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

(11) **EP 2 306 407 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
06.04.2011 Bulletin 2011/14

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

(21) Numéro de dépôt: **09170475.9**

(22) Date de dépôt: **16.09.2009**

(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)

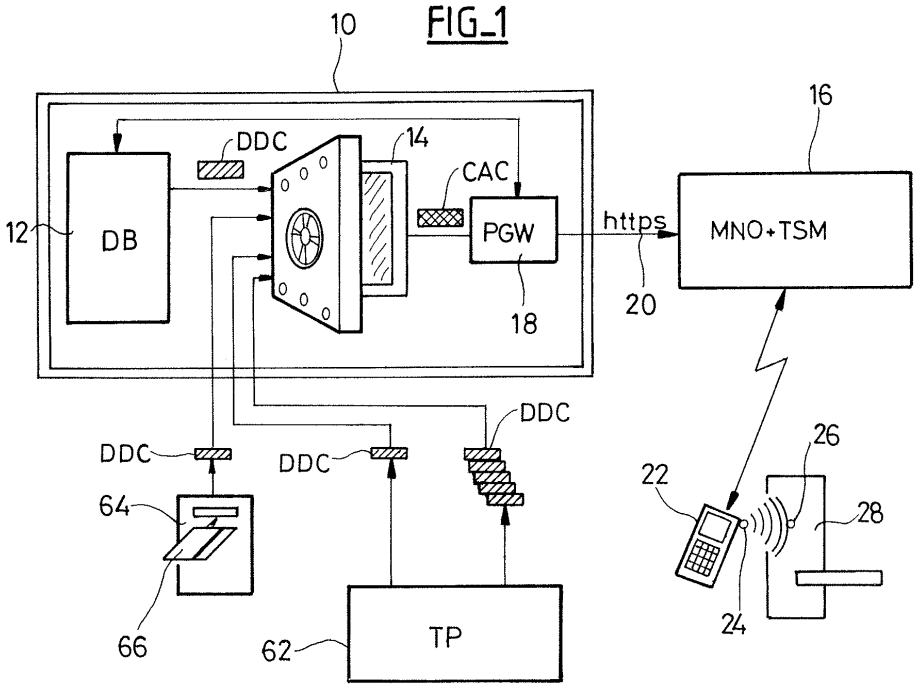
(72) Inventeur: **Metivier, Pascal**
78810 Feucherolles (FR)

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

(54) **Système de gestion sécurisée de serrures à commande numérique, adapté à un fonctionnement par accréditations acoustiques chiffrées**

(57) Ce système met en oeuvre un téléphone mobile (22) à disposition d'un utilisateur habilité à ouvrir une serrure (28). Un site gestionnaire (10) distant comprend une base de données (12) d'utilisateurs habilités identifiés par leur numéro de téléphone mobile, ainsi qu'un générateur (14) de données d'accréditation. Les accréditations sont des accréditations acoustiques chiffrées (CAC) en forme de signaux audio à usage unique, et elles sont générées à partir des données numériques d'accréditation (DDC) normalement mises en oeuvre par la serrure lorsque celle-ci est utilisée avec un badge ou une carte. Le système comprend des moyens (16, 18, 20) de transmission sécurisée des accréditations acoustiques au téléphone de l'utilisateur. La serrure (22) capte les accréditations acoustiques reproduites par le téléphone préalablement placé à proximité de la serrure, extrait les données numériques d'accréditation à partir des accréditations acoustiques chiffrées captées, et applique les données numériques d'accréditation ainsi extraites aux moyens d'analyse, d'authentification et de commande de la serrure.

FIG_1



EP 2 306 407 A1

Description

[0001] L'invention concerne les dispositifs de serrure commandés électriquement au moyen d'une clé dématérialisée et chiffrée, cette clé pouvant être véhiculée par un objet portatif détenu par l'utilisateur tel qu'une carte magnétique, une carte à puce, un badge ou une carte sans contact, etc.

[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.

[0004] L'objet portatif, lorsqu'il est approché de la serrure, joue le rôle d'une clé permettant d'en commander l'ouverture au moyen d'une donnée ci-après désignée "accréditation" (*credential*). Diverses techniques de codage et de cryptage peuvent être implémentées dans la serrure et/ou dans l'objet portatif pour assurer une protection à l'encontre de manipulations frauduleuses et sécuriser la communication entre l'objet portatif et la serrure. On connaît de nombreux systèmes à cartes magnétiques, ou encore à cartes ou badges à microcircuit mettant en oeuvre avec la serrure un couplage galvanique (carte à puce à contacts) ou non galvanique (carte à couplage inductif ou carte de type RFID). Ce couplage assure entre serrure et badge une communication permettant notamment à la serrure de lire dans la mémoire du badge la donnée d'accréditation afin de commander l'ouverture si cette donnée est reconnue conforme.

[0005] 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. 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] Un autre inconvénient est lié à la variété des techniques mises en oeuvre, chaque fabricant ayant ses spécifications propres aussi bien au niveau de la couche physique (choix technologique du couplage : inductif, RF, magnétique, galvanique, etc.) qu'au niveau du format des données et des protocoles d'échange de ces données entre le lecteur et l'objet portatif. Cette variété des techniques, liée aux choix technologiques et aux implémentations propres aux différents constructeurs, est un frein à l'interopérabilité, à la standardisation des matériels et des procédures et à l'évolution technologique, ce qui empêche la généralisation rapide de ces techniques, malgré leurs avantages incontestables.

[0007] De plus, le système est un système figé, car 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 nécessité de manipulations physiques et de déplacements.

[0008] L'un des buts de l'invention est de proposer une technique alternative de gestion et de commande de serrures qui puisse compléter les techniques existantes, ou même se substituer à elles, sans nécessiter de modifications substantielles tant au niveau du matériel que du logiciel, et qui offre un niveau de sécurité maximal, une très grande souplesse de mise en oeuvre et soit utilisable sans recours à un objet portatif spécifique. Comme on le verra par la suite, la technique de l'invention est utilisable au moyen de n'importe quel téléphone mobile conventionnel servant l'objet portatif véhiculant la clé de commande de la serrure, sans que l'utilisateur n'ait besoin de recourir à un objet portatif spécifique et dédié, tel que badge ou carte.

[0009] Le système de l'invention pourra être ainsi immédiatement généralisé au plus grand nombre, en étant utilisable par tout un chacun à partir d'un téléphone de modèle standard, non modifié, mais en bénéficiant de toute la sécurité et de toute la souplesse propres aux techniques cryptographiques modernes.

