il faut comprendre au sens de l'invention que *« l'appareil/serveur fait quelque chose »* signifie « *l'application informatique exécutée sur l'appareil/serveur fait quelque chose* ». Tout comme « *l'application informatique fait quelque chose* » signifie « *l'application informatique exécutée par l'appareil/serveur fait quelque cho*se ».

La mise en œuvre du procédé objet de l'invention nécessite l'utilisation d'un ou plusieurs appareils électroniques 1a, 1b (figures 1, 2 et 3) se présentant par exemple sous la forme d'un ordinateur fixe ou portable, d'une tablette, préférentiellement sous la forme d'un Smartphone du type iPhone®, Samsung Galaxy®, iPad®, Samsung Tab®, ou sous la forme d'un autre appareil électronique, fonctionnant avec un système d'exploitation de type Windows, Mac, iOS, Android, etc.. L'appareil 1a, 1b est adapté pour être exploité par un utilisateur, qui, en pratique, est une personne physique.

En se rapportant à la figure 4, chaque appareil électronique 1a, 1b comprend notamment un ou plusieurs processeurs ou microprocesseurs 10, une ou plusieurs mémoires 11, une interface réseau 12, une interface graphique 13, un module de détermination de position 14, un 'émetteur/récepteur de signaux infrarouges 16, qui sont mutuellement connectés via un bus 15. Une ou plusieurs applications informatiques - ou programmes informatiques - sont enregistrées dans la ou les mémoires 11 et dont les instructions (ou codes), lorsqu'elles sont exécutées par le ou les processeurs 10 permettent de réaliser les fonctionnalités décrites plus avant dans la description.

La ou les mémoires 11 doivent être considérées comme un dispositif de stockage également adapté pour stocker des données et/ou des fichiers de données. Il peut s'agir d'une mémoire native ou d'une mémoire rapportée telle qu'une carte Secure Digital (SD).

L'interface réseau 12 est adaptée pour établir une communication avec le serveur distant S décrit plus avant dans la description, via une liaison sans fil ou filaire, de manière à recevoir et émettre des signaux. L'interface réseau 12 peut par exemple comprendre un module Bluetooth, un module GSM, ou un module fournissant une

connectivité de réseau à l'appareil 1a, 1b. De manière générale, l'interface réseau 12 a pour fonction de gérer les connexions entre l'appareil 1a, 1b et un réseau R de télécommunication (Internet, téléphonie mobile, ...), et éventuellement entre les appareils entre eux via les technologies de réseau telles que, mais sans s'y limiter, GSM, 3G, 4G Wifi, Bluetooth, etc.

L'interface graphique 13 offre à l'utilisateur la possibilité de saisir, sélectionner et/ou entrer des données pour définir au moins une condition d'authentification. Il se présente par exemple sous la forme d'un écran tactile, d'un écran connecté à un clavier et/ou une souris, etc.

Le module de détermination de position 14 est préférentiellement un module de géo-localisation par satellite de type GPS ou basé sur une technique de triangulation de signaux acquis par des bornes relais de téléphonie cellulaire.

L'émetteur/récepteur de signaux infrarouges 16 permet à un appareil 1a de communiquer sans fil avec un autre appareil 1b.

L'utilisateur doit installer une application informatique dans au moins un de ses appareil 1a (préférentiellement chaque appareils 1a, 1b) pour mettre en œuvre tout ou partie de l'invention depuis ledit appareil. Avantageusement, l'application informatique peut être préinstallée sur l'appareil 1a, par exemple par un opérateur réseau. L'utilisateur a toutefois la possibilité de rechercher l'application informatique sur une boutique en ligne telles que Google Play®, Itunes® ou sur un site internet dédié, et ensuite la télécharger sur son appareil 1a. Les informations pour télécharger et installer l'application informatique sur l'appareil peuvent par exemple être récupérées à l'aide d'un code QR ou d'un tag NFC. En tout état de cause, l'application informatique peut être installée dans toute mémoire 11 de l'appareil 1a.

La mise en œuvre du procédé objet de l'invention nécessite également l'utilisation d'un serveur distant S. Ce dernier peut consister en un serveur physique ou, dans certains cas, être composé de plusieurs ordinateurs distincts qui communiquent et interagissent sur un réseau pour exécuter les fonctions décrites plus avant.

En se rapportant à la figure 5, le serveur distant S comprend notamment un ou plusieurs processeurs ou microprocesseurs 20, une ou plusieurs mémoires 21, une interface réseau 22, qui sont mutuellement connectés via un bus 25. Une ou plusieurs applications informatiques - ou programmes informatiques - sont enregistrées dans la ou les mémoires 21 et dont les instructions, lorsqu'elles sont exécutées par le ou les

processeurs 20 permettent de réaliser les fonctionnalités décrites plus avant dans la description.

L'interface réseau 22 est une interface de communication filaire ou sans fil adaptée pour établir une communication avec les appareils 1a, 1b, un site internet S', et éventuellement une base de donnée 23, via un réseau R de télécommunication (Internet, téléphonie mobile, ...) et en employant des technologies de réseau telles que, mais sans s'y limiter, GSM, 3G, 4G Wifi, Bluetooth, etc. L'interface réseau 22 permet notamment au serveur distant S de recevoir et émettre des signaux.

La base de données 23 peut être hébergée directement dans le serveur distant S, ou dans un autre serveur ou dans un réseau de serveur type Cloud Computing, ou dans un ordinateur.

Une application informatique est installée dans le serveur distant S pour mettre en œuvre tout ou partie de l'invention depuis ledit serveur comme cela est expliqué plus avant dans la description. Cette application informatique peut être préinstallée sur le serveur distant S ou être téléchargée ultérieurement.

Conformément à l'invention, on crée une liste de paramètres d'authentification qui sont utilisés pour autoriser la connexion à un site internet ou l'accès à des données chiffrées. Ces paramètres d'authentification sont avantageusement répartis en au moins deux groupes.

Un premier groupe consiste en au moins une donnée de géo-localisation de l'appareil 1a et/ou une plage horaire de fonctionnement dudit appareil.

La donnée de géo-localisation peut être générée depuis le module de détermination de position 14. Pour générer cette donnée, l'utilisateur peut par exemple activer ce module pour déterminer une position exacte et définir un périmètre, ou rayon, autour de cette position. Il peut également s'agir d'un lieu (ex : la tour Eiffel) et/ou d'une zone géographique (ex : Paris) sélectionnés par l'utilisateur depuis une carte interactive, par exemple GoogleMap®, affichée sur une interface graphique 13.

La plage horaire de fonctionnement de l'appareil peut consister en un ou plusieurs jours de la semaine et/ou un laps de temps. Par exemple, cette plage horaire peut être : le lundi, entre 8h et 10h. Cette plage horaire peut notamment être définie par l'utilisateur de la même façon que l'on règle une alarme sur un Smartphone.

Le second groupe consiste en au moins une autre donnée autre qu'un mot de passe, qu'un login, qu'une donnée de géo-localisation de l'appareil informatique et qu'une

plage horaire de fonctionnement dudit appareil. Il s'agit préférentiellement, mais non exclusivement, de :

- L'identifiant intégré dans la carte SIM (pour Subscriber Identity Module) d'un Smartphone dans le cas où l'appareil 1a est un Smartphone ;
- Un identifiant associé à l'appareil 1a. Cet identifiant peut être généré de façon aléatoire lors de l'installation de l'application informatique, ou généré automatiquement à partir de l'adresse IP (pour Internet Protocol) attribuée à l'appareil lors de sa connexion à un réseau de télécommunication pour télécharger l'application informatique. L'identifiant peut encore être saisi manuellement par l'utilisateur lors du processus d'installation, ou récupéré à partir d'un fichier stocké localement ou sur un serveur distant.
- Le SSID (pour Service Set Identifier) d'un réseau wifi. Ce SSID peut être défini automatiquement par défaut, ou être saisi manuellement par l'utilisateur, lors du paramétrage du réseau wifi.
- Détection d'une connexion Bluetooth entre l'appareil 1a et un autre appareil électronique.
- Un identifiant enregistré dans un tag NFC ou RFID. L'acquisition de cet identifiant peut notamment être effectuée par un scan du tag depuis l'appareil 1a, au moyen d'un lecteur adapté à cet effet.
- Une empreinte digitale, d'un scan rétinien, d'une reconnaissance d'iris, ou autre. L'acquisition de cet identifiant peut notamment être effectuée par un moyen d'acquisition adapté à la nature de cet identifiant, lequel moyen équipe l'appareil 1a.
- Détection d'une connexion entre l'appareil 1a et un serveur proxy.
- Détection d'une connexion entre l'appareil 1a et un serveur VPN (pour Virtual Private Network).
- L'adresse IP (pour Internet Protocol) attribuée à l'appareil 1a lors de sa connexion à un réseau de télécommunication.
- Détection d'une connexion de l'appareil 1a à un réseau social du type Facebook®, Twitter®, Viadeo®, Instagram®, Snapchat®, LinkedIn®, etc.
- Détection d'une connexion de l'appareil 1a à la page d'un ami spécifique ou d'une personne spécifique suivie sur un réseau social du type Facebook®, Twitter®, Viadeo®, Instagram®, Snapchat®, LinkedIn®, etc.

