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

(11) **EP 1 780 680 B1**

(12) **FASCICULE DE BREVET EUROPEEN**

(45) Date de publication et mention de la délivrance du brevet:
17.01.2018 Bulletin 2018/03

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

(21) Numéro de dépôt: **05109900.0**

(22) Date de dépôt: **24.10.2005**

(54) **Procédé de contrôle de verrouillage de serrure, et serrure**

Verfahren zur Steuerung der Verriegelung von Verschlüssen und Verschluss

Procedure for control of interlock and lock

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

(43) Date de publication de la demande:
02.05.2007 Bulletin 2007/18

(73) Titulaire: **dormakaba Schweiz AG**
8623 Wetzikon (CH)

(72) Inventeur: **Pellaton, Pierre**
8623 Wetzikon (CH)

(74) Mandataire: **P&TS SA (AG, Ltd.)**
Av. J.-J. Rousseau 4
P.O. Box 2848
2001 Neuchâtel (CH)

(56) Documents cités:
EP-A- 0 935 041
EP-A- 1 281 588
WO-A-01/03078
WO-A-01/59725
GB-A- 2 219 676
US-A- 5 259 029
US-A- 5 367 572
US-A- 5 774 058
US-A1- 2003 231 103

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).

EP 1 780 680 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Domaine technique

[0001] La présente invention concerne un procédé de contrôle de verrouillage de serrure électronique. La présente invention concerne également une serrure électronique utile à la mise en oeuvre de ce procédé. La présente invention concerne en particulier une serrure offrant le niveau de sécurité requis pour des distributeurs d'argent (ATM, Automatic Teller Machines) ou des coffres-forts.

Etat de la technique

[0002] Les serrures conventionnelles sont verrouillées ou déverrouillées au moyen de clés mécaniques ou électroniques. La distribution des clés est restreinte aux utilisateurs autorisées à accéder au contenu protégé par la serrure. Le niveau de protection dépend de la facilité avec laquelle les clés peuvent être falsifiées et de la confiance accordée aux porteurs de la clé.

[0003] Dans le cas de distributeurs de billets de banque, l'accès par la face avant est sécurisé au moyen d'un lecteur de carte et d'un clavier permettant à différents utilisateurs de s'identifier avant de prélever un nombre limité de billets. L'accès à la face arrière du distributeur est en revanche généralement fermé au moyen d'une serrure à clé conventionnelle. Les employés de banque, les convoyeurs de fond chargés de remplir le distributeur et les réparateurs techniques se partagent tous des copies de la même clé qui permet d'accéder à des coffres contenant fréquemment des dizaines de milliers d'Euros en cash ou dans un container. Le risque est important qu'une de ces clés soit perdue ou volée et qu'elle tombe dans de mauvaises mains. En outre, il est extrêmement difficile de retrouver le coupable en cas de vol par un employé indélicat lorsqu'une clé est distribuée à de nombreux utilisateurs.

[0004] Afin de remédier à ces problèmes, la société Kaba Mas (marque déposée) propose depuis plusieurs années une serrure vendue sous le nom de Cencon System 2000 (marque déposée). Cette serrure peut être ouverte au moyen d'une clé électronique conventionnelle, permettant d'identifier son porteur, et d'un code secret à usage unique OTC (One Time Combination, marque déposée). Le code OTC est communiqué à l'utilisateur depuis une centrale, par exemple au travers d'un appel téléphonique. Seul un utilisateur qui parvient à présenter à la fois une clé électronique et un code OTC valide est autorisé à accéder au contenu du distributeur protégé.

[0005] Cette solution présente cependant l'inconvénient de toujours requérir des clés physiques associées à chaque distributeur. Un convoyeur nécessite autant de clés que de distributeurs à réapprovisionner au cours de sa tournée, ou alors une clé programmée pour ouvrir plusieurs distributeurs en combinaisons avec différents codes OTC. La gestion et la programmation des clés à distribuer aux différents utilisateurs est un casse-tête administratif, notamment lorsqu'une clé est perdue.

[0006] Par ailleurs, un utilisateur ayant acquis frauduleusement une clé pourrait tenter d'appeler la centrale en usurpant l'identité du porteur autorisé de la clé afin d'obtenir un code OTC valide. La sécurité offerte est donc insuffisante.

[0007] D'autre part, le lecteur de clé électronique comporte des éléments électriques, électroniques et/ou électromécaniques qui offrent des possibilités de manipulations et de fraudes supplémentaires.

[0008] La demande de brevet EP0546701 décrit un procédé de contrôle de déverrouillage de coffres dans lequel la sécurité est assurée au moyen de différents codes PIN et de messages encodés que l'utilisateur doit introduire dans un terminal qui lui appartient. Ce terminal est ensuite connecté au coffre protégé afin de provoquer son déverrouillage. Le terminal qui se trouve habituellement entre les mains de l'utilisateur constitue une cible pour des hackers tentés de l'étudier ou de fabriquer un terminal compatible pour accéder à des coffres non autorisés.

[0009] La demande de brevet EP0935041 décrit un dispositif de commande d'accès physique ou logique pouvant s'appliquer à une serrure (accès physique). Dans ce cas, un premier circuit électronique est monté dans un sabot solidaire de la serrure et un deuxième circuit électronique est monté dans un boîtier séparé. Lorsque le boîtier est inséré dans le sabot, le premier circuit électronique est relié au deuxième circuit électronique. Un premier code aléatoire est élaboré par ces premier et deuxième circuits électroniques associés, puis est transmis vers un centre de commande distant qui procède à des vérifications avant d'élaborer puis de délivrer un second code aléatoire vers les premier et deuxième circuits électroniques associés. La saisie de ce second code aléatoire permet, lorsqu'il est correct, de déverrouiller la serrure. La détention par un fraudeur du boîtier constituant un facteur déterminant pour accéder à l'ouverture de la serrure, cette procédure ne permet donc pas de prendre en compte une éventuelle situation de contrainte.

[0010] Le brevet US5774058 décrit un système d'accès au déverrouillage de serrures à distance. Un ordinateur distant comporte un réceptacle destiné à recevoir une clé physique permettant à un premier utilisateur l'entrée effective dans le système de commande de la serrure à distance, tandis qu'un écran et un clavier situés sur la serrure permettent à un second utilisateur d'interagir notamment avec la serrure. On prévoit cependant toujours impérativement l'usage d'une clé physique, ce qui pose des problèmes en cas de perte comme déjà exposé précédemment.

Un but de la présente invention est donc de proposer un procédé et une serrure qui permettent d'éviter les inconvénients des procédés et des serrures de l'art antérieur.

[0011] Selon l'invention, ces objectifs sont notamment atteints au moyen d'un procédé de contrôle de verrouilla-

ge de serrure électronique, selon la revendication 1.

[0012] Ce procédé a notamment l'avantage de forcer l'utilisateur à transmettre une question posée par la serrure du distributeur à la centrale. Cette opération supplémentaire permet de prévoir des tests supplémentaires, par exemple pour vérifier dans la centrale si la question posée est bel et bien valide.

[0013] Ce procédé a également l'avantage de baser l'identification de l'utilisateur non plus nécessairement sur une clé physique, mais par exemple au moyen de mot de passe, PIN, ou de données biométriques, plus difficiles à dérober.

[0014] Dans le cas d'une identification de l'utilisateur au moyen d'un mot de passe ou d'un PIN, ce procédé a l'avantage de permettre de distribuer, de remplacer ou d'invalider très facilement des mots de passe, à distance par de simples manipulations logicielles depuis une centrale.

[0015] Dans une variante, le code secret utilisé pour identifier l'utilisateur est vérifié par la centrale 1, et pas par la serrure. On évite ainsi la transmission de listes d'utilisateurs autorisés aux différentes serrures.

[0016] Ce procédé a également l'avantage que toutes les données et tous les codes nécessaires pour déverrouiller la serrure peuvent être introduits directement dans la serrure, sans transiter par un équipement intermédiaire offrant une vulnérabilité supplémentaire aux attaques.

[0017] La présente invention concerne aussi une serrure électronique selon la revendication 17.

[0018] Cette serrure est adaptée au procédé ci-dessus ; elle présente en outre l'avantage de ne pas nécessiter impérativement de lecteur de clé, vulnérable et coûteux.

[0019] La présente invention concerne aussi un procédé pour une centrale de gestion de parc de serrures électroniques, 26. Ce procédé peut être mis en oeuvre de manière entièrement automatique par un ordinateur programmé pour ces différentes tâches, ou de manière assistée par un opérateur humain, ou un groupe d'opérateurs humains, mettant en oeuvre un ordinateur.

Brève description des dessins

[0020] Des exemples de mise en oeuvre de l'invention sont indiqués dans la description illustrée par les figures annexées dans lesquelles :

La figure 1 illustre sous forme de schéma bloc un système mettant en oeuvre le procédé et la serrure de l'invention.

La figure 2 illustre sous forme de diagramme de flux les échanges d'information au cours du processus de l'invention.

Exemple(s) de mode de réalisation de l'invention

[0021] La figure 1 illustre sous forme de schéma bloc un système comprenant une centrale 1 à laquelle différents utilisateurs 4 peuvent se connecter à l'aide d'un équipement mobile 3 au travers d'un réseau 2. Le système comporte en outre une ou plusieurs serrures 5 pour protéger des dispositifs non représentés, par exemple des distributeurs de billets, des coffres, des salles ou d'autres volumes protégés.

