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

(11) EP 1 653 415 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
03.05.2006 Bulletin 2006/18

(21) Numéro de dépôt: **05292321.6**

(22) Date de dépôt: **28.10.2005**

(51) Int Cl.:
G07C 9/00 *(2006.01)* ***H04L 9/32*** *(2006.01)*
G06K 19/07 *(2006.01)*

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

(30) Priorité: **29.10.2004 FR 0411585**

(71) Demandeur: **Immotec Systems**
94042 Creteil Cedex (FR)

(72) Inventeur: **Jonquieres, Rémi**
94100 Saint Maur des Fosses (FR)

(74) Mandataire: **Debay, Yves**
Cabinet Debay,
126 Elysée 2
78170 La Celle Saint Cloud (FR)

(54) Procédé et équipement de gestion de badges de contrôle d'accès

(57) L'invention consiste à pourvoir des bornes de contrôle d'accès (2, 3, 10) non seulement de la fonction de lecture d'un badge mais aussi de celle d'écriture, les bornes mémorisant en association avec l'identifiant du badge (4) les données associées (nom du porteur, droit d'accès, profil des usagers) et l'indice de perte. Ces informations contenues dans les bornes (2, 3, 10) sont utilisées lors de la présentation d'un badge (4). Si l'indice de perte lu dans le badge révèle que le nombre de déclarations de perte est inférieur à celui prévu selon l'indice de perte mémorisé par la borne, l'indice de perte du badge est effacé par la borne. Si ce nombre de déclarations de perte est en revanche supérieur, il est procédé à une modification pour tenir compte du nouvel indice de perte.

L'équipement doté de telles bornes permet la réalisation de mises à jour des données de badge.

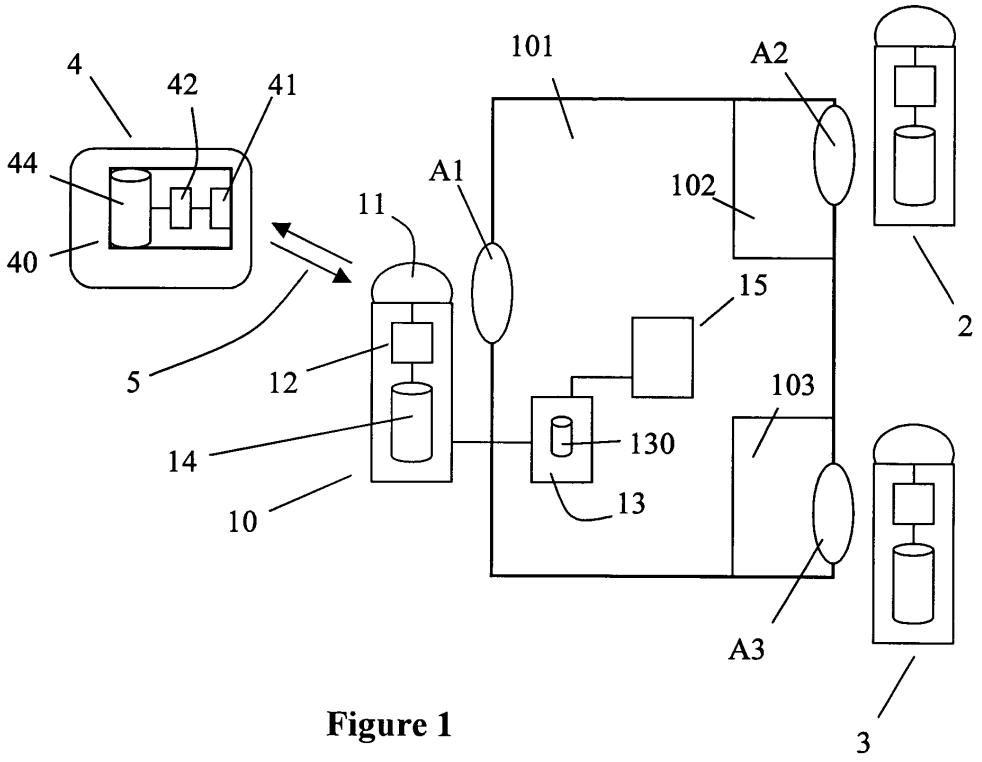

Figure 1

EP 1 653 415 A1

Description

[0001] La présente invention concerne le contrôle d'accès, et plus particulièrement un procédé et un équipement de gestion de badges de contrôle d'accès par utilisation de phases de lecture-écriture.

[0002] Dans l'art antérieur, sont apparus des badges sans contact à lecture-écriture pouvant à la fois être lus à distance par un appareil lecteur mais aussi susceptibles sous certaines conditions de pouvoir être reprogrammés. Des modifications dans la programmation des badges peuvent être notamment effectuées en utilisant le logiciel Residor de chez Immotec Systèmes et les terminaux tels que le Palm Pilot ou autre PDA (Personal Digital Assistant) ou encore l'encodeur de badges sans contact Mifare®.

[0003] La technologie de ces badges, qualifiés également de "transpondeurs", est basée sur un dialogue radio dans des fréquences typiques de 125 kHz pour les badges les plus courants (pouvant être lus mais non écrits) et de 13,56 MHz pour les badges à lecture-écriture. Une norme ISO 14 443 décrit le principe de ces badges dont la fréquence et le débit de communication permet un transfert de données généralement suffisant pour la plupart des applications actuelles.

[0004] Il est connu des méthodes de contrôle d'accès avec invalidation du badge perdu, nécessitant la mise en place d'un réseau câblé. Pour invalider un badge, ces méthodes prévoient l'obligation de devoir accéder à tous les lecteurs ; chaque lecteur reconnaissant séparément l'invalidation du badge. Ces méthodes reposent pour la plupart sur des indices de perte : lorsqu'un badge est perdu, le badge nouvellement créé possède un indice de perte incrémenté de un. Lorsque l'usager l'utilise, il indique au lecteur de badge que l'ancien badge, à l'indice inférieur, doit être refusé s'il est présenté devant le lecteur par une personne l'ayant retrouvé.

[0005] L'inconvénient de ce procédé est qu'il est nécessaire de présenter le nouveau badge sur chacun des lecteurs concernés si l'on veut être sûr que l'ancien badge ne fonctionnera sur aucun d'entre eux. Et dans le cas de sites importants avec de nombreuses portes, cette tâche peut s'avérer très longue et rébarbative. Il peut en résulter une sécurisation insuffisante par ces méthodes classiques.

[0006] Il est également connu, par le document WO 02/091311, une méthode de contrôle d'accès de cartes à puce permettant d'éviter aux bornes d'accès de communiquer avec un ordinateur central et de minimiser le coût et la gestion de l'ensemble du système. Toutefois les bornes d'accès utilisent de nombreuses informations devant régulièrement être mises à jour, comme par exemple des données d'identification et des listes noires de cartes interdites d'accès. L'invalidation de cartes à puce ne peut alors pas être effectuée de façon très efficace sans nécessiter des lecteurs de carte à puce sophistiqués.

[0007] La présente invention a donc pour objet de pallier un ou plusieurs des inconvénients de l'art antérieur en définissant un procédé de gestion de badges de contrôle d'accès sans contact offrant une sécurisation optimale et permettant de modifier aisément les informations du badge notamment relatives aux autorisations d'accès.

[0008] A cet effet, l'invention concerne un procédé de gestion de badges de contrôle d'accès destiné à faciliter la mise à jour d'informations sur des badges sans contact incluant chacun une puce électronique dotée d'un organe de communication radio ou optique, utilisant un équipement d'accès comportant plusieurs bornes de contrôle d'accès munies chacune de moyens de communication radio ou optique permettant au moins de lire des donnés de la puce du badge, au moins une base de données étant à la disposition de chaque borne de contrôle d'accès, procédé dans lequel au moins une communication sans contact radio ou optique est établie entre une des bornes de contrôle d'accès et un badge sans contact, ladite communication sans contact comprenant une étape d'authentification du badge par lecture de données d'identification stockées dans la puce du badge, caractérisé en ce que ladite communication sans contact comporte :

- une étape de lecture, par les moyens de communication de la borne de contrôle d'accès, d'un indice de perte de la puce du badge représentatif d'un nombre de déclarations de perte pour le badge authentifié ;
- une étape de comparaison réalisée par un module de gestion installé dans la borne de contrôle d'accès pour comparer ledit indice de perte avec un indice de perte analogue stocké dans ladite base de données correspondant au badge authentifié ; et
- si l'étape de comparaison révèle que l'indice de perte lu sur la puce du badge représente un nombre de déclarations de perte supérieur à celui prévu selon l'indice de perte de la base de données, une étape de modification de la base de données pour tenir compte de l'indice de perte lu sur le badge authentifié ; et
- si l'étape de comparaison révèle que l'indice de perte lu sur la puce du badge représente un nombre de déclarations de perte inférieur à celui prévu selon l'indice de perte de la base de données, une étape de modification et/ou effacement de données de la puce du badge pour invalider le badge.

