(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 132 372**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **22 00949**

(51) Int Cl[8] : ***G 07 C 9/00*** *(2022.01), E 05 B /, H 04 L 9/32, 9/14, 9/30, G 06 F 21/33*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 03.02.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.08.23 Bulletin 23/31.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *COGELEC Société anonyme à conseil d'administration* — FR et *SYNACKTIV Société par actions simplifiée à associé unique* — FR.

(72) **Inventeur(s) :** KLUBA Patrice et CARPENTIER Jean.

(73) **Titulaire(s) :** COGELEC Société anonyme à conseil d'administration, SYNACKTIV Société par actions simplifiée à associé unique.

(74) **Mandataire(s) :** INNOV-GROUP.

(54) Procédé de contrôle d'accès à des bâtiments.

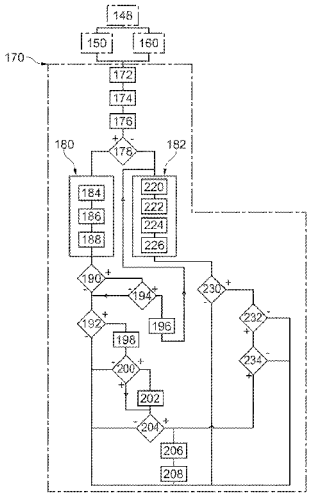
(57) Procédé de contrôle d'accès à des bâtiments

Lorsqu'un terminal mobile trouve (178) dans sa mémoire un premier cryptogramme associé à un identifiant d'une serrure électronique, il transmet (188) à cette serrure électronique son identifiant de terminal. En réponse, la serrure électronique :

- construit (192) un deuxième cryptogramme à partir de l'identifiant de terminal transmis, puis
- dans le cas où les premier et deuxième cryptogrammes sont identiques, la serrure électronique est autorisée à se déplacer dans son état déverrouillé.

Dans le cas contraire, le terminal mobile construit (220) un troisième cryptogramme (KKpub') à partir d'un identifiant de serrure (Cpub) transmis par la serrure électronique, puis dans le cas où un quatrième cryptogramme enregistré dans la mémoire de la serrure électronique est identique au troisième cryptogrammes, la serrure électronique est autorisée à se déplacer dans son état déverrouillé.

Fig. 7



FR 3 132 372 - A1

Description

Titre de l'invention : Procédé de contrôle d'accès à des bâtiments

[0001] L'invention concerne un procédé et un système de contrôle d'accès à des bâtiments. L'invention concerne également un terminal mobile et une serrure électronique pour la réalisation de ce système de contrôle d'accès.

[0002] Le déposant connaît un procédé de contrôle d'accès dans lequel, pour déverrouiller une serrure électronique, un terminal mobile transmet un certificat cryptographique à la serrure électronique. Ce certificat cryptographique contient typiquement un identifiant du terminal mobile, un identifiant de la serrure électronique à ouvrir et un code d'accès. De plus, ce certificat cryptographique comporte aussi une signature numérique construite à partir de l'identifiant du terminal mobile, de l'identifiant de la serrure électronique et du code d'accès. Cette signature numérique est un cryptogramme obtenu en chiffrant un condensat de l'identifiant du terminal mobile, de la serrure électronique et du code d'accès avec une clé secrète et en mettant en œuvre un algorithme de chiffrement asymétrique. La clé secrète n'est pas enregistrée dans le terminal mobile, de sorte qu'il n'est pas possible de construire, seulement à partir des données contenues dans ce terminal mobile, un nouveau certificat cryptographique pour, par exemple, déverrouiller une autre serrure électronique . Ainsi, si les données contenues dans ce terminal mobile sont compromises, cela ne remet pas en cause la sécurité du système.

[0003] Les serrures électroniques contiennent seulement la clé publique qui permet de vérifier l'intégrité et l'authenticité du certificat cryptographique reçu. Si l'intégrité et l'authenticité du certificat graphique reçu est confirmée, la serrure électronique se déplace dans son état déverrouillé pour autoriser l'accès au bâtiment. Dans le cas contraire, l'accès est refusé.

[0004] Un tel procédé est par exemple divulgué dans la demande EP1321901.

[0005] Ce procédé présente plusieurs avantages. Premièrement, il n'est pas nécessaire d'établir, entre la serrure et le terminal mobile, un canal sécurisé puis ensuite d'utiliser ce canal sécurisé pour transmettre des autorisations d'accès à la serrure électronique. En effet, pour établir un canal sécurisé, il faut générer dans le terminal mobile et dans la serrure électronique une clé de session qui varie à chaque fois que le terminal mobile est présenté devant cette serrure électronique. Ensuite, cette clé de session doit être utilisée pour chiffrer, à l'aide d'un algorithme de chiffrement symétrique, toutes les informations échangées entre le terminal mobile et la serrure électronique. Puisque aucun canal sécurisé n'est établi dans le procédé connu du déposant, cela évite d'avoir à générer de telles clés de session. Cela limite donc le nombre de trames d'informations à échanger entre le terminal mobile et la serrure électronique.

[0006] Deuxièmement, dans le procédé de la demande EP1321901, la clé privée qui permet de générer un certificat cryptographique qui permet de déverrouiller une serrure électronique n'est pas contenue dans le terminal mobile ni dans la serrure électronique à déverrouiller. Ainsi, même si la sécurité de la serrure électronique ou du terminal mobile est compromise, il n'est pas possible de construire de nouveaux certificats cryptographiques valides permettant de déverrouiller d'autres serrures électroniques seulement à partir des informations contenues dans cette serrure électronique ou dans ce terminal mobile. Dès lors, le fait que la sécurité d'une serrure électronique ou d'un terminal mobile soit compromise ne remet pas en cause la sécurité du système de contrôle d'accès.

[0007] Troisièmement, comme le souligne la demande EP1321901, ce procédé de contrôle d'accès est avantageux en ce qu'il faut simplement configurer les terminaux mobiles et non pas les serrures électroniques pour autoriser le déverrouillage de ces serrures électroniques. Plus précisément, pour qu'un terminal mobile soit autorisé à déverrouiller une serrure électronique particulière, il suffit d'enregistrer dans la mémoire de ce terminal mobile le certificat cryptographique correspondant à ce terminal mobile et à cette serrure électronique. Il n'est pas nécessaire de programmer la serrure électronique. Dès lors, les serrures électroniques n'ont pas besoin d'être directement raccordées à un réseau de télécommunication ou similaire.

[0008] Toutefois, la vérification d'un certificat cryptographique nécessite la mise en œuvre d'algorithmes de chiffrement asymétrique. Ces algorithmes sont complexes et entraînent une consommation d'énergie supérieure à celle nécessaire, par exemple, à la mise en œuvre d'algorithmes de chiffrement/déchiffrement symétrique. Or, dans la majorité des systèmes de contrôle d'accès, les terminaux mobiles et/ou les serrures électroniques sont alimentés par une pile ou une batterie. Il est donc souhaitable de disposer d'un procédé de contrôle d'accès qui présente les mêmes avantages que celui de la demande EP1321901 mais tout en permettant l'utilisation d'algorithmes de chiffrement symétrique à la place des algorithmes de chiffrement asymétriques.

[0009] De plus, le procédé de la demande EP1321901 impose de programmer chaque terminal mobile pour pouvoir ouvrir une serrure électronique. Or, de temps en temps, plutôt que de programmer un terminal mobile, il est préférable, par exemple parce que c'est plus simple, de programmer la serrure électronique plutôt que le terminal mobile. Ainsi, il est également souhaitable de disposer d'un procédé de contrôle d'accès qui présente les mêmes avantages que celui de la demande EP1321901 tout en autorisant en plus un fonctionnement inverse. Le fonctionnement inverse consiste à pouvoir programmer une serrure électronique pour qu'elle se déverrouille lorsqu'un terminal mobile particulier est présenté alors que ce terminal mobile particulier n'a pas été, au préalable, programmé pour ouvrir cette serrure électronique particulière. De plus, ce

fonctionnement inverse ne doit pas diminuer la sécurité du système de contrôle d'accès. Par exemple, il ne serait pas acceptable de prévoir que la serrure électronique transmette au terminal mobile un certificat cryptographique et que le déverrouillage de la serrure électronique soit autorisé dès que le terminal mobile confirme la validité, l'intégrité et l'authenticité du certificat cryptographique reçu. En effet, un terminal mobile pourrait facilement être modifié pour répondre systématiquement que le certificat cryptographique reçu est valide alors que ce n'est pas le cas et ainsi déclencher le déverrouillage de la serrure électronique.

[0010] Dans les procédés connus, lorsqu'un terminal mobile doit être invalidé, il est nécessaire de reprogrammer ce terminal ou de reprogrammer la serrure électronique pour que celle-ci ne se déplace plus dans son état déverrouillé lorsque ce terminal mobile est présenté. Dans ce texte, "invalider un terminal mobile" signifie annuler les autorisations d'accès du terminal mobile pour qu'il ne puisse plus déverrouiller une serrure électronique qu'il pouvait, par le passé, déverrouiller. Par exemple, dans le cas du procédé de la demande EP1321901, un terminal mobile peut être invalidé en ne lui transmettant pas le certificat cryptographique qui l'autorise à déverrouiller une serrure électronique particulière. Un terminal mobile peut aussi être invalidé en révoquant son certificat cryptographique. Lorsqu'une serrure électronique est déplacée d'un bâtiment vers un autre, il peut être nécessaire d'invalider tous les terminaux mobiles qui étaient autorisés à déverrouiller cette serrure électronique. Dans ce cas, chaque terminal mobile doit être invalidé individuellement ce qui est long et fastidieux à faire si le nombre de terminaux mobiles est important. Il est donc aussi souhaitable de disposer d'un procédé plus simple pour invalider l'ensemble des terminaux mobiles qui précédemment étaient autorisés à déverrouiller une serrure électronique particulière.

[0011] L'invention vise à proposer un procédé de contrôle d'accès qui satisfait au moins l'un des souhaits précédents. Elle a donc pour objet un procédé de contrôle d'accès à des bâtiments, ce procédé comportant :

- la fourniture de plusieurs serrures électroniques déplaçables chacune entre :
- un état verrouillé dans lequel elle interdit l'accès au bâtiment, et
- un état déverrouillé dans lequel elle autorise l'accès au bâtiment,

chaque serrure électronique comportant un microprocesseur et une mémoire contenant un identifiant de serrure qui identifie de façon unique cette serrure électronique parmi l'ensemble des serrures électroniques fournies et une première clé de chiffrement, et

- la fourniture de plusieurs terminaux mobiles d'ouverture, chacun de ces terminaux mobiles comportant un microprocesseur et une mémoire contenant un identifiant de terminal qui identifie de façon unique ce terminal mobile parmi l'ensemble des terminaux mobiles fournis,

- la programmation d'au moins un premier des terminaux mobiles fournis pour l'autoriser à déplacer une première des serrures électroniques fournies dans son état déverrouillé, cette programmation comportant l'enregistrement, dans la mémoire de ce premier terminal mobile, d'un premier cryptogramme et de l'identifiant de serrure de la première serrure électronique associé à ce premier cryptogramme, le premier cryptogramme étant construit à partir de l'identifiant de terminal du premier terminal, de l'identifiant de serrure de la première serrure électronique et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la première clé de chiffrement de la première serrure électronique, la première clé de chiffrement n'étant pas enregistrée dans la mémoire du premier terminal mobile de sorte qu'il n'est pas possible de construire ce premier cryptogramme seulement à partir des informations contenues dans la mémoire de ce premier terminal mobile,
- à chaque fois que le premier terminal mobile souhaite déplacer la première serrure électronique dans son état déverrouillé, le procédé comporte les étapes suivantes :
1) la première serrure électronique transmet au premier terminal mobile son identifiant de serrure contenu dans sa mémoire,
2) en réponse, le premier terminal mobile recherche dans sa mémoire s'il existe un premier cryptogramme associé à l'identifiant de serrure transmis, et
3) lorsqu'un tel premier cryptogramme est trouvé dans la mémoire du premier terminal mobile, alors le premier terminal mobile transmet à la première serrure électronique une première trame d'informations contenant son identifiant de terminal,
4) en réponse à la réception de la première trame d'informations, la première serrure électronique :
- construit un deuxième cryptogramme à partir de l'identifiant de terminal contenu dans la première trame d'informations, de son identifiant de serrure contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le premier cryptogramme paramétré par la première clé contenue dans la mémoire de la première serrure électronique, puis
- la première serrure électronique vérifie que le deuxième cryptogramme construit est identique au premier cryptogramme, et
- dans le cas où les premier et deuxième cryptogrammes sont identiques, la première serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les premier et deuxième cryptogrammes sont différents, le déplacement de la première serrure électronique depuis son état verrouillé vers son état déverrouillé est systématiquement interdit,
dans lequel :
- la fourniture de plusieurs terminaux mobiles comporte la fourniture de plusieurs terminaux mobiles dont la mémoire de chacun de ces terminaux mobiles comporte une

deuxième clé de chiffrement différente de la première clé de chiffrement, et
- le procédé comporte la programmation d'une seconde des serrures électroniques fournies pour l'autoriser à être déplacée dans son état déverrouillé par le premier terminal mobile, cette programmation comportant l'enregistrement, dans la mémoire de la seconde serrure électronique, d'un troisième cryptogramme construit à partir de l'identifiant de cette seconde serrure électronique, de l'identifiant de terminal du premier terminal mobile et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la deuxième clé de chiffrement du premier terminal mobile, la deuxième clé de chiffrement du premier terminal mobile n'étant pas enregistrée dans la mémoire de la seconde serrure électronique de sorte qu'il n'est pas possible de construire le troisième cryptogramme seulement à partir des informations contenues dans la mémoire de cette seconde serrure électronique, et
- à chaque fois que le premier terminal mobile souhaite déplacer la seconde serrure électronique dans son état déverrouillé, le procédé comporte les étapes suivantes :
5) la seconde serrure électronique transmet au premier terminal mobile son identifiant de serrure,
6) en réponse, le premier terminal mobile recherche dans sa mémoire un premier cryptogramme associé à l'identifiant de serrure transmis, puis
7) lorsque aucun premier cryptogramme associé à l'identifiant de serrure transmis n'est trouvé dans la mémoire du premier terminal mobile :
- le premier terminal mobile construit un quatrième cryptogramme à partir de l'identifiant de serrure transmis par la seconde serrure électronique, de son identifiant de terminal contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le troisième cryptogramme paramétré par la deuxième clé de chiffrement contenue dans la mémoire de ce premier terminal mobile, puis
- le premier terminal mobile transmet à la seconde serrure électronique une seconde trame d'informations, à la place de la première trame d'informations, cette seconde trame d'informations contenant l'identifiant de terminal du premier terminal , puis
8) en réponse à la réception de la seconde trame d'informations, la seconde serrure électronique vérifie, que le troisième cryptogramme enregistré dans sa mémoire est identique au quatrième cryptogramme, et
9) dans le cas où les troisième et quatrième cryptogrammes sont identiques, la seconde serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les troisième et quatrième cryptogrammes sont différents, le déplacement de la seconde serrure électronique depuis son état verrouillé vers son état déverrouillé est systématiquement interdit.

[0012] Les modes de réalisation de ce procédé peuvent comporter une ou plusieurs des ca-

ractéristiques suivantes :

R1)

- la programmation du premier terminal mobile comporte également l'enregistrement dans la mémoire de ce premier terminal mobile d'un premier indice de priorité spécifiquement associé au premier cryptogramme,
- le procédé comporte la programmation de la première serrure électronique fournies pour l'autoriser à être déplacée dans son état déverrouillé par le premier terminal mobile, cette programmation comportant l'enregistrement, dans la mémoire de la première serrure électronique :
- d'un troisième cryptogramme construit à partir de l'identifiant de cette première serrure électronique, de l'identifiant de terminal du premier terminal mobile et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la deuxième clé de chiffrement du premier terminal mobile, et
- d'un second indice de priorité spécifiquement associé au troisième cryptogramme,

la deuxième clé de chiffrement du premier terminal mobile n'étant pas enregistrée dans la mémoire de la première serrure électronique de sorte qu'il n'est pas possible de construire le troisième cryptogramme seulement à partir des informations contenues dans la mémoire de cette première serrure électronique, et

- lors de l'étape 3), la première trame d'informations contient, en plus, le premier indice de priorité associé au premier cryptogramme,
- après l'étape 3) et avant l'étape 4), en réponse à la réception par la première serrure électronique de la première trame d'informations, la première serrure électronique recherche dans sa mémoire un troisième cryptogramme préenregistré et un second indice de priorité associés à l'identifiant de terminal contenu dans la première trame d'informations, puis
- lorsqu'un tel second indice de priorité est trouvé dans la mémoire de la première serrure électronique, la première serrure électronique compare le premier indice de priorité contenu dans la première trame d'informations au second indice de priorité trouvé dans la mémoire de la première serrure électronique, et
- lorsque le premier indice de priorité est supérieur au second indice de priorité, la première serrure électronique exécute l'étape 4) et inhibe l'exécution de l'étape 7), et
- lorsque le premier indice de priorité est inférieur au second indice de priorité, la première serrure électronique exécute l'étape 7) et inhibe l'exécution de l'étape 4).

R2)

- la programmation de la seconde serrure électronique comporte la transmission à la seconde serrure électronique, par un second des terminaux mobiles fournis différent du premier terminal mobile, de l'identifiant de terminal du premier terminal mobile et du troisième cryptogramme, et

- en réponse, la seconde serrure électronique enregistre dans sa mémoire le troisième cryptogramme reçu associé à l'identifiant de terminal du premier terminal.

R3) La première clé de chiffrement est une clé unique.

