(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 106 949***

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

(21) **N° d'enregistrement national :** **20 00912**

(51) Int Cl[8] : ***H 04 W 12/06*** *(2019.12), G 06 F 21/45*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 30.01.20.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 06.08.21 Bulletin 21/31.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *ORANGE Société anonyme* — FR.

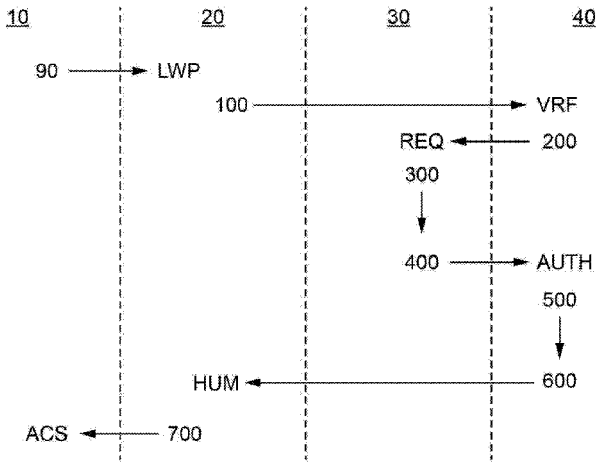
(72) **Inventeur(s) :** KIRSCHBAUM Patrick et GASPAR Sylvie.

(73) **Titulaire(s) :** ORANGE Société anonyme.

(74) **Mandataire(s) :** Plasseraud IP.

(54) Procédé de vérification du caractère humain d'un utilisateur pour l'accès à un service.

(57) L'invention propose un procédé de vérification du caractère humain d'un utilisateur pour l'accès à un service (20) depuis un terminal d'accès (10), le procédé étant mis en œuvre par une entité de vérification (40) et comprenant : - l'émission (200), à réception d' une demande de vérification (VRF) du caractère humain d'un utilisateur émise par le service (20), d'une requête (REQ) d'authentification de l'utilisateur auprès d'un terminal d'authentification (30), la requête d'authentification (REQ) commandant une authentification de l'utilisateur par le terminal d'authentification;- l'obtention (400), en réponse à la requête d'authentification (REQ), d'une confirmation d'authentification (AUTH) de l'utilisateur auprès du terminal d'authentification (30), et- l'émission (600), auprès du service (20), d'une confirmation (HUM) du caractère humain de l'utilisateur.Figure 2



FR 3 106 949 - A1

Description

Titre de l'invention : Procédé de vérification du caractère humain d'un utilisateur pour l'accès à un service

Domaine technique

[0001] L'invention concerne un procédé de vérification du caractère humain d'un utilisateur pour l'accès à un service. Elle trouve une application intéressante dans la sécurisation de l'accès à des services distants.

Technique antérieure

[0002] Il est connu pour certains services sur Internet, notamment pour l'accès à des sites internet, de vérifier le caractère humain d'un utilisateur souhaitant accéder au service, afin de différencier un utilisateur humain d'un éventuel robot. Pour cette vérification, des tests appelés CAPTCHA, acronyme de l'anglais « Completely Automated Public Turing test to tell Computers and Humans Apart », sont habituellement utilisés.

[0003] Ces tels consistent à soumettre l'utilisateur souhaitant accéder au service à un exercice qui est censé être simple à résoudre pour un humain, mais complexe voire impossible par un robot. Il s'agit par exemple de recopier un texte court affiché sur l'écran et parfois déformé ou barré, ou bien saisir le résultat d'un calcul simple, ou encore analyser des images affichées sur l'écran, par exemple pour sélectionner celles représentant un objet particulier.

[0004] La limite de l'utilisation des CAPTCHAS actuel est qu'elle peut pénaliser les utilisateurs, car parfois le texte à recopier est très déformé et illisible, ou encore le test proposé n'est pas adapté à des personnes handicapées, par exemple des personnes présentant une déficience visuelle.

[0005] Par ailleurs, l'efficacité de certains CAPTCHAS est de plus en plus limitée du fait d'algorithmes d'attaque de plus en plus puissants, permettant par exemple de déchiffrer des textes très déformés. D'autres méthodes d'attaque des CAPTCHAS existent, comme des méthodes consistant à tester toutes les combinaisons possibles de caractères, ou des méthodes consistant à tester des séries de textes potentiels, ces méthodes étant éventuellement facilitées par la reconnaissance partielle de certains caractères affichés par le CAPTCHA.

Résumé

[0006] Compte-tenu de ce qui précède, un but de l'invention est de proposer une solution améliorée pour sécuriser l'accès à un service.

[0007] Un autre but de l'invention est de proposer un procédé de vérification du caractère humain d'un utilisateur qui soit à la fois robuste et simple à utiliser pour un utilisateur.