[0022] La centrale 1 peut être constituée par exemple par une centrale d'appel, animée par plusieurs opérateurs humains, ou un serveur ou groupe de serveur exécutant une application spécifique. Le réseau 2 est par exemple un réseau de télécommunication, par exemple un réseau téléphonique conventionnel, un réseau de type Internet ou Intranet, ou de préférence un réseau cellulaire mobile. Les utilisateurs peuvent se connecter à la centrale 1 en établissant une communication vocale ou de données au travers du réseau 2.

[0023] Dans une variante préférentielle, les utilisateurs se connectent à la centrale 1 au travers d'un réseau cellulaire mobile 2 et en envoyant des données, par exemple des SMS (Short Message System), des e-mails ou des paquets de données IP au travers d'un réseau 2 de type GSM, GPRS, HSCSD, EDGE ou GPRS par exemple. La centrale reçoit de préférence automatiquement des données au moyen d'un modem ou d'un routeur adapté, et peut également répondre à l'utilisateur en lui envoyant ses propres données au travers du même canal, ou d'un canal différent. Les données échangées dans un des sens, ou dans les deux sens, peuvent être signées électroniquement et/ou encryptées par la centrale 1 et/ou par l'équipement mobile 3, par exemple en utilisant une carte à puce dans l'équipement mobile 3.

[0024] Dans une autre variante, les utilisateurs 4 se connectent à la centrale 1 au moyen d'une communication vocale. La centrale 1 emploie dans ce cas des opérateurs humains pour réagir à cet appel vocal, et/ou un système de reconnaissance vocal IVR (Interactive Voice Response) pour analyser le contenu des requêtes et/ou des codes DTMFs de l'utilisateur et pour synthétiser une réponse vocale.

[0025] La centrale 1 comporte en outre une banque de données 10 d'utilisateurs autorisés, qui contient pour chaque utilisateur au moins un code personnel - ou des données de vérification de code personnel - ainsi que des autorisations, par exemple une liste de serrures que l'utilisateur est autorisé à ouvrir. L'enregistrement comportant à chaque utilisateur peut en outre indiquer des fenêtres temporelles durant lesquelles un accès à une ou plusieurs serrures est autorisé, un profil d'utilisateur, incluant par exemple son nom, ses coordonnées, des clés cryptographiques de communication avec chaque utilisateur, un historique d'utilisation du système (nombre d'essais fructueux, d'essais infructueux, dates, heures, etc), et d'autres données d'identification ou d'authentification, y compris par exemple un numéro d'appelant

MSISDN correspondant à son équipement mobile 3, des données biométriques, etc.

[0026] Des moyens de calcul 11 dans la centrale 1 permettent d'exécuter un programme applicatif pour gérer les différents utilisateurs et leurs droits dans la banque de données 10. Les moyens de calcul permettent en outre d'exécuter un algorithme permettant de calculer la réponse à une question (« challenge ») reçue d'un utilisateur. Cet algorithme peut par exemple consulter une table de correspondance en mémoire morte qui indique la réponse à chaque question attendue, ou de préférence calculer une fonction mathématique à partir de chaque question. La fonction exécutée est de préférence choisie de manière à ce que la connaissance d'un nombre quelconque de réponses à des questions précédentes ne permet pas de prédire quelle sera la réponse à la prochaine question (fonction pseudo-aléatoire). L'algorithme choisi, ou les valeurs permettant de le paramétrer (par exemple le seed dans le cas d'une fonction pseudo-aléatoire) sont de préférence maintenus confidentiels. En outre, un algorithme différent, ou des valeurs différentes, sont de préférence employés pour chaque serrure 5, et/ou même pour chaque utilisateur 4.

[0027] La centrale 1 peut en outre comporter une banque de données de serrures (non représentée), comportant pour chaque serrure 5 un profil avec des informations telles que l'emplacement géographique, le type de dispositif protégé, des clés cryptographiques de communication, etc.

[0028] L'équipement mobile 3 dépend du type de réseau employé. Dans une variante préférentielle, cet équipement est constitué par un équipement mobile cellulaire, par exemple un téléphone cellulaire ou un assistant personnel, un smartphone ou un ordinateur personnel muni d'une carte de connexion à un réseau cellulaire, d'un modem ou d'un routeur. Il est aussi possible d'employer un appareil de communication dédié à cet usage.

[0029] L'équipement mobile 3 peut comporter des moyens de géolocalisation 30, par exemple un récepteur satellitaire de type GPS permettant de déterminer sa position et éventuellement de la transmettre à la centrale 1. Un équipement de protection de travailleur isolé (PTI) 31 permet de vérifier si l'utilisateur 4 de l'équipement mobile 3 est éveillé, par exemple en vérifiant s'il bouge, s'il est vertical, s'il réagit à des demandes de réponse, etc. L'équipement mobile 3 peut en outre comporter des moyens d'identification et/ou d'authentification 32 supplémentaires, par exemple une carte à puce (carte SIM par exemple), des moyens d'introduction et de vérification de code PIN, un capteur biométrique, etc. L'identification et/ou l'authentification d'utilisateur 4 peut être effectuée localement, c'est-à-dire dans l'équipement mobile ou dans une carte à puce insérée dans l'équipement, ou à distance, c'est-à-dire par exemple dans la centrale 1 qui dispose alors de moyens de vérifications des données de la carte à puce, des codes PIN et/ou des données biométriques saisies. L'équipement mobile 3 peut être par exemple portable ou installé dans un véhicule.

[0030] Il est cependant possible d'employer un téléphone mobile conventionnel comme équipement mobile dans le cadre de l'invention ; il est seulement nécessaire que l'utilisateur puisse se mettre en relation au moyen de cet équipement avec une centrale 1 pour envoyer une question et recevoir une réponse correspondante. Il est même avantageux, pour augmenter la sécurité, d'établir des communications entre les différents utilisateurs et la centrale par des canaux de type différents. La centrale peut par exemple employer cette information supplémentaire et convenir avec un convoyeur, par exemple, que la question devra être transmise oralement, même si le convoyeur dispose d'un équipement permettant une communication de données.

[0031] L'utilisateur 4 est par exemple un employé de banque, un convoyeur de fond, un réparateur technique, ou n'importe quelle personne physique autorisée par la centrale 1 à ouvrir la serrure 5. L'utilisateur 4 a la connaissance d'un code personnel secret qui lui a été transmis par la centrale 1 et avec lequel il peut s'identifier envers une ou plusieurs serrures 5 d'un parc de serrures gérées par la centrale 1. L'utilisateur 4 est en outre de préférence apte à s'identifier envers son équipement mobile 3 au moyen d'un autre code secret, par exemple le code PIN du téléphone et/ou de la carte SIM. D'autres moyens d'identification de l'utilisateur 4 envers la serrure 5 et/ou envers l'équipement mobile 3 sont envisageables dans le cadre de l'invention ; par exemple, l'utilisateur pourrait prouver son identité en présentant un objet personnel, tel qu'une clé ou une carte à puce, ou par identification biométriques à l'aide d'empreintes digitales, de l'iris, de la rétine, de la voix, du visage, etc. Bien entendu, des procédés différents peuvent être mis en oeuvre pour identifier ou authentifier l'utilisateur 4 envers l'équipement mobile 3 et envers la serrure 5. Il est en outre possible de cumuler plusieurs procédés d'identification. Par ailleurs, les données d'identification introduites dans l'équipement mobile 3 peuvent être transmises à la centrale 1 pour vérification.

[0032] La serrure 5 comporte un élément électromécanique 52, par exemple un pêne, dont la position est contrôlée par un dispositif logique à l'intérieur de la serrure 5 pour agir sur un mécanisme mécanique (« tringlerie ») permettant de verrouiller ou au contraire de déverrouiller l'accès au volume protégé, par exemple à l'intérieur d'un distributeur. La serrure est de préférence destinée à être utilisée en combinaison avec un dispositif contenant un volume à protéger, par exemple avec un distributeur de billets ou un coffre ; elle ne constitue donc pas elle-même un tel coffre, et ne comporte pas de volume protégé, mais dispose de moyens non représentés pour l'associer mécaniquement et/ou électriquement, de manière difficilement démontable avec un tel coffre ou un tel distributeur.

[0033] Un clavier numérique ou alphanumérique 51 associé à la serrure 5 permet à l'utilisateur d'introduire son code personnel et la réponse aux questions posées. D'autres éléments d'introduction de données (non repré-

sentés), par exemple un capteur biométrique, une caméra, un microphone, etc, peuvent éventuellement être prévus dans la serrure 5. La serrure comporte en outre un écran 50 pour afficher des messages en mode texte ou matriciel, y compris des questions, des invitations à introduire une réponse, et des messages d'état.