R4)

- à chaque fois que le premier terminal mobile souhaite déplacer l'une des serrures électroniques fournies dans son état déverrouillé, le premier terminal mobile et cette serrure électronique échangent un nombre aléatoire, appelé "nonce", de sorte que ce nonce est connu à la fois du premier terminal mobile et de cette serrure électronique, ce nonce variant à chaque fois que le procédé de contrôle d'accès est exécuté entre le premier terminal mobile et cette serrure électronique,
- lors de l'étape 3), la première trame d'informations transmise contient en plus une première signature numérique construite à l'aide de l'identifiant de terminal du premier terminal et du nonce échangé, et
- lors de l'étape 7), la seconde trame d'informations transmise contient en plus une deuxième signature numérique construite à l'aide de l'identifiant de terminal du premier terminal et du nonce échangé.

R5) La première clé de chiffrement d'une serrure électronique est une clé unique de serrure différente de toutes les clés uniques de serrure des autres serrures électroniques.

R6) La deuxième clé de chiffrement d'un terminal mobile est une clé unique de terminal différente de toutes les clés uniques de terminal des autres terminaux mobiles.

[0013] L'invention a également pour objet un système de contrôle d'accès à des bâtiments comportant :

- plusieurs serrures électroniques déplaçables chacune entre :
- un état verrouillé dans lequel elle interdit l'accès au bâtiment, et
- un état déverrouillé dans lequel elle autorise l'accès au bâtiment,

chaque serrure électronique comportant un microprocesseur et une mémoire contenant un identifiant de serrure qui identifie de façon unique cette serrure électronique parmi l'ensemble des serrures électroniques du système de contrôle d'accès et une première clé de chiffrement, et

- plusieurs terminaux mobiles d'ouverture, chacun de ces terminaux mobiles comportant un microprocesseur et une mémoire contenant un identifiant de terminal qui identifie de façon unique ce terminal mobile parmi l'ensemble des terminaux mobiles du système de contrôle d'accès,
- au moins un premier des terminaux mobiles étant autorisé à déplacer une première des serrures électroniques dans son état déverrouillé, la mémoire de ce premier terminal mobile contenant à cet effet un premier cryptogramme et l'identifiant de serrure de la première serrure électronique associé à ce premier cryptogramme, le premier cryptogramme étant construit à partir de l'identifiant de terminal du premier

terminal, de l'identifiant de serrure de la première serrure électronique et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la première clé de chiffrement de la première serrure électronique, la première clé de chiffrement n'étant pas enregistrée dans la mémoire du premier terminal mobile de sorte qu'il n'est pas possible de construire ce premier cryptogramme seulement à partir des informations contenues dans la mémoire de ce premier terminal mobile,

- le premier terminal mobile et la première serrure électronique étant configurés pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la première serrure électronique dans son état déverrouillé, :

1) la première serrure électronique transmet au premier terminal mobile son identifiant de serrure contenu dans sa mémoire,

2) en réponse, le premier terminal mobile recherche dans sa mémoire s'il existe un premier cryptogramme associé à l'identifiant de serrure transmis, et

3) lorsqu'un tel premier cryptogramme est trouvé dans la mémoire du premier terminal mobile, alors le premier terminal mobile transmet à la première serrure électronique une première trame d'informations contenant son identifiant de terminal,

4) en réponse à la réception de la première trame d'informations, la première serrure électronique :

- construit un deuxième cryptogramme à partir de l'identifiant de terminal contenu dans la première trame d'informations, de son identifiant de serrure contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le premier cryptogramme paramétré par la clé contenue dans la mémoire de la première serrure électronique, puis

- la première serrure électronique vérifie, que le deuxième cryptogramme construit est identique au premier cryptogramme, et

- dans le cas où les premier et deuxième cryptogrammes sont identiques, la première serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les premier et deuxième cryptogrammes sont différents, le déplacement de la première serrure électronique depuis son état verrouillé vers son état déverrouillé est systématiquement interdit,

dans lequel :

- la mémoire de chacun des terminaux mobiles comporte une deuxième clé de chiffrement différente de la première clé de chiffrement, et

- une seconde des serrures électroniques étant autorisée à être déplacée dans son état déverrouillé par le premier terminal mobile, la mémoire de cette seconde serrure électronique contenant un troisième cryptogramme construit à partir de l'identifiant de cette seconde serrure électronique, de l'identifiant de terminal du premier terminal mobile et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la

deuxième clé de chiffrement du premier terminal mobile,
la deuxième clé de chiffrement du premier terminal mobile n'étant pas enregistrée dans la mémoire de la seconde serrure électronique de sorte qu'il n'est pas possible de construire le troisième cryptogramme seulement à partir des informations contenues dans la mémoire de cette seconde serrure électronique, et
- le premier terminal et la seconde serrure électronique sont configurés pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la seconde serrure électronique dans son état déverrouillé :
5) la seconde serrure électronique transmet au premier terminal mobile son identifiant de serrure,
6) en réponse, le premier terminal mobile recherche dans sa mémoire un premier cryptogramme associé à l'identifiant de serrure transmis, puis
7) lorsque aucun premier cryptogramme associé à l'identifiant de serrure transmis n'est trouvé dans la mémoire du premier terminal mobile :
- le premier terminal mobile construit un quatrième cryptogramme à partir de l'identifiant de serrure transmis par la seconde serrure électronique, de son identifiant de terminal contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le troisième cryptogramme paramétré par la deuxième clé de chiffrement contenue dans la mémoire de ce premier terminal mobile, puis
- le premier terminal mobile transmet à la seconde serrure électronique une seconde trame d'informations, à la place de la première trame d'informations, cette seconde trame d'informations contenant l'identifiant de terminal du premier terminal , puis
8) en réponse à la réception de la seconde trame d'informations, la seconde serrure électronique vérifie, que le troisième cryptogramme enregistré dans sa mémoire est identique au quatrième cryptogramme, et
9) dans le cas où les troisième et quatrième cryptogrammes sont identiques, la seconde serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les troisième et quatrième cryptogrammes sont différents, le déplacement de la seconde serrure électronique depuis son état verrouillé vers son état déverrouillé est systématiquement interdit.

[0014] L'invention a également pour objet un premier terminal mobile pour la réalisation du système ci-dessus de contrôle d'accès à des bâtiments, dans lequel ce premier terminal mobile comporte un microprocesseur et une mémoire contenant un identifiant de terminal qui identifie de façon unique ce premier terminal mobile parmi l'ensemble des terminaux mobiles du système de contrôle d'accès,

- ce premier terminal mobile étant autorisé à déplacer une première des serrures électroniques du système de contrôle d'accès dans son état déverrouillé, la mémoire de ce

premier terminal mobile contenant à cet effet un premier cryptogramme et l'identifiant de serrure de la première serrure électronique associé à ce premier cryptogramme, le premier cryptogramme étant construit à partir de l'identifiant de terminal du premier terminal, de l'identifiant de serrure de la première serrure électronique et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la première clé de chiffrement de la première serrure électronique, la première clé de chiffrement n'étant pas enregistrée dans la mémoire du premier terminal mobile de sorte qu'il n'est pas possible de construire ce premier cryptogramme seulement à partir des informations contenues dans la mémoire de ce premier terminal mobile,

- le premier terminal mobile étant configuré pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la première serrure électronique dans son état déverrouillé, :

1) le premier terminal mobile reçoit l'identifiant de serrure contenu dans la mémoire de la première serrure électronique,

2) en réponse, le premier terminal mobile recherche dans sa mémoire s'il existe un premier cryptogramme associé à l'identifiant de serrure reçu, et

3) lorsqu'un tel premier cryptogramme est trouvé dans la mémoire du premier terminal mobile, alors le premier terminal mobile transmet à la première serrure électronique une première trame d'informations contenant son identifiant de terminal,

dans lequel :

- la mémoire du premier terminal mobile comporte une deuxième clé de chiffrement différente de la première clé de chiffrement,

- le premier terminal est configuré pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la seconde serrure électronique dans son état déverrouillé :

5) le premier terminal reçoit de la seconde serrure électronique son identifiant de serrure,

6) en réponse, le premier terminal mobile recherche dans sa mémoire un premier cryptogramme associé à l'identifiant de serrure reçu, puis

7) lorsque aucun premier cryptogramme associé à l'identifiant de serrure reçu n'est trouvé dans la mémoire du premier terminal mobile :

- le premier terminal mobile construit un quatrième cryptogramme à partir de l'identifiant de serrure reçu, de son identifiant de terminal contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le troisième cryptogramme paramétré par la deuxième clé de chiffrement contenue dans la mémoire de ce premier terminal mobile, puis

- le premier terminal mobile transmet à la seconde serrure électronique une seconde trame d'informations, à la place de la première trame d'informations, cette seconde

trame d'informations contenant l'identifiant de terminal du premier terminal et une signature numérique construite à partir du quatrième cryptogramme construit.

[0015] Les modes de réalisation de ce premier terminal peuvent comporter la caractéristique suivante :

- L'identifiant de terminal de ce terminal mobile est enregistré dans une zone non-réinscriptible de sa mémoire.

[0016] L'invention a également pour objet un ensemble d'une première et d'une seconde serrures électroniques pour la réalisation du système ci-dessus de contrôle d'accès à des bâtiments, dans lequel la première et la seconde serrures électroniques sont chacune déplaçables entre :

- un état verrouillé dans lequel elle interdit l'accès au bâtiment, et
- un état déverrouillé dans lequel elle autorise l'accès au bâtiment,

chacune des première et seconde serrures électroniques comportant un micro-processeur et une mémoire contenant un identifiant de serrure qui identifie de façon unique cette serrure électronique parmi l'ensemble des serrures électroniques du système de contrôle d'accès et une première clé de chiffrement, et

- la première serrure électronique est configurée pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la première serrure électronique dans son état déverrouillé, :

4) en réponse à la réception de la première trame d'informations, la première serrure électronique :

- construit un deuxième cryptogramme à partir de l'identifiant de terminal contenu dans la première trame d'informations, de son identifiant de serrure contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le premier cryptogramme paramétré par la clé contenue dans la mémoire de la première serrure électronique, puis
- la première serrure électronique vérifie que le deuxième cryptogramme construit est identique au premier cryptogramme, et
- dans le cas où les premier et deuxième cryptogrammes sont identiques, la première serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les premier et deuxième cryptogrammes sont différents, le déplacement de la première serrure électronique depuis son état verrouillé vers son état déverrouillé est systématiquement interdit,

dans lequel :

- la seconde des serrures électroniques est autorisée à être déplacée dans son état déverrouillé par le premier terminal mobile, la mémoire de cette seconde serrure électronique contenant un troisième cryptogramme construit à partir de l'identifiant de cette seconde serrure électronique, de l'identifiant de terminal du premier terminal mobile et

en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la deuxième clé de chiffrement du premier terminal mobile,
la deuxième clé de chiffrement du premier terminal mobile n'étant pas enregistrée dans la mémoire de la seconde serrure électronique de sorte qu'il n'est pas possible de construire le troisième cryptogramme seulement à partir des informations contenues dans la mémoire de cette seconde serrure électronique, et
- la seconde serrure électronique est configurée pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la seconde serrure électronique dans son état déverrouillé :
5) la seconde serrure électronique transmet au premier terminal mobile son identifiant de serrure, puis
8) en réponse à la réception de la seconde trame d'informations, la seconde serrure électronique vérifie que le troisième cryptogramme enregistré dans sa mémoire est identique au quatrième cryptogramme, et
9) dans le cas où les troisième et quatrième cryptogrammes sont identiques, la seconde serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les troisième et quatrième cryptogrammes sont différents, le déplacement de la seconde serrure électronique depuis son état verrouillé vers son état déverrouillé est systématiquement interdit.

[0017] L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple non limitatif et faite en se référant aux dessins sur lesquels :

- la [Fig.1] est une illustration schématique de l'architecture d'un système de contrôle d'accès à des bâtiments ;
- la [Fig.2] est une illustration schématique en coupe verticale d'une serrure électronique du système de contrôle d'accès de la [Fig.1] ;
- la [Fig.3] est une illustration schématique d'une table d'autorisation d'accès contenue dans la serrure électronique de la [Fig.2] ;
- la [Fig.4] est une illustration schématique d'une liste d'indices de terminaux mobiles contenue dans la serrure électronique de la [Fig.2] ;
- la [Fig.5] est une illustration schématique du contenu d'une mémoire d'un terminal mobile du système de contrôle d'accès de la [Fig.1] ;
- la [Fig.6] est une illustration schématique d'une table d'autorisation d'accès contenue dans la mémoire représentée sur la [Fig.5] ;
- la [Fig.7] est un organigramme d'un procédé de contrôle d'accès à des bâtiments mis en œuvre dans le système de contrôle accès de la [Fig.1] ;
- la [Fig.8] est une illustration schématique de l'architecture d'une première trame d'informations transmise d'un terminal mobile vers une serrure électronique du

système de la [Fig.1], et

- la [Fig.9] est une illustration schématique de l'architecture d'une seconde trame d'informations transmise d'un terminal mobile vers une serrure électronique du système de la [Fig.1].

[0018] Dans la suite de cette description, les caractéristiques et fonctions bien connues de l'homme du métier ne sont pas décrites en détail.

[0019] Dans cette description, des exemples détaillés de mode de réalisation sont d'abord décrits dans un chapitre I en référence aux figures. Ensuite, dans un chapitre II, des variantes de ces modes de réalisation sont présentées. Enfin, les avantages des différents modes de réalisation sont présentés dans un chapitre III.

[0020] Chapitre I : Exemples de mode de réalisation détaillé

[0021] La [Fig.1] représente un système 2 de contrôle d'accès à des bâtiments équipés chacun d'au moins une porte d'accès. Pour simplifier la [Fig.1] seul un bâtiment 4 équipé d'une porte 6 d'accès est représenté. La porte 6 est équipée d'une serrure électronique 10.

[0022] La porte 6 est déplaçable entre une position ouverte et une position fermée. Dans la position fermée, elle interdit l'accès à l'intérieur du bâtiment 4. Dans la position ouverte, un visiteur ou un résident peut librement entrer à l'intérieur du bâtiment 4.

[0023] Pour contrôler les accès au bâtiment 4, le système 2 comporte en plus plusieurs terminaux mobiles d'ouverture. Seul un terminal mobile 16 est représenté sur la [Fig.1] .

[0024] Typiquement, le système 2 comporte plusieurs portes d'accès chacune équipée d'une serrure électronique pour contrôler les accès à plusieurs bâtiments ou à différentes parties d'un même bâtiment. Les différentes serrures électroniques et les différents terminaux mobiles fonctionnent alors comme décrit, respectivement, pour la serrure 10 et le terminal 16. Ainsi, par la suite, ces autres serrures électriques et ces autres terminaux mobiles ne sont pas décrits en détails et n'ont pas été représentés sur la [Fig.1].

[0025] Ici, la serrure 10 et le terminal 16 sont, par exemple, structurellement identiques, respectivement, à la serrure et à la clé électronique décrites dans la demande EP3431684. Ainsi, par la suite, seules les caractéristiques de la serrure 10 et du terminal 16 nécessaires pour comprendre l'invention sont décrites.

[0026] La serrure 10 se déplace, de façon réversible, entre un état verrouillé et un état déverrouillé. Dans l'état verrouillé, elle maintient la porte 6 dans sa position fermée. Dans l'état déverrouillé, la porte 6 peut librement être déplacée de sa position fermée vers sa position ouverte. La serrure 10 se déplace de son état verrouillé vers son état déverrouillé lorsqu'un terminal mobile autorisé à déverrouiller cette serrure 10 est présenté devant cette serrure 10.

[0027] Dans ce mode de réalisation, la serrure 10 est dépourvue de source d'alimentation interne et n'est pas raccordée à un réseau public d'alimentation électrique. La serrure 10 est alimentée par le terminal 16 lorsque celui-ci est présenté devant la serrure 10. La serrure 10 est également dépourvue d'émetteur-récepteur susceptible de lui permettre d'établir directement une liaison longue distance de transmissions d'informations avec un dispositif distant, comme un serveur de droits d'accès ou un poste d'administration. La serrure 10 est uniquement apte à communiquer avec le terminal 16 et un programmeur, tel que le programmeur 90 décrit plus loin, par l'intermédiaire d'une liaison courte distance. Dans ce texte, une liaison courte distance est une liaison de transmission d'informations qui peut s'établir entre deux dispositifs uniquement s'ils sont à moins de 10 m l'un de l'autre et, de préférence, à moins de 50 cm ou 10 cm l'un de l'autre.

[0028] Le terminal 16 est facilement transportable, à la main, par un être humain. Ici, le terminal 16 est une clé électronique pourvue d'une lame 38. Le terminal 16 comporte un microprocesseur 40, une mémoire non-volatile 42 et une batterie 44. Bien que le terminal 16 est ici la forme d'une clé mécanique, dans ce texte, le terme "terminal" est utilisé pour éviter toutes confusions avec les clés cryptographiques décrites plus loin.

[0029] La lame 38 est destinée à être insérée à l'intérieur de la serrure 10. Ainsi, dans ce cas, présenter le terminal 16 devant la serrure 10 consiste à introduire la lame 38 à l'intérieur de la serrure 10. Lorsque la lame 38 est introduite à l'intérieur de la serrure 10, cela établit des liaisons filaires entre le terminal 16 et la serrure 10. C'est par l'intermédiaire de ces liaisons filaires que le terminal 16 alimente la serrure 10 et échange des trames d'informations avec la serrure 10. Un exemple possible de mécanisme pour établir ces liaisons filaires est décrit en détail dans la demande EP3431684.

[0030] Le système 2 comporte aussi un serveur 50 de droit d'accès et un poste 60 d'administration pour gérer les autorisations d'accès aux différents bâtiments du système 2. Le serveur 50 et le poste 60 sont raccordés l'un à l'autre par l'intermédiaire d'un réseau 80 grande distance de transmission d'informations. Le réseau 80 est, par exemple, un réseau à commutation de paquets tel que le réseau Internet. Ici, ni la serrure 10 ni le terminal 16 n'est directement raccordé au réseau 80.