[0008] A cet égard l'invention a pour objet un procédé de vérification du caractère humain

d'un utilisateur pour l'accès à un service depuis un terminal d'accès, le procédé étant mis en œuvre par une entité de vérification et comprenant :

- l'émission, à réception d' une demande de vérification du caractère humain d'un utilisateur émise par le service, d'une requête d'authentification de l'utilisateur auprès d'un terminal d'authentification, la requête d'authentification commandant une authentification de l'utilisateur par le terminal d'authentification;
- l'obtention, en réponse à la requête d'authentification, d'une confirmation d'authentification de l'utilisateur auprès du terminal d'authentification, et
- l'émission, auprès du service, d'une confirmation du caractère humain de l'utilisateur.

[0009] Dans un mode de réalisation, la demande de vérification du caractère humain de l'utilisateur comprend un identifiant du service auquel l'utilisateur souhaite accéder.

[0010] Dans un mode de réalisation, le procédé comprend en outre une vérification, à réception de la confirmation d'authentification de l'utilisateur auprès du terminal d'authentification, du fait que le terminal d'authentification dont provient la confirmation d'authentification correspond à celui auprès de qui la requête d'authentification a été émise,

une vérification positive déclenchant l'émission auprès du service de la confirmation du caractère humain de l'utilisateur.

[0011] Dans un mode de réalisation, la confirmation d'authentification de l'utilisateur auprès du terminal d'authentification comprend un identifiant du terminal d'authentification. Dans ce cas, la vérification peut être mise en œuvre par comparaison de l'identifiant du terminal d'authentification avec au moins un identifiant de terminal d'authentification autorisé.

[0012] Dans un mode de réalisation, la demande de vérification du caractère humain émise par le service comprend un identifiant du terminal d'authentification.

[0013] Dans un mode de réalisation, l'entité de vérification comprend une mémoire stockant une liste d'utilisateurs et pour chaque utilisateur, un identifiant d'au moins un terminal d'authentification associé, la demande de vérification du caractère humain émise par le service comprend un identifiant de l'utilisateur souhaitant accéder au service, et l'entité de vérification détermine, à partir de l'identifiant de l'utilisateur, au moins un identifiant de terminal d'authentification pour l'émission de la requête d'authentification.

[0014] La présente a également pour objet une entité de vérification du caractère humain d'un utilisateur pour l'accès à un service comprenant :

- un générateur d'une requête d'authentification d'un utilisateur auprès d'un terminal d'authentification, la requête étant apte à être émise auprès d'un terminal d'authentification à réception d'une demande de vérification du caractère humain d'un

utilisateur émise par un service, et commandant une authentification de l'utilisateur par le terminal d'authentification, et

- un générateur de signal de confirmation du caractère humain d'un utilisateur, apte à générer un signal de confirmation du caractère humain de l'utilisateur auprès du service considéré si le terminal d'authentification a authentifié l'utilisateur.

[0015] L'entité de vérification du caractère humain d'un utilisateur peut être implémentée dans un équipement distant du terminal d'accès et du terminal d'authentification du réseau de communication, ou être une application logicielle mise en œuvre par le terminal d'authentification.

[0016] La présente a également pour objet un procédé d'authentification d'un utilisateur pour l'accès à un site web, le procédé étant mis en œuvre par un terminal d'authentification, et comprenant, sur réception d'une requête d'authentification provenant d'une entité de vérification, la fourniture à ladite entité d'un signal de confirmation d'authentification déclenchant, par ladite entité, l'émission auprès du service, d'une confirmation du caractère humain de l'utilisateur.

[0017] Dans un mode de réalisation, le procédé d'authentification comprend en outre :

- sur réception de la requête d'authentification provenant de l'entité de vérification, la capture d'une donnée d'authentification d'un utilisateur du terminal d'authentification,
- la comparaison de la donnée d'authentification captée avec une donnée de référence pré-enregistrée,
- en cas de correspondance entre la donnée d'authentification et la donnée de référence, la fourniture du signal de confirmation d'authentification de l'utilisateur.

[0018] Dans un mode de réalisation, la capture met en œuvre l'un de :

- une capture de l'empreinte digitale de l'utilisateur, et/ou
- une saisie d'un code personnel de l'utilisateur.

[0019] La présente a également pour objet un terminal d'authentification apte à authentifier un utilisateur pour l'accès à un service, le terminal d'authentification comprenant :

- un fournisseur de signal de confirmation d'authentification de l'utilisateur, sur réception d'une requête d'authentification provenant d'une entité de vérification du caractère humain de l'utilisateur, le signal de confirmation d'authentification étant apte à déclencher une émission auprès du service, par ladite entité de vérification, d'une confirmation (HUM) du caractère humain de l'utilisateur.

[0020] Dans un mode de réalisation, le terminal d'authentification comprend en outre :

- un récepteur d'une requête d'authentification provenant de l'entité de vérification, et
- un certificateur de l'identité de l'utilisateur, le certificateur étant apte à déclencher le fournisseur de signal de confirmation d'authentification si l'utilisateur est authentifié.

[0021] La présente a également pour objet un produit programme d'ordinateur, comprenant des instructions de code pour la mise en œuvre du procédé de vérification, et/ou du procédé d'authentification selon les descriptions qui précèdent, lorsqu'il est exécuté par un calculateur.