L'adresse MAC (pour Media Access Control) d'une passerelle réseau. Il s'agit typiquement d'un identifiant stocké dans une carte réseau ou une interface réseau similaire.

En se rapportant à la figure 6, l'interface graphique 13 de l'appareil 1a propose à l'utilisateur de choisir les paramètres d'authentification. L'interface graphique 13 affiche da ns une fenêtre, par exemple sous la forme d'un menu 130, par exemple un menu déroulant, l'ensemble des paramètres d'authentification disponibles A, B, C, D,…., Z. Cette fenêtre peut apparaître automatiquement lors de la sélection d'une touche dédiée 131. L'utilisateur peut alors sélectionner dans le menu 130 les paramètres d'authentification qu'il aura choisis et les définir précisément, notamment pour les données de géo-localisation et la plage horaire.

En pratique, l'utilisateur sélectionne au moins un paramètre d'authentification du premier groupe et au moins un paramètre d'authentification du second groupe.

Il définit ensuite, depuis l'interface graphique 13, au moins une condition d'authentification en sélectionnant un ou plusieurs opérateurs logiques appartenant à la liste suivante : ET logique, OU logique, NON logique, et en combinant le ou les opérateurs logiques sélectionnés aux paramètres d'authentification choisis. Sur la figure 6, les opérateurs logiques sont également affichés dans le menu 130, avec les paramètres d'authentification disponibles A, B, C, D,…., Z, dans la même fenêtre. Les opérateurs logiques peuvent toutefois être affichés dans une autre fenêtre et/ou dans un autre menu.

Sur la figure 6, la condition d'authentification est la suivante : 'A' ET 'B' ('C' OU 'D') ET NON 'E'. A titre d'exemple, A peut être choisi dans le premier groupe de paramètres d'authentification. B, C et D peuvent être choisis dans le second groupe de paramètres d'authentification. E peut être choisi dans le premier ou le second groupe de paramètres d'authentification.

Par exemple, la condition d'authentification peut être la suivante :

'le lundi de 8h à 10h' (A)
ET 'connecté à Facebook®' (B)
'Sur la page de Paul' (C)
OU
'Sur la page de Pierre' (D)
ET NON 'situé à PARIS' (E)

En d'autres termes, pour que la condition d'authentification soit remplie, il faut que l'appareil 1a soit en état de fonctionnement un Lundi de 8h à 10h, que l'appareil 1a soit connecté au site internet facebook.com et qu'il consulte la page Facebook® de Paul ou la page Facebook® de Pierre, l'appareil 1a ne devant pas être localisé à Paris (France). Si

l'un de ces paramètres n'est pas respecté, la condition d'authentification n'est pas remplie.

Selon un autre exemple, la condition d'authentification peut être la suivante :

'empreinte digitale' (A)
ET 'connexion à un réseau wifi' (B)
'réseau wifi de Paul' (C)
OU
'réseau wifi de Pierre' (D)
ET NON 'le lundi de 8h à 10h' (E)

Pour que cette condition d'authentification soit remplie, il faut que l'utilisateur scanne son empreinte digitale, que l'appareil 1a soit connecté à un réseau wifi, ce réseau wifi devant être celui de Paul ou de Pierre, tous les jours de la semaine, sauf le Lundi de 8h à 10h. Si l'un de ces paramètres n'est pas respecté, la condition d'authentification n'est pas remplie.

La condition d'authentification définie par l'utilisateur est une condition statique. C'est-à-dire que la sélection d'un paramètre n'influence pas les autres paramètres sélectionnés. En particulier, la sélection d'une plage horaire de fonctionnement est sans incidence sur les autres paramètres, contrairement au processus décrit dans le document brevet US2013/0036462 (QUALCOMM) où on détermine une plage horaire pour faire varier de manière dynamique un ou plusieurs autres paramètres de la condition d'authentification.

On comprend aisément que le nombre élevé de combinaisons possibles de paramètres d'authentification et d'opérateurs logiques, rend la condition d'authentification unique, conférant de fait un degré de sécurité optimal. Il est en effet peu probable qu'un utilisateur mal intentionné puisse découvrir la condition d'authentification.

Bien évidemment, les conditions d'authentification peuvent être plus ou moins complexes selon le type de site internet pour lequel la connexion est demandée ou le type de données chiffrées devant être consultées. Si le site internet est un réseau social ou les données chiffrées un simple texte, la condition d'authentification peut être relativement simple, et par exemple constituée de la combinaison d'un paramètre du premier groupe et d'un paramètre du second groupe avec un seul opérateur logique. La condition sera toutefois plus complexe, du type décrit précédemment en référence à la figure 6, lorsque le site internet est un compte bancaire en ligne ou que les données chiffrées sont des fichiers hautement confidentiels.

Ceci étant exposé, les mises en œuvre du procédé objet de l'invention, d'une part pour autoriser l'accès à un site internet et d'autre part autoriser l'accès à des données chiffrées, vont maintenant êtres décrites plus en détails.

Accès à un site internet (figures 1, 7 et 8)

Dans ce cas, l'objectif est de sécuriser l'accès à un site internet S', cet accès étant limité à l'utilisateur et protégé, c'est-à-dire que son accès est bloqué. Ce site internet S' peut par exemple être un compte bancaire en ligne de l'utilisateur, un réseau social, un groupe de discussion, etc.

En pratique, le site internet S' est géré par un serveur informatique du type décrit précédemment en référence à la figure 5. Une application informatique est avantageusement installée dans le serveur gérant le site internet S' pour mettre en œuvre tout ou partie de l'invention depuis ledit serveur. Cette application informatique peut être préinstallée sur ce serveur ou être téléchargée ultérieurement.

Phase préalable de paramétrage (figures 1 et 7)

Dans une étape 101, l'appareil 1a se connecte au site internet S'. Cette connexion est réalisée via un réseau de télécommunication R et est schématisée par une double flèche sur la figure 1. L'utilisateur peut être amené à suivre une procédure habituelle pour s'enregistrer sur le site internet S' en question. Pour effectuer cet enregistrement, il peut notamment être demandé à l'utilisateur de s'identifier en renseignant une ou plusieurs données d'identification, par exemple : nom, prénom, âge, adresse, numéro de téléphone, adresse mail, etc.

Dans une étape 102, le site interne S' se connecte au serveur S. Cette connexion est réalisée via un réseau de télécommunication R et est schématisée par une flèche sur la figure 1. Cette connexion est accompagnée d'une requête par laquelle le site S' demande au serveur S de générer un identifiant unique.

Dans une étape 103, le serveur S génère un identifiant unique ainsi qu'une paire de clés RSA. Cet identifiant est préférentiellement généré de façon aléatoire. Le chiffrement RSA est bien connu de l'homme du métier. Il utilise une paire de clés (des nombres entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. L'homme du métier pourra se référer au document brevet US4405829 (MASSACHUSETTS INST TECHNOLOGY) en cas de besoin. L'identifiant unique est enregistré dans la mémoire 21 du serveur S.

Dans une étape 104, le serveur S transfère l'identifiant unique au site S'. Cette transmission est réalisée via un réseau de télécommunication R.

Dans une étape 105, le site S' crée un nouvel identifiant unique en associant l'identifiant renvoyé par le serveur S aux données que l'utilisateur a renseigné lors de la procédure d'enregistrement (étape 101). Ce nouvel identifiant unique est enregistré dans la mémoire du site S'.

Dans une étape 106, le site S' transfère ce nouvel identifiant unique à l'appareil 1a, via un réseau de télécommunication R. Cet identifiant peut s'afficher sur l'interface graphique dudit site, par exemple sous la forme d'un code QR, d'un code barres, ou sous toute autre forme convenant à l'homme du métier.

Dans une étape 107, l'appareil 1a acquiert ce nouvel identifiant, par exemple en scannant le code QR sur l'interface graphique du site internet S'.

Dans une étape 108, l'appareil 1a se connecte au serveur S, via un réseau de télécommunication R. Cette connexion est accompagnée d'une requête contenant l'identifiant acquis et par laquelle l'appareil 1a demande au serveur S de lui envoyer la clé RSA publique associée audit identifiant.

Dans une étape 109, le serveur S transfère à l'appareil 1a, via un réseau de télécommunication R, la clé RSA publique associée à l'identifiant.