[0010] Du point de vue du fabricant de serrures, la technique de l'invention permettra d'adapter sans modification majeure le parc de serrures existantes, sans devoir remplacer ni les éléments matériels ni le logiciel déjà intégrés à la serrure. On verra en effet que l'invention est parfaitement compatible avec les techniques préexistantes mises en oeuvre par les différents fabricants actuels, dans la mesure où elle limite l'intervention à une seule couche du protocole de communication (la transmission de l'accréditation à la serrure), donc en conservant la même gestion logique des différents niveaux de sécurité déjà prévus par le fabricant.

[0011] Le principe de l'invention repose sur l'utilisation, pour la transmission de la donnée d'accréditation à la serrure, d'informations de type accréditations acoustiques chiffrées.

[0012] 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.

[0013] Essentiellement, la présente invention consiste à traduire, au niveau d'un site sécurisé, l'accréditation conventionnelle utilisée pour la gestion d'accès (un bloc de données comprenant un identifiant du fabricant, un identifiant unique de la serrure et éventuellement des informations additionnelles) et de les traduire dans un format d'accréditation acoustique chiffrée. Cette accréditation acoustique se présente sous forme d'un signal audio qui peut être véhiculé par des canaux de transmission audio, notamment des canaux de transmission téléphonique, et reproduits tels quels par des transducteurs acoustiques.

[0014] L'accréditation acoustique est envoyée de cette manière au téléphone mobile de l'utilisateur, qui est répertorié dans une base de données du site sécurisé. Pour utiliser l'accréditation, l'utilisateur approche son téléphone de la serrure et déclenche l'émission par le haut-parleur de son téléphone de la série de tonalités correspondant à l'accréditation acoustique chiffrée, de manière que ces tonalités puissent être captées par un microphone incorporé ou couplé à la serrure. Cette dernière opère une traduction inverse de l'accréditation acoustique permettant de restituer le format original de l'accréditation conventionnelle, qui est ensuite appliquée aux circuits de la serrure pour y être traitée de la même manière que si cette accréditation avait été lue par un lecteur standard couplé à la serrure (lecteur de cartes magnétiques ou à puce, lecteur à couplage inductif ou RFID, etc.).

[0015] 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).

[0016] 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.

[0017] 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. Dans le cas de l'invention, les accréditations acoustiques chiffrées sont au contraire des accréditations "descendantes", c'est-à-dire qu'elles sont issues d'un site gestionnaire distant et transmises au téléphone mobile de l'utilisateur.

[0018] Plus précisément, l'invention concerne, de façon en elle-même connue, un système sécurisé de commande d'ouverture de dispositifs de serrure, comportant au moins un dispositif de serrure muni de circuits électroniques pour la commande conditionnelle d'organes mécaniques de verrouillage/déver-rouillage à partir de données numériques d'accréditation. Ce dispositif de serrure comprend des moyens de reconnaissance, d'analyse et d'authentification desdites données numériques d'accréditation, et des moyens de commande du déverrouillage des organes mécaniques sur reconnaissance de données numériques d'accréditation conformes.

[0019] De façon caractéristique de l'invention, le système comprend également 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. Le site gestionnaire comprend une base de données d'utilisateurs habilités, avec pour chaque utilisateur un identifiant associé à un numéro de téléphone mobile, des moyens pour recevoir en entrée des données numériques d'accréditation propres à permettre l'ouverture de dispositifs de serrure spécifiques, et un générateur d'accréditations acoustiques chiffrées comportant des moyens de conversion des données numériques d'accréditation en accréditations acoustiques chiffrées sous forme de signaux audio à usage unique. L'opérateur de réseau mobile est couplé au site gestionnaire et au téléphone mobile, avec des moyens de transmission sécurisée des accréditations acoustiques chiffrées du site gestionnaire au téléphone mobile de l'utilisateur, le téléphone comprenant un transducteur électro-acoustique apte à reproduire ces accréditations acoustiques chiffrées.

[0020] Le système de l'invention est également **caractérisé en ce que** le dispositif de serrure comporte un module acoustique comprenant un transducteur électro-acoustique apte à capter des accréditations acoustiques chiffrées reproduites par le transducteur du téléphone préalablement placé à proximité du dispositif de serrure. Le module acoustique comprend en outre des moyens pour extraire les données numériques d'accréditation à partir des accréditations acoustiques chiffrées captées par le transducteur, et des moyens pour appliquer aux moyens de reconnaissance, d'analyse et d'authentification les données numériques d'accréditation ainsi extraites.

[0021] Avantageusement, l'accréditation acoustique chiffrée produite par le générateur d'accréditations acoustiques comprend un champ résultant de la conversion des données numériques d'accréditation, et un champ variable, avec un contenu différent pour chaque accréditation acoustique chiffrée générée. Ce champ va-

riable peut notamment être un numéro de séquence ou un horodatage, auquel cas le module acoustique comprend en outre des moyens pour mémoriser à chaque utilisation le numéro de séquence ou l'horodatage de l'accréditation acoustique chiffrée ayant permis le déverrouillage des organes mécaniques, et pour comparer et vérifier la conformité du numéro de séquence ou de l'horodatage de toute accréditation acoustique chiffrée ultérieure.

[0022] Les données numériques d'accréditation peuvent être : des données issues de la base de données du site gestionnaire, celle-ci mémorisant également des informations de dispositifs de serrure, 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 informations additionnelles ; des données transmises en ligne au site gestionnaire par un site tiers ; des données transmises hors ligne, par lots, au site gestionnaire par un site tiers ; des données délivrées par un lecteur couplé à un support physique mémorisant les données numériques d'accréditation ; et des combinaisons des données ci-dessus.

[0023] Dans une forme de réalisation avantageuse, le module acoustique comprend en outre des moyens pour produire des signaux acoustiques en retour, sur captation de données numériques d'accréditation, et un transducteur électro-acoustique apte à reproduire ces signaux acoustiques en retour. Ces derniers peuvent notamment comprendre un marqueur temporel émis pendant, ou immédiatement après, la réception de l'accréditation acoustique, ce marqueur étant émis à un instant correspondant à une position temporelle prédéterminée, propre au dispositif de serrure, par rapport à l'accréditation acoustique.

[0024] En variante ou en complément, le module acoustique comprend en outre des moyens pour définir un paramètre additionnel de transmission de l'accréditation, des moyens pour, préalablement à toute émission d'accréditation acoustique, produire un message acoustique codé par ledit paramètre additionnel, et un transducteur électro-acoustique apte à reproduire ce message acoustique. Le téléphone comprend, quant à lui, un transducteur électro-acoustique apte à capter le message acoustique, et des moyens pour transmettre au site gestionnaire un message codé par ce message acoustique. L'accréditation acoustique chiffrée produite par le générateur d'accréditations acoustiques inclut le paramètre additionnel, et le module acoustique comprend également des moyens pour vérifier la conformité du paramètre additionnel inclus dans l'accréditation acoustique captée.