[0022] La présente a également un système d'accès à un service, comprenant un terminal d'accès à un service, une entité de vérification du caractère humain d'un utilisateur, et un terminal d'authentification selon les descriptions qui précèdent.

[0023] Un générateur d'une requête d'authentification peut être un module logiciel de l'entité de vérification. Un générateur de signal de confirmation peut être une interface de communication avec un service, éventuellement sécurisée.

[0024] Un fournisseur de signal d'authentification peut comprendre une application logicielle implémentée sur le terminal d'authentification et configurée pour communiquer avec l'entité de vérification.

[0025] Le procédé proposé permet de vérifier le caractère humain d'un utilisateur pour l'accès à un service, sans utiliser de CAPTCHA. A la place, l'utilisateur est invité à s'authentifier auprès d'un terminal d'utilisation, cette authentification confirmant le caractère humain auprès du service et permettant à l'utilisateur d'accéder à ce service.

[0026] La mise en œuvre de cette vérification est donc à la fois simplifiée pour l'utilisateur, mais elle est présente également une sécurité accrue.

Brève description des dessins

[0027] D'autres caractéristiques, détails et avantages apparaîtront à la lecture de la description détaillée ci-après, et à l'analyse des dessins annexés, sur lesquels :

Fig. 1a

[0028] [fig.1a] représente un système vérification du caractère humain d'un utilisateur selon un premier mode de réalisation.

Fig. 1b

[0029] [fig.1b] représente un système de vérification du caractère humain d'un utilisateur selon un deuxième mode de réalisation.

Fig. 2

[0030] [fig.2] représente un exemple de mise en œuvre d'un procédé de vérification du caractère humain d'un utilisateur.

Description des modes de réalisation

[0031] Un procédé de vérification du caractère humain d'un utilisateur pour accéder à un service sera décrit ci-après en référence à la figure 2. Ce procédé est mis en œuvre dans un environnement dont plusieurs exemples sont représentés schématiquement dans les figures 1a et 1b.

[0032] En référence à ces figures, le procédé de vérification du caractère humain d'un uti-

lisateur est mis en œuvre dans un système 1 comprenant un terminal 10 d'accès à un service. Le terminal d'accès 10 peut être par exemple un ordinateur personnel (« PC ») fixe ou mobile. Il peut également s'agir d'une tablette numérique, ou encore d'un téléphone mobile.

[0033] Le terminal d'accès 10 comporte un fournisseur d'accès 11 à un service dont l'accès est sécurisé par une vérification du caractère humain de l'utilisateur souhaitant y accéder. Le fournisseur d'accès peut être un navigateur web. Le service auquel l'utilisateur souhaite accéder peut être un service hébergé sur un serveur distant 20 auquel il peut être accéder par un réseau de communications. Par exemple, le service peut être un site web, auquel l'utilisateur peut accéder soit directement par saisie, dans le navigateur web, de l'adresse url du site web, soit par un lien depuis un autre site web ou un moteur de recherche. La vérification du caractère humain de l'utilisateur peut être requise soit par le site web de destination, soit par le moteur de recherche, le cas échéant.

[0034] Le système 1 comprend également un terminal 30 d'authentification. Le terminal 30 d'authentification est apte à authentifier un utilisateur pour permettre de confirmer au service le caractère humain de l'utilisateur, et donc permettre à l'utilisateur l'accès au service depuis le terminal 10 d'accès. A cet égard, le terminal 30 d'authentification peut être distinct du terminal d'accès 10. Dans un mode de réalisation, le terminal 30 d'authentification est un téléphone mobile. En variante, le terminal d'accès 10 et le terminal d'authentification 30 sont un même terminal, par exemple un téléphone mobile.

[0035] Le terminal d'accès 10 et le terminal 30 d'authentification sont deux terminaux de communication d'un réseau de communication 2 local ou distant. Le terminal d'accès peut être connecté au réseau de communication par l'intermédiaire d'un réseau d'accès, par exemple filaire ou sans fil. Le terminal d'authentification peut être connecté au réseau de communication par l'intermédiaire d'un réseau d'accès sans fil, tel qu'un réseau mobile GSM, UMTS, LTE, 3G, 4G, 5G, etc.

[0036] Dans un mode de réalisation, la mise en œuvre du procédé peut être conditionnée à une co-localisation des deux terminaux 10, 30 à une même adresse, auquel cas les terminaux peuvent comprendre un dispositif de localisation tel qu'un récepteur GNSS ou un émetteur/récepteur Bluetooth pour l'établissement d'un lien Bluetooth entre les deux terminaux.

[0037] Le système 1 comprend également une entité 40 de vérification du caractère humain d'un utilisateur.

[0038] L'entité 40 de vérification peut être implémentée dans le terminal d'authentification 30, comme dans l'exemple représenté sur la figure 1a. L'entité 40 de vérification peut être une application logicielle installée sur le terminal 30 d'authentification.

[0039] En variante, l'entité 40 de vérification peut être implémentée dans un équipement du réseau de communication distinct des terminaux 10, 30, par exemple un serveur distant, comme représenté dans l'exemple de la figure 1b.

