



(11) **EP 2 284 803 B1**

(12) **FASCICULE DE BREVET EUROPEEN**

(45) Date de publication et mention
de la délivrance du brevet:
13.03.2013 Bulletin 2013/11

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

(21) Numéro de dépôt: **09167248.5**

(22) Date de dépôt: **05.08.2009**

(54) **Système sécurisé de programmation de dispositifs de serrure à commande électronique par accréditations acoustiques chiffrées**

Gesichertes System zum Programmieren von Schließvorrichtungen über elektronische Steuerung durch chiffrierte akustische Akkreditierungen

Secure system for programming electronically controlled lock devices using encoded acoustic verifications

(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**

(43) Date de publication de la demande:
16.02.2011 Bulletin 2011/07

(73) Titulaire: **OPENWAYS SAS**
75016 Paris (FR)

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

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

(56) Documents cités:
WO-A1-03/093997 WO-A1-2007/046804
WO-A2-2008/107595 US-A- 5 933 090

EP 2 284 803 B1

Il est rappelé que: Dans un délai de neuf mois à compter de la publication de la mention de la délivrance du brevet européen au Bulletin européen des brevets, toute personne peut faire opposition à ce brevet auprès de l'Office européen des brevets, conformément au règlement d'exécution. L'opposition n'est réputée formée qu'après le paiement de la taxe d'opposition. (Art. 99(1) Convention sur le brevet européen).

Description

[0001] L'invention concerne les dispositifs de serrure commandés électriquement au moyen d'un objet portatif formant clé, tel qu'une carte ou un badge sans contact, ou également un téléphone mobile équipé de moyens de couplage (inductif, radiofréquence, acoustique, ...) à la serrure.

[0002] 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. Le dispositif de serrure peut également comprendre, ou être associé à, un système d'alarme qu'il s'agit de désactiver pour permettre l'accès à un espace donné, ou inversement d'activer pour protéger cet espace avant ou après l'avoir quitté.

[0003] 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. L'invention concerne plus précisément la programmation de ces serrures par les "droits d'accès" qui leur correspondent, c'est-à-dire l'indication des utilisateurs habilités à ouvrir telle ou telle serrure, avec pour chacun d'entre eux une définition des droits qui lui sont propres, droits qui peuvent par exemple être limités dans le temps (péremption du droit d'accès), ou limités à certains jours de la semaine, ou à certaines plages horaires, etc. Dans certains systèmes, chaque serrure est reliée à un réseau permettant une gestion centralisée des accès et du contrôle des droits. Ces systèmes sont bien adaptés à des environnements d'entreprise ou hôteliers, mais beaucoup moins à des applications de type résidentiel, ou bien à la modernisation d'installations préexistantes où il serait difficilement envisageable de créer un réseau local, avec notamment toutes les difficultés de câblage que cela impliquerait.

[0004] L'invention vise plus particulièrement, mais de façon non exclusive, un autre type d'installations, où les serrures sont des dispositifs autonomes, chacune d'entre elles mémorisant en interne les droits d'accès qui lui sont attachés (utilisateurs habilités et, pour chacun, restrictions éventuelles d'accès).

[0005] La programmation de ce type de serrure implique une intervention sur place d'un opérateur (ci-après "utilisateur-maître") muni d'un appareil qui puisse être couplé à la serrure pour y inscrire ou mettre à jour les

droits d'accès. La mise à jour peut également concerner divers autres paramètres de fonctionnement de la serrure tels que date et heure, données d'identification, algorithmes de calcul, éléments cryptographiques, etc.

[0006] Les WO 03/093997 A1 et US 5 933 090 A décrivent de tels systèmes de contrôle d'accès programmables ou reprogrammables en fonction des besoins.

[0007] En pratique, la programmation de telles serrures autonomes est une opération délicate, nécessitant un appareillage spécifique et coûteux ainsi qu'un apprentissage préalable, obligeant la plupart du temps à recourir à un opérateur professionnel.

[0008] Ces inconvénients sont un frein important au déploiement de ces systèmes de serrures autonomes.

[0009] Il serait à cet égard souhaitable de pouvoir disposer d'un moyen de programmation simple à mettre en oeuvre et ne nécessitant pas d'appareillage spécifique, de sorte que la programmation puisse être réalisée par des manipulations simples, à la portée de tout un chacun.

[0010] Ceci permettrait notamment de développer les applications résidentielles, où les clients souhaitent pouvoir programmer eux-mêmes les serrures qu'ils ont acquises, et/ou les mettre à jour eux-mêmes sans recours à un professionnel, notamment chaque fois qu'il est nécessaire de modifier les droits d'accès ou en créer de nouveaux.

[0011] L'un des buts de la présente invention est de proposer une nouvelle technique de programmation de ces serrures, qui puisse être mise en oeuvre aisément au moyen d'un téléphone mobile, et d'une façon suffisamment simple pour être à la portée d'un utilisateur-maître non professionnel d'habileté moyenne.

[0012] Un autre but de l'invention est de proposer une technique de programmation 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, préexistant, sans que l'utilisateur-maître n'ait besoin de recourir à un appareil de programmation particulier. Le système de l'invention pourra être ainsi immédiatement généralisable et utilisable par tout un chacun, en bénéficiant de la sécurité et de la souplesse propres aux techniques cryptographiques modernes.

[0013] Le principe de l'invention repose sur l'utilisation d'accréditations acoustiques chiffrées pour la programmation de la serrure. 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. 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-maître. Pour utiliser l'accréditation, l'utilisateur-maître 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 programme ou reprogramme les droits d'accès dans sa mémoire interne.

[0014] 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).

[0015] 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 le destinataire 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.

[0016] Plus précisément, la présente invention concerne un système du type général divulgué par le WO03/093997 A1 précité, comprenant les éléments énoncés au préambule de la revendication 1.

[0017] Pour atteindre les buts indiqués plus haut, l'invention propose d'y combiner les éléments énoncés dans la partie caractéristique de la revendication 1.

[0018] Les sous-revendications exposent diverses mises en oeuvre possible de l'invention, ainsi que des perfectionnements avantageux.

[0019] 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.

[0020] On va expliquer le principe et la mise en oeuvre de l'invention, en référence aux Figures 1 et 2.

[0021] 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 serrures avec leurs données de droits d'accès associées, comprenant une liste d'utilisateurs habilités avec pour chacun les conditions d'accès autorisées : accès réservé à certains jours ou certaines plages horaires, date d'expiration du droit d'accès, etc.