[0025] Ce paramètre additionnel peut être un mot de passe généré par le module acoustique et ajouté en tant que champ variable à l'accréditation acoustique produite par le générateur cryptographique. Ce peut également être un décalage temporel appliqué à l'émission de l'accréditation acoustique produite par le générateur cryptographique.

[0026] On va maintenant décrire un exemple de mise en oeuvre du dispositif 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 les différentes transformations subies par l'accréditation au cours des étapes mises en oeuvre par l'invention.

La Figure 4 est une série de chronogrammes illustrant les diverses techniques de sécurité permettant d'assurer l'utilisation unique de l'accréditation acoustique dans le cadre de l'invention.

[0027] On vatout d'abord décrire en référence aux Figures 1 et 2 les différents éléments servant à l'implémentation de l'invention. On exposera ensuite diverses manières de la mettre en oeuvre, ainsi que des variantes perfectionnées permettant d'ne renforcer la sécurité.

Architecture générale du système

[0028] 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 et d'utilisateurs habilités pour chacune de ces 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.).

[0029] 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.

[0030] D'autres données peuvent également être conservées par la base de données, notamment les algorithmes utilisés par la serrure, une ou plusieurs clés cryptographiques, une dénomination libre simplifiée ("entrée", "garage", "cave", etc.) pour faciliter la sélection par un utilisateur d'une serrure parmi plusieurs, etc.

[0031] Le site gestionnaire 10 comprend également un moteur cryptographique formant générateur 14 de données d'accréditation.

[0032] De façon caractéristique de l'invention, les "données d'accréditation" (*credentials*) sont des accréditations acoustiques chiffrées ou CAC (*Crypto Acoustic*

Credential) 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 après numérisation par des canaux de transmission audio téléphonique et reproduits tels quels par des transducteurs acoustiques.

[0033] Le site gestionnaire 10 est couplé à un réseau 16 d'un opérateur de téléphonie mobile MNO (*Mobile Network Operator*) par l'intermédiaire d'une passerelle téléphonique audio PGW (*Phone GateWay*) 18 et d'une liaison sécurisée 20, par exemple une liaison IP de type *https*, de manière à pouvoir véhiculer les accréditations acoustiques depuis le générateur 14 jusqu'au téléphone 22 de l'utilisateur par les canaux de transmission audio (canal voix) du réseau de téléphonie mobile.

[0034] Le réseau de téléphonie mobile 16 est utilisé de façon conventionnelle par ses divers abonnés, chaque utilisateur étant en possession d'un téléphone mobile 22 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.

[0035] La sécurisation de la liaison entre le réseau 16 et le téléphone mobile 22 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 transmission d'informations entre le site gestionnaire 10 et le téléphone mobile 22 via l'opérateur de réseau mobile 16.

[0036] 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, répertorié dans sa base de données 12.

[0037] La mise en oeuvre de l'invention implique de faire reproduire par le haut-parleur 24 du téléphone mobile 22, 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 18 et de l'opérateur du réseau mobile 16.

[0038] L'accréditation reproduite par le haut-parleur 24 du téléphone mobile est destinée à être captée par un microphone 26 d'une serrure 28 de manière à commander l'ouverture de cette serrure. Il s'agit de permettre à l'utilisateur, détenteur du numéro du téléphone mobile 22 connu de la base de données 12, de prouver à la serrure 28 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 elle est à usage unique afin d'éviter toute fraude par enregistrement et duplication, car sinon il serait très aisé d'enregistrer le signal acoustique et de le reproduire ensuite à volonté.

[0039] La Figure 2 illustre sous forme de schéma par blocs les principaux organes du téléphone mobile 22 et de la serrure 28.

[0040] Le téléphone 22 comporte un microcontrôleur 30 couplé à divers organes périphériques tels qu'un circuit d'émission/réception 32, un afficheur 34, un clavier 36, une mémoire de données 38, une carte UICC (*Universal In-tegrated Circuit Card,* correspondant à la "carte SIM" pour les fonctions de téléphonie GSM) 40, et le transducteur acoustique 24.

[0041] Diverses précautions, en elles-mêmes connues, peuvent être prévues pour augmenter la sécurité du processus, notamment par une validation supplémentaire demandée l'utilisateur, par exemple l'entrée d'un code personnel de type "PIN code", 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).

[0042] La serrure 28, 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 :

- l'identifiant unique UID (*Unique IDentifier*) permettant de reconnaître cette serrure entre toutes, de manière univoque ;
- des algorithmes de reconnaissance et de décodage ;
- des clés cryptographiques ;
- ainsi que d'autre paramètres spécifiques à la mise en oeuvre de l'invention et qui seront décrits par la suite.

[0043] Il existe de nombreux modèles de serrures de ce type, proposés par un grand nombre de fabricants. L'ouverture en est commandée par un module lecteur 52 intégré à la serrure, qui comprend une interface de communication avec une clé ou un badge, par un couplage

qui peut être galvanique (lecteur de carte à puce) ou non galvanique (lecteur optique pour badge portant un code à barres, lecteur de carte magnétique, lecteur sans contact à couplage inductif ou RF, etc.). Le lecteur 52 délivre au microcontrôleur 44 une accréditation en données numériques, ci-après désignée DDC (*Digital Data Credential*), selon un format et un contenu propres à chaque fabricant et qui comprend typiquement (mais non exclusivement), comme illustré sur la ligne a de la Figure 3 :

- un identifiant de fabricant VID (*Vendor ID*),
- l'identifiant unique UID de la carte,
- et un champ DATA (facultatif) contenant diverses données nécessaires ou utiles au contrôle du fonctionnement de la serrure.

[0044] Cette accréditation en données numériques DDC, lue par le module 52 dans une clé ou badge que l'utilisateur a couplé avec ce module, est analysée par le microcontrôleur 44 qui délivre conditionnellement une autorisation d'ouverture de la serrure 46 si les critères requis sont remplis, notamment la conformité de l'identifiant UID.

[0045] L'invention propose de substituer au module 52, ou de compléter ce module 52, par un module 54 apte à traiter des accréditations envoyées à la serrure sous forme d'accréditations acoustiques CAC émises par un téléphone mobile 22, en lieu et place d'accréditations numériques DDC lues dans une carte ou un badge couplé au module 52.

