(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 282 297 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
09.02.2011 Bulletin 2011/06

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Numéro de dépôt: **09166002.7**

(22) Date de dépôt: **21.07.2009**

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Etats d'extension désignés:
AL BA RS

(71) Demandeur: **OPENWAYS SAS**
75016 Paris (FR)

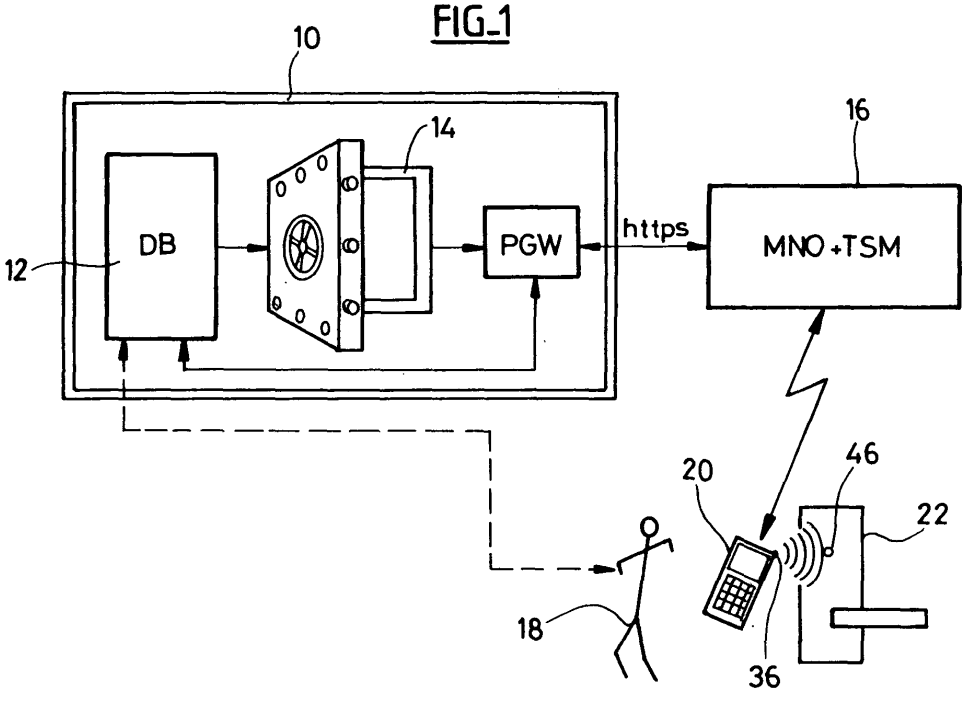
(72) Inventeur: **Metivier, Pascal**
78810 Feucherolles (FR)

(74) Mandataire: **Dupuis-Latour, Dominique et al**
SEP Bardehle Pagenberg Dost Altenburg Geissler
10, boulevard Haussmann
75009 Paris (FR)

(54) **Système sécurisé de commande d'ouverture de dispositifs de serrure par accréditions acoustiques chiffrées**

(57) Ce système met en oeuvre un téléphone mobile (20) à disposition d'un utilisateur (18) habilité à ouvrir une serrure (22). Un site gestionnaire (10) distant comprend une base de données (12) de serrures et d'utilisateurs habilités et identifiés par leur numéro de téléphone mobile, ainsi qu'un générateur (14) de données d'accréditation. Les accréditations sont des accréditations acoustiques chiffrées en forme de signaux audio à usage unique, propres à permettre l'ouverture des serrures répertoriés dans la base de données. Le système comprend des moyens de transmission sécurisée des accréditations acoustiques chiffrées du site gestionnaire au téléphone mobile de l'utilisateur habilité correspondant via un opérateur de réseau mobile (16). La serrure (22) comprend un transducteur électroacoustique apte à capter les accréditations acoustiques reproduites par le téléphone préalablement placé à proximité de la serrure, ainsi que des moyens pour reconnaître, analyser et authentifier les accréditations acoustiques captées, et commander le déverrouillage des organes mécaniques sur reconnaissance d'une accréditation conforme.

FIG_1



EP 2 282 297 A1

Description

[0001] L'invention concerne les serrures commandées au moyen d'une clé dématérialisée et chiffrée, cette clé étant véhiculée par un objet portatif détenu par l'utilisateur.

[0002] L'objet portatif, lorsqu'il est approché de la serrure, joue le rôle d'une clé permettant de commander l'ouverture de la serrure au moyen d'une donnée chiffrée, ci-après désignée "accréditation" (*credential*). L'accréditation peut être protégée par mise en oeuvre de diverses techniques de codage et de cryptage implémentées dans la serrure et/ou dans l'objet portatif, et permettant de protéger la serrure et l'objet portatif contre des manipulations frauduleuses, et de sécuriser la communication entre ces deux éléments.

[0003] On connaît de nombreux systèmes de cartes ou badges à microcircuit mettant en oeuvre un couplage sans fil non galvanique avec la serrure, généralement un couplage par induction. Ce couplage assure une communication bidirectionnelle entre serrure et badge, permettant notamment à la serrure de lire dans la mémoire du badge la donnée d'accréditation et de commander l'ouverture si cette donnée est reconnue conforme.

[0004] L'un des inconvénients de cette technique est la nécessité de disposer d'un objet portatif spécifique, qui doit être remis à l'utilisateur et que celui-ci doit conserver avec lui.

[0005] Ceci aboutit en outre à la multiplication des objets portatifs, chacun correspondant à une serrure différente (domicile, bureau, porte d'immeuble, garage, etc.), ce qui rend au final l'ensemble malcommode et sujet au risque d'oublis.

[0006] De plus, le système est un système figé, dans la mesure où si l'on souhaite mettre à jour les habilitations, supprimer des habilitations existantes ou en créer de nouvelles, il faut soit procéder à l'échange de l'objet portatif, soit mettre à jour la mémoire de celui-ci au moyen d'un protocole et/ou d'un lecteur spécifique, avec toujours nécessité de manipulation physique et de déplacements.

[0007] Une technique développée récemment consiste à utiliser à la place d'un badge dédié un téléphone mobile équipé d'une puce NFC (*Near Field Communication,* communication en champ proche) et d'une antenne NFC, la carte UICC ("carte SIM") du téléphone étant utilisée comme élément de sécurité. La mise en communication du téléphone avec un site gestionnaire permet de modifier aisément les accréditations conservées dans le téléphone ou dans la carte SIM, de procéder à des vérifications en ligne, de modifier les éléments de sécurité ou d'en télécharger de nouveaux, etc.

[0008] L'inconvénient majeur de cette technique est qu'elle nécessite un téléphone spécialement équipé pour mettre en oeuvre la technologie NFC. Ces technologies existent et sont tout à fait au point, mais on ne trouve aujourd'hui qu'un très faible parc d'appareils, empêchant toute généralisation rapide du système.

[0009] L'un des buts de l'invention est de proposer une technique de gestion et de commande de serrures présentant un niveau de sécurité maximal, une très grande souplesse de mise en oeuvre, et qui soit utilisable avec n'importe quel téléphone mobile conventionnel, non nécessairement muni de circuits NFC, en d'autres termes une technique qui soit utilisable avec un téléphone préexistant, sans que l'utilisateur n'ait besoin de changer son appareil pour un modèle NFC, et sans recours à un objet portatif additionnel tel que badge ou carte.

[0010] Le système de l'invention pourra être ainsi immédiatement généralisable au plus grand nombre, utilisable par tout un chacun à partir d'un téléphone de modèle standard, non modifié, mais en bénéficiant de toute la sécurité et de tout la souplesse propre aux techniques cryptographiques modernes.

[0011] Le principe de l'invention repose sur l'utilisation d'accréditations acoustiques chiffrées. Ces accréditations acoustiques se présentent par exemple sous forme d'une série codée de tonalités (tonalités DTMF ou autres), émises par le haut-parleur d'un dispositif émetteur et captées par le microphone d'un dispositif récepteur.

[0012] Dans le cas de l'invention, ces accréditations acoustiques chiffrées sont des accréditations "descendantes", c'est-à-dire qu'elles sont issues d'un site gestionnaire distant, et transmises au téléphone mobile de l'utilisateur par le réseau de l'opérateur de téléphonie. Pour utiliser l'accréditation, l'utilisateur approche son téléphone de la serrure et déclenche l'émission de la série de tonalités correspondant à l'accréditation acoustique chiffrée par le haut-parleur de son téléphone, de manière que ces tonalités puissent être captées par un microphone incorporé ou couplé à la serrure. Cette dernière décode l'accréditation, la vérifie et en cas de conformité déverrouille les organes mécaniques.

[0013] L'utilisation d'accréditations acoustiques n'est pas en elle-même nouvelle, elle a déjà été proposée dans d'autres contextes et pour d'autres applications, par exemple par le WO 2008/107595 A2 (Tagattitude).