[0009] Selon une autre particularité de l'invention, si l'étape de comparaison révèle que l'indice de perte lu sur la puce du badge représente un nombre de déclarations de perte supérieur ou égal à celui prévu selon l'indice de perte de la base de données, ladite communication sans contact comporte :

- une étape de lecture, par les moyens de communication de la borne de contrôle d'accès, de données de profil mémorisées par la puce du badge repré-

sentatives d'un profil d'utilisation du badge ;

- une étape de comparaison réalisée par le module de gestion pour comparer les données de profil lues avec des données de profil correspondant aux données d'identification dans ladite base de données ; et
- en cas de non correspondance entre données de profil comparées, une étape de modification des données sur la puce utilisant en premier lieu ledit module de gestion et lesdits moyens de communication pour transmettre à la puce du badge les données de profil considérées comme nouvelles et utilisant en second lieu des moyens d'écriture de ladite puce pour remplacer les données de profil stockées dans une mémoire de la puce par les données nouvelles transmises via les moyens de communication de la borne de contrôle d'accès.

[0010] Ainsi, il peut être avantageusement procédé à des modifications de données du badge pour par exemple mettre à jour ou invalider un badge actif utilisé dans un système de contrôle d'accès.

[0011] Selon une autre particularité de l'invention, l'étape d'authentification du badge comprend une étape de lecture utilisant les moyens de communication de la borne de contrôle d'accès pour lire des données d'identification associées à une signature sur la puce du badge et une étape de comparaison entre signatures utilisant le module de gestion installé dans la borne de contrôle d'accès pour comparer les données de signature calculée par la borne avec les données de signature transmises depuis la puce.

[0012] Selon une autre particularité, chacun des badges sans contact est initialisé par un appareil encodeur de badges lors d'une étape de personnalisation, l'appareil encodeur transmettant dans une mémoire non volatile reprogrammable de la puce du badge au moins une donnée d'identification du badge et des données de profil représentatives d'un profil d'utilisation du badge.

[0013] Selon une autre particularité, une étape de cryptage est réalisée par l'appareil encodeur de badges pour stocker au moins une donnée d'identification du badge sous la forme d'une signature cryptée dans une zone mémoire du badge sans contact.

[0014] Selon une autre particularité, ladite étape d'authentification du badge comprend une émission préalable depuis la borne de contrôle à destination du badge d'une requête d'envoi d'une donnée d'identification du badge, la communication sans contact s'établissant entre borne et badge sans contact en cas de réception par le badge de ladite requête. L'étape d'authentification du badge comprend ensuite la réception de ladite donnée d'identification avec sa signature associée, la lecture de la donnée d'identification du badge par le module de gestion de la borne de contrôle d'accès, au moins une clé associée à ladite donnée d'identification étant utilisée par le module de gestion pour d'une part calculer ladite signature calculée à partir de la signature transmise par le badge en réponse à ladite requête, et d'autre part comparer ladite signature calculée avec la signature transmise par le badge avec ladite donnée d'identification en réponse à ladite requête.

[0015] Selon une autre particularité, le procédé selon l'invention comporte une étape de chiffrage utilisant une clé de lecture stockée dans un secteur de la mémoire du badge pour chiffrer des informations dudit secteur avant la transmission des ces informations à une borne de contrôle d'accès et une étape de déchiffrage utilisant une clé d'écriture stockée dans un secteur pour déchiffrer les informations reçues d'une borne et destinées audit secteur, la mémoire du badge comprenant un nombre déterminé de secteurs incluant chacun une clé de lecture et une clé d'écriture.

[0016] Selon une autre particularité, un arrêt de la communication sans contact est déclenché par l'intermédiaire du module de gestion et des moyens de communication de la borne lorsque la comparaison entre signatures ne donne aucun résultat.

[0017] Selon une autre particularité, chaque étape de modification de données sur la puce comprend une étape de transmission par la borne vers la puce du badge d'une information chiffrée avec une clé correspondant à un secteur déterminé de la mémoire du badge puis une étape de déchiffrement utilisant une clé d'écriture associée au secteur déterminé de la mémoire du badge pour déchiffrer l'information correspondant à ce secteur.

[0018] Selon une autre particularité, les données de profil de la base de données sont mises à jour par l'intermédiaire d'un module de mise à jour de données de profil.

[0019] Selon une autre particularité, le module de mise à jour fournit, pour chacun des badges sans contact, des données d'identification de badge et des données de profil à une base de données locale d'au moins une borne de contrôle d'accès.

[0020] Selon une autre particularité, la communication est du type radio et s'effectue à une fréquence déterminée dans une zone restreinte ayant un rayon inférieur à 12 mètres autour des moyens de communication de la borne de contrôle d'accès.

[0021] Un autre but de l'invention est d'apporter une solution à un ou plusieurs des problèmes rencontrés dans l'art antérieur en définissant un équipement de gestion de badges de contrôle d'accès sans contact permettant de modifier des paramètres des badges de façon automatique.

[0022] Ce but est atteint par un équipement de gestion de badges sans contact pour du contrôle d'accès, destiné à faciliter la mise à jour d'informations contenues dans une puce électronique des badges, comportant plusieurs bornes de contrôle d'accès munies chacune de moyens de communication radio ou optique permettant de lire des donnés de la puce d'un badge, caractérisé en ce qu'il comprend :

- un module de mise à jour de données de badge représentatives notamment d'une identification et d'un

indice de perte, agencé pour fournir à au moins une base de données des données mises à jour, à chaque badge géré par ledit équipement étant associé un unique jeu de données de badge ;

- un module de gestion installé dans chaque borne de contrôle d'accès et associé aux moyens de communication de la borne pour comparer des données de badge lues par les moyens de communication avec des données de badge associées stockées dans la base de données, le module de gestion incluant des moyens de sélection pour sélectionner dans la base de données les données associées à un badge déterminé, et des moyens de décision du remplacement d'au moins une partie des données dudit badge déterminé ; et
- des moyens de transmission dans lesdits moyens de communication de chaque borne de contrôle d'accès pour transmettre à une puce d'un badge des données de remplacement sélectionnées par l'intermédiaire du module de gestion, le module de gestion étant agencé pour effacer au moins un champ de données de façon à invalider un badge par transmission parmi lesdites données de remplacement d'au moins un champ de données correspondant à l'effacement de l'indice de perte du badge.

[0023] Selon une autre particularité, les données de badge comportent des données de profil représentatives d'un profil d'utilisation du badge.

[0024] Selon une autre particularité, les données de profil sont au moins une des informations suivantes :

- le(s) numéro(s) d'un ou plusieurs sites autorisés ;
- le nom de l'usager ;
- le numéro d'appartement ;
- la catégorie du personnel ou le niveau hiérarchique ;
- les droits d'accès,
- le numéro de badge,
- l'indice de perte ;
- les dates de validité ;

chacune de ces informations étant destinée à un secteur spécifique de la mémoire du badge utilisant une clé d'écriture ou de lecture associée.

[0025] Selon une autre particularité, un appareil encodeur de badges est prévu pour initialiser et personnaliser chacun des badges sans contact, l'appareil encodeur disposant de moyens d'émission pour transmettre dans une mémoire de la puce d'un badge au moins une donnée d'identification du badge et des données de profil représentatives d'un profil d'utilisation du badge.

[0026] Selon une autre particularité, les moyens de communication sont reliés au module de gestion pour, d'une part émettre par l'intermédiaire desdits moyens de transmission une requête d'identification de badge, et d'autre part recevoir au moins une donnée d'identification d'un badge.

[0027] Selon une autre particularité, le module de gestion comporte des moyens de décryptage et de lecture du type utilisant au moins une clé pour décrypter une donnée d'un secteur cryptée reçue par les moyens de communication de la borne.

[0028] Selon une autre particularité, des moyens interactifs incluant une interface de saisie sont reliés au module de mise à jour pour permettre la saisie de données d'accès, le module de mise à jour comprenant dans des moyens de mémorisation, pour chacun des badges gérés par l'équipement, une table de données d'accès représentatives d'autorisations d'accès correspondant spécifiquement à des bornes définies de l'équipement.