[0022] Outre les utilisateurs habilités, la base de données recense également pour chaque serrure un identifiant UID (*Unique Identifier*) qui est attribué de manière unique et permet d'identifier de façon univoque la serrure dans les divers protocoles d'échange de données. La serrure peut être également identifiée par une dénomination libre ("entrée", "garage", "cave", etc.), notamment pour faciliter la sélection par un utilisateur d'une serrure parmi plusieurs, de la même manière qu'une étiquette qui serait attachée à une clé traditionnelle.

[0023] D'autres données peuvent également être conservées par la base de données, notamment les algorithmes utilisés par la serrure, une ou plusieurs clés cryptographiques, etc.

[0024] Le site gestionnaire 10 comprend également un moteur cryptographique formant générateur 14 de données d'accréditation.

[0025] 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) constituées d'une succession de tonalités doubles DTMF. Ces signaux audio sont conçus de manière à pouvoir être véhiculés par des canaux de transmission audio et reproduits tels quels par des transducteurs acoustiques.

[0026] La programmation d'une serrure implique, en premier lieu, de définir ou mettre à jour dans la base de données DB la liste des utilisateurs habilités, avec pour chacun les conditions d'accès correspondantes. Ces différentes informations seront communiquées au site gestionnaire 10 par un opérateur autorisé (ci-après désigné "utilisateur-maître") lors d'une phase initiale.

[0027] Comme on l'expliquera par la suite, la programmation peut également impliquer, outre la détermination des droits d'accès, la mise à jour d'autres informations propres à la serrure et relatives à son fonctionnement, telles que : date et heure, algorithme utilisé pour la reconnaissance et le décodage des accréditations acoustiques, clé cryptographique, et dénomination libre.

[0028] La saisie par l'utilisateur-maître des listes d'utilisateurs habilités et des droits d'accès correspondants peut se faire commodément au moyen d'un micro-ordinateur 16 relié au site gestionnaire 10 par une liaison sécurisée, par exemple une liaison IP de type *https* 18.

[0029] L'utilisation d'un micro-ordinateur 16 n'est cependant pas indispensable, l'opérateur-maître pouvant

également saisir les données relatives aux droits d'accès au moyen de son téléphone mobile 20, celui-ci opérant lors de cette phase initiale en tant que terminal connecté au site gestionnaire distant 10 via un opérateur de téléphonie mobile.

[0030] Une fois les diverses données de droits d'accès saisies et introduites dans la base de données 12, il convient de programmer ou reprogrammer une serrure correspondante 22 avec ces droits d'accès, et/ou éventuellement avec d'autres informations propres à la serrure : date et heure, algorithmes, clé cryptographique, dénomination libre, etc.

[0031] Le principe de base de l'invention consiste à opérer cette programmation en faisant reproduire par le haut-parleur du téléphone mobile 20 de l'utilisateur-maître, en tant que signal audio, une accréditation acoustique chiffrée contenant les différentes informations nécessaires à la programmation, le téléphone mobile 20 étant approché de la serrure 22 qui comporte un microphone permettant de capter cette accréditation acoustique chiffrée.

[0032] Les accréditations acoustiques, générées par le moteur cryptographique 14, peuvent être envoyées au téléphone mobile 20 via le réseau de l'opérateur de téléphonie mobile ou MNO (*Mobile Network Operator*) 24, lui-même couplé au site gestionnaire 10 par une liaison sécurisée, par exemple une liaison IP de type *https*, ou simplement par une passerelle téléphonique audio PGW (*Phone GateWay*) 26 permettant de véhiculer les accréditations acoustiques depuis le générateur 14 jusqu'au téléphone 20 par les canaux de transmission audio (canal voix) du réseau de téléphonie mobile. La sécurisation de la liaison entre le réseau mobile 24 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 ci-après d'échange ou de téléchargement d'informations entre le site gestionnaire 10 et le téléphone mobile 20 de l'utilisateur-maître via l'opérateur de réseau mobile 24.

[0033] En variante ou en complément, les accréditations acoustiques chiffrées peuvent être transmises du site gestionnaire 10 au téléphone 20 via le micro-ordinateur 16, par des moyens de couplage appropriés 28 tels que : liaison filaire (câble USB) ou sans fil (*Bluetooth*), via un dispositif de stockage intermédiaire (carte SD ou *MicroSD*, ou *dongle* USB), ou encore par couplage acoustique entre le haut-parleur du micro-ordinateur et le microphone du téléphone mobile 20 (puisque les accréditations acoustiques se présentent sous forme de signaux audio).

[0034] La Figure 2 illustre, sous forme de schéma par blocs, les principaux organes du téléphone mobile 20 et de la serrure 22.

[0035] Le téléphone 20 comporte un microcontrôleur 30 couplé à divers organes périphériques tels que circuit d'émission/réception 32, afficheur 34, clavier 36, mémoire de données 38, carte UICC (*Universal Integrated Cir-*

cuit Card, correspondant à la "carte SIM" pour les fonctions de téléphonie GSM) 40, et transducteur acoustique 42.

[0036] La serrure 22, quant à elle, comprend un microcontrôleur 44 ainsi qu'un système électromécanique 46 permettant de commander le déverrouillage d'un pêne ou d'une poignée 48 sur ordre du microcontrôleur 44. Une mémoire de données 50 conserve diverses données modifiables propres à la serrure, notamment :

- la liste des utilisateurs habilités, ces utilisateurs étant chacun répertorié de façon univoque par un identifiant unique UID (*Unique IDentifier*) d'une clef constituée d'un objet portatif mis à disposition de l'utilisateur habilité, objet qui peut être - de façon non limitative - une carte ou badge à couplage sans contact avec la serrure (de type RFID notamment), ou bien une télécommande radio ou acoustique, ou encore un téléphone mobile identifié par son numéro d'abonné ;
- pour chaque utilisateur, les conditions d'accès autorisées (jours ou plages horaires, date d'expiration du droit d'accès...) ;
- l'identifiant unique UID de la serrure, qui est un identifiant programmable, répertorié dans la base de données DB du site gestionnaire et permettant de reconnaître la serrure entre toutes, de manière univoque ;
- une dénomination libre ("entrée", "garage", ...) ;
- des algorithmes de reconnaissance et de décodage ;
- des clés cryptographiques.

[0037] La serrure comporte ses propres moyens d'alimentation sous forme d'une batterie 52, de manière à la rendre autonome sur le plan électrique. Une alimentation externe est néanmoins possible.