[0014] Ce document décrit une technique de sécurisation de l'accès logique à un réseau informatique par un terminal distant, par exemple par un ordinateur relié à ce réseau via internet. L'utilisateur se connecte au réseau avec son ordinateur, allume en même temps son téléphone mobile, et appelle au moyen de celui-ci un site de contrôle interfacé avec le réseau auquel l'accès est demandé. Pour vérifier l'habilitation de l'utilisateur, le réseau envoie un signal sonore (l'accréditation acoustique) vers l'ordinateur distant qui vient de se connecter, signal qui est reproduit par le haut-parleur de l'ordinateur. L'utilisateur ayant placé son téléphone devant ce haut-parleur, ce signal sonore est capté par le téléphone, transmis au site de contrôle distant via l'opérateur de réseau téléphonique mobile et "écouté" par le site de contrôle, qui peut alors vérifier l'accréditation et autoriser l'accès au réseau informatique par le terminal. On notera que dans ce cas il s'agit d'une accréditation

"remontante" : l'accréditation acoustique est captée par le microphone du téléphone qui la retransmet au site de contrôle. Connaissant l'origine de l'appel téléphonique, le site de contrôle peut identifier l'utilisateur par le biais du téléphone mobile utilisé pour cette opération, et ainsi autoriser l'accès logique au réseau par le terminal situé à proximité du téléphone ainsi identifié.

[0015] Plus précisément, la présente invention concerne un système sécurisé de commande d'ouverture de dispositifs de serrure, comportant de manière en elle-même connue : au moins un dispositif de serrure muni de circuits électroniques pour la commande d'organes mécaniques de verrouillage/déverrouillage ; un téléphone mobile à disposition d'un utilisateur habilité à ouvrir le dispositif de serrure ; un site gestionnaire distant ; et un opérateur de réseau mobile, couplé au site gestionnaire et au téléphone mobile.

[0016] De façon caractéristique de l'invention, le site gestionnaire distant comprend une base de données de dispositifs de serrure et d'utilisateurs habilités, avec pour chaque utilisateur un identifiant unique associé à un numéro de téléphone mobile, et des données de droits d'accès et de conditions d'utilisation, et un générateur de données d'accréditation, les accréditations étant des accréditations acoustiques chiffrées en forme de signaux audio à usage unique, propres à permettre l'ouverture des dispositifs de serrure répertoriés dans la base de données. Par ailleurs : le système comprend des moyens de transmission sécurisée desdites données d'accréditation du site gestionnaire au téléphone mobile de l'utilisateur habilité correspondant ; le téléphone comprend un transducteur électro-acoustique apte à reproduire lesdites accréditations acoustiques ; le dispositif de serrure comprend un transducteur électro-acoustique apte à capter les accréditations acoustiques reproduites par le transducteur du téléphone préalablement placé à proximité du dispositif de serrure ; et le dispositif de serrure comprend des moyens pour reconnaître, analyser et authentifier les accréditations acoustiques captées par le transducteur, et commander le déverrouillage des organes mécaniques sur reconnaissance d'une accréditation conforme.

[0017] Dans une première forme de mise en oeuvre, le système comporte des moyens propres, sur envoi d'une requête par le téléphone mobile au site gestionnaire, à : vérifier l'habilitation de l'utilisateur dans la base de données du site ; générer une accréditation acoustique par le générateur du site ; et transmettre cette accréditation au téléphone, pour reproduction directe par le transducteur de celui-ci préalablement placé à proximité du transducteur du dispositif de serrure.

[0018] Dans une deuxième forme de mise en oeuvre, le système comporte des moyens propres, sur envoi d'une requête par le téléphone mobile au site gestionnaire, à : vérifier l'habilitation de l'utilisateur dans la base de données du site ; générer au moins une accréditation acoustique par le générateur du site ; transmettre au téléphone cette accréditation, ou ces accréditations, par mise en oeuvre d'une appliquette interne du téléphone apte à en exécuter le téléchargement et la mémorisation dans une mémoire du téléphone ; puis, dans un second temps, activer l'appliquette interne pour reproduction de l'accréditation, ou de l'une des accréditations, par le transducteur du téléphone préalablement placé à proximité du transducteur du dispositif de serrure.

[0019] Dans une troisième forme de mise en oeuvre, le téléphone comprend une appliquette interne formant, en combinaison avec une clé cryptographique, générateur cryptographique, et la donnée d'accréditation transmise par le site distant au téléphone est ladite clé cryptographique, de manière à permettre, sur commande de l'utilisateur, la génération de l'accréditation acoustique par l'appliquette interne et sa reproduction par le transducteur de celui-ci préalablement placé à proximité du transducteur du dispositif de serrure.

[0020] Dans ce dernier cas, la clé cryptographique, et éventuellement l'appliquette, peuvent être conservées dans un mémoire d'une carte à microcircuit sécurisée du téléphone, et le système peut comprendre en outre des moyens pour conditionner la génération de l'accréditation acoustique par l'appliquette interne du téléphone à la mise à jour par le site distant, ou par l'opérateur de réseau mobile, d'une donnée de validation nécessaire pour que l'appliquette puisse continuer à opérer ladite génération.

[0021] Dans une quatrième forme de mise en oeuvre, le système comporte des moyens propres, sur envoi d'une requête par le téléphone mobile au site gestionnaire, ou à l'initiative du site gestionnaire, à : vérifier l'habilitation de l'utilisateur dans la base de données ; générer au moins une accréditation acoustique et convertir cette accréditation, ou ces accréditations, en un fichier audio ; transmettre au téléphone ce fichier audio pour téléchargement et mémorisation dans une mémoire du téléphone ; puis, dans un second temps, reproduire le fichier audio par le transducteur du téléphone préalablement placé à proximité du transducteur du dispositif de serrure.

[0022] Selon diverses caractéristiques subsidiaires avantageuses :

- dans le cas des première et quatrième formes de mise en oeuvre précitées, le système comprend en outre des moyens pour générer automatiquement ladite requête à partir d'un seuil prédéfini d'accréditations restant mémorisées dans le téléphone, afin d'opérer un rechargement de la mémoire du téléphone par de nouvelles accréditations ;
- le système comprend en outre des moyens pour conditionner la reproduction de l'accréditation acoustique par le transducteur du téléphone à la présentation préalable d'une donnée personnelle de validation délivrée par l'utilisateur au téléphone ;
- le dispositif de serrure comprend un transducteur électro-acoustique apte à reproduire des signaux acoustiques en retour, générés par le dispositif de

serrure et codés par des données d'état ou d'historique propres au dispositif de serrure ; et le téléphone comprend un transducteur électro-acoustique apte à capter lesdits signaux en retour ;

- dans ce dernier cas, le téléphone peut comprendre en outre des moyens pour décoder lesdits signaux en retour et afficher le cas échéant à destination de l'utilisateur un message d'alerte fonction desdites données d'état ou d'historique propres au dispositif de serrure, et/ou comprendre des moyens pour transmettre au site gestionnaire lesdits signaux en retour avec lesdites données d'état ou d'historique propres au dispositif de serrure ;
- lorsque l'utilisateur est habilité pour une pluralité de dispositifs de serrure différents, le téléphone est apte à reproduire en une salve unique une pluralité d'accréditations, ladite salve contenant une accréditation correspondant à chacune des dispositifs de serrure pour lesquelles l'utilisateur est habilité ;
- le téléphone comprend en outre une commande rapide d'obtention et/ou de reproduction de l'accréditation par appui sur un bouton dédié du téléphone, ou par activation d'une icône spécifique d'une surface tactile du téléphone ;
- le système est également apte à commander l'activation/désactivation d'une installation d'alarme sur reconnaissance d'une accréditation conforme.

[0023] On va maintenant décrire divers exemples de mise en oeuvre de l'invention, en référence aux dessins annexés où les mêmes références numériques désignent d'une figure à l'autre des éléments identiques ou fonctionnellement semblables.

La Figure 1 illustre de façon schématique les principaux éléments contribuant au fonctionnement du système selon l'invention.

La Figure 2 illustre plus précisément, sous forme de schéma par blocs, les principaux organes constitutifs du téléphone mobile et de la serrure avec laquelle ce dernier est couplé.

La Figure 3 illustre la manière d'appliquer l'invention à la gestion d'un ensemble de chambres d'hôtel, de façon entièrement automatique et sans qu'il y ait besoin de distribuer aux clients des cartes, badges ou clés.

[0024] On va expliquer le principe de mise en oeuvre de l'invention, en référence aux figures 1 et 2.

[0025] L'un des éléments essentiels de l'invention est un site gestionnaire sécurisé 10 centralisant dans une base de données DB 12 les informations permettant de recenser et d'identifier un certain nombre de dispositifs de serrures et d'utilisateurs habilités pour chacun de ces dispositifs de serrures. Pour chaque utilisateur, la base de données répertorie un numéro de téléphone mobile unique associé à cet utilisateur, ainsi que des données de droit d'accès et de conditions d'utilisation (accès réservé à certains jours ou certaines plages horaires, date d'expiration d'un droit accès, etc.). Chaque serrure, quant à elle, est répertoriée au moyen d'un identifiant UID (*Unique IDentifier*), qui est attribué de manière unique.

[0026] Le site gestionnaire 10 comprend également un moteur cryptographique formant générateur 14 de données d'accréditation.

[0027] De façon caractéristique de l'invention, les "données d'accréditation" (*credentials*) sont des accréditations acoustiques chiffrées en forme de signaux audio à usage unique, par exemple (mais de façon non limitative) constitués d'une succession de tonalités doubles DTMF. Ces signaux audio sont conçus de manière à pouvoir être véhiculés par les canaux de transmission audio (canal voix) d'un réseau de téléphonie mobile après numérisation.