[0046] Le module acoustique 54 est pourvu d'un transducteur acoustique sous forme d'un microphone 56 permettant de capter les signaux sonores environnants, en particulier l'accréditation acoustique qui sera reproduite par le haut-parleur 24 du téléphone 22, et de transformer les signaux acoustiques captés en signaux numériques appliqués à un étage 58 formant traducteur, pour convertir les accréditations acoustiques CAC en signaux de même format que les accréditations en données numériques DDC qu'aurait fourni le module 52 par lecture d'un badge ou d'une carte.

[0047] Le module acoustique 54 comprend également, de façon avantageuse, un transducteur 60 permettant de reproduire un signal sonore émis par l'étage 58 et audible depuis l'extérieur de la serrure, ce transducteur 60 pouvant comprendre un haut-parleur ou, dans une version simplifiée, un simple composant de type buzzer (ronfleur). Il est également possible d'utiliser le transducteur 46 du module acoustique 54 en le faisant fonctionner en mode inversé (pour émettre des signaux sonores au lieu de les capter).

Mise en oeuvre de l'invention

[0048] On va maintenant décrire plusieurs modes opératoires pour la mise en oeuvre de l'invention au moyen des différents éléments du système que l'on vient de décrire.

[0049] Le but premier de l'invention est de remplacer, ou compléter, la technologie "propriétaire", spécifique au fabricant et implémentée dans le module lecteur 52, par une technologie universelle à base d'accréditations acoustiques chiffrées CAC, pouvant être mise en oeuvre sans modification substantielle des organes de la serrure, tant matériels que logiciels.

[0050] Le principe de base consiste à conserver les accréditations en données numériques (DDC) originelles avec leur contenu et leur format propres au fabricant, et à convertir ces accréditations DDC en accréditations acoustiques CAC, à transmettre les CAC au téléphone, puis à faire reproduire par l'utilisateur, au moyen du haut-parleur de son téléphone mobile, l'accréditation acoustique CAC ainsi transmise. L'accréditation captée par le module acoustique 54 fait alors l'objet d'une conversion inverse, opérée par l'étage 58 de traduction incorporé au module acoustique 54, afin de reconstituer l'accréditation en données numériques DDC originelle à partir de l'accréditation acoustique CAC qui a été captée.

[0051] Une étape préliminaire consiste donc à convertir l'accréditation numérique DDC en une accréditation acoustique chiffrée CAC.

[0052] L'accréditation numérique DDC peut avoir plusieurs origines (voir Figure 1), en étant générée :

- en temps réel par un site tiers 62, c'est-à-dire à la demande de l'utilisateur au moment où celui-ci veut ouvrir la serrure ;
- par le site tiers 62 en mode "hors ligne", les accréditations étant délivrées à l'avance sous forme de lots ;
- de façon manuelle au moyen d'un lecteur 64, à partir d'une clé ou badge conventionnel 66 ;
- ou bien directement par le site sécurisé 10, l'accréditation numérique DDC étant conservée dans la base de données 12.

[0053] Ces accréditations DDC sous forme de blocs de données numériques sont converties par le moteur cryptographique 14 du site sécurisé 10 en accréditations acoustiques CAC.

[0054] Comme illustré Figure 3, la conversion peut être effectuée à partir d'un bloc de données dans lequel les champs VID, UID et DATA se présentent de façon explicite, vers un champ CORE/CAC de l'accréditation acoustique CAC (de la ligne a vers la ligne c de la Figure 3). Toutefois, le moteur cryptographique peut très bien recevoir à ce stade l'information sous une forme non explicite (CORE), qui est directement convertie pour donner le champ CORE/CAC de l'accréditation acoustique CAC (de la ligne b vers la ligne c de la Figure 3). En effet, la connaissance du contenu de l'accréditation numérique DDC n'est pas nécessaire pour opérer la conversion, qui consiste simplement à créer une "enveloppe" acoustique dans laquelle est "glissée" l'accréditation numérique DDC quel que soit le contenu de cette dernière car le moteur cryptographique 14 n'a pas besoin de connaître

la définition des champs, le codage, etc. de l'accréditation DCC.

[0055] Le moteur cryptographique 14 ajoute également au champ CORE/CAC contenant les données d'accréditation proprement dites un champ variable, différent à chaque génération d'une accréditation acoustique, de façon à rendre unique cette accréditation acoustique. Il peut s'agir d'une donnée produite par un générateur pseudo-aléatoire ou, de préférence, d'un numéro de séquence SEQ. Le champ SEQ peut être un compteur incrémenté à chaque génération d'une accréditation par le générateur cryptographique 14, ou encore un horodatage qui sera fonctionnellement équivalent à l'incrémentation d'un compteur.

[0056] Le générateur cryptographique 14 peut également prévoir l'adjonction à l'accréditation acoustique CAC d'un mot de passe PWD permettant d'augmenter encore la sécurisation du processus.

[0057] Lorsqu'il souhaite obtenir l'ouverture de la serrure devant laquelle il se trouve, l'utilisateur entre en contact avec le site gestionnaire 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.

[0058] Dans un mode de mise en oeuvre "en ligne", la transmission de cette accréditation est exécutée immédiatement et directement. En variante, elle 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 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. Quelle que soit la manière dont l'utilisateur entre en contact avec le site distant, celui-ci délivre l'accréditation acoustique directement à l'utilisateur, sans stockage intermédiaire.

[0059] Ce mode 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. 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). 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.

[0060] Un autre mode de mise en oeuvre, "hors ligne", 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). 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. L'application permettant cette mise en oeuvre est une appliquette conservée dans le téléphone, préalablement envoyée à celui-ci via 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 "SMS", "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. Lorsque la provision d'accréditations mémorisées dans le téléphone sera épuisée, ou sera en voie d'épuisement, et que l'utilisateur sera à nouveau capable d'accéder au réseau, cette réserve d'accréditations sera rechargée, pour permettre des utilisations ultérieures. 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.

[0061] En tout état de cause, et quel que soit le mode de transmission de l'accréditation acoustique chiffrée CAC, lorsqu'il souhaite obtenir l'ouverture de la serrure, l'utilisateur place son téléphone mobile à proximité de la serrure qu'il souhaite déverrouiller et déclenche l'émission, sous forme de signal sonore, de l'accréditation acoustique CAC.

[0062] Comme cela a été expliqué précédemment, le module acoustique 54 de la serrure reçoit cette accréditation acoustique chiffrée CAC (correspondant à la ligne c de la Figure 3). L'étage de traduction 58 en extrait alors le bloc de données CORE (ligne d de la Figure 3), c'est-à-dire, en termes imagés, qu'il "ouvre l'enveloppe (acoustique)" contenant ces données. Il est alors possible d'obtenir, directement ou après décodage, une l'accréditation en données numériques DDC (ligne e de la

Figure 3) avec ses différents champs utiles VID, UID et DATA, qui est identique à l'accréditation correspondante DDC avant que celle-ci n'ait été convertie par le moteur cryptographique (ligne a de la Figure 3).