[0040] Le procédé de vérification du caractère humain d'un utilisateur mis en œuvre par l'entité de vérification 40, et décrit plus en détails ci-après, peut être rendu accessible au moyen d'une interface de programmation applicative ou API utilisée par le service (site web ou moteur de recherche par exemple). Dans ce cas, le terminal d'accès 10 peut comprendre un module d'extension pour son navigateur web, permettant à un utilisateur de saisir un identifiant utilisateur ou un identifiant de contact de terminal d'authentification, que ce soit pour enregistrer cet identifiant pour toutes les mises en œuvre futures du procédé de vérification, ou à chaque mise en œuvre de ce procédé. Le module d'extension peut être installé au moyen d'une application logicielle implémentée par le terminal d'accès 10.

[0041] Dans le cas où l'entité 40 de vérification est implémentée sur un équipement distinct des terminaux 10, 30, elle peut comprendre une mémoire stockant un ensemble d'identifiants d'utilisateurs, et pour chaque utilisateur au moins un terminal d'authentification associé, qui est un terminal d'authentification autorisé pour mettre en œuvre une authentification dans le contexte du procédé de vérification décrit ci-après. Chaque terminal d'authentification peut être identifié par un identifiant permettant de contacter le terminal. Par exemple, si le terminal d'authentification est un téléphone mobile, l'identifiant peut être un numéro de téléphone, par exemple un numéro IMSI ou MSISDN.

[0042] Pour la mise en œuvre du procédé décrit ci-après, le terminal d'authentification 30 faire partie des terminaux d'authentification autorisés stockés, le cas échéant, dans la mémoire de l'entité 40 de vérification.

[0043] En variante, l'entité de vérification 40 ne comprend aucun identifiant de terminal d'authentification autorisé en mémoire, mais reçoit celui-ci du service, comme décrit plus en détails ci-après.

[0044] En référence à la figure 2 on a représenté schématiquement un exemple de mise en œuvre de l'accès d'un utilisateur à un service.

[0045] Lorsqu'un utilisateur souhaite accéder à un service par le terminal d'accès 10, en utilisant par exemple un navigateur web installé sur le terminal d'accès 10, et que le service conditionne l'accès par l'utilisateur à une vérification du caractère humain de celui-ci, un procédé de vérification du caractère humain de l'utilisateur est mis en œuvre. Sur la figure 2, on a représenté par une étape 90 une requête de chargement d'une page web LWP envoyée par le navigateur du terminal d'accès 10 au serveur hébergeant le service 20. Cette requête comprend ou est accompagnée d'un identifiant de terminal d'authentification fourni par le module complémentaire du navigateur, ou

éventuellement un identifiant d'utilisateur. Comme indiqué précédemment, l'utilisateur peut avoir saisi un identifiant dans le navigateur au moment de l'accès au service, ou le module complémentaire du navigateur peut fournir un identifiant pré-enregistré par l'utilisateur.

[0046] Le procédé comprend ensuite la réception 100, par l'entité 40 de vérification, d'une demande de vérification VRF du caractère humain de l'utilisateur émise par le service. Dans le mode de réalisation dans lequel le service utilise une interface de programmation dédiée pour cette vérification, l'interface de programmation peut afficher un bouton apparent dans le navigateur et actionnable par l'utilisateur, et qui commande l'envoi de la demande de vérification VRF à l'entité 40.

[0047] Dans un mode de réalisation, l'entité de vérification 40 est implémentée dans le terminal d'authentification 40, et la demande de vérification VRF est envoyée à l'entité de vérification au moyen d'un identifiant de contact du terminal d'authentification.

[0048] Dans un autre mode de réalisation, l'entité de vérification 40 est implémentée dans un équipement distinct des terminaux 10, 30, et peut donc être commune à plusieurs terminaux d'authentification. Dans ce cas, la demande de vérification VRF peut comprendre un identifiant de contact d'un terminal d'authentification. En variante, si l'entité de vérification comprend en mémoire des identifiants d'utilisateur et des identifiants de terminaux d'authentification associés, la demande de vérification VRF peut comprendre un identifiant de l'utilisateur et l'entité de vérification 40 est configurée pour déterminer un identifiant de contact de terminal d'authentification à partir de l'identifiant d'utilisateur reçu.

[0049] La demande de vérification VRF peut également comprendre un identifiant du service duquel émane la demande, par exemple une adresse IP du service, et auquel l'utilisateur souhaite accéder.

[0050] Lors d'une étape 200, l'entité émet, en réaction à la réception de la demande VRF, une requête REQ d'authentification de l'utilisateur auprès d'un terminal d'authentification 30, la requête commandant une authentification de l'utilisateur par le terminal d'authentification. L'utilisateur du terminal d'accès 10 souhaitant accéder au service peut être le même que l'utilisateur s'authentifiant auprès du terminal d'authentification 30. En variante, l'utilisateur du terminal d'accès 10 peut être différent de celui du terminal d'authentification.