[0034] La serrure comporte en outre de préférence une ou plusieurs interfaces 53 optionnelles qui lui permettent d'échanger des données avec le dispositif qu'elle doit protéger, par exemple un distributeur monétique, et/ou avec la centrale 1 au travers de n'importe quel réseau adapté, par exemple un réseau téléphonique ou Internet. La communication de données avec le dispositif à protéger dans lequel la serrure est montée permet notamment d'améliorer la sécurité, grâce à l'échange d'informations permettant de détecter des fraudes probables à l'aide de combinaisons d'indices et grâce à la génération des fichiers de logs tenant compte de données récoltées aussi bien par la serrure que par le dispositif protégé. Cette communication peut aussi, le cas échéant, être employée pour commander la serrure 5 au moyen du clavier du distributeur, d'afficher des messages dépendant du comportement de la serrure 5 sur l'écran du distributeur, de répercuter des alarmes déclenchées par la serrure au moyen du distributeur, ou de déclencher d'autres actions effectuées par le distributeur. La communication de préférence bidirectionnelle entre la serrure 5 et la centrale 10 permet par exemple de modifier à distance la liste des utilisateurs autorisés à s'identifier envers chaque serrure 5 (à moins que cette vérification ne soit faite par la centrale), de modifier les algorithmes de vérification de réponse à distance, de consulter les fichiers de logs générés par la serrure, et de détecter à distance d'autres événements liés à l'utilisation de la serrure. Cette communication avec la centrale 1 peut aussi être effectuée au travers du dispositif protégé par la serrure, par exemple en utilisant un modem ou un routeur de ce dispositif. Dans un mode de réalisation, les données échangées par la serrure et la centrale 1 sont signées et encryptées électroniquement, par exemple au travers d'un tunnel privé virtuel (VPN, virtual private network) de manière à préserver leur confidentialité et leur authenticité même vis-à-vis du distributeur à protéger.

[0035] La serrure 5 comporte en outre de préférence une montre électronique 54 qui lui permet de déterminer la date et l'heure de façon autonome, et de calculer des intervalles de temps. Des moyens de calcul non représentés, par exemple un microcontrôleur, un microprocesseur avec une mémoire, un microordinateur industriel, un circuit de type asic et/ou un circuit FPGA, etc, permettent de gérer les dialogues avec l'utilisateur, et de commander le dispositif électromécanique provoquant le verrouillage ou le déverrouillage de la serrure. Les moyens de calcul comportent en outre de préférence un module, par exemple un module logiciel, pour générer puis afficher une question en réponse à l'introduction d'un code d'identification personnel accepté, et un module, par exemple logiciel, pour vérifier si une réponse à la question est correcte, et pour provoquer le déverrouillage de la serrure en cas de réponse correcte

[0036] Les moyens de calcul sont de préférence protégés contre les manipulations physiques ou logicielles et peuvent par exemple s'autodétruire, en maintenant la serrure fermée, lors de manipulations frauduleuses. La serrure 5 peut en outre comporter des éléments de connexion sans fils avec l'équipement mobile 3, par exemple une interface de type Bluetooth, afin par exemple de détecter et de vérifier la présence de cet équipement à proximité ; on peut cependant renoncer à ces moyens s'ils introduisent une vulnérabilité supplémentaire.

[0037] La serrure 5 est de préférence autonome électriquement et alimentée à l'aide de piles ou de batterie ; elle reste mécaniquement verrouillée lorsque les piles ou batteries sont déchargés. La recharge ou le remplacement des piles ou batteries peut alors être effectué sans déverrouiller la serrure. Dans une variante, la serrure est alimentée électriquement par le dispositif dans lequel elle est montée, par exemple un distributeur de billets. Dans encore une autre variante, elle est alimentée au moyen d'une génératrice actionnée par l'utilisateur ; la montre 54 utilise dans cas sa propre source d'énergie afin de conserver l'heure même lorsque le reste du système n'est plus alimenté électriquement.

[0038] Nous allons maintenant décrire à l'aide de la figure 2 un exemple de mise en oeuvre du procédé de l'invention.

[0039] Initialement, un utilisateur 4 souhaitant déverrouiller la serrure 5 se trouve physiquement devant cette serrure et introduit au cours de l'étape 100 un code personnel sur le clavier 51, par exemple un code numérique ou alphanumérique, par exemple un code à 6 chiffres.

[0040] Au cours de l'étape 101, les moyens de calcul dans la serrure vérifient le code personnel introduit. Dans une première variante, le code personnel est comparé avec une liste de codes acceptés (« liste blanche ») stockée dans la serrure. Cette variante a cependant l'inconvénient de devoir transmettre une telle liste à la serrure, par exemple au travers d'un réseau de télécommunication ou par le biais des convoyeurs. Une telle transmission est sujette à des risques d'interception ou d'espionnage. Afin d'éviter ce risque, dans une deuxième variante préférentielle, la serrure se contente de vérifier au cours de l'étape 101 si le code personnel introduit est plausible, par exemple si le format du code est admissible, si un éventuel code de parité est correct, ou si le code personnel introduit n'appartient pas une liste de codes rejetés (« liste noire ») parce que inexistants ou appartenant à des utilisateurs refusés. La vérification du code personnel particulier introduit par l'utilisateur est dans cette deuxième variante déléguée à la centrale, à qui le code devra être transmis implicitement ou explicitement ultérieurement.

[0041] Si la serrure détecte au cours de l'étape 101 que le code personnel introduit est invalide, il est rejeté, et un message d'erreur peut être affiché sur l'affichage

50 pour informer l'utilisateur et l'inviter à introduire un nouveau code. Afin d'empêcher des attaques par « force brute », c'est-à-dire en testant successivement un grand nombre de codes différents, il est possible par exemple d'introduire un délai entre chaque tentative et/ou de limiter le nombre de tentatives infructueuses possibles avant de bloquer la serrure pour une plus longue période, ou jusqu'à l'introduction d'une manoeuvre de déblocage.

[0042] Dans une variante, l'utilisateur s'identifie envers la serrure en prouvant la possession d'un objet, par exemple une clé, une clé électronique, une carte à puce, etc. L'objet présenté peut être lui-même protégé par un code, notamment dans le cas d'une carte à puce. Cette solution a cependant l'inconvénient de nécessiter une organisation pour distribuer et gérer les objets à présenter. L'utilisateur peut aussi s'identifier au moyen de données biométriques acquises au moyen d'un capteur biométrique, par exemple à l'aide de ses empreintes digitales, de l'iris, de la rétine, du visage, de la voix, etc. Ces données biométriques ont cependant l'inconvénient de ne pas pouvoir être remplacées avec la facilité d'un code personnel qui peut être transmis au dernier moment à l'utilisateur; un enregistrement de l'utilisateur est en outre requis pour acquérir ses données biométriques de référence.

[0043] Différents procédés d'identification peuvent en outre être combinés. Il est aussi possible de réclamer une identification supplémentaire ou différente selon les circonstances ; par exemple, une identification biométrique, ou par clé, peut être exigée lorsque l'identification par code personnel n'a pas fonctionné après un nombre d'essais prédéterminé, ou lorsque la somme à disposition dans le volume protégé dépasse une certaine somme, ou lorsque d'autres circonstances imposent une sécurité accrue.

[0044] Si le code personnel est valide, les moyens de calcul de la serrure (ou, ultérieurement, ceux de la centrale) vérifient les droits d'accès attachés à l'utilisateur identifié par ce code. Les droits d'accès peuvent dépendre du temps ; par exemple, il est possible de n'autoriser un déverrouillage de la serrure que pendant une fenêtre temporelle limitée correspondant à l'heure à laquelle l'utilisateur est attendu. Cette fenêtre temporelle peut être codée, avec d'autres informations, dans la réponse de la centrale décrite plus bas.

[0045] Selon l'objet protégé, il est aussi possible de permettre un accès à des parties différentes du volume protégé à différents utilisateurs ; il est par exemple envisageable d'autoriser un technicien à accéder uniquement à différents organes d'un distributeur, par exemple pour recharger le papier, prélever des fichiers de logs ou effectuer d'autres opérations de maintenance, tandis que l'accès au coffre est réservé à d'autres utilisateurs identifiés à l'aide d'autres codes. Selon l'invention, la serrure 5 vérifie aussi si une manipulation particulière a été effectuée lors de l'introduction du code personnel par l'utilisateur 4 afin de signaler qu'il est sous contrainte, par exemple parce qu'un assaillant est en train de le forcer à introduire le code. La manipulation particulière peut impliquer par exemple l'introduction d'un code personnel différent, la pression d'une touche ou d'un organe supplémentaire, un appui prolongé sur une touche, ou d'autres manipulations identifiables sans ambiguïtés par la serrure 5 mais difficile à détecter pour un assaillant observant la manoeuvre. La détection d'une manipulation particulière entraîne un comportement différent de la serrure, comme on le verra plus bas.

[0046] En cas d'identification valide, la serrure 5 affiche ensuite au cours de l'étape 102 une question sur l'affichage 50. La question affichée peut dépendre de l'heure, de la date, de l'utilisateur identifié, de la serrure, d'autres paramètres collectés par la serrure, et/ou d'une éventuelle détection de manipulation pour signaler une contrainte. Par ailleurs, le choix de la question peut dépendre d'un facteur aléatoire. Chaque question est de préférence affichée une seule fois et n'est pas réutilisée, ou au moins pas pour le même utilisateur. La question affichée peut être générée par une fonction mathématique, par exemple une fonction pseudo-aléatoire, et/ou choisie dans une table de questions prédéfinies. Dans une variante préférentielle, la fonction pseudo-aléatoire dépend au moins partiellement de la valeur d'un compteur incrémentée à chaque ouverture du coffre et/ou à chaque tentative de déverrouillage ; le compteur ne peut jamais être décrémenté, et la valeur maximale qui peut être comptée est suffisante pour assurer que le compteur ne reboucle. Il serait aussi possible d'employer l'heure comptée par l'horloge de la serrure pour initialiser la fonction pseudo-aléatoire ; toutefois, une horloge doit pouvoir être mise à l'heure, et donc pouvoir être retardée, ce qui pourrait être utilisé pour « remonter dans le temps » afin de forcer la serrure à générer à nouveau une question dont la réponse est déjà connue.

