



(51) Classification internationale des brevets :

H04L 29/06 (2006.01) G06K 7/00 (2006.01)
H04W 12/02 (2009.01) G06K 19/07 (2006.01)
H04L 9/32 (2006.01) H04N 1/44 (2006.01)

(21) Numéro de la demande internationale :

PCT/EP2009/053200

(22) Date de dépôt international :

18 mars 2009 (18.03.2009)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

0851754 18 mars 2008 (18.03.2008) FR

(71) Déposant (pour tous les États désignés sauf US) : **EADS SECURE NETWORKS** [FR/FR]; 1 boulevard Jean Moulin, ZAC de la Clef Saint Pierre, F-78990 Elancourt (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **ROUSSEAU, Frédéric** [FR/FR]; 22, rue Victor Hugo, F-78180 Montigny Le Bretonneux (FR). **ELOY,**

Stéphane [FR/FR]; 17 Promenade Paul Doumer, F-92400 Courbevoie (FR).

(74) Mandataires : **MILLET, Sandrine** et al.; Cabinet Plasseraud, 52 rue de la Victoire, F-75440 Paris Cedex 09 (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, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

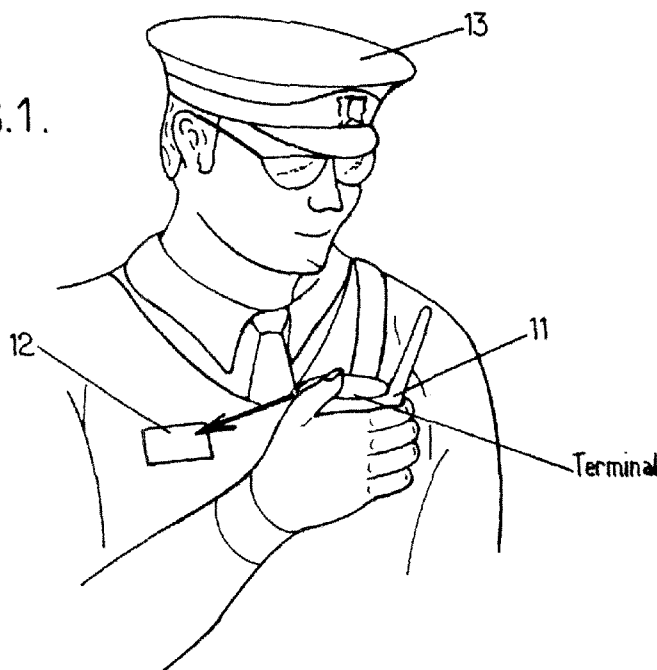
(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR),

[Suite sur la page suivante]

(54) Title : MANAGEMENT OF THE IDENTITIES OF USERS IN A SYSTEM

(54) Titre : GESTION D'IDENTITES D'UTILISATEURS DANS UN SYSTEME

FIG.1.



(57) Abstract : The invention comprises managing the identity of a user to be associated with a terminal (11) adapted for communication in a communication network that provides a service based on the identity of the user. A contactless transaction is established at the terminal with an identification entity (12). During the transaction, a piece of information on the identity of the user stored in the identification entity is received. Finally, the identity of the user obtained from said information is stored. It is also provided that the identity of the user is erased at the terminal when the terminal is subjected to a specific action.

(57) Abrégé : On gère une identité d'utilisateur à associer à un terminal (11) qui est adapté pour communiquer dans un réseau de communication offrant un service fondé sur l'identité utilisateur. Au niveau du terminal, on établit une transaction sans contact avec une entité d'identification (12). Puis, on reçoit, au cours de la transaction, une information relative à une identité d'utilisateur stockée sur l'entité d'identification. Enfin, on stocke l'identité d'utilisateur obtenue à partir de cette information. Il est en outre prévu que l'identité d'utilisateur soit effacée au niveau du terminal lorsque le terminal est soumis à une

action spécifique.



OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée
dès réception de ce rapport (règle 48.2.g)*

Déclarations en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)*

GESTION D'IDENTITES D'UTILISATEURS DANS UN SYSTEME

La présente invention se rapporte à la gestion d'une identité d'utilisateur pour un terminal électronique, et plus particulièrement à l'association temporaire d'une identité d'utilisateur à un terminal d'un système.

- 5 Certains systèmes offrent des services à des utilisateurs en fonction des identités respectives de ces utilisateurs. Ainsi, lorsqu'un utilisateur souhaite accéder, via un terminal du système, à un service auquel il a par exemple souscrit un abonnement, il associe à ce terminal du système une entité d'identification à partir de laquelle est accessible son identité d'utilisateur. Une
- 10 telle entité d'identification peut être par exemple un lecteur d'identité ou un support de mémorisation d'identité tel qu'une carte d'identité, ou une carte de paiement ou une carte d'abonnement à un service profilé, par exemple une carte UICC/USIM (pour 'Universal Integrated Circuit Card / Universal Subscriber Identity Module') dans le contexte des réseaux GSM ou 3GPP.
- 15 Dans l'exemple relatif au réseau GSM utilisant une entité d'identification conforme au standard ISO/IEC 7816, cette dernière et le terminal sont en contact physique puisque, et, bien qu'amovible, cette entité d'identification est en général maintenue à l'intérieur du boîtier du terminal. Par conséquent, lorsque le terminal est subtilisé, le voleur peut usurper l'identité de l'abonné
- 20 puisqu'en subtilisant le terminal il a simultanément récupéré l'entité d'identification utilisée par cet abonné.

On peut alternativement prévoir que l'interface entre le terminal et l'entité d'identification soit une interface électromagnétique, telle qu'une interface radio sans contact. Avec une telle interface, le terminal et l'entité d'identification ne

25 sont pas physiquement connectés. Le niveau de sécurité en est alors amélioré

car, lors d'un vol de terminal, l'entité d'identification n'est pas nécessairement volée.

Toutefois, quel que soit le type d'interface utilisée, il convient de noter qu'il est requis que le terminal et l'entité d'identification soient reliés durant
5 toute la période d'utilisation du service de communication considéré.

Il peut en être ainsi, par exemple, pour une transaction financière. Dans ce cas là, si au cours de la transaction financière, l'interface entre l'entité d'identification et le terminal est détectée comme interrompue, toute la transaction doit être réitérée depuis le début.

10 Ainsi, lorsque l'interface est une interface électromagnétique, il est requis que la distance séparant l'entité d'identification et le terminal soit suffisamment faible afin de dépasser un seuil de qualité minimale de l'interface électromagnétique en deçà duquel la transaction entre la l'entité d'identification et le terminal serait interrompue. Cette distance seuil est dépendante de la
15 norme mise en œuvre sur cette interface. En effet, on connaît par exemple les normes d'interface de proximité ISO/IEC 14443, ISO/IEC 18092 et ISO/IEC 21481 (ISO/IEC pour 'International Organisation for Standardization') qui requièrent que la distance entre l'entité d'identification et le terminal soit de l'ordre de quelques centimètres au plus, alors que d'autres normes, telle que la
20 norme d'interface de voisinage ISO/IEC 15693, tolèrent des distances de l'ordre de plusieurs décimètres.

Ainsi, en utilisant une interface électromagnétique entre l'entité d'identification et le terminal, on peut se prémunir d'une usurpation d'identité mais des coupures de service peuvent se produire sur rupture de l'interface
25 entre le terminal et l'entité d'identification.