[0029] Selon une autre particularité, le module de mise à jour est doté de moyens de mémorisation permettant de stocker une base de données centrale rassemblant pour chacun des badges sans contact des données d'identification de badge et des données de profil, ladite base de données centrale étant reliée à une pluralité de bornes de contrôle d'accès.

[0030] Selon une autre particularité, chacune des bornes de contrôle d'accès comporte une base de données locale, le module de mise à jour étant relié à chacune desdites bases de données locales.

[0031] L'invention, avec ses caractéristiques et avantages, ressortira plus clairement à la lecture de la description faite en référence aux dessins annexés dans lesquels :

- les figures 1 et 2 représentent une vue d'ensemble schématique d'un équipement selon l'invention avec respectivement un réseau non câblé et un réseau câblé ;
- la figure 3 présente un type de communication permis par l'équipement dans un mode de réalisation de l'invention ;
- la figure 4 représente schématiquement le principe d'autorisation d'accès d'un badge en fonction d'un indice de perte ;
- la figure 5 représente schématiquement une mémoire d'un badge utilisé dans un mode de réalisation de l'invention,
- la figure 6 représente un logigramme correspondant à un mode de réalisation du procédé selon l'invention.

[0032] L'invention va être à présent décrite en référence aux figures 1 et 2. Le type de fréquence utilisée pour les communications radio est de préférence celui spécifié dans la norme ISO 14 443, s'élevant à 13,56 MHz. Le badge est alimenté par l'énergie du message transmis à une telle fréquence, aucune batterie n'étant alors nécessaire. L'invention peut être également transposée à d'autres fréquences radioélectriques pour lesquelles des badges auraient été conçus ou encore pour des modes de communication optique.

[0033] Le procédé de gestion de badges de contrôle d'accès selon l'invention présente la particularité de faciliter l'invalidation de badges perdus ainsi que la mise

à jour d'informations sur des badges sans contact (4) en utilisant une fonctionnalité de lecture-écriture disponible pour ces badges. Chacun de ces badges (4) comporte dans une puce (40) une mémoire (44) non volatile reprogrammable de type EEPROM (Electrically Erasable Programmable Read Only Memory) ou une mémoire flash. Au moins une donnée d'identification du badge (4) et des données de profil représentatives d'un profil d'utilisation du badge (4) sont mémorisées dans cette mémoire (44) de la puce (40).

[0034] Le procédé de l'invention propose de modifier certaines de ces données, par exemple en effaçant des données nécessaires pour l'obtention d'une autorisation d'accès pour des badges identifiés comme ayant été perdus ou volés. En référence aux figures 1 et 2, l'équipement (1) de gestion de badges (4) comporte plusieurs bornes de contrôle d'accès (2, 3, 10, 20, 30) munies chacune de moyens de communication radio (11) permettant de lire des donnés de la puce (40) d'un badge (4). Dans un mode de réalisation, un module de mise à jour (13) de données de badge prévu pour fournir à au moins une base de données (14) notamment des données de profil mises à jour. Les données de profil représentatives d'un profil d'utilisation du badge ainsi que des données d'identification et d'indice de perte du badge peuvent être mémorisées de la même façon dans la base de données, avec une mise à jour réalisée par le module (13) de mise à jour. Il est donc permis avec ce module (13) de mettre à jour par exemple des données d'accès à certaines des bornes (10, 20, 30). Dans un mode de réalisation préféré de l'invention, un unique jeu de données de profil est associé à chaque badge (4) géré par ledit équipement (1).

[0035] Le module de mise à jour (13) peut être doté de moyens de mémorisation (130) permettant de stocker une base de données rassemblant pour chacun des badges sans contact (4) des données d'identification de badge et des données de profil. Cette base de données peut être centrale et reliée à une pluralité de bornes de contrôle d'accès (10, 20, 30), ce qui permet de concentrer par exemple dans un même lieu une pluralité de bornes de contrôle d'accès (10, 20, 30). Afin de faciliter la mise à jour d'informations contenues dans la puce électronique des badges, chaque borne de contrôle d'accès (10) peut être dotée d'un module de gestion (12) associé aux moyens de communication radio (11). Il est permis grâce à ce module de gestion (12) installé dans la borne (10) de comparer des données de profil d'un badge (4) lues par les moyens de communication radio (11) avec des données de profil associées à ce badge (4) stockées dans ladite base de données (14). Dans le mode de réalisation des figures 1 et 2, les bornes de contrôle d'accès (2, 3, 10, 20, 30) comprennent une base de données locale (14) incluant lesdites données de profil ainsi que des données permettant d'identifier les badges (4), par exemple sous la forme d'une table d'authentification. L'équipement (1) peut aussi comporter une unique base de données centralisée comprenant une liste de données d'identification des badges (4) du type numéro de série ou analogue et une table de correspondance entre ces numéros et des autorisations pour différents contrôles d'accès (A1, A2, A3). Cette base de données centralisée est stockée dans les moyens de mémorisation (130) du module de mise à jour (13).

[0036] Dans l'exemple de la figure 1, des zones distinctes (101, 102, 103) ont chacune un accès (A1, A2, A3) différent. L'utilisation de l'équipement (1) permet d'affecter à un utilisateur des autorisations d'accès pour une seule ou pour plusieurs de ces zones (101, 102, 103). Chaque borne (2, 3, 10) affectée à une des ces zones peut disposer par exemple d'une base de données locale (14). Lorsque les accès (A1, A2, A3) sont utilisés pour le contrôle d'une même zone (100) comme illustré à la figure 2, il peut être envisagé soit de relier par un réseau (6) les bornes (10, 20, 30) au module de mise à jour (13), soit de relier une ou quelques bornes (10) contrôlant un accès principal (porte principale d'accès).

[0037] Les moyens interactifs (15) illustrés dans les figures 1 et 2 permettent la saisie de données d'accès, un opérateur pouvant utiliser une interface de saisie de ces moyens interactifs (15) pour modifier certaines données ou pour supprimer/créer des nouveaux droits d'accès. Ces moyens interactifs (15) sont reliés au module de mise à jour (13). Les moyens de mémorisation (130) de ce module (13) stockent, pour chacun des badges (4) gérés par l'équipement (1), une table de données d'accès représentatives d'autorisations d'accès. Pour chaque badge (4), les autorisations correspondent alors spécifiquement à des accès bien définis contrôlés par des bornes définies de l'équipement (1). Les possibilités d'accès peuvent donc varier en fonction du profil de l'utilisateur.

[0038] Dans un mode de réalisation de l'invention, le module de gestion (12) de chaque borne (10, 20, 30) comporte des moyens de sélection pour sélectionner dans la base de données (14) à la disposition de la borne, les données associées à un badge déterminé. Le module (12) comporte en outre des moyens de décision du remplacement d'au moins une partie des données dudit badge déterminé (4).

[0039] Autrement dit, pour les opérations de modification du paramétrage d'un badge (4), une borne de contrôle d'accès (10) dotée du module de gestion (12) et disposant d'une base de données (14) mise à jour par le module de mise à jour (13) peut servir à modifier sélectivement les données d'un ancien badge (4). Ainsi pour une opération d'invalidation d'un badge (4) perdu ou volé, l'équipement (1) selon l'invention est apte à effacer sélectivement les donnés du badge (4) ou bien effectuer une régression d'indice de perte. Pour cela, des moyens de transmission sont prévus dans les moyens de communication radio (11) de chaque borne de contrôle d'accès pour notamment assurer la transmission vers la puce (40) d'un badge de données de remplacement sélectionnées par l'intermédiaire du module de gestion (12). Pour initier la communication radio (5), les moyens de communication radio (11), reliés au module de gestion (12),

émettent par l'intermédiaire desdits moyens de transmission une requête d'identification/authentification de badge (4). Une telle requête peut être envoyée toutes les 2 à 7 secondes. Une ou plusieurs données d'identification d'un badge (4) peuvent être reçues via ces moyens de communication (11) et transmises au module de gestion (12). La communication radio (5) s'effectue à une fréquence déterminée dans une zone restreinte ayant par exemple un rayon inférieur à 12 mètres autour des moyens de communication radio (11) de la borne de contrôle d'accès (10, 20, 30).