Dans une étape 110, l'utilisateur définit, depuis l'appareil 1a, une condition d'authentification, en sélectionnant des paramètres d'authentification et en les combinant aux opérateurs logiques.

Dans une étape 111, l'appareil 1a génère une clé AES (pour Advanced Encryption Standard). Le chiffrement AES est bien connu de l'homme du métier. En cas de besoin, ce dernier pourra se référer à la publication : « Federal Information Processing Standards Publication 197, November 26, 2001, Announcing the ADVANCED ENCRYPTION STANDARD (AES) ». L'appareil 1a chiffre, avec cette clé AES, la condition d'authentification définie à l'étape 110.

Dans une étape 112, l'appareil 1a chiffre la clé AES avec la clé RSA publique précédemment récupérée auprès du serveur S.

Dans une étape 113, l'appareil 1a se connecte au serveur S, via un réseau de télécommunication R, pour lui transférer l'identifiant acquit à l'étape 107, la condition d'authentification chiffrée et la clé AES chiffrée.

Dans une étape 114, le serveur S déchiffre la clé AES avec sa clé RSA privée. Le serveur S déchiffre alors la condition d'authentification, la vérifie et l'associe à l'identifiant.

Dans une étape 115, le serveur se connecte au site S', via un réseau de télécommunication R, et lui notifie le bon déroulement des opérations.

Phase ultérieure d'accès au site internet (figures 1 et 8)

Dans une étape 201, l'appareil 1a se connecte au site S' dont l'accès est protégé, via un réseau de télécommunication R. L'utilisateur peut être amené à suivre une procédure habituelle pour s'authentifier sur le site S', par exemple en saisissant uniquement son nom d'utilisateur ou son adresse mail. La connexion de l'appareil 1a au site S' déclenche alors la mise en œuvre d'un processus décrit ci-après, lequel processus entraine la connexion automatique dudit appareil au serveur S.

Dans une étape 202, le site S' transfère l'identifiant créé à l'étape 105, à l'appareil 1a, via un réseau de télécommunication R. Cet identifiant s'affiche sur l'interface graphique du site internet S', par exemple sous la forme d'un code QR, d'un code barres, ou sous toute autre forme convenant à l'homme du métier.

Dans une étape 203, l'appareil 1a acquiert cet identifiant, par exemple en scannant le code QR.

Dans une étape 204, l'appareil 1a se connecte automatiquement au serveur S, via un réseau de télécommunication R. Cette connexion est accompagnée d'une requête contenant l'identifiant acquis et par laquelle l'appareil 1a demande au serveur S de lui envoyer la clé RSA publique associée audit identifiant.

Dans une étape 205, le serveur S génère une nouvelle paire de clés RSA qu'il associe à l'identifiant.

Dans une étape 206, le serveur S transfère la clé RSA publique à l'appareil 1a. Cette transmission est réalisée via un réseau de télécommunication R.

Dans une étape 207, l'utilisateur peut être amené à générer un paramètre d'authentification, par exemple : connexion à un réseau wifi ; connexion Bluetooth ; empreinte digitale ; scan rétinien ; reconnaissance d'iris, scan d'un tag NFC ou RFID ; etc. Cela n'intervient que si la génération d'un des paramètres d'authentification nécessite une action volontaire de l'utilisateur sur l'appareil 1a. Dans tous les autre cas, l'appareil 1a détecte automatiquement tous les paramètres d'authentification déterminés à l'étape 110.

Dans une étape 208, l'appareil 1a génère une clé AES et chiffre, avec cette clé, les paramètres d'authentification de l'étape 207 et la clé RSA publique précédemment récupérée auprès du serveur S.

Dans une étape 209, l'appareil 1a se connecte au serveur S, via un réseau de télécommunication R, pour lui transférer l'identifiant, les paramètres d'authentification chiffrés et la clé AES chiffrée.

Dans une étape 210, le serveur S déchiffre la clé AES avec sa clé RSA privée. Le serveur S déchiffre alors les paramètres d'authentification. Il les confronte à la condition d'authentification définie à l'étape 110 et reçue à l'étape 114.

Dans une étape 211, le serveur S génère une instruction pour autoriser l'accès au site S'. Cette instruction d'autorisation n'est générée que si les paramètres d'authentification transmis à l'étape 209 respectent la condition d'authentification définie à l'étape 110.

Dans une étape 212, le serveur S se connecte au site S', via un réseau de télécommunication R, et lui notifie la réussite ou l'échec de la connexion. En cas de réussite, le serveur S transfert au site S' l'instruction d'autorisation, et en réponse à la réception de cette instruction, ledit site S' autorise son accès à l'appareil 1a. En cas d'échec, le site S' refuse son accès à l'appareil 1a et lui notifie éventuellement l'interdiction de cet accès.

Accès à des données chiffrées (figures 2, 9 et 10) – Cas n°1

L'objectif est ici de sécuriser l'accès à des données chiffrées, cet accès étant limité à l'utilisateur et protégé. Ces données chiffrées sont par exemple des documents ou des fichiers (contenant du texte, donnée audio, donnée vidéo, photo, …) enregistrés dans la mémoire 11 de l'appareil 1a.

Phase préalable de paramétrage (figures 2 et 9)

Dans une étape 301, l'utilisateur définit, depuis l'appareil 1a, une condition d'authentification, en sélectionnant des paramètres d'authentification et en les combinant aux opérateurs logiques.

Dans une étape 302, l'appareil 1a génère une paire de clés RSA ainsi qu'une clé AES. L'appareil 1a chiffre, avec cette clé AES, la condition d'authentification définie à l'étape 301.

Dans une étape 303, l'appareil 1a se connecte au serveur S, via un réseau de télécommunication R, pour lui transférer la condition d'authentification chiffrée à l'étape 302 et la clé RSA publique. Ces éléments sont enregistrés dans la mémoire 21 du serveur S.

Dans une étape 304, le serveur S génère un identifiant unique et l'enregistre dans sa mémoire 21.

Dans une étape 305, le serveur S génère une paire de clés RSA ainsi qu'une clé AES. Le serveur S chiffre cette clé AES avec la clé RSA publique reçue à l'étape 303. La clé AES ainsi chiffrée et la clé RSA privée sont enregistrées dans la mémoire 21 du serveur S.

Dans une étape 306, le serveur S transfère à l'appareil 1a : l'identifiant unique généré à l'étape 304, la clé AES chiffrée à l'étape 305 et la clé RSA publique générée à l'étape 305. Cette transmission est réalisée via un réseau de télécommunication R.

Dans une étape 307, l'appareil 1a déchiffre la clé AES reçue à l'étape 306 avec sa clé RSA privée.

Dans une étape 308, l'appareil 1a crée et chiffre ses données dont l'accès doit être limité et protégé. Ce chiffrement des données est réalisé avec la clé AES déchiffrée à l'étape 307.

Dans une étape 309, l'appareil 1a chiffre sa clé AES générée à l'étape 302, avec la clé RSA publique du serveur S reçue à l'étape 306.

Dans une étape 310, l'appareil 1a enregistre dans ses données chiffrées à l'étape 308 : l'identifiant unique reçu à l'étape 306, sa paire de clés RSA générée à l'étape 302, la clé AES chiffrée à l'étape 309, la clé RSA publique du serveur S reçue à l'étape 306.

Phase ultérieure d'accès aux données chiffrées (figures 2 et 10)

Dans une étape 401, l'utilisateur peut être amené à générer un paramètre d'authentification, par exemple : connexion à un réseau wifi ; connexion Bluetooth ; empreinte digitale ; scan rétinien ; reconnaissance d'iris, scan d'un tag NFC ou RFID ; etc. Cela n'intervient que si la génération d'un des paramètres d'authentification nécessite une action volontaire de l'utilisateur. Dans tous les autre cas, l'appareil 1a détecte automatiquement tous les paramètres d'authentification déterminés à l'étape 301.

Dans une étape 402, l'utilisateur sélectionne ses données chiffrées et l'appareil 1a extrait de ces données chiffrées : l'identifiant unique reçu à l'étape 306, la paire de clés RSA générée à l'étape 302, la clé AES chiffrée à l'étape 309, la clé RSA publique du serveur S reçue à l'étape 306.

Dans une étape 403, l'appareil 1a génère une nouvelle clé AES. L'appareil 1a chiffre, avec cette nouvelle clé AES, les paramètres d'authentification relevés à l'étape 401.

Dans une étape 404, l'appareil 1a chiffre la nouvelle clé AES générée à l'étape 403, avec la clé RSA publique du serveur S extraite à l'étape 402.