Or, dans certains domaines, il peut être désavantageux de subir l'interruption du service dès lors que l'interface entre le terminal et l'entité d'identification est rompue. Tel est notamment le cas pour des communications critiques, mises en œuvre par exemple par des professionnels de force de
30 sécurité et de secours.

La présente invention vient améliorer la situation.

Un premier aspect de la présente invention propose un procédé d'association d'une identité d'utilisateur à un terminal électronique adapté pour offrir un service fondé sur ladite identité d'utilisateur ;
ledit procédé d'association comprenant les étapes suivantes, au niveau du
5 terminal :

- /1/ établir une transaction sans contact avec une entité d'identification ;
 - /2/ recevoir, au cours de ladite transaction, une information relative à une identité d'utilisateur stockée sur ladite entité d'identification ; et
 - 10 /3/ stocker ladite identité d'utilisateur obtenue à partir de ladite information ;
- dans lequel l'identité d'utilisateur est effacée au niveau du terminal lorsque ledit terminal est soumis à une action spécifique.

Ainsi, le terminal est en mesure de récupérer et de stocker, de manière
15 aisée, une identité d'utilisateur depuis une entité d'identification, cette identité d'utilisateur étant stockée de manière temporaire sur le terminal puisqu'elle est effacée quand on soumet le terminal à une certaine action.

Une telle action spécifique peut notamment correspondre à la mise hors tension du terminal ou encore à une action quelconque d'utilisateur sur le
20 terminal, ou bien une action mise en œuvre par une application embarquée au niveau du terminal, comme par exemple l'occurrence d'un événement interne au terminal (e.g. l'échéance d'une temporisation ou d'un compteur d'échecs).

Grâce à de telles dispositions, il est possible de garantir une continuité dans le service auquel l'utilisateur a accès tout en maintenant un niveau de
25 sécurité élevé contre l'usurpation de l'identité de l'utilisateur. En effet, d'une part, si le terminal est subtilisé à l'utilisateur, l'entité d'identification n'étant pas physiquement liée au terminal, elle n'est pas obligatoirement subtilisée elle aussi. D'autre part, il n'est pas requis que la transaction entre le terminal et l'entité d'identification soit en cours pour que le terminal puisse offrir le service
30 fondé sur l'identité utilisateur puisque cette identité d'utilisateur est stockée au niveau du terminal.

En outre, le stockage de cette identité d'utilisateur est temporaire. Il est à cet effet avantageusement prévu d'effacer cette identité d'utilisateur sous une action appliquée au terminal. Cette action peut être appliquée soit par un utilisateur soit encore par une application embarquée au niveau du terminal.

5 Une fois que la transaction sans contact entre le terminal et l'entité d'identification est établie, l'identité peut alors être transmise depuis cette entité vers le terminal. A ce moment là, l'identité peut être stockée au niveau du terminal afin de permettre à l'utilisateur d'accéder au service souhaité.

Ainsi, l'interface sans contact entre le terminal et l'entité d'identification
10 permet non seulement d'éviter une usurpation d'identité de l'utilisateur et en outre ne requiert pas que la transaction entre le terminal et l'entité d'identification reste établie tout au long de l'utilisation du service considéré.

Il suffit donc que le terminal et l'entité d'identification puissent communiquer quelques instants seulement pour que le terminal puisse recevoir
15 l'identité d'utilisateur et bénéficier ensuite, sur cette base, d'un service.

Avantageusement, un tel procédé selon un mode de réalisation de la présente invention permet d'obtenir l'identité d'utilisateur rapidement et de manière indépendante d'autres transactions ultérieures effectuées par le terminal.

20 Il convient de noter que la disparition, le retrait ou l'absence d'entité d'identification peut ne pas impliquer de conséquence sur les communications ou transactions ultérieures du terminal.

Dans ces conditions, la gestion de la protection des opérations, communications ou encore transactions du terminal peut rester indépendante
25 de la gestion de la protection des échanges entre le terminal et l'entité d'identification d'utilisateur.

Une telle caractéristique est un avantage recherché dans le contexte des systèmes de communications critiques professionnels, notamment parce que le vol du terminal en cours d'utilisation n'implique pas le vol de l'entité
30 d'identification, contrairement au cas d'un terminal adapté pour un réseau de communication de type GSM ou 3GPP. En outre, une fois l'identité d'utilisateur obtenue et stockée au niveau du terminal, ce dernier peut effectuer de

5 multiples opérations sans nécessiter une nouvelle transaction avec l'entité d'identification, jusqu'à ce qu'une action spécifique effaçant l'identité d'utilisateur soit mise en œuvre, la mise hors de tension du terminal, ou bien dans le cas où une procédure de détection de présence de l'entité d'identification (ou 'watch dog') est mise en œuvre, jusqu'à effacement de l'identité d'utilisateur au niveau du terminal.

En mettant en œuvre un procédé d'association selon un mode de réalisation de la présente invention, on peut avantageusement supprimer la gestion d'un mot de passe ou code PIN (pour 'Personal Identification Number' en anglais) comme c'est le cas notamment pour débloquer l'usage du clavier d'un terminal adapté pour les réseaux de communications de type GSM ou UMTS.

Avantageusement, la mise en œuvre d'un procédé d'association selon un mode de réalisation de la présente invention est bien adaptée à une utilisation banalisée de terminal, c'est-à-dire à l'utilisation d'un terminal par différents utilisateurs successifs.

On peut prévoir que l'utilisateur puisse effectuer une manipulation quelconque du terminal permettant d'effacer l'identité d'utilisateur stockée au niveau du terminal avant de cesser de l'utiliser. La mise hors tension du terminal peut permettre notamment cet effacement volontaire de l'identité d'utilisateur stockée.

On peut en outre fournir une fonction spécifique d'effacement dans un menu du terminal, via une application embarquée au niveau du terminal, ou encore commander l'effacement de cette identité d'utilisateur par l'appui sur une ou plusieurs touches du clavier du terminal.

Le terminal n'est pas opérationnel, c'est-à-dire qu'il ne peut pas offrir le service fondé sur une identité, tant qu'il ne possède pas cette identité d'utilisateur. Le terminal peut, avant d'obtenir une identité d'utilisateur, opérer avec une autre identité propre au terminal. Cette identité de terminal peut, par exemple, être un numéro de série du terminal.

Le service offert au niveau du terminal peut être un service local au terminal ou encore un service offert via un réseau de communication. Un

service local peut par exemple correspondre à un contrôle de papier d'identité effectué par scannage d'un papier d'identité au niveau du terminal selon un mode de réalisation de la présente invention. L'identité d'utilisateur peut alors être utilisée pour autoriser ou interdire l'utilisation du terminal considéré sur la

5 base d'une liste d'identifiants utilisateur qui est stockée localement au terminal. On peut en outre prévoir que l'entité d'identification stocke, outre l'information relative à l'identité d'utilisateur, un profil d'utilisateur, ou profil d'abonné, qui est transmis au terminal pour adapter le service ou les services offerts par le terminal à l'utilisateur. La présente invention est décrite ici dans son application

10 à une identité d'utilisateur, mais n'est en rien limitée à cette seule identité d'utilisateur. Il est en effet aisé de prévoir de prendre en compte en association à une identité d'utilisateur, d'autres informations, tel que des paramètres individuels comme un numéro d'annuaire, ou un profil d'utilisateur, ou encore un élément de sécurité, comme par exemple une clé d'initialisation ('ignition

15 key' en anglais) ou un certificat de sécurité, ou une combinaison d'entre eux.