[0038] De façon caractéristique, la serrure 22 est en outre pourvue d'un transducteur acoustique sous forme d'un microphone 54 permettant de capter les signaux sonores environnants, en particulier l'accréditation acoustique qui sera reproduite par le haut-parleur 42 du téléphone 20, et de transformer les signaux acoustiques captés en signaux électriques appliqués au microcontrôleur 44 pour décodage, vérification, et programmation ou reprogrammation dans la mémoire 50 des diverses données modifiables indiquées plus haut.

Mise en oeuvre de l'invention

[0039] 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.

[0040] Au préalable, si les listes d'utilisateurs habilités et de droits d'accès ne sont pas encore dans la base de données DB du site gestionnaire 10, ou si ces données doivent être mises à jour, l'utilisateur-maître (ou un autre utilisateur accrédité par ce dernier) doit les saisir et les

communiquer au site gestionnaire, par les étapes successives suivantes :

1. accès sécurisé (par *login* + mot de passe) au site gestionnaire 10 ;
2. saisie des UID des serrures et des UID des clés des utilisateurs habilités ;
3. le cas échéant, saisie des numéros d'abonnés mobile des utilisateurs habilités à utiliser un téléphone mobile pour ouvrir les serrures (voire même accrédités pour la programmation) ;
4. affectation éventuelle de noms abrégés de ports aux UID des serrures, et/ou de noms abrégés d'utilisateurs aux UID des clés ;
5. affectation des droits et conditions d'accès aux différents utilisateurs ;
6. validation des saisies précédentes ;
7. le cas échéant (voir plus bas), délivrance par le site gestionnaire du (des) numéro(s) d'appel(s) montant(s) à composer par l'utilisateur-maître pour programmer chaque serrure, cette information pouvant également lui être envoyée par SMS, MMS, e-mail, messagerie instantanée, etc.

[0041] Lorsqu'il souhaite programmer ou reprogrammer une serrure, l'utilisateur-maître reçoit du site gestionnaire 10 les données qu'il y a lieu d'inscrire ou de mettre à jour dans la mémoire 50 de la serrure 22, via le micro-ordinateur 16 et le couplage 28, ou bien directement via l'opérateur de téléphonie mobile 24.

[0042] Comme indiqué plus haut, les données reçues du site gestionnaire distant 10 peuvent comprendre, outre les droits d'accès attachés à chaque utilisateur habilité, un certain nombre d'informations propres à la serrure telles que : algorithme utilisé, clé cryptographique, nom abrégé, etc. La mise à jour pourra également concerner la date et l'heure de l'horloge interne du microcontrôleur 44, à distance depuis le site gestionnaire 10.

[0043] Les données de programmation peuvent également comprendre des données qui sont propres au téléphone mobile 20 de l'utilisateur-maître, telles que :

- la date et l'heure, lorsque l'on veut mettre à jour ces informations depuis le téléphone mobile au lieu de le faire depuis le site gestionnaire 10) ;
- le numéro IMEI qui identifie le téléphone de manière unique ;
- l'identifiant de la carte UICC 40 (identifiant de carte SIM) ;
- éventuellement, des informations de localisation géographique donnant la position du téléphone 20 au moment de la programmation (coordonnées GPS si le téléphone est équipé de cette fonction, ou localisation approchée d'après la cellule du réseau depuis laquelle émet le téléphone).

[0044] Pour programmer la serrure, l'utilisateur présente son téléphone 20 devant la serrure 22 qu'il souhaite

programmer et déclenche l'émission, sous forme de signal sonore, de l'accréditation acoustique correspondante. Cette émission peut également être déclenchée (comme on l'expliquera plus bas) par la simple réponse ou le décrochage à un appel descendant à l'attention du téléphone mobile de l'utilisateur-maître provenant du site gestionnaire distant.

[0045] L'accréditation acoustique, captée par le microphone 54 de la serrure, est analysée par le microcontrôleur 44 qui, en cas de conformité, commande la programmation ou la mise à jour des informations correspondantes dans la mémoire 50.

[0046] Le fait que l'accréditation acoustique chiffrée soit une accréditation à usage unique empêche toute fraude par enregistrement et duplication de l'accréditation.

[0047] Une précaution permettant d'augmenter la sécurité consiste à prévoir une validation supplémentaire par l'utilisateur, par exemple l'entrée d'un code personnel de type "PIN code" avant la délivrance de l'accréditation acoustique, ou une validation de type biométrique, par un lecteur biométrique incorporé au téléphone ou au moyen d'un système de reconnaissance d'empreintes vocales utilisant le microphone du téléphone (l'empreinte biométrique spécifique pouvant être stockée dans la mémoire 38 du téléphone, ou bien dans la carte UICC 40, ou encore dans la base de données 12).

[0048] Avantageusement, la serrure 22 est pourvue de moyens permettant d'émettre en retour un signal acoustique validant la bonne exécution de l'opération de programmation.

[0049] Il est possible d'utiliser à cet effet le transducteur 54 de la serrure en le faisant fonctionner en mode inversé (pour émettre des signaux sonores au lieu de les capter), ou bien de prévoir un transducteur spécifique pour reproduire des signaux sonores.

[0050] Le signal sonore ainsi émis par la serrure sera capté par le microphone du téléphone 20 et traduit par une applique du téléphone en un message sonore ou visuel à destination de l'utilisateur-maître pour confirmer (ou infirmer) la bonne exécution de la programmation. L'applique peut également garder une trace des serrures qui ont été programmées et de celles qui ne l'ont pas encore été, par exemple par affichage d'une liste de serrures, pour alerter l'utilisateur-maître s'il a oublié de programmer certaines d'entre elles.

[0051] Avantageusement, il est possible de profiter du retour d'informations après programmation de la serrure pour récupérer des données mémorisées dans cette dernière, ou des informations d'état telles que signal de batterie faible, besoin d'entretien, dysfonctionnement, preuve d'ouverture, etc. Ces données ou informations pourront être traduites par l'applique du téléphone en messages d'alerte ("*batterie faible*", ...) affichés sur l'écran du téléphone, ces messages étant répétés si nécessaire à intervalles réguliers.

[0052] Par ailleurs, ces données ou informations pourront être avantageusement envoyées vers le site ges-

tionnaire par l'intermédiaire du réseau mobile 24, profitant ainsi de l'établissement par l'utilisateur-maître 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). En d'autres termes, l'utilisateur-maître, lors de la programmation ou reprogrammation, devient pour le système une source d'informations. Cette manière de procéder est particulièrement avantageuse ici, car il s'agit de serrures de type *stand alone*, c'est-à-dire fonctionnant de manière entièrement autonome sans être raccordées à un quelconque réseau local qui permettrait d'échanger des données ou de transmettre certains messages d'état ou d'anomalie.