[0031] Le serveur 50 est capable de générer des autorisations d'accès à enregistrer dans la mémoire 42 et dans la serrure 10. Une autorisation d'accès contient l'ensemble des informations nécessaires à enregistrer dans un terminal mobile ou dans une serrure électronique pour que ce terminal puisse déverrouiller cette serrure électronique. Ainsi, en absence de cette autorisation d'accès, le terminal mobile ne peut pas déverrouiller la serrure électronique. A cet effet, le serveur 50 comporte un microprocesseur 52 et une mémoire 54. La mémoire 54 comporte les instructions et les données nécessaires pour

mettre en œuvre le procédé de la [Fig.7] lorsque ces instructions sont exécutées par le microprocesseur 52.

[0032] Le poste 60 d'administration permet à un utilisateur d'administrer les autorisations d'accès. A cet effet, il permet notamment, sous la commande de l'utilisateur, de déclencher la création, par le serveur 50, de nouvelles autorisations d'accès. Il permet aussi, toujours sous la commande de l'utilisateur, de commander le serveur 50 pour que celui génère des commandes d'invalidation d'autorisations d'accès précédemment générées. A cet effet, le poste 60 comporte, par exemple, une unité centrale 62 et une interface 64 homme-machine. A titre d'illustration, l'interface 64 comporte ici un écran 66 et un clavier 68.

[0033] L'unité centrale 62 comporte un microprocesseur 70 et une mémoire 72. La mémoire 72 comporte les instructions et les données nécessaires pour mettre en œuvre le procédé de la [Fig.7] lorsque ces instructions sont exécutées par le microprocesseur 70.

[0034] Dans ce mode de réalisation, le poste 60 est en plus utilisé pour programmer les autorisations d'accès dans les terminaux mobiles. A cet effet, le poste 60 est raccordé à un programmateur 90 de terminaux mobiles, par exemple, par l'intermédiaire d'une liaison filaire ou d'une liaison sans fil. Le programmateur 90 est capable d'écrire dans la mémoire 42 du terminal 16. Par exemple, pour cela, il établit une liaison courte distance avec le terminal 16 lorsque celui-ci est situé à proximité. Par exemple, le programmateur 90 comporte un orifice qui permet d'introduire la lame 38 à l'intérieur du programmateur 90 pour établir des liaisons filaires avec le terminal mobile 16. Le programmateur 90 est utilisé pour écrire dans la mémoire 42 des autorisations d'accès qui ont été générées par le serveur 50 puis transmises au poste 60.

[0035] Dans ce mode de réalisation, le programmeur 90 permet aussi d'écrire dans une mémoire de la serrure 10. Par exemple, à cet effet, le programmeur 90 comporte une lame, identique à la lame 38, qui peut être introduite à l'intérieur de la serrure 10 pour établir les liaisons filaires entre ce programmeur 90 et cette serrure 10. Dans ce cas, de préférence, le programmeur 90 est un dispositif portable qui peut facilement être transporté à la main par un être-humain. De plus, le programmeur 90 comporte une mémoire tampon 92 dans laquelle les autorisations d'accès à enregistrer dans une serrure électronique sont temporairement stockées. Ainsi, les autorisations d'accès peuvent être transférées du poste 60 vers cette mémoire tampon 92. Ensuite, le programmeur 90 est déconnecté du poste 60 et transporté jusqu'à la serrure 10. Sa lame est alors introduite à l'intérieur de la serrure 10 puis les autorisations d'accès stockées dans sa mémoire tampon 92 sont transférées dans la mémoire de la serrure 10.

[0036] La [Fig.2] représente plus en détail l'architecture de la serrure 10. La serrure 10 comporte un cylindre 100 conforme au format européen. Ce cylindre 100 est représenté de profil sur la [Fig.2]. Le cylindre 100 comporte un orifice 101 pour in-

troduire la lame 38 à l'intérieur de la serrure 10.

[0037] Un mécanisme commandable 102 de déverrouillage de la serrure est logé à l'intérieur de ce cylindre 100. Ce mécanisme 102 est apte à déplacer la serrure 10 depuis son état verrouillé vers son état déverrouillé. Par exemple, le mécanisme 102 est similaire à celui décrits dans la demande FR3025236 ou la demande EP3431684. Pour accroître la lisibilité de la [Fig.2], la représentation du mécanisme 102 a été simplifiée.

[0038] Le mécanisme 102 comporte typiquement un actionneur électrique et/ou magnétique commandable 104 et une unité électronique 106 de commande de cet actionneur 104.

[0039] L'actionneur 104 est apte à déplacer la serrure 10 dans son état déverrouillé en réponse à une commande de déverrouillage transmise par l'unité 106. En absence de commande de déverrouillage, l'actionneur 104 maintient la serrure 10 dans son état verrouillé.

[0040] L'unité 106 est apte :

- à échanger des trames d'informations avec le terminal mobile introduit à l'intérieur de la serrure 10, et
- lorsque le terminal mobile introduit dans la serrure est autorisé à déverrouiller la serrure 10, à transmettre à l'actionneur 104 la commande de déverrouillage qui déclenche le déplacement de la serrure 10 dans son état déverrouillé.

[0041] A cet effet, l'unité 106 comporte un microprocesseur 108 et une mémoire 110. La mémoire 110 contient les instructions nécessaires pour mettre en œuvre le procédé de la [Fig.7] lorsque ces instructions sont exécutées par le microprocesseur 108. La mémoire 110 contient aussi les données nécessaires pour la mise en œuvre du procédé de la [Fig.7]. En particulier, elle contient :

- une clé unique Caes de serrure,
- un identifiant Cpub de serrure,
- un indice Cindice de serrure,
- une constante Ct de dérivation de clés,
- une table 112 d'autorisation d'accès pour des terminaux mobiles autorisés à déverrouiller la serrure 10, et
- une liste 114 d'indices de terminaux.

[0042] La clé Caes est une clé de chiffrement unique dans le système 2. Autrement dit, aucune autre serrure électronique du système 2 ne contient la même clé Caes. La clé Caes est seulement connue de la serrure 10 et du serveur 50. Par exemple, ici, la clé Caes est enregistrée dans une zone non-réinscriptible de la mémoire 110. Cette zone non-réinscriptible est obtenue en rendant impossible l'écriture dans cette zone par des moyens logiciels et/ou par des moyens matériels. Ainsi, cette clé Caes ne peut pas être modifiée ou effacée.

[0043] L'identifiant Cpub est un identifiant qui permet d'identifier la serrure 10 parmi

l'ensemble des serrures électroniques du système 2. L'identifiant Cpub est lui aussi enregistré dans la zone non-réinscriptible de la mémoire 110.

[0044] L'indice Cindice est un indice qui a été programmé dans la serrure 10, par exemple, lors de sa mise en service. L'indice Cindice est enregistré dans une zone ré-inscriptible de la mémoire 110 de sorte qu'il peut être modifié ultérieurement après la première mise en service de la serrure 10.

[0045] La constante Ct est une constante dont la valeur est la même dans toutes les serrures électroniques du système 2.

[0046] La [Fig.3] représente plus en détail la table 112 d'autorisation d'accès. La table 112 comporte quatre colonnes 120, 122, 124 et 126 et de zéro à plusieurs lignes. Pour chaque ligne de la table 112, la colonne 120 contient un identifiant Kpub d'un terminal, la colonne 122 contient un cryptogramme KKpub, la colonne 124 contient un indice Cpr de priorité et la colonne 126 contient un code d'accès Ov. Les données situées sur une même ligne de cette table sont toutes associées à l'identifiant Kpub contenu dans la colonne 120 de cette ligne.

[0047] La [Fig.4] représente plus en détail la liste 114. La liste 114 comporte deux colonnes 130 et 132 et des lignes. Chaque ligne contient dans la colonne 130 un identifiant Kpub d'un terminal et, dans la colonne 132, un indice Kindice associé à cet identifiant Kpub.

[0048] Les différentes données contenues dans la table 112 et dans la liste 114 et leur utilisation sont décrites plus loin. La table 112 et la liste 114 sont enregistrées dans la zone ré-inscriptible de la mémoire 110.

[0049] La [Fig.5] représente plus en détail la mémoire 42 du terminal 16. La mémoire 42 contient :

- une clé unique Kaes de terminal,
- un identifiant Kpub de terminal,
- un indice Kindice de terminal,
- une constante Ct de dérivation de clés, et
- une table 140 d'autorisation d'accès pour des serrures électroniques que ce terminal est autorisé à déverrouiller.

[0050] La clé Kaes est une clé de chiffrement unique dans le système 2. Autrement dit, aucun autre terminal mobile du système 2 ne contient la même clé Kaes. La clé Kaes est seulement connue du terminal 16 et du serveur 50. Par exemple, ici, la clé Kaes est enregistrée dans une zone non-réinscriptible de la mémoire 42. Ainsi, cette clé Kaes ne peut pas être modifiée ou effacée.

[0051] L'identifiant Kpub est un identifiant qui permet d'identifier le terminal 16 parmi l'ensemble des terminaux mobiles du système 2. L'identifiant Kpub est enregistré dans la mémoire 42. Par exemple, l'identifiant Kpub est enregistré dans une zone de la mémoire 42 qui peut être écrite lorsque le terminal 16 est programmé pour la première

fois.

[0052] L'indice Kindice est un indice qui a été programmé dans le terminal 16, par exemple, lors de sa mise en service ou lors d'une mise à jour de ses autorisations d'accès. L'indice Kindice est enregistré dans une zone de la mémoire 42 qui peut être modifiée ultérieurement après la première mise en service du terminal 16.

[0053] La constante Ct enregistrée dans la mémoire 42 est la même dans tous les terminaux mobiles du système 2. Elle est égale à la constante Ct enregistrée dans toutes les serrures électroniques du système 2.

[0054] La [Fig.6] représente plus en détail la table 140 d'autorisation d'accès. La table 140 comporte quatre colonnes 142, 144, 146 et 148 et de zéro à plusieurs lignes. Pour chaque ligne de la table 140, la colonne 142 contient un identifiant Cpub de serrure, la colonne 144 contient un cryptogramme KCpub, la colonne 146 contient un indice Kpr de priorité et la colonne 148 contient un code d'accès Ov. Le code Ov peut prendre une première valeur et, en alternance, une seconde valeur différente. La première valeur indique que le terminal 16 est autorisé à déverrouiller la serrure 10. Les autres valeurs de ce code Ov indique que le terminal 16 n'est pas autorisé à déverrouiller la serrure 10. Les données situées sur une même ligne de cette table 140 sont toutes associées à l'identifiant Cpub contenu dans la colonne 142 de cette ligne.

[0055] Le fonctionnement du système 2 va maintenant être décrit en référence au procédé de la [Fig.7].

[0056] Initialement, lors d'une phase 148, le système 2 est installé. Cette phase 148 consiste notamment à fournir les différentes serrures électroniques qui sont utilisées dans le système 2 et à les installer sur des portes respectives. Lors de la phase 148, les terminaux mobiles qui sont utilisés dans le système 2 sont également fournis.

[0057] Ensuite, lors d'une phase 150, des autorisations d'accès sont programmées dans un ou plusieurs terminaux mobiles du système 2. Ici, cette phase 150 est décrite dans le cas particulier du terminal 16. Toutefois, ce qui est décrit dans ce cas particulier s'applique à tous terminaux mobiles du système 2.

[0058] Lors de la phase 150, par exemple, un administrateur, à l'aide du poste 60, identifie les serrures électroniques du système 2 que le terminal 16 peut déverrouiller. Ensuite, il déclenche la génération par le serveur 50 des autorisations d'accès à enregistrer dans la table 140 du terminal 16 pour chacune des serrures électroniques identifiées. La génération de ces autorisations d'accès est ici illustrée dans le cas particulier où le terminal 16 doit être autorisé à déverrouiller la serrure 10. Pour cela, le serveur 50 construit le cryptogramme KCpub en chiffrant les données suivantes à l'aide de la clé Caes de la serrure 10 :

- l'identifiant Kpub du terminal 16,
- l'indice Kindice du terminal 16,

– l'identifiant Cpub de la serrure 10, et
– l'indice Cindice de la serrure 10.

[0059] Autrement dit, le cryptogramme KCpub est construit à l'aide de la relation suivante : KCpub = CBC_MAC(Caes; Kpub; Kindice; Cpub; Cindice), où CBC_MAC() est une fonction de construction prédéterminée paramétrée par une clé de chiffrement et des données en clair. Le terme "données en clair" désigne des données qui sont directement utilisables sans nécessiter au préalable un déchiffrement. Par la suite, dans la liste des arguments de la fonction CBC_MAC(), la clé de chiffrement utilisée est placée en première position avant les données à chiffrer. Ici, cette fonction CBC_MAC() met seulement en œuvre un algorithme de chiffrement symétrique. Aucun algorithme de chiffrement asymétrique n'est utilisé. Par exemple, dans ce mode de réalisation, la fonction CBC_MAC() est une fonction de chiffrement symétrique tel que la fonction de chiffrement symétrique connue sous l'acronyme AES ("Advanced Encryption Standard").

[0060] Dans le cas de la construction du cryptogramme KCpub, la clé de chiffrement est la clé Caes et les données en clair sont les données Kpub, Kindice, Cpub, et Cindice. Le cryptogramme KCpub construit est donc spécifique au terminal 16 puisqu'il dépend de son identifiant Kpub et également spécifique à la serrure 10 puisqu'il dépend de la clé Caes et de l'identifiant Cpub. Le cryptogramme KCpub constitue donc une autorisation d'accès pour un terminal mobile particulier à une serrure électronique particulière. Dès lors, le serveur 50 construit un cryptogramme KCpub pour chaque serrure électronique qui doit être déverrouillée par le terminal 16.

[0061] A chaque fois qu'un nouveau cryptogramme KCpub est construit pour le même terminal mobile et pour la même serrure électronique, l'indice Kpr associé à ce terminal mobile et à cette serrure électronique est incrémenté, par exemple, de 1 par rapport à sa précédente valeur.

[0062] De plus, si le terminal 16 est programmé pour remplacer un précédent exemplaire d'un terminal 16 qui, par exemple, a été perdu :

- un identifiant Kpub identique à celui du terminal 16 perdu est enregistré dans sa mémoire 42 de sorte que les identifiants Kpub du terminal 16 programmé et du terminal 16 perdu sont identiques, et
- l'indice Kindice du terminal 16 programmé est incrémenté d'un pas prédéterminé, par exemple égal à 1, par rapport à l'indice Kindice du terminal 16 perdu.

[0063] Enfin, l'identifiant Cpub de la serrure 10, le cryptogramme KCpub construit par le serveur 50 pour la serrure 10, l'indice Kpr incrémenté et, éventuellement, l'indice Kindice incrémenté sont transmis au poste 60.

[0064] Lorsque le terminal 16 est raccordé au programmeur 90, le poste 60 transmet à son tour ces données au programmeur 90 qui les transmet au terminal 16. Le terminal 16

les enregistre dans une ligne de sa table 140. Si la table 140 contient déjà une ligne pour l'identifiant Cpub, les nouvelles données viennent remplacer les anciennes données contenues dans cette ligne dans les colonnes 144, 146 et 148. Dans le cas contraire, une nouvelle ligne est créée dans la table 140 pour y enregistrer les données reçues associée à l'identifiant Cpub. Si un indice Kindice incrémenté est aussi transmis au terminal 16, celui-ci remplace le précédent indice Kindice enregistré dans la mémoire 42.

[0065] Le terminal 16 ne comporte pas la clé Caes. Ainsi, les informations contenues dans la mémoire 42 sont insuffisantes à elles seules pour construire d'autres cryptogrammes KCpub susceptibles d'autoriser ce terminal 16 à déverrouiller d'autres serrures électroniques du système 2. Dès lors, même si les informations contenues dans la mémoire 42 sont compromises, cela ne remet pas en question la sécurité du système 2. En effet, il n'est pas possible de construire à partir de ces informations des autorisations d'accès pour déverrouiller d'autres serrures électroniques. De plus, le fait de simplement copier les informations contenues dans la table 140 du terminal 16 dans la mémoire 42 d'un autre terminal ne permet pas de simplement construire un double du terminal 16. En effet, l'identifiant Kpub de cet autre terminal est alors différent de l'identifiant Kpub du terminal 16, ce qui empêche de déverrouiller une serrure électronique en utilisant pour cela un cryptogramme KCpub spécifiquement construit pour le terminal 16.

[0066] La phase 150 peut être exécutée à tout moment et pas seulement au moment de la mise en service d'un nouveau terminal mobile.

[0067] En parallèle, une phase 160 de configuration d'autorisation d'accès dans une serrure électronique peut être exécutée. Cette phase 160 est par exemple exécutée s'il est plus simple de configurer une serrure électronique plutôt que de configurer chacun des terminaux mobiles qui doivent être autorisés à déverrouiller cette serrure électronique.

[0068] Ici, cette phase 160 est décrite dans le cas particulier où la serrure 10 doit être configurée pour être déplacée dans son état déverrouillé par le terminal 16.

[0069] Pour cela, l'utilisateur, à l'aide du poste 60, identifie le ou les terminaux mobiles du système 2 qui sont autorisés à déverrouiller la serrure 10. Ensuite, il déclenche la génération par le serveur 50 des autorisations d'accès nécessaires à enregistrer dans la table 112 de la serrure 10.

[0070] A cet effet, le serveur 50 construit un cryptogramme KKpub en chiffrant les données suivantes à l'aide de la clé Kaes du terminal 16 :

- l'identifiant Kpub du terminal 16,
- l'indice Kindice du terminal 16,
- l'identifiant Cpub de la serrure 10, et
- l'indice Cindice de la serrure 10.

[0071] Autrement dit, le cryptogramme KKpub est construit à l'aide de la relation suivante :

KKpub = CBC_MAC(Kaes; Kpub; Kindice; Cpub; Cindice), où CBC_MAC() est la même fonction que celle utilisée pour construire le cryptogramme KCpub.

[0072] Le cryptogramme KKpub ainsi construit est lui aussi spécifique au terminal 16 puisqu'il dépend de l'identifiant Kpub et de la clé Kaes et également spécifique à la serrure 10 puisqu'il dépend de l'identifiant Cpub. Le cryptogramme KKpub constitue donc une autorisation d'accès pour un terminal particulier à une serrure électronique particulière. Le serveur 50 construit donc un cryptogramme KKpub pour chaque terminal mobile qui doit être autorisé à déverrouiller la serrure 10.

