(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 974 261**

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

(21) **N° d'enregistrement national :** **11 53324**

(51) Int Cl[8] : ***H 04 L 9/32*** *(2012.01), H 04 L 29/06, H 04 W 12/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 15.04.11.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 19.10.12 Bulletin 12/42.

(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 :**

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

(72) **Inventeur(s) :** GROULT REMI et RABOT WILFRID.

(73) **Titulaire(s) :** FRANCE TELECOM Société anonyme.

(74) **Mandataire(s) :** FRANCE TELECOM.

(54) PROCEDE D'OBTENTION DE DONNEES DE CONFIGURATION POUR L'ETABLISSEMENT D'UNE COMMUNICATION ENTRE DEUX TERMINAUX.

(57) L'invention a trait à un procédé d'établissement d'une connexion entre deux terminaux (TRM1,TRM2) aptes à communiquer au travers d'au moins deux moyens de communication dont un premier moyen de communication (RES1) nécessitant des données de configuration (DC). Le procédé est caractérisé en ce que les données de configuration nécessaires à la connexion des deux terminaux via le premier moyen de communication (RES1) sont communiquées par un premier terminal à un deuxième terminal via un deuxième moyen de communication sur lequel une communication entre les deux terminaux inclut une étape d'authentification des terminaux.

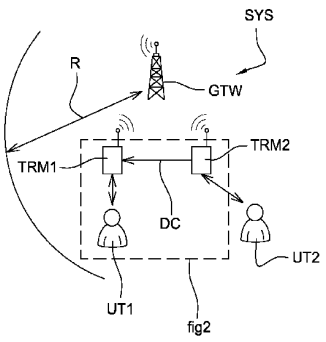

fig2

FR 2 974 261 - A1

Procédé d'obtention de données de configuration pour l'établissement d'une communication entre deux terminaux

Domaine technique

L'invention se rapporte à un procédé d'obtention de données de configuration pour l'établissement d'une communication entre deux terminaux au travers d'un moyen de communication tel qu'un réseau de télécommunication.

Les terminaux en question englobe tout dispositif de traitement de données, c'est-à-dire équipé de ressources physiques et/ou logicielles dont au moins un microprocesseur, apte à communiquer au travers d'au moins deux moyens de communication.

Etat de la technique

Généralement, une communication entre deux terminaux nécessite une étape préalable de configuration apte à garantir une légitimité des terminaux souhaitant communiquer entre eux.

Par exemple, si le moyen utilisé est un réseau WI-FI (contraction du terme anglais Wireless Fidelity, norme IEEE 802.11), l'étape de configuration correspond à une étape d'authentification mutuelle entre les deux terminaux qui a lieu avant que ces deux terminaux puissent communiquer entre eux. Cette étape d'authentification assure que deux terminaux communiquant ensembles sur un réseau WI-FI sont des terminaux légitimes.

Plusieurs types d'authentification mutuelle existent dont les suivantes.

Un premier type d'authentification consiste à inclure dans les terminaux des mécanismes de certificats signés par une autorité de certification reconnue par les différents terminaux. Grâce à ces certificats, deux terminaux peuvent communiquer entre eux en toute sécurité. Cette solution a l'inconvénient d'être complexe à déployer et à maintenir car elle nécessite une tiers de confiance à savoir une autorité de certification.

Un deuxième type d'authentification fait appel à un dispositif du réseau jouant un rôle de tiers de confiance sur lequel les deux terminaux sont connectés et authentifiés via un moyen de communication tel qu'un réseau de télécommunication. Le tiers de confiance établit une communication en créant un lien sécurisé entre les deux terminaux et en en certifiant que les deux terminaux sont des terminaux légitimes. Le problème est que cette solution est coûteuse car elle nécessite un tiers accessible au moment de la connexion.

L'invention vient améliorer la situation.

L'invention

A cet effet, selon un aspect fonctionnel, l'invention a pour objet un procédé d'établissement d'une connexion entre deux terminaux, un premier terminal et un deuxième terminal aptes à communiquer au travers d'au moins deux moyens de communication dont un premier moyen de communication nécessitant des données de configuration, caractérisé en ce que les données de configuration nécessaires à la connexion des deux terminaux via le premier moyen de communication sont communiquées par le premier terminal au deuxième terminal via un deuxième moyen de communication sur lequel une communication entre les deux terminaux inclut une étape d'authentification des terminaux.

Ainsi, selon l'invention, les données de configuration relatives au premier moyen sont transmises via un autre moyen de communication que le premier moyen de communication, ici le deuxième moyen, apte à assurer une légitimité des terminaux, par exemple par le biais d'une authentification mutuelle, avant une communication entre deux terminaux. L'invention évite ainsi une nouvelle phase de vérification de la légitimité des terminaux sur le premier moyen de communication. L'invention évite ainsi l'intervention d'un tiers de confiance sur le premier moyen de communication tout en assurant une légitimité des terminaux concernés sur ce premier moyen de communication.