[0053] Avantageusement, avant d'opérer la programmation proprement dite, le téléphone 20 reproduit une accréditation spécifique d'ouverture de session, propre à faire entrer la serrure dans un mode de programmation différent de son fonctionnement normal. Une fois achevée la programmation, une autre accréditation acoustique spécifique fait sortir la serrure du mode de programmation et la replace dans son mode de fonctionnement normal. Cette manière de procéder est particulièrement avantageuse pour augmenter la sécurité lorsque la serrure est une serrure à commande acoustique, c'est-à-dire que le déverrouillage ultérieur par l'utilisateur autorisé se fera par émission d'une accréditation acoustique chiffrée, d'une nature semblable à l'accréditation acoustique ayant servi à la programmation.

[0054] Un autre perfectionnement vise à éviter une fraude consistant à démonter une serrure déjà programmée pour la remonter, telle quelle, à un autre emplacement. A cet effet, la serrure 22 mémorise les informations de localisation géographique (coordonnées GPS ou autres) du téléphone 20 au moment où celui-ci opère la programmation. La serrure comprend par ailleurs des moyens pour recueillir les informations de localisation géographique du téléphone de l'utilisateur qui se présentera ultérieurement comme un utilisateur habilité, et comparer ces coordonnées à celles qui ont été mémorisées au moment de la programmation, et l'ouverture ne sera autorisée que si les informations concordent, à une marge d'erreur donnée près. En absence de couverture réseau ou GPS au moment où l'accès est demandé par l'utilisateur, la donnée de localisation utilisée sera la donnée la plus récente obtenue avant la perte de contact, avec dans ce cas une marge d'erreur supérieure, définie par l'administrateur du système.

[0055] On va maintenant décrire plusieurs manières dont le site gestionnaire 10 peut délivrer l'accréditation au téléphone mobile 20, notamment lorsque cette délivrance intervient via le réseau de l'opérateur mobile 24.

1°) Mode en ligne (délivrance directe de l'accréditation)

[0056] Lorsqu'il souhaite programmer la serrure 22, l'utilisateur-maître 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 un procédé de type *call back* : dans ce cas, l'utilisateur-maître entre en contact téléphonique ou par un message (SMS, MMS, e-mail, messagerie instantanée, etc.) avec le site gestionnaire, qui ne lui répond pas immédiatement, mais après raccrochage fait sonner le téléphone mobile 20 pour que l'utilisateur-maître établisse à nouveau le contact avec le site gestionnaire (le numéro rappelé par le site gestionnaire étant le numéro d'abonné, répertorié dans la base de données DB, de l'utilisateur-maître ou de tout autre utilisateur autorisé par ce dernier).

[0057] Si les paramètres de programmation ont été préalablement définis de la manière indiquée plus haut, il suffit à l'utilisateur-maître de valider ces paramètres ainsi que son numéro d'abonné de téléphonie mobile auprès du site gestionnaire 10.

[0058] La simple réponse du site gestionnaire à l'appel de l'utilisateur-maître, ou en cas de *call-back* le décrochage par ce dernier, provoque la transmission immédiate et directe de l'autorisation l'accréditation acoustique chiffrée.

[0059] Dans ce mode de réalisation, quelle que soit la manière dont l'utilisateur-maître entre en contact avec le site gestionnaire distant, celui-ci délivre l'accréditation acoustique directement à l'utilisateur-maître, "en ligne", sans stockage intermédiaire.

[0060] 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 applique 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 l'habilitation de l'utilisateur-maître. De plus, grâce à ce mode en ligne, il est possible de disposer au niveau du site gestionnaire d'informations sur l'utilisation faite de l'accréditation acoustique, notamment la date et l'heure de la programmation, et éventuellement la situation géographique de cette opération (par identification de la cellule du réseau d'où l'utilisateur-maître appelle).

[0061] En revanche, ce mode implique de disposer d'un accès au réseau mobile, ce qui n'est pas toujours possible (caves, 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.

[0062] En cas de pluralité de serrures, il est possible de prévoir une validation par étapes après chaque serrure, ou bien d'utiliser un numéro d'appel différent pour chaque serrure.

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

[0063] Ce mode est utilisable notamment si l'accès au réseau n'est pas assuré au moment de l'utilisation. Dans ce cas, l'utilisateur-maître se connecte à l'avance au site gestionnaire et reçoit de celui-ci l'accréditation correspondant à la serrure qu'il veut programmer, ou plusieurs de ces accréditations, en cas de pluralité de serrures à programmer. Ces accréditations sont stockées de façon sûre dans le téléphone ou dans une mémoire périphérique du téléphone (par exemple une carte SD ou *MicroSD*).

[0064] Ici encore, le contact préalable avec le site gestionnaire 10 peut être établi soit directement sur envoi au site d'une requête émise par le téléphone mobile de l'utilisateur-maître, soit via un message descendant émis par le site gestionnaire distant vers un numéro d'abonné préalablement spécifié par l'utilisateur-maître (ou le numéro de tout autre utilisateur autorisé par ce dernier).

[0065] Lorsque l'utilisateur-maître veut programmer une serrure, il lance une application intégrée à son téléphone qui recherche l'accréditation correspondante parmi celles qui ont été stockées, la reproduit pour programmer la serrure, puis la supprime de la mémoire. Et ainsi de suite pour utiliser les accréditations suivantes.

[0066] L'application permettant cette mise en oeuvre est une applique 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-maître un lien permettant le téléchargement de l'applique.

3°) Mode hors ligne

[0067] 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 applique ou *applet*, notamment de type *cardlet* (stockée dans la carte UICC 40) ou *midlet* (stockée dans la mémoire 38 de l'appareil téléphonique). Cette applique 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.

[0068] 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 40 pour des raisons de sécurité. Cette clé cryptographique, combinée à l'applique, permettra de constituer un générateur

cryptographique au sein du téléphone 20. Lorsqu'il souhaite programmer une serrure, l'utilisateur-maître commande la génération de l'accréditation acoustique par l'applique interne et sa reproduction par le transducteur de son téléphone.

4°) Mode "pièce jointe"

[0069] Ce mode de mise en oeuvre est une variante du mode semi-en ligne.

[0070] 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.