[0047] Les identifications fructueuses et les tentatives d'identifications infructueuses sont de préférence enregistrées dans un fichier de log dans la serrure, avec la date et l'heure de l'événement. Ce fichier peut être consulté par un technicien, par exemple en introduisant un code particulier sur le clavier 51, en branchant un ordinateur sur un connecteur sur la face frontale de la serrure, et/ou à distance depuis la centrale 1 au travers d'un réseau de communication.

[0048] L'utilisateur 4 lit la question affichée au cours de l'étape 103, puis l'introduit au cours de l'étape 104 sur le clavier de son équipement mobile 3. Comme la question affichée sur l'affichage 50 est imprévisible, et qu'il est possible de distinguer les questions possibles des questions non licites, on s'assure ainsi que l'utilisateur 4 se trouve bel et bien à proximité de la serrure 5 à ouvrir.

[0049] Au cours de l'étape 105, la question introduite par l'utilisateur est transmise par l'équipement mobile 3 à la centrale, par exemple sous forme de message court, par exemple de SMS, de e-mail, de paquets de données, de code DTMF, ou de message vocal parlé par l'utilisateur.

[0050] Une application dédiée, par exemple un applet Java (marque déposée), peut être exécutée par l'équipement mobile 3 pour faciliter l'introduction de la question et sa transmission vers la centrale 1. Dans une variante, la question est simplement introduite par l'utilisateur et transmise à un numéro téléphonique ou vers une adresse e-mail connus de l'utilisateur.

[0051] L'accès à l'équipement mobile 3, ou à l'application de l'équipement mobile, peut être protégé par un mot de passe, un code pin, ou requérir d'autres mesures d'identification ou d'authentification de l'utilisateur 4.

[0052] Outre la question introduite par l'utilisateur, le message transmis à la centrale 1 au cours de l'étape 105 peut inclure d'autres informations, y compris par exemple une identification de l'équipement mobile 3 employé (par exemple un numéro d'appelant MSISDN), des données d'identification d'utilisateur (y compris son code personnel, mais aussi par exemple un mot de passe, un code PIN, des données biométriques, des données extraites d'une carte à puce dans l'équipement mobile, etc), des informations de positions fournies par le module de géolocalisation 30, des informations fournies par le module PTI 31, etc. Le message peut en outre être signé électroniquement par une carte à puce dans l'équipement mobile 3, afin de prouver son authenticité et son intégrité, et/ou encrypté afin de garantir sa confidentialité.

[0053] Au cours de l'étape 106, la centrale 1 reçoit le message transmis par l'utilisateur et le vérifie. La vérification implique par exemple de contrôler si la question transmise est une question licite, en fonction de l'utilisateur qui l'emploie, de la serrure devant laquelle il se trouve, de l'heure, etc. Si le code personnel de l'utilisateur a été transmis avec la question, ou s'il est implicitement contenu dans la question, la centrale 1 peut aussi s'assurer que cet utilisateur est effectivement autorisé à accéder à cette serrure à ce moment, par exemple en fonction d'un plan de route préalablement établi pour un convoyeur se déplaçant entre plusieurs serrures. D'autres vérifications peuvent tenir compte de l'emplacement géographique de l'utilisateur, des données fournies par le dispositif PTI, d'éventuelles données fournies directement par la serrure, des vérifications d'informations signalant une manipulation pour indiquer une contrainte, etc.

[0054] Si les vérifications effectuées au cours de l'étape 106 permettent de déterminer que la question est une question légitime transmise au bon moment par un utilisateur autorisé, les droits de cet utilisateur sont de préférence déterminés. Lorsque l'utilisateur possède au moins certains droits, une réponse à cette question est calculée au cours de l'étape 107, au moyen d'un algorithme inconnu des utilisateurs et exécuté par les moyens de calcul 11. La réponse est de préférence constituée par une suite numérique ou alphanumérique ne permettant pas à un utilisateur de déterminer immédiatement si elle contient des instructions implicites pour la serrure.

[0055] Dans le cas contraire où la question reçue n'est pas valide, ou si elle a été transmise par un utilisateur non autorisé, ou lorsque l'utilisateur ne possède pas les droits d'accès nécessaires, ou lorsque d'autres anomalies ont été détectées, aucune réponse n'est calculée. Dans une variante, un message d'erreur informant l'utilisateur est alors transmis à l'équipement mobile 3 et affiché par ce dernier, afin par exemple de permettre à l'utilisateur de corriger une erreur de frappe lors de l'introduction de la question. Alternativement, la centrale peut fournir une réponse modifiée entraînant un comportement modifié de la serrure. La réaction de la centrale et la réponse envoyée peut aussi dépendre de l'anomalie détectée, du nombre d'essais infructueux, ou d'autres conditions.

[0056] Si la centrale détecte à partir de la question reçue, que l'utilisateur a effectué une manipulation particulière pour indiquer qu'il est sous contrainte, elle calcule une réponse modifiée par rapport à la réponse normale, afin de provoquer un comportement particulier de la serrure. Différentes réponses modifiées peuvent être choisies automatiquement ou par des opérateurs humains selon les circonstances, afin de déclencher différentes réactions.

[0057] D'autres informations complémentaires peuvent être codées dans la réponse, par exemple pour définir les droits d'accès de l'utilisateur à la serrure, par exemple en fonction du temps.

[0058] La réponse à la question est ensuite transmise à l'équipement mobile au cours de l'étape 108, puis affichée et lue par l'utilisateur au cours de l'étape 109. La réponse peut comporter par exemple un code numérique ou alphanumérique et est introduite par l'utilisateur 4 sur le clavier 51 de la serrure 5 au cours de l'étape 110.

[0059] Au cours de l'étape 111, les moyens de calcul dans la serrure 5 vérifient si la réponse reçue est correcte. Dans une variante, cette vérification implique une comparaison avec une réponse calculée par la serrure elle-même, en exécutant le même algorithme que celui exécuté par la centrale 1. Dans une variante, la vérification de la réponse reçue est effectuée sans la recalculer indépendamment, par exemple en vérifiant la réponse reçue au moyen d'une clé de vérification permettant de distinguer la ou les réponses possibles à la question des réponses non valides, en fonction de la question et/ou d'autres paramètres. Cette variante a l'avantage de ne pas requérir de copies de l'algorithme dans une multitude de serrures disséminées sur un territoire ; elle est en outre compatible avec des algorithmes susceptibles de fournir plusieurs réponses valides à une même question.

[0060] Les moyens de calcul 5 vérifient en outre au cours de l'étape 111 si la réponse reçue tient compte d'une détection de manipulation par un utilisateur sous contrainte, ou si d'autres paramètres sont codés dans cette réponse.

[0061] Dans une variante non revendiquée, l'utilisateur indique un état de contrainte à la serrure 5 lors de l'introduction de la réponse sur le clavier au cours de l'étape 110, par exemple en introduisant un chiffre supplémentaire, etc. Cette solution est cependant moins sûre car

un usurpateur pourrait introduire lui-même la réponse, sans effectuer de manipulation supplémentaire. En outre la centrale n'est pas informée d'une manipulation.

[0062] Dans une variante supplémentaire non revendiquée, un état de contrainte est directement détecté par la serrure 5 à partir de capteurs ou de données supplémentaires, de données transmises par le distributeur auquel la serrure est associée, ou de données directement transmises par la centrale 1.

[0063] Si la serrure détermine au cours de l'étape 111 que la réponse introduite est correcte, et qu'elle ne correspond pas à un état de contrainte, la serrure est déverrouillée au cours de l'étape 112, jusqu'au prochain verrouillage manuel ou pendant une durée limitée. L'utilisateur peut ainsi accéder au volume protégé, ou à une partie de ce volume. Cet événement est protocolé dans le fichier de log, en indiquant l'heure et la durée du déverrouillage. Par ailleurs, le compteur employé pour initialiser la fonction pseudo-aléatoire est incrémenté de façon irréversible.

[0064] Si la serrure détermine au cours de l'étape 111 que la réponse introduite est incorrecte, la serrure reste verrouillée, et un message d'erreur peut s'afficher sur l'affichage 50. Après un nombre prédéterminé d'essais infructueux, une alarme peut être déclenchée localement ou envoyée à la centrale 1 ou vers une autre adresse prédéterminée. Dans une variante, les billets dans le distributeur sont automatiquement détruits ou marqués avec une encre indélébile.

[0065] Si la serrure détermine au cours de l'étape 111 que la réponse introduite est correcte, mais qu'elle correspond à un état de contrainte, elle effectue l'une des actions suivantes selon la réponse :

- maintien du verrouillage, éventuellement même si une réponse correcte est introduite ultérieurement pendant une durée limitée,
- déverrouillage retardé de la serrure après un délai court, mais plus long que le délai usuel
- déverrouillage retardé de la serrure après un délai long, par exemple supérieur à trois minutes,
- affichage d'un message particulier sur l'affichage 50 de la serrure, par exemple pour indiquer à l'assaillant qu'il a été repéré,
- déclenchement d'une alarme, par exemple une alarme sonore ou
- destruction du contenu du volume protégé par la serrure par exemple par marquage des billets au moyen d'une encre indélébile.