[0063] L'accréditation DDC, qui est en tous points identique à celle qui aurait été lue par le module 52 à partir d'une clé ou d'un badge conventionnel selon les prescriptions propres du fabricant, est appliquée au microcontrôleur 44 pour analyse, vérification et déverrouillage conditionnel du système 46 de commande de la serrure.

[0064] On notera que les différentes vérifications opérées par le microcontrôleur 44 sont identiques à celles qui auraient été effectuées à partir d'informations lues de manière conventionnelle par le module 52, selon les spécifications propres à chaque fabricant. Le rôle de l'étage traducteur 58 est simplement d"'ouvrir l'enveloppe" de l'accréditation acoustique CAC pour en extraire les informations numériques DDC qui avaient été auparavant placées dans cette enveloppe par le moteur cryptographique 14, mais sans intervenir sur le contenu de cette accréditation numérique DDC.

Détection des fraudes par captation de signal

[0065] Diverses mesures peuvent être envisagées pour éviter des fraudes, notamment celle qui consisterait à enregistrer le signal audio reproduit par le téléphone au moment de l'utilisation, puis utiliser ce signal enregistré pour ouvrir une autre serrure, ou pour tenter d'obtenir une nouvelle ouverture de la même serrure (alors que l'accréditation est normalement à usage unique et doit être renouvelée à chaque fois).

1°) Contrôle de l'unicité de l'accréditation acoustique : du fait de la présence du champ unique SEQ généré différent à chaque version de l'accréditation acoustique CAC, le système ne doit jamais produire deux accréditations acoustiques identiques. De ce fait, le module acoustique de la serrure doit pouvoir détecter et refuser une accréditation qui aurait déjà été produite, et qui serait donc une accréditation frauduleusement captée et réutilisée.
A cet effet, lors de l'initialisation de la serrure (au moment de l'installation du module acoustique 54 ou à l'occasion d'une réinitialisation de celui-ci), un registre du module 54 est mis à zéro. Lors de la première utilisation, c'est-à-dire lorsque la première accréditation acoustique CAC est captée, le module 54 mémorise le numéro de séquence SEQ inclus dans cette accréditation acoustique (ou la date et l'heure, dans le cas d'un horodatage).
A chaque utilisation ultérieure, le module 54 vérifie que le numéro de séquence de l'accréditation captée est supérieur au numéro de séquence qu'il avait conservé en mémoire dans le registre (ou vérifie que la date et l'heure sont postérieures aux informations correspondantes mémorisées). Si tel n'est pas le cas, l'ouverture est refusée, car il s'agit d'une fraude. En revanche, si la condition est bien remplie, la serrure est déverrouillée et le registre est mis à jour avec le nouveau numéro de séquence (ou avec les nouvelles valeurs de date et d'heure).

2°) Génération d'un marquage temporel par la serrure : une autre mesure de précaution, expliquée notamment en référence à la Figure 4, consiste à faire émettre par le HP ou buzzer 60 du module acoustique 54, pendant la réception de l'accréditation acoustique CAC ou juste après celle-ci, un parasite acoustique ou "bip" à un instant prédéfini, toujours le même pour une serrure donnée mais toujours différent d'une serrure à l'autre.

[0066] Sur la ligne a du chronogramme de la Figure 4, on a illustré l'accréditation acoustique CAC émise par le téléphone, et sur la ligne b, le bip, désigné BEEP1, émis par le module acoustique 54 à un instant décalé de T_1 par rapport au début de la réception de l'accréditation CAC.

[0067] Le signal entendu à proximité du téléphone, et donc susceptible d'être enregistré, est celui illustré ligne c, avec superposition du signal CAC émis par le téléphone et du signal BEEP1 émis par le module acoustique de la serrure.

[0068] Si un fraudeur enregistre ce signal combiné et le présente à une autre serrure en tant qu'accréditation acoustique, cette autre serrure va émettre un parasite BEEP2 selon la même technique que la première, mais à une position temporelle T_2 différente (ligne d de la Figure 4).

[0069] Le signal combiné reçu par le module acoustique de cette autre serrure sera donc celui illustré ligne e de la Figure 4, c'est-à-dire un signal comportant deux parasites acoustiques BEEP1 et BEEP2. La présence de ces deux parasites sera immédiatement reconnue par le module acoustique, qui refusera l'ouverture.

[0070] On notera que, si le fraudeur avait représenté sur la même serrure (et non plus une autre serrure) l'accréditation acoustique CAC qu'il avait enregistrée, celle-ci correspondrait à la ligne f de la Figure 4, avec donc un parasite acoustique BEEP1 confondu avec celui émis au même moment par le module acoustique 54. Mais dans ce cas le numéro de séquence SEQ1 serait égal, ou inférieur, à celui déjà enregistré dans la mémoire du module acoustique de la serrure, qui pourra ainsi détecter la fraude du fait de ce numéro de séquence SEQ1 non conforme.

Sécurités additionnelles avec communication bidirectionnelle

[0071] Une communication bidirectionnelle peut être établie avec le site sécurisé 10 s'il est possible au téléphone d'obtenir une liaison avec le réseau au moment de l'utilisation, ce qui permet de faire remonter vers celui-ci des informations provenant du téléphone.

[0072] En particulier, préalablement à la génération de l'accréditation acoustique CAC, le module acoustique 54 de la serrure peut produire sous forme acoustique un mot de passe, qui est capté par le microphone du téléphone, puis transmis au réseau et au site distant 10 pour être incorporé à l'accréditation acoustique CAC qui va être générée par le moteur cryptographique 14 (champ PWD de la ligne c de la Figure 3). L'accréditation acoustique CAC reproduite ensuite par le téléphone inclura donc ce mot de passe, qui pourra alors être décodé par le module acoustique 54, qui vérifiera qu'il concorde bien avec celui qui vient d'être généré par ce même module juste auparavant.

[0073] En variante ou en complément de ce mot de passe, une autre sécurité consiste à faire générer par le module acoustique 54 une valeur de retard ou décalage temporel Δt_1, différente à chaque fois (par exemple un retard aléatoire), et à la transmettre au site sécurisé 10 afin que celui-ci ajoute ce décalage temporel Δt_1 à l'accréditation acoustique CAC lors de l'émission de celle-ci (ligne g de la Figure 4). Le module acoustique 54 vérifie alors, à réception de l'accréditation acoustique CAC, que celle-ci commence bien avec un décalage temporel Δt_1, introduit par le serveur distant, qui est égal à la valeur de décalage qu'il avait lui-même générée juste auparavant et envoyée au serveur.