[0028] Le site gestionnaire 10 est couplé à un réseau d'un opérateur de téléphonie mobile ou MNO (*Mobile Network Operator*) par l'intermédiaire d'une passerelle téléphonique audio PGW (*Phone GateWay*) et d'une liaison sécurisée, par exemple une liaison IP de type *https.*

[0029] Le réseau de téléphonie mobile 16 est utilisé de façon conventionnelle par ses divers abonnés, chaque utilisateur 18 étant en possession d'un téléphone mobile 20 qui lui est propre, individualisé par les informations de la carte SIM contenue dans l'appareil téléphonique ou par un autre élément unique si le téléphone opère sans carte SIM. Ainsi, lorsqu'il utilise son téléphone mobile personnel, un utilisateur est reconnu et identifié par le réseau 16 au moyen de son numéro d'abonné, et donc de la même façon par le site gestionnaire 10.

[0030] La sécurisation de la liaison entre le réseau mobile 16 et le téléphone mobile 20 peut être opérée par l'intermédiaire d'un fournisseur de services de confiance ou TSM (*Trusted Service Manager*), propre à assurer de manière efficace et sûre les diverses procédures que l'on décrira d'échange ou de téléchargement d'informations entre le site gestionnaire 10 et le téléphone mobile 20 via l'opérateur de réseau mobile 16.

[0031] Dans le cas d'une clé matérialisée par un support tel qu'une carte ou un badge, une part importante de la sécurité est assurée par la remise physique de cet objet à l'utilisateur légitime, de la même façon que la remise d'un jeu de clés. En revanche, dans le cadre de l'invention, l'objet utilisé est un téléphone mobile, donc un objet banalisé. Mais celui-ci est reconnu et authentifié par la carte SIM qu'il contient (ou par un autre élément unique) et qui, surtout, identifie l'utilisateur via son numéro de téléphone (numéro d'abonné). Le site gestionnaire 10 peut donc ainsi identifier tel téléphone auquel il a été relié via l'opérateur de réseau mobile 16 comme étant bien celui de l'utilisateur habilité 18, répertorié dans sa base de données 12.

[0032] Le principe de base de l'invention consiste à faire reproduire par le haut-parleur du téléphone mobile 20, en tant que signal audio, l'accréditation acoustique

chiffrée générée par le générateur cryptographique 14 et transmise sous forme de signal vocal par l'intermédiaire de la passerelle téléphonique PGW et l'opérateur du réseau mobile 16.

[0033] Cette accréditation reproduite par le téléphone mobile 20 est destinée à être captée par un microphone d'un dispositif de serrure 22 de manière à commander l'ouverture de ce dispositif de serrure.

[0034] Par "dispositif de serrure" on entendra non seulement une serrure *stricto sensu,* c'est-à-dire un mécanisme posé par exemple sur une porte pour en condamner l'ouverture, mais également tout dispositif permettant d'aboutir à un résultat comparable, par exemple un canon de serrure considéré isolément, ou un dispositif de verrouillage plus spécifique comprenant divers organes non regroupés dans un même coffre de serrure, le but final étant d'obtenir la condamnation par des moyens mécaniques de l'accès physique à un lieu ou espace donné, et l'accès à ce lieu ou espace par déverrouillage du dispositif de serrure, sur commande d'un utilisateur, après vérification que cet utilisateur dispose bien des droits d'accès (i) qui lui sont propres et (ii) qui sont propres au dispositif de serrure.

[0035] Pour la simplicité de la description, on parlera par la suite simplement de "serrure", mais ce terme doit être entendu dans son sens le plus large, sans aucun caractère restrictif à un type d'équipement particulier.

[0036] La Figure 2 illustre, sous forme de schéma par blocs, les principaux organes du téléphone mobile 20 et de la serrure 22.

[0037] Le téléphone 20 comporte un microcontrôleur 24 couplé à divers organes périphériques tels que circuit d'émission/réception 26, afficheur 28, clavier 30, mémoire de données 32, carte UICC (*Universal Integrated Circuit Card,* correspondant à la "carte SIM" pour les fonctions de téléphonie GSM) 34, et transducteur acoustique 36.

[0038] La serrure 22, quant à elle, comprend un microcontrôleur 38 ainsi qu'un système électromécanique 40 permettant de commander le déverrouillage d'un pêne ou d'une poignée 42 sur ordre du microcontrôleur 38. La serrure comporte ses propres moyens d'alimentation sous forme d'une batterie 44, de manière à la rendre autonome sur le plan électrique. Une alimentation externe est néanmoins possible

[0039] La serrure 22 est par ailleurs individualisée au moyen d'un identifiant unique UID (*Unique IDentifier*), qui est un identifiant programmable, répertorié dans la base de données 12 du site gestionnaire 10, permettant de reconnaître telle ou telle serrure entre toutes, de manière unique.

[0040] De façon caractéristique, la serrure 22 est en outre pourvue d'un transducteur acoustique sous forme d'un microphone 46 permettant de capter les signaux sonores environnants, en particulier l'accréditation acoustique qui sera reproduite par le haut-parleur 36 du téléphone 20, et de transformer les signaux acoustiques captés en signaux électriques appliqués au microcontrôleur 38 pour décodage, vérification, et commande éventuelle du déverrouillage des organes mécaniques 40.

Modes de mise en oeuvre de l'invention

[0041] On va maintenant décrire plusieurs modes opératoires pour la mise en oeuvre de l'invention avec les différents éléments du système que l'on vient de décrire.

[0042] Le but premier de l'invention est de permettre à l'utilisateur 18 de reproduire au moyen du haut-parleur 36 (haut-parleur primaire ou haut-parleur secondaire, en mode "conférence") de son téléphone mobile 20 l'accréditation acoustique chiffrée générée par le site distant 10.

[0043] Pour cela, l'utilisateur place son téléphone mobile 20 à proximité du microphone 46 de la serrure 22 qu'il souhaite déverrouiller et déclenche l'émission, sous forme de signal sonore, de l'accréditation acoustique. Celle-ci, captée par le microphone 46 de la serrure, sera analysée par le microcontrôleur 38 qui, en cas de conformité, commandera le déverrouillage des organes mécaniques 40.

[0044] Il s'agit de permettre à l'utilisateur, détenteur du numéro du téléphone mobile 20 connu de la base de données 12, de prouver à la serrure 22, également connue de cette même base de données 12, qu'il a bien l'identité qu'il proclame, et qu'il bénéficie des droits d'accès permettant l'ouverture de cette serrure. Le signal sonore reproduit constitue ainsi un justificatif de l'identité de l'utilisateur et de ses droits d'ouverture, d'où la terminologie "accréditation acoustique". Cette accréditation acoustique est en outre chiffrée (par des moyens cryptographiques en eux-mêmes connus), et à usage unique afin d'éviter toute fraude, notamment par duplication, car il serait très aisé d'enregistrer le signal acoustique et de le reproduire ensuite à volonté.

1°) <u>Mode en ligne (délivrance directe de l'accréditation)</u>

[0045] Lorsqu'il souhaite obtenir l'ouverture de la serrure 22 devant laquelle il se trouve, l'utilisateur 18 entre en contact avec le site gestionnaire 10 par tout moyen approprié. Ceci peut être obtenu par l'appel d'un numéro téléphonique, ou par l'envoi d'un message (SMS, MMS, e-mail, messagerie instantanée, etc.) au serveur, qui rappellera le téléphone de l'utilisateur pour lui délivrer l'autorisation sous forme d'une accréditation acoustique chiffrée. La transmission de cette accréditation est exécutée immédiatement et directement. La transmission de l'accréditation acoustique peut également être exécutée par un procédé de type "call back" : dans ce cas, l'utilisateur entre en contact téléphonique avec le site gestionnaire, qui ne lui répond pas immédiatement, mais après raccrochage fait sonner le téléphone mobile 20 pour que l'utilisateur établisse à nouveau le contact avec le site, et c'est à ce moment que l'accréditation acoustique lui est délivrée. Dans ce mode de réalisation, quelle que soit la manière dont l'utilisateur entre en contact avec le site distant, celui-ci délivre l'accréditation acoustique direc-

tement à l'utilisateur, "en ligne", sans stockage intermédiaire. Ce mode de réalisation est particulièrement simple à mettre en oeuvre, dans la mesure où il suffit d'utiliser l'infrastructure existante, sans adaptation préalable du téléphone, notamment sans aucun besoin de charger une appliquette ou *applet,* notamment de type *midlet* ou *cardlet.* L'invention peut être ainsi mise en oeuvre avec n'importe quel type de téléphone mobile, même très simple, et sans aucune intervention préalable sur celui-ci. Un autre avantage réside dans la possibilité de vérifier en temps réel la validité de l'accréditation, avec par exemple la possibilité de prendre en compte immédiatement une "liste noire" d'utilisateurs ou de serrures. On notera en particulier que, si la serrure est une serrure autonome et indépendante comme cela est le plus souvent le cas, il ne serait pas possible d'obtenir un échange d'informations entre le serveur et la serrure par le biais de cette dernière.

[0046] De plus, grâce à ce mode en ligne, il est possible de disposer au niveau du site gestionnaire d'un grand nombre d'informations sur l'utilisation faite de l'accréditation acoustique, notamment la date et l'heure de l'utilisation, et éventuellement la situation géographique de l'utilisateur (par identification de la cellule du réseau d'où l'utilisateur appelle).