[0073] A chaque fois qu'un nouveau cryptogramme KKpub est construit pour un terminal mobile particulier et pour la serrure 10, la précédente valeur de l'indice Cpr associé à ce terminal mobile et à cette serrure 10 est incrémenté du même pas que celui utilisé pour incrémenter l'indice Kpr.

[0074] L'identifiant Kpub du terminal 16, le cryptogramme KKpub construit et l'indice Cpr incrémenté sont transmis au poste 60 puis enregistrés dans la mémoire tampon 92 du programmeur 90. Le programmeur 90 est alors déconnecté du poste 60 et transporté jusqu'à la serrure 10. Sa lame est alors introduite dans la serrure 10 et les données stockées dans sa mémoire tampon 92 sont enregistrées dans la table 112 de la serrure 10. De façon similaire à ce qui a déjà été décrit pour l'enregistrement de données dans la table 140 :

- si l'identifiant Cpub est déjà contenu dans la table 112, les données transférées sont utilisées pour mettre à jour le contenu des colonnes 122, 124 et 126 déjà associées à cet identifiant Cpub, et
- sinon, une nouvelle lignée est créée dans la table 112 et les données transférées y sont enregistrées.

[0075] La clé Kaes n'est pas contenue dans la serrure 10. Ainsi, les informations contenues dans la serrure 10 ne permettent pas à elles seules de construire un cryptogramme KKpub. Dès lors, si les données contenues dans une serrure électronique sont compromises, cela ne permet pas la construction de nouvelles autorisations d'accès pour autoriser d'autres terminaux mobiles à déverrouiller la serrure 10.

[0076] Alternativement, l'identifiant Kpub du terminal 16, le cryptogramme KKpub construit et l'indice Cpr incrémenté sont transmis du poste 60 vers le programmeur 90, puis du programmeur 90 vers un autre terminal mobile que le terminal 16. Cet autre terminal mobile enregistre ces autorisations d'accès pour le terminal 16 dans sa mémoire 42. Ensuite, lorsque cet autre terminal mobile est introduit dans la serrure 10, il transmet à la serrure 10 les autorisations d'accès pour le terminal 16 et, en réponse, la serrure 10 les enregistre dans sa table 112 comme précédemment décrit. Ainsi, dans ce dernier cas, ce n'est pas le programmeur 90 qui est utilisé pour transporter les autorisations d'accès du terminal 16 jusqu'à la serrure 10 mais un autre terminal mobile du

système 2.

[0077] Lors de la phase 160, il est possible de générer une commande d'invalidation générique de tous les terminaux mobiles précédemment autorisés à déverrouiller la serrure 10. Cette commande d'invalidation générique est transmise à la serrure 10 selon les mêmes chemins possibles que ceux décrits ci-dessus pour la transmission des autorisations d'accès à la serrure 10. Lorsque cette commande d'invalidation générique est reçue par la serrure 10, en réponse, la serrure 10 incrémente d'un pas prédéterminé son indice Cindice contenu dans sa mémoire 110. En parallèle, les autorisations d'accès enregistrées dans les terminaux mobiles pour déverrouiller la serrure 10 ne sont pas modifiées. Comme expliqué plus loin, l'incrémentation de l'indice Cindice dans la serrure 10 provoque alors l'invalidation de tous les terminaux mobiles précédemment programmés pour déverrouiller cette serrure 10.

[0078] La phase 160 peut être exécutée à tout moment et pas seulement au moment de la mise en service d'une serrure électronique.

[0079] Après avoir exécuté au moins l'une des phases 150 et 160, une phase 170 de contrôle d'accès est exécutée. Ici, la phase 170 est décrite dans le cas particulier où, au préalable :

- la phase 150 a été exécutée pour autoriser le terminal 16 à déverrouiller la serrure 10, et
- la phase 160 a été exécutée pour autoriser le terminal 16 à déverrouiller la serrure 10.

Ainsi, le terminal 16 comporte des autorisations d'accès pour déverrouiller la serrure 10 et la serrure 10 comporte aussi des autorisations d'accès pour être déverrouillée par le terminal 16.

[0080] Lorsqu'un résident souhaite ouvrir la porte 6, lors d'une étape 172, il introduit la lame 38 du terminal 16 à l'intérieur de l'orifice 101 de la serrure 10. Les liaisons filaires entre le terminal 16 et la serrure 10 sont alors établies et le terminal 16 alimente la serrure 10 et son microprocesseur 108. En réponse à l'alimentation de la serrure 10, lors d'une étape 174, le microprocesseur 108 génère une valeur, appelée par la suite « nonce », qui varie à chaque fois que l'étape 174 est exécutée. Par exemple, cette valeur est générée par tirage aléatoire ou pseudo-aléatoire.

[0081] Ensuite, lors d'une étape 176, le microprocesseur 108 transmet une trame d'informations, appelée ici trame T_{ini}, au terminal 16 par l'intermédiaire des liaisons filaires établies.

[0082] La trame T_{ini} comporte notamment les données suivantes en clair :

- l'identifiant Cpub et l'indice Cindice enregistrés dans la mémoire 110 de la serrure 10, et
- le nonce généré lors de l'étape 174.

[0083] En réponse à la réception de la trame T_{ini}, lors d'une étape 178, le microprocesseur 40 du terminal 16 recherche dans la table 140 enregistrée dans sa mémoire 42 si celle-ci comporte un cryptogramme KCpub associé à l'identifiant Cpub contenu dans la trame T_{ini} reçue.

[0084] Dans l'affirmative, le microprocesseur 40 procède à une étape 180 de construction et de transmission d'une trame T_{180} ([Fig.8]). Dans la négative, le microprocesseur 40 procède à une étape 182 de construction et de transmission d'une trame T_{182} ([Fig.9]).

[0085] La trame T_{180} comporte des données D_{180} en clair, éventuellement des autorisations d'accès A_{180} pour d'autres terminaux mobiles et une signature numérique S_{180}.

[0086] Les données D_{180} comportent :

- l'identifiant Kpub et l'indice Kindice contenus dans la mémoire 42 du terminal 16,
- l'indice Kpr et le code d'accès Ov associés à l'identifiant Cpub trouvé dans la table 140.

[0087] Les autorisations A_{180} correspondent à des autorisations d'accès destinées à être enregistrées dans la table 112 de la serrure 10 pour autoriser d'autres terminaux mobiles que le terminal 16 à déverrouiller cette serrure 10. Ces autorisations d'accès A_{180} sont enregistrées dans le terminal 16 lors de la phase 160 comme décrit précédemment. Si le terminal 16 ne comporte aucune autorisation d'accès A_{180} destinée à la serrure 10, la trame T_{180} est alors dépourvue de telles autorisations d'accès A_{180}. Ainsi, par la suite, toutes les opérations de traitement des autorisations d'accès A_{180} sont réalisées uniquement si le terminal 16 comporte des autorisations d'accès à enregistrer dans la table 112 de la serrure 10. Dans le cas contraire, les traitements des autorisations A_{180} sont omis.

[0088] La signature S_{180} permet de vérifier l'intégrité et l'authenticité, notamment des données D_{180} et des autorisations d'accès A_{180} contenues dans la trame T_{180}. Ici, « vérifier l'intégrité » signifie vérifier que les données et les autorisations d'accès contenues dans une trame n'ont pas été modifiées depuis l'émission de cette trame par un terminal mobile. « Vérifier l'authenticité » signifie vérifier qu'une trame a bien été générée et transmise par le terminal mobile qui prétend avoir transmis cette trame d'informations. La signature S_{180} est construite à partir des données D_{180}, des autorisations A_{180} et du nonce échangé lors de l'étape 176.

[0089] La trame T_{182} ([Fig.9]) comporte elle aussi des données D_{182} en clair et une signature numérique S'_{182}. Les données D_{182} comportent ici notamment l'identifiant Kpub du terminal mobile qui émet la trame T_{182}.

[0090] La signature S'_{182} est construite à partir de l'identifiant Kpub contenu dans la mémoire 42 du terminal mobile et du nonce échangé lors de l'étape 176.

[0091] L'étape 180 débute par une opération 184 de dérivation d'une clé KCpub1 à partir du cryptogramme KCpub trouvé dans la table 140. Pour cela, le microprocesseur 108

exécute une fonction prédéterminée AES_CBC() de dérivation de clé. Par exemple, dans ce mode de relation, la fonction à AES_CBC() met seulement en œuvre un algorithme de chiffrement symétrique tel que l'algorithme connu sous l'acronyme à AES (« Advanced Encryption System »). Par exemple, ici, la clé KCpub1 est le résultat du chiffrement de la constante Ct préenregistrée dans la mémoire 42 en mettant en œuvre la fonction AES_CBC() et en utilisant le cryptogramme KCpub comme clé de chiffrement. Ainsi, la clé KCpub1 est obtenue à l'aide de la relation suivante : KCpub1 = AES_CBC(KCpub ; Ct).

[0092] La fonction AES_CBC() exécutée est toujours la même à chaque exécution de l'opération 184. Ainsi, la clé KCpub1 dérivée du cryptogramme KCpub est toujours la même lors de chaque exécution de la phase 170 entre le terminal 16 et la serrure 10 tant que le cryptogramme KCpub trouvé dans la table 140 est le même.

[0093] Ensuite, lors d'une opération 186, le microprocesseur 40 génère la trame T_{180}. Pour cela, le microprocesseur 40 construit la signature S_{180} en utilisant les données D_{180}, les autorisations d'accès A_{180} à transmettre à la serrure 10 et le nonce échangé lors de l'étape 176. Pour obtenir cette signature, une fonction de construction prédéterminée paramétrée par la clé KCpub1 est mise en œuvre. Cette fonction prédéterminée fait intervenir des opérations de chiffrement symétrique et aucune opération de chiffrement asymétrique. Ici, cette fonction de construction est la même fonction CBC_MAC() que celle utilisée pour construire les cryptogrammes KCpub et KKpub. Ainsi, ici, la signature S_{180} est obtenue à l'aide de la relation suivante : S_{180} = CBC_MAC(KCpub1 ; Kpub ; Kindice ; Kpr ; Ov ; A_{180}; nonce) où :

- KCpub1 est la clé de chiffrement dérivée lors de l'opération 184,
- Kpub, Kindice, Kpr, Ov sont les données D_{180} associées dans la table 140 à l'indice Cpub trouvé,
- le nonce est celui échangé lors de l'étape 176.

[0094] Ensuite, la signature S_{180} ainsi obtenue est concaténée aux données D_{180} en clair et aux autorisations d'accès A_{180} pour former la trame T_{180}.

[0095] Lors d'une opération 188, la trame T_{180} ainsi générée est transmise à la serrure 10 par l'intermédiaire des liaisons filaires établies. L'étape 180 est alors terminée.

[0096] En réponse à la réception de la trame T_{180}, lors d'une étape 190, le microprocesseur 108 de la serrure 10 recherche dans sa table 112 si celle-ci comporte une ligne associée à l'identifiant Kpub contenu dans les données D_{180} de la trame T_{180}.

[0097] Dans la négative, le microprocesseur 108 procède directement à une étape 192 de vérification de l'intégrité et de l'authenticité de la trame T_{180} reçue.

[0098] Dans le cas contraire, lors d'une étape 194, le microprocesseur 108 compare l'indice Kpr contenu dans les données D_{180} reçues à l'indice Cpr associé par la table 112 à l'identifiant Kpub reçu.

[0099] Si l'indice Kpr reçu est supérieur ou égal à l'indice Cpr, le procédé se poursuit directement par l'étape 192. A l'inverse, si l'indice Kpr reçu est strictement inférieur à l'indice Cpr enregistré dans la table 112, lors d'une étape 196, le microprocesseur 108 transmet une trame T_{196} au terminal 16. En réponse à la réception de cette trame T_{196}, le microprocesseur 40 du terminal 16 exécute l'étape 182 pour construire et transmettre la trame T_{182}.

[0100] Lors de l'étape 192, le microprocesseur 108 vérifie que l'autorisation d'accès enregistrée dans la table 140 pour la serrure 10 est une autorisation d'accès valide. Ici, pour cela, il vérifie l'intégrité et l'authenticité de la trame T_{180} reçue.

[0101] Plus précisément, le microprocesseur 108 commence par construire un cryptogramme KCpub' à l'aide de la relation suivante : KCpub' = CBC_MAC(Caes ; Kpub ; Kindice ; Cpub ; Cindice), où :

- CBC_MAC() est la même fonction de construction que celle mise en œuvre par le serveur 50 lors de la phase 150 pour construire le cryptogramme KCpub,
- Caes est la clé unique de chiffrement enregistrée dans la mémoire 110 de la serrure 10,
- Kpub et Kindice sont respectivement l'identifiant de terminal et l'indice de terminal contenus dans la trame T_{180} reçue,
- Cpub et Cindice sont, respectivement, l'identifiant de serrure et l'indice de serrure contenus dans la mémoire 110 de la serrure 10.

[0102] Ensuite, le microprocesseur 108 vérifie que le cryptogramme KCpub' construit est identique au cryptogramme KCpub utilisé pour construire la signature S_{180} reçue. Pour cela, ici, le microprocesseur 108 dérive une clé KCpub1' à partir du cryptogramme KCpub'. La clé KCpub1' est calculée à l'aide de la relation suivante : KCpub1' = AES_CBC(KCpub' ; Ct), où :

- AES_CBC() est la même fonction de dérivation de clé que celle mise en œuvre lors de l'opération 184,
- KCpub' est le cryptogramme qui vient d'être construit par le microprocesseur 108, et
- Ct est la constante enregistrée dans la mémoire 110.

[0103] Ensuite, le microprocesseur 108 construit une signature S'_{180} calculée à l'aide de la relation suivante : S'_{180} = CBC_MAC(KCpub1' ; Kpub ; Kindice ; Kpr ; Ov ; A_{180} ; nonce), où :

- CBC_MAC() est la même fonction de construction que celle mise en œuvre lors de l'opération 186,
- KCpub1' est la clé précédemment dérivée du cryptogramme KCpub',
- Kpub, Kindice, Kpr et Ov proviennent des données D_{180} contenues dans la trame T_{180} reçue,

- A_{180} sont les autorisations d'accès contenues dans la trame T_{180} si celle-ci en contient, et
- "nonce" est le nonce transmis par la serrure 10 au terminal 16 lors de l'étape 176.

[0104] Enfin, le microprocesseur 108 compare la signature S'_{180} obtenue à la signature S_{180} contenue dans la trame T_{180} reçue. Si ces deux signatures S'_{180} et S_{180} sont égales, cela signifie que les cryptogrammes KCpub et KCpub' sont égaux et donc que les identifiants Kpub, Cpub, Kindice et Cindice utilisés pour les construire sont identiques. De plus, dans ce cas, l'intégrité et l'authenticité de la trame T_{180} est confirmée. Lorsque l'intégrité et l'authenticité de la trame T_{180} est confirmée, le procédé se poursuit par une étape 198 lors de laquelle les autorisations d'accès A_{180} sont enregistrées dans la table 112. Si la trame T_{180} ne comporte aucune autorisation d'accès A_{180}, l'étape 198 est omise.

[0105] Ensuite, lors d'une étape 200, le microprocesseur 108 compare l'indice Kindice contenu dans la trame T_{180} à l'indice Kindice enregistré dans la liste 114 et associé à l'identifiant Kpub contenu dans la trame T_{180}.

[0106] Si l'indice Kindice contenu dans la trame T_{180} est supérieur à l'indice Kindice contenu dans la liste 114, lors d'une étape 202, le microprocesseur 108 remplace l'indice Kindice associé à l'identifiant Kpub dans la liste 114 par l'indice Kindice contenu dans la trame T_{180}.

[0107] S'il n'existe aucun indice Kindice associé à l'identifiant Kpub reçu dans la table 114, le microprocesseur 108 ajoute, lors de l'étape 202, une ligne dans la table 114. La ligne ajoutée contient l'identifiant Kpub reçu dans la colonne 130 et l'indice Kindice reçu dans la colonne 132.

[0108] Après l'étape 202, le microprocesseur 108 procède à une étape 204 lors de laquelle il teste la valeur du code Ov contenu dans la trame T_{180}.

[0109] Si la valeur du code Ov reçue est égale à la première valeur, alors, lors d'une étape 206, le microprocesseur 108 génère la commande de déverrouillage et la transmet à l'actionneur 104.

[0110] En réponse, lors d'une étape 208, l'actionneur 104 déplace la serrure 10 dans son état déverrouillé et la porte 6 peut être ouverte.

[0111] Si l'indice Kindice reçu est égal à l'indice Kindice associé à l'identifiant Kpub reçu dans la table 114, alors le procédé se poursuit directement à l'étape 204 sans exécuter l'étape 202.

[0112] Si lors de l'étape 192, l'intégrité et l'authenticité de la trame T_{180} n'est pas confirmée ou si l'indice Kindice reçu est inférieur à l'indice Kindice contenu dans la table 114 ou si lors de l'étape 204, le microprocesseur 108 détermine que la valeur du code Ov est différente de la première valeur, alors l'exécution des étapes 206 et 208 est inhibée et la serrure 10 reste dans son état verrouillé.

[0113] Il est souligné que l'intégrité et l'authenticité de la trame T_{180} ne peut être confirmée que si le cryptogramme KCpub utilisé par le terminal 16 pour construire la signature S_{180} est bien celui correspondant à ce terminal 16 et à la serrure 10. En effet, ce cryptogramme KCpub dépend de l'identifiant Kpub et de la clé unique Caes. Ainsi, il ne peut pas être utilisé par un autre terminal mobile que le terminal 16 pour déverrouiller une serrure électronique. Il ne peut pas non plus être utilisé pour déverrouiller une autre serrure électronique que la serrure 10.