[0040] En référence à la figure 4, le principe de l'indice de perte est illustré pour représenter une façon connue d'invalider un badge, en prenant l'exemple simple d'un usager ayant perdu un badge (4) qui lui permettait d'accéder à plusieurs bâtiments (B1, B2). Lorsque cet usager perd son badge (4), le gestionnaire utilise des moyens interactifs (15) et un appareil encodeur (17) pour lui en fournir un autre (4') qui possède un indice de perte incrémenté de un. Par la suite, l'usager passe son nouveau badge (4') sur les lecteurs (R) les plus utilisés, leur indiquant ainsi que le badge antérieur (4) a été égaré. Si une tierce personne retrouve cet ancien badge (4) et tente d'entrer dans un bâtiment (B1, B2) en "badgeant" un de ces lecteurs (R), il se verra certes refuser l'accès mais le badge ancien (4) reste susceptible d'autoriser l'accès via des lecteurs (R) qui n'ont pas lu le nouveau badge (4'). Pour remédier à ce type d'inconvénient, l'équipement (1) de l'invention met en oeuvre un processus différent : en effet, l'indice de perte est automatiquement effacé et l'ancien badge (4) ne pourra ouvrir aucun des autres accès qui lui étaient attribués, même ceux que l'usager n'avait pas validés avec son nouveau badge (4').

[0041] L'invention consiste pour cela à pourvoir les bornes de contrôle d'accès (10, 20, 30) non seulement de la fonction de lecture du badge mais aussi de celle d'écriture, les bornes (10, 20, 30) mémorisant en association avec l'identifiant du badge les données associées (nom du porteur, droit d'accès, profil des usagers incluant un profil horaire, etc.) et l'indice de perte. Ces informations contenues dans les bornes (10, 20,30) sont utilisées lors de la présentation d'un badge, et si l'indice de perte lu dans le badge (4) révèle que le nombre de déclarations de perte annoncé par le badge (4) est inférieur à celui prévu selon l'indice de perte de la base de données à la disposition de la borne, la borne efface par exemple l'indice de perte. Si en revanche, ce nombre de déclarations de perte est supérieur à celui prévu selon l'indice de perte de la base de données, il est procédé à une modification de la base de données (14) pour tenir compte de l'indice de perte lu sur le badge authentifié.

[0042] Il est entendu que l'équipement (1) peut comprendre des lecteurs (R) classiques et des bornes de contrôle d'accès (10, 20, 30) dotées du module de gestion (12) permettant la fonctionnalité de remplacement de données sur la puce (40) du badge (4). Ces bornes (10, 20, 30) peuvent être installées en priorité aux endroits les plus à même d'être utilisés par la personne qui aurait récupéré l'ancien badge (4) : par exemple une porte principale d'accès (A1).

[0043] Dans un mode de réalisation de l'invention, l'équipement (1) peut utiliser une technologie de type MIFARE® conforme à la norme ISO 14443 permettant de lire soit le numéro de série du badge, soit un numéro de badge contenu dans un des 16 secteurs (S) de la mémoire (44, figure 5) du badge (4). Dans ce dernier cas, le numéro de badge peut être crypté pour plus de sécurité. Chacun des badges sans contact (4) est initialisé par un appareil encodeur de badges (17) lors d'une étape de personnalisation qui peut inclure une phase de cryptage. L'appareil encodeur (17) transmet dans une mémoire (44) non volatile reprogrammable de la puce (40), par l'intermédiaire de moyens d'émission radio, au moins une donnée d'identification du badge (4) et des données de profil représentatives d'un profil d'utilisation du badge (4). L'appareil encodeur de badges (17) comprend par exemple un module de cryptage et est agencé pour transmettre sous la forme d'une signature cryptée au moins une donnée d'identification du badge (4) à destination d'une zone mémoire (442, figure 3) du badge sans contact (4).

[0044] Les badges sans contact (4) permettant la lecture et écriture intègrent en association avec leur organe de communication radio (41) des moyens d'écriture (42) disposés dans la puce électronique (40). Des données de profil nouvelles peuvent être transmises à la puce (40) du badge (4) et stockées en mémoire (44) par l'intermédiaire de ces moyens d'écriture (42) de façon à remplacer des données de profil obsolètes. Parmi les données de profil, un champ de données peut être prévu pour représenter l'indice de perte du badge (4). Dans la borne de contrôle d'accès (10), le module de gestion (12) est apte à effacer ce champ de données pour invalider le badge (4) par transmission parmi lesdites données de remplacement d'un champ de données représentant l'effacement de l'indice de perte du badge.

[0045] Dans le mode de réalisation de la figure 3, une zone mémoire (442) du badge sans contact (4) peut stocker une signature cryptée. La protection des données du badge (4) par utilisation d'une procédure d'authentification d'une signature cryptée fournit une forte sécurisation. Chaque badge (4) possède une zone mémoire (441) pour les données (nom du porteur, droits d'accès etc.) et une autre (442) pour une signature cryptée. Cette signature est un code généré à l'aide d'un algorithme RSA ou autre algorithme de signature à partir des données d'identification du badge (ces données étant enregistrées dans le badge). L'algorithme RSA est un procédé complexe qui utilise les données du badge (4), une clé publique enregistrée dans un système central de l'équipement (1) et une clé secrète que seul le prestataire de l'équipement (1) possède. Ainsi, lorsqu'un usager passe son badge (4) devant une borne de contrôle d'accès (10), le module de gestion (12) de cette borne (10) procède au décryptage de la signature par algorithme inverse, et compare ce qui est obtenu avec les données effective-

ment enregistrées dans le badge (4). Si les deux informations ne sont pas strictement identiques, la borne (10) refuse l'accès à l'usager.

[0046] Dans l'exemple de la figure 3, le module de gestion (12) peut disposer de moyens de décryptage et de lecture du type utilisant au moins une clé pour décrypter une donnée d'identification cryptée reçue par les moyens de communication radio (1). Les moyens de décryptage peuvent être inclus dans le module de gestion (12) ou fournis depuis un système central. En référence à la figure 3, le module de gestion (12) compare lors de la communication radio (5) la donnée d'identification décryptée avec des données d'identification de badge associées à ladite borne de contrôle d'accès (10) dans la base de données (14).

[0047] Un autre type de protection avec sécurisation par clé peut être utilisé. La mémoire de chaque badge, par exemple du type EEPROM, peut être composée de 16 secteurs (S) comme montré sur la figure 5. Chacun des secteurs (S) est muni d'une clé codée (Kr) sur par exemple 6 octets en lecture et d'une autre clé (Kw) en écriture. Dans un mode de réalisation de l'invention, seuls un système central relié aux bornes (10, 20, 30) et l'appareil encodeur (17) détiennent ces clés (qui leur permettent d'identifier le badge), de sorte qu'une personne malveillante ne peut pas se les procurer. On comprend qu'il est possible de réaliser un chiffrage par utilisation d'une clé de lecture (Kr) stockée dans un secteur (S) de la mémoire (44) du badge (4) pour chiffrer des informations dudit secteur (S) avant la transmission des ces informations à une borne de contrôle d'accès (10) et de réaliser un déchiffrage par utilisation d'une clé d'écriture (Kw) stockée dans un secteur (S) pour déchiffrer les informations reçues d'une borne (10) et destinées audit secteur (S).

[0048] Un exemple de processus de gestion de badges selon l'invention va à présent être décrit en référence aux figures 1 et 6.

[0049] Dans l'exemple de la figure 1, les badges (4) contiennent en mémoire (44) les informations nécessaires à un contrôle d'accès optimal et peuvent être de plusieurs types (Résidant, Pass, Tertiaire) ayant chacun leurs caractéristiques propres : on en retiendra à titre d'exemple non limitatif quelques-unes comme le numéro du ou des sites, le nom de l'usager, le numéro d'appartement, la catégorie du personnel ou le niveau hiérarchique, les droits d'accès, le numéro de badge, l'indice de perte, les dates de validité. Chacune de ces informations est destinée à un secteur (S) spécifique de la mémoire (44) du badge (4) utilisant une clé d'écriture (Kw) ou de lecture (Kr) associée. Les données des badges (4), principalement les données de profil usagers, les profils horaires et les droits d'accès aux portes, sont couramment modifiées. Les opérations de modification sont simplifiées grâce à l'invention.