Dans une étape 405, l'appareil 1a se connecte au serveur S, via un réseau de télécommunication R, pour lui transférer : les paramètres d'authentification chiffrés à l'étape 403, la nouvelle clé AES chiffrée à l'étape 404, la clé AES extraite à l'étape 402, l'identifiant extrait à l'étape 402.

Dans une étape 406, le serveur S déchiffre les clés AES reçues à l'étape 405 avec sa clé RSA privée.

Dans une étape 407, le serveur S déchiffre les paramètres d'authentification reçus à l'étape 405, avec la nouvelle clé AES déchiffrée à l'étape 406.

Dans une étape 408, le serveur S déchiffre la condition d'authentification reçue à l'étape 303, avec la clé AES extraite à l'étape 402 et déchiffrée à l'étape 406.

Dans une étape 409, le serveur S confronte les paramètres d'authentification déchiffrés à l'étape 407 à la condition d'authentification déchiffrée à l'étape 408.

Dans une étape 410, le serveur S génère une instruction pour autoriser l'accès aux données chiffrées. Cette instruction n'est générée que si les paramètres d'authentification déchiffrés à l'étape 407 respectent la condition d'authentification déchiffrée à l'étape 408. Cette instruction se matérialise avantageusement sous la forme de la clé AES chiffrée à l'étape 305.

Dans une étape 411, le serveur S transfère à l'appareil 1a : la clé AES chiffrée à l'étape 305. Cette transmission est réalisée via un réseau de télécommunication R.

Dans une étape 412, l'appareil 1a déchiffre la clé AES reçue à l'étape 411, avec sa clé RSA privée générée à l'étape 302.

Dans une étape 413, l'appareil 1a déchiffre les données chiffrées. Ce déchiffrement est réalisé avec la clé AES déchiffrée à l'étape 412.

Accès à des données chiffrées (figures 3, 11 et 12) – Cas n°2

L'objectif est ici de sécuriser l'accès à des données chiffrées, cet accès étant limité à l'utilisateur et protégé. Ces données chiffrées sont par exemple des documents ou des fichiers (contenant du texte, donnée audio, donnée vidéo, photo, ...) enregistrés dans la mémoire d'un autre appareil électronique 1b. A titre d'exemple, cet appareil électronique 1b est un ordinateur portable alors que l'appareil électronique 1a est un Smartphone.

Phase préalable de paramétrage (figures 3 et 11)

Dans une étape 501, l'appareil 1b génère une paire de clés RSA.

Dans une étape 502, l'appareil 1b se connecte au serveur S, via un réseau de télécommunication R, pour lui transférer la clé RSA publique.

Dans une étape 503, le serveur S génère un identifiant unique et l'enregistre dans sa mémoire 21.

Dans une étape 504, le serveur S génère une paire de clés RSA. La clé RSA privée est enregistrée dans la mémoire 21 du serveur S.

Dans une étape 505, le serveur S génère un jeton d'authentification (token en anglais) et y associe : la clé RSA publique reçue à l'étape 502 et la clé RSA publique générée à l'étape 504 et l'identifiant unique généré à l'étape 503.

Dans une étape 506, le serveur S se connecte à l'appareil 1b, via un réseau de télécommunication R, pour lui transférer le jeton d'authentification de l'étape 505.

Dans une étape 507, le jeton reçu à l'étape 506 s'affiche sur l'interface graphique 13 de l'appareil 1b, par exemple sous la forme d'un code QR, d'un code barres, ou sous toute autre forme convenant à l'homme du métier.

Dans une étape 508, l'appareil 1a acquiert le jeton affiché sur l'interface graphique 13 de l'appareil 1b, par exemple en scannant le code QR.

Dans une étape 509, l'appareil 1a se connecte au serveur S, via un réseau de télécommunication R. Cette connexion intervient automatiquement en réponse à l'acquisition de l'étape 508.

Dans une étape 510, le serveur S transfère à l'appareil 1a : le jeton d'authentification de l'étape 505, la clé RSA publique générée à l'étape 504 et l'identifiant unique généré à l'étape 503.

Dans une étape 511, l'utilisateur définit, depuis l'appareil 1a, une condition d'authentification, en sélectionnant des paramètres d'authentification et en les combinant aux opérateurs logiques.

Dans une étape 512, l'appareil 1a génère une clé AES. L'appareil 1a chiffre, avec cette clé AES, la condition d'authentification définie à l'étape 511.

Dans une étape 513, l'appareil 1a chiffre sa clé AES générée à l'étape 512, avec la clé RSA publique du serveur S reçue à l'étape 510.

Dans une étape 514, l'appareil 1a se connecte au serveur S, via un réseau de télécommunication R, pour lui transférer : la condition d'authentification chiffrée à l'étape 512, la clé AES chiffrée à l'étape 513, le jeton reçu à l'étape 510, l'identifiant reçu à l'étape 510.

Dans une étape 515, le serveur enregistre dans sa mémoire 21, la condition d'authentification chiffrée reçue à l'étape 514.

Dans une étape 516, le serveur S génère une clé AES et la chiffre avec la clé RSA publique reçue à l'étape 502. Cette clé AES chiffrée est enregistrée dans la mémoire 21 du serveur S.

Dans une étape 517, le serveur S se connecte à l'appareil 1b, via un réseau de télécommunication R, pour lui transférer : l'identifiant unique reçu à l'étape 514, la clé AES chiffrée de l'étape 513 reçue à l'étape 514, la clé AES chiffrée à l'étape 516, la clé RSA publique générée à l'étape 504.

Dans une étape 518, l'appareil 1b déchiffre la clé AES de l'étape 516 avec sa clé RSA privée.

Dans une étape 519, l'appareil 1b crée et chiffre ses données dont l'accès doit être limité et protégé. Ce chiffrement des données est réalisé avec la clé AES déchiffrée à l'étape 518.

Dans une étape 520, l'appareil 1b enregistre dans ses données chiffrées à l'étape 519 : l'identifiant unique reçu à l'étape 517, sa paire de clés RSA générée à l'étape 501, la clé AES chiffrée de l'étape 513, la clé RSA publique du serveur S reçue à l'étape 517.

Phase ultérieure d'accès aux données chiffrées (figures 3 et 12)

Dans une étape 601, l'utilisateur sélectionne ses données chiffrées et l'appareil 1b extrait de ces données chiffrées : l'identifiant unique, la clé AES chiffrée de l'étape 513, sa paire de clés RSA générée à l'étape 501, la clé RSA publique du serveur S reçue à l'étape 517.

Dans une étape 602, l'appareil 1b se connecte au serveur S, via un réseau de télécommunication R, pour lui transférer : l'identifiant unique, la clé AES chiffrée de l'étape 513, la clé RSA publique du serveur S.

Dans une étape 603, le serveur S génère un jeton d'authentification et y associe les données reçues à l'étape 602, c'est-à-dire : l'identifiant unique, la clé AES chiffrée de l'étape 513, la clé RSA publique du serveur S.

Dans une étape 604, le serveur S se connecte à l'appareil 1b, via un réseau de télécommunication R, pour lui transférer le jeton d'authentification de l'étape 603.

Dans une étape 605, le jeton reçu à l'étape 604 s'affiche sur l'interface graphique 13 de l'appareil 1b, par exemple sous la forme d'un code QR, d'un code barres, ou sous toute autre forme convenant à l'homme du métier.

Dans une étape 606, l'appareil 1a acquiert le jeton affiché sur l'interface graphique 13 de l'appareil 1b, par exemple en scannant le code QR.

Dans une étape 607, l'appareil 1a se connecte au serveur S, via un réseau de télécommunication R. Cette connexion intervient automatiquement en réponse à l'acquisition de l'étape 606.

Dans une étape 608, le serveur S transfère à l'appareil 1a : le jeton d'authentification de l'étape 603, la clé RSA publique du serveur S et l'identifiant unique reçu à l'étape 602.

Dans une étape 609, l'utilisateur peut être amené à générer un paramètre d'authentification, par exemple : connexion à un réseau wifi ; connexion Bluetooth ; empreinte digitale ; scan rétinien ; reconnaissance d'iris, scan d'un tag NFC ou RFID ; etc. Cela n'intervient que si la génération d'un des paramètres d'authentification nécessite une action volontaire de l'utilisateur. Dans tous les autre cas, l'appareil 1a détecte automatiquement tous les paramètres d'authentification déterminés à l'étape 511.

Dans une étape 610, l'appareil 1a génère une nouvelle clé AES. L'appareil 1a chiffre, avec cette nouvelle clé AES, les paramètres d'authentification relevés à l'étape 609.

Dans une étape 611, l'appareil 1a chiffre la nouvelle clé AES générée à l'étape 610, avec la clé RSA publique du serveur S reçue à l'étape 608.