Les deux terminaux en question sont aptes à être utilisés par un utilisateur respectif. Selon un premier mode de réalisation particulier, la

transmission des données de configuration est commandée suite à une action d'un utilisateur sur l'un des deux terminaux et en ce que l'action est réalisée par l'utilisateur lorsque les deux terminaux se situent dans le champ visuel d'au moins un utilisateur choisi parmi le premier ou le deuxième utilisateur. Au même titre que pour l'émission, la réception des données peuvent aussi est commandée suite à une action d'un utilisateur sur l'un des deux terminaux. Ainsi, un utilisateur a la maîtrise de l'instant de la transmission et/ou de la réception; de plus, l'utilisateur visualise la scène et est assuré que les terminaux impliqués dans une communication via ce deuxième moyen de communication sont des terminaux légitimes. Ce mode évite l'utilisation d'une autorité de certification ou d'un dispositif connecté au deuxième réseau jouant le rôle de tiers de confiance.

Selon un deuxième mode de réalisation pouvant être mis en œuvre cumulativement ou alternativement avec le premier mode, le deuxième moyen de communication est un moyen de communication d'une portée limitée en distance. La portée sera choisie judicieusement de telle sorte que la couverture du deuxième moyen se trouve dans le champ visuel d'un utilisateur. De cette façon, cette caractéristique évite qu'un troisième terminal supplémentaire situé dans la couverture en question, par exemple un champ électromagnétique, capture les données de configuration transmises depuis un premier vers un deuxième terminal, en particulier à des fins malveillantes.

Rappelons ici que la portée d'un moyen de communication correspond à la distance maximale en deçà de laquelle une communication est possible.

Selon une variante des deux modes qui précèdent, un terminal est équipé de moyens de prise de vue, un autre terminal est équipé d'un moyen de restitution d'une information représentative des données de configuration. Dans cette configuration, pour la communication des données de configuration via le deuxième moyen de connexion, les moyens de prise de vue capturent l'information. Par exemple, si les moyens de restitution sont un écran apte à afficher les données de configuration, et les moyens de capture sont un appareil photographique, ce dernier prend en photo les données de configuration affichées sur l'écran.

L'information en question peut être codée pour éviter qu'un troisième terminal malveillant n'utilise cette information à des fins malveillantes.

Selon un troisième mode de réalisation, qui pourra être mis en œuvre alternativement ou cumulativement avec les précédents, une donnée numérique créée par le deuxième terminal est ajoutée aux données de configuration lors de la communication des données de configuration au premier terminal, et en ce que la donnée numérique reçue par le premier terminal est transmise depuis le premier terminal vers le deuxième terminal via le premier moyen de communication. Nous verrons que cette donnée numérique, désignée par le terme "jeton" dans la description, aura une valeur apte à être modifiée dans le temps pour éviter un éventuel rejeu par un tiers malveillant.

Rappelons qu'une attaque par « rejeu » (en anglais « replay attaque ») est une attaque de type « Man in the middle » consistant à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quel (sans aucun déchiffrement) à un terminal destinataire.

Cette donnée numérique est par exemple différente à chaque communication de données de configuration depuis le deuxième vers le premier terminal. Ainsi, le deuxième terminal vérifie si le jeton qu'il a transmis au premier terminal via le deuxième moyen de communication et celui qu'il reçoit par la suite via le premier moyen de communication sont les mêmes ; dans l'affirmative, le premier terminal est authentifié sur le premier réseau, et ce sans qu'un tiers de confiance ne soit intervenu sur ce premier réseau.

Selon un aspect matériel, l'invention a trait aussi à un système informatique comprenant un premier terminal et un deuxième terminal aptes à communiquer au travers d'au moins deux moyens de communication dont un premier moyen de communication nécessitant des données de configuration, caractérisé en que le deuxième terminal comprend des moyens de transmission des données de configuration via un deuxième moyen de communication sur lequel une communication entre les deux terminaux inclut une étape d'authentification des terminaux, et en ce que le premier terminal comprend des

moyens de réception des données de configuration via ce deuxième moyen de communication.

On verra par la suite que le premier terminal comprend en outre des moyens de prise en compte des données de configuration reçus pour établir une communication via le premier réseau avec le deuxième terminal.

Selon un autre aspect matériel, l'invention a trait à un Terminal, dit deuxième terminal, apte à communiquer avec un autre terminal, dit premier terminal, via au moins deux moyens de communication dont un premier moyen de communication nécessitant des données de configuration, caractérisé en ce qu'il comprend des moyens de transmission des données de configuration via un deuxième moyen de communication sur lequel une communication entre deux terminaux inclut une étape d'authentification des terminaux.

Selon une variante, le deuxième terminal comprend des moyens de création d'une donnée numérique, dite première donnée numérique. Selon cette variante, la donnée numérique accompagne les données de configuration lors de la transmission des données de configuration. Le deuxième terminal comprend

- des moyens de réception d'une deuxième donnée numérique

- des moyens de comparaison aptes à comparer la première et la deuxième donnée

- des moyens aptes à conditionner une communication avec le premier terminal via le premier réseau en fonction du résultat de la comparaison.