Dans un mode de réalisation de la présente invention, l'information relative à l'identité d'utilisateur est l'identité d'utilisateur elle-même. Ainsi, dans ce cas, l'identité d'utilisateur peut être récupérée directement à partir de l'entité d'identification.

20 Dans un mode de réalisation de la présente invention, on prévoit que le terminal est adapté pour communiquer dans un réseau de communication. On peut alors prévoir qu'une association entre l'information relative à une identité d'utilisateur et l'identité d'utilisateur est gérée au niveau de ce réseau de communication, et que le terminal obtient l'identité d'utilisateur à l'étape /3/,

25 selon les étapes suivantes :

/i/ fournir au réseau de communication l'information relative à une identité d'utilisateur ; et

/ii/ recevoir depuis le réseau de communication ladite identité d'utilisateur.

30 Ici, l'identité d'utilisateur n'est pas directement stockée sur l'entité d'identification, cette dernière stockant seulement une information à partir de

laquelle il est possible d'obtenir cette identité d'utilisateur. Le niveau de sécurité contre une usurpation d'identité d'utilisateur est amélioré.

On peut prévoir que le procédé comprenne en outre les étapes suivantes :

- 5 /4/ déterminer si l'entité d'identification est située à proximité du terminal ;
- /5/ répéter l'étape /4/ N fois, N étant un nombre entier ;
- /6/ décider d'effacer l'identité d'utilisateur au niveau du terminal si on
- 10 détermine N fois consécutives que l'entité d'identification n'est pas située à
- proximité du terminal.

La distance entre le terminal et l'entité d'identification requise pour détecter au niveau du terminal la présence de l'entité d'identification est fonction du protocole d'échange de messages utilisé.

- Un tel mode de réalisation de la présente invention permet d'augmenter
- 15 encore le niveau de sécurité de l'identité d'utilisateur, puisque cette identité d'utilisateur est effacée sur le terminal si ce dernier détecte plusieurs fois consécutivement que l'entité d'identification n'est pas présente dans le voisinage. En effet, plusieurs détections de ce type peuvent faire suspecter fortement le fait que l'utilisateur réel du terminal n'est pas celui qu'il prétend
 - 20 être puisqu'il ne semble pas posséder l'entité d'identification correspondante.

- Aucune limitation n'est attachée à la présente invention, au regard des messages échangés entre le terminal et l'entité d'identification ou encore entre le terminal et le réseau de communication. Ainsi, notamment, une telle détection de présence d'entité d'identification dans le voisinage d'un terminal
- 25 peut être mise en œuvre selon un quelconque protocole.

- On peut notamment prévoir que la communication radio entre le terminal et l'entité d'identification visant à fournir au terminal l'information relative à l'identité d'utilisateur est de type NFC (pour 'Near Field Communication' en anglais), comme par exemple les normes d'interfaces de proximité ISO/IEC
- 30 14443, ISO/IEC 18092 et ISO/IEC 21481. Dans ce cas, cette communication peut être établie lorsque la distance entre le terminal et l'entité d'identification est comprise entre 4 cm et 10 cm environ. Cette distance étant relativement

faible, la protection de l'identité d'utilisateur est améliorée et en outre la consommation d'énergie est avantageusement relativement faible au niveau du terminal.

On peut également envisager que l'interface radio entre le terminal et
5 l'entité d'identification soit d'un autre type qui supporte de plus grandes distances entre le terminal et l'entité d'identification, comme par exemple la norme d'interface de voisinage ISO/IEC 15693.

Dans un mode de réalisation de la présente invention, un terminal peut
gérer une interface de voisinage en sus de l'interface de proximité utilisée pour
10 récupérer l'identité selon le procédé décrit supra. Dans ce cas, on peut prévoir que, lorsque le terminal utilise une entité d'identification, une temporisation de validité (watch dog timer) soit déclenchée.

Le procédé d'association temporaire d'une identité d'utilisateur et d'un
terminal peut alors comprendre optionnellement les étapes suivantes au niveau
15 du terminal, ces dernières pouvant être réalisées en parallèle d'autres étapes :

- activer périodiquement l'interface de communication de
voisinage pendant une certaine période de temps, par exemple
sur expiration d'un temporisateur ; et vérifier la présence dans le
voisinage de l'identité d'identification utilisée ;
- 20 - si la présence de l'entité d'identification est vérifiée, réinitialiser
le temporisateur et, de préférence, désactiver l'interface de
communication de voisinage, pour économiser la consommation
d'énergie ;
- si le temporisateur expire avant qu'une entité d'identification
25 n'ait pu être détectée présente dans le voisinage du terminal ;
l'utilisateur du terminal en est averti, par un signal visuel ou
sonore). Optionnellement, dans ce cas, l'identité courante de
l'utilisateur est effacée du terminal.

Dans un mode de réalisation de la présente invention, un terminal peut à
30 la fois gérer un protocole d'échange de messages de type NFC et un protocole
d'un autre type.

On peut prévoir que, lorsque le terminal est adapté pour communiquer dans un réseau de communication, après l'étape /3/, le terminal émet un signal, par exemple un signal sonore. Ainsi, l'utilisateur est informé d'une initialisation correcte du terminal qu'il utilise quant à son identité d'utilisateur.

- 5 Après l'étape /3/, le terminal peut ensuite avantageusement s'enregistrer auprès du réseau de communication sur la base de l'identité d'utilisateur. L'utilisateur peut ensuite bénéficier du ou des services offerts dans ce réseau au regard de son identité d'utilisateur.

- 10 On peut prévoir que, lorsque le terminal est adapté pour communiquer dans un réseau de communication, avant l'étape /3/, le terminal s'enregistre auprès du réseau de communication sur la base d'une identité du terminal, puis, après l'étape /3/, sur la base de l'identité d'utilisateur.

- 15 Dans ce cas, même avant que le terminal n'ait stocké l'identité d'utilisateur, il est en mesure de bénéficier rapidement, du ou des services offerts dans le réseau de communication sans identité d'utilisateur, comme par exemple un accès à un numéro de téléphone d'urgence.

- 20 On peut avantageusement prévoir que les étapes /1/ à /3/ soient mises en œuvre lors d'un mouvement d'utilisateur du terminal consistant à rapprocher le terminal de l'entité d'identification. Ainsi, par exemple, l'utilisateur du terminal peut porter sur lui, comme un badge, l'entité d'identification. Dans ce cas, afin de pouvoir utiliser un terminal selon un mode de réalisation de la présente invention, il peut récupérer son identité d'utilisateur d'un simple geste de la main visant à rapprocher le terminal de son entité d'identification pendant une brève période de temps, qui peut être de quelques secondes.

- 25 Un deuxième aspect de la présente invention propose un terminal adapté pour la mise en œuvre d'un procédé d'association selon le premier aspect.

- 30 Un troisième aspect de la présente invention propose un système d'association d'une identité d'utilisateur, comprenant un terminal selon le deuxième aspect de la présente invention et une entité d'identification sur laquelle est stockée une information relative à une identité d'utilisateur.