[0047] En revanche, ce mode implique de disposer d'un accès au réseau mobile, ce qui n'est pas toujours possible (parkings souterrains, zones non couvertes, etc.). D'autre part il ne permet pas en principe de disposer, au choix de l'utilisateur, de plusieurs accréditations correspondant à plusieurs serrures possibles, dans la mesure où il est nécessaire d'avoir une correspondance "un pour un" entre accréditation et serrure.

2°) Mode semi-en ligne (mode en ligne différé avec téléchargement)

[0048] Ce mode est utilisable notamment si l'accès au réseau n'est pas assuré au moment de l'utilisation. Dans ce cas, l'utilisateur se connecte à l'avance au site gestionnaire et reçoit de celui-ci un nombre prédéterminé d'accréditations acoustiques. Ces accréditations sont stockées de façon sûre dans le téléphone ou dans une mémoire périphérique du téléphone (par exemple une carte SD ou MicroSD).

[0049] Lorsque l'utilisateur veut reproduire une accréditation acoustique pour ouvrir une serrure, il lance une application intégrée à son téléphone qui recherche la première accréditation parmi celles qui ont été stockées, la reproduit pour ouvrir la porte, puis la supprime de la mémoire. Et ainsi de suite pour utiliser les accréditations suivantes.

[0050] L'application permettant cette mise en oeuvre est une appliquette conservée dans le téléphone, préalablement envoyée à celui-ci par l'opérateur de réseau mobile, ou bien par téléchargement sur un support externe (carte SD ou MicroSD), ou encore via une connexion internet. Dans le cas d'un téléchargement via l'opérateur de réseau mobile, le site gestionnaire aura envoyé au préalable un message par exemple de type "push SMS" ou "WAP push" au téléphone, afin d'identifier la marque et le modèle de celui-ci et présenter à l'utilisateur un lien permettant le téléchargement de l'appliquette.

[0051] Lorsque la provision d'accréditations mémorisées dans le téléphone a été épuisée, ou est en voie d'épuisement, et que l'utilisateur est à nouveau capable d'accéder au réseau, cette réserve d'accréditations est rechargée, pour permettre des utilisations ultérieures.

[0052] Il est possible de bénéficier de la liaison au réseau pour, au même moment, faire remonter vers le site gestionnaire un certain nombre d'informations, notamment un historique daté de l'utilisation des accréditations précédentes.

[0053] Pour révoquer un utilisateur, plusieurs solutions sont envisageables :

- attente de l'expiration des accréditations (chaque accréditation étant affectée d'une date limite d'utilisation) ;
- blocage de la fonction de rechargement pour ce téléphone ;
- envoi à la serrure, par le téléphone mobile d'un autre utilisateur, d'une accréditation spécifique de révocation, qui sera conservée dans la serrure pour empêcher le fonctionnement de celle-ci lorsque l'utilisateur révoqué tentera d'en obtenir l'ouverture ;
- programmation spécifique de la serrure, avec déplacement et intervention d'un administrateur qui supprimera les droits d'accès de l'utilisateur pour cette serrure.

3°) Mode hors ligne

[0054] Dans ce mode de mise en oeuvre, les accréditations acoustiques sont générées localement, par le téléphone lui-même. A cet effet, le téléphone contient une appliquette ou *applet,* notamment de type *cardlet* (stockée dans la carte UICC 34) ou *midlet* (stockée dans la mémoire 32 de l'appareil téléphonique). Cette appliquette est téléchargée par tout moyen approprié, de la même manière que celle utilisée dans le mode de mise en oeuvre précédent : téléchargement via l'opérateur mobile, via internet, etc., ou bien préchargée dans le téléphone à l'acquisition de celui-ci.

[0055] Le site gestionnaire 10 envoie au téléphone 20 une "donnée d'accréditation", qui ici n'est plus l'accréditation acoustique proprement dite, mais une clé cryptographique, conservée dans la carte UICC 34 pour des raisons de sécurité. Cette clé cryptographique, combinée à l'appliquette, permettra de constituer un générateur cryptographique au sein du téléphone 20. Lorsqu'il souhaite obtenir l'ouverture d'une serrure, l'utilisateur commande la génération de l'accréditation acoustique par l'appliquette interne et sa reproduction par le transducteur de son téléphone.

[0056] On notera incidemment que le stockage dans l'UICC permet de révoquer les droits d'accès de l'utilisateur via le contrôle effectué par le réseau mobile sur cette UICC.

[0057] La sécurité du système peut être accrue par un processus de validation des droits de l'utilisateur au moyen d'un bit de validation dans la carte UICC. Ce bit de validation peut être par exemple envoyé par le réseau de façon non sollicitée et à intervalles réguliers (ou non). En variante, le téléphone peut requérir du site gestionnaire distant l'envoi du bit de validation lorsque sont réunies un certain nombre de conditions prédéterminées. En tout état de cause, si le bit de validation n'est pas obtenu l'utilisateur est immédiatement révoqué.

[0058] Comme dans le cas précédent, d'autres modes de révocation sont possibles :

- attente de l'expiration des accréditations ;
- envoi à la serrure par un tiers d'une accréditation spécifique de révocation ;
- déplacement d'un administrateur pour intervention sur la serrure et annulation des droits de l'utilisateur.

4°) Mode "pièce jointe"

[0059] Ce mode de mise en oeuvre est une variante du mode semi-en ligne.

[0060] La différence tient essentiellement au fait que les accréditations ne sont pas envoyées par le canal vocal du réseau de téléphonie mobile, mais sous forme d'un fichier annexé à un message de type e-mail, MMS ou messagerie instantanée.

[0061] L'avantage de cette solution est d'utiliser les moyens de téléchargement de fichiers préexistants dans le téléphone, notamment avec les téléphones comportant des fonctions élaborées de type "smartphone", et ceci sans qu'il soit nécessaire de télécharger au préalable une appliquette spécifique, de conserver celle-ci dans le téléphone et de la faire exécuter par ce dernier le moment venu.

5°) Modes mixtes

[0062] Diverses adaptations et variantes des modes ci-dessus peuvent être envisagées.

[0063] Ainsi, il est possible de combiner entre eux plusieurs modes, pour délivrer l'accréditation acoustique. Par exemple, le système peut imposer que la première ouverture d'une serrure par un utilisateur donné soit nécessairement effectuée selon un mode "en ligne" direct, les accès suivants pouvant en revanche être opérés selon d'autres modes, par exemple "semi-en ligne" ou "hors ligne"

[0064] Le système peut également imposer à l'utilisateur qu'à une certaine fréquence prédéterminée (par exemple une fois sur *N*), l'ouverture soit nécessairement effectuée selon un mode "en ligne", les autres utilisations pouvant être effectuées au moyen des autres modes.

6°) Validation complémentaire

[0065] Une autre précaution permettant d'augmenter la sécurité consiste, quel que soit le mode de mise en oeuvre choisi, de prévoir une validation supplémentaire par l'utilisateur, par exemple :

- entrée d'un code personnel de type "PIN code" avant la délivrance de l'accréditation acoustique, soit à chaque utilisation, soit une fois sur *N*, soit à intervalles de temps réguliers ;
- validation de type biométrique, au moyen d'un lecteur biométrique incorporé au téléphone ou par un système de reconnaissance d'empreinte vocale utilisant le microphone du téléphone. Une empreinte biométrique spécifique est stockée dans la mémoire 32 du téléphone ou dans la carte UICC 34, ou encore dans la base de données 12 pour traitement par le serveur distant. La fréquence de la validation biométrique peut, ici encore, être choisie : à chaque utilisation, une fois toutes les N utilisations, à intervalles réguliers, etc.

Perfectionnements et compléments de mise en oeuvre

Retour d'information

[0066] Ce perfectionnement consiste, essentiellement, à utiliser le téléphone mobile pour capter des signaux émis par la serrure, de manière à transmettre des informations depuis la serrure jusqu'au site gestionnaire via le téléphone d'un utilisateur et le réseau mobile, en profitant de l'établissement par cet utilisateur d'une liaison dans le sens descendant (du site gestionnaire vers la serrure) pour faire remonter des informations en sens inverse (de la serrure jusqu'au site gestionnaire).

[0067] Il est en effet très utile pour le site gestionnaire de disposer d'informations mémorisées dans la serrure, par exemple des données d'état (indicateur d'anomalies, de niveau de batterie, preuve d'ouverture, etc.) ou des données d'historique sur les utilisations successives de cette serrure.

[0068] Le perfectionnement de l'invention s'applique tout particulièrement aux serrures de type *stand alone,* c'est-à-dire fonctionnant de manière entièrement autonome sans être raccordées à un quelconque réseau qui lui permettrait d'échanger des données.

[0069] Il est possible d'utiliser le transducteur 46 de la serrure en le faisant fonctionner en mode inversé (pour émettre des signaux sonores au lieu de les capter), ou bien prévoir un transducteur spécifique pour reproduire des signaux sonores.

[0070] Le retour d'informations peut être déclenché par un administrateur du système, au moyen d'une appliquette téléchargée sur son téléphone mobile. Lorsqu'il souhaite récupérer des données d'une serrure, il présente son téléphone à la serrure et délivre un signal acoustique spécifique de commande qui ordonne, avec toutes

les garanties nécessaires de sécurité, à la serrure de renvoyer les informations requises. Ces informations sont transmises en retour sous forme de signaux acoustiques, chiffrés ou non, reproduits par le transducteur acoustique de la serrure. Ces signaux sont ensuite captés par le microphone du téléphone et traités par l'appliquette embarquée dans celui-ci, pour transmission immédiate ou ultérieure au site gestionnaire.