Revendications

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

- au moins un dispositif de serrure (28) muni de circuits électroniques pour la commande conditionnelle d'organes mécaniques (46) de verrouillage/déverrouillage à partir de données numériques d'accréditation (DDC), ce dispositif de serrure comprenant :

  • des moyens (44) de reconnaissance, d'analyse et d'authentification desdites données numériques d'accréditation, et
  • des moyens (44) de commande du déverrouillage des organes mécaniques sur reconnaissance de données numériques d'accréditation conformes ;

système **caractérisé en ce qu'**il comprend également :
- un téléphone mobile (22) à disposition d'un utilisateur habilité à ouvrir le dispositif de serrure ;
- un site gestionnaire distant (10), comprenant :

  • une base de données (12) d'utilisateurs habilités, avec pour chaque utilisateur un identifiant associé à un numéro de téléphone mobile,
  • des moyens pour recevoir en entrée des données numériques d'accréditation (DDC) propres à permettre l'ouverture de dispositifs de serrure spécifiques, et
  • un générateur (14) d'accréditations acoustiques chiffrées, comportant des moyens de conversion desdites données numériques d'accréditation (DDC) en accréditations acoustiques chiffrées (CAC) sous forme de signaux audio à usage unique ; et

- un opérateur de réseau mobile (16), couplé au site gestionnaire et au téléphone mobile, avec des moyens de transmission sécurisée desdites accréditations acoustiques chiffrées du site gestionnaire au téléphone mobile de l'utilisateur, le téléphone comprenant un transducteur électro-acoustique (24) apte à reproduire lesdites accréditations acoustiques chiffrées,

le système étant également **caractérisé en ce que** le dispositif de serrure (28) comporte un module acoustique (54) comprenant :

  • un transducteur électro-acoustique (56) apte à capter des accréditations acoustiques chiffrées reproduites par le transducteur (24) du téléphone préalablement placé à proximité du dispositif de serrure ;
  • des moyens (58) pour extraire lesdites données numériques d'accréditation (DDC) à partir des accréditations acoustiques chiffrées (CAC) captées par le transducteur ; et
  • des moyens pour appliquer auxdits moyens (44) de reconnaissance, d'analyse et d'authentification les données numériques d'accréditation (DDC) ainsi extraites.

2. Le système de la revendication 1, dans lequel l'accréditation acoustique chiffrée (CAC) produite par le générateur d'accréditations acoustiques (14) comprend :

- un champ (CORE/CAC) résultant de la conversion desdites données numériques d'accréditation (CAC), et
- un champ variable, avec un contenu différent pour chaque accréditation acoustique chiffrée générée.

3. Le système de la revendication 2, dans lequel :

- ledit champ variable est un numéro de séquence (SEQ) ou un horodatage, et
- le module acoustique (54) comprend en outre des moyens pour mémoriser à chaque utilisation le numéro de séquence (SEQ) ou l'horodatage de l'accréditation acoustique chiffrée (CAC) ayant permis le déverrouillage des orga-

nes mécaniques, et pour comparer et vérifier la conformité du numéro de séquence ou de l'horodatage de toute accréditation acoustique chiffrée ultérieure.

4. Le système de la revendication 1, dans lequel lesdites données numériques d'accréditation (DDC) sont des données du groupe constitué par :

- données issues de la base de données (12) du site gestionnaire (10), celle-ci mémorisant également des informations de dispositifs de serrure, 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 informations additionnelles ;
- données transmises en ligne au site gestionnaire (10) par un site tiers (62) ;
- données transmises hors ligne, par lots, au site gestionnaire (10) par un site tiers (62) ;
- données délivrées par un lecteur (64) couplé à un support physique (66) mémorisant les données numériques d'accréditation ; et
- combinaisons des données ci-dessus.

5. Le système de la revendication 1, dans lequel le module acoustique (54) comprend en outre :

• des moyens pour produire des signaux acoustiques en retour, sur captation de données numériques d'accréditation ; et
• un transducteur électro-acoustique (56) apte à reproduire lesdits signaux acoustiques en retour.

6. Le système de la revendication 5, dans lequel lesdits signaux acoustiques en retour comprennent au moins un marqueur temporel (BEEP1, BEEP2) émis pendant, ou immédiatement après, la réception de l'accréditation acoustique (CAC), ce marqueur étant émis à un instant correspondant à une position temporelle (T1, T2) prédéterminée, propre au dispositif de serrure, par rapport à l'accréditation acoustique.

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

- le module acoustique (54) comprend en outre :

• des moyens pour définir un paramètre additionnel de transmission de l'accréditation ;
• des moyens pour, préalablement à toute émission d'accréditation acoustique, produire un message acoustique codé par ledit paramètre additionnel ; et
• un transducteur électro-acoustique (56) apte à reproduire ledit message acoustique,

- le téléphone (22) comprend un transducteur électro-acoustique apte à capter ledit message acoustique, et des moyens pour transmettre au site gestionnaire (10) un message codé par ce message acoustique ;
- l'accréditation acoustique chiffrée (CAC) produite par le générateur d'accréditations acoustiques (14) inclut ledit paramètre additionnel ; et
- le module acoustique comprend également des moyens pour vérifier la conformité du paramètre additionnel inclus dans l'accréditation acoustique captée.

8. Le système de la revendication 7, dans lequel ledit paramètre additionnel est un mot de passe (PWD) généré par le module acoustique (54) et ajouté en tant que champ variable à l'accréditation acoustique (CAC) produite par le générateur cryptographique (14).

9. Le système de la revendication 7, dans lequel ledit paramètre additionnel est un décalage temporel ($\Delta t1$) appliqué à l'émission de l'accréditation acoustique (CAC) produite par le générateur cryptographique (14).