Dans une étape 612, l'appareil 1a se connecte au serveur S, via un réseau de télécommunication R, pour lui transférer : les paramètres d'authentification chiffrés à l'étape 610, la nouvelle clé AES de l'étape 610 chiffrée à l'étape 611, la clé AES extraite à l'étape 601, le jeton d'authentification reçu à l'étape 608, l'identifiant unique reçu à l'étape 608.

Dans une étape 613, le serveur S déchiffre les clés AES reçues à l'étape 612 avec sa clé RSA privée.

Dans une étape 614, le serveur S déchiffre les paramètres d'authentification reçus à l'étape 612, avec la nouvelle clé AES de l'étape 610 déchiffrée à l'étape 613.

Dans une étape 615, le serveur S déchiffre la condition d'authentification reçue à l'étape 514, avec la clé AES extraite à l'étape 601 et déchiffrée à l'étape 613.

Dans une étape 616, le serveur S confronte les paramètres d'authentification déchiffrés à l'étape 614 à la condition d'authentification déchiffrée à l'étape 615.

Dans une étape 617, le serveur S génère une instruction pour autoriser l'accès aux données chiffrées. Cette instruction n'est générée que si les paramètres

d'authentification déchiffrés à l'étape 614 respectent la condition d'authentification déchiffrée à l'étape 615. Cette instruction se matérialise avantageusement sous la forme de la clé AES chiffrée à l'étape 516.

Dans une étape 618, le serveur S transfère à l'appareil 1b : la clé AES chiffrée à l'étape 516. Cette transmission est réalisée via un réseau de télécommunication R.

Dans une étape 619, l'appareil 1b déchiffre la clé AES reçue à l'étape 618, avec sa clé RSA privée générée à l'étape 501.

Dans une étape 620, l'appareil 1b déchiffre les données chiffrées. Ce déchiffrement est réalisé avec la clé AES déchiffrée à l'étape 619.

L'agencement des différents éléments et/ou moyens et/ou étapes de l'invention, dans les modes de réalisation décrits ci-dessus, ne doit pas être compris comme exigeant un tel agencement dans toutes les implémentations. Il est évident que d'autres modes de réalisation qui partent de ces détails pourraient encore être compris comme entrant dans le cadre des revendications annexées. En tout état de cause, on comprendra que diverses modifications peuvent être apportées à ces éléments et/ou moyens et/ou étapes, sans s'écarter de l'esprit et de la portée de l'invention. En particulier :

- Les étapes de chiffrement RSA et AES ne sont pas essentielles bien qu'elles renforcent davantage la sécurité.
- Le chiffrement RSA peut être remplacé par n'importe quel autre algorithme de cryptographie asymétrique, ou symétrique.
- Le chiffrement AES peut être remplacé par n'importe quel autre algorithme de cryptographie symétrique, ou asymétrique.

Revendications

1. Procédé d'authentification pour autoriser l'accès à un site internet (S') depuis un appareil informatique (1a) d'un utilisateur,

- **dans lequel**, une phase préalable de paramétrage comprend les étapes suivantes :
  - créer une liste de paramètres d'authentification (A, B, C, D, ..., Z), lesquels paramètres sont répartis :
    - dans un premier groupe consistant en au moins une donnée de géo-localisation de l'appareil informatique (1a) et/ou une plage horaire de fonctionnement dudit appareil,
    - et dans un second groupe consistant en au moins une donnée autre qu'un mot de passe, qu'un login, qu'une donnée de géo-localisation de l'appareil informatique (1a) et qu'une plage horaire de fonctionnement dudit appareil,
  - sélectionner au moins un paramètre d'authentification du premier groupe et au moins un paramètre d'authentification du second groupe,
  - définir une condition d'authentification en sélectionnant un ou plusieurs opérateurs logiques appartenant à la liste suivante : ET logique, OU logique, NON logique, et combiner le ou les opérateurs logiques sélectionnés aux paramètres d'authentification choisis,
  - enregistrer, dans un serveur informatique (S) qui est distant de l'appareil informatique (1a), cette condition d'authentification, lequel serveur informatique est adapté pour gérer la connexion au site internet (S'),
- **et dans lequel**, une phase ultérieure d'accès au site internet (S') comprend les étapes suivantes :
  - l'appareil informatique (1a) se connecte au site internet (S') dont l'accès est protégé,
  - la connexion de l'appareil informatique (1a) au site internet (S') déclenche la mise en œuvre d'un processus qui entraine la connexion automatique dudit appareil au serveur informatique (S),
  - l'appareil informatique (1a) transmet au serveur informatique (S) des paramètres d'authentification,

- le serveur informatique (S) analyse les paramètres d'authentification transmis par l'appareil informatique (1a) et les confronte à la condition d'authentification,
- le serveur informatique (S) génère une instruction d'autorisation d'accès au site internet (S'), cette instruction n'étant générée que si les paramètres d'authentification transmis respectent la condition d'authentification,
- le serveur informatique (S) transfert l'instruction d'autorisation au site internet (S'),
- en réponse à la réception de l'instruction d'autorisation, le site internet (S') autorise son accès à l'appareil informatique (1a).

2. Procédé selon la revendication 1, dans lequel, durant la phase préalable de paramétrage, les paramètres d'authentification sont sélectionnés de manière à ce que durant la phase ultérieure d'accès au site internet (S'), l'appareil informatique (1a) puisse détecter automatiquement tous ces paramètres d'authentification sans action volontaire sur ledit appareil.

3. Procédé selon l'une des revendications précédentes, dans lequel la condition d'authentification est une condition statique, la sélection d'un paramètre n'influençant pas les autres paramètres sélectionnés.

4. Procédé selon l'une des revendications précédentes, dans lequel le second groupe consiste en au moins une donnée choisie dans la liste suivante : détection d'une connexion de l'appareil informatique (1a) à un réseau social ; détection d'une connexion de l'appareil informatique (1a) à la page d'un ami spécifique ou d'une personne spécifique suivie sur un réseau social.

5. Procédé selon l'une des revendications précédentes, dans lequel le second groupe consiste en au moins une donnée choisie dans la liste suivante : identifiant intégré dans une carte SIM de l'appareil informatique (1a) ; identifiant associé à l'appareil informatique (1a) ; SSID d'un réseau wifi ; détection d'une connexion Bluetooth entre l'appareil informatique (1a) et un autre appareil électronique ; identifiant enregistré dans un tag NFC ou RFID ; empreinte digitale ; scan rétinien ; reconnaissance d'iris ; détection d'une connexion entre l'appareil informatique (1a) et un serveur proxy ; détection d'une connexion entre l'appareil informatique (1a) et un serveur VPN ; adresse IP attribuée à l'appareil informatique (1a) lors de sa connexion à un réseau de télécommunication ; adresse MAC d'une passerelle réseau.

6. Procédé selon l'une des revendications précédentes, dans lequel la donnée de géo-localisation de l'appareil informatique (1a) est sélectionnée par l'utilisateur depuis une carte interactive affichée sur une interface graphique (13) dudit appareil.

7. Procédé selon l'une des revendications précédentes, dans lequel la plage horaire de fonctionnement de l'appareil informatique (1a) consiste en un ou plusieurs jours de la semaine et un laps de temps.

8. Procédé selon l'une des revendications précédentes, dans lequel la phase préalable de paramétrage comprend en outre les étapes suivantes :

- afficher, depuis un menu (130) accessible depuis une interface graphique (13) de l'appareil informatique (1a), l'ensemble des paramètres d'authentification (A, B, C, D,…., Z),
- sélectionner, dans le menu (130), des paramètres d'authentification parmi l'ensemble des paramètres d'authentification affichés.

9. Procédé selon la revendication 8, dans lequel les opérateurs logiques sont affichés dans le menu (130) avec l'ensemble des paramètres d'authentification (A, B, C, D,…., Z).

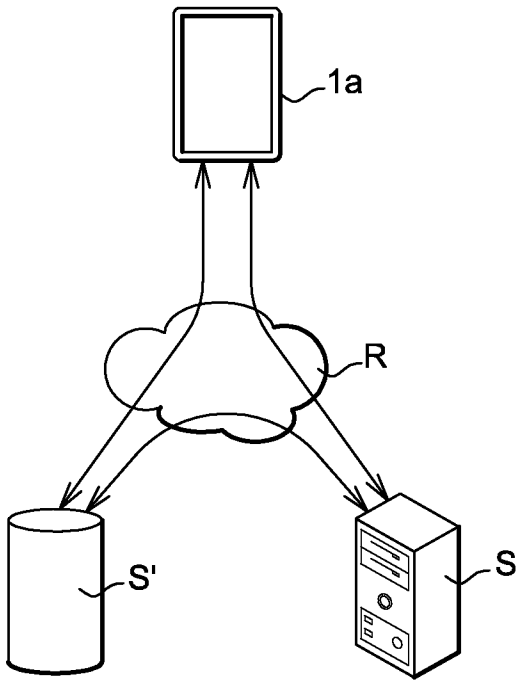
10. Procédé selon l'une des revendications précédentes, comprenant une étape consistant à chiffrer la condition d'authentification avec un algorithme de cryptographie.