[0051] La requête d'authentification peut être envoyée au deuxième terminal par SMS. En variante, le terminal d'authentification peut exécuter une application hébergée sur un équipement du réseau de communication, et la requête est envoyée au terminal d'authentification via l'application qui y est exécutée.

[0052] La requête REQ peut comprendre un identifiant du service auquel l'utilisateur veut accéder depuis le terminal d'accès 10, comme par exemple une adresse IP du service.

[0053] Le procédé comprend ensuite la mise en œuvre d'un procédé d'authentification 300 de l'utilisateur par le terminal d'authentification 20 à réception de la requête d'authentification REQ provenant du premier terminal.

[0054] Pour la mise en œuvre de l'authentification, le terminal d'authentification 30 capture une donnée d'authentification de l'utilisateur. La donnée d'authentification peut être un code personnel ou un mot de passe saisi sur un clavier d'une interface du terminal 30 tel qu'un écran tactile. Il peut s'agir également d'une capture d'une empreinte digitale acquise par un capteur dédié, ou encore une photographie d'un œil ou du visage de l'utilisateur. Il peut encore s'agir d'une signature manuscrite acquise au moyen d'un stylet ou d'un doigt de l'utilisateur sur une interface tactile comme l'écran tactile, ou encore une capture audio d'une empreinte vocale de l'utilisateur, ou une capture audio d'un code prononcé par l'utilisateur, etc. A cet égard, le terminal d'authentification comporte au moins une interface 31 de capture de la donnée d'authentification, pouvant être un capteur d'empreinte digitale, un appareil photo, un écran tactile, un microphone, etc.

[0055] Une fois la donnée d'authentification acquise, elle est ensuite comparée à une donnée de référence de même nature pré-enregistrée, par exemple dans une mémoire du terminal d'authentification 30. En cas de correspondance entre la donnée d'authentification et la donnée de référence, le terminal 30 génère un signal AUTH de confirmation d'authentification.

[0056] Ce signal AUTH est fourni lors d'une étape 400 à l'entité de vérification pour déclencher l'émission, par ladite entité 40, auprès du service, d'une confirmation HUM du caractère humain de l'utilisateur souhaitant accéder au service par le terminal d'accès 10.

[0057] Dans un mode de réalisation, le signal AUTH comprend au moins l'un d'un identifiant du terminal d'authentification 30, par exemple le numéro MSISDN ou le numéro IMSI, et d'un identifiant du service auquel le terminal d'accès 10 cherche à accéder.

[0058] A réception du signal AUTH de confirmation d'authentification de l'utilisateur, l'entité 40 de validation émet 600 auprès du service 20, en réponse à la requête d'authentification REQ, une confirmation HUM du caractère humain de l'utilisateur si le terminal d'authentification a authentifié l'utilisateur. Pour ce faire, l'entité 40 de vérification peut vérifier au cours d'une étape 500 l'existence d'une correspondance entre l'identifiant du terminal d'authentification 30 reçu dans le signal AUTH l'identifiant du terminal d'authentification auquel la requête d'authentification REQ a été envoyée.

[0059] Le fait de vérifier que le terminal d'authentification dont provient la confirmation d'authentification est celui auquel la requête d'authentification REQ a été envoyée permet de sécuriser l'accès au service.

[0060] La réception par le service de la confirmation HUM du caractère humain de l'utilisateur, déclenche enfin lors d'une étape 700 l'autorisation ACS de l'utilisateur à accéder au service depuis le terminal d'accès 10.

Revendications

[Revendication 1] Procédé de vérification du caractère humain d'un utilisateur pour l'accès à un service (20) depuis un terminal d'accès (10), le procédé étant mis en œuvre par une entité de vérification (40) et comprenant :
- l'émission (200), à réception d' une demande de vérification (VRF) du caractère humain d'un utilisateur émise par le service (20), d'une requête (REQ) d'authentification de l'utilisateur auprès d'un terminal d'authentification (30), la requête d'authentification (REQ) commandant une authentification de l'utilisateur par le terminal d'authentification;
- l'obtention (400), en réponse à la requête d'authentification (REQ), d'une confirmation d'authentification (AUTH) de l'utilisateur auprès du terminal d'authentification (30), et
- l'émission (600), auprès du service (20), d'une confirmation (HUM) du caractère humain de l'utilisateur.

[Revendication 2] Procédé selon la revendication 1, dans lequel la demande de vérification (VRF) du caractère humain de l'utilisateur comprend un identifiant du service auquel l'utilisateur souhaite accéder.

[Revendication 3] Procédé selon l'une des revendications 1 ou 2, comprenant en outre une vérification (500), à réception de la confirmation d'authentification (AUTH) de l'utilisateur auprès du terminal d'authentification (30), du fait que le terminal d'authentification (30) dont provient la confirmation d'authentification correspond à celui auprès de qui la requête d'authentification (REQ) a été émise,
une vérification positive déclenchant l'émission (600) auprès du service (20) de la confirmation du caractère humain de l'utilisateur.