[0114] L'intégrité et l'authenticité de la trame T_{180} est confirmée uniquement si l'indice Cindice utilisé pour construire le cryptogramme KCpub est égal à l'indice Cindice enregistré dans la serrure 10. Ainsi, le fait d'incrémenter l'indice Cindice contenu dans la mémoire 110 de la serrure 10, par exemple à l'aide du programmateur 90, permet en une seule opération d'invalider tous les terminaux mobiles qui précédemment étaient autorisés à déverrouiller cette serrure.

[0115] Pour autoriser un nouveau terminal mobile à déverrouiller la serrure 10, il suffit de programmer ce nouveau terminal mobile comme décrit lors de la phase 150. Il n'est pas nécessaire pour cela de programmer aussi la serrure 10.

[0116] Dans ce mode de relation, aucun algorithme de chiffrement asymétrique n'est mis en œuvre pour vérifier l'intégrité et l'authenticité de la trame T_{180}. Cela limite la consommation d'énergie nécessaire pour faire cela.

[0117] L'étape 182 débute par une opération 220 de construction d'un cryptogramme KKpub' par le microprocesseur 42 du terminal 16. Ce cryptogramme KKpub' est construit en mettant en œuvre la relation suivante : KKpub' = CBC_MAC(Kaes ; Kpub ; Kindice ; Cpub ; Cindice), où :

- Kaes, Kpub et Kindice sont, respectivement, la clé unique Kaes, l'identifiant Kpub et l'indice Kindice enregistrés dans la mémoire 42 du terminal 16, et
- Cpub et Cindice sont, respectivement, l'identifiant de serrure et l'indice de serrure contenus dans la trame T_{ini}.

[0118] Ensuite, lors d'une opération 222, le microprocesseur 40 dérive une clé KKpub1' à partir du cryptogramme KKpub' construit lors de l'opération 220. Pour cela, une fonction prédéterminée de dérivation de clé est exécutée. Ici, la clé KKpub1' est obtenue à l'aide de la relation suivante : KKpub1' = AES_CBC(KKpub' ; Ct), où :

- AES_CBC() est la même fonction de dérivation que celle utilisée lors de la phase 160, et
- Ct est la constante enregistrée dans la mémoire 42.

[0119] Lors d'une opération 224, le microprocesseur 40 génère la trame T_{182}. Pour cela, le microprocesseur 40 construit la signature S'_{182} à partir des données D_{182}, du nonce échangé lors de l'étape 176 et en mettant en œuvre la fonction CBC_MAC() paramétrée par la clé KKpub1'. La signature S'_{182} est donc construite en mettant en œuvre

la relation suivante : S'_{182} = CBC_MAC(KKpub1' ; Kpub ; nonce).

[0120] Ensuite, la signature S'_{182} construite est concaténée aux données D_{182} pour former la trame T_{182}.

[0121] Lors d'une opération 226, la trame T_{182} construite est transmise à la serrure 10 par l'intermédiaire des liaisons filaires établies.

[0122] En réponse à la réception de la trame T_{182}, lors d'une étape 230, le microprocesseur 108 recherche dans la table 112 si celle-ci comporte une ligne associée à l'identifiant Kpub contenu dans les données D_{182} de la trame T_{182}. Dans la négative, l'exécution des étapes 206 et 208 est inhibée et la serrure 10 reste dans son état verrouillé.

[0123] Si une ligne de la table 112 contient le même identifiant Kpub que celui reçu, le microprocesseur 108 procède à une étape 232 de vérification de l'intégrité et de l'authenticité de la trame T_{182} reçue.

[0124] Lors de l'étape 232, le microprocesseur 108 sélectionne dans la table 112 le cryptogramme KKpub associé à l'identifiant Kpub reçu. Ensuite, le microprocesseur 108 dérive une clé KKpub1 à partir du cryptogramme KKpub sélectionné. Pour cela, la relation suivante est mise en œuvre : KKpub1 = AES_CBC(KKpub ; Ct), où :

- AES_CBC() est la même fonction de dérivation de clé que celle mise en œuvre lors de l'opération 222,
- KKpub est le cryptogramme associé à l'identifiant Kpub reçu dans la table 112,
- Ct est la constante enregistrée dans sa mémoire 110.

[0125] Le microprocesseur 108 construit alors une signature S_{182} en mettant en œuvre la relation suivante : S_{182} = CBC_MAC(KKpub1 ; Kpub ; nonce), où :

- CBC_MAC() est la même fonction de construction que celle mise en œuvre lors de l'opération 224,
- Kpub est l'identifiant Kpub contenu dans la trame T_{182}, et
- "nonce" est le nonce échangé lors de l'étape 176.

[0126] Enfin, le microprocesseur 108 compare la signature S_{182} obtenue à la signature S'_{182} contenue dans la trame T_{182} reçue. Si les deux signatures S_{182} et S'_{182} sont égales, l'intégrité et l'authenticité de la trame T_{182} est confirmée.

[0127] Dans ce cas, le procédé se poursuit par une étape 234 de test de la valeur du code Ov associé à l'identifiant Kpub reçu dans la table 112.

[0128] Si la valeur du code Ov lu dans la table 112 est égale à la première valeur, alors le procédé se poursuit par l'exécution des étapes 206 et 208 pour déplacer la serrure 10 dans son état déverrouillé.

[0129] Si lors de l'étape 232, l'intégrité et l'authenticité de la signature S_{182} n'est pas confirmée ou si la valeur du code Ov associé à l'identifiant Kpub reçu est différente de la première valeur, l'exécution des étapes 206 et 208 est inhibée. Ainsi, le code Ov permet d'invalider un terminal spécifique sans avoir besoin de reprogrammer ce

terminal spécifique ou d'incrémenter l'indice Cindice de cette serrure.

[0130] Ainsi, dans ce mode de réalisation, si un terminal mobile ne comporte pas d'autorisation d'accès pour déverrouiller la serrure 10 mais que cette serrure 10 comporte dans sa table 112 une autorisation d'accès pour ce terminal mobile, la serrure 10 est déplacée dans son état déverrouillé. Ainsi, le système 2 permet aussi d'utiliser des terminaux mobiles qui n'ont pas été programmés à l'avance pour ouvrir une serrure électronique particulière.

[0131] L'utilisation des indices Kpr et Cpr permet de plus de garantir que lorsqu'un terminal mobile et une serrure électronique comportent tous les deux des autorisations d'accès l'un pour l'autre, seules l'autorisation d'accès la plus récente est systématiquement utilisée.

[0132] Chapitre II : Variantes :

[0133] Variantes du système de contrôle d'accès :

[0134] La porte 6 n'est pas nécessairement une porte d'entrée d'un bâtiment. Il peut aussi s'agir d'une porte d'accès à un local situé à l'intérieur du bâtiment comme, par exemple, un garage ou un local à ordures.

[0135] Ici, le serveur 50 a été décrit comme étant une seule entité. Toutefois, le serveur 50 peut, en réalité, être formé d'un ou plusieurs serveurs redondants ou de plusieurs serveurs interconnectés remplissant chacun une fonction spécifique pour gérer les autorisations d'accès.

[0136] Le poste 60 d'administration peut être réalisé différemment. Par exemple, dans un autre mode de réalisation, le poste 60 est un téléphone intelligent, plus connu sous le terme de "smartphone", qui exécute un module d'administration du système 2. Dans ce cas, l'interface homme-machine est typiquement un écran tactile.

[0137] Les fonctions d'administration du système 2 et de programmation des terminaux mobiles peuvent être réparties sur deux machines différentes, l'une d'elle étant alors dédiée à l'administration du système 2 et l'autre étant dédiée à la programmation des terminaux mobiles. La machine dédiée à l'administration du système 2 n'est alors pas raccordée au programmateur 90.

[0138] En variante, la serrure électronique est alimentée et c'est le terminal mobile qui est dépourvu de source d'alimentation. Par exemple, la serrure électronique comporte une batterie ou est raccordée à un réseau d'alimentation électrique. Dans ce cas, c'est la serrure électronique qui alimente le terminal mobile lorsque celui-ci est présenté devant cette serrure électronique. Dans un autre mode de réalisation, le terminal mobile ou la serrure électronique est équipée d'un mécanisme qui transforme le déplacement mécanique du terminal mobile à l'intérieur de la serrure électronique en énergie électrique. Par exemple, un tel mécanisme de récupération d'énergie est décrit dans la demande EP2765264.

[0139] La serrure électronique peut être réalisée en deux parties mécaniquement distinctes l'une de l'autre, à savoir un mécanisme de déverrouillage et l'unité 106 de commande. Le mécanisme de déverrouillage comporte l'actionneur 104. Dans ce cas, l'unité 106 de commande est reliée à l'actionneur 104 par une liaison filaire. L'unité 106 est par exemple identique à celle précédemment décrite sauf qu'elle est logée à l'extérieur du cylindre 100. Par exemple, l'unité 106 est logée à l'intérieur d'une centrale d'accès située à proximité de la porte. Une telle centrale d'accès comporte typiquement à minima une tête de lecture apte à établir une liaison courte distance de transmission d'informations avec les terminaux mobiles. Dans ce cas, par exemple, chaque terminal mobile comporte une étiquette RFID (« Radio Frequency Identification ») apte à établir cette liaison courte distance.

[0140] En variante, le programmeur 90 permet seulement de programmer un terminal mobile et non pas une serrure électronique. Dans ce cas, les autorisations d'accès à enregistrer dans la table 112 sont systématiquement transportées jusqu'à la serrure 10 en utilisant des terminaux mobiles comme décrit précédemment lors de la phase 160. Alternativement ou en plus, un autre programmeur spécifique pour la programmation des serrures électroniques est utilisé lorsqu'il faut programmer directement une serrure électronique. Dans le cas où le programmeur 90 permet uniquement de programmer un terminal mobile, la lame de ce programmeur 90 peut être omise.

[0141] La liaison courte distance entre le programmeur 90 et le terminal 16 n'est pas nécessairement une liaison filaire. En variante, elle est remplacée par une liaison courte distance sans fil.

[0142] D'autres modes de réalisation des terminaux mobiles sont possibles. Par exemple, les liaisons filaires entre le terminal mobile et la serrure électronique utilisées pour transmettre les trames d'informations peuvent être remplacées par une liaison courte distance de transmission sans fil. Par exemple, cette liaison courte distance est une liaison conforme à la norme Bluetooth ou utilisant une communication en champ proche plus connue sous l'acronyme NFC ("Near Field Communication").

[0143] Le terminal mobile peut aussi être un téléphone mobile équipé du microprocesseur 40 et de la mémoire 42. Dans ce cas, la mémoire 42 est de préférence uniquement accessible à partir du microprocesseur 40. Généralement, le téléphone mobile est dépourvu de lame 38 et la liaison de transmission d'informations entre le téléphone mobile et la serrure électronique est une liaison sans fil comme décrit dans le paragraphe précédent.

[0144] Dans cette demande, les mémoires du terminal 16 et de la serrure 10 ont été représentées sous la forme d'un seul bloc de mémoire pour simplifier la description. Toutefois, en pratique, ces mémoires peuvent être chacune composées de plusieurs blocs de mémoire distincts.

[0145] Variantes du procédé :

[0146] Le nonce peut être généré par d'autre méthode qu'un tirage aléatoire ou pseudo-aléatoire. Par exemple, lors de chaque exécution de l'étape 174, le nonce est simplement incrémenté d'un pas prédéterminé, par exemple, à partir d'une combinaison de paramètres variables de la serrure 10.

[0147] La sélection du cryptogramme KCpub à partir de l'identifiant Cpub reçu peut être réalisée différemment. Par exemple, le terminal 16 sélectionne le premier cryptogramme KCpub contenu dans la table 140, puis les étapes 180, 190 et 192 sont exécutées. Si cela ne permet pas de déverrouiller la serrure 10, alors ces étapes sont réitérées mais en utilisant cette fois-ci le programme KCpub enregistré dans la ligne suivante de la table 140. En réitérant ces opérations, il est possible de retrouver le cryptogramme KCpub qui permet de déverrouiller la serrure 10 sans au préalable avoir à recevoir l'identifiant Kpub de cette serrure électronique. Si aucun cryptogramme KCpub contenu dans la table 140 ne permet de déverrouiller la serrure électronique, alors l'étape 194 est exécutée. Une telle variante est plus particulièrement adaptée au cas des systèmes de contrôle d'accès dans lequel le nombre de serrures électroniques est faible, c'est-à-dire inférieur à quatre ou cinq ou égal à une. Dans cette variante, il n'est pas nécessaire que la serrure électronique transmettre son identifiant Cpub au terminal mobile dans la trame T_{ini}.

[0148] La même méthode de sélection d'un cryptogramme que celle décrite au paragraphe précédent peut aussi être mise en œuvre pour sélectionner le cryptogramme KKpub dans la table 112 de la serrure électronique sans pour cela avoir reçu au préalable l'identifiant Kpub du terminal. Dans ce cas, la transmission de l'identifiant Kpub à la serrure électronique peut être omise.

[0149] L'étape 200 peut être omise dans tous les modes de réalisation où le cryptogramme KCpub est construit en fonction de l'indice Kindice. En effet, dans ce cas, si l'indice Kindice contenu dans le terminal 16 est différent de celui contenu dans la liste 114 de la serrure 10, alors les cryptogrammes KCpub et KCpub' sont différents et l'étape 192 échoue. La serrure 10 reste donc systématiquement dans son état verrouillé.

[0150] L'étape 202 peut être réalisée différemment. Par exemple, au lieu de remplacer l'ancien indice Kindice par l'indice Kindice incrémenté reçu, le microprocesseur 108 ajoute une nouvelle ligne dans la liste 114 et y enregistre l'indice Kindice incrémenté associé à l'identifiant Kpub. La ligne de la liste 114 qui contient l'ancien indice Kindice n'est pas supprimée. Dans ce cas, lors de l'étape 200, le microprocesseur 108 compare l'indice Kindice contenu dans la trame T_{180} à l'indice Kindice le plus élevé enregistré dans la liste 114 et associé à l'identifiant Kpub contenu dans la trame T_{180}.

[0151] Variantes des trames d'informations :

[0152] Le nonce peut en variante être généré dans la clé. Dans ce cas, la trame T_{ini} ne

comporte pas le nonce. Par contre, le nonce est incorporé dans les données D_{180} et D_{182} en clair des trames, respectivement, T_{180} et T_{182}. Toutefois, ce mode de réalisation est moins avantageux que celui décrit dans le chapitre I. En effet, dans ce cas, une attaque par rejeu est possible en enregistrant puis rejouant la trame T_{180} ou T_{182} générée par un terminal valide.

[0153] Dans un autre mode de réalisation, le code d'accès Ov n'est pas utilisé. Il peut donc être omis dans la trame T_{180} et dans les tables 112 et 140. Dans ce cas, l'étape 204 de test de la valeur de ce code Ov est omise et, à l'issue de l'étape 200 ou 202, le procédé se poursuit systématiquement par les étapes 206 et 208. Ainsi, dès que l'intégrité et l'authenticité de la trame T_{180} est confirmée et que l'indice Kindice reçu est supérieur ou égale à celui mémorisé dans la liste 114, la serrure électronique se déplace systématiquement dans son état déverrouillé. Dans ce cas, l'étape 234 peut aussi être omise. Dans une autre variante, le code Ov est omis seulement dans la table 112 des serrures ou seulement dans la table 140 des terminaux. Ainsi, l'une ou l'autre des étapes 204 et 234 peut être conservée.

[0154] La signature S_{180} peut être construite en prenant en compte d'autres données que celles précédemment décrites ou au contraire en prenant en compte moins de données que celles précédemment décrites. Par exemple, les données D_{180} peuvent comporter des informations supplémentaires comme, par exemple, des en-têtes de trame d'informations. Les données D_{180} peuvent aussi comporter une date et une heure courante. La date et l'heure courante sont par exemple utilisées pour autoriser le déverrouillage de la serrure 10 à l'aide du terminal 16 uniquement dans certaines plages horaires et uniquement pour certains jours préenregistrés dans la serrure 10.

[0155] Dans un autre mode de réalisation simplifié, l'indice Kindice n'est pas utilisé et peut donc être omis. Dans ce cas, la liste 114 est elle aussi omise. Dans ce mode de réalisation simplifié, il n'est alors pas possible d'invalider un terminal mobile simplement en introduisant dans la serrure électronique un nouveau terminal mobile ayant le même identifiant Kpub et un indice Kindice incrémenté. L'invalidation d'un terminal mobile est alors typiquement mise en œuvre différemment sans utiliser d'indice Kindice. Par exemple, l'invalidation des terminaux mobiles est gérée à l'aide d'une liste noire enregistrée dans la mémoire 110 et contenant les identifiants Kpub de tous les terminaux mobiles qui ne sont plus autorisés à déverrouiller cette serrure électronique. L'invalidation des terminaux mobiles peut aussi être gérée à l'aide d'une « liste blanche » contenue dans la mémoire 110 de chaque serrure électronique. Une liste blanche est une liste qui contient les identifiants Kpub de chaque terminal mobile autorisé à déverrouiller la serrure électronique. Le déverrouillage de la serrure électronique est alors interdit à tout terminal mobile dont l'identifiant Kpub n'appartient pas à cette liste blanche.

[0156] L'utilisation des indices Kpr et Cpr peut aussi être omise. Dans ce cas, les étapes 194 et 196 sont omises. Dès lors, si un terminal mobile comporte une autorisation d'accès pour la serrure 10 dans sa table 140, c'est systématiquement cette autorisation d'accès qui est utilisée et cela même si, de son côté, la table 112 de la serrure 10 comporte elle aussi des autorisations d'accès pour ce même terminal mobile. Cette variante est aussi applicable dans le cas particulier où les serrures ne sont jamais programmées, c'est-à-dire que la phase 160 est omise.

[0157] D'autres modes de réalisation de la fonction CBC_MAC() sont possibles. Dans les exemples de mode de réalisation précédemment décrits, il n'est pas nécessaire que l'on puisse déchiffrer le cryptogramme KCpub ou KKpub construit pour vérifier l'intégrité et l'authenticité des trames d'informations transmises. Dès lors, la fonction CBC_MAC() peut être une fonction à sens unique, c'est-à-dire une fonction non-inversible, paramétrée par une clé de chiffrement. Par exemple, la fonction CBC_MAC() génère d'abord un condensat ou une empreinte numérique (appelé « hash » en anglais) des données en clair à signer à l'aide d'une fonction de hachage prédéterminée puis c'est ce condensat qui est chiffré à l'aide d'un algorithme de chiffrement symétrique et en utilisant pour cela une clé de chiffrement.