[0071] 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 applique spécifique, de conserver celle-ci dans le téléphone et de la faire exécuter par ce dernier le moment venu. Le fichier peut également être téléchargé via le micro-ordinateur 16 et le couplage 28 avec le téléphone 20.

Revendications

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

- un site gestionnaire (10) distant, comprenant :

- une base de données (12) de dispositifs de serrure et d'utilisateurs habilités, avec pour chaque dispositif de serrure un identifiant unique associé, une liste d'utilisateurs habilités avec des données correspondantes de droits d'accès, et éventuellement des données additionnelles ;

- au moins un dispositif de serrure (22) comprenant :

- une mémoire de données (50) contenant :
 - i) un identifiant unique de la serrure, répertorié dans la base de données du site gestionnaire et permettant de reconnaître la serrure entre toutes, de manière univoque ;
 - ii) des droits d'accès préalablement définis ; et

- des circuits électroniques pour la commande conditionnelle d'organes mécaniques de verrouillage/déverrouillage en

fonction desdits droits d'accès,
système **caractérisé**
en ce que lesdits droits d'accès sont définis
par

- i) une liste des utilisateurs habilités, chacun répertorié de façon univoque par un identifiant unique d'une clef constituée d'un objet portatif mis à disposition de cet utilisateur habilité ; et
- ii) pour chaque utilisateur, les conditions d'accès autorisées,

et en ce qu'il comprend en outre :

- dans le site gestionnaire :

- un générateur (14) de données d'accréditation propres à permettre la programmation des dispositifs de serrure par les droits d'accès répertoriés dans la base de données, ces accréditations étant des accréditations acoustiques chiffrées en forme de signaux audio à usage unique ;

- un téléphone mobile (20) à disposition de l'utilisateur-maître, comprenant un transducteur électro-acoustique (42) apte à reproduire lesdites accréditations acoustiques ; et

- des moyens de transmission sécurisée desdites données d'accréditation du site gestionnaire au téléphone mobile de l'utilisateur-maître ;

- dans le dispositif de serrure (22) :

- un transducteur électro-acoustique (54) apte à capter les accréditations acoustiques reproduites par le transducteur du téléphone préalablement placé à proximité du dispositif de serrure ; et
- des moyens pour reconnaître, analyser et authentifier les accréditations acoustiques captées par le transducteur, et opérer, sur reconnaissance d'une accréditation acoustique conforme, une programmation ou une reprogrammation des droits d'accès.

2. Le système de la revendication 1, dans lequel les moyens de transmission sécurisée des données d'accréditation du site gestionnaire au téléphone mobile de l'utilisateur-maître comprennent des moyens (28) de couplage de ce téléphone mobile avec un terminal informatique (16) relié au site gestionnaire.

3. Le système de la revendication 1, dans lequel les moyens de transmission sécurisée des données d'accréditation du site gestionnaire au téléphone mobile de l'utilisateur-maître comprennent un opé-

rateur de réseau mobile (24) couplé au site gestionnaire et au téléphone de l'utilisateur-maître.

4. Le système de la revendication 1, dans lequel, pour la génération des données d'accréditation à transmettre au téléphone, le site gestionnaire est apte à combiner les données de droits d'accès propres aux utilisateurs habilités avec des données additionnelles propres à la serrure et obtenues au niveau du site gestionnaire, et à générer une accréditation acoustique fonction à la fois desdites données de droits d'accès et desdites données additionnelles.

5. Le système de la revendication 1, dans lequel le téléphone est apte à combiner les données d'accréditation transmises par le site gestionnaire avec des données additionnelles inhérentes au téléphone et obtenues localement, et à générer une accréditation acoustique fonction à la fois desdites données d'accréditation et desdites données additionnelles.

6. Le système de la revendication 5, dans lequel lesdites données additionnelles comprennent en outre une information de localisation géographique du téléphone au moment de l'opération de programmation, et le dispositif de serrure comprend en outre des moyens pour mémoriser cette information de localisation géographique à la programmation, et la comparer ultérieurement avec une information de localisation géographique d'un téléphone d'un utilisateur au moment d'une tentative d'ouverture du dispositif de serrure par cet utilisateur.

7. Le système de la revendication 1, dans lequel le téléphone est apte à :

- préalablement à la reproduction des accréditations acoustiques de programmation des droits d'accès, reproduire une accréditation spécifique d'ouverture de session propre à faire entrer le dispositif de serrure dans un mode de programmation ; et
- éventuellement, après reproduction desdites accréditations acoustiques de programmation, reproduire une accréditation spécifique de fermeture de session propre à faire sortir le dispositif de serrure dudit mode de programmation.

8. 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 propres au dispositif de serrure ; et
- le téléphone comprend un transducteur électro-acoustique apte à capter lesdits signaux en retour.

9. Le système de la revendication 8, 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 fonction desdites données propres au dispositif de serrure. 5
10. Le système de la revendication 8, dans lequel le téléphone comprend en outre des moyens pour transmettre au site gestionnaire lesdits signaux en retour codés par lesdites données propres au dispositif de serrure. 10
11. Le système de la revendication 1, dans lequel le téléphone comprend en outre des moyens pour mémoriser et mettre à jour une liste de dispositifs de serrure déjà programmés et de dispositifs de serrure non encore programmés. 15
12. 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-maître au téléphone. 20 25
13. Le système de la revendication 1, comportant des moyens aptes à :
- vérifier l'habilitation de l'utilisateur-maître à opérer une programmation du dispositif de serrure ; 30
 - générer une accréditation acoustique par le générateur (14) du site gestionnaire ; 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. 35
14. Le système de la revendication 1, comportant des moyens aptes à : 40
- vérifier l'habilitation de l'utilisateur-maître à opérer une programmation du dispositif de serrure ; 45
 - générer une accréditation acoustique par le générateur (14) du site gestionnaire ; et
 - activer une applique interne du téléphone pour télécharger ladite accréditation et mémoriser celle-ci dans une mémoire (32) du téléphone, puis, dans un second temps :
 - activer l'applique interne pour reproduction de l'accréditation par le transducteur du téléphone préalablement placé à proximité du transducteur du dispositif de serrure. 50 55
15. Le système de la revendication 1, comportant en outre des moyens de mise à jour à distance, depuis

le site gestionnaire, de la date et de l'heure de l'horloge interne du dispositif de serrure.

16. Le système de la revendication 1, comportant en outre des moyens de mise à jour à distance, depuis le site gestionnaire : d'algorithmes de reconnaissance et de décodage, de clefs cryptographiques et/ou d'une dénomination libre conservés dans la mémoire de données (50) du dispositif de serrure.