FIG_1

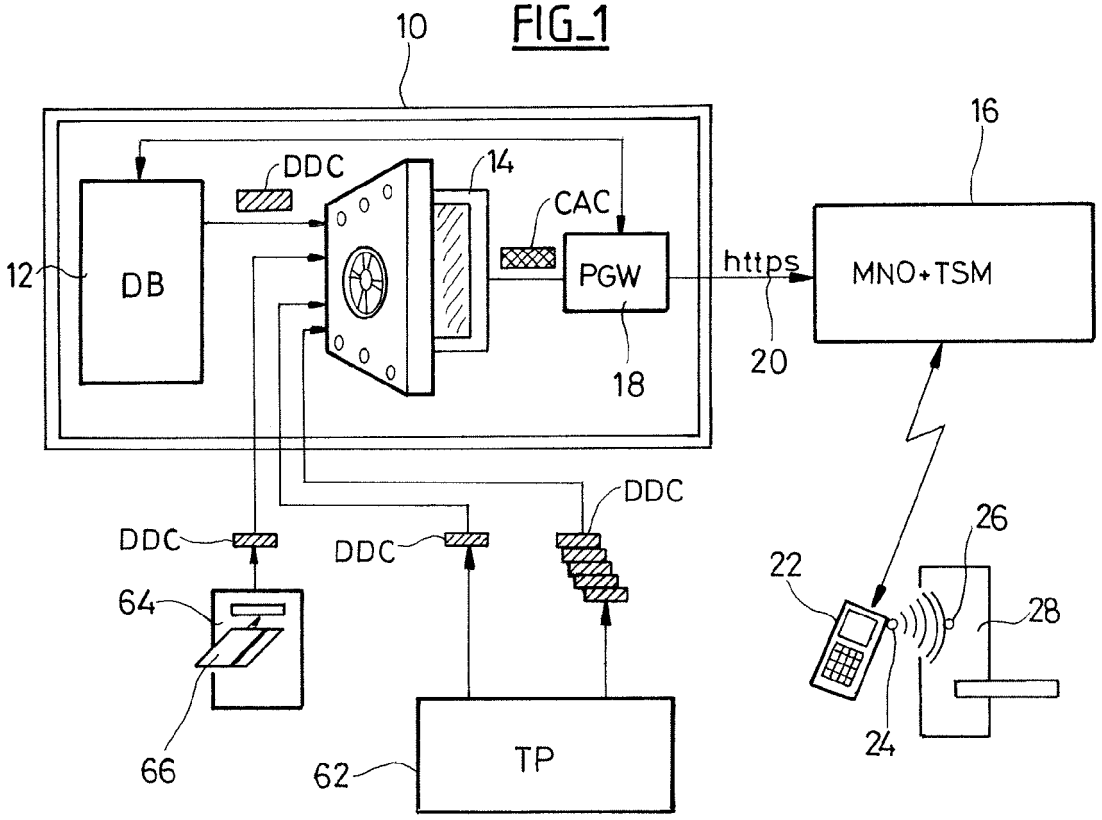

10
16
DDC
14
CAC
12
DB
PGW
https
MNO+TSM
18
20
DDC
DDC
DDC
26
22
64
28
24
66
62
TP

FIG_2

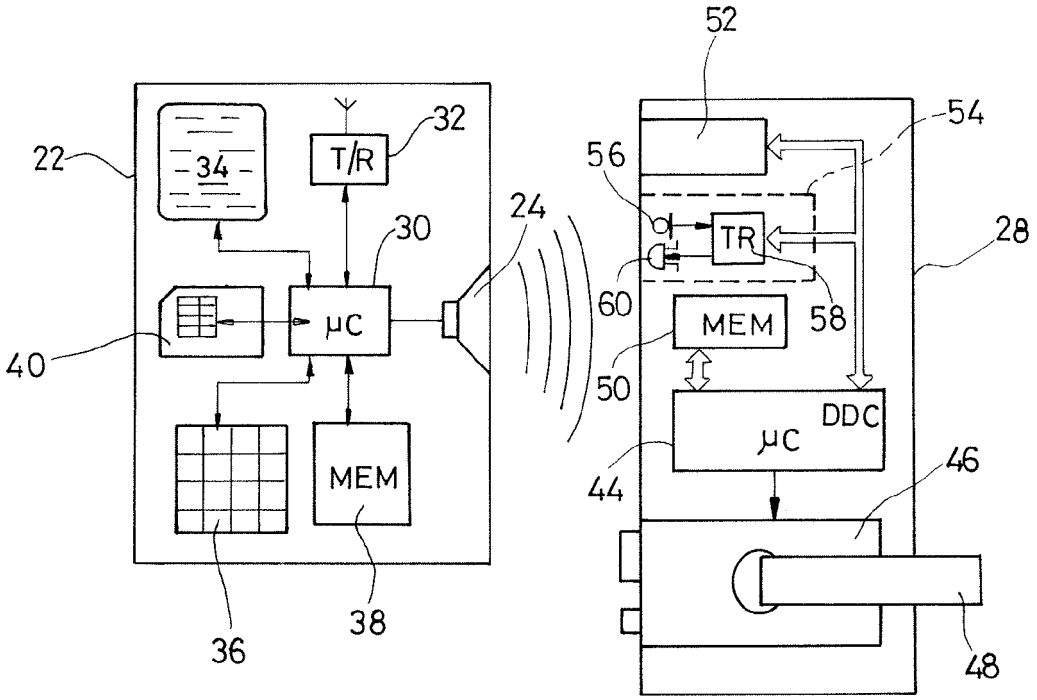

52
54
22
34
T/R
32
56
24
28
30
TR
μC
60
MEM
58
40
50
DDC
μC
44
46
MEM
36
38
48

FIG_3

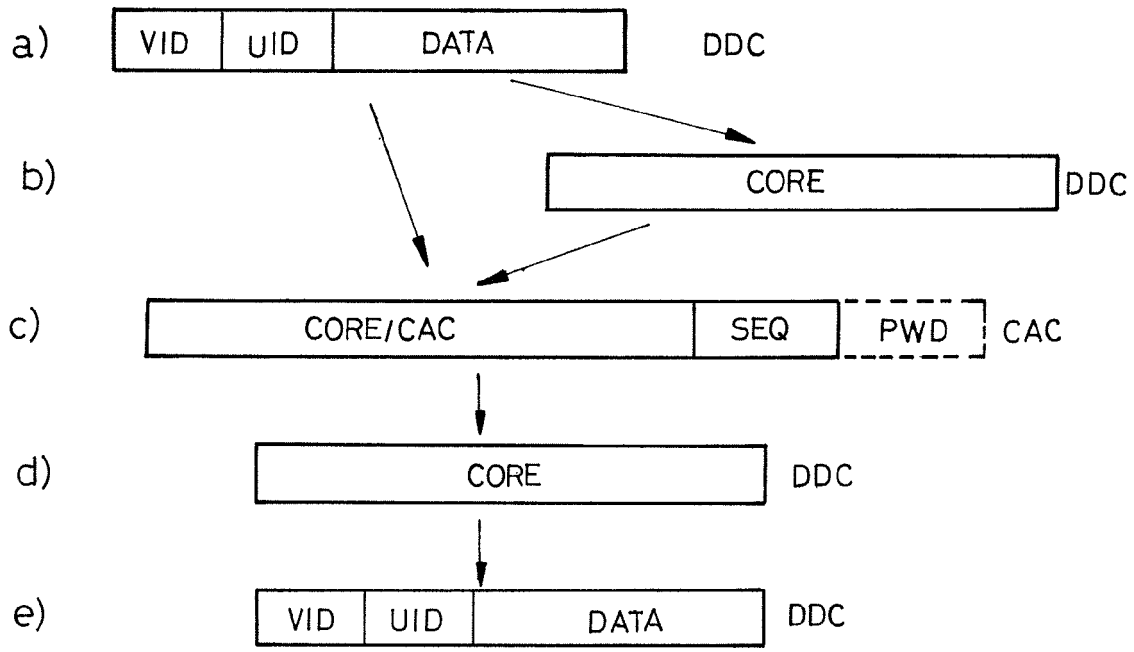
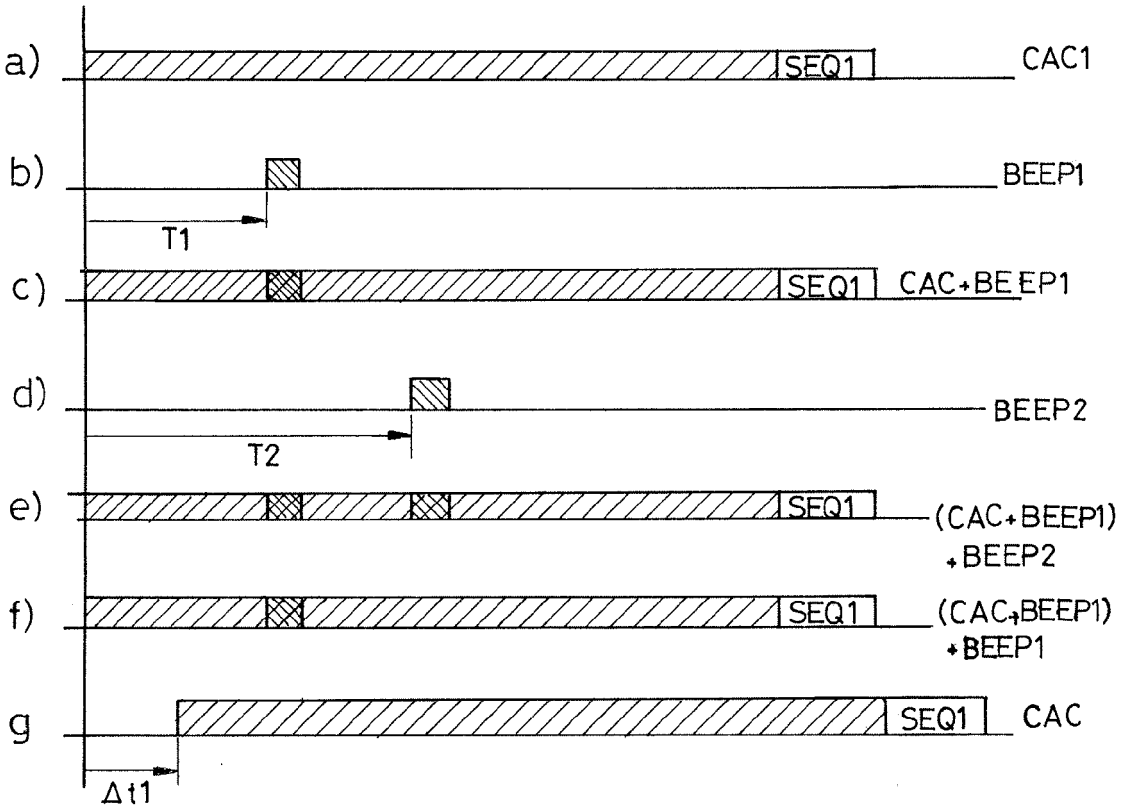

a)
VID
UID
DATA
DDC
b)
CORE
DDC
c)
CORE/CAC
SEQ
PWD
CAC
d)
CORE
DDC
e)
VID
UID
DATA
DDC

FIG_4


a)
SEQ1
CAC1
b)
BEEP1
T1
c)
SEQ1
CAC+BEEP1
d)
BEEP2
T2
e)
SEQ1
(CAC+BEEP1)
+BEEP2
f)
SEQ1
(CAC+BEEP1)
+BEEP1
g
SEQ1
CAC
Δt1

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 09 17 0475

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 03/093997 A1 (GE INTERLOGIX INC [US]; KUENZI ADAM [US]; LANGFORD SUSAN [US]; CHAPIN) 13 novembre 2003 (2003-11-13)	1-6	INV. G07C9/00
A	* page 3, ligne 12 - ligne 25 * * page 4, ligne 25 - page 6, ligne 15 * * page 7, ligne 18 - page 8, ligne 17 * * page 9, ligne 8 - ligne 14 * * page 22, ligne 15 - page 23, ligne 13 * * figures 1-4 *	7-9	
Y	US 5 933 090 A (CHRISTENSON KEITH A [US]) 3 août 1999 (1999-08-03) * colonne 2, ligne 12 - ligne 52 * * colonne 3, ligne 17 - colonne 4, ligne 55 * * figures 1,3 *	1-6	