[0158] Dans un mode de réalisation avantageux, la fonction CBC_MAC() est égale à la composition d'un algorithme de dérivation de clé et d'un algorithme de chiffrement. Ceci est illustré dans le cas de la construction du cryptogramme KCpub. Dans ce mode de réalisation, pour construire le cryptogramme KCpub, l'exécution de la fonction CBC_MAC() provoque d'abord l'exécution de l'algorithme de dérivation de clé. Ainsi, une clé de chiffrement Caes1 est dérivée à partir de la clé de chiffrement Caes. Cette clé de chiffrement Caes1 est différente de la clé Caes. Par exemple, la clé Caes1 est obtenue à l'aide de la relation suivante : Caes1 = AES_CBC(Caes ; Ct). Ensuite, l'algorithme de chiffrement paramétré par la clé Caes1 est exécuté pour obtenir le cryptogramme KCpub. Ainsi, dans ce mode de réalisation, le cryptogramme KCpub est obtenu en chiffrant les données Kpub, Kindice, Cpub et Cindice à l'aide de la clé Caes1 dérivée de la clé Caes. Dans ce cas là aussi, le cryptogramme KCpub est construit à l'aide de la clé Caes. De façon similaire, ce mode de réalisation peut être appliqué à la fonction CBC_MAC() utilisée pour construire le cryptogramme KKpub. Ainsi, dans ce dernier cas, lorsque la fonction CBC_MAC() est exécutée, une clé Kaes1 est d'abord dérivée à partir de la clé Kaes puis la clé Kaes1 est utilisée comme clé de chiffrement des données Kpub, Kindice, Cpub et Cindice.

[0159] En variante, l'algorithme de chiffrement mis en œuvre lors de l'exécution de la fonction CBC_MAC(), est un algorithme de chiffrement asymétrique. Puisque les signatures S_{180} et S_{182} ne sont pas déchiffrées, même dans le cas de cette variante, l'exécution d'un algorithme de déchiffrement en utilisant la clé publique correspondant

à la clé privée utilisée pour construire les signatures S_{180} et S_{182} n'est pas mis œuvre.

[0160] Les fonctions de construction utilisées pour construire les cryptogrammes KCpub, KKpub et les signatures S_{180} et S_{182} peuvent être différentes les unes des autres. Toutefois, de préférence, chacune de ces fonctions fait uniquement intervenir des algorithmes de chiffrement symétrique.

[0161] Les variantes décrites ci-dessus dans le cas particulier de la fonction CBC_MAC() sont transposables à la fonction AES_CBC().

[0162] En variante, le cryptogramme KCpub est construit sans prendre en compte l'identifiant Cpub. Dans ce cas aussi, le programme KCpub permet uniquement de déverrouiller la serrure 10 car ce cryptogramme dépend de la clé unique Caes de cette serrure 10.

[0163] Dans un autre mode de réalisation simplifié, les opérations de dérivation des clés KCpub1 et KKpub1 consistent simplement à prendre les clés KCpub1 et KKpub1 égales, respectivement, aux cryptogrammes KCpub et KKpub. Dans ce cas, ce sont directement les cryptogrammes KCpub et KKpub qui sont utilisés comme clé de chiffrement pour construire les signatures S_{180} et S_{182}.

[0164] Variantes de l'utilisation du cryptogramme KCpub :

[0165] Les caractéristiques, appelée ici "caractéristique A)", qui permettent d'obtenir les mêmes avantages que ceux obtenus à l'aide du procédé de contrôle d'accès de la demande EP1321901 tout en rendant possible l'utilisation d'algorithmes de chiffrement symétriques à la place des algorithmes de chiffrement asymétriques peuvent être mises en œuvre indépendamment des autres caractéristiques des procédés de contrôle d'accès décrits ici. Par exemple, dans un mode de réalisation simplifiée, la table 112 est omise. Dans ce cas, aucune autorisation d'accès ne peut être enregistrée dans la serrure électronique. Dès lors, la phase 160 et les étapes 182, 194, 196, 230, 232, 234 sont omises. Dans un tel mode de réalisation, il n'est pas possible de programmer une serrure électronique pour que celle-ci se déplace dans son état déverrouillé lorsqu'un terminal mobile qui n'a pas au préalable été programmé pour déverrouiller cette serrure est présenté.

[0166] De même, les caractéristiques A) sont indépendantes de l'utilisation de l'indice Cindice précédemment décrite. Ainsi, en variante, l'indice Cindice n'est pas utilisé et peut être omis. Dans ce cas, il n'est pas possible d'invalider en une seule opération l'ensemble des terminaux mobiles qui étaient préalablement autorisés à déverrouiller cette serrure 10. Dans ce mode de réalisation, les cryptogrammes KCpub et KKpub sont construits sans utiliser l'indice Cindice.

[0167] Variantes de l'utilisation du cryptogramme KKpub

[0168] Les caractéristiques, appelée ici "caractéristiques B)", qui permettent d'utiliser à la fois des terminaux mobiles programmés pour ouvrir la serrure 10 et des terminaux

mobiles non-programmés pour ouvrir la serrure 10, peuvent être mises en œuvre indépendamment des caractéristiques A). Dans ce cas, les fonctions CBC_MAC() et/ou AES_MAC() peuvent être remplacées par des fonctions qui jouent le même rôle mais en faisant intervenir des algorithmes de chiffrement asymétriques. Par exemple, la trame T_{180} comporte un certificat cryptographique. Ce certificat cryptographique contient les données D_{180} en clair, les autorisations A_{180}, le nonce et une signature numérique S_{180} des données D_{180}, des autorisation A_{180} et du nonce. Dans ce cas, la signature numérique S_{180} est typiquement construite en utilisant un algorithme de chiffrement asymétrique paramétré par une clé privée. La vérification de l'intégrité et de l'authenticité des données contenues dans la trame T_{180} reçue par la serrure électronique consiste alors à vérifier l'intégrité et l'authenticité du certificat cryptographique reçu à l'aide de la clé publique correspondant à la clé privée utilisée pour signer ce certificat. Dans un tel mode de réalisation, la vérification de l'intégrité et de l'authenticité impose alors l'exécution d'algorithmes de chiffrement asymétrique.

[0169] Les caractéristiques B) peuvent aussi être mise en œuvre indépendamment de l'utilisation de l'indice Cindice ou de l'utilisation d'un nonce.

[0170] Les caractéristiques B) peuvent aussi être mise en œuvre avec d'autres méthodes pour vérifier que les cryptogrammes construits et pré-enregistrés sont identiques. Par exemple, dans un mode de réalisation simplifié, la signature S_{180} est remplacée par le cryptogramme KCpub pré-enregistré dans le terminal 16. Dans ce cas simplifié, la vérification que le cryptogramme KCpub est identique au cryptogramme KCpub' construit consiste alors simplement à comparer le cryptogramme KCpub contenu dans la trame T_{180} au cryptogramme KCpub' construit par la serrure 10. De façon analogue, la signature S_{182} est remplacée par le cryptogramme KKpub' construit par le terminal 16. La vérification que le cryptogramme KKpub' est identique au cryptogramme KKpub consiste alors simplement à comparer le cryptogramme KKpub' contenu dans la trame T_{182} au cryptogramme KKpub contenu dans la table 112. Dans ce cas, de préférence, un mécanisme pour éviter les attaques par rejeu et qui n'utilise pas les signatures S_{180} et S_{182} est en plus implémenté.

[0171] Les caractéristiques B) peuvent aussi être mise en œuvre dans un système où les autorisations d'accès sont transmises par l'intermédiaire d'un canal sécurisé.

[0172] Pour la mise en œuvre des caractéristiques B), les clés Kaes et Caes n'ont pas besoin d'être uniques. Ainsi, la clé Kaes et/ou la clé Caes peut être commune, respectivement, à plusieurs terminaux mobiles et à plusieurs serrures électroniques.

[0173] <u>Variantes de l'utilisation de l'indice Cindice :</u>

[0174] L'utilisation de l'indice Cindice décrite ici pour invalider en une seule opération l'ensemble des terminaux mobiles précédemment autorisés à déverrouiller la serrure 10, peut aussi être mise en œuvre indépendamment des caractéristiques A) et B). Par

exemple, l'utilisation de l'indice Cindice tel que décrit ici peut être mise en œuvre dans des procédés de contrôle d'accès où la vérification de l'intégrité et de l'authenticité de l'indice Cindice transmis est réalisée de façon différente de ce qui a été décrit ici. Par exemple, l'utilisation de l'indice Cindice peut être mise en œuvre dans les procédés de contrôle d'accès décrits dans la demande EP1024239A1. Dans ce dernier cas, l'indice Cindice est, par exemple, inclus dans l'autorisation d'accès a_{ij} générée par un serveur de droit d'accès et transmise sous forme chiffrée par le terminal mobile à la serrure électronique. Dans la demande EP1024239A1, l'autorisation d'accès a_{ij} est chiffrée avec une clé s_j connue seulement du serveur de droit d'accès et des serrures électroniques de sorte que le terminal mobile ne peut pas falsifier l'autorisation d'accès a_{ij}. Dans la serrure électronique, l'autorisation d'accès a_{ij} est déchiffrée avec la clé s_j puis l'indice Cindice contenu dans l'autorisation d'accès a_{ij} déchiffrée est comparée à un indice Cindice pré-enregistré dans la mémoire de la serrure électronique. Si l'indice Cindice contenu dans l'autorisation d'accès a_{ij} est inférieur à l'indice Cindice pré-enregistré, alors le déplacement de la serrure électronique dans son état déverrouillé est systématiquement inhibé.

[0175] Dans le contexte du procédé de contrôle d'accès de la demande EP1321901, l'indice Cindice transmis par le terminal mobile peut être incorporé au certificat cryptographique transmis par ce terminal mobile à la serrure électronique. Ensuite, le reste du fonctionnement se déduit des explications données dans ce texte.

[0176] Chapitre III : Avantages des modes de réalisation décrits :

[0177] Avantages du procédé utilisant le cryptogramme KCpub :

[0178] Grâce au fait que la serrure électronique reconstruit le cryptogramme KCpub à partir de sa clé unique Caes et de l'identifiant Kpub reçu, la serrure électronique n'a pas besoin d'être programmée à l'avance pour se déplacer dans son état déverrouillé lorsqu'un terminal autorisé à déverrouiller cette serrure est présenté. Autrement dit, la serrure électronique n'a pas besoin d'être programmée à l'avance pour être déverrouillée par des terminaux mobiles.

[0179] Grâce au fait que la clé Caes est unique pour chaque serrure électronique du système 2, si les informations contenues dans une serrure électronique particulière sont compromises, cela ne remet pas en cause la sécurité du système 2. En particulier, cela ne remet pas en cause la sécurité des autres serrures électroniques du système 2. En effet, les informations compromises sont inutilisables pour déverrouiller d'autres serrures électroniques du système 2.

[0180] De façon réciproque, le fait que chaque terminal mobile ne contient pas la clé Caes de la serrure électronique qu'il est autorisé à déverrouiller mais seulement le cryptogramme KCpub correspondant à cette serrure électronique, garantit que si ces informations sont compromises, alors cela ne remet pas non plus en cause la sécurité du

système 2. En effet, puisque les cryptogrammes KCpub contenus dans les terminaux mobiles sont, chacun, spécifiques à une serrure électronique et à ce terminal mobile, ils ne peuvent pas être utilisés par d'autres terminaux mobiles pour déverrouiller d'autres serrures électroniques.

[0181] Le procédé de contrôle d'accès décrit ici permet de déverrouiller une serrure électronique en absence de toute liaison de transmission d'informations avec le serveur 50 de droit d'accès. De plus, le fait que le nonce soit utilisé pour construire la signature S_{180} rend le système robuste vis-à-vis des attaques par rejeu. Ce procédé n'utilise pas non plus de canal sécurisé pour transmettre les autorisations d'accès. Il n'est donc pas nécessaire de générer des clés de session pour créer un tel canal sécurisé de transmission d'informations.

[0182] En fait, en mettant en œuvre l'enseignement décrit ici, un appariement robuste est créé entre chaque terminal mobile et la chaque serrure électronique que ce terminal mobile est susceptible de déverrouiller. En effet, le cryptogramme KCpub dépend à la fois de l'identifiant Kpub de ce terminal et de la clé unique Caes de la serrure électronique à déverrouiller. Ainsi, ce cryptogramme ne peut être utilisé que par ce terminal mobile pour déverrouiller cette serrure électronique.

[0183] Le fait de transmettre l'identifiant Cpub au terminal mobile permet au terminal mobile de sélectionner rapidement le cryptogramme KCpub à utiliser.

[0184] Le fait de construire la clé KCpub en fonction de l'identifiant Cpub permet de rendre encore plus difficile la falsification de l'identité de la serrure électronique à déverrouiller.

[0185] Dans le cas où le terminal mobile ne comporte aucun cryptogramme KCpub pour déverrouiller la serrure électronique, le fait de transmettre la trame T_{182}, à la place de la trame T_{180}, permet de provoquer le déverrouillage de la serrure électronique même si ce terminal mobile n'avait pas été préalablement explicitement programmé pour déverrouiller cette serrure électronique. De plus, ce résultat est atteint tout en étant robuste vis-à-vis des cas où les données dans le terminal mobile ou la serrure électronique sont compromises. En effet, le cryptogramme KKpub dépend à la fois de la clé Kaes unique du terminal et de l'identifiant Cpub de la serrure électronique. Ainsi, les informations contenues dans ce terminal mobile et cette serrure ne permettent pas de construire des autorisations d'accès valides pour déverrouiller une autre serrure électronique du système ou autoriser un autre terminal mobile à déverrouiller cette serrure électronique.

[0186] L'utilisation de l'identifiant Kpub pour sélectionner le cryptogramme KKpub enregistré dans la mémoire 110 de la serrure électronique permet de sélectionner rapidement cet identifiant KKpub.

[0187] Le fait d'utiliser des algorithmes de chiffrement symétriques au lieu d'algorithmes de

chiffrement asymétriques simplifie les fonctions exécutées par la serrure électronique et par le terminal mobile pour construire les signatures numériques S_{180} et S_{182}. Dès lors les fonctions mises en œuvre sont plus simples et moins énergivores. La consommation électrique des terminaux mobiles et des serrures électroniques est donc réduite par rapport au cas où des algorithmes de chiffrement asymétriques seraient utilisés.

[0188] L'utilisation de l'indice Kindice pour construire le cryptogramme KCpub rend le procédé de contrôle d'accès robuste vis-à-vis des tentatives de falsification visant à rendre un terminal mobile, précédemment invalidé, à nouveau valide.

[0189] Le fait d'utiliser un code d'accès Ov pour chaque serrure qu'un terminal est autorisé à déverrouiller permet d'éviter d'avoir à reprogrammer tous les droits d'accès de ce terminal alors qu'un seul de ses droits d'accès est modifié. Par exemple, si le terminal 16 est initialement autorisé à déverrouiller une première et une seconde serrures alors, ultérieurement, pour lui interdire de déverrouiller seulement la seconde serrure, il suffit de modifier la valeur du code d'accès Ov associé à l'identifiant Cpub de la seconde serrure dans sa table 140 tout en laissant son indice Kindice inchangé. Lorsque le code d'accès Ov n'est pas utilisé, la seule solution pour interdire au terminal 16 de déverrouiller la seconde serrure consiste à incrémenter son indice Kindice. Dès lors, en même temps, le cryptogramme KCpub qui l'autorise à déverrouiller la première serrure doit aussi être immédiatement reconstruit à l'aide de la nouvelle valeur de l'indice Kindice sans quoi le terminal 16 ne peut plus déverrouiller la première serrure. De plus, le fait d'intégrer le code Ov dans les données utilisées pour construire la signature S_{180} permet de rendre difficile la falsification de la valeur de ce code Ov.

[0190] <u>Avantages du procédé utilisant le cryptogramme KKpub :</u>

[0191] Le procédé de contrôle d'accès décrit ici présente les mêmes avantages que celui décrit dans la demande EP1321901. En particulier, il est possible de programmer un terminal mobile pour déplacer une serrure électronique particulière dans son état déverrouillé. Dans ce cas, il n'est pas nécessaire de programmer cette serrure électronique. Seul le terminal mobile a besoin d'être programmé pour déverrouiller cette serrure électronique. De plus, ici, le fonctionnement inverse est aussi possible. En effet, chaque serrure électronique peut être programmée pour se déplacer dans son état déverrouillé lorsqu'un terminal mobile spécifique non-programmé est présenté devant cette serrure électronique. Dans ce deuxième cas, il n'est pas nécessaire d'avoir programmé à l'avance le terminal mobile. Seule la serrure électronique a été programmée.

[0192] L'implémentation de la fonctionnalité inverse est ici réalisée sans amoindrir la sécurité du système de contrôle d'accès. En effet, le fait que le cryptogramme KKpub soit fonction de l'identifiant Kpub du terminal mobile rend difficile la falsification de l'identifiant Kpub transmis dans la trame T_{182}.

[0193] Le fait que le cryptogramme KKpub utilisé pour vérifier l'intégrité et l'authenticité de la signature S_{182} soit fonction de l'identifiant Kpub de terminal et de l'identifiant Cpub de la serrure électronique empêche que la sécurité du système 2 soit remise en cause si les informations contenues dans la mémoire 110 de la serrure 10 sont compromises. En effet, les cryptogrammes KKpub enregistrés dans la mémoire 110 ne peuvent pas être utilisés pour déverrouiller d'autres serrures électroniques du système 2.

[0194] Le fait que le cryptogramme KKpub soit construit à l'aide de la clé Kaes qui n'est pas contenue dans la mémoire de la serrure 10 rend impossible la construction de nouvelles autorisations d'accès pour cette serrure 10 à partir des seules informations contenues dans sa mémoire 110.