[Revendication 4] Procédé selon l'une des revendications précédentes, dans lequel la confirmation d'authentification (AUTH) de l'utilisateur auprès du terminal d'authentification (30) comprend un identifiant du terminal d'authentification.

[Revendication 5] Procédé selon l'une des revendications précédentes, dans lequel la demande de vérification (VRF) du caractère humain émise par le service comprend un identifiant du terminal d'authentification.

[Revendication 6] Procédé selon l'une des revendications précédentes, dans lequel l'entité de vérification (40) comprend une mémoire (41) stockant une liste d'utilisateurs et pour chaque utilisateur, un identifiant d'au moins un terminal d'authentification (30) associé, la demande de vérification

(VRF) du caractère humain émise par le service (20) comprend un identifiant de l'utilisateur souhaitant accéder au service, et l'entité de vérification détermine, à partir de l'identifiant de l'utilisateur, au moins un identifiant de terminal d'authentification pour l'émission de la requête d'authentification.

[Revendication 7] Entité de vérification (40) du caractère humain d'un utilisateur pour l'accès à un service comprenant :
- un générateur d'une requête (REQ) d'authentification d'un utilisateur auprès d'un terminal d'authentification (30), la requête étant apte à être émise auprès d'un terminal d'authentification (30) à réception d'une demande de vérification (VRF) du caractère humain d'un utilisateur émise par un service, et commandant une authentification de l'utilisateur par le terminal d'authentification,
- un générateur de signal de confirmation (HUM) du caractère humain d'un utilisateur, apte à générer un signal de confirmation du caractère humain de l'utilisateur auprès du service considéré si le terminal d'authentification a authentifié l'utilisateur.

[Revendication 8] Entité (40) selon la revendication 6, dans laquelle l'entité est implémentée dans un équipement distant du terminal d'accès (10) et du terminal d'authentification (30) du réseau de communication, ou est une application logicielle mise en œuvre par le terminal d'authentification.

[Revendication 9] Procédé d'authentification d'un utilisateur pour l'accès à un site web, le procédé étant mis en œuvre par un terminal d'authentification (30), et comprenant, sur réception d'une requête d'authentification (REQ) provenant d'une entité de vérification (40), la fourniture à ladite entité d'un signal de confirmation d'authentification (AUTH) déclenchant, par ladite entité, l'émission auprès du service, d'une confirmation du caractère humain de l'utilisateur.

[Revendication 10] Procédé d'authentification selon la revendication précédente, dans lequel le procédé comprend en outre :
- sur réception de la requête d'authentification (REQ) provenant de l'entité de vérification, la capture d'une donnée d'authentification d'un utilisateur du terminal d'authentification,
- la comparaison de la donnée d'authentification captée avec une donnée de référence pré-enregistrée,
- en cas de correspondance entre la donnée d'authentification et la donnée de référence, la fourniture (400) du signal de confirmation d'authentification (AUTH) de l'utilisateur.

[Revendication 11] Procédé d'authentification selon la revendication précédente, dans lequel la capture met en œuvre l'un de :
- une capture de l'empreinte digitale de l'utilisateur, et/ou
- une saisie d'un code personnel de l'utilisateur.

[Revendication 12] Terminal d'authentification (30) apte à authentifier un utilisateur pour l'accès à un service, le terminal d'authentification comprenant :
- un fournisseur de signal de confirmation d'authentification (AUTH) de l'utilisateur, sur réception d'une requête d'authentification provenant d'une entité de vérification du caractère humain de l'utilisateur, le signal de confirmation d'authentification étant apte à déclencher une émission auprès du service, par ladite entité de vérification, d'une confirmation (HUM) du caractère humain de l'utilisateur.

[Revendication 13] Terminal d'authentification (30) selon la revendication précédente, dans lequel le terminal d'authentification (30) comprend :
- un récepteur d'une requête d'authentification (REQ) provenant de l'entité de vérification (40),
- un certificateur de l'identité de l'utilisateur, le certificateur étant apte à déclencher le fournisseur de signal de confirmation d'authentification si l'utilisateur est authentifié.

[Revendication 14] Produit programme d'ordinateur, comprenant des instructions de code pour la mise en œuvre du procédé de vérification selon l'une quelconque des revendications 1 à 5, et/ou du procédé d'authentification selon l'une des revendications 8 à 10, lorsqu'il est exécuté par un calculateur.

[Revendication 15] Système d'accès à un service, comprenant un terminal d'accès (10) à un service, une entité (40) de vérification du caractère humain d'un utilisateur selon l'une des revendications 8 à 9, et un terminal (30) d'authentification selon l'une des revendications 13 ou 14.