[0050] En référence à la figure 6, l'étape (50) d'authentification du badge (4) par la borne de contrôle d'accès (10) débute par une émission préalable (500) depuis la borne de contrôle (10) à destination du badge (4) d'une requête d'envoi d'au moins une donnée d'identification du badge (4), la communication radio (5) s'établissant entre borne (10) et badge sans contact (4) en cas de réception par le badge (4) de ladite requête. Après que la donnée d'identification requise a été transmise (501) par le badge (4) en réponse à ladite requête, l'étape (50) d'authentification du badge se poursuit avec la réception (502) de ladite donnée d'identification avec sa signature associée, et la lecture (503) de la donnée d'identification du badge (4) par le module de gestion (12) de la borne de contrôle d'accès (10). Au moins une clé associée à ladite donnée d'identification est utilisée par le module de gestion (12) pour d'une part calculer (504) ladite signature calculée à partir de la signature transmise par le badge (4) en réponse à ladite requête, et d'autre part comparer (505) ladite signature calculée avec la signature transmise par le badge (4) avec ladite donnée d'identification en réponse à ladite requête. La comparaison (505) par le module de gestion (12) achève l'étape (50) d'authentification. Lorsque la comparaison (505) avec les données d'identification de base de données (14) ne donne aucun résultat, un arrêt (506) de la communication radio (5) est déclenché par l'intermédiaire du module de gestion (12) et des moyens de communication radio (11) de la borne de contrôle d'accès (10).

[0051] De manière conventionnelle, en cas d'identification du badge lors de l'étape (50) d'identification, le déblocage d'un accès (A1, A2, A3) peut être actionné par l'intermédiaire d'un signal de commande provenant du module de gestion (12) à destination d'un dispositif de blocage/déblocage d'accès. Dans le cas contraire, aucun signal de commande n'est envoyé et l'accès est refusé.

[0052] Dès que l'authentification du badge (4) est réalisée, le procédé selon l'invention prévoit une étape (51) de lecture de l'indice de perte déclaré par le badge (4). Le module de gestion (12) peut effacer le champ de données correspondant à l'indice de perte du badge lors d'une étape (54) d'invalidation de badge (4) si une étape (52) préalable de comparaison révèle une différence pour ce champ de données.

[0053] Une étape (53) de mémorisation d'un nouvel indice de perte est réalisée lorsque la borne (10) lit pour la première fois un badge de remplacement d'un badge perdu. Après le contrôle portant sur l'indice de perte du badge, si le badge authentifié (4) n'est pas un badge déclaré perdu/remplacé, la communication (5) se poursuit avec une étape (510) de lecture, par les moyens de communication (11) de la borne de contrôle d'accès (10), des données de profil stockées dans la puce (40). Une étape (520) de comparaison est ensuite réalisée par le module de gestion (12) de la borne de contrôle d'accès (10) pour comparer les données de profil lues avec des données de profil correspondant aux données d'identification dans la base de données (14). Si cette étape (520) de comparaison révèle au moins une différence, il s'ensuit une étape (540) de modification de données sur la

puce (40) utilisant en premier lieu le module de gestion (12) et les moyens de communication radio (11) pour transmettre (541) à la puce (40) du badge des données de profil considérées comme nouvelles et en second lieu des moyens d'écriture (42) de ladite puce (40) pour remplacer (542) des données de profil stockées dans une mémoire (44) de la puce (40) par les nouvelles données transmises via les moyens de communication radio (11) de la borne de contrôle d'accès (10). La base de données servant à stocker les données associées aux badges (4) peut être locale ou distante (base de données centralisée).

[0054] En variante, ladite étape (520) de comparaison peut consister en la consultation par le module de gestion (12) d'une donnée d'indication de la nécessité de modifier les données du badge (4). Cette donnée d'indication peut être par exemple un bit 0 si le système central n'a constaté aucune mise à jour effectuée depuis le dernier "badgeage" et un bit de 1 si au contraire des nouvelles données ont été saisies dans la base de données stockant les données de profil.

[0055] L'invention permet donc de réaliser plus rapidement et plus simplement les opérations comme le changement du nom de l'usager, de la date de validité du badge, le calcul des temps de présence, ou bien la mise en accès temporaire ou définitive d'une porte. Dans un mode de réalisation de l'invention, le module de mise à jour (13) permet de modifier des paramètres sur le nombre de badges (4) désiré à l'aide d'un logiciel dédié de type Residor ou logiciel analogue de reprogrammation. La prise en compte des modifications s'effectue par exemple par réseau (6) filaire ou à l'aide d'un badge intermédiaire programmé avec ledit logiciel et l'appareil encodeur (17). Le module de mise à jour (13) transfère les informations à la borne de contrôle d'accès équipée avec le module de gestion (12). Ainsi, quand l'usager passe son badge (4) devant la borne (10) à lecteur de badge, la moindre modification est automatiquement réalisée grâce à la fonction écriture intégrée dans l'émetteur de ladite borne (10). Si cet émetteur est placé dans la borne de contrôle d'accès (10) de l'entrée principale, la totalité du parc pourra être mise à jour dans un laps de temps court, par exemple en 24h.

[0056] Dans un mode de réalisation de l'invention, chaque étape de modification de données (54, 540) sur la puce (40) comprend une étape de transmission par la borne (10) vers la puce du badge (4) d'une information chiffrée avec une clé correspondant à un secteur (S) déterminé de la mémoire (44) du badge (4) puis une étape de déchiffrement utilisant une clé d'écriture (Kw) associée au secteur (S) déterminé de la mémoire (44) du badge (4) pour déchiffrer l'information correspondant à ce secteur (S). L'utilisation de clés de chiffrement/déchiffrement apporte une sécurisation du protocole de communication entre une borne de contrôle d'accès (10) et un badge (4).

[0057] Lorsqu'il n'est pas nécessaire de procéder à des modifications, l'étape (520) de comparaison est suivie d'une étape de fin de communication (55) s'accompagnant par exemple du déblocage d'un accès (A1, A2, A3). Dans un mode de réalisation de l'invention, le module de gestion (12) peut commander par exemple un électro-aimant (40) d'une gâche électrique pour débloquer un portillon d'accès. Le module de gestion (12) peut également commander, dans un autre exemple, une télécommande, un actionneur, etc. Dans des exemples de réalisation de l'invention, au moins un récepteur radio des moyens de communication radio (11) de la borne (10) est associé à une horloge enregistrant les heures d'arrivées et de départ des utilisateurs et permet de gérer les heures de travail.

[0058] Un des avantages de l'invention réside dans la simplicité de mise en oeuvre, les mises à jour étant réalisées de façon automatique. La gestion du parc de badges est ainsi simplifiée et les usagers ne sont plus dans l'obligation de restituer leur badge lorsque le gestionnaire doit effectuer des modifications. De plus, une sécurisation des données d'identification peut être assurée puisqu'un badge perdu ou volé ne peut pas être utilisé de manière frauduleuse.

[0059] Il doit être évident pour les personnes versées dans l'art que la présente invention permet des modes de réalisation sous de nombreuses autres formes spécifiques sans l'éloigner du domaine d'application de l'invention comme revendiqué.

Revendications

1. Procédé de gestion de badges de contrôle d'accès destiné à faciliter la mise à jour d'informations sur des badges sans contact (4) incluant chacun une puce électronique (40) dotée d'un organe de communication (41) radio ou optique, ledit procédé utilisant un équipement d'accès (1) comportant plusieurs bornes (10, 20, 30) de contrôle d'accès munies chacune de moyens de communication (11) radio ou optique permettant de lire des donnés de la puce (40) du badge (4), au moins une base de données étant à la disposition de chaque borne de contrôle d'accès (10, 20, 30), procédé dans lequel au moins une communication sans contact (5) radio ou optique est établie entre une des bornes de contrôle d'accès et un badge sans contact (4), ladite communication sans contact (5) comprenant une étape (50) d'authentification du badge (4) par lecture de données d'identification stockées dans la puce (40) du badge, **caractérisé en ce que** ladite communication sans contact (5) comprend :

   - une étape (51) de lecture, par les moyens de communication (11) de la borne de contrôle d'accès (10), d'un indice de perte de la puce (40) du badge représentatif d'un nombre de déclarations de perte pour le badge authentifié ;
   - une étape (52) de comparaison réalisée par

un module de gestion (12) installé dans la borne de contrôle d'accès (10) pour comparer ledit indice de perte avec un indice de perte analogue stocké dans ladite base de données correspondant au badge authentifié ;
- si l'étape (52) de comparaison révèle que l'indice de perte lu sur la puce (40) du badge représente un nombre de déclarations de perte supérieur à celui prévu selon l'indice de perte de la base de données, une étape (53) de modification de la base de données pour tenir compte de l'indice de perte lu sur le badge authentifié ; et
- si l'étape (52) de comparaison révèle que l'indice de perte lu sur la puce (40) du badge représente un nombre de déclarations de perte inférieur à celui prévu selon l'indice de perte de la base de données, une étape (54) de modification et/ou effacement de données de la puce (40) du badge pour invalider le badge (4).