[0195] Le fait que la clé Kaes soit unique garantit aussi que si les informations contenues dans la mémoire 42 du terminal 16 sont compromises, alors la sécurité des autres serrures électroniques et des autres terminaux mobiles n'est pas remise en cause. En effet, la clé unique Kaes permet seulement de construire des cryptogrammes KKpub' pour ce terminal 16 et non par pour d'autres terminaux mobiles. De plus, si une autre serrure électronique ne contient aucun cryptogramme KKpub correspondant au terminal 16, le fait de connaître la clé unique Kaes du terminal 16 n'est d'aucune aide pour déverrouiller cette autre serrure électronique.

[0196] L'utilisation des indices de priorité Kpr et Cpr permet de garantir que lorsque des autorisations d'accès sont enregistrées à la fois dans un terminal mobile et dans une serrure électronique, alors c'est systématiquement les autorisations d'accès les plus récentes qui sont utilisées. Ainsi, l'utilisation d'autorisations d'accès périmées est rendue impossible dans une telle situation.

[0197] Le fait d'utiliser un terminal mobile pour transmettre des autorisations d'accès à une serrure électronique évite d'avoir à raccorder cette serrure électronique à un réseau grande distance de transmission d'informations pour la programmer.

[0198] Le fait que les signatures numériques transmises du terminal mobile vers la serrure électronique soient fonction d'un nonce permet de rendre le procédé robuste contre les attaques par rejeu. Ces attaques par rejeu consistent à enregistrer puis rejouer les trames d'informations transmises du terminal mobile vers la serrure électronique. De plus, cette robustesse est atteinte sans qu'il soit nécessaire de communiquer avec la serrure électronique par l'intermédiaire d'un canal sécurisé de communication.

[0199] Le fait d'établir l'identité des cryptogrammes KKpub et KKpub' à partir de l'identité des signatures S_{182} et S'_{182} permet d'établir l'identité de ces cryptogrammes sans les transmettre entre le terminal mobile et la serrure électronique.

[0200] <u>Avantages des procédés utilisant l'indice Cindice :</u>

[0201] L'utilisation de l'indice Cindice permet en une seule opération d'interdire le déverrouillage de cette serrure électronique par l'ensemble des terminaux mobiles qui

étaient précédemment autorisés à la déverrouiller. Pour cela, il suffit simplement d'incrémenter l'indice Cindice enregistré dans la mémoire 110 de la serrure électronique. Lorsque le nombre de terminaux mobiles autorisés à déverrouiller une serrure électronique est important, cette façon de procéder pour invalider l'ensemble des terminaux mobiles est beaucoup plus rapide et simple que si chaque terminal mobile devait être reprogrammé individuellement afin de lui interdire de déverrouiller cette serrure électronique. Typiquement, une telle procédure est particulièrement utile lorsqu'une serrure électronique est déplacée d'un bâtiment vers un autre bâtiment.

[0202] Le fait d'utiliser l'indice Cindice pour construire le cryptogramme KCpub, permet de rendre simplement le procédé de contrôle d'accès très robuste vis-à-vis des tentatives de falsification de cet indice Cindice dans un terminal mobile.

[0203] Le fait d'utiliser l'un des terminaux mobiles pour transmettre la commande d'invalidation générique à une serrure électronique évite d'avoir à raccorder cette serrure électronique à un réseau grande distance de transmission d'informations pour la programmer.

Revendications

[Revendication 1] Procédé de contrôle d'accès à des bâtiments, ce procédé comportant :
- la fourniture (148) de plusieurs serrures électroniques déplaçables chacune entre :
- un état verrouillé dans lequel elle interdit l'accès au bâtiment, et
- un état déverrouillé dans lequel elle autorise l'accès au bâtiment,
chaque serrure électronique comportant un microprocesseur et une mémoire contenant un identifiant de serrure (Cpub) qui identifie de façon unique cette serrure électronique parmi l'ensemble des serrures électroniques fournies et une première clé de chiffrement (Caes), et
- la fourniture (148) de plusieurs terminaux mobiles d'ouverture, chacun de ces terminaux mobiles comportant un microprocesseur et une mémoire contenant un identifiant de terminal (Kpub) qui identifie de façon unique ce terminal mobile parmi l'ensemble des terminaux mobiles fournis,
- la programmation (150) d'au moins un premier des terminaux mobiles fournis pour l'autoriser à déplacer une première des serrures électroniques fournies dans son état déverrouillé, cette programmation comportant l'enregistrement, dans la mémoire de ce premier terminal mobile, d'un premier cryptogramme (KCpub) et de l'identifiant de serrure (Cpub) de la première serrure électronique associé à ce premier cryptogramme, le premier cryptogramme (KCpub) étant construit à partir de l'identifiant de terminal (Kpub) du premier terminal, de l'identifiant de serrure (Cpub) de la première serrure électronique et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la première clé de chiffrement (Caes) de la première serrure électronique, la première clé de chiffrement n'étant pas enregistrée dans la mémoire du premier terminal mobile de sorte qu'il n'est pas possible de construire ce premier cryptogramme seulement à partir des informations contenues dans la mémoire de ce premier terminal mobile,
- à chaque fois que le premier terminal mobile souhaite déplacer la première serrure électronique dans son état déverrouillé, le procédé comporte les étapes suivantes :
1) la première serrure électronique transmet (176) au premier terminal mobile son identifiant de serrure (Cpub) contenu dans sa mémoire,
2) en réponse, le premier terminal mobile recherche (178) dans sa mémoire s'il existe un premier cryptogramme (KCpub) associé à

l'identifiant de serrure transmis, et
3) lorsqu'un tel premier cryptogramme (KCpub) est trouvé dans la mémoire du premier terminal mobile, alors le premier terminal mobile transmet (188) à la première serrure électronique une première trame (T_{180}) d'informations contenant son identifiant de terminal (Kpub),
4) en réponse à la réception de la première trame d'informations (T_{180}), la première serrure électronique :
- construit (192) un deuxième cryptogramme (KCpub') à partir de l'identifiant de terminal (Kpub) contenu dans la première trame d'informations, de son identifiant de serrure (Cpub) contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le premier cryptogramme (KCpub) paramétré par la première clé (Caes) contenue dans la mémoire de la première serrure électronique, puis
- la première serrure électronique vérifie (192) que le deuxième cryptogramme (KCpub') construit est identique au premier cryptogramme (KCpub), et
- dans le cas où les premier et deuxième cryptogrammes (KCpub, KCpub') sont identiques, la première serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les premier et deuxième cryptogrammes (KCpub, KCpub') sont différents, le déplacement de la première serrure électronique depuis son état verrouillé vers son état déverrouillé est interdit,
caractérisé en ce que :
- la fourniture (148) de plusieurs terminaux mobiles comporte la fourniture de plusieurs terminaux mobiles dont la mémoire de chacun de ces terminaux mobiles comporte une deuxième clé de chiffrement (Kaes) différente de la première clé de chiffrement (Caes), et
- le procédé comporte la programmation (160) d'une seconde des serrures électroniques fournies pour l'autoriser à être déplacée dans son état déverrouillé par le premier terminal mobile, cette programmation comportant l'enregistrement, dans la mémoire de la seconde serrure électronique, d'un troisième cryptogramme (KKpub) construit à partir de l'identifiant (Cpub) de cette seconde serrure électronique, de l'identifiant de terminal (Kpub) du premier terminal mobile et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la deuxième clé de chiffrement (Kaes) du premier terminal mobile,
la deuxième clé de chiffrement (Kaes) du premier terminal mobile

n'étant pas enregistrée dans la mémoire de la seconde serrure électronique de sorte qu'il n'est pas possible de construire le troisième cryptogramme seulement à partir des informations contenues dans la mémoire de cette seconde serrure électronique, et

- à chaque fois que le premier terminal mobile souhaite déplacer la seconde serrure électronique dans son état déverrouillé, le procédé comporte les étapes suivantes :

5) la seconde serrure électronique transmet (176) au premier terminal mobile son identifiant de serrure (Cpub),

6) en réponse, le premier terminal mobile recherche (178) dans sa mémoire un premier cryptogramme associé à l'identifiant de serrure transmis, puis

7) lorsque aucun premier cryptogramme associé à l'identifiant de serrure transmis n'est pas trouvé dans la mémoire du premier terminal mobile :

- le premier terminal mobile construit (220) un quatrième cryptogramme (KKpub') à partir de l'identifiant de serrure (Cpub) transmis par la seconde serrure électronique, de son identifiant de terminal (Kpub) contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le troisième cryptogramme (KKpub) paramétré par la deuxième clé de chiffrement (Kaes) contenue dans la mémoire de ce premier terminal mobile, puis

- le premier terminal mobile transmet (226) à la seconde serrure électronique une seconde trame (T_{182}) d'informations, à la place de la première trame (T_{180}) d'informations, cette seconde trame d'informations contenant l'identifiant de terminal (Kpub) du premier terminal , puis

8) en réponse à la réception de la seconde trame d'informations (T_{182}), la seconde serrure électronique vérifie (232), que le troisième cryptogramme (KKpub) enregistré dans sa mémoire est identique au quatrième cryptogramme (KKpub'), et

9) dans le cas où les troisième et quatrième cryptogrammes (KKpub, KKpub') sont identiques, la seconde serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les troisième et quatrième cryptogrammes (KKpub, KKpub') sont différents, le déplacement de la seconde serrure électronique depuis son état verrouillé vers son état déverrouillé est interdit.

[Revendication 2] Procédé selon la revendication 1, dans lequel :

- la programmation (150) du premier terminal mobile comporte

également l'enregistrement dans la mémoire de ce premier terminal mobile d'un premier indice de priorité (Kpr) spécifiquement associé au premier cryptogramme (KCpub),
- le procédé comporte la programmation (160) de la première serrure électronique fournies pour l'autoriser à être déplacée dans son état déverrouillé par le premier terminal mobile, cette programmation comportant l'enregistrement, dans la mémoire de la première serrure électronique :
- d'un troisième cryptogramme (KKpub) construit à partir de l'identifiant (Cpub) de cette première serrure électronique, de l'identifiant de terminal (Kpub) du premier terminal mobile et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la deuxième clé de chiffrement (Kaes) du premier terminal mobile, et
- d'un second indice de priorité (Cpr) spécifiquement associé au troisième cryptogramme (KKpub),
la deuxième clé de chiffrement (Kaes) du premier terminal mobile n'étant pas enregistrée dans la mémoire de la première serrure électronique de sorte qu'il n'est pas possible de construire le troisième cryptogramme seulement à partir des informations contenues dans la mémoire de cette première serrure électronique, et
- lors de l'étape 3), la première trame d'informations (T_{180}) contient, en plus, le premier indice de priorité (Kpr) associé au premier cryptogramme (KCpub),
- après l'étape 3) et avant l'étape 4), en réponse à la réception par la première serrure électronique de la première trame d'informations, la première serrure électronique recherche (190) dans sa mémoire un troisième cryptogramme préenregistré (KKpub) et un second indice de priorité (Cpr) associés à l'identifiant de terminal (Kpub) contenu dans la première trame d'informations (T_{180}), puis
- lorsqu'un tel second indice de priorité (Cpr) est trouvé dans la mémoire de la première serrure électronique, la première serrure électronique compare (192) le premier indice de priorité (Kpr) contenu dans la première trame d'informations (T_{180}) au second indice de priorité (Cpr) trouvé dans la mémoire de la première serrure électronique, et
- lorsque le premier indice de priorité (Kpr) est supérieur au second indice de priorité (Cpr), la première serrure électronique exécute l'étape 4) et inhibe l'exécution de l'étape 7), et
- lorsque le premier indice de priorité (Kpr) est inférieur au second

indice de priorité (Cpr), la première serrure électronique exécute l'étape 7) et inhibe l'exécution de l'étape 4).

[Revendication 3] Procédé selon l'une quelconque des revendications précédentes, dans lequel :
- la programmation (160) de la seconde serrure électronique comporte la transmission à la seconde serrure électronique, par un second des terminaux mobiles fournis différent du premier terminal mobile, de l'identifiant de terminal (Kpub) du premier terminal mobile et du troisième cryptogramme (KKpub), et
- en réponse, la seconde serrure électronique enregistre dans sa mémoire le troisième cryptogramme reçu associé à l'identifiant de terminal (Kpub) du premier terminal.

[Revendication 4] Procédé selon l'une quelconque des revendications précédentes, dans lequel la première clé de chiffrement est une clé unique (Kaes).

[Revendication 5] Procédé selon l'une quelconque des revendications précédentes, dans lequel :
- à chaque fois que le premier terminal mobile souhaite déplacer l'une des serrures électroniques fournies dans son état déverrouillé, le premier terminal mobile et cette serrure électronique échangent (176) un nombre aléatoire, appelé "nonce", de sorte que ce nonce est connu à la fois du premier terminal mobile et de cette serrure électronique, ce nonce variant à chaque fois que le procédé de contrôle d'accès est exécuté entre le premier terminal mobile et cette serrure électronique,
- lors de l'étape 3), la première trame d'informations transmise contient en plus une première signature numérique (S_{180}) construite à l'aide de l'identifiant de terminal (Kpub) du premier terminal et du nonce échangé, et
- lors de l'étape 7), la seconde trame d'informations transmise contient en plus une deuxième signature numérique (S_{182}) construite à l'aide de l'identifiant de terminal (Kpub) du premier terminal et du nonce échangé.

[Revendication 6] Procédé selon l'une quelconque des revendications précédentes, dans lequel la première clé de chiffrement d'une serrure électronique est une clé unique de serrure (Caes) différente de toutes les clés uniques de serrure des autres serrures électroniques.

[Revendication 7] Procédé selon l'une quelconque des revendications précédentes, dans lequel la deuxième clé de chiffrement d'un terminal mobile est une clé unique de terminal (Kaes) différente de toutes les clés uniques de

terminal des autres terminaux mobiles.

[Revendication 8] Système de contrôle d'accès à des bâtiments comportant :
- plusieurs serrures électroniques (10) déplaçables chacune entre :
- un état verrouillé dans lequel elle interdit l'accès au bâtiment, et
- un état déverrouillé dans lequel elle autorise l'accès au bâtiment,
chaque serrure électronique comportant un microprocesseur (108) et une mémoire (110) contenant un identifiant de serrure (Cpub) qui identifie de façon unique cette serrure électronique parmi l'ensemble des serrures électroniques du système de contrôle d'accès et une première clé de chiffrement (Caes), et
- plusieurs terminaux mobiles (16) d'ouverture, chacun de ces terminaux mobiles comportant un microprocesseur (40) et une mémoire (42) contenant un identifiant de terminal (Kpub) qui identifie de façon unique ce terminal mobile parmi l'ensemble des terminaux mobiles du système de contrôle d'accès,
- au moins un premier des terminaux mobiles étant autorisé à déplacer une première des serrures électroniques dans son état déverrouillé, la mémoire (42) de ce premier terminal mobile contenant à cet effet un premier cryptogramme (KCpub) et l'identifiant de serrure (Cpub) de la première serrure électronique associé à ce premier cryptogramme, le premier cryptogramme (KCpub) étant construit à partir de l'identifiant de terminal (Kpub) du premier terminal, de l'identifiant de serrure (Cpub) de la première serrure électronique et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la première clé de chiffrement (Caes) de la première serrure électronique, la première clé de chiffrement n'étant pas enregistrée dans la mémoire du premier terminal mobile de sorte qu'il n'est pas possible de construire ce premier cryptogramme (KCpub) seulement à partir des informations contenues dans la mémoire de ce premier terminal mobile,
- le premier terminal mobile et la première serrure électronique étant configurés pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la première serrure électronique dans son état déverrouillé, :
1) la première serrure électronique transmet au premier terminal mobile son identifiant de serrure (Cpub) contenu dans sa mémoire,
2) en réponse, le premier terminal mobile recherche dans sa mémoire s'il existe un premier cryptogramme (KCpub) associé à l'identifiant de serrure transmis, et

3) lorsqu'un tel premier cryptogramme (KCpub) est trouvé dans la mémoire du premier terminal mobile, alors le premier terminal mobile transmet à la première serrure électronique une première trame (T_{180}) d'informations contenant son identifiant de terminal (Kpub),
4) en réponse à la réception de la première trame d'informations (T_{180}), la première serrure électronique :
- construit un deuxième cryptogramme (KCpub') à partir de l'identifiant de terminal (Kpub) contenu dans la première trame d'informations, de son identifiant de serrure (Cpub) contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le premier cryptogramme (KCpub) paramétré par la clé (Caes) contenue dans la mémoire de la première serrure électronique, puis
- la première serrure électronique vérifie, que le deuxième cryptogramme (KCpub') construit est identique au premier cryptogramme (KCpub), et
- dans le cas où les premier et deuxième cryptogrammes (KCpub, KCpub') sont identiques, la première serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les premier et deuxième cryptogrammes (KCpub, KCpub') sont différents, le déplacement de la première serrure électronique depuis son état verrouillé vers son état déverrouillé est interdit,
caractérisé en ce que :
- la mémoire de chacun des terminaux mobiles comporte une deuxième clé de chiffrement (Kaes) différente de la première clé de chiffrement (Caes), et
- une seconde des serrures électroniques étant autorisée à être déplacée dans son état déverrouillé par le premier terminal mobile, la mémoire de cette seconde serrure électronique contenant un troisième cryptogramme (KKpub) construit à partir de l'identifiant (Cpub) de cette seconde serrure électronique, de l'identifiant de terminal (Kpub) du premier terminal mobile et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la deuxième clé de chiffrement (Kaes) du premier terminal mobile,
la deuxième clé de chiffrement (Kaes) du premier terminal mobile n'étant pas enregistrée dans la mémoire de la seconde serrure électronique de sorte qu'il n'est pas possible de construire le troisième cryptogramme seulement à partir des informations contenues dans la

mémoire de cette seconde serrure électronique, et
- le premier terminal et la seconde serrure électronique sont configurés pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la seconde serrure électronique dans son état déverrouillé :
5) la seconde serrure électronique transmet au premier terminal mobile son identifiant de serrure (Cpub),
6) en réponse, le premier terminal mobile recherche dans sa mémoire un premier cryptogramme associé à l'identifiant de serrure transmis, puis
7) lorsque aucun premier cryptogramme associé à l'identifiant de serrure transmis n'est trouvé dans la mémoire du premier terminal mobile :
- le premier terminal mobile construit un quatrième cryptogramme (KKpub') à partir de l'identifiant de serrure (Cpub) transmis par la seconde serrure électronique, de son identifiant de terminal (Kpub) contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le troisième cryptogramme (KKpub) paramétré par la deuxième clé de chiffrement (Kaes) contenue dans la mémoire de ce premier terminal mobile, puis
- le premier terminal mobile transmet à la seconde serrure électronique une seconde trame (T_{182}) d'informations, à la place de la première trame (T_{180}) d'informations, cette seconde trame d'informations contenant l'identifiant de terminal (Kpub) du premier terminal , puis
8) en réponse à la réception de la seconde trame d'informations (T_{182}), la seconde serrure électronique vérifie (232), que le troisième cryptogramme (KKpub) enregistré dans sa mémoire est identique au quatrième cryptogramme (KKpub'), et
9) dans le cas où les troisième et quatrième cryptogrammes (KKpub, KKpub') sont identiques, la seconde serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les troisième et quatrième cryptogrammes (KKpub, KKpub') sont différents, le déplacement de la seconde serrure électronique depuis son état verrouillé vers son état déverrouillé est interdit.