Selon un autre aspect matériel, l'invention a trait à un terminal, dit premier terminal, apte à communiquer avec un autre terminal, dit deuxième terminal, au travers d'au moins deux moyens de communication dont un premier moyen de communication nécessitant des données de configuration, caractérisé en ce qu'il comprend des moyens de réception des données de configuration via un deuxième moyen de communication, et des moyens de prise en compte des données de configuration reçus pour établir une communication via le premier moyen de communication avec le deuxième terminal.

Selon un mode de réalisation particulier, en liaison avec le troisième mode de réalisation relatif au procédé, le premier terminal comprend des moyens de réception aptes à recevoir les données de configuration ainsi que la donnée numérique, et des moyens de transmission aptes à transmettre de la donnée numérique au deuxième terminal via le premier moyen de communication après que les terminaux aient établi une connexion via le premier moyen.

Selon un autre aspect matériel, l'invention a trait à un programme d'ordinateur apte à être mis en œuvre sur ledit deuxième terminal, le programme comprenant des instructions de code qui, lorsqu'il est exécuté par un processeur réalise une étape de transmission de données de configuration relatives à un premier moyen de communication via un deuxième moyen de communication sur lequel une communication entre deux terminaux inclut une étape d'authentification des terminaux.

Selon un autre aspect matériel, l'invention a trait à un programme d'ordinateur apte à être mis en œuvre sur ledit premier terminal, le programme comprenant des instructions de code qui, lorsqu'il est exécuté par un processeur réalise une étape de réception de données de configuration via un deuxième moyen de communication, et des moyens de prise en compte des données de configuration reçus pour établir une communication via un premier réseau avec le deuxième terminal.

L'invention sera mieux comprise à la lecture de la description qui suit, donnée à titre d'exemple et faite en référence aux dessins annexés.

Les figures:

La figure 1 représente un système informatique sur lequel est illustré un exemple de réalisation du procédé de l'invention.

La figure 2 représente une scène illustrant un exemple de réalisation.

La figure 3 est un organigramme illustrant les étapes d'un exemple de réalisation de l'invention.

Description détaillée d'un exemple de réalisation illustrant l'invention

La figure 1 représente un système SYS comprenant deux terminaux, un premier terminal TRM1 et un deuxième terminal TRM2, aptes à être utilisés par deux utilisateurs respectifs, un premier utilisateur UT1 et un deuxième utilisateur UT2. Notons ici que les deux utilisateurs pourraient être un seul et même utilisateur.

Les terminaux incluent des ressources physiques et logicielles, dont au moins un microprocesseur, pour traiter des données numériques. La structure des terminaux sera décrite en référence à la figure 2.

Dans notre exemple, les deux terminaux sont aptes à communiquer via un premier moyen de communication illustré par un réseau sans fil RES1 de type WI-FI.

Les deux terminaux sont aussi aptes à communiquer via un deuxième moyen de communication dont la portée sera, selon l'invention, choisie judicieusement de telle sorte qu'une communication entre les deux terminaux peut être supervisée par le premier utilisateur UT1 et/ou le deuxième UT2.

Le réseau sans fil RES1 est formé par l'émission d'ondes électromagnétiques issues d'une passerelle domestique GTW telle que la passerelle Livebox (marque déposée par la demanderesse) connue de l'homme du métier. Sur la figure 1, la couverture du réseau sans fil RES1 peut être assimilée à un disque D ayant un rayon R dans laquelle une communication est possible entre un terminal et la passerelle GTW.

Dans notre exemple de réalisation, la communication via le réseau sans fil RES1 nécessite la connaissance de données telles que des informations de connexion relatives au réseau sans fil RES1, par exemple une adresse IP (ou un nom de terminal) et un numéro de port du terminal avec lequel une communication est souhaitée. Ces données seront désignées par l'expression "données de configuration" DC.

Le figure 2 est une vue détaillée des circuits présents sur les terminaux

Les deux terminaux TRM1 et TRM2 appartiennent à un premier utilisateur UT1 et à un deuxième utilisateur UT2, respectivement. Les terminaux sont équipés d'un premier microprocesseur CPU1 et d'un deuxième microprocesseur MP2, respectivement.

Le premier terminal TRM1 comprend en outre

- des premiers moyens de communication COM1, reliés à une première antenne ANT1, permettant de communiquer avec le premier moyen RES1 ;
- des moyens de captures CPT aptes à capturer un signal, reliés à des moyens de traitement aptes à traiter le signal capturé ;
- Une première mémoire MEM1 apte à stocker des données;

Les moyens décrits ci-dessus ainsi que le premier microprocesseur CPU1 sont reliés entre eux par l'intermédiaire d'un premier bus BUS1

Le deuxième terminal TRM2 comprend en outre

- des deuxièmes moyens de communication COM2, reliés à une deuxième antenne ANT2, permettant de communiquer avec le premier moyen RES1 ;
- des moyens de transmission EMT, par exemple des moyens de restitution (écran, émetteur de son, etc.) aptes à restituer des signaux;
- une deuxième mémoire MEM2 apte à stocker des données notamment les données de configuration DC.