D'autres aspects, buts et avantages de l'invention apparaîtront à la

lecture de la description d'un de ses modes de réalisation.

L'invention sera également mieux comprise à l'aide des dessins, sur lesquels :

- 5 - la figure 1 illustre une application d'un mode de réalisation de la présente invention ;
- la figure 2 illustre un échange de messages entre un terminal et une entité d'identification selon un mode de réalisation de la présente invention permettant de garantir un certain niveau de sécurité contre l'usurpation d'identité ;
- 10 - la figure 3 illustre un échange de messages entre un terminal, une entité d'identification et le réseau relatif à un enregistrement d'un terminal auprès du réseau, selon un mode de réalisation de la présente invention ;
- la figure 4 illustre un échange de messages entre un terminal, une entité d'identification et un réseau relatif à la gestion d'un double enregistrement d'un terminal auprès du réseau, selon un mode de réalisation de la présente invention ;
- 15 - la figure 5 illustre un échange de messages entre un terminal, une entité d'identification et un réseau selon un mode de réalisation de la présente invention au cours duquel l'identité d'utilisateur est obtenue à partir du réseau, et
- 20 - la figure 6 illustre un système d'association d'une identité d'utilisateur selon un mode de réalisation de la présente invention.

La figure 1 illustre une application d'un mode de réalisation de la présente invention. Un utilisateur 13 dispose d'un terminal 11 et d'une entité d'identification 12 selon un mode de réalisation de la présente invention. On peut ici prévoir que l'entité d'identification 12 est portée par l'utilisateur au niveau de la poitrine et qu'au moment de l'initialisation de son terminal 11, l'utilisateur approche ce terminal 11 de l'endroit où il porte cette entité d'identification 12. Ainsi, la transaction entre l'entité d'identification 12 et le terminal peut s'établir selon un mode de réalisation de la présente invention afin que le terminal puisse disposer par la suite de l'identité d'utilisateur de

l'utilisateur 13 sur la base de laquelle il peut disposer d'un service offert. La transaction permettant au terminal de récupérer l'identité peut être mise en œuvre en effectuant un mouvement de rapprochement du terminal vers l'entité d'identification. On peut prévoir que le terminal émette un signal tel qu'un signal
5 sonore dès que l'identité est récupérée. Ainsi, suite à l'émission de ce signal, le terminal peut alors être éloigné de l'entité d'identification.

Il convient de prévoir que le terminal ne dispose que temporairement d'une identité d'utilisateur afin d'anticiper un vol potentiel.

A cet effet, on prévoit d'effacer l'identité d'utilisateur en mettant en
10 œuvre une action spécifique sur le terminal, comme par exemple la mise hors tension du terminal. Ainsi, le terminal ne dispose au mieux que temporairement de l'identité d'utilisateur.

Dans un mode de réalisation de la présente invention, afin d'augmenter la protection contre une usurpation potentielle d'identité de l'utilisateur, on peut
15 avantageusement prévoir de mettre en place un contrôle de temps en temps de la présence de l'entité d'identification dans le voisinage du terminal qui a stocké l'identité correspondante, par selon une interface sans contact de voisinage complémentaire de l'interface sans contact de proximité utilisée pour la précédente transaction.

20 La figure 2 illustre un échange de messages entre un terminal et une entité d'identification selon un mode de réalisation de la présente invention permettant d'augmenter le niveau de sécurité contre l'usurpation d'identité.

Ici, un échange de messages d'identification 21 <user-id> correspond à la transaction entre le terminal 11 et l'entité d'identification 12 au cours de
25 laquelle l'identité d'utilisateur user-id est récupérée par le terminal. Cet échange de messages peut être un échange de messages sécurisé pour augmenter la protection contre une éventuelle usurpation de l'identité d'utilisateur.

Une fois l'identité ainsi récupérée au niveau du terminal, elle y est stockée à une étape 24. Afin de garantir une sécurité contre l'usurpation
30 d'identité, on peut avantageusement prévoir la mise en œuvre d'une protection par un mécanisme de chien de garde ('watch dog' en anglais) entre le terminal 11 et l'entité d'identification 12 de sorte à vérifier que, de temps en temps au

moins, le terminal 11 est à proximité de l'entité d'identification 12 à partir de laquelle il a récupéré l'identité d'utilisateur qu'il a stockée. Ainsi, une fois que la transaction a été établie entre le terminal et l'entité d'identification, et que le terminal 11 a stocké l'identité qui lui permet de disposer du service considéré,
5 le terminal vérifie de temps en temps la présence à proximité de l'entité d'identification 12.

Un tel 'watch dog' peut se composer d'une succession d'échanges de messages de contrôle de présence 23 <CTRL>, chacun de ces échanges de messages visant à déterminer la présence ou non de l'entité d'identification 12
10 à proximité du terminal 11. Deux échanges de messages 23 successifs peuvent par exemple être séparés d'une période de temps T.

On peut alors avantageusement prévoir que si un nombre N d'exécutions successives d'échanges de messages 23 permet au terminal de déterminer que l'entité d'identification 12 n'est pas à proximité du terminal 11,
15 le terminal efface l'identité stockée. En effet, dans ces conditions, on peut suspecter une usurpation d'identité puisqu'on suppose que l'utilisateur de cette identité dispose, à proximité du terminal qu'il utilise, de son entité d'identification et que, de ce fait, il peut de temps en temps au moins en détecter la présence.

20 On peut en outre prévoir que l'utilisateur est informé de ce contrôle de présence négatif, et de l'effacement de l'identité d'utilisateur au niveau du terminal par un signal, par exemple un signal lumineux ou sonore produit au niveau de ce terminal.

Les valeurs de T et de N peuvent avantageusement être déterminées en
25 fonction de l'application d'un mode de réalisation de la présente invention.

Le terminal est adapté pour mettre en œuvre l'échange de messages 23 visant à détecter la présence de l'entité d'identification 12 dans son voisinage. Aucune limitation n'est attachée à la présente invention au regard de cet échange de messages.

30 Dans de telles conditions, même si la transaction entre le terminal et l'entité d'identification est interrompue, le terminal dispose encore de l'identité de l'utilisateur. Toutefois, comme l'absence de l'entité d'identification 12 est

détectée pendant un certain temps au niveau du terminal 11, par mesure de sécurité contre l'usurpation d'identité, cette identité d'utilisateur est effacée sur le terminal 11.

Par conséquent, ce mode de réalisation permet de garantir une
5 continuité de service au niveau du terminal, même si le terminal 11 est parfois éloigné de l'entité d'identification 12, tout en garantissant un niveau élevé de sécurité contre le vol d'identité d'utilisateur.

Dans une modalité, la vérification de présence de l'entité d'identification par le terminal est effectuée par une interface électromagnétique sans contact
10 de voisinage au lieu d'être effectuée par l'interface sans contact de proximité utilisée pour transférer l'identité.

Dans un mode de réalisation de la présente invention, le terminal est adapté pour communiquer dans un réseau de communication 31, et l'identité d'utilisateur est destinée à être utilisée dans ce réseau de communication 31
15 afin d'accéder au niveau du terminal 11 à un ou plusieurs services de communication.