2. Procédé selon la revendication 1, dans lequel, si l'étape (52) de comparaison révèle que l'indice de perte lu sur la puce (40) du badge (4) représente un nombre de déclarations de perte supérieur ou égal à celui prévu selon l'indice de perte de la base de données, ladite communication sans contact (5) comporte :

- une étape (510) de lecture, par les moyens de communication (11) de la borne de contrôle d'accès (10), de données de profil mémorisées par la puce (40) du badge représentatives d'un profil d'utilisation du badge (4) ;
- une étape (520) de comparaison réalisée par le module de gestion (12) pour comparer les données de profil lues avec des données de profil correspondant aux données d'identification dans ladite base de données ; et
- en cas de non correspondance entre données de profil comparées, une étape (540) de modification de données sur la puce (40) utilisant en premier lieu ledit module de gestion (12) et lesdits moyens de communication (11) pour transmettre (541) à la puce (40) du badge les données de profil considérées comme nouvelles et utilisant en second lieu des moyens d'écriture (42) de ladite puce (40) pour remplacer (542) les données de profil stockées dans une mémoire (44) de la puce (40) par les données nouvelles transmises via les moyens de communication (11) de la borne de contrôle d'accès (10).

3. Procédé selon la revendication 1 ou 2, dans lequel l'étape (50) d'authentification du badge (4) comprend une étape (503) de lecture utilisant les moyens de communication (11) de la borne de contrôle d'accès (10) pour lire des données d'identification associées à une signature sur la puce (40) du badge (4) et une étape (505) de comparaison entre signatures utilisant le module de gestion (12) installé dans la borne de contrôle d'accès (10) pour comparer les données de signature calculée (504) par la borne (10) avec les données de signature transmises depuis la puce (40).

4. Procédé selon une des revendications 1 à 3, dans lequel chacun des badges sans contact (4) est initialisé par un appareil encodeur de badges (17) lors d'une étape de personnalisation, l'appareil encodeur (17) transmettant dans une mémoire non volatile reprogrammable de la puce (40) du badge (4) au moins une donnée d'identification du badge (4) et des données de profil représentatives d'un profil d'utilisation du badge (4).

5. Procédé selon la revendication 4, dans lequel une étape de cryptage est réalisée par l'appareil encodeur de badges (17) pour stocker au moins une donnée d'identification du badge (4) sous la forme d'une signature cryptée dans une zone mémoire (442) du badge sans contact (4).

6. Procédé selon la revendication 5, dans lequel ladite étape (50) d'authentification du badge (4) comprend une émission préalable (500) depuis la borne de contrôle (10) à destination du badge (4) d'une requête d'envoi d'au moins une donnée d'identification du badge (4), la communication sans contact (5) s'établissant entre borne (10) et badge sans contact (4) en cas de réception par le badge (4) de ladite requête, l'étape (50) d'authentification du badge comprenant ensuite la réception (502) de ladite donnée d'identification avec sa signature associée, la lecture (503) de la donnée d'identification du badge (4) par le module de gestion (12) de la borne de contrôle d'accès (10), au moins une clé associée à ladite donnée d'identification étant utilisée par le module de gestion (12) pour d'une part calculer (504) ladite signature calculée à partir de la signature transmise par le badge (4) en réponse à ladite requête, et d'autre part comparer (505) ladite signature calculée avec la signature transmise par le badge (4) avec ladite donnée d'identification en réponse à ladite requête.

7. Procédé selon une des revendications 2 à 6, comportant une étape de chiffrage utilisant une clé de lecture (Kr) stockée dans un secteur (S) de la mémoire (44) du badge (4) pour chiffrer des informations dudit secteur (S) avant la transmission des ces informations à une borne de contrôle d'accès (10) et une étape de déchiffrage utilisant une clé d'écriture (Kw) stockée dans un secteur (S) pour déchiffrer les informations reçues d'une borne (10) et destinées audit secteur (S), la mémoire (44) du badge (4)

comprenant un nombre déterminé de secteurs (S) incluant chacun une clé de lecture (Kr) et une clé d'écriture (Kw).

8. Procédé selon une des revendications 3 à 7, dans lequel un arrêt (506) de la communication sans contact (5) est déclenché par l'intermédiaire du module de gestion (12) et des moyens de communication (11) de la borne (10) lorsque la comparaison (505) entre signatures ne donne aucun résultat.

9. Procédé selon une des revendications 2 à 8, dans lequel chaque étape de modification de données (54, 540) sur la puce (40) comprend une étape de transmission par la borne (10) vers la puce du badge (4) d'une information chiffrée avec une clé correspondant à un secteur (S) déterminé de la mémoire (44) du badge (4) puis une étape de déchiffrement utilisant une clé d'écriture (Kw) associée au secteur (S) déterminé de la mémoire (44) du badge (4) pour déchiffrer l'information correspondant à ce secteur (S).

10. Procédé selon une des revendications 2 à 9, dans lequel les données de profil de la base de données (14) sont mises à jour par l'intermédiaire d'un module de mise à jour (13) de données de profil.

11. Procédé selon la revendication 10, dans lequel le module de mise à jour (13) fournit, pour chacun des badges sans contact (4), des données d'identification de badge et des données de profil à une base de données locale (14) d'au moins une borne de contrôle d'accès (10).

12. Procédé selon une des revendications 1 à 11, dans lequel la communication est du type radio (5) et s'effectue à une fréquence déterminée dans une zone restreinte ayant un rayon inférieur à 12 mètres autour des moyens de communication (11) de la borne de contrôle d'accès (10, 20, 30).

13. Equipement (1) de gestion de badges sans contact (4) pour du contrôle d'accès, destiné à faciliter la mise à jour d'informations contenues dans une puce électronique (40) des badges, comportant plusieurs bornes de contrôle d'accès (10, 20, 30) munies chacune de moyens de communication radio ou optique (11) permettant de lire des donnés de la puce (40) d'un badge (4), **caractérisé en ce qu'**il comprend :

- un module de mise à jour (13) de données de badge représentatives notamment d'une identification et d'un indice de perte, agencé pour utiliser des données de mises à jour d'une base de données (14), à chaque badge (4) géré par ledit équipement (1) étant associé un unique jeu de données de badge ;
- un module de gestion (12) installé dans chaque borne de contrôle d'accès (10) et associé aux moyens de communication (11) de la borne (10) pour comparer des données de badge lues par les moyens de communication (11) avec des données de badge associées stockées dans la base de données, le module de gestion (12) incluant des moyens de sélection pour sélectionner dans la base de données les données associées à un badge déterminé, et des moyens de décision du remplacement d'au moins une partie des données dudit badge déterminé ; et
- des moyens de transmission dans lesdits moyens de communication (11) de chaque borne de contrôle d'accès (10, 20, 30) pour transmettre à une puce (40) d'un badge des données de remplacement sélectionnées par l'intermédiaire du module de gestion, le module de gestion (12) étant agencé pour effacer au moins un champ de données de façon à invalider un badge (4) par transmission parmi lesdites données de remplacement d'au moins un champ de données correspondant à l'effacement de l'indice de perte du badge.

14. Equipement selon la revendication 13, dans lequel les données de badge comportent des données de profil représentatives d'un profil d'utilisation du badge.

15. Equipement selon la revendication 14, dans lequel les données de profil sont au moins une des informations suivantes :

- le(s) numéro(s) d'un ou plusieurs sites autorisés ;
- le nom de l'usager ;
- le numéro d'appartement ;
- la catégorie du personnel ou le niveau hiérarchique ;
- les droits d'accès,
- le numéro de badge,
- l'indice de perte ;
- les dates de validité ;

chacune de ces informations étant destinée à un secteur (S) spécifique de la mémoire (44) du badge (4) utilisant une clé d'écriture ou de lecture associée.

16. Equipement selon une des revendications 13 à 15, dans lequel un appareil encodeur de badges (17) est prévu pour initialiser et personnaliser chacun des badges sans contact, l'appareil encodeur (17) disposant de moyens d'émission pour transmettre dans une mémoire (44) de la puce (40) d'un badge (4) au moins une donnée d'identification du badge (4) et des données de profil représentatives d'un profil d'utilisation du badge (4).

17. Equipement selon la revendication 16, dans lequel l'appareil encodeur de badges (17) comprend un module de cryptage et est agencé pour transmettre sous la forme d'une signature cryptée au moins une donnée d'identification du badge (4) à destination d'une zone mémoire (442) du badge sans contact (4).

18. Equipement selon une des revendications 13 à 17, dans lequel les moyens de communication (11) sont reliés au module de gestion (12) pour , d'une part émettre par l'intermédiaire desdits moyens de transmission une requête d'identification de badge (4), et d'autre part recevoir au moins une donnée d'identification d'un badge (4).