[Revendication 9] Premier terminal mobile pour la réalisation d'un système de contrôle d'accès à des bâtiments conforme à la revendication 8, dans lequel ce premier terminal mobile comporte un microprocesseur (40) et une mémoire (42) contenant un identifiant de terminal (Kpub) qui identifie de façon unique ce premier terminal mobile parmi l'ensemble des

terminaux mobiles du système de contrôle d'accès,
- ce premier terminal mobile étant autorisé à déplacer une première des serrures électroniques du système de contrôle d'accès dans son état déverrouillé, la mémoire (42) de ce premier terminal mobile contenant à cet effet un premier cryptogramme (KCpub) et l'identifiant de serrure (Cpub) de la première serrure électronique associé à ce premier cryptogramme, le premier cryptogramme (KCpub) étant construit à partir de l'identifiant de terminal (Kpub) du premier terminal, de l'identifiant de serrure (Cpub) de la première serrure électronique et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la première clé de chiffrement (Caes) de la première serrure électronique, la première clé de chiffrement n'étant pas enregistrée dans la mémoire du premier terminal mobile de sorte qu'il n'est pas possible de construire ce premier cryptogramme (KCpub) seulement à partir des informations contenues dans la mémoire de ce premier terminal mobile,
- le premier terminal mobile étant configuré pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la première serrure électronique dans son état déverrouillé, :
1) le premier terminal mobile reçoit l'identifiant de serrure (Cpub) contenu dans la mémoire de la première serrure électronique,
2) en réponse, le premier terminal mobile recherche dans sa mémoire s'il existe un premier cryptogramme (KCpub) associé à l'identifiant de serrure reçu, et
3) lorsqu'un tel premier cryptogramme (KCpub) est trouvé dans la mémoire du premier terminal mobile, alors le premier terminal mobile transmet à la première serrure électronique une première trame (T_{180}) d'informations contenant son identifiant de terminal (Kpub),
caractérisé en ce que :
- la mémoire du premier terminal mobile comporte une deuxième clé de chiffrement (Kaes) différente de la première clé de chiffrement (Caes),
- le premier terminal est configuré pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la seconde serrure électronique dans son état déverrouillé :
5) le premier terminal reçoit de la seconde serrure électronique son identifiant de serrure (Cpub),
6) en réponse, le premier terminal mobile recherche dans sa mémoire un premier cryptogramme associé à l'identifiant de serrure reçu, puis
7) lorsque aucun premier cryptogramme associé à l'identifiant de serrure

reçu n'est trouvé dans la mémoire du premier terminal mobile :
- le premier terminal mobile construit un quatrième cryptogramme (KKpub') à partir de l'identifiant de serrure (Cpub) reçu, de son identifiant de terminal (Kpub) contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le troisième cryptogramme (KKpub) paramétré par la deuxième clé de chiffrement (Kaes) contenue dans la mémoire de ce premier terminal mobile, puis
- le premier terminal mobile transmet à la seconde serrure électronique une seconde trame (T_{182}) d'informations, à la place de la première trame (T_{180}) d'informations, cette seconde trame d'informations contenant l'identifiant de terminal (Kpub) du premier terminal et une signature numérique (S_{182}) construite à partir du quatrième cryptogramme (KKpub') construit.

[Revendication 10] Premier terminal selon la revendication 9, dans lequel l'identifiant de terminal (Kpub) de ce terminal mobile est enregistré dans une zone non-réinscriptible de sa mémoire.

[Revendication 11] Ensemble d'une première et d'une seconde serrures électroniques pour la réalisation d'un système de contrôle d'accès à des bâtiments conforme à la revendication 8, dans lequel la première et la seconde serrures électroniques (10) sont chacune déplaçables entre :
- un état verrouillé dans lequel elle interdit l'accès au bâtiment, et
- un état déverrouillé dans lequel elle autorise l'accès au bâtiment,
chacune des première et seconde serrures électroniques comportant un microprocesseur (108) et une mémoire (110) contenant un identifiant de serrure (Cpub) qui identifie de façon unique cette serrure électronique parmi l'ensemble des serrures électroniques du système de contrôle d'accès et une première clé de chiffrement (Caes), et
- la première serrure électronique est configurée pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la première serrure électronique dans son état déverrouillé, :
4) en réponse à la réception de la première trame d'informations (T_{180}), la première serrure électronique :
- construit un deuxième cryptogramme (KCpub') à partir de l'identifiant de terminal (Kpub) contenu dans la première trame d'informations, de son identifiant de serrure (Cpub) contenu dans sa mémoire et en mettant en œuvre le même algorithme de chiffrement prédéterminé que celui mis en œuvre pour construire le premier cryptogramme (KCpub)

paramétré par la clé (Caes) contenue dans la mémoire de la première serrure électronique, puis
- la première serrure électronique vérifie que le deuxième cryptogramme (KCpub') construit est identique au premier cryptogramme (KCpub), et
- dans le cas où les premier et deuxième cryptogrammes (KCpub, KCpub') sont identiques, la première serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les premier et deuxième cryptogrammes (KCpub, KCpub') sont différents, le déplacement de la première serrure électronique depuis son état verrouillé vers son état déverrouillé est interdit,
caractérisé en ce que :
- la seconde des serrures électroniques est autorisée à être déplacée dans son état déverrouillé par le premier terminal mobile, la mémoire de cette seconde serrure électronique contenant un troisième cryptogramme (KKpub) construit à partir de l'identifiant (Cpub) de cette seconde serrure électronique, de l'identifiant de terminal (Kpub) du premier terminal mobile et en mettant en œuvre un algorithme de chiffrement prédéterminé paramétré par la deuxième clé de chiffrement (Kaes) du premier terminal mobile,
la deuxième clé de chiffrement (Kaes) du premier terminal mobile n'étant pas enregistrée dans la mémoire de la seconde serrure électronique de sorte qu'il n'est pas possible de construire le troisième cryptogramme seulement à partir des informations contenues dans la mémoire de cette seconde serrure électronique, et
- la seconde serrure électronique est configurée pour exécuter les étapes suivantes à chaque fois que le premier terminal mobile souhaite déplacer la seconde serrure électronique dans son état déverrouillé :
5) la seconde serrure électronique transmet au premier terminal mobile son identifiant de serrure (Cpub), puis
8) en réponse à la réception de la seconde trame d'informations (T_{182}), la seconde serrure électronique vérifie (232) que le troisième cryptogramme (KKpub) enregistré dans sa mémoire est identique au quatrième cryptogramme (KKpub'), et
9) dans le cas où les troisième et quatrième cryptogrammes (KKpub, KKpub') sont identiques, la seconde serrure électronique est autorisée à se déplacer dans son état déverrouillé et, dans le cas où les troisième et quatrième cryptogrammes (KKpub, KKpub') sont différents, le déplacement de la seconde serrure électronique depuis son état verrouillé

vers son état déverrouillé est interdit.

[Fig. 1]

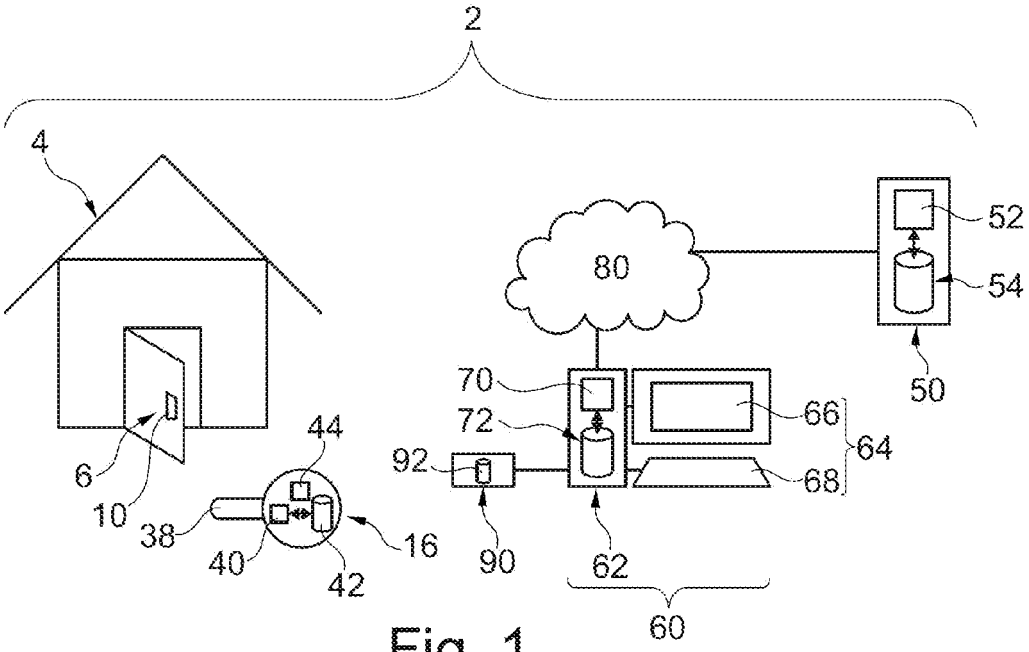


Fig. 1

[Fig. 2]

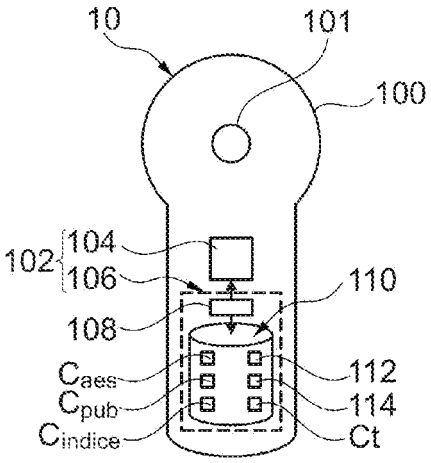


Fig. 2

[Fig. 3]

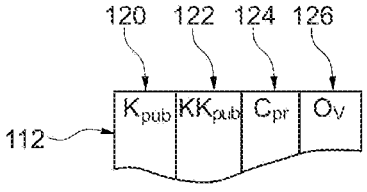


Fig. 3

[Fig. 4]

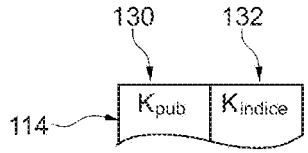


Fig. 4

[Fig. 5]

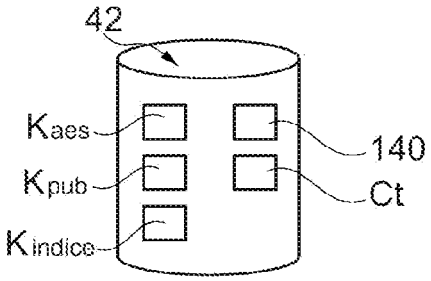


Fig. 5

[Fig. 6]

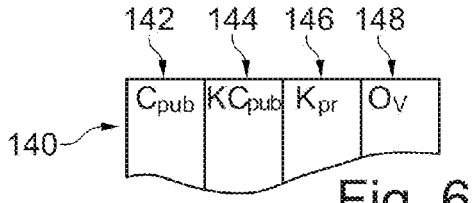


Fig. 6

[Fig. 7]

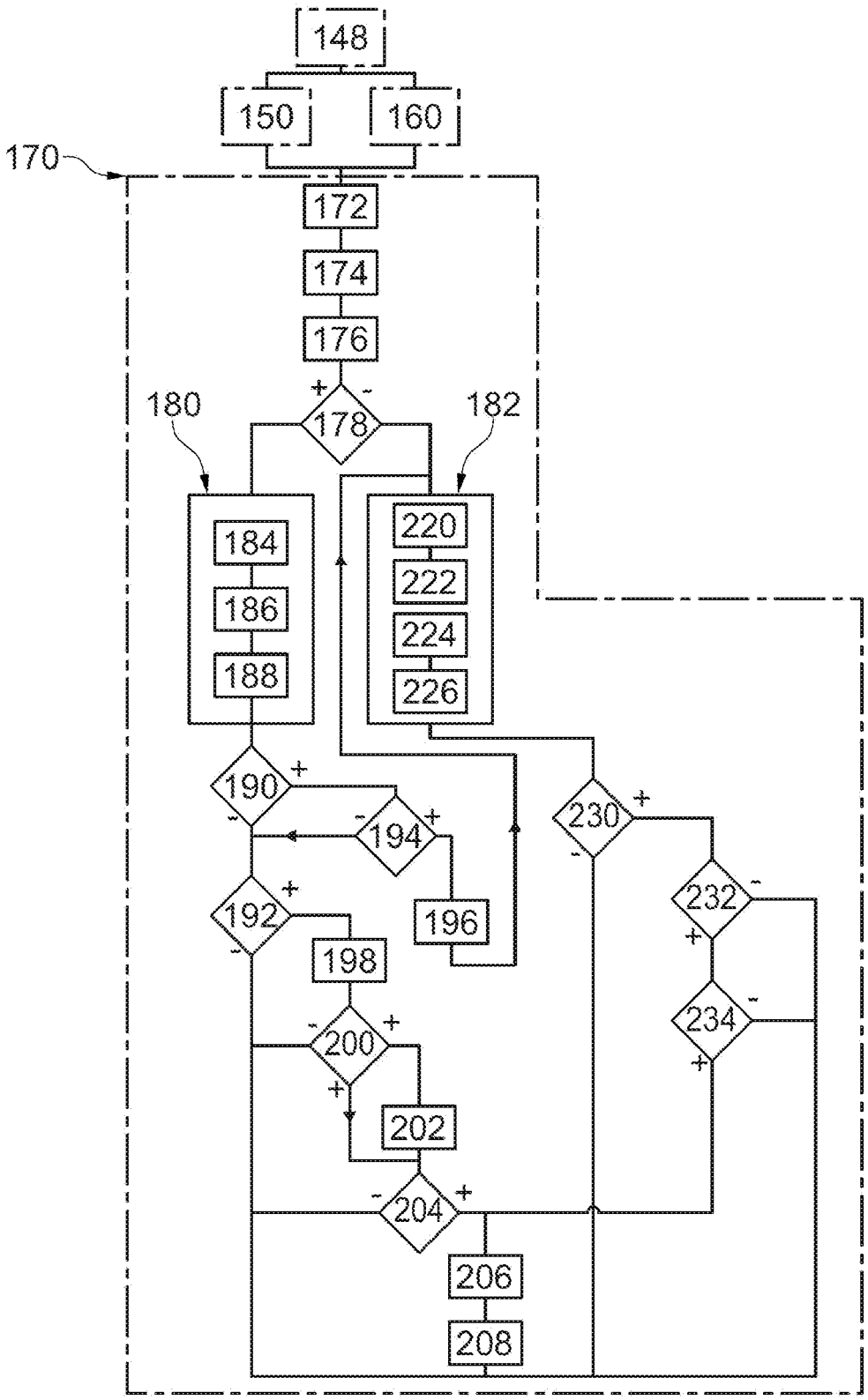

148
150
160
170
172
174
176
178
180
182
184
186
188
190
192
194
196
198
200
202
204
206
208
220
222
224
226
230
232
234

Fig. 7

[Fig. 8]

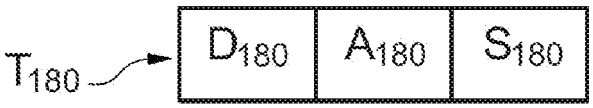


Fig. 8

[Fig. 9]

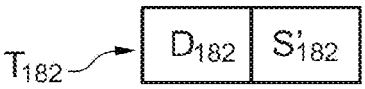


Fig. 9

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 904706
FR 2200949

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A,D	EP 1 321 901 A2 (KABA AG [CH]) 25 juin 2003 (2003-06-25) * abrégé; figures 1,2 * * alinéa [0001] - alinéa [0063] * -----	1-11	G07C9/00 E05B H04L9/32 H04L9/14 H04L9/30
A	WO 2016/023558 A1 (POLY CARE APS [DK]) 18 février 2016 (2016-02-18) * abrégé; figure 1 * * page 1, ligne 5 - page 1, ligne 6 * * page 2, ligne 19 - page 18, ligne 11 * -----	1-11	G06F21/33

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

H04L
G07C
E05B
G06F

Date d'achèvement de la recherche	Examinateur
19 septembre 2022	Holzmann, Wolf

CATÉGORIE DES DOCUMENTS CITÉS

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 bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2200949 FA 904706

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **19-09-2022**
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1321901 A2	25-06-2003	AT 463810 T	15-04-2010
		EP 1321901 A2	25-06-2003
WO 2016023558 A1	18-02-2016	AUCUN	

EPO FORM P0465