Claims

1. A secure system for controlling the opening of lock devices, comprising:

- a remote management site (10) comprising:

- a database (12) of lock devices and of authorised users, with, for each lock device, an associated unique identifier, a list of authorised users with corresponding data of access rights, and optionally additional data;

- at least one lock device (22) comprising:

- a data memory (50) containing:

- i) a unique identifier of the lock, listed in the database of the management site and used for recognizing the lock amongst them all, on a one-to-one basis;
- ii) previously defined access rights; and

- electronic circuits for the conditional control of mechanical locking/unlocking members as a function of the said access rights, the said system being **characterized in that** the said access rights are defined by

- i) a list of authorised users, each listed on a one-to-one basis by a unique identifier of a key consisting of a portable object made available to this authorised user; and
- ii) for each user, the authorised access

conditions,
and **in that** it also comprises:

- in the management site:

- a generator (14) of accreditation data suitable for allowing the programming of the lock devices by the access rights listed in the database, these accreditations being

acoustic accreditations encrypted in the form of single-use audio signals;

- a mobile telephone (20) made available to the master user, comprising an electro-acoustic transducer (42) capable of reproducing the said acoustic accreditations; and
 - means for secure transmission of the said accreditation data from the management site to the mobile telephone of the master user;
 - in the lock device (22):
 - an electro-acoustic transducer (54) capable of sensing the acoustic accreditations reproduced by the transducer of the telephone previously placed close to the lock device; and
 - means for recognizing, analysing and authenticating the acoustic accreditations sensed by the transducer and, on recognition of a correct acoustic accreditation, carrying out a programming or a reprogramming of the access rights.
2. The system of Claim 1, in which the means for secure transmission of the accreditation data from the management site to the mobile telephone of the master user comprise means (28) for coupling this mobile telephone with a computer terminal (16) connected to the management site.
 3. The system of Claim 1, in which the means for secure transmission of the accreditation data from the management site to the mobile telephone of the master user comprise a mobile network operator (24) coupled to the management site and to the telephone of the master user.
 4. The system of Claim 1, in which, for the generation of the accreditation data to be transmitted to the telephone, the management site is capable of combining the data of access rights specific to the authorised users with additional data specific to the lock and obtained at the management site, and of generating an acoustic accreditation as a function of both the said data of access rights and of the said additional data.
 5. The system of Claim 1, in which the telephone is capable of combining the accreditation data transmitted by the management site with additional data inherent in the telephone and obtained locally, and of generating an acoustic accreditation as a function of both the said accreditation data and the said additional data.
 6. The system of Claim 5, in which the said additional data also comprise an item of geographic location information of the telephone at the time of the programming operation, and the lock device also comprises means for storing this item of geographic location information on the programming, and subsequently comparing it with an item of geographic location information of a telephone of a user at the time of an attempt by this user to open the lock device.
 7. The system of Claim 1, in which the telephone is capable of:
 - prior to the reproduction of the acoustic accreditations of programming of the access rights, reproducing a specific accreditation for the opening of a session suitable for having the lock device entered in a programming mode; and
 - optionally, after reproduction of the said acoustic accreditations of programming, reproducing a specific accreditation of closure of a session suitable for having the lock device taken out of the said programming mode.
 8. The system of Claim 1, in which:
 - the lock device comprises an electro-acoustic transducer capable of reproducing the return acoustic signals, generated by the lock device and encoded by data specific to the lock device; and
 - the telephone comprises an electro-acoustic transducer capable of sensing the said return signals.
 9. The system of Claim 8, in which the telephone also comprises means for decoding the said return signals and displaying, as required, to the user a message as a function of the said data specific to the lock device.
 10. The system of Claim 8, in which the telephone also comprises means for transmitting to the management site the said return signals encoded by the said data specific to the lock device.
 11. The system of Claim 1, in which the telephone also comprises means for storing and updating a list of lock devices already programmed and of lock devices not yet programmed.
 12. The system of Claim 1, also comprising means for making the reproduction of the acoustic accreditation by the transducer of the telephone conditional upon the prior presentation of an item of personal validation data delivered by the master user to the telephone.
 13. The system of Claim 1, comprising means capable of:

- verifying the authorisation of the master user to carry out a programming of the lock device;
 - generating an acoustic accreditation by the generator (14) of the management site; and
 - transmitting this accreditation to the telephone, for direct reproduction by the transducer of the latter previously placed close to the transducer of the lock device. 5
14. The system of Claim 1, comprising means capable of: 10
- verifying the authorization of the master user to carry out a programming of the lock device;
 - generating an acoustic accreditation by the generator (14) of the management site; and
 - activating an internal applet of the telephone in order to download the said accreditation and store the latter in a memory (32) of the telephone, then, secondly; 20
 - to activate the internal applet for reproduction of the accreditation by the transducer of the telephone previously placed close to the transducer of the lock device. 25
15. The system of Claim 1, also comprising means for remotely updating, from the management site, the date and time of the internal clock of the lock device.
16. The system of Claim 1, also comprising means for remotely updating, from the management site: 30
- recognition and decoding algorithms, cryptographic keys and/or a free denomination, which items are kept in the data memory (50) of the lock device. 35

Patentansprüche

1. Gesichertes System zur Öffnungssteuerung von Schlossvorrichtungen, das Folgendes aufweist: 40
- einen fernen Manager-Standort (10), der Folgendes enthält: 45
 - eine Datenbank (12) von Schlossvorrichtungen und von berechtigten Benutzern, mit für jede Schlossvorrichtung einer einzigen zugeordneten Kennung, einer Liste von berechtigten Benutzern mit entsprechenden Daten von Zugangsrechten, und ggf. zusätzlichen Daten; 50
 - mindestens eine Schlossvorrichtung (22), die Folgendes enthält: 55
 - einen Datenspeicher (50), der Folgendes

enthält:

- i) eine einzige Kennung des Schlosses, die in der Datenbank des Manager-Standorts verzeichnet ist und es ermöglicht, das Schloss unter allen eindeutig zu erkennen;
- ii) vorab definierte Zugangsrechte; und

• elektronische Schaltkreise für die bedingte Steuerung von mechanischen Verriegelungs-/Entriegelungsorganen abhängig von den Zugangsrechten, wobei das System **dadurch gekennzeichnet ist, dass** die Zugangsrechte definiert sind durch