19. Equipement selon la revendication 17 ou 18, dans lequel le module de gestion (12) comporte des moyens de décryptage et de lecture du type utilisant au moins une clé pour décrypter une donnée d'un secteur cryptée reçue par les moyens de communication (11).

20. Equipement selon une des revendications 14 à 19, dans lequel des moyens interactifs (15) incluant une interface de saisie sont reliés au module de mise à jour (13) pour permettre la saisie de données d'accès, le module de mise à jour (13) comprenant dans des moyens de mémorisation (130), pour chacun des badges (4) gérés par l'équipement (1), une table de données d'accès représentatives d'autorisations d'accès correspondant spécifiquement à des bornes définies de l'équipement (1).

21. Equipement selon une des revendications 14 à 20, dans lequel le module de mise à jour (13) est doté de moyens de mémorisation (130) permettant de stocker une base de données centrale rassemblant pour chacun des badges sans contact (4) des données d'identification de badge et des données de profil, ladite base de données centrale étant reliée à une pluralité de bornes de contrôle d'accès (10, 20, 30).

22. Equipement selon une des revendications 13 à 20, dans lequel chacune des bornes de contrôle d'accès (10, 20, 30) comporte une base de données (14) locale, le module de mise à jour étant relié à chacune desdites bases de données (14) locales.