[0066] Les deux dernières options doivent cependant être utilisées avec parcimonie pour éviter le risque que l'utilisateur légitime soit pris en otage ou victime de représailles.

[0067] Ces différentes mesures peuvent en outre être combinées.

[0068] Après l'introduction d'une réponse correcte, ou d'une réponse indiquant une manipulation, un code de quittance est de préférence affiché au cours d'une étape supplémentaire non illustrée sur l'affichage 50. L'utilisateur introduit ensuite ce code de quittance sur son équipement mobile et le transmet à la centrale 1, de la même façon que la question auparavant, afin d'indiquer à la centrale la fin de sa mission. Le code de quittance requis est de préférence unique et imprévisible à l'avance, de manière à s'assurer que l'utilisateur l'a bien lu à la suite de la manipulation et qu'il ne l'a pas déduit autrement. La centrale est cependant en mesure de vérifier si le code de quittance transmis est licite.

[0069] A nouveau, le code de quittance généré par la serrure ou réintroduit par l'utilisateur peut contenir des indications signalant à la centrale des événements particuliers, par exemple pour indiquer si la serrure a été ouverte, un nouvel état de contrainte, ou tout autre événement. Le code de quittance transmis peut en outre, de la même façon que la question auparavant, être signé, encrypté, et accompagné de données telles que la date, l'heure, l'identification d'utilisateur, d'équipement mobile, de position géographique, etc. La centrale peut ainsi vérifier ces données, ou détecter l'absence d'envoi de message de quittance après un délai prédéterminé, pour décider d'une action appropriée, y compris le déclenchement d'une alarme, le déclenchement d'une intervention, et/ou le verrouillage d'autres serrures à proximité ou sur le parcours prévu de l'utilisateur même en cas de manoeuvre correcte.

[0070] Le code de quittance généré est de préférence, de la même façon que la question ou la réponse, dépendant de l'utilisateur en cours, de la serrure en cours et/ou d'autres paramètres tels que la date, l'heure, la détection de manipulations éventuelles.

[0071] Dans le procédé ci-dessus, une autorisation de déverrouillage d'une serrure particulière par un utilisateur particulier peut être modifiée par la centrale 1 de l'une des façons suivantes :

- En communiquant un nouveau code personnel à l'utilisateur, par exemple par le biais d'un appel téléphonique, d'un SMS, d'un e-mail ou d'un autre message envoyé à l'équipement mobile 3, ou transmis oralement à l'utilisateur

- En modifiant les codes personnels acceptés par les serrures 5, par exemple en envoyant de nouvelles listes de codes acceptés (liste blanche ; seulement dans la variante où ces listes sont stockées dans la serrure), de nouvelles listes de codes refusés (liste noire), de nouvelles listes de codes suspects, nécessitant des vérifications supplémentaires (liste grise), ou en modifiant les droits d'accès associés à ces codes. Les listes de codes et les droits d'accès peuvent être transmis par un canal de télécommunication au travers d'une interface de télécommunication dans la serrure, et/ou au moyen d'une interface de télécommunication liée au dispositif protégé par la serrure, ou introduit directement, au travers

d'un support de données physique, par un technicien chargé de la maintenance.

- En modifiant les codes personnels acceptés par la centrale, en fonction de listes blanches, grises ou noires, ou d'autres paramètres tels que le plan de route prévu de l'utilisateur.

- En modifiant la réponse donnée à une question transmise par un utilisateur, ou en refusant de répondre à ces questions.

- En envoyant un ordre directement à la serrure, par exemple un ordre de maintenir le verrouillage pendant un intervalle.

[0072] Par ailleurs, indépendamment du comportement de la centrale, la serrure 5 peut elle-même autoriser ou refuser le déverrouillage en fonction de paramètres acquis directement ou au travers du dispositif protégé, par exemple à l'aide de capteurs, caméras ou microphones associés à la serrure ou au dispositif, obtenus en analysant les manipulations de l'utilisateur sur le clavier 5, ou selon un historique interne des manipulations de cet utilisateur et/ou de la serrure 5.

[0073] Il est cependant possible, dans le cadre de l'invention, de ne prévoir qu'une partie des possibilités d'autorisation de déverrouillage mentionnées ci-dessus.

[0074] La serrure décrite ci-dessus peut être employée pour sécuriser des volumes autres que des distributeurs de billet, par exemple des armoires d'armes employées dans les commissariats ou par l'armée, des coffres-forts, ou d'autres volumes dont le verrouillage ou le déverrouillage par un utilisateur local doit être autorisé par une centrale à distance.

[0075] Par ailleurs, la serrure de l'invention peut être programmée à n'importe quel moment, par exemple depuis la centrale et/ou à l'aide d'un code particulier introduit par un utilisateur à proximité, pour fonctionner dans un mode autre que le mode interactif décrit plus haut. Par exemple, il serait possible de reprogrammer cette serrure pour autoriser son déverrouillage par certains utilisateurs, ou même par tous les utilisateurs, sans établir de connexion avec la centrale.

Revendications

1. Procédé de contrôle de verrouillage de serrure électronique (5), comportant les étapes suivantes :

un utilisateur (4) s'identifie auprès de la serrure électronique (5) en introduisant un code personnel sur des moyens d'introduction de données (51) de la serrure,
la serrure électronique (5) affiche une question, l'utilisateur transmet la question à l'aide d'un équipement mobile à une centrale (1),
la centrale calcule la réponse à la question et transmet cette réponse à l'équipement mobile de l'utilisateur pour y être affichée puis lue par l'utilisateur,
l'utilisateur introduit la réponse dans la serrure, la serrure vérifie si la réponse est correcte et décide en fonction de cette réponse du déverrouillage de la serrure,
dans lequel
ledit utilisateur (4) effectue une manipulation particulière lors de l'introduction de son code personnel lorsqu'il souhaite signaler qu'il est sous contrainte,
la serrure détecte si une manipulation particulière est effectuée lors de l'introduction du code personnel de l'utilisateur,
la serrure génère et affiche une question dépendant d'une éventuelle détection de manipulation particulière,
ladite centrale (1) réagit alors en générant une réponse modifiée à ladite question, ladite réponse modifiée étant différente de la réponse générée lorsque ladite manipulation particulière n'est pas effectuée,
lorsque ledit utilisateur introduit ladite réponse modifiée, ladite serrure effectue au moins l'une des actions suivantes :

maintien du verrouillage de la serrure (5) ;
temporisation du déverrouillage de la serrure (5) par déverrouillage après un délai plus long que le délai usuel ;
affichage d'un message sur l'affichage (50) de ladite serrure (5) ;
déclenchement d'une alarme ;
destruction ou marquage du contenu du dispositif protégé par ladite serrure (5).

2. Le procédé la revendication 1, dans lequel à la fin de la manipulation un code de quittance est affiché par ladite serrure (5) et transmis par ledit utilisateur à la centrale (1) à l'aide d'un équipement mobile (3).

3. Le procédé de l'une des revendications 1 ou 2, dans lequel une question différente est affichée à chaque accès à la serrure.

4. Le procédé de l'une des revendications 1 à 3, dans lequel ladite centrale vérifie si ladite question est valide.

5. Le procédé de l'une des revendications 1 à 4, dans lequel les questions affichées dépendent desdits utilisateurs.

6. Le procédé de l'une des revendications 1 à 5, dans lequel ladite réponse à ladite question est calculée au moyen d'un algorithme dans ladite centrale (1),

et dans lequel ladite serrure vérifie au moyen du ou d'un algorithme exécuté dans la serrure si ladite réponse est correcte.

7. Le procédé de l'une des revendications 1 à 6, dans lequel ledit utilisateur (4) transmet ladite réponse à ladite centrale au moyen d'une communication établie au travers d'un réseau cellulaire (2) indépendant de ladite serrure.

8. Le procédé de la revendication 7, dans lequel ledit utilisateur (4) transmet ladite réponse à ladite centrale (1) au moyen d'un équipement mobile (3) apte à se connecter dans un réseau cellulaire,
ledit équipement mobile déterminant la position dudit utilisateur au moyen d'un dispositif de géolocalisation (30),
ladite position étant transmise à ladite centrale (1),
ladite centrale vérifiant ladite position avant de transmettre ladite réponse à ladite question.

9. Le procédé de l'une des revendications 7 à 8, ledit équipement mobile (3) mettant en oeuvre un équipement de protection de travailleur isolé (31) afin de déterminer si ledit utilisateur est vivant et/ou s'il est éveillé.

10. Le procédé de l'une des revendications 7 à 9, ledit équipement mobile (3) authentifiant ledit utilisateur au moyen d'une carte à puce, d'un code personnel et/ou de données biométriques (32).

11. Le procédé de la revendication 10, l'identité dudit utilisateur (4) déterminée dans ledit équipement mobile (3) étant transmise à ladite centrale (1) pour vérification.

12. Le procédé de l'une des revendications 1 à 11, dans lequel ledit utilisateur (4) s'identifie auprès de la serrure électronique (5) au moyen d'un code personnel introduit sur un clavier (51) de la serrure (5).

13. Le procédé de la revendication 12, dans lequel un nouveau code personnel est transmis par ladite centrale audit utilisateur (4).

14. Le procédé de l'une des revendications 1 à 13, comportant une étape préalable de définition de droits d'accès des utilisateurs identifiées à ladite serrure.