- i) eine Liste der berechtigten Benutzer, von denen jeder eindeutig durch eine einzige Kennung eines Schlüssels verzeichnet ist, der aus einem tragbaren Gegenstand besteht, der diesem berechtigten Benutzer zur Verfügung gestellt wird; und
- ii) für jeden Benutzer, die genehmigten Zugangsbedingungen,

und **dass** es außerdem Folgendes enthält:

- im Manager-Standort:

• einen Generator (14) von Akkreditierungsdaten, die geeignet sind, um die Programmierung der Schlossvorrichtungen durch die in der Datenbank verzeichneten Zugangsrechte zu erlauben, wobei diese Akkreditierungen akustische Akkreditierungen sind, die in Form von Einweg-Audiosignalen verschlüsselt sind;

- ein dem Master-Benutzer zur Verfügung stehendes Mobiltelefon (20), das einen elektroakustischen Wandler (42) enthält, der die akustischen Akkreditierungen reproduzieren kann; und

- Einrichtungen zur gesicherten Übertragung der Akkreditierungsdaten vom Manager-Standort zum Mobiltelefon des Master-Benutzers; und

- in der Schlossvorrichtung (22):

• einen elektro-akustischen Wandler (54), der die akustischen Akkreditierungen erfassen kann, die vom Wandler des Telefons reproduziert werden, der vorher in der Nähe der Schlossvorrichtung angeordnet wird; und

• Einrichtungen, um die vom Wandler erfas-

- sten akustischen Akkreditierungen zu erkennen, zu analysieren und zu authentifizieren, und bei Erkennung einer konformen akustischen Akkreditierung eine Programmierung oder eine Neuprogrammierung der Zugangsrechte durchzuführen.
2. System nach Anspruch 1, bei dem die Einrichtungen zur gesicherten Übertragung der Akkreditierungsdaten vom Manager-Standort zum Mobiltelefon des Master-Benutzers Einrichtungen (28) zum Koppeln dieses Mobiltelefons mit einem EDV-Endgerät (16) enthalten, das mit dem Manager-Standort verbunden ist.
3. System nach Anspruch 1, bei dem die Einrichtungen zur gesicherten Übertragung der Akkreditierungsdaten vom Manager-Standort zum Mobiltelefon des Master-Benutzers einen Mobilfunknetz-Operator (24) enthalten, der mit dem Manager-Standort und mit dem Telefon des Master-Benutzers gekoppelt ist.
4. System nach Anspruch 1, bei dem zur Generierung der zum Telefon zu übertragenden Akkreditierungsdaten der Manager-Standort die den berechtigten Benutzern eigenen Zugangsrechten mit dem Schloss eigenen und auf der Ebene des Manager-Standorts erhaltenen zusätzlichen Daten kombinieren und eine akustische Akkreditierung generieren kann, die sowohl von den Zugangsrechten als auch von den zusätzlichen Daten abhängt.
5. System nach Anspruch 1, bei dem das Telefon die vom Manager-Standort übertragenen Akkreditierungsdaten mit zusätzlichen Daten kombinieren kann, die dem Telefon inhärent sind und lokal erhalten werden, und eine akustische Akkreditierung generieren kann, die sowohl von den Akkreditierungsdaten als auch von den zusätzlichen Daten abhängt.
6. System nach Anspruch 5, bei dem die zusätzlichen Daten außerdem eine Information über die geographische Lokalisierung des Telefons zum Zeitpunkt der Durchführung der Programmierung enthalten und die Schlossvorrichtung außerdem Einrichtungen enthält, um diese Information über die geographische Lokalisierung bei der Programmierung zu speichern und sie später mit einer Information über die geographische Lokalisierung eines Telefons eines Benutzers zum Zeitpunkt eines Öffnungsversuchs der Schlossvorrichtung durch diesen Benutzer zu vergleichen.
7. System nach Anspruch 1, bei dem das Telefon in der Lage ist:
- vor der Reproduktion der akustischen Pro-
- grammierungs-Akkreditierungen der Zugangsrechte eine spezifische Sitzungseröffnungs-Akkreditierung zu reproduzieren, die geeignet ist, um die Schlossvorrichtung in eine Programmierungsbetriebsart zu bringen; und
- ggf. nach Reproduktion der akustischen Programmierungs-Akkreditierungen eine spezifische Sitzungsschließungs-Akkreditierung zu reproduzieren, die geeignet ist, um die Schlossvorrichtung aus der Programmierungsbetriebsart herauszubringen.
8. System nach Anspruch 1, bei dem:
- die Schlossvorrichtung einen elektro-akustischen Wandler enthält, der akustische Rücksignale reproduzieren kann, die von der Schlossvorrichtung generiert und von der Schlossvorrichtung eigenen Daten codiert werden; und
 - das Telefon einen elektro-akustischen Wandler enthält, der die Rücksignale auffangen kann.
9. System nach Anspruch 8, bei dem das Telefon außerdem Einrichtungen enthält, um die Rücksignale zu decodieren und ggf. dem Benutzer eine Mitteilung anzuzeigen, die von den der Schlossvorrichtung eigenen Daten abhängt.
10. System nach Anspruch 8, bei dem das Telefon außerdem Einrichtungen enthält, um an den Manager-Standort die von den der Schlossvorrichtung eigenen Daten codierten Rücksignale zu übertragen.
11. System nach Anspruch 1, bei dem das Telefon außerdem Einrichtungen enthält, um eine Liste von bereits programmierten Schlossvorrichtungen und von noch nicht programmierten Schlossvorrichtungen zu speichern und zu aktualisieren.
12. System nach Anspruch 1, das außerdem Einrichtungen enthält, um die Reproduktion der akustischen Akkreditierung durch den Wandler des Telefons von der vorhergehenden Vorlage eines persönlichen Validierungsdatenwerts abhängig zu machen, der vom Master-Benutzer an das Telefon geliefert wird.
13. System nach Anspruch 1, das Einrichtungen aufweist, die in der Lage sind:
- die Berechtigung des Master-Benutzers zur Durchführung einer Programmierung der Schlossvorrichtung zu überprüfen;
 - eine akustische Akkreditierung durch den Generator (14) des Manager-Standorts zu generieren; und
 - diese Akkreditierung an das Telefon zur direkten Reproduktion durch dessen Wandler zu

übertragen, der vorher in der Nähe des Wandlers der Schlossvorrichtung angeordnet wurde.