Les moyens décrits ci-dessus ainsi que le deuxième microprocesseur CPU2 sont reliés entre eux par l'intermédiaire d'un deuxième bus BUS2.

A noter que les bus décrits ci-dessus ont pour fonction d'assurer le transfert de données numériques entre les différents circuits reliés au microprocesseur par un bus. Dans notre exemple, le bus en question inclut un bus de données et un bus de contrôle.

A noter aussi que, dans notre exemple, les mémoires décrites ci-dessus sont des mémoires permanentes de type ROM (acronyme anglo-saxon de Read Only Memory).

Nous avons vu précédemment que les deux terminaux peuvent communiquer via un deuxième moyen de communication. Dans notre exemple, le deuxième moyen est choisi de telle sorte qu'il assure une étape d'authentification, en particulier une authentification mutuelle des terminaux, avant toute communication entre deux terminaux via ce deuxième moyen. En particulier, le deuxième moyen est choisi de telle sorte que les deux terminaux se situent dans le champ visuel CHP du premier utilisateur UT1 et/ou du deuxième utilisateur UT2, au moins lors de la communication des données de configuration DC entre les terminaux via ce deuxième moyen de communication.

Rappelons que le champ visuel CHV est un cône comprenant un sommet C qui désigne un œil (ou les deux yeux) de l'utilisateur et un angle d'ouverture W.

Ce deuxième moyen peut être indifféremment un moyen de communication longue distance ou ayant une portée limitée en distance.

Un moyen de communication longue distance est par exemple un réseau étendu de type WAN (acronyme anglo-saxon de "Wide Area Network")

Un moyen de communication ayant une portée limitée en distance est par exemple un câble USB (acronyme anglo-saxon de "Universal Serial Bus"), un réseau sans fil tel qu'un réseau WI-FI, un moyen de communication de type NFC (acronyme de "Near Fiel Communication"), ou de type RFiD (acronyme de "Radio Frequency Identification"), ou un moyen de communication Bluetooth, ou un moyen de communication formé par les moyens de capture CPT et les moyens

de restitution EMT comme décrit dans ce qui suit. En effet, dans notre exemple, les moyens de restitution EMT, illustrés par un écran présents sur le deuxième terminal, sont aptes à restituer les données de configuration ; et les moyens de capture CPT présents sur le premier terminal sont aptes à capturer les données de configuration restituées. L'ensemble incluant le capteur et les moyens de restitution forme le deuxième réseau permettant aux données de configuration DC d'être transmises depuis le deuxième terminal TRM2 vers le premier terminal TRM1.

Selon une variante, les données de configuration sont transformées en un code apte à être restitué par l'écran du deuxième terminal TRM2. Pour cela, le deuxième terminal comprend un générateur de code GNT apte à générer un code, par exemple un code 2D connu de l'homme du métier, représentatif des données de configuration. Aussi, le premier dispositif est équipé d'un décodeur DEC apte à décoder le code capturé par les moyens de captures.

Dans notre exemple, les moyens de captures sont un appareil photographique numérique et les moyens de restitution EMT sont un écran apte à afficher des données telles que les données de configuration DC par exemple sous forme de code 2D.

A noter ici que d'autres moyens de restitution auraient pu être utilisés. Le terminal émetteur des données de configuration pourrait inclure un dispositif émetteur de son, ou émetteur de lumière en lieu et place d'un appareil d'un écran, pour émettre des signaux aptes à transporter une information, en particulier les données de configuration. Les données de configuration sont alors transmises sous la forme d'un son ou de lumière, respectivement. Aussi, le terminal récepteur est équipé en conséquence d'un microphone et d'un capteur de lumière, respectivement.

A noter que si les moyens de restitution sont un émetteur sonore, ceux-ci peuvent émettre des sons haute fréquence interprétables uniquement que par les terminaux. Ou si les moyens de restitution sont des émetteurs lumineux,

ceux-ci peuvent clignoter, et le clignotement serait interprétable uniquement par les moyens de traitement TRT du terminal récepteur.

Les étapes d'un exemple de réalisation sont maintenant décrites en référence à la figure 3.

On suppose que les deux terminaux TRM1 et TRM2 sont géographiquement proches l'un de l'autre. On fait l'hypothèse qu'ils se trouvent dans le champ électromagnétique de la passerelle GTW, c'est-à-dire dans le disque D, et qu'une communication via le réseau WI-FI de la passerelle est souhaitée.

Les deux terminaux TRM1 et TRM2 ne disposent pas des données de configuration DC nécessaires à un appariement entre les deux terminaux via le réseau WI-FI.

Une variante aurait pu consister pour l'utilisateur à déclarer au moyen d'une commande transmise au processeur concerné le souhait de communiquer avec un autre terminal.

Lors de l'obtention des données DC, dans notre exemple, le processus de communication via le réseau WI-FI est mis en attente. La durée de mise en attente est choisie raisonnablement pour permettre à un terminal de recevoir des données de configuration DC depuis l'autre terminal.

Les étapes qui précèdent processus de communication via le réseau WI-FI sont les suivantes.