15. Le procédé de l'une des revendications 2 à 14, dans lequel un code de quittance différent est affiché à la fin de chaque manipulation.

16. Le procédé de l'une des revendications 2 à 15, dans lequel ledit code de quittance dépend de l'utilisateur en cours, de l'ouverture de la serrure, de la serrure en cours, de la date, de l'heure, et/ou de la détection de manipulations éventuelles.

17. Serrure électronique (5) comportant :

des moyens d'introduction de données (51) pour l'introduction d'un code d'identification personnel par un utilisateur,
des moyens pour détecter une manipulation particulière effectuée par l'utilisateur lors de l'introduction de son code personnel lorsqu'il souhaite signaler qu'il est sous contrainte,
un module configuré pour générer puis afficher une question en réponse à l'introduction d'un code d'identification personnel, ladite question générée dépendant d'une éventuelle détection de manipulation particulière lors de l'introduction du code d'identification personnel et correspondant à un état de contrainte,
un module (11) configuré pour vérifier si une réponse à ladite question introduite par lesdits moyens d'introduction de données (51) est correcte, et pour provoquer le déverrouillage de ladite serrure en cas de réponse correcte, ledit module (11) permettant en outre de vérifier si ladite réponse est une réponse modifiée correspondant à un état de contrainte
des moyens pour temporiser le déverrouillage de la serrure (5) après un délai plus long que le délai usuel ou pour maintenir le verrouillage de la serrure (5) ou pour afficher un message ou pour déclencher une alarme ou pour détruire ou marquer le contenu du dispositif protégé par ladite serrure en cas d'introduction de réponse modifiée.

18. La serrure de la revendication 17, comportant des moyens pour générer et afficher un code de quittance après une tentative de déverrouillage.

19. La serrure de l'une des revendications 17 à 18, comportant des moyens pour vérifier la plausibilité dudit code personnel, lesdits moyens étant dépourvus de liste d'utilisateurs autorisés.

20. La serrure de l'une des revendications 17 à 19, comportant un fichier de log pour répertorier les événements provoqués par lesdits utilisateurs.

21. La serrure de l'une des revendications 17 à 20, comportant une horloge alimentée en permanence pour déterminer l'heure et la date.

22. La serrure de l'une des revendications 17 à 21, comportant un compteur incrémentable de façon irréversible pour initialiser une fonction pseudo-aléatoire employée pour générer ladite question.

23. La serrure de l'une des revendications 17 à 22, com-

portant une interface pour échanger des données avec un dispositif protégé par ladite serrure.

24. La serrure de l'une des revendications 17 à 23, comportant une interface pour échanger des données avec une centrale à distance.

25. Procédé pour une centrale (1) de gestion de parc de serrures électroniques selon l'une des revendications 17 à 24, comportant les étapes de :

distribution de codes personnels à une pluralité d'utilisateurs (4) afin de leur permettre de s'identifier envers au moins certaines desdites serrures,
détermination des droits d'accès de chaque utilisateur (4) à chaque serrure (5),
réception d'une question transmise par un dit utilisateur au travers d'un réseau de télécommunication (2) à l'aide d'un équipement mobile dudit utilisateur,
vérification de la plausibilité de ladite question,
calcul d'une réponse à ladite question au moyen d'un algorithme confidentiel,
transmission de ladite réponse audit équipement mobile de l'utilisateur,
caractérisé par une étape de détection d'indications dans ladite question que ledit utilisateur (4) est sous contrainte, et de modification de ladite réponse dans ce cas, de sorte que lorsque ledit utilisateur introduit ladite réponse modifiée, ladite serrure effectue au moins l'une des actions suivantes :

maintien du verrouillage de la serrure (5) ;
temporisation du déverrouillage de la serrure (5) par déverrouillage après un délai plus long que le délai usuel ;
affichage d'un message sur l'affichage (50) de ladite serrure (5) ;
déclenchement d'une alarme ;
destruction ou marquage du contenu du dispositif protégé par ladite serrure (5).

26. Le procédé de la revendication 25, dans lequel ledit algorithme est différent pour chaque utilisateur (4).

27. Le procédé de l'une des revendications 25 à 26, comportant une étape de vérification de la position géographique dudit utilisateur à l'aide d'informations transmises par ce dernier.

Patentansprüche

1. Verfahren zur Steuerung der Verriegelung von elektronischen Verschlüssen (5), mit den folgenden Schritten:

ein Benutzer (4) identifiziert sich gegenüber dem elektronischen Verschluss, indem ein persönlicher Code auf Dateneingabemitteln (51) des Verschlusses eingegeben wird,
der elektronische Verschluss (5) zeigt eine Frage an,
der Benutzer überträgt die Frage mittels einer mobilen Ausrüstung an eine Steuereinheit (1),
die Steuereinheit berechnet die Antwort auf die Frage und übermittelt diese Antwort an die mobile Ausrüstung des Benutzers, damit sie dort angezeigt und anschliessend durch den Benutzer gelesen werden kann,
der Benutzer gibt die Antwort in den Verschluss ein,
der Verschluss überprüft, ob die Antwort richtig ist und entscheidet, basierend auf dieser Antwort, ob der Verschluss entriegelt wird,
worin
der besagte Benutzer (4) eine besondere Manipulation bei der Eingabe des persönlichen Codes durchführt, wenn er/sie anzeigen will, dass er/sie unter Zwang steht,
der Verschluss ermittelt, ob eine besondere Manipulation bei der Eingabe des persönlichen Codes eines Benutzers durchgeführt wurde,
der Verschluss eine auf der allfälligen Ermittlung der besonderen Manipulation basierende Anfrage erzeugt und anzeigt,
die besagte Steuereinheit (1) durch Erzeugung einer modifizierten Antwort auf die besagte Anfrage reagiert, wobei die besagte modifizierte Antwort sich unterscheidet von der Antwort, welche erzeugt wird, wenn die besondere Manipulation nicht durchgeführt wird,
wenn der besagte Benutzer die besagte modifizierte Antwort eingibt, der besagte Verschluss mindestens eine der folgenden Handlungen durchführt:

Aufrechterhalten der Verriegelung des Verschlusses (5);
Entriegelung des Verschlusses (5) verzögern, indem die Entriegelung nach einer Zeitspanne länger als die gewohnte Zeitspanne erfolgt;
Anzeigen einer Meldung auf der Anzeige (50) des besagten Verschlusses (5);
Alarmauslösung;
Zerstörung oder Kennzeichnung des Inhalts der Vorrichtung, welche durch den besagten Verschluss (5) geschützt ist.

2. Das Verfahren von Anspruch 1, worin am Ende der Manipulation ein Empfangscode durch den besagten Verschluss (5) angezeigt und durch den besagten Benutzer an die Steuereinheit (1) mittels einer mobilen Ausrüstung (3) übermittelt wird.

3. Das Verfahren eines der Ansprüche 1 oder 2, worin eine verschiedene Anfrage bei jedem Zugriff auf den Verschluss angezeigt wird.

4. Das Verfahren eines der Ansprüche 1 bis 3, worin die besagte Steuereinheit überprüft, ob die besagte Anfrage gültig ist.

5. Das Verfahren eines der Ansprüche 1 bis 4, worin die angezeigte Anfrage von den besagten Benutzern abhängig ist.

6. Das Verfahren eines der Ansprüche 1 bis 5, worin die besagte Antwort auf die besagte Anfrage mittels eines Algorithmus in der besagten Steuereinheit (1) berechnet wird,
und worin der besagte Verschluss mittels des oder eines im Verschluss durchgeführten Algorithmus überprüft, ob die besagte Antwort korrekt ist.

7. Das Verfahren eines der Ansprüche 1 bis 6, worin der besagte Benutzer (4) die besagte Antwort an die besagte Steuereinheit übermittelt, mittels einer Kommunikation, welche durch ein vom besagten Verschluss unabhängiges Mobilfunknetz (2) hergestellt wird.

8. Das Verfahren von Anspruch 7, worin der besagte Benutzer (4) die besagte Antwort an die besagte Steuereinheit (1) mittels einer mobilen Ausrüstung (3), die sich mit einem Mobilfunknetz verbinden kann, übermittelt,
worin die besagte mobile Ausrüstung die Position des besagten Benutzers mittels einer Standortbestimmungsvorrichtung (30) bestimmt,
worin die besagte Position an die besagte Steuereinheit (1) übermittelt wird,
worin die besagte Steuereinheit die besagte Position überprüft, bevor die besagte Antwort auf die besagte Anfrage übermittelt wird.

9. Das Verfahren eines der Ansprüche 7 bis 8, worin die besagte mobile Ausrüstung (3) eine Schutzausrüstung für isolierte Arbeiter (31) verwendet, um zu bestimmen, ob der besagte Benutzer lebt und/oder wach ist.

10. Das Verfahren eines der Ansprüche 7 bis 9, worin die besagte mobile Ausrüstung (3) den besagten Benutzer mittels einer Chipkarte, eines persönlichen Codes und/oder biometrischen Daten (32) authentifiziert.

11. Das Verfahren von Anspruch 10, worin die in der besagten mobilen Ausrüstung (3) bestimmte Identität des besagten Benutzers (4) an die besagte Steuereinheit (1) zwecks Überprüfung übermittelt wird.

12. Das Verfahren eines der Ansprüche 1 bis 11, worin der besagte Benutzer (4) sich gegenüber dem elektronischen Verschluss (5) mittels eines auf einer Tastatur (51) des Verschlusses (5) eingegebenen persönlichen Codes identifiziert.