[0071] Le retour d'informations peut être également opéré sans qu'il soit besoin de déplacer un administrateur jusqu'à l'endroit où se trouve la serrure, en profitant de ce qu'un utilisateur autorisé demande l'ouverture de la serrure. À cet effet, pendant le processus d'ouverture déclenché à l'initiative de l'utilisateur, la serrure envoie en retour vers le téléphone de l'utilisateur des informations pertinentes telles que signal de batterie faible, besoin d'entretien, dysfonctionnement, preuve d'ouverture, etc. Ces informations peuvent être traduites par l'appliquette du téléphone en messages d'alerte ("*batterie faible*") affichés sur l'écran du téléphone, ces messages d'alerte étant répétés si nécessaire à intervalles réguliers. Une autre possibilité consiste à envoyer ces informations vers le site gestionnaire par l'intermédiaire du réseau mobile, afin qu'un administrateur puisse ensuite prendre les mesures correctrices appropriées.

[0072] En d'autres termes, chaque utilisateur devient pour le système une source d'informations, ce qui est particulièrement avantageux dans le cas de serrures entièrement autonomes.

[0073] Dans une variante de ce perfectionnement, le signal de commande, au lieu d'être délivré par le téléphone, est émis par une installation de sonorisation générale du bâtiment, ce qui permet de transmettre simultanément ce signal à un très grand nombre de serrures. Cette même installation peut être équipée de microphones pouvant également écouter le signal délivré par les serrures.

Accréditations multiples en salve

[0074] Lorsqu'un utilisateur possède des droits d'accès sur une pluralité de serrures différentes, il doit normalement choisir manuellement, dans une liste qui lui est présentée sur l'afficheur de son téléphone, le type de serrure dont il veut commander l'ouverture, ceci pour obtenir l'émission d'une accréditation conforme correspondante.

[0075] Un perfectionnement consiste, pour éviter cette manipulation, à faire délivrer par le téléphone une pluralité d'accréditations en une salve unique, la salve contenant une accréditation correspondant à chacune des serrures pour lesquelles l'utilisateur est habilité. Parmi les multiples accréditations qui seront captées par la serrure, celle-ci reconnaîtra, au moyen d'un code approprié, celle qui lui est destinée, et c'est cette dernière, et elle seule, qui pourra ensuite commander l'ouverture de la serrure.

Commande rapide (*speed dial*)

[0076] Il est possible et avantageux de commander l'émission des accréditations acoustiques par le téléphone par appui sur un bouton ou une touche dédiée du téléphone, ou par activation d'une icône spécifique dans le cas d'un téléphone à écran tactile.

[0077] Dans le mode "en ligne", l'utilisateur attribue un bouton ou une icône à cette fonction, qui déclenchera la composition du numéro d'appel du serveur et lui permettra de recevoir en retour l'accréditation acoustique. Dans les modes "semi-en ligne" ou "hors ligne", l'appliquette (*cardlet* ou *midlet*) demande à l'utilisateur de choisir automatiquement ou manuellement le bouton ou l'icône qu'il souhaite pour commander l'obtention rapide de l'accréditation acoustique par la technique décrite plus haut.

Application : gestion hôtelière

[0078] Cette application à la gestion des clés d'un hôtel sera décrite en référence à la Figure 3. Cette figure reprend les divers éléments de l'ensemble de la Figure 1, auquel sont en outre associés :

- un système 48 de gestion de l'établissement ou PMS (*Property Management System*), qui est un système de gestion d'hôtel classique, ici relié à la base de données 12 du site gestionnaire 10 par une liaison sécurisée, par exemple une liaison internet de type *https,*
- un système 50 de réservation hôtelière ou RS (*Reservation System*), qui est un système permettant à tout utilisateur qui se connecte d'obtenir une réservation dans un hôtel de son choix et de fournir les différentes informations nécessaires à l'enregistrement de cette réservation. Le système de réservation RS est couplé au système PMS 48 de gestion de l'établissement, et éventuellement à la base de données 12 du site gestionnaire 10.
- un système 52 de création de cartes de chambre ou LFDS (*Lock Front Desk System*) 52, permettant d'enregistrer l'utilisateur au moment de son arrivée ou *check-in* à l'hôtel, soit par l'intermédiaire d'un réceptionniste, soit directement par l'utilisateur dans le cas d'un système en libre-service. Ce système LFDS est relié au système PMS 48 et éventuellement à la base de données 12.

[0079] On va maintenant décrire les différentes étapes de cette application hôtelière, en insistant notamment sur les particularités résultant de l'utilisation du système de l'invention (pour le reste, le processus mis en oeuvre est un processus conventionnel, qui ne sera décrit que de façon sommaire).

1°) Réservation

[0080] Le système 50 de réservation hôtelière RS

communique avec une base de données répertoriant parmi les hôtels proposés ceux qui sont équipés pour mettre en oeuvre la technique de l'invention.

[0081] Le client opère une réservation auprès du système RS 50 par toute technique conventionnelle : internet, application WAP par son téléphone, appel téléphonique, par une agence de voyage, etc. Lors de la réservation, le système RS vérifie si l'hôtel demandé peut fonctionner avec le système d'accréditations acoustiques selon l'invention. Dans l'affirmative, cette option est offerte au client qui demande la réservation, et il peut accepter cette proposition par une technique classique d'acceptation de "termes et conditions" de ce service particulier.

[0082] Le client communique alors au système RS un certain nombre d'informations, comprenant notamment :

- informations personnelles (nom, etc.),
- numéro de carte de crédit,
- numéro éventuel de carte de fidélité,
- numéro de passeport ou de carte d'identité,
- numéro de téléphone mobile,
- adresse électronique (e-mail qu'il peut recevoir sur son téléphone mobile, identifiant de messagerie instantanée).

[0083] À la fin du processus de réservation, le client reçoit un message de confirmation, l'informant notamment du fait qu'il pourra obtenir la délivrance de la clé de sa chambre directement au moyen de son mobile, sans remise de badge ni de carte à la réception lors de son arrivée à l'hôtel. Il peut également recevoir l'appliquette (*midlet* ou *cardlet*) nécessaire dans le cas d'une mise en oeuvre par un mode "semi-en ligne" ou "hors ligne".

[0084] Si le client ne participe pas encore à un programme de fidélisation, le système peut lui proposer d'y souscrire, ce programme de fidélisation pouvant notamment inclure le bénéfice du système de l'invention, qui lui permettra d'obtenir la délivrance de la clé sous forme d'une accréditation acoustique.

2°) Préparation à l'accueil du client

[0085] Une fois que le client a effectué sa réservation et accepté de recevoir sa clé sous forme d'accréditation acoustique sur son téléphone mobile, le système 50 de réservation hôtelière RS communique au système 48 de gestion de l'établissement PMS 48 les détails de la réservation, en particulier le fait que cette réservation inclut la délivrance d'une clé sous forme d'accréditation acoustique.

[0086] Le système RS 50 informe également le système PMS 48 du moyen de communication mobile choisi par le client (numéro de téléphone mobile, e-mail sur téléphone mobile, messagerie instantanée). Un niveau de priorité d'affectation de chambre peut également être attribué à la réservation. Parallèlement, le système de réservation RS 50 ou le système PMS 48 informe le site gestionnaire 10 de la réservation, par envoi des informations suivantes :

- numéro de téléphone mobile,
- adresse électronique,
- dates d'arrivée et de départ,
- numéro de réservation,
- coordonnées de l'hôtel.

3°) Activation avant l'arrivée du client

[0087] Cette phase consiste essentiellement à attribuer une chambre au client pour la durée de son séjour, et faire générer par le site gestionnaire une accréditation acoustique chiffrée correspondante. Elle peut être commandée de plusieurs manières.

a) commande à l'initiative du système de gestion de l'établissement PMS

[0088] Le système 48 de gestion de l'établissement PMS attribue tout d'abord un numéro de chambre et envoie les informations suivantes au système 52 de création de cartes de chambre LFDS :

- numéro de chambre,
- numéro de téléphone mobile,
- adresse électronique,
- dates d'arrivée et de départ,
- numéro de réservation.

[0089] Le système LFDS 52 génère alors une clé virtuelle pour cette chambre et cette période, et envoie les informations suivantes au site gestionnaire 10, via une liaison sécurisée :

- chaîne de données correspondant, sous forme chiffrée, à la clé virtuelle de la chambre,
- numéro de téléphone mobile,
- adresse électronique,
- dates d'arrivée et de départ,
- numéro de réservation,
- coordonnées de l'hôtel.

[0090] Le site gestionnaire 10 accuse réception de ces informations et traduit en une accréditation acoustique, générée par le générateur 14, les données correspondant à la clé virtuelle de la chambre.

[0091] Le site gestionnaire 10 envoie ensuite au téléphone mobile du client un message (SMS, e-mail ou messagerie instantanée) l'informant du numéro de la chambre qui lui a été attribuée et du numéro de téléphone qu'il devra composer lorsqu'il se trouvera devant la porte de cette chambre afin d'obtenir l'accréditation acoustique lui permettant d'accéder à cette dernière. En variante, le site gestionnaire peut envoyer les accréditations acoustiques sous forme d'un fichier joint (par MMS, messagerie instantanée ou e-mail), fichier que le client ouvrira pour reproduire l'accréditation acoustique lorsqu'il se trouvera

devant la porte de sa chambre.