11. Procédé selon la revendication 10, consistant à chiffrer la condition d'authentification avec une clé AES générée par l'appareil informatique (1a).

12. Procédé selon la revendication 11, comprenant une étape consistant à chiffrer la clé AES avec une clé RSA publique générée par le serveur informatique (S).

13. Procédé selon la revendication 12, dans lequel la clé RSA publique est générée par le serveur informatique (S) en réponse à une requête transmise par le site internet (S').

Fig. 1



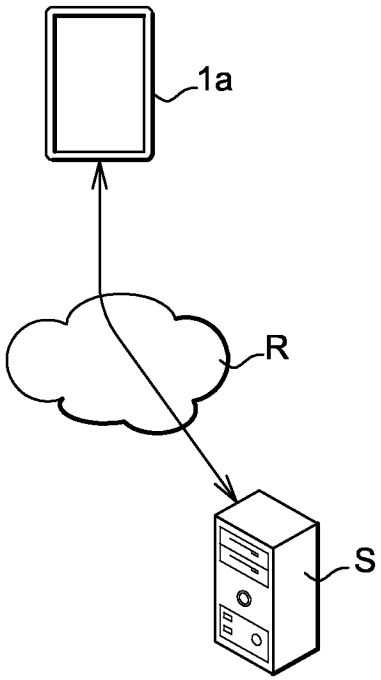


Fig. 2

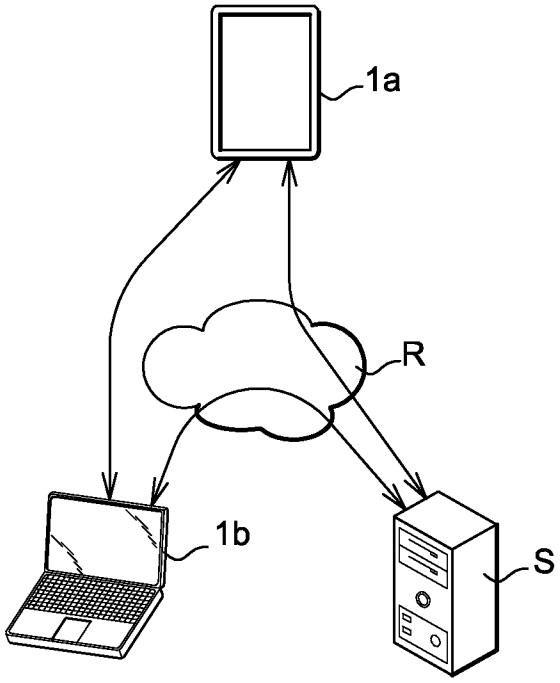


Fig. 3

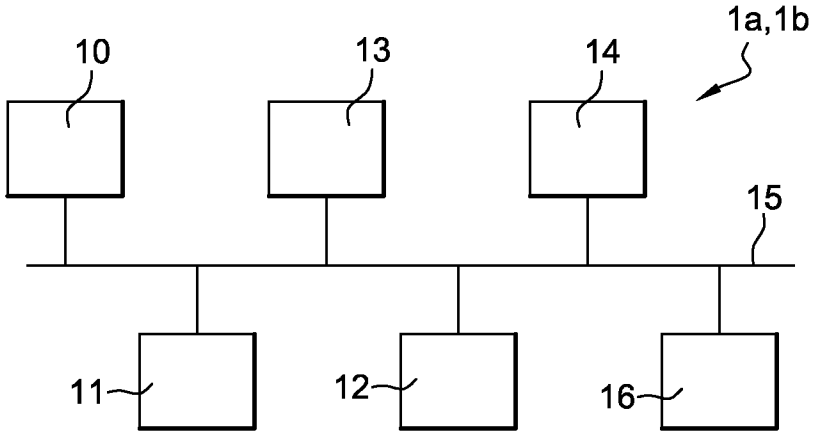


Fig. 4

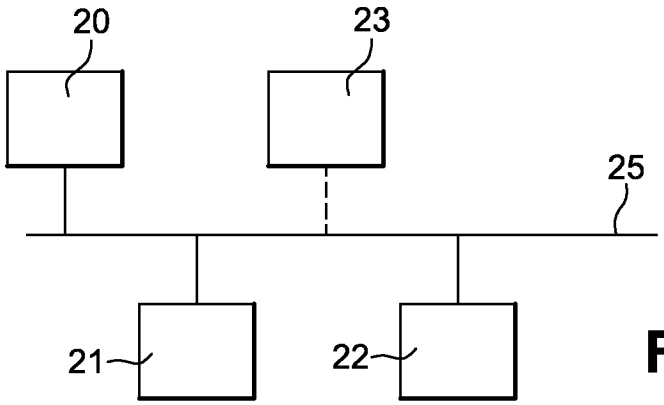


Fig. 5

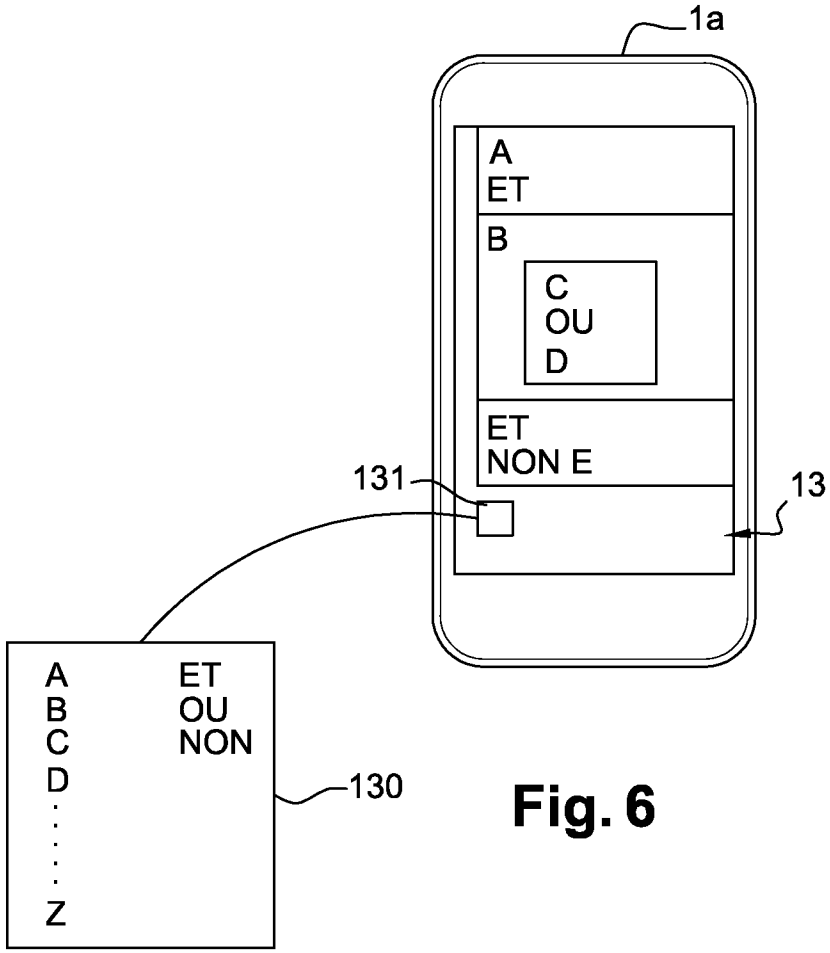

1a
A
ET
B
C
OU
D
ET
NON E
131
13
A
B
C
D
Z
ET
OU
NON
130

Fig. 6

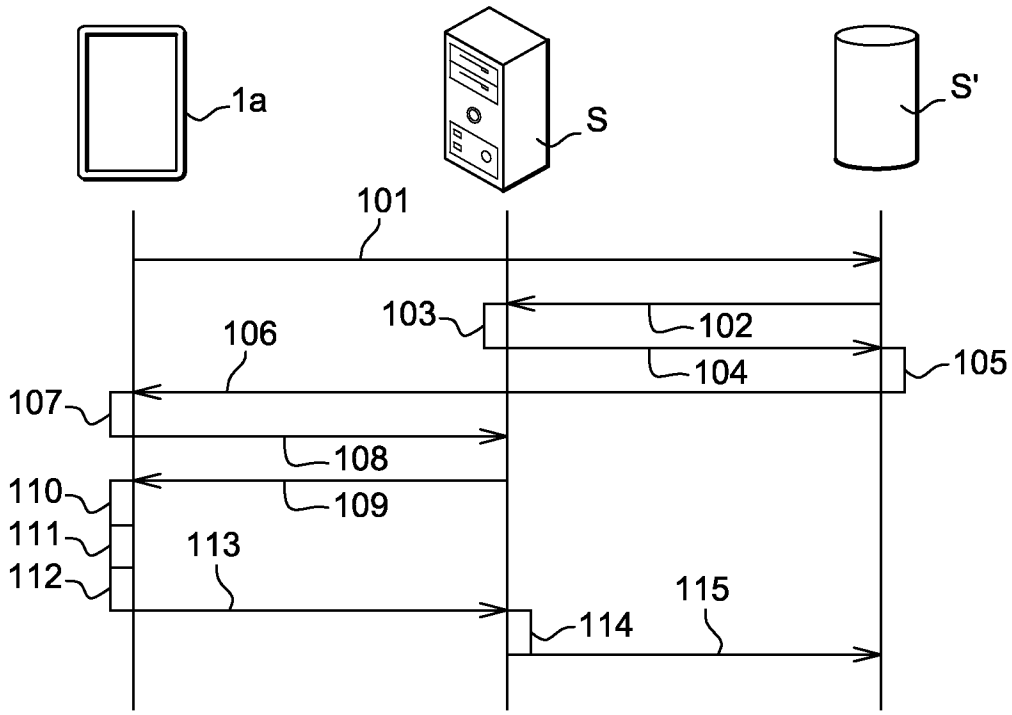

1a
S
S'
101
103
102
106
104
105
107
108
110
109
111
113
112
115
114

Fig. 7

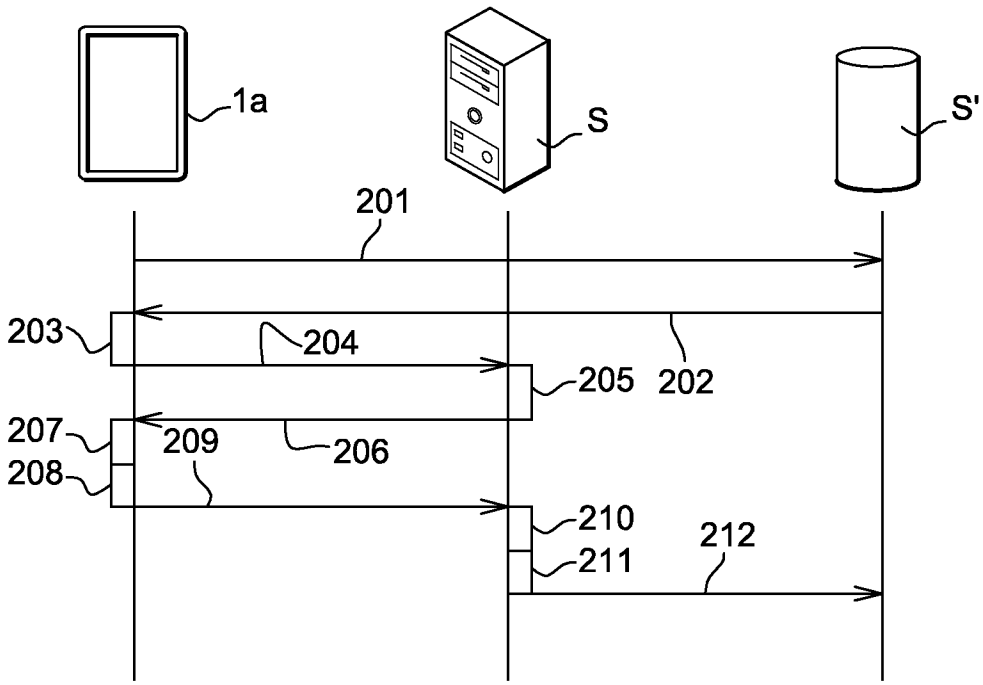

1a
S
S'
201
203
204
205
202
207
209
206
208
210
211
212

Fig. 8

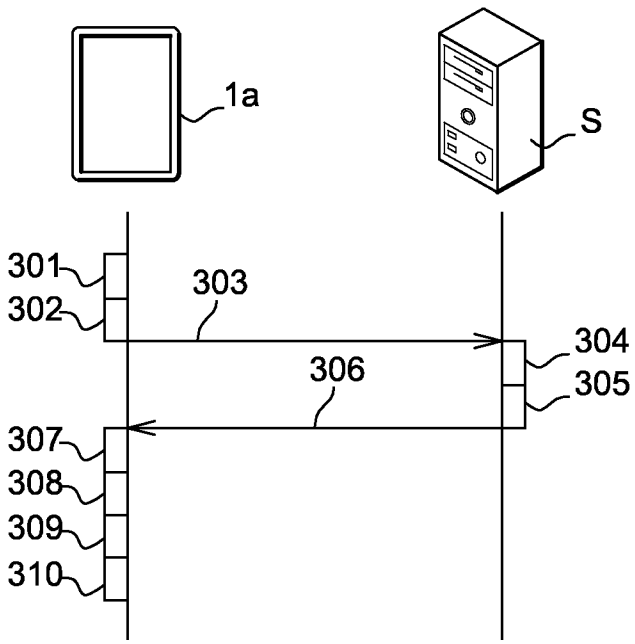

1a
S
301
302
303
304
306
305
307
308
309
310

Fig. 9

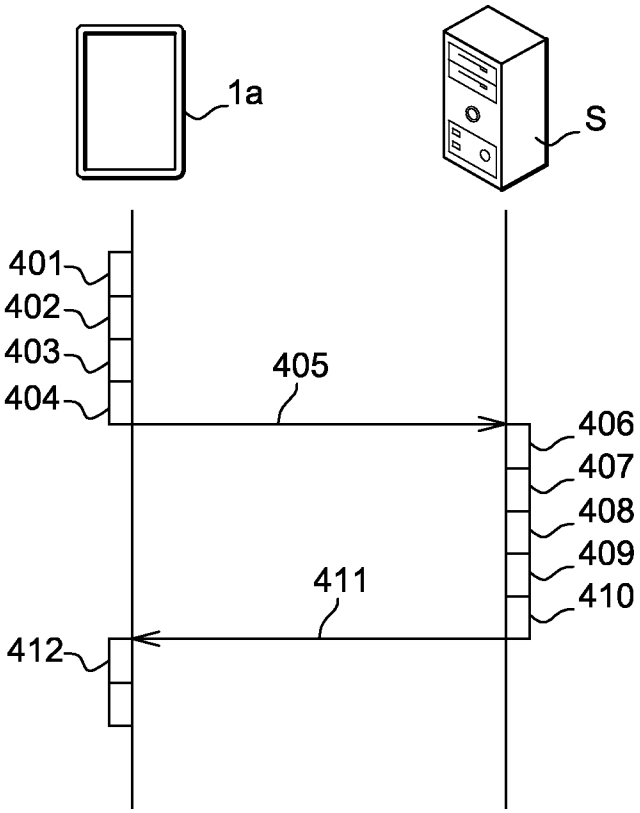

1a
S
401
402
403
404
405
406
407
408
409
410
411
412

Fig. 10

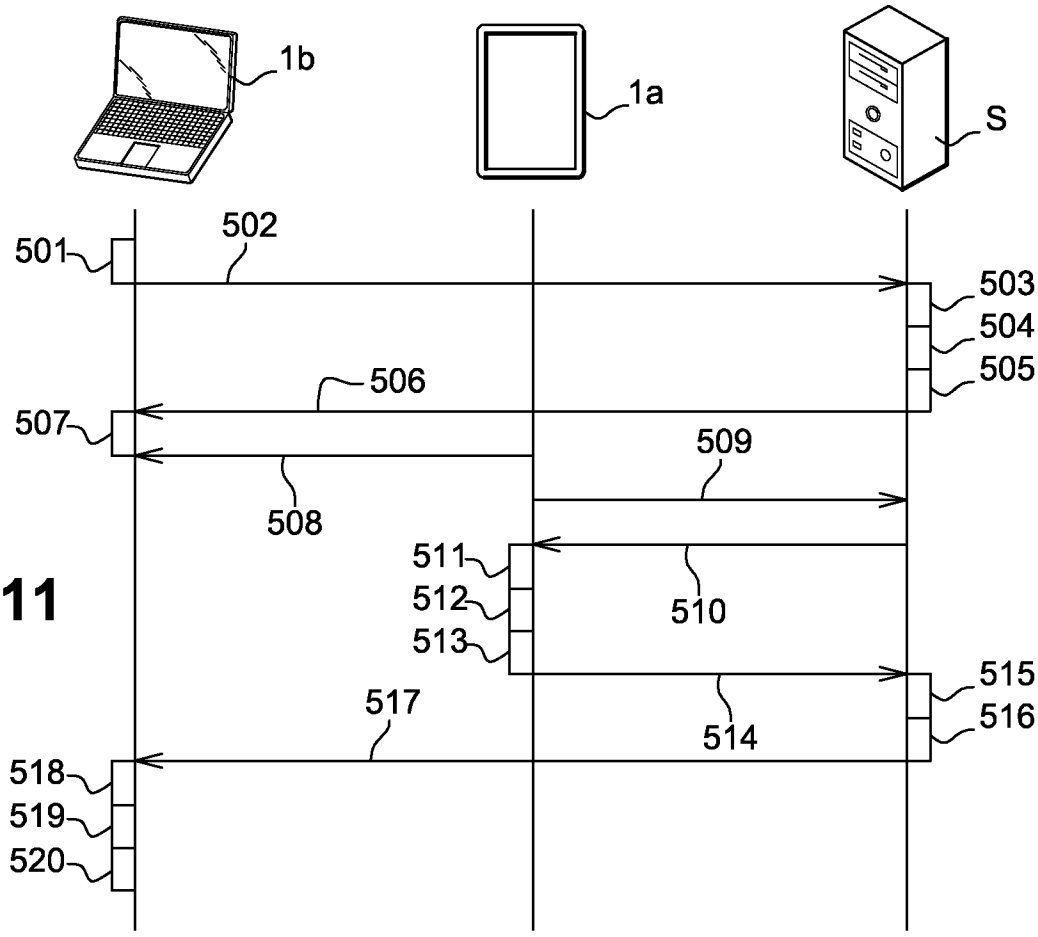

1b
1a
S
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520

Fig. 11

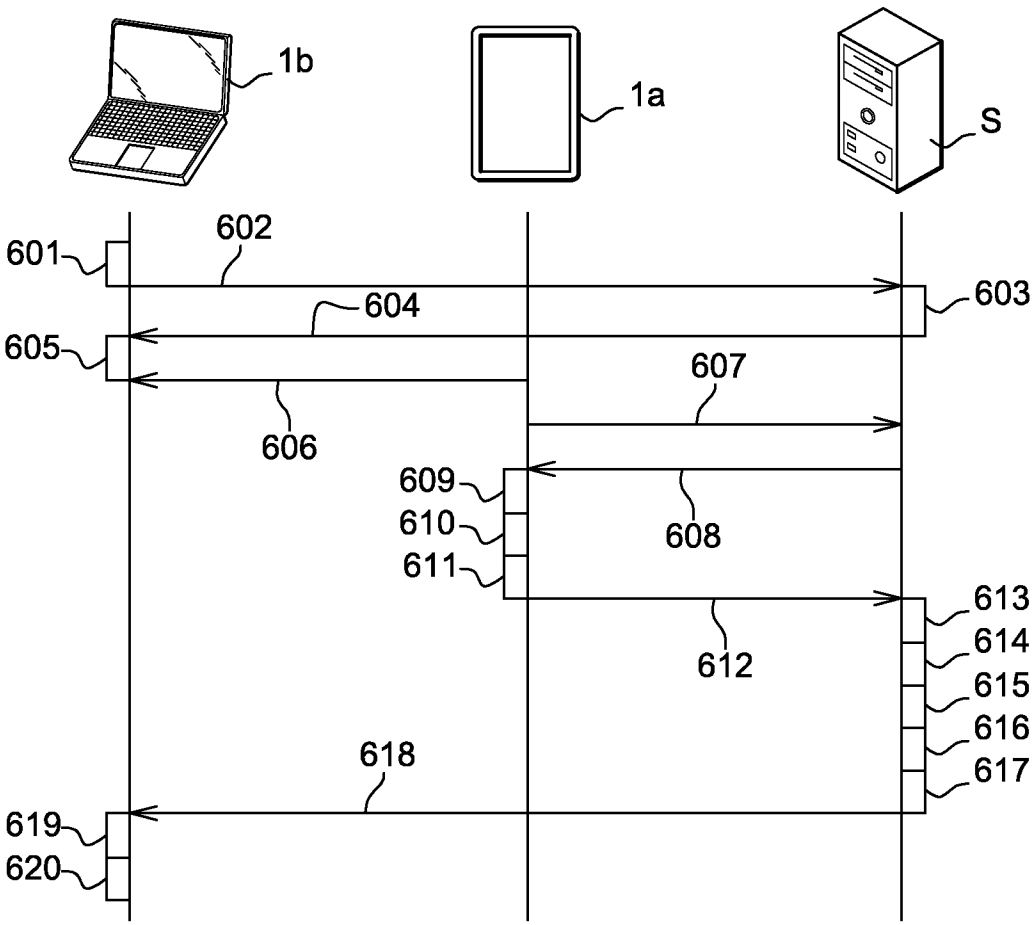

1b
1a
S
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620

Fig. 12

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/050694

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F21/40
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)
H04L G06F