A,D	WO 2008/107595 A2 (TAGATTITUDE [FR]; MANCERON HERVE [FR]; EONNET YVES [FR]) 12 septembre 2008 (2008-09-12) * page 4, ligne 33 - page 7, ligne 4 * * figure 1 *	1	DOMAINES TECHNIQUES RECHERCHES (IPC) G07C
A	WO 2007/046804 A1 (HARROW PRODUCTS LLC [US]; MILLER KEVIN D [US]; FROLOV GEORGE [US]; CAT) 26 avril 2007 (2007-04-26) * page 3, ligne 27 - page 5, ligne 17 * * page 8, ligne 4 - ligne 20 * * page 10, ligne 12 - page 11, ligne 11 * * figures 1-4 *	1	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
Munich	16 février 2010	Paraf, Edouard

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)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 09 17 0475

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.

16-02-2010

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 03093997 A1	13-11-2003	AU 2002303561 A1	17-11-2003
		EP 1502181 A1	02-02-2005
US 5933090 A	03-08-1999	CA 2261757 A1	26-02-1998
		DE 69728775 D1	27-05-2004
		DE 69728775 T2	07-10-2004
		EP 0923662 A1	23-06-1999
		JP 2000516675 T	12-12-2000
		WO 9807940 A1	26-02-1998
WO 2008107595 A2	12-09-2008	FR 2911751 A1	25-07-2008
		FR 2911752 A1	25-07-2008
WO 2007046804 A1	26-04-2007	EP 1938157 A1	02-07-2008

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 **[0015]**