[0092] Dans une variante de cette première solution, la chaîne de données correspondant à la clé virtuelle de la chambre, au lieu d'être envoyée par le système LFDS 52, l'est par le système PMS 48, qui envoie cette chaîne de données au site gestionnaire 10, le reste des opérations étant inchangé.

[0093] Dans une autre variante de cette première solution, la chaîne de données, au lieu d'être envoyée au site gestionnaire 10 par le système LFDS 52, l'est via le système de réservation RS 50, évitant ainsi le recours à une liaison sécurisée spécifique entre le système LFDS 52 et le site gestionnaire 10.

b) commande avec pré-enregistrement

[0094] Dans cette autre solution, le site gestionnaire 10 envoie au client sur son téléphone mobile, peu avant son arrivée à l'hôtel, une information de pré-enregistrement, avec un lien auquel il devra se connecter, ou un numéro de téléphone à composer, pour confirmer l'enregistrement. Cette information de pré-enregistrement peut être envoyée par un SMS de type "push SMS", par e-mail ou par messagerie instantanée.

[0095] A tout moment, le client peut accepter l'enregistrement en cliquant sur le lien ou en appelant le numéro de téléphone qui lui a été indiqué. Le site gestionnaire 10 informe alors le système PMS 48 de cette acceptation de l'enregistrement, qui pourra être ensuite exécuté par le système PMS de la manière décrite précédemment.

c) *commande manuelle*

[0096] Dans cette autre solution, l'activation est gérée de façon manuelle. À cet effet, avant l'arrivée du client à l'hôtel, un opérateur se connecte sur internet à une application d'un fournisseur d'applications hébergées ASP (*Application Service Provider*) et lui fournit les informations suivantes:

- numéro de chambre attribuée,
- numéro de téléphone mobile du client,
- adresse électronique du client,
- dates d'arrivée et de départ,
- numéro de réservation,
- coordonnées de l'hôtel.

[0097] L'application du fournisseur ASP communique au site gestionnaire 10 les données correspondantes, et ce dernier peut alors soit envoyer une information de pré-enregistrement au client sur son mobile (voir ci-dessus), soit lui envoyer directement l'information du numéro de chambre et les informations nécessaires pour obtenir l'accréditation acoustique lorsqu'il se trouvera devant la porte de celle-ci.

[0098] Les variantes exposées plus haut, par exemple l'envoi des accréditations acoustiques sous forme de fichier joint, sont également applicables à cette mise en oeuvre manuelle.

4°) Délivrance de l'accréditation

[0099] Le client arrive sur place et va directement à sa chambre. L'accréditation acoustique peut lui être délivrée de plusieurs façons :

- le client appelle le numéro de téléphone qui est indiqué dans le message qu'il a reçu (en cliquant directement sur un lien ou en composant le numéro de téléphone), pour obtenir et reproduire l'accréditation acoustique ;
- en variante, le site gestionnaire ne répond pas directement mais délivre un message accusant réception de l'appel et demandant au client de raccrocher ; juste après, le site gestionnaire rappelle le client et lui délivre l'accréditation acoustique ;
- en mode "pièce jointe", le client ouvre le fichier audio qu'il a reçu en du site gestionnaire par e-mail, messagerie instantanée ou MMS, de manière à reproduire l'accréditation acoustique ;
- en mode "semi-hors ligne" ou "hors ligne", le client lance l'application lui permettant de reproduire l'accréditation acoustique.

5°) Ouverture de la porte

[0100] Le client approche son téléphone mobile de la serrure de la porte, qui est pourvue d'un système permettant d'écouter le téléphone. La serrure traduit l'accréditation acoustique en une autorisation de déblocage. Si l'accréditation acoustique est conforme, la serrure se débloque et il suffit au client d'ouvrir la porte, de la même manière qu'il aurait procédé avec un badge qui lui aurait été délivré à la réception de l'hôtel.

[0101] Le même processus est répété à chaque ouverture de porte durant le séjour de l'hôtel. Éventuellement, le client peut obtenir auprès de la réception un badge qu'il pourra utiliser en plus de son téléphone mobile. Toutes les transactions sont bien entendu enregistrées de manière à pouvoir établir un historique des utilisations de la serrure.

6°) Retour d'information

[0102] Au moment où le client reçoit l'accréditation acoustique du site gestionnaire 10, ce dernier informe le système PMS 48 que l'accréditation a bien été délivrée au client, et à quel moment. Dans les modes "semi-en ligne", "hors ligne" et "pièce jointe", le site gestionnaire 10 peut également générer un retour d'informations à destination du système PMS 48.

7°) Cas particuliers

[0103] Le système permet de gérer aisément divers

cas particuliers.

[0104] Lors de la réservation, le client peut informer le système que plusieurs autres personnes seront amenées à accéder également à la chambre. Il indique alors les numéros de téléphone mobile et les adresses électroniques des autres personnes, afin que chacun puisse recevoir également une accréditation acoustique pour la durée prévue du séjour.

[0105] Par ailleurs, à tout moment, le client peut demander à la réception de l'hôtel, ou de façon automatique par le système LFDS 52, la délivrance d'un "duplicata" de son accréditation acoustique sous forme d'un badge. Ces badges sont susceptibles de fonctionner en parallèle avec les accréditations acoustiques reproduites par le téléphone mobile.

[0106] Enfin, en cas de perte ou de vol de son téléphone mobile, le client informera la réception de l'hôtel ou bien son opérateur mobile afin qu'un badge de remplacement puisse lui être délivré. Une fois ce badge utilisé pour ouvrir la porte, les accréditations acoustiques antérieures seront révoquées par le système.

8°) Départ

[0107] Plusieurs solutions peuvent être mises en oeuvre.

[0108] Par exemple, le départ peut être enregistré via le système interne de télévision de l'hôtel, avec paiement par carte de crédit. Pour ce faire, le client sélectionne l'option "check out" du système interne de télévision, ce qui fait apparaître sa facture sur l'écran du téléviseur. Il accepte alors cette facture en cliquant sur un bouton "acceptation", ce qui déclenche l'établissement d'un formulaire de paiement par carte de crédit. Le client remplit ou complète ce formulaire avec toutes les informations nécessaires et valide le paiement.

[0109] Dans un perfectionnement, le site gestionnaire 10 est impliqué dans le processus de validation du paiement, en délivrant un signal d'accréditation acoustique via l'application de paiement. Cette accréditation acoustique est reproduite par les haut-parleurs du téléviseur situé dans la chambre du client et, au même moment, le site gestionnaire 10 compose le numéro de téléphone mobile du client. Ce dernier répond et présente son téléphone devant les haut-parleurs du téléviseur, ce qui "ferme la boucle" du processus et permet de valider le paiement, avec l'autorisation du site gestionnaire 10.

[0110] Dans une autre variante encore, au lieu d'utiliser le circuit interne de télévision de l'hôtel, il est seulement demandé au client de décrocher le téléphone de sa chambre et de composer un numéro correspondant à la fonction "check out". Une fois en communication avec le service correspondant, le client valide son acceptation de la facture en transmettant à ce service, via son téléphone mobile, l'accréditation acoustique qu'il utilisait pour ouvrir sa porte. Cette manoeuvre est interprétée comme une acceptation de la facture, dont le montant sera débité sur la carte de crédit du client.

[0111] Dans tous les cas, un e-mail est envoyé au client mentionnant la bonne réception du paiement et donnant les détails de la facture. Le client peut également obtenir une copie papier de la facture à la réception de l'hôtel ou auprès d'un automate situé dans le hall d'accueil.

Revendications

1. Un système sécurisé de commande d'ouverture de dispositifs de serrure, comportant :

- au moins un dispositif de serrure (22) muni de circuits électroniques pour la commande d'organes mécaniques de verrouillage/déverrouillage;
- un téléphone mobile (20) à disposition d'un utilisateur (18) habilité à ouvrir le dispositif de serrure ;
- un site gestionnaire (10) distant ; et
- un opérateur de réseau mobile (16), couplé au site gestionnaire et au téléphone mobile ,

système **caractérisé en ce que**:

- le site gestionnaire distant comprend:
  · une base de données (12) de dispositifs de serrure et d'utilisateurs habilités, avec pour chaque utilisateur un identifiant unique associé à un numéro de téléphone mobile, et des données de droits d'accès et de conditions d'utilisation, et
  · un générateur (14) de données d'accréditation, les accréditations étant des accréditations acoustiques chiffrées en forme de signaux audio à usage unique, propres à permettre l'ouverture des dispositifs de serrure répertoriés dans la base de données ;
- le système comprend des moyens de transmission sécurisée desdites données d'accréditation du site gestionnaire au téléphone mobile de l'utilisateur habilité correspondant ;
- le téléphone (20) comprend un transducteur électro-acoustique (36) apte à reproduire lesdites accréditations acoustiques ;
- le dispositif de serrure (22) comprend un transducteur électro-acoustique (46) apte à capter les accréditations acoustiques reproduites par le transducteur du téléphone préalablement placé à proximité du dispositif de serrure ; et
- le dispositif de serrure (22) comprend des moyens pour reconnaître, analyser et authentifier les accréditations acoustiques captées par le transducteur, et commander le déverrouillage des organes mécaniques sur reconnaissance d'une accréditation conforme.