Une première étape ET1 (AFF->TRM2) au cours de laquelle le deuxième utilisateur UT2 requiert l'affichage d'un code représentatif des données de configuration DC sur le deuxième terminal TRM2. Cette demande est représentative du souhait de communiquer via le réseau sans fil RES1.

Lors d'une deuxième étape ET2 (CDE1->CPU2), le deuxième processeur CPU2 reçoit une demande d'affichage CDE1 et commande aux moyens de génération GNT la génération d'un code.

Une fois le code généré, le deuxième processeur CPU2 requiert lors d'une troisième étape ET3 (AFF->2D) l'affichage sur l'écran EMT du code généré.

Lors d'une quatrième étape ET4 (CHV), le premier utilisateur approche le premier terminal du deuxième à une distance telle que son champ visuel permet de visualiser les deux terminaux afin de garantir la légitimité des deux terminaux.

Lors d'une cinquième étape ET5 (CDE2->CPU1), le premier utilisateur UT1 requiert une capture du code affiché sur l'écran EMT du deuxième terminal.

On remarque ici que c'est l'utilisateur qui commande l'affichage du code 2D et qui commande la capture du code 2D. De plus, ces actions de commander d'affichage du code 2D et de commander la capture du code 2D, sont réalisées lorsque les deux terminaux se situent dans le champ visuel du premier utilisateur UT1 et/ou du deuxième utilisateur UT2. Les utilisateurs ont non seulement la maîtrise de l'instant de la transmission des données de configuration mais ils peuvent aussi visualiser les terminaux impliqués à savoir le premier et le deuxième terminal.

L'approche du premier terminal TRM1 vers le deuxième terminal TRM2 est également une action réalisée par le premier utilisateur UT2.

A noter ici que les actions réalisées par un utilisateur sur l'un ou l'autre des terminaux sont réalisées au travers d'interfaces graphiques respectives (non représentées sur les figures) présentes sur les deux terminaux. Nous ne rentrerons pas dans les détails techniques des interfaces graphiques car sans intérêt pour l'exposé de l'invention.

Lors d'une sixième étape ET6 (CPU1-> PRV), le premier processeur CPU1 reçoit une commande CDE2 de prise de vue et transmet une commande aux moyens de traitement TRT apte à commander une prise de vue du code.

Lors d'une septième étape ET7 (2D->CPT), les moyens de capture CPT capturent le code, les moyens de traitement TRT traitent le code reçus et après traitement les transmet au premier processeur CPU1.

Lors d'une huitième étape ET8 (CPU1->DEC), le premier processeur CPU1 transmet une commande à destination des moyens de décodages DEC requérant le décodage du code reçu.

Lors d'une neuvième étape ET9 (DC->MOD), une fois le décodage réalisé et les données de configuration extraites, le premier microprocesseur CPU1 fournit les données de configuration à un module MOD chargé de la phase de configuration décrite ci-dessus en liaison avec le premier réseau RES1.

Le module MOD comprend à cet effet des moyens de prise en compte des données de configuration reçus et des moyens pour poursuivre le processus de communication via le réseau WI-FI avec ces données de configuration DC. Ainsi, lors d'une dixième étape ET10 (MOD->COM RES1), le module MOD ayant connaissance des données de configuration DC poursuit le processus de communication via le réseau WI-FI avec le deuxième terminal.

A ce stade du procédé les deux terminaux peuvent communiquer via le premier réseau RES1.

On a vu précédemment que les données de configuration étaient transmises sous forme de code 2D. Une variante peut consister à utiliser un code 2D représentatif d'un identifiant. Le premier terminal TRM1 peut ensuite interroger une base de données à laquelle il est connecté via le réseau WI-FI par exemple. La base de données en question fournit ensuite les données de configuration utiles à la phase de configuration.

Selon une autre variante, une donnée numérique (JT), ci-après désignée par "jeton", créée par le deuxième terminal TRM2 est ajoutée aux données de configuration DC. Dans notre exemple, les données de configuration et le jeton JT sont incluent dans le code 2D généré par le générateur de code. Pour des raisons de sécurité, ce jeton est de préférence un mot de passe à usage unique modifié à chaque communication de données de configuration. Dans cette configuration, dans notre exemple, le premier terminal reçoit le code 2D incluant des données de connexion accompagné d'un jeton JT. Ensuite, lors de la poursuite du processus de communication via le réseau sans fil RES1, le premier

terminal TRM1 transmet au deuxième terminal TRM2 le jeton reçu, que le deuxième terminal compare avec le jeton transmis initialement vers le premier terminal TRM1. Si le résultat de la comparaison est que le jeton transmis au premier terminal et le jeton reçu sont les mêmes, le deuxième terminal est assuré que le premier terminal est celui qui a reçu le code 2D. En d'autres mots, le premier terminal est authentifié.

A cet effet, le deuxième terminal comprend

- des moyens de création d'une donnée numérique (JT), dite première donnée numérique, qui est dans notre exemple le générateur de code GNT, la première donnée numérique accompagnant les données de configuration lors de la transmission des données de configuration ;

- des moyens de réception d'une deuxième donnée numérique ;

- des moyens de comparaison aptes à comparer la première et la deuxième donnée et des moyens aptes à conditionner une communication avec le premier terminal via le premier réseau en fonction du résultat de la comparaison. S'il y a correspondance, par exemple si les données sont les mêmes, la communication peut avoir lieu via le premier réseau.