[Fig. 1a]

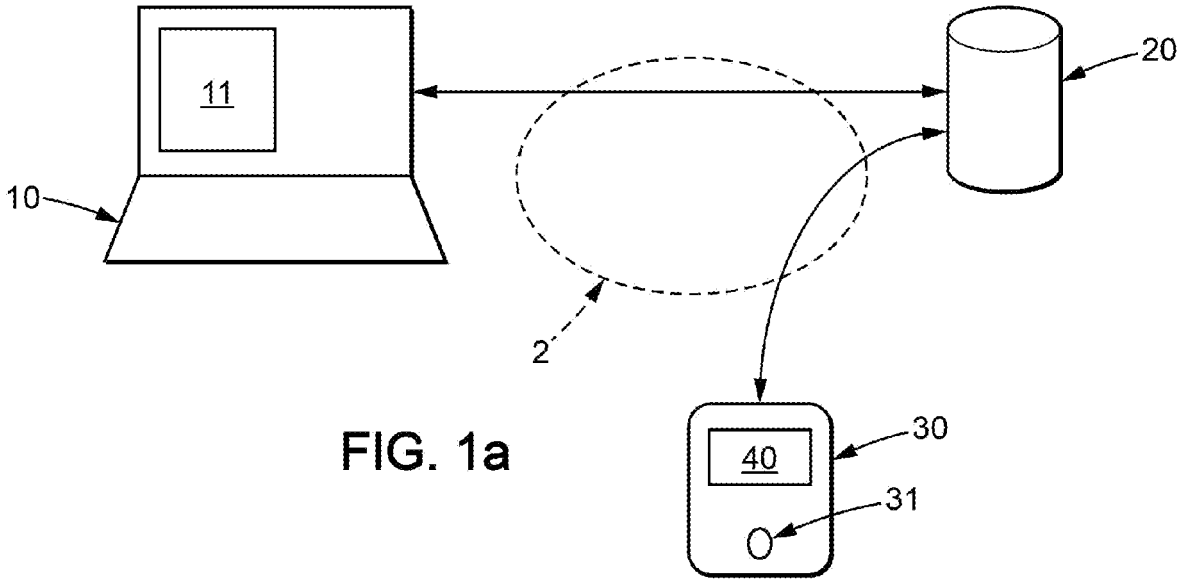


FIG. 1a

[Fig. 1b]

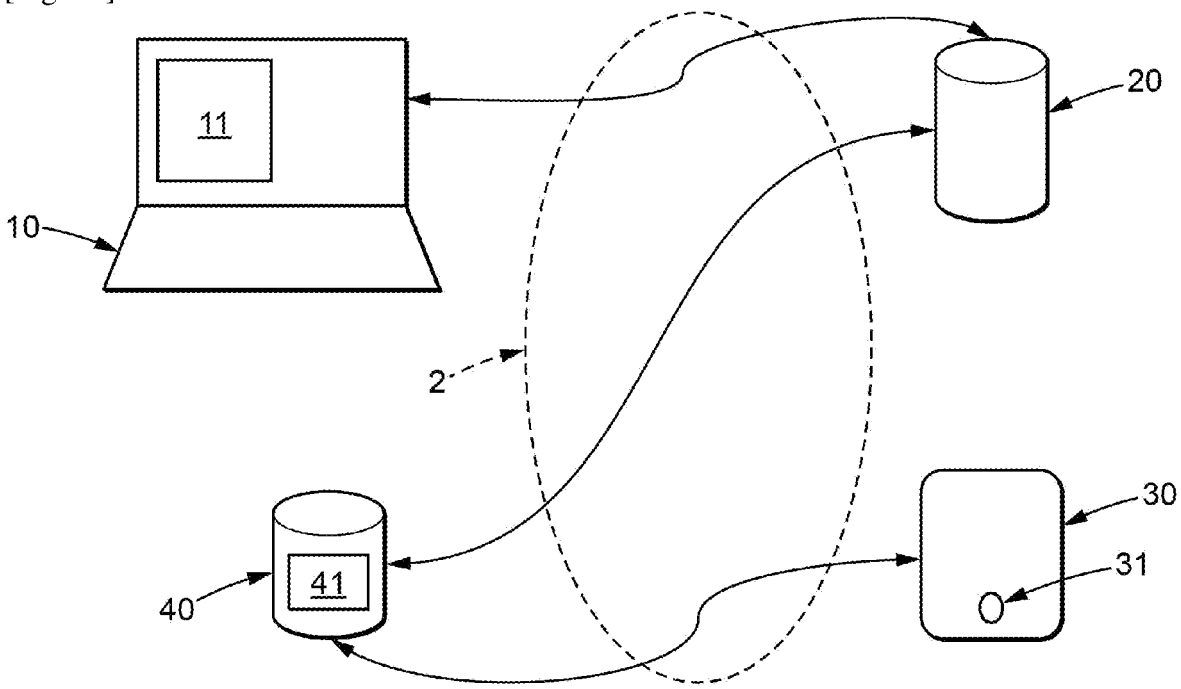


FIG. 1b

[Fig. 2]