2. Le système de la revendication 1, comportant des moyens propres, sur envoi d'une requête par le téléphone mobile au site gestionnaire, à :

- vérifier l'habilitation de l'utilisateur dans la base de données du site,
- générer une accréditation acoustique par le générateur du site, et
- transmettre cette accréditation au téléphone, pour reproduction directe par le transducteur de celui-ci préalablement placé à proximité du transducteur du dispositif de serrure.

3. Le système de la revendication 1, comportant des moyens propres, sur envoi d'une requête par le téléphone mobile au site gestionnaire, à :

- vérifier l'habilitation de l'utilisateur dans la base de données du site,
- générer au moins une accréditation acoustique par le générateur du site,
- transmettre au téléphone cette accréditation, ou ces accréditations, par mise en oeuvre d'une appliquette interne du téléphone apte à en exécuter le téléchargement et la mémorisation dans une mémoire (32) du téléphone,

puis, dans un second temps :

- activer l'appliquette interne pour reproduction de l'accréditation, ou de l'une des accréditations, par le transducteur du téléphone préalablement placé à proximité du transducteur du dispositif de serrure.

4. Le système de la revendication 1, dans lequel :

- le téléphone comprend une appliquette interne formant, en combinaison avec une clé cryptographique, générateur cryptographique,
- la donnée d'accréditation transmise par le site distant au téléphone est ladite clé cryptographique,

de manière à permettre, sur commande de l'utilisateur, la génération de l'accréditation acoustique par l'appliquette interne et sa reproduction par le transducteur de celui-ci préalablement placé à proximité du transducteur du dispositif de serrure.

5. Le système de la revendication 4, dans lequel la clé cryptographique, et éventuellement l'appliquette, sont conservées dans un mémoire d'une carte à microcircuit sécurisée (34) du téléphone.

6. Le système de la revendication 4, comprenant en outre des moyens pour conditionner la génération de l'accréditation acoustique par l'appliquette interne du téléphone à la mise à jour par le site distant, ou par l'opérateur de réseau mobile, d'une donnée de validation nécessaire pour que l'appliquette puisse continuer à opérer ladite génération.

7. Le système de la revendication 1, comportant des moyens propres, sur envoi d'une requête par le téléphone mobile au site gestionnaire, ou à l'initiative du site gestionnaire, à :

- vérifier l'habilitation de l'utilisateur dans la base de données,
- générer au moins une accréditation acoustique et convertir cette accréditation, ou ces accréditations, en un fichier audio,
- transmettre au téléphone ce fichier audio pour téléchargement et mémorisation dans une mémoire du téléphone,

puis, dans un second temps :

- reproduire le fichier audio par le transducteur du téléphone préalablement placé à proximité du transducteur du dispositif de serrure.

8. Le système de l'une des revendications 3 ou 7, comprenant en outre des moyens pour générer automatiquement ladite requête à partir d'un seuil prédéfini d'accréditations restant mémorisées dans le téléphone, afin d'opérer un rechargement de la mémoire du téléphone par de nouvelles accréditations.

9. Le système de la revendication 1, comprenant en outre des moyens pour conditionner la reproduction de l'accréditation acoustique par le transducteur du téléphone à la présentation préalable d'une donnée personnelle de validation délivrée par l'utilisateur au téléphone.

10. Le système de la revendication 1, dans lequel :

- le dispositif de serrure comprend un transducteur électro-acoustique apte à reproduire des signaux acoustiques en retour, générés par le dispositif de serrure et codés par des données d'état ou d'historique propres au dispositif de serrure ; et
- le téléphone comprend un transducteur électro-acoustique apte à capter lesdits signaux en retour.

11. Le système de la revendication 10, dans lequel :

- le téléphone comprend en outre des moyens pour décoder lesdits signaux en retour et afficher le cas échéant à destination de l'utilisateur un message d'alerte fonction desdites données d'état ou d'historique propres au dispositif de serrure.

12. Le système de la revendication 10, dans lequel :

- le téléphone comprend en outre des moyens pour transmettre au site gestionnaire lesdits signaux en retour avec lesdites données d'état ou d'historique propres au dispositif de serrure.

13. Le système de la revendication 1, dans lequel :

- l'utilisateur est habilité pour une pluralité de dispositifs de serrure différents ;
- le téléphone est apte à reproduire en une salve unique une pluralité d'accréditations, ladite salve contenant une accréditation correspondant à chacune des dispositifs de serrure pour lesquelles l'utilisateur est habilité.

14. Le système de la revendication 1, dans lequel :

- le téléphone comprend en outre une commande rapide d'obtention et/ou de reproduction de l'accréditation par appui sur un bouton dédié du téléphone, ou par activation d'une icône spécifique d'une surface tactile du téléphone.

15. Le système de la revendication 1, dans lequel le système est également apte à commander l'activation/désactivation d'une installation d'alarme sur reconnaissance d'une accréditation conforme.