Aussi, le premier terminal comprend

- des moyens de réception aptes à recevoir les données de configuration ainsi que la donnée numérique JT ; à savoir, dans notre exemple, le capteur CPT;

- des moyens de transmission, à savoir dans notre exemple les premiers moyens de communication COM1, de la donnée numérique JT au deuxième terminal TRM2 via le premier moyen de communication après que les terminaux aient établi une connexion via le premier moyen.

Le jeton peut être par exemple une clé secrète. Dans notre exemple, ce jeton est généré par les moyens de génération GNT.

Revendications

1. Procédé d'établissement d'une connexion entre deux terminaux, un premier terminal (TRM1) et un deuxième terminal (TRM2) aptes à communiquer au travers d'au moins deux moyens de communication dont un premier moyen de communication (RES1) nécessitant des données de configuration (DC), caractérisé en ce que les données de configuration nécessaires à la connexion des deux terminaux via le premier moyen de communication (RES1) sont transmises par le premier terminal au deuxième terminal via un deuxième moyen de communication sur lequel une communication entre les deux terminaux inclut une étape d'authentification des terminaux.

2. Procédé selon la revendication 1, caractérisé en ce que les deux terminaux (TRM1,TRM2) sont aptes à être utilisés par un utilisateur respectif (UT1,UT2), et en ce que la transmission des données de configuration est commandée suite à une action d'un utilisateur sur l'un des deux terminaux et en ce que l'action est réalisée lorsque les deux terminaux se situent dans le champ visuel d'au moins un utilisateur choisi parmi le premier ou le deuxième utilisateur.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que le deuxième moyen de communication est un moyen de communication d'une portée limitée en distance.

4. Procédé selon la revendication 3, caractérisé en ce qu'un terminal est équipé de moyens de prise de vue, un autre terminal est équipé d'un moyen de restitution d'une information représentative des données de configuration, et en ce que pour la communication des données de configuration via le deuxième moyen de connexion, les moyens de prise de vue capturent l'information.

5. Procédé selon la revendication 1, caractérisé en ce qu'une donnée numérique (JT) créée par le deuxième terminal est ajoutée aux données de configuration (DC) lors de la communication des données de

configuration au premier terminal, et en ce que la donnée numérique (JT) reçue par le premier terminal (TRM1) est transmise depuis le premier terminal vers le deuxième terminal via le premier moyen de communication après que les terminaux aient établi une connexion via le premier moyen.

6. Système informatique (SYS) comprenant un premier terminal (TRM1) et un deuxième terminal (TRM2) aptes à communiquer au travers d'au moins deux moyens de communication dont un premier moyen de communication nécessitant des données de configuration (DC), caractérisé en que le deuxième terminal (TRM2) comprend des moyens de transmission (EMT) des données de configuration via un deuxième moyen de communication sur lequel une communication entre les deux terminaux inclut une étape d'authentification des terminaux, et en ce que le premier terminal (TRM1) comprend des moyens de réception (CPT) des données de configuration (DC) via ce deuxième moyen de communication.

7. Terminal (TRM2) , dit deuxième terminal, apte à communiquer avec un autre terminal (TRM1), dit premier terminal, via au moins deux moyens de communication dont un premier moyen de communication nécessitant des données de configuration (DC), caractérisé en ce qu'il comprend des moyens de transmission (EMT) des données de configuration (DC) via un deuxième moyen de communication sur lequel une communication entre deux terminaux inclut une étape d'authentification des terminaux.

8. Terminal selon la revendication 7, caractérisé en qu'il comprend des moyens de création d'une donnée numérique (JT), dite première donnée numérique, et en ce que la donnée numérique accompagne les données de configuration lors de la transmission des données de configuration, en ce qu'il comprend des moyens de réception d'une deuxième donnée numérique et en ce qu'il comprend des moyens de comparaison aptes à comparer la première et la deuxième donnée et des moyens aptes à

conditionner une communication avec le premier terminal via le premier réseau en fonction du résultat de la comparaison.

9. Programme d'ordinateur apte à être mis en œuvre sur un terminal tel que défini dans la revendication 7, le programme comprenant des instructions de code qui, lorsqu'il est exécuté par un processeur réalise une étape de transmission (EMT) de données de configuration (DC) relatives à un premier moyen de communication (RES1) via un deuxième moyen de communication (RES2) sur lequel une communication entre deux terminaux inclut une étape d'authentification des terminaux.