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/036462 A1 (KRISHNAMURTHI GOVINDARAJAN [US]) 7 February 2013 (2013-02-07) abstract; figure 1 paragraph [0006] - paragraph [0007] paragraph [0015] - paragraph [0017] paragraph [0019] - paragraph [0029] paragraph [0038] paragraph [0040] - paragraph [0043] paragraph [0045] paragraph [0048] - paragraph [0049] paragraph [0057] paragraph [0062] - paragraph [0067] paragraph [0070] - paragraph [0071] ----- -/--	1-13

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2017	06/07/2017

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

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/050694

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/262873 A1 (READ DAVID MCARTHUR [US] ET AL) 3 October 2013 (2013-10-03) abstract; figures 1,2b paragraph [0002] paragraph [0019] paragraph [0023] - paragraph [0026] paragraph [0032] - paragraph [0033] paragraph [0076] -----	1-13
A	US 2015/281279 A1 (SMITH NED M [US] ET AL) 1 October 2015 (2015-10-01) figure 1 paragraph [0011] -----	1-13

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2017/050694

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013036462 A1	07-02-2013	CN 103814380 A	21-05-2014
		EP 2740065 A1	11-06-2014
		JP 6140788 B2	31-05-2017
		JP 2014526105 A	02-10-2014
		JP 2015144026 A	06-08-2015
		JP 2016042376 A	31-03-2016
		KR 20140054172 A	08-05-2014
		KR 20170044769 A	25-04-2017
		US 2013036462 A1	07-02-2013
		WO 2013019880 A1	07-02-2013
US 2013262873 A1	03-10-2013	NONE	
US 2015281279 A1	01-10-2015	CN 106063189 A	26-10-2016
		EP 3123661 A1	01-02-2017
		KR 20160113247 A	28-09-2016
		US 2015281279 A1	01-10-2015
		WO 2015148023 A1	01-10-2015

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2017/050694

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06 G06F21/40