FIG_1

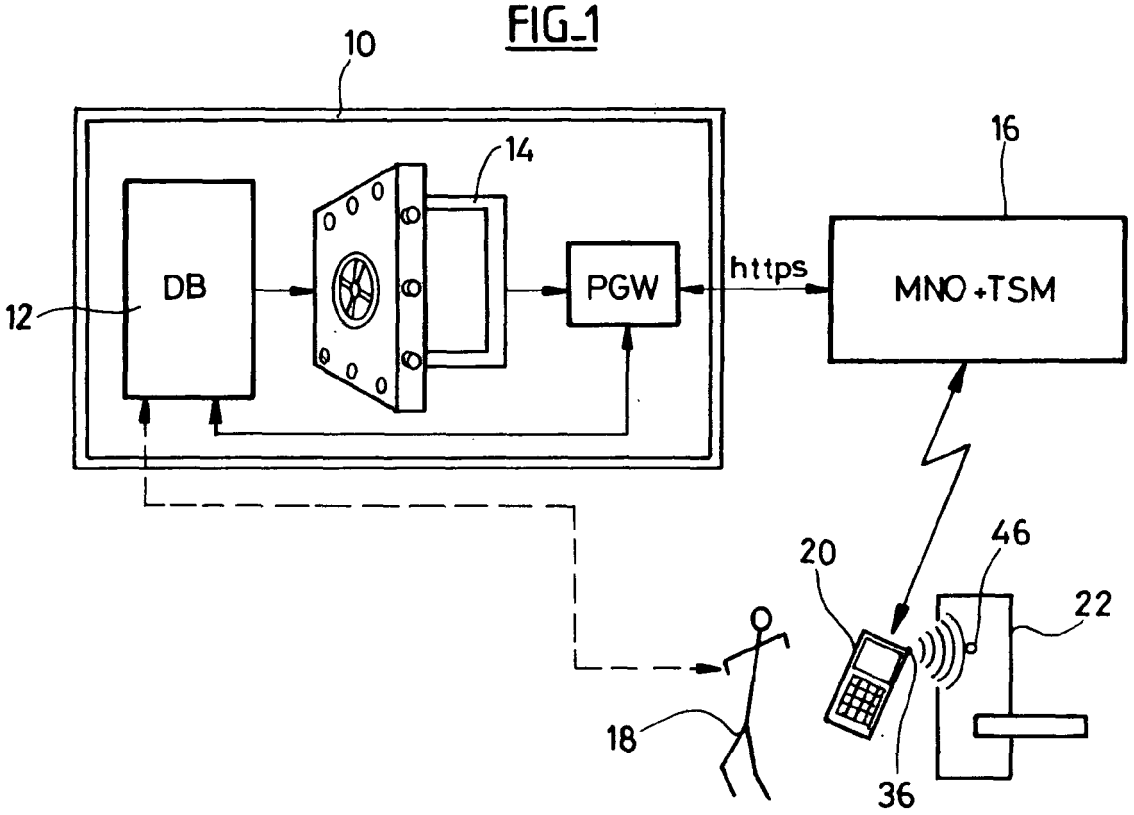

10
14
16
DB
PGW
https
MNO+TSM
12
20
46
22
18
36

FIG_2

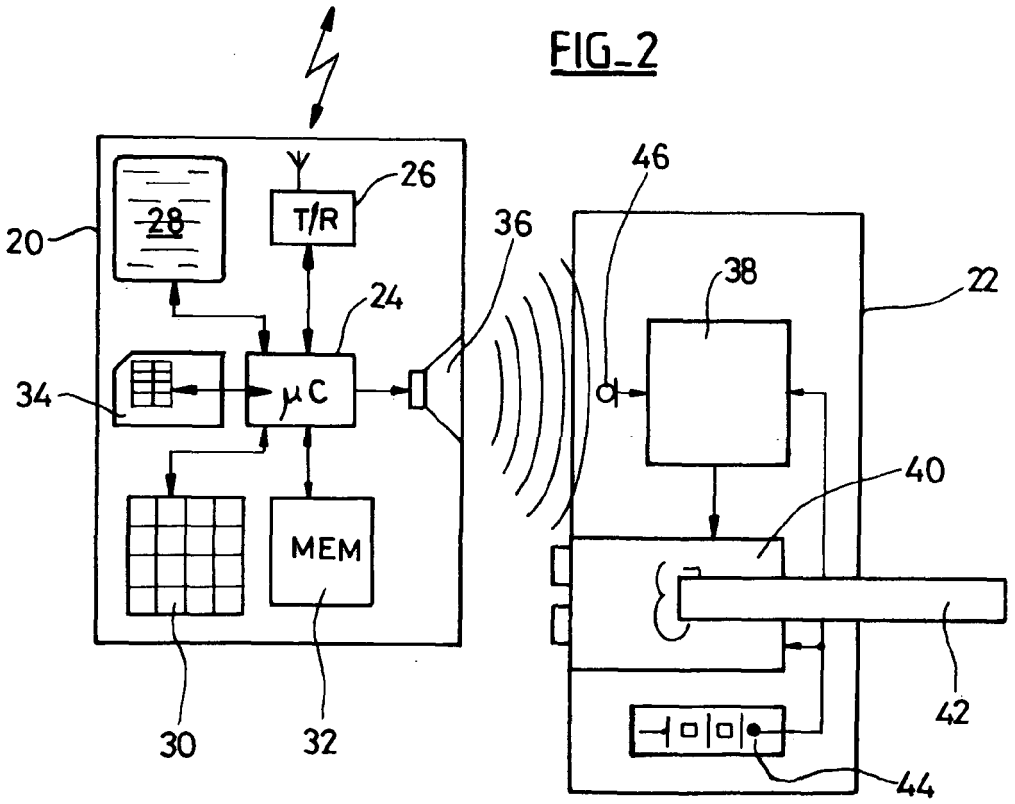
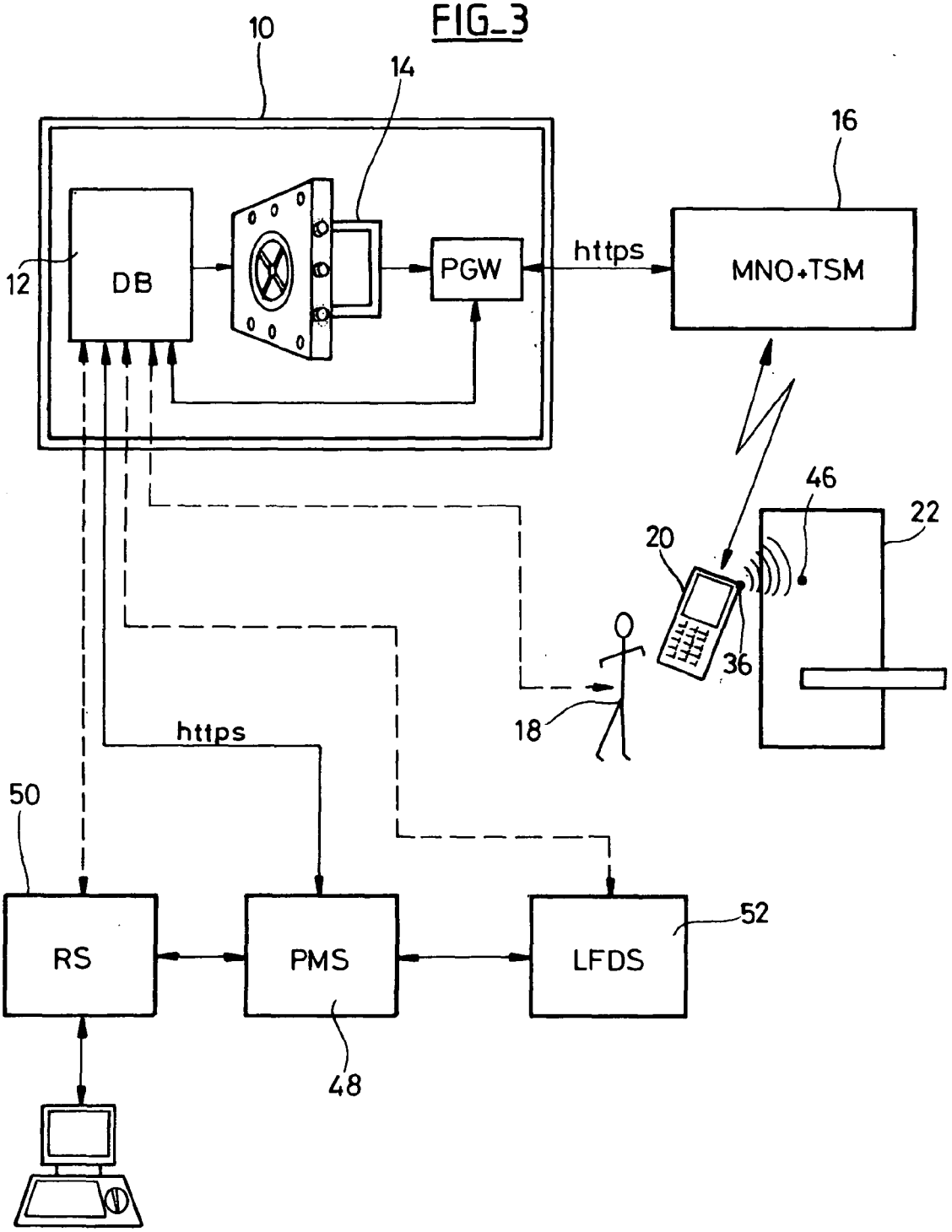

20
28
T/R
26
46
36
38
22
24
34
μC
40
MEM
30
32
42
44

FIG_3


10
14
16
12
DB
PGW
https
MNO+TSM
46
22
20
36
18
https
50
RS
PMS
LFDS
52
48

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 09 16 6002

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
X	DE 100 54 633 A1 (CALL A BIKE MOBILITAETSSYSTEME [DE] HOGL CHRISTIAN [DE]) 25 avril 2002 (2002-04-25)	1-2,7, 9-10	INV. G07C9/00
Y	* revendications 16,23 * * alinéa [0001] * * alinéa [0016] - alinéa [0017] * * alinéa [0030] - alinéa [0032] * * alinéa [0038] - alinéa [0039] * * alinéa [0048] * * alinéa [0052] - alinéa [0053] * * figure 1 *	3-6,8, 11-15	
Y	WO 2006/136662 A1 (MOHINET OY [FI]; KOLJONEN JOUNI [FI]) 28 décembre 2006 (2006-12-28) * page 4, ligne 27 - page 5, ligne 13 *	3	
Y	WO 02/095689 A1 (ERICSSON INC [US]; DENT PAUL [US]; SKUBIC JANEZ [SE]) 28 novembre 2002 (2002-11-28) * page 4, ligne 4 - ligne 17 * * page 8, ligne 16 - ligne 19 * * page 12, ligne 8 - ligne 13 * * figure 1 *	4-6	DOMAINES TECHNIQUES RECHERCHES (IPC) G07C G06Q
Y	EP 1 703 479 A1 (HEWLETT PACKARD DEVELOPMENT CO [US]) 20 septembre 2006 (2006-09-20) * alinéa [0030] - alinéa [0032] * * alinéa [0038] *	8	
Y	GB 2 402 840 A (WALKER GUY FRANK HOWARD [GB]) 15 décembre 2004 (2004-12-15) * page 9, ligne 13 - ligne 23 *	11-12,14	
Y	GB 2 364 202 A (NOKIA MOBILE PHONES LTD [FI]) 16 janvier 2002 (2002-01-16) * page 9, ligne 18 - ligne 21 *	13	

-/--

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	20 novembre 2009	Roth, Lucia

CATEGORIE DES DOCUMENTS CITES

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 antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1 EPO FORM 1503 03.82 (P04C02)

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 09 16 6002

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
Y	WO 00/35178 A2 (PHONE COMMUNICATIONS AB M [SE]; JERVILL MARTIN [SE]; JEPPSSON PER [SE]) 15 juin 2000 (2000-06-15) * page 5, ligne 3 - ligne 16 * -----	15	
A	DE 103 21 307 A1 (DEUTSCHE TELEKOM AG [DE]) 2 décembre 2004 (2004-12-02) * revendications 1,2 * -----	1-15	
			DOMAINES TECHNIQUES RECHERCHES (IPC)

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	20 novembre 2009	Roth, Lucia

CATEGORIE DES DOCUMENTS CITES

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 antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 09 16 6002

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

20-11-2009

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
DE 10054633 A1	25-04-2002	AUCUN	
WO 2006136662 A1	28-12-2006	EP 1897066 A1	12-03-2008
WO 02095689 A1	28-11-2002	AU 2002308549 A1	03-12-2002
		EP 1423826 A1	02-06-2004
		US 2002178385 A1	28-11-2002
EP 1703479 A1	20-09-2006	AUCUN	
GB 2402840 A	15-12-2004	AUCUN	
GB 2364202 A	16-01-2002	US 2002031228 A1	14-03-2002
WO 0035178 A2	15-06-2000	AU 1594200 A	26-06-2000
		SE 516589 C2	29-01-2002
		SE 9804055 A	27-05-2000
DE 10321307 A1	02-12-2004	AUCUN	

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

RÉFÉRENCES CITÉES DANS LA DESCRIPTION

Cette liste de références citées par le demandeur vise uniquement à aider le lecteur et ne fait pas partie du document de brevet européen. Même si le plus grand soin a été accordé à sa conception, des erreurs ou des omissions ne peuvent être exclues et l'OEB décline toute responsabilité à cet égard.

Documents brevets cités dans la description

- WO 2008107595 A2 **[0013]**