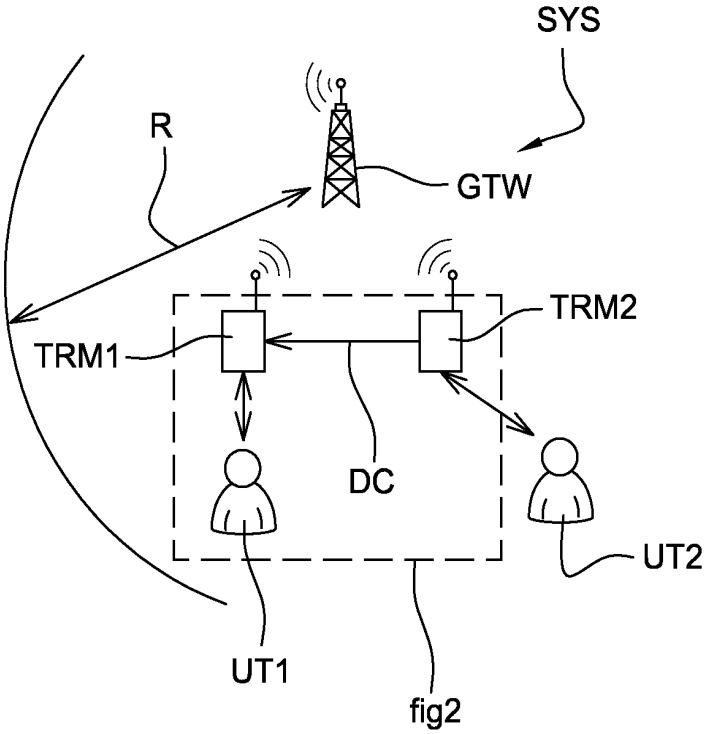
SYS
R
GTW
TRM2
TRM1
DC
UT2
UT1
fig2

Fig. 1

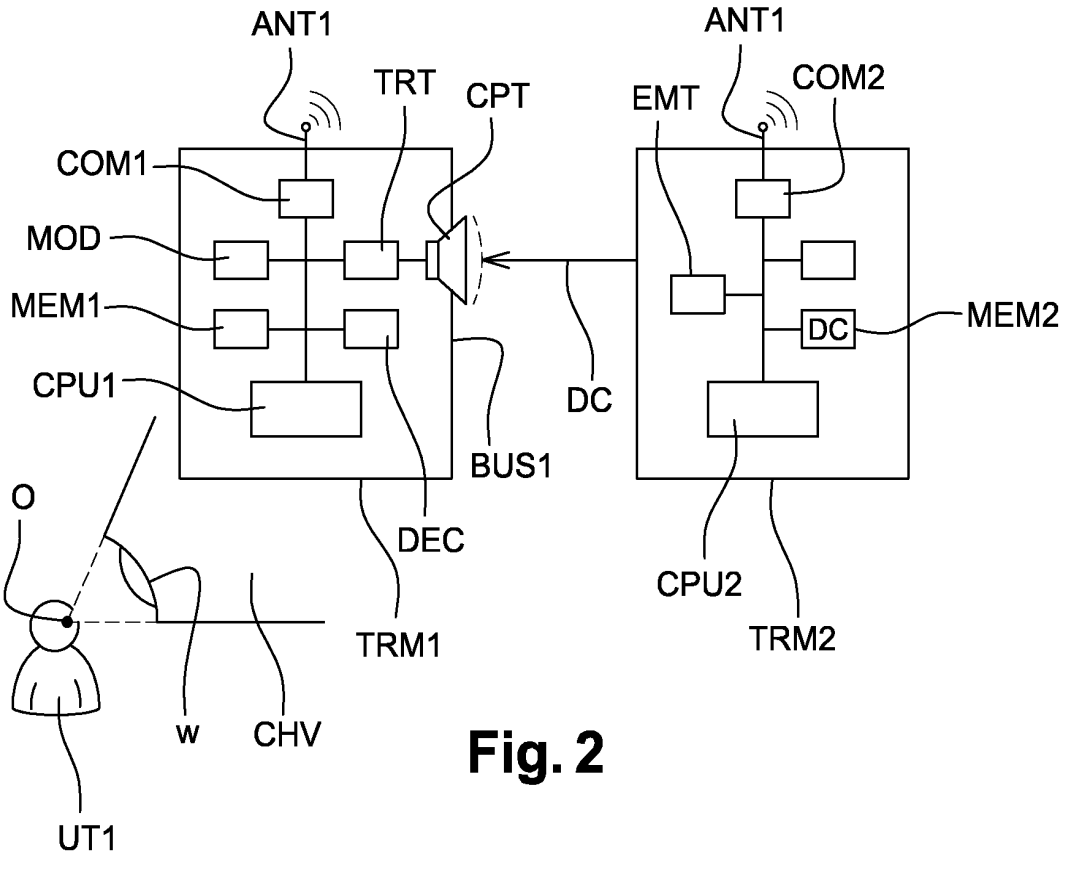
ANT1
TRT
CPT
ANT1
EMT
COM2
COM1
MOD
MEM1
CPU1
DC
MEM2
BUS1
O
DEC
CPU2
TRM2
TRM1
w
CHV
UT1