La figure 3 illustre un échange de messages entre le terminal 11, l'entité d'identification 12 et le réseau 31 relatif à un enregistrement d'un terminal auprès du réseau de communication dans lequel il peut communiquer, selon un
20 mode de réalisation de la présente invention.

En premier lieu, le terminal 11 récupère l'identité d'utilisateur user-id de son utilisateur auprès de l'entité d'identification 12 au cours de l'échange de messages d'identification 21 <user-id> et le stocke localement à l'étape 24.

Le terminal 11 est ensuite en mesure de s'enregistrer sur la base de
25 cette identité user-id en mettant en œuvre un échange de messages d'enregistrement d'utilisateur 32 <reg user-id> avec le réseau de communication 31.

La figure 4 illustre un échange de messages, entre le terminal, l'entité d'identification et le réseau, relatif à la gestion d'un double enregistrement d'un
30 terminal auprès du réseau, selon un mode de réalisation de la présente invention. Cet échange peut être mis en œuvre lorsque le terminal 11 a une identité qui lui est propre, id-term.

Dans un mode de réalisation de la présente invention, à la mise sous tension du terminal 11, ce dernier ne dispose d'aucune identité d'utilisateur, comme illustré à une étape 40. Ainsi, avant que l'échange de messages d'identification 21 ne soit mis en œuvre, au moment de l'initialisation du terminal, ce dernier peut s'enregistrer avec son propre identifiant id-term selon un échange de messages d'enregistrement de terminal 41 <reg id-term>.

Puis, une fois que l'identité d'utilisateur est récupérée, en étape 24, par l'échange de messages d'identification 21, le terminal peut alors procéder à un enregistrement auprès du réseau fondé sur l'identité d'utilisateur via un échange de messages d'enregistrement d'utilisateur 32.

Ce mode de réalisation permet avantageusement d'augmenter l'efficacité du procédé d'enregistrement d'un terminal à un réseau qui requiert à la fois une identité du terminal et une identité de l'utilisateur en permettant de procéder en premier lieu à l'enregistrement du terminal avant que la procédure de récupération de l'identité d'utilisateur n'ait été effectuée.

Il peut également être particulièrement avantageux lorsque le réseau considéré 31 offre en outre des services basés sur l'enregistrement du terminal seulement. En effet, l'utilisateur peut alors utiliser ces services en attendant de disposer de l'identité d'utilisateur user-id et de mettre en œuvre l'enregistrement de l'utilisateur 32.

Dans une variante du mode de réalisation de la présente invention décrit en référence à la figure 4, on peut prévoir de fournir au réseau 31, de manière associée, à la fois l'identité propre au terminal id-term et l'identité d'utilisateur user-id au cours d'un même échange de messages, l'échange de message d'enregistrement 32.

La figure 5 illustre un échange de messages entre le terminal 11, l'entité d'identification 12 et le réseau 32 selon un mode de réalisation de la présente invention au cours duquel l'identité d'utilisateur est finalement obtenue à partir du réseau.

Dans ce mode de réalisation, à l'initialisation du terminal 11, ce dernier ne détient aucune identité d'utilisateur stockée localement, comme illustré à l'étape 40. En premier lieu, dans sa phase d'initialisation, le terminal 11 met en

œuvre un enregistrement de terminal auprès du réseau de communication 31 sur la base des échanges de messages 41 <reg id-term>, fournissant ainsi au réseau 31 son identifiant propre id-term.

5 Ensuite, il met en œuvre en œuvre l'étape consistant à récupérer une identité d'utilisateur user-id. Dans ce mode de réalisation de la présente invention, l'identité d'utilisateur elle-même n'est pas directement stockée au niveau de l'entité d'identification 12 que détient l'utilisateur du terminal 11. L'entité d'identification 12 stocke ici seulement une information id-info permettant de récupérer par la suite l'identité d'utilisateur auprès du réseau 31.

10 Ainsi, l'étape consistant à récupérer l'identité d'utilisateur au niveau du terminal se décompose en deux parties au niveau du terminal, une première partie consistant à récupérer l'information d'utilisateur id-info auprès de l'entité d'identification 12, et une seconde partie consistant à récupérer l'identité d'utilisateur user-id auprès du réseau 31 sur la base de l'information
15 d'utilisateur id-info. Dans ce cas, on peut prévoir que le réseau 31 comprend un serveur d'annuaire qui est adapté pour gérer une association entre une information d'utilisateur et une identité d'utilisateur.

Le terminal met en œuvre en premier lieu la première partie selon un échange de messages 51 avec l'entité d'identification 12 au cours duquel il
20 récupère l'information d'utilisateur qui est stockée sur cette entité d'identification 12.

Dans un mode réalisation particulier, on peut prévoir que le terminal stocke l'information d'utilisateur id-info, comme illustré à une étape 54 de la figure 5.

25 Puis, il procède alors à la récupération de l'identité d'utilisateur en lui-même auprès du réseau 31 sur la base de l'information d'utilisateur via un échange de messages d'identification avec le réseau au cours duquel il fournit l'information d'utilisateur dans un message 52 et reçoit en échange l'identité d'utilisateur user-id associée dans un message 53.

30 Le message 52 peut en outre indiquer l'identité de terminal id-term, pour ne permettre qu'à un terminal préalablement enregistré de pouvoir obtenir une identité d'utilisateur.

Sur réception du message 53 indiquant l'identité d'utilisateur user-id, le terminal 11 la stocke à l'étape 24.

La figure 6 illustre un système d'association d'une identité d'utilisateur selon un mode de réalisation de la présente invention.

5 Un tel système d'association 60 comprend une entité d'identification 12 stockant une information relative à une identité d'utilisateur et un terminal 11 selon un mode de réalisation de la présente invention. Ce dernier comprend :

- 10 - une unité d'interface radio 61 adaptée pour établir une transaction 21 avec une entité d'identification 12 et pour recevoir une information relative à une identité d'utilisateur stockée sur ladite entité d'identification, au cours de ladite transaction ;
- une unité de stockage 62 adaptée pour stocker ladite identité d'utilisateur obtenue à partir de ladite information relative à une identité d'utilisateur ; et
- 15 - une unité de gestion de stockage 63 adaptée pour effacer l'identité d'utilisateur lorsque le terminal est soumis à une action spécifique.

Lorsque le terminal est adapté pour communiquer dans le réseau de communication 31, l'unité d'interface radio 61 peut en outre être adaptée pour
20 fournir au réseau de communication 31, via le message 52, l'information d'utilisateur et pour recevoir depuis le réseau de communication 31, via le message 53, l'identité d'utilisateur.

L'unité d'interface radio 61 peut en outre être adaptée pour déterminer si l'entité d'identification 12 est située à proximité du terminal et l'unité de gestion
25 de stockage 63 peut en outre être adaptée pour décider d'effacer l'identité d'utilisateur quand l'unité d'interface radio détermine N fois consécutives que l'entité d'identification n'est pas située à proximité du terminal, N étant un nombre entier quelconque.

Le terminal selon un mode de réalisation de la présente invention est en
30 charge de fournir l'énergie à l'entité d'identification sans contact. Le terminal peut être par exemple un équipement d'extrémité d'un système de

communication, tel qu'un système de radiocommunications professionnelles mobiles ou PMR (pour 'Professional Mobile Radio' en anglais).