14. System nach Anspruch 1, das Einrichtungen aufweist, die in der Lage sind: 5
- die Berechtigung des Master-Benutzers zur Durchführung einer Programmierung der Schlossvorrichtung zu überprüfen; 10
 - eine akustische Akkreditierung durch den Generator (14) des Manager-Standorts zu generieren; und
 - ein internes Applet des Telefons zu aktivieren, um die Akkreditierung herunterzuladen und sie in einem Speicher (32) des Telefons zu speichern, 15
- dann:
- das interne Applet zur Reproduktion der Akkreditierung durch den Wandler des Telefons zu aktivieren, der vorher in der Nähe des Wandlers der Schlossvorrichtung angeordnet wurde. 20
15. System nach Anspruch 1, das außerdem Einrichtungen zur Fernaktualisierung, ausgehend vom Manager-Standort, des Datums und der Uhrzeit des internen Taktgebers der Schlossvorrichtung aufweist. 25
16. System nach Anspruch 1, das außerdem Einrichtungen zur Fernaktualisierung, ausgehend vom Manager-Standort, aufweist von: Erkennungs- und Decodierungsalgorithmen, kryptographischen Schlüsseln und/oder einer freien Bezeichnung, die im Datenspeicher (50) der Schlossvorrichtung aufbewahrt werden. 30

35

40

45

50

55

FIG. 1

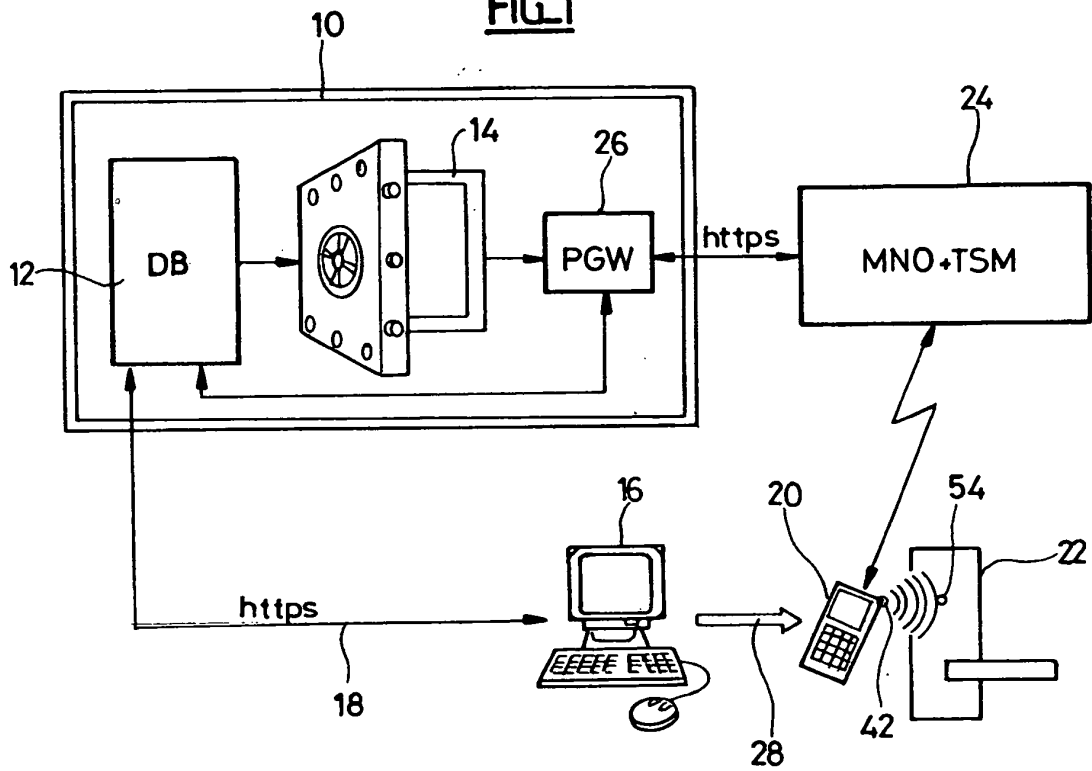
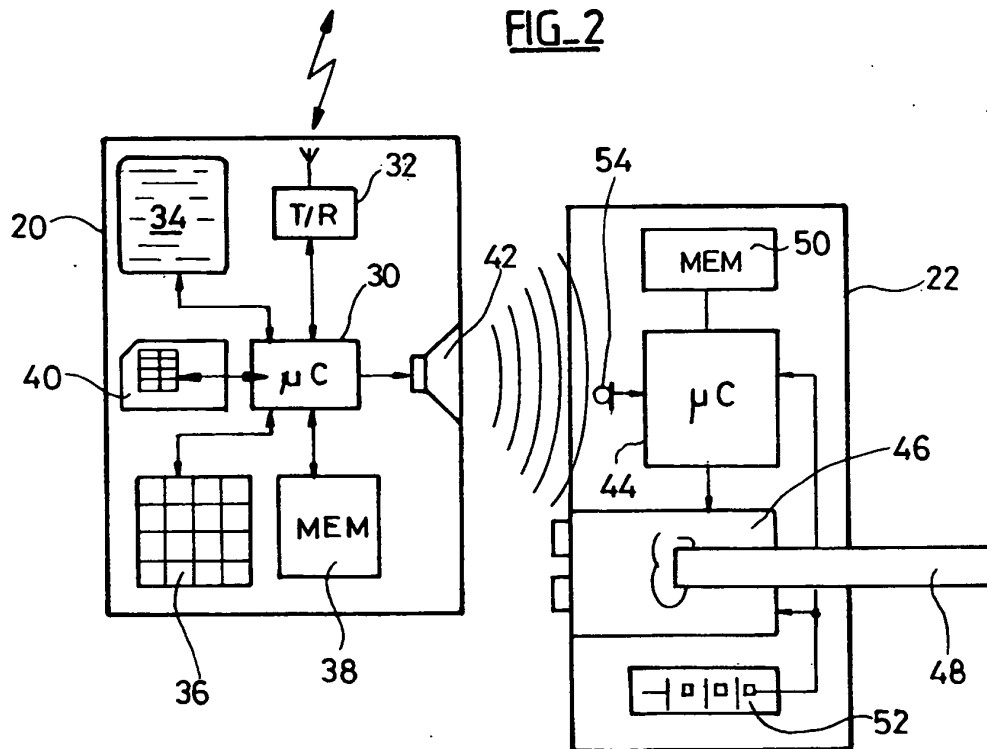


FIG. 2



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 03093997 A1 [0006] [0016]
- US 5933090 A [0006]
- WO 2008107595 A2 [0014]