Fig. 2

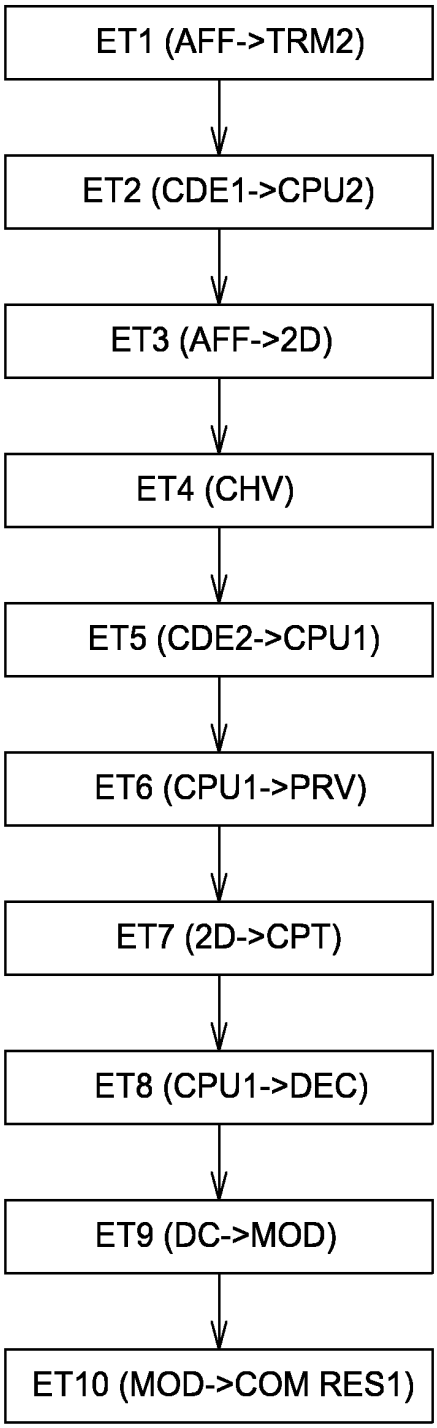
ET1 (AFF->TRM2)
ET2 (CDE1->CPU2)
ET3 (AFF->2D)
ET4 (CHV)
ET5 (CDE2->CPU1)
ET6 (CPU1->PRV)
ET7 (2D->CPT)
ET8 (CPU1->DEC)
ET9 (DC->MOD)
ET10 (MOD->COM RES1)

Fig. 3

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 754746
FR 1153324

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2007/178882 A1 (TEUNISSEN HAROLD W A [NL] ET AL TEUNISSEN HAROLD WILHELM ANTONIE [NL]) 2 août 2007 (2007-08-02) * abrégé * * alinéas [0001] - [0012] * * alinéas [0025] - [0049] * * figures 2-4 * -----	1-9	H04L9/32 H04L29/06 H04W12/06
X	US 2007/063055 A1 (GRAF HANS [DE] ET AL) 22 mars 2007 (2007-03-22) * abrégé * * alinéas [0001] - [0012] * * alinéas [0031] - [0047] * * figures 3-6 * -----	1-9	
X	US 2005/076216 A1 (NYBERG KAISA [FI]) 7 avril 2005 (2005-04-07) * abrégé * * alinéas [0011] - [0051] * -----	1-9	
X	US 2002/169988 A1 (VANDERGEEST RON J [CA] ET AL) 14 novembre 2002 (2002-11-14) * abrégé * * alinéas [0003] - [0008] * * alinéas [0015] - [0026] * * figures 1-2 * -----	1,5-9	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L
X	US 2011/035788 A1 (WHITE CONOR ROBERT [US] ET AL WHITE CONOR [IE] ET AL) 10 février 2011 (2011-02-10) * abrégé * * alinéas [0004] - [0014] * ----- -/--	1,5-9	

Date d'achèvement de la recherche	Examinateur
16 décembre 2011	Di Felice, M

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

1

EPO FORM 1503 12.99 (P04C14)

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 754746
FR 1153324

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	TAYLOR D: "How do I sign up for Google Gmail with my cell phone?", INTERNET CITATION, 21 août 2006 (2006-08-21), pages 1-6, XP002597911, Extrait de l'Internet: URL:http://www.askdavetaylor.com/how_do_i_sign_up_for_google_gmail_with_my_cell_phone.html [extrait le 2010-08-23] * le document en entier * -----	1,5-9	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
16 décembre 2011	Di Felice, M

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

1

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1153324 FA 754746

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 16-12-2011
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2007178882 A1	02-08-2007	EP 1980085 A2	15-10-2008
		US 2007178882 A1	02-08-2007
		WO 2007089758 A2	09-08-2007
US 2007063055 A1	22-03-2007	AT 428152 T	15-04-2009
		CN 1799058 A	05-07-2006
		DE 10317257 A1	04-11-2004
		EP 1616291 A2	18-01-2006
		EP 2081135 A2	22-07-2009
		JP 4759505 B2	31-08-2011
		JP 2006524851 A	02-11-2006
		PT 1616291 E	14-07-2009
		US 2007063055 A1	22-03-2007
		WO 2004090800 A2	21-10-2004
US 2005076216 A1	07-04-2005	AUCUN	
US 2002169988 A1	14-11-2002	AUCUN	
US 2011035788 A1	10-02-2011	AUCUN	

EPO FORM P0465