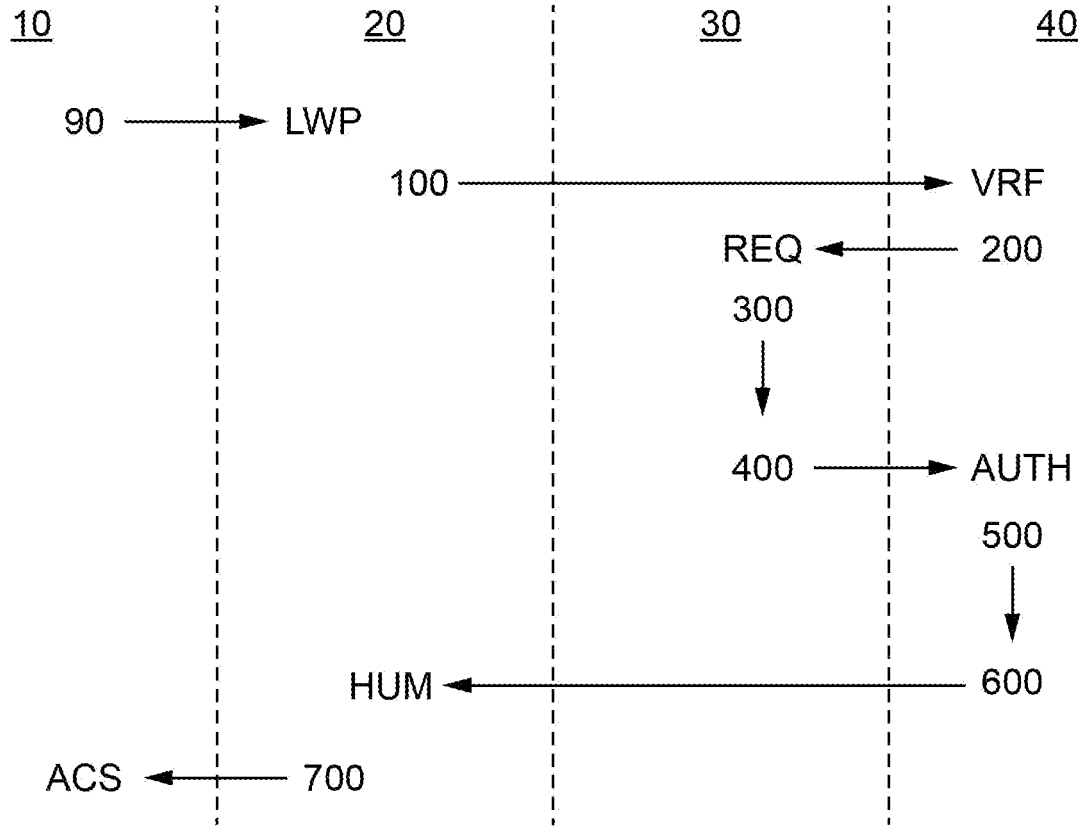

10
20
30
40
90
LWP
100
VRF
REQ
200
300
400
AUTH
500
HUM
600
ACS
700

FIG. 2

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 879099
FR 2000912

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 2015/165827 A1 (PREDICSIS [FR]) 5 novembre 2015 (2015-11-05) * page 3, ligne 7 - page 5, ligne 14 * * page 5, ligne 29 - page 7, ligne 3 * * revendication 1; figure 4 * * revendications 7,8; figure 1 * * page 10, ligne 10 - page 15, ligne 14 * -----	1-15	H04W12/06 G06F21/45
X	WO 2016/128645 A1 (ORANGE [FR]) 18 août 2016 (2016-08-18) * page 1, ligne 23 - page 2, ligne 21 * * page 5, ligne 19 - ligne 25 * * page 6, ligne 15 - ligne 23 * * page 9, ligne 24 - ligne 34; figure 3 * * page 6, ligne 24 - page 8, ligne 21; figure 2 * -----	1-15	
X	EP 2 819 052 A1 (ORANGE [FR]) 31 décembre 2014 (2014-12-31) * revendications 1,8,10,13; figures 1,4a, 4b * * alinéa [0013] - alinéa [0015] * * alinéas [0018], [0028], [0030], [0031] * -----	1-15	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L H04W G06F
A	US 2014/196133 A1 (SHUSTER GARY STEPHEN [US]) 10 juillet 2014 (2014-07-10) * alinéa [0006] * * alinéa [0030] - alinéa [0033]; figure 1 * * alinéa [0045] * -----	1-15	

Date d'achèvement de la recherche	Examinateur
22 septembre 2020	Losseau, Dominique

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2000912 FA 879099

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 22-09-2020
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2015165827 A1	05-11-2015	FR 3020696 A1	06-11-2015
		WO 2015165827 A1	05-11-2015
WO 2016128645 A1	18-08-2016	EP 3257224 A1	20-12-2017
		FR 3032847 A1	19-08-2016
		US 2018034809 A1	01-02-2018
		WO 2016128645 A1	18-08-2016
EP 2819052 A1	31-12-2014	EP 2819052 A1	31-12-2014
		FR 3007551 A1	26-12-2014
		US 2014380048 A1	25-12-2014
US 2014196133 A1	10-07-2014	US 2014196133 A1	10-07-2014
		US 2015180856 A1	25-06-2015
		US 2016112393 A1	21-04-2016
		US 2017026367 A1	26-01-2017
		US 2018124045 A1	03-05-2018
		WO 2014107618 A1	10-07-2014

EPO FORM P0465