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 G06F

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

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

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 2013/036462 A1 (KRISHNAMURTHI GOVINDARAJAN [US]) 7 février 2013 (2013-02-07) abrégé; figure 1 alinéa [0006] - alinéa [0007] alinéa [0015] - alinéa [0017] alinéa [0019] - alinéa [0029] alinéa [0038] alinéa [0040] - alinéa [0043] alinéa [0045] alinéa [0048] - alinéa [0049] alinéa [0057] alinéa [0062] - alinéa [0067] alinéa [0070] - alinéa [0071] ----- -/--	1-13

[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
28 juin 2017	06/07/2017

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

1

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2013/262873 A1 (READ DAVID MCARTHUR [US] ET AL) 3 octobre 2013 (2013-10-03) abrégé; figures 1,2b alinéa [0002] alinéa [0019] alinéa [0023] - alinéa [0026] alinéa [0032] - alinéa [0033] alinéa [0076] -----	1-13
A	US 2015/281279 A1 (SMITH NED M [US] ET AL) 1 octobre 2015 (2015-10-01) figure 1 alinéa [0011] -----	1-13

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2017/050694

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2013036462 A1	07-02-2013	CN 103814380 A	21-05-2014
		EP 2740065 A1	11-06-2014
		JP 6140788 B2	31-05-2017
		JP 2014526105 A	02-10-2014
		JP 2015144026 A	06-08-2015
		JP 2016042376 A	31-03-2016
		KR 20140054172 A	08-05-2014
		KR 20170044769 A	25-04-2017
		US 2013036462 A1	07-02-2013
		WO 2013019880 A1	07-02-2013
US 2013262873 A1	03-10-2013	AUCUN	
US 2015281279 A1	01-10-2015	CN 106063189 A	26-10-2016
		EP 3123661 A1	01-02-2017
		KR 20160113247 A	28-09-2016
		US 2015281279 A1	01-10-2015
		WO 2015148023 A1	01-10-2015