5 L'entité d'identification 12 peut correspondre à une carte à puce sans contact de proximité. Elle peut être par exemple une carte professionnelle portée par l'utilisateur sur sa poitrine ou dans son portefeuille, ou bien une carte d'identité, un permis de conduire ou un document de voyage.

10 On peut prévoir que l'interface radio entre le terminal 11 et l'entité d'identification 12 soit désactivée dès que l'identité d'utilisateur est stockée au niveau du terminal, excepté lorsqu'une procédure de contrôle de présence d'entité d'identification est mise en œuvre telle qu'illustrée à la figure 2.

15 En effet, dans ce cas, il peut être prévu que le terminal active alors périodiquement et temporairement son interface radio seulement pendant une période déterminée lui permettant de mettre en œuvre un contrôle de présence de l'entité d'identification dans le voisinage. En procédant ainsi, on est en mesure d'économiser de l'énergie au niveau du terminal.

REVENDICATIONS

1. Procédé d'association d'une identité d'utilisateur (user-id) à un terminal électronique (11) adapté pour offrir un service fondé sur ladite identité d'utilisateur ;
- 5 ledit procédé d'association comprenant les étapes suivantes, au niveau du terminal :
 - /1/ établir une transaction sans contact (21) avec une entité d'identification (12) ;
 - /2/ recevoir, au cours de ladite transaction, une information relative à
 - 10 une identité d'utilisateur stockée sur ladite entité d'identification ; et
 - /3/ stocker ladite identité d'utilisateur obtenue à partir de ladite information ;dans lequel l'identité d'utilisateur est effacée au niveau du terminal lorsque le terminal est soumis à une action spécifique ;
- 15 dans lequel le terminal est adapté pour communiquer dans un réseau de communication (31) ;
dans lequel une association entre l'information relative à une identité d'utilisateur et l'identification d'utilisateur est gérée au niveau du réseau de communication (31), et
- 20 dans lequel le terminal obtient l'identité d'utilisateur à l'étape /3/, selon les étapes suivantes :
 - /i/ fournir (52) au réseau de communication (31) l'information relative à l'identité d'utilisateur ;
 - /ii/ recevoir (53) depuis le réseau de communication ladite identité
 - 25 d'utilisateur.

2. Procédé d'association d'une identité d'utilisateur selon l'une quelconque des revendications précédentes, comprenant en outre les étapes suivantes au niveau du terminal (11) :
- 5 /4/ déterminer si l'entité d'identification (12) est située à proximité du terminal ;
- /5/ répéter l'étape /4/ N fois, N étant un nombre entier ; et
- /6/ décider d'effacer l'identité d'utilisateur au niveau du terminal si on détermine N fois consécutives que l'entité d'identification n'est pas située à
- 10 proximité du terminal.
3. Procédé d'association d'une identité d'utilisateur selon l'une quelconque des revendications précédentes, dans lequel, après l'étape /3/, le terminal émet un signal sonore ou lumineux.
- 15
4. Procédé d'association d'une identité d'utilisateur selon l'une quelconque des revendications précédentes, dans lequel le terminal est adapté pour communiquer dans un réseau de communication (31) ; et dans lequel, après l'étape /3/, le terminal s'enregistre auprès du réseau de
- 20 communication (31) sur la base de l'identité d'utilisateur.
5. Procédé d'association d'une identité d'utilisateur selon l'une quelconque des revendications précédentes, dans lequel le terminal est adapté pour communiquer dans un réseau de communication (31) ; et
- 25 dans lequel, avant l'étape /3/, le terminal s'enregistre auprès du réseau de communication (31) sur la base d'une identité du terminal, puis, après l'étape /3/, sur la base de l'identité d'utilisateur.
6. Procédé d'association selon l'une quelconque des revendications
- 30 précédentes, dans lequel les étapes /1/ à /3/ sont mises en œuvre lors d'un mouvement d'utilisateur du terminal consistant à rapprocher ledit terminal de l'entité d'identification.

7. Terminal (11) adapté pour offrir un service fondé sur une identité d'utilisateur ; ledit terminal étant adapté pour communiquer dans un réseau de communication (31) ;
- 5 une association entre l'information relative à une identité d'utilisateur et l'identification d'utilisateur étant gérée au niveau du réseau de communication (31),
- ledit terminal comprenant :
- 10 - une unité d'interface radio (61) adaptée pour établir une transaction (21) sans contact avec une entité d'identification (12) et pour recevoir une information relative à une identité d'utilisateur stockée sur ladite entité d'identification, au cours de ladite transaction ;
 - 15 - une unité de stockage (62) adaptée pour stocker ladite identité d'utilisateur obtenue à partir de ladite information ;
 - une unité de gestion de stockage (63) adaptée pour effacer l'identité d'utilisateur lorsque le terminal est soumis à une action spécifique ;
 - 20 - des moyens pour fournir (52) au réseau de communication (31) l'information relative à l'identité d'utilisateur ; et
 - des moyens pour recevoir (53) depuis le réseau de communication ladite identité d'utilisateur.
8. Terminal (11) selon la revendication 7, étant en outre adapté pour
- 25 communiquer dans un réseau de communication (31), dans lequel l'unité d'interface radio (61) est en outre adaptée pour fournir (52) au réseau de communication (31) l'information d'utilisateur et pour recevoir (53) depuis le réseau de communication ladite identité d'utilisateur.
- 30 9. Terminal (11) selon la revendication 7 ou 8, dans lequel l'unité d'interface radio est en outre adaptée pour déterminer si l'entité d'identification (12) est située à proximité du terminal ; et

dans lequel l'unité de gestion de stockage (63) est en outre adaptée pour décider d'effacer l'identité d'utilisateur quand l'unité d'interface radio détermine N fois consécutives que l'entité d'identification n'est pas située à proximité du terminal, N étant un nombre entier quelconque.

5

10. Système d'association (60) d'une identité d'utilisateur, comprenant un terminal (11) selon l'une quelconque des revendications 7 à 9 et une entité d'identification (12) sur laquelle est stockée une information relative à une identité d'utilisateur.