13. Das Verfahren von Anspruch 12, worin ein neuer persönlicher Code durch die besagte Steuereinheit an den besagten Benutzer (4) übermittelt wird.

14. Das Verfahren eines der Ansprüche 1 bis 13, umfassend einen vorläufigen Schritt, worin die Zugriffsrechte der Benutzer gegenüber dem besagten Verschluss identifiziert werden.

15. Das Verfahren eines der Ansprüche 2 bis 14, worin eine andere Empfangsquitung am Ende jeder Manipulation angezeigt wird.

16. Das Verfahren eines der Ansprüche 2 bis 15, worin die besagte Empfangsquitung vom gegenwärtigen Benutzer, vom Öffnen des Verschlusses, vom gegenwärtigen Verschluss, vom Datum, von der Uhrzeit und/oder von der Erkennung von möglichen Manipulationen abhängt.

17. Elektronischer Verschluss (5), umfassend:

Dateneingabemittel (51) zur Eingabe eines persönlichen Identifizierungscodes durch einen Benutzer, Mittel zur Ermittlung einer besonderen Manipulation, die durch den Benutzer bei der Eingabe seines/ihres persönlichen Codes durchgeführt wird, wenn er/sie anzugeben wünscht, dass er/sie sich unter Zwang befindet, ein Modul, konfiguriert zum Erzeugen und dann zum Anzeigen einer Anfrage als Antwort auf die Eingabe eines persönlichen Identifizierungscodes, worin die besagte erzeugte Anfrage abhängig ist auf die allfällige Ermittlung einer besonderen Manipulation, wenn das persönliche Identifizierungscode eingegeben wird und einem Zwangszustand entspricht,
ein Modul (11), konfiguriert um zu überprüfen, ob eine durch die besagten Dateneingabemittel (51) eingegebene Antwort auf die besagte Anfrage korrekt ist, und um die Entriegelung des besagten Verschlusses im Fall einer korrekten Antwort zu verursachen, worin das besagte Modul (11) es zudem erlaubt zu überprüfen, ob die besagte Antwort eine modifizierte Antwort entsprechend einem Zwangszustand ist,
Mittel für die Verzögerung der Entriegelung des Verschlusses (5) nach einer Zeitspanne länger als die gewohnte Zeitspanne oder für das Aufrechterhalten der Verriegelung des Verschlusses (5) oder für das Anzeigen einer Meldung oder für das Auslösen eines Alarms oder für die

Zerstörung oder Kennzeichnung des Inhalts der Vorrichtung, welche durch den besagten Verschluss (5) geschützt ist, wenn eine modifizierte Antwort eingegeben wird.

18. Der Verschluss von Anspruch 17, umfassend Mittel zur Erzeugung und zum Anzeigen einer Empfangsquittung nach einem Entriegelungsversuch.

19. Der Verschluss eines der Ansprüche 17 bis 18, umfassend Mittel zur Überprüfung der Plausibilität des besagten persönlichen Codes, worin die besagten Mittel keine Liste von erlaubten Benutzern umfassen.

20. Der Verschluss eines der Ansprüche 17 bis 19, umfassend eine Protokolldatei zur Inventur der durch die besagten Benutzer verursachten Ereignisse.

21. Der Verschluss eines der Ansprüche 17 bis 20, umfassend eine dauerhaft gespeiste Uhr zur Bestimmung der Zeit und des Datums.

22. Der Verschluss eines der Ansprüche 17 bis 21, umfassend einen Zähler, der irreversible inkrementiert werden kann, um eine für die Erzeugung der besagten Anfrage verwendete Pseudozufallsfunktion zu initialisieren.

23. Der Verschluss eines der Ansprüche 17 bis 22, umfassend eine Schnittstelle zum Datenaustausch mit einer durch den besagten Verschluss geschützten Vorrichtung.

24. Der Verschluss eines der Ansprüche 17 bis 23, umfassend eine Schnittstelle zum Datenaustausch mit einer fernen Steuereinheit.

25. Verfahren für eine Steuereinheit (1) zur Verwaltung eines Parks von elektronischen Verschlüssen gemäss einem der Ansprüche 17 bis 24, mit den Schritten von:

Verteilung von persönlichen Codes an eine Vielzahl von Benutzern (4), um ihnen zu erlauben, sich gegenüber mindestens einigen der besagten Verschlüssen identifizieren zu können;
Bestimmung der Zugriffsrechte jedes Benutzers (4) zu jedem Verschluss (5),
Empfang einer Anfrage, welche von einem der Benutzer durch ein Telekommunikationsnetz (2) mittels einer mobilen Ausrüstung des besagten Benutzers übermittelt wurde,
Überprüfung der Plausibilität der besagten Anfrage,
Berechnung einer Antwort auf die besagte Anfrage mittels eines vertraulichen Algorithmus,
Übermittlung der besagten Antwort an die besagte mobile Ausrüstung des Benutzers,
gekennzeichnet durch einen Schritt der Ermittlung von Angaben in der besagten Anfrage, dass der besagte Benutzer (4) sich unter Zwang befindet, und der Modifizierung der besagten Antwort in diesem Fall, so dass wenn der besagte Benutzer die besagte modifizierte Antwort eingibt, der besagte Verschluss mindestens einen der folgenden Schritte durchführt:

Aufrechterhalten der Verriegelung des Verschlusses (5);
Entriegelung des Verschlusses (5) verzögern, indem die Entriegelung nach einer Zeitspanne länger als die gewohnte Zeitspanne erfolgt;
Anzeigen einer Meldung auf der Anzeige (50) des besagten Verschlusses (5);
Alarmauslösung;
Zerstörung oder Kennzeichnung des Inhalts der Vorrichtung, welche durch den besagten Verschluss (5) geschützt ist.

26. Verfahren gemäss Anspruch 25, worin der besagte Algorithmus für jeden Benutzer (4) anders ist.

27. Verfahren gemäss einem der Ansprüche 25 bis 26, umfassend einen Schritt der Überprüfung des geografischen Standortes des besagten Benutzers mittels von Letzterem übermittelten Informationen.

Claims

1. Method for controlling the locking of an electronic lock (5), including the following steps:

a user (4) is identified vis-à-vis the electronic lock (5) by entering a personal code on data input means (51) of the lock,
the electronic lock (5) displays a question,
the user transmits the question by means of a mobile equipment to a central station (1),
the central station computes the answer to the question and transmits this answer to the user's mobile equipment for it to be displayed to and read by the user,
the user enters the answer in the lock,
the lock verifies whether the answer is correct and decides according to this answer whether to unlock the door,
wherein
said user (4) performs a particular manipulation when entering his/her personal code when wishing to indicate he/she is under duress,
the lock detects if a particular manipulation is performed when the user's personal code is entered,

the lock generates and displays a question depending on a possible detection of a particular manipulation,
said central station (1) reacts by generating a modified answer to said question, said modified answer being different from the answer generated when said particular manipulation is not performed,
when said user enters said modified answer, said lock performs at least one of the following actions:

keeping the lock (5) locked;
temporizing the unlocking of the lock (5) by unlocking after a time lapse longer than the usual time lapse;
displaying a message on the display (50) of said lock (5);
triggering an alarm;
destroying or marking the contents of the device protected by said lock (5).

2. The method of claim 1, wherein at the end of the manipulation, a receipt code is displayed by said lock (5) and transmitted by said user to the central station (1) by means of a mobile equipment (3).

3. The method of claim 1 or 2, wherein a different question is displayed at each access to the lock.

4. The method of one of the claims 1 to 3, wherein said central station verifies if said question is valid.

5. The method of one of the claims 1 to 4, wherein the displayed questions depend on said users.

6. The method of one of the claims 1 to 5, wherein said answer to said question is computed by means of an algorithm in said central station (1),
and wherein said lock verifies by means of the or of an algorithm executed in the lock whether said answer is correct.

7. The method of one of the claims 1 to 6, wherein said user (4) transmits said answer to said central station by means of a communication established through a cellular network (2) independent from said lock.

8. The method of claim 7, wherein said user (4) transmits said answer to said central station (1) by means of a mobile equipment (3) capable of connecting into a cellular network,
wherein said mobile equipment determines the position of said user by means of a geolocation device (30),
wherein said position is transmitted to said central station (1),
wherein said central station checks said position before transmitting said answer to said question.

9. The method of one of the claims 7 to 8, wherein said mobile equipment (3) uses a protection equipment for lone workers (31) in order to determine whether said user is alive and/or awake.

10. The method of one of the claims 7 to 9, wherein said mobile equipment (3) authenticates said user by means of a chip card, a personal code and/or biometric data (32).

11. The method of claim 10, wherein the identity of said user (4) determined in said mobile equipment (3) is transmitted to said central station (1) for verification.

12. The method of one of the claims 1 to 11, wherein said user (4) is identified vis-à-vis the electronic lock (5) by means of a personal code entered on a keypad (51) of the lock (5).

13. The method of claim 12, wherein a new personal code is transmitted by said central station to said user (4).

14. The method of one of the claims 1 to 13, including a preliminary step of defining the access rights of the users identified to said lock.

15. The method of one of the claims 2 to 14, wherein a different receipt code is displayed at the end of each manipulation.