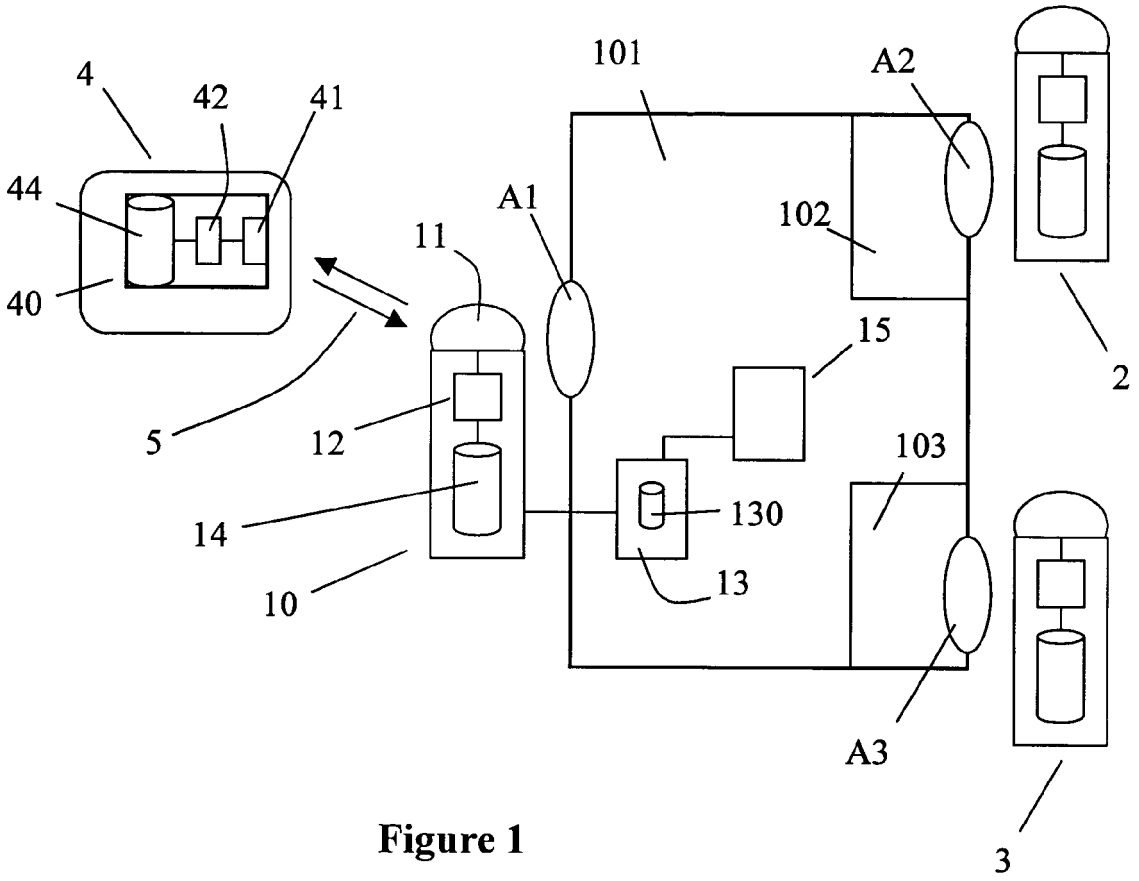

Figure 1

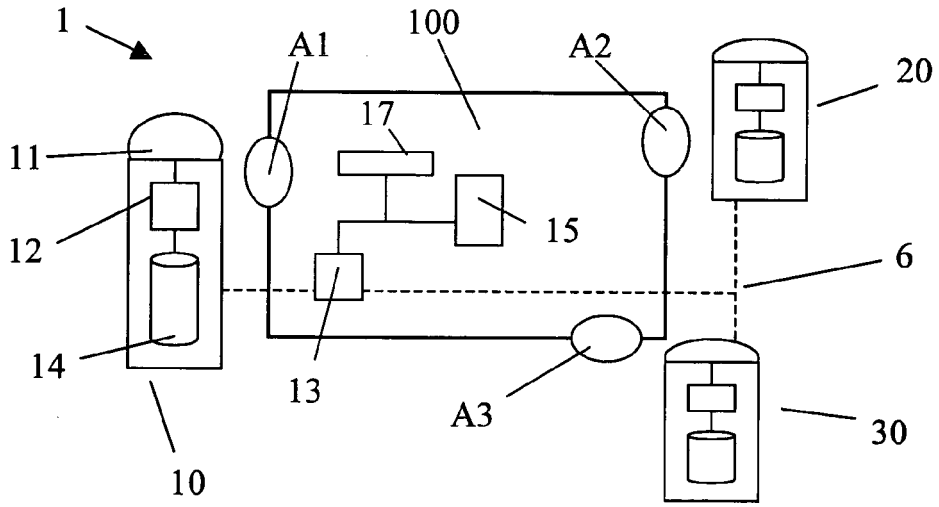

Figure 2

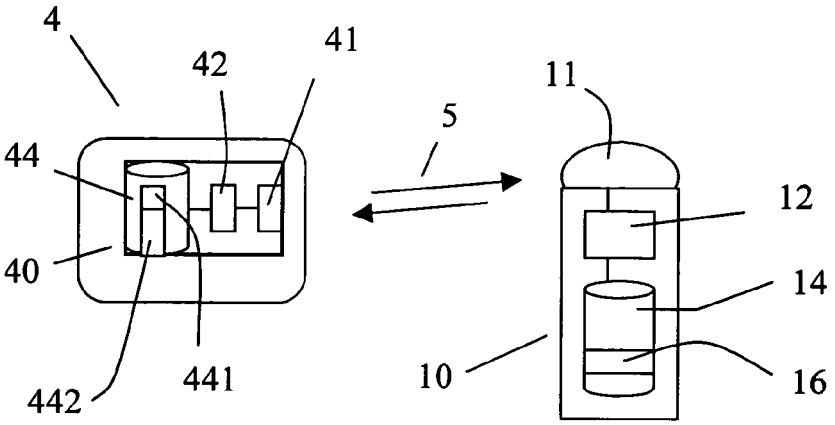

Figure 3

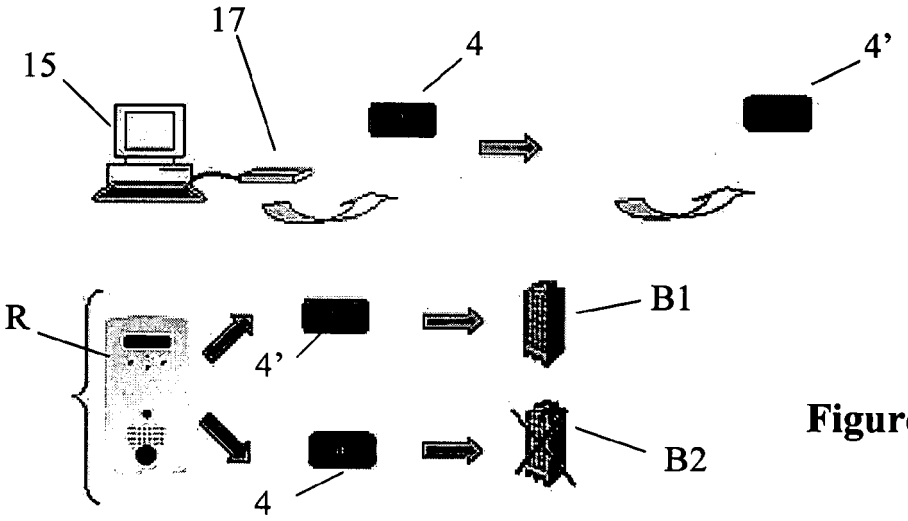

Figure 4

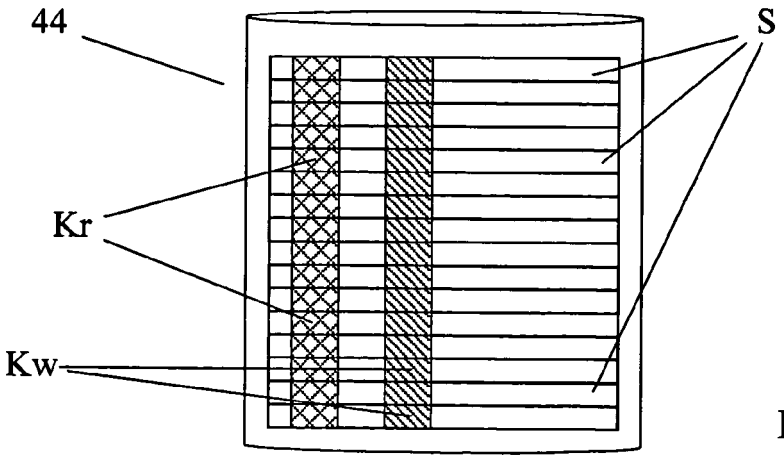

Figure 5

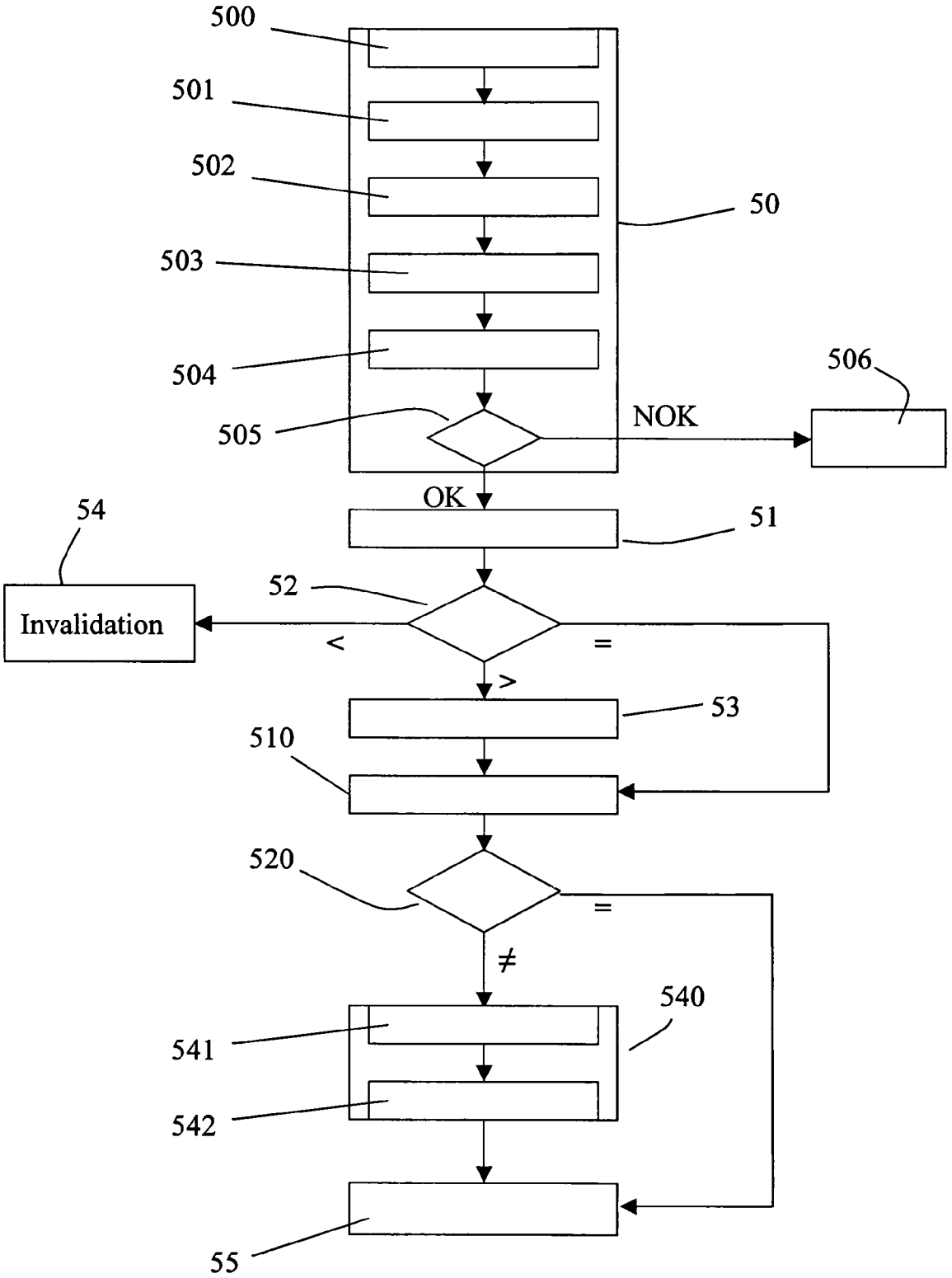
500
501
502
503
504
505
50
506
NOK
OK
51
54
Invalidation
52
<
=
>
53
510
520
=
≠
540
541
542
55

Figure 6

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 05 29 2321

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
Y	US 5 602 536 A (HENDERSON ET AL) 11 février 1997 (1997-02-11) * abrégé * * colonne 3, ligne 61 - colonne 37, ligne 25 * * colonne 44, ligne 35 - colonne 52, ligne 9 * * figures 1-29 *	1-22	G07C9/00 H04L9/32 G06K19/07
Y	US 6 233 588 B1 (MARCHOILI JOHN ET AL) 15 mai 2001 (2001-05-15) * abrégé * * figures 1-6 *	1-22	
A	WO 02/091311 A (CUBIC CORPORATION; CARTA, DAVID, R; KELLY, M., GUY; RAVENIS, JOSEPH, V) 14 novembre 2002 (2002-11-14) * abrégé * * alinéa [0013] - alinéa [0015] * * alinéa [0019] - alinéa [0037] * * revendications 1-20 * * figures 1-9 *	1-22	DOMAINES TECHNIQUES RECHERCHES (IPC) G07C H04L
A	EP 1 450 312 A (COMPUTERIZED SECURITY SYSTEMS, INC) 25 août 2004 (2004-08-25) * abrégé * * alinéa [0006] - alinéa [0022] * * figures 1-12 * * revendications 1-31 *	1-22	
A	WO 03/056511 A (VASSALLO, DAVID; SAFECAB PTY LIMITED) 10 juillet 2003 (2003-07-10) * abrégé * * page 4, ligne 1 - page 5, ligne 2 * * page 6, ligne 3 - page 15, ligne 15 * * figure 11 *	1-22	

-/--

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	8 février 2006	Pañeda Fernández, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 05 29 2321

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
A	EP 1 265 121 A (SYSTEMNEEDS INC) 11 décembre 2002 (2002-12-11) * abrégé * * figures 2,3 * * alinéa [0010] - alinéa [0017] * * alinéa [0036] * -----	1-22	

DOMAINES TECHNIQUES RECHERCHES (IPC)

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	8 février 2006	Pañeda Fernández, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

3

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 05 29 2321

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

08-02-2006

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5602536 A	11-02-1997	US 6842105 B1	11-01-2005
		US 2005168320 A1	04-08-2005
US 6233588 B1	15-05-2001	AUCUN	
WO 02091311 A	14-11-2002	CA 2446295 A1	14-11-2002
		CN 1524250 A	25-08-2004
		EP 1384207 A1	28-01-2004
		JP 2004528655 T	16-09-2004
EP 1450312 A	25-08-2004	US 2004160305 A1	19-08-2004
WO 03056511 A	10-07-2003	EP 1500040 A1	26-01-2005
		US 2005035882 A1	17-02-2005
EP 1265121 A	11-12-2002	CA 2389632 A1	07-12-2002
		JP 2003085149 A	20-03-2003
		US 2002188855 A1	12-12-2002

EPO FORM P0460

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