10

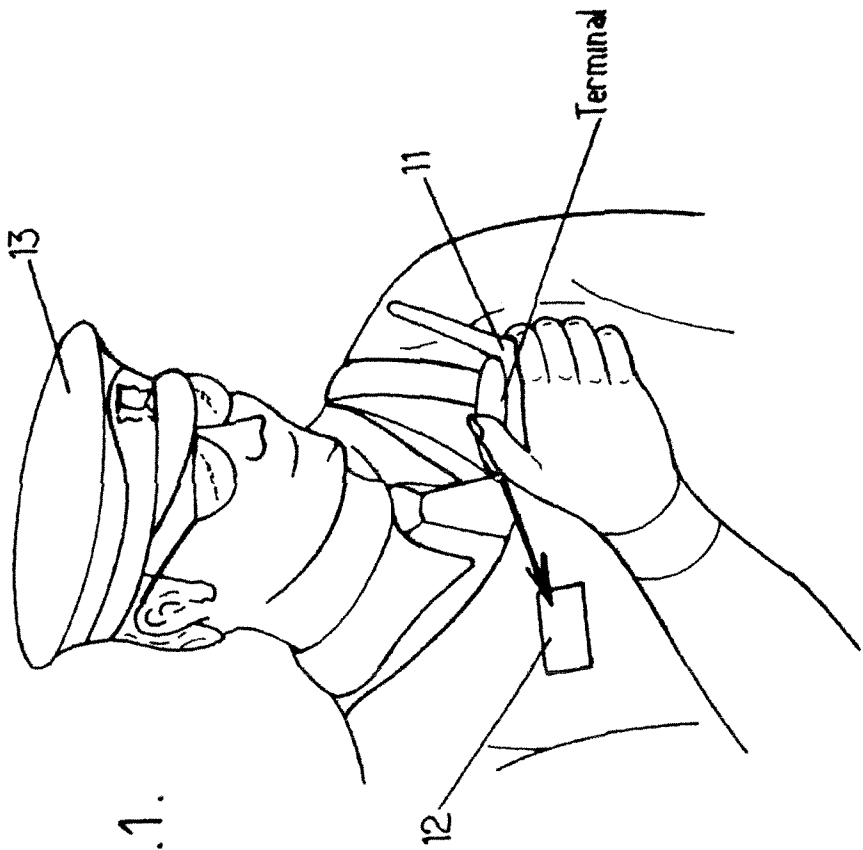


FIG.1.

2/4

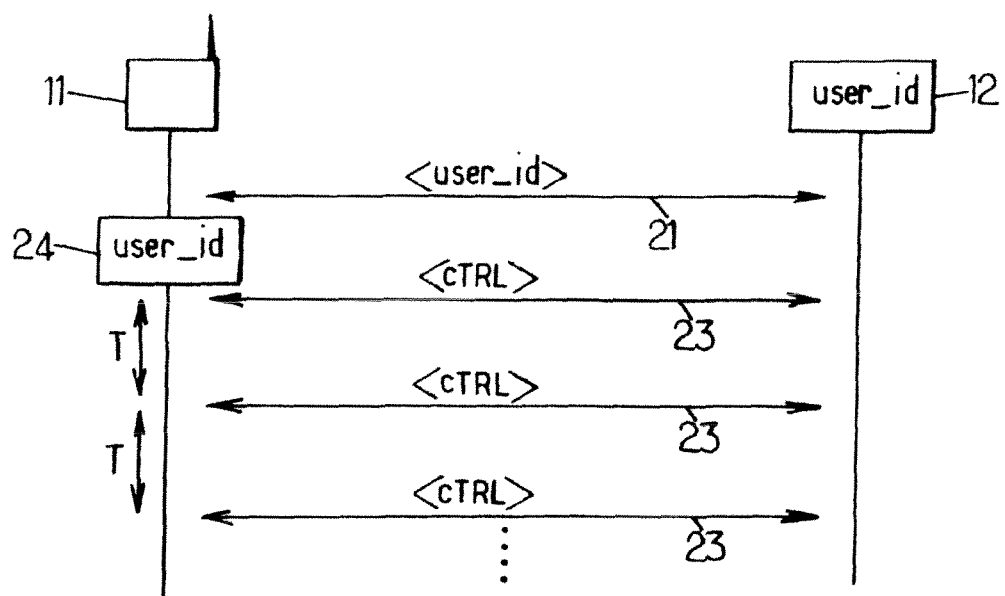


FIG.2.

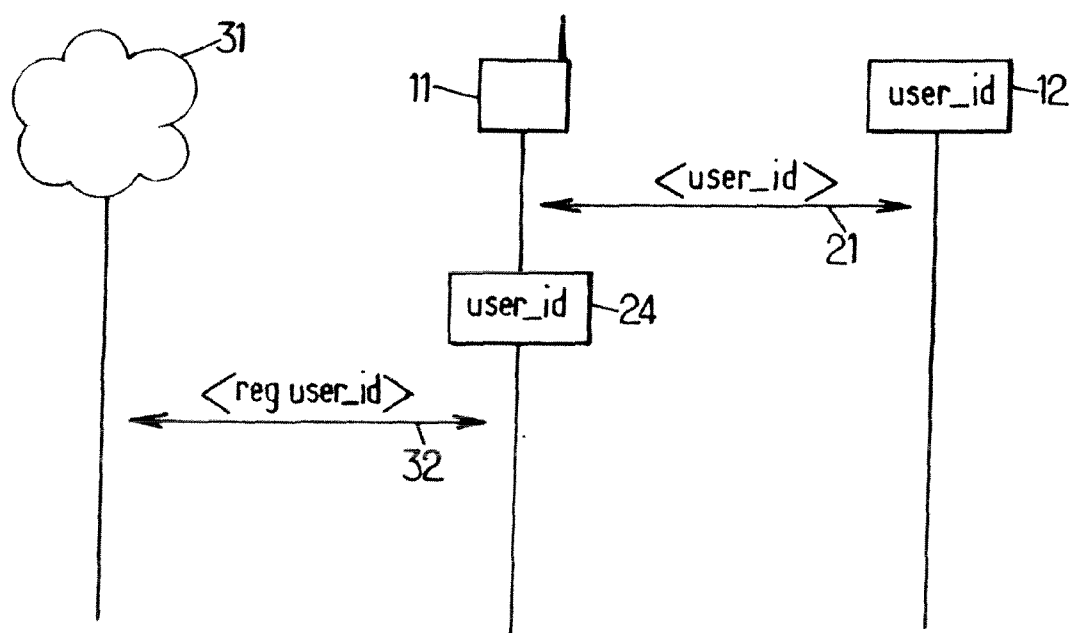
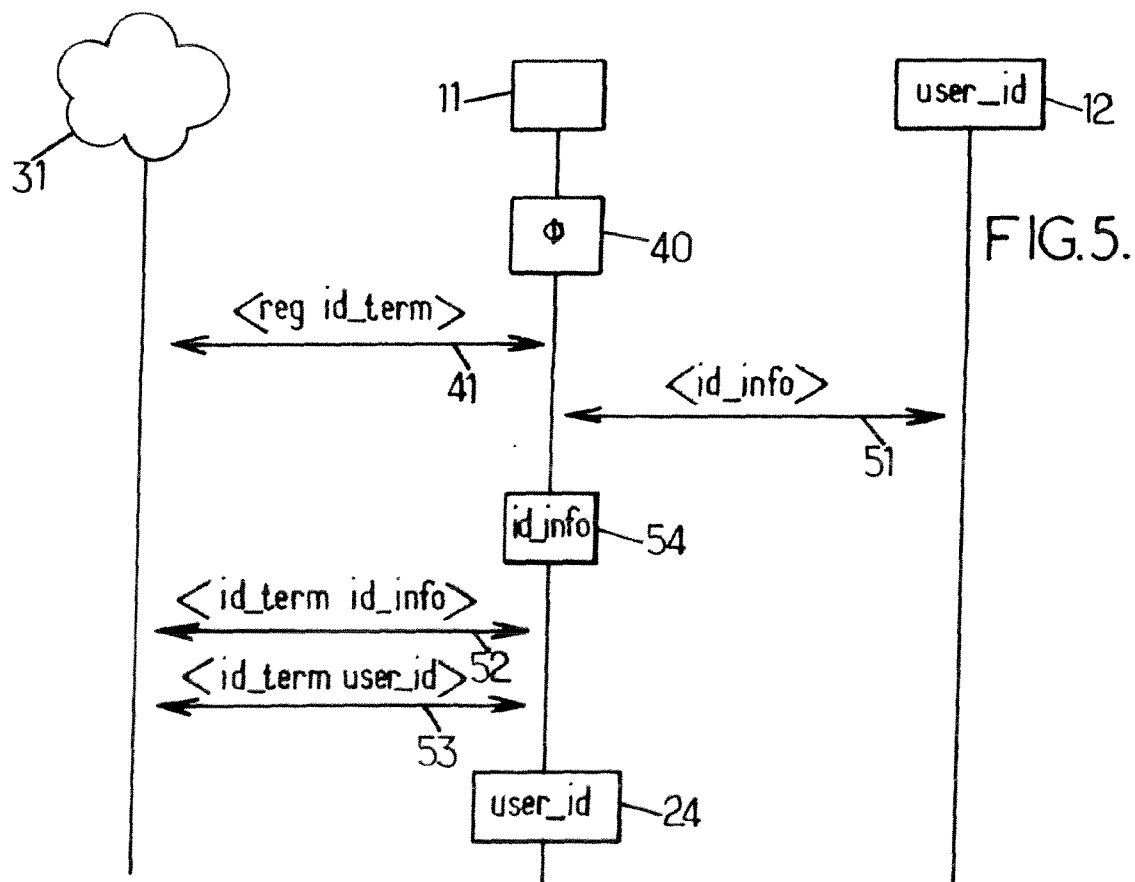
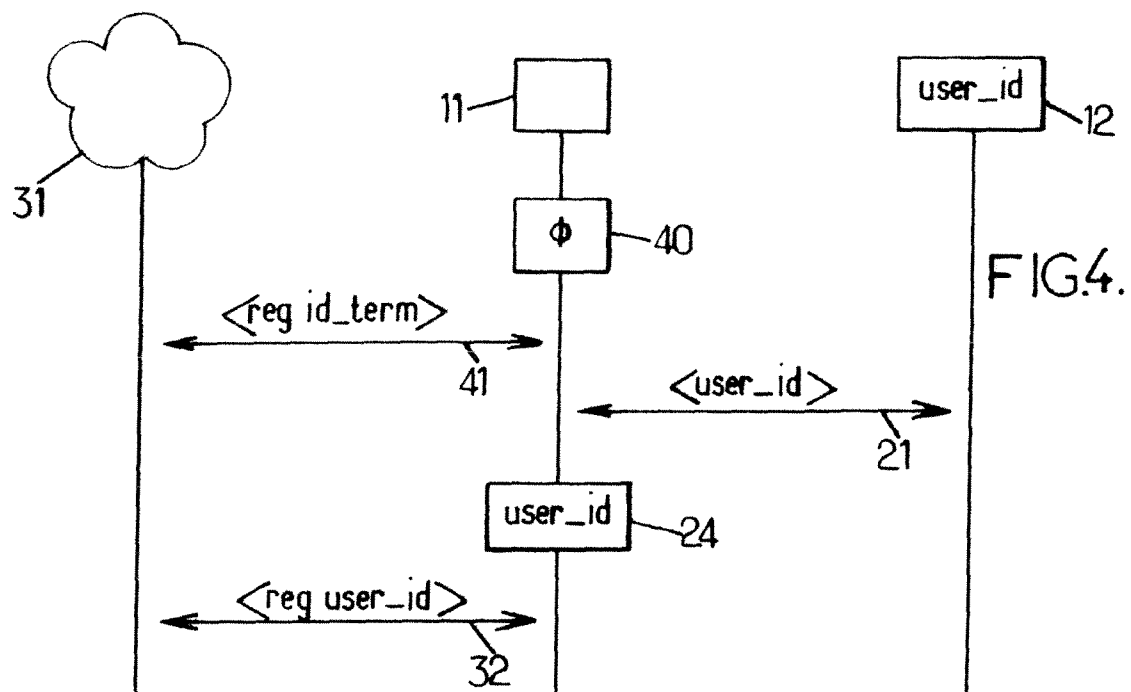