16. The method of one of the claims 2 to 15, wherein said receipt code depends on the current user, the opening of the lock, the current lock, the date, the time and/or the detection of possible manipulations.

17. Electronic lock (5), including:

data entering means (51) for entering a personal identification code by a user, means for detecting a particular manipulation performed by the user when entering his/her personal code when wishing to indicate he/she is under duress,
a module configured for generating and then displaying a question in reply to the entering of a personal identification code, wherein said generated question depends on the possible detection of a particular manipulation when the personal identification code is entered and corresponding to a duress state,
a module (11) configured for verifying whether an answer to said question entered by said data input means (51) is correct and for causing said lock to unlock in case of a correct answer, wherein said module (11) further makes it possible to verify whether said answer is a modified answer

corresponding to a duress state,
means for temporizing the unlocking of the lock (5) after a time lapse longer than the usual time lapse or for keeping the lock (5) locked or for displaying a message or for triggering an alarm or for destroying or marking the contents of the device protected by said lock when a modified answer is entered.

18. The lock of claim 17, including means for generating and displaying a receipt code after an unlocking attempt.

19. The lock of one of the claims 17 to 18, including means for verifying the plausibility of said personal code, wherein said means is without any list of authorized users.

20. The lock of one of the claims 17 to 19, including a log file for inventorying the events caused by said users.

21. The lock of one of the claims 17 to 20, including a clock powered permanently to determine the time and date.

22. The lock of one of the claims 17 to 21, including a counter that can be incremented irreversibly to initialize a pseudo-random function used for generating said question.

23. The lock of one of the claims 17 to 22, including an interface for exchanging data with a device protected by said lock.

24. The lock of one of the claims 17 to 23, including an interface for exchanging data with a remote central station.

25. Method for a central unit (1) for managing a fleet of electronic locks according to one of the claims 17 to 24, comprising the steps of:

distributing personal codes to a plurality of users (4) in order to allow them to identify themselves vis-à-vis at least some of said locks;
determining the access rights of each user (4) to each lock (5),
receiving a question transmitted by one said user through a telecommunications network (2) by means of a mobile equipment of said user,
verifying the plausibility of said question,
computing an answer to said question by means of a confidential algorithm,
transmitting said answer to said mobile equipment of the user,
characterized by a step of detecting indications in said question that said user (4) is under duress and of modifying said answer in this case, so that when said user enters said modified answer, said lock performs at least one of the following
keeping the lock (5) locked;
temporizing the unlocking of the lock (5) by unlocking after a time lapse longer than the usual time lapse;
displaying a message on the display (50) of said lock (5);
triggering an alarm;
destroying or marking the contents of the device protected by said lock (5).

26. Method according to claim 25, wherein said algorithm is different for each user (4).

27. Method according to one of the claims 25 to 26, including a step of verifying the geographic location of said user by means of information transmitted by the latter.

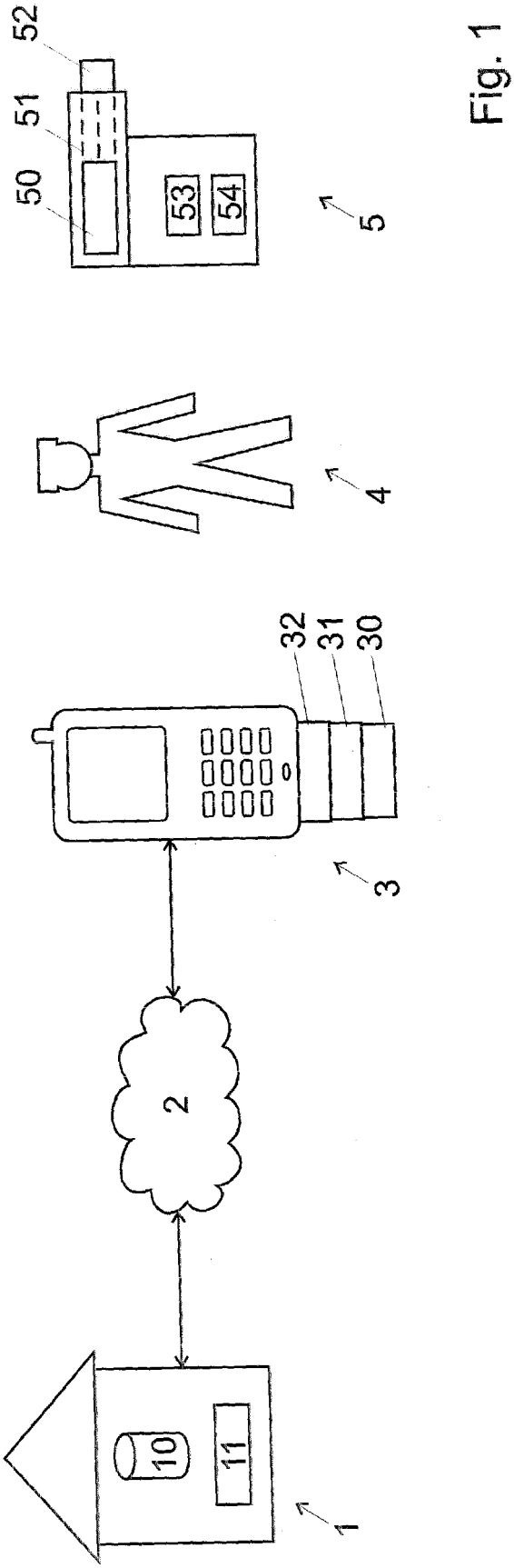


Fig. 1

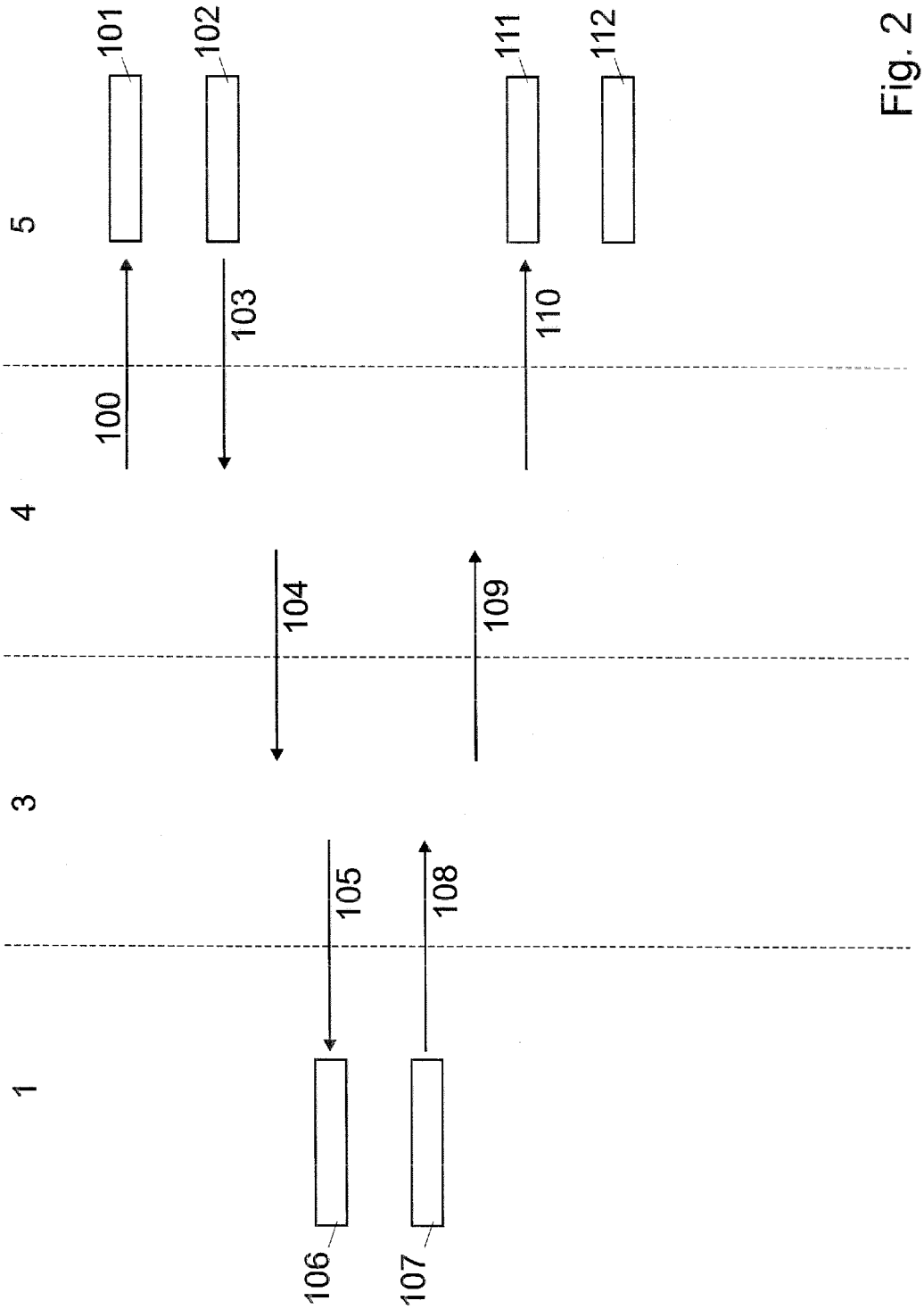


Fig. 2

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

- EP 0546701 A **[0008]**
- EP 0935041 A **[0009]**
- US 5774058 A **[0010]**