FIG.3.

3/4



4/4

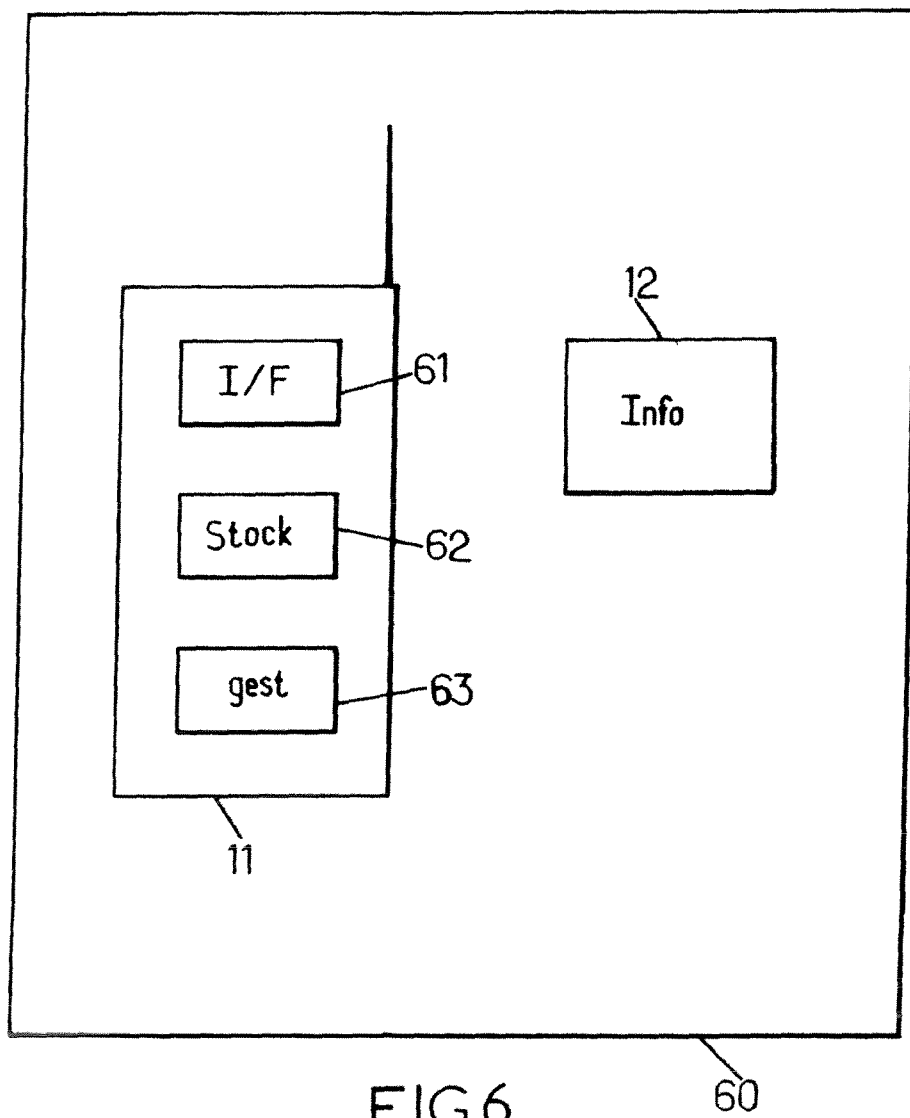


FIG.6.