ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 33891 B1

(51) Cl. internationale :
G06F 21/00

(43) Date de publication :
02.01.2013

(21) N° Dépôt :
34996

(22) Date de Dépôt :
22.06.2012

(30) Données de Priorité :
22.12.2009 FR 0959414

(86) Données relatives à l'entrée en phase nationale selon le PCT :
PCT/FR2010/052767 16.12.2010

(71) Demandeur(s) :
MEREAL BIOMETRICS, 141 bis rue de Saussure F-75017 Paris (FR)

(72) Inventeur(s) :
PARTOUCHE, Patrick ; BLOT, Philippe ; MOBETIE, Didier

(74) Mandataire :
M. MEHDI SALMOUNI-ZERHOUNI

(54) Titre : **CARTE A PUCE MULTI-APPLICATIFS AVEC VALIDATION BIOMETRIQUE**

(57) Abrégé : L'invention concerne une carte à puce intelligente comprenant; une pluralité de circuits applicatifs qui sont associés chacun à au moins un service applicatif contenu de façon sécurisée au sein de la carte, chaque circuit applicatif étant apte à être excité par un signal externe, une unité de commande permettant d'identifier le circuit applicatif excité, le service associé et d'activer ledit service en réponse à une autorisation d'activation, et un circuit biométrique pour authentifier l'utilisateur de façon à générer ladite autorisation d'activation.

Abrège

L'INVENTION CONCERNE UNE CARTE À PUCE INTELLIGENTE COMPRENANT; UNE PLURALITÉ DE CIRCUITS APPLICATIFS QUI SONT ASSOCIÉS CHACUN À AU MOINS UN SERVICE APPLICATIF CONTENU DE FAÇON SÉCURISÉE AU SEIN DE LA CARTE, CHAQUE CIRCUIT APPLICATIF ÉTANT APTE À ÊTRE EXCITÉ PAR UN SIGNAL EXTERNE, UNE UNITÉ DE COMMANDE PERMETTANT D'IDENTIFIER LE CIRCUIT APPLICATIF EXCITÉ, LE SERVICE ASSOCIÉ ET D'ACTIVER LEDIT SERVICE EN RÉPONSE À UNE AUTORISATION D'ACTIVATION, ET UN CIRCUIT BIOMÉTRIQUE POUR AUTHENTIFIER L'UTILISATEUR DE FAÇON À GÉNÉRER LADITE AUTORISATION D'ACTIVATION.

" Carte à puce multi-applicatifs avec validation biométrique."

La présente invention concerne le domaine technique des dispositifs d'accès sécurisé ou de communication sécurisée. Elle trouve une application particulièrement intéressante, mais non exclusivement, dans la technologie des cartes à puces avec ou sans contact telles que des cartes à puce RFID (Identification par Radio Fréquence ou « Radio Frequency Identification » en anglais). L'invention concerne notamment une carte à puce sans contact de type NFC, Mifare, ISO 14443 ou 15693, c'est-à-dire ayant une antenne RF et émettant quand elle se trouve dans un champ électromagnétique approprié.

D'une façon générale, une carte à puce comprend une (ou plusieurs) puce électronique en silicium contenant des informations plus ou moins sensibles et relatives au porteur de la carte. A titre d'exemple, dans la technologie RFID, la puce est généralement connectée à une antenne. Une carte RFID peut avoir le format d'une carte à puce classique, mais peut également revêtir différentes formes telles qu'un badge, une étiquette (« tag »), un porte-clés ou autre... Une batterie intégrée peut être prévue de façon à étendre les fonctionnalités de la carte.

La technologie RFID, basée sur le principe de l'induction électromagnétique est de plus en plus répandue dans la vie de tous les jours. Initialement utilisée pour la gestion des stocks, cette technologie a été massivement répandue dans le domaine du contrôle d'accès. Elle est en plein essor dans le domaine du passeport et du paiement. Au Japon par exemple, elle est très utilisée comme moyen de paiement par le protocole Felica. Aux Etats-Unis, les premiers terminaux de paiement basés sur le protocole ISO14443A ont déjà été déployés. Le déploiement en France est en cours aujourd'hui.

Malheureusement, l'engouement pour cette technologie s'est fait au détriment de l'aspect sécuritaire. En effet, une personne mal intentionnée peut accéder librement aux informations contenues dans une puce RFID. Et l'entité qui dispose d'un lecteur RFID n'est pas certaine que le possesseur de la carte RFID est bien la personne dont des données confidentielles sont stockées dans la carte.

On connaît des systèmes permettant d'authentifier une personne en utilisant un circuit biométrique.

On connaît le document US20070016940 décrivant une carte dotée d'un circuit biométrique pour identifier le porteur de la carte et des moyens de contrôle d'accès par mot de passe. Le document wo03084124 décrit une carte à puce dotée d'un circuit biométrique pour authentifier l'utilisateur et d'un bouton de sélection pour sélectionner des données contenues dans la carte ; un circuit RFID permettant la communication avec l'extérieur.

La présente invention a pour but une solution alternative aux solutions existantes de sécurisation de données contenues dans une carte.

La présente invention est d'un cadre plus large puisqu'elle a pour but une nouvelle carte intelligente capable d'intégrer de nombreuses fonctionnalités. La présente invention ambitionne de nombreuses applications dans la technologie sans fil et/ou avec contact.

Un autre but de l'invention est un dispositif enrichi capable de prendre en compte l'environnement dans lequel il se trouve.

On atteint au moins l'un des buts précités avec un dispositif de communication sans fil, comprenant :

- une pluralité de circuits applicatifs qui sont associés chacun à au moins un service applicatif contenu de façon sécurisée au sein du dispositif, chaque circuit applicatif étant apte à être excité par un signal externe,
- une unité de commande :
- pour identifier un circuit applicatif excité,
- pour identifier un service applicatif associé à ce circuit applicatif excité, et
- pour activer ledit service applicatif excité en réponse à une autorisation d'activation, et
- un circuit biométrique pour authentifier l'utilisateur de façon à générer ladite autorisation d'activation.

Un service applicatif peut comprendre une application logicielle que l'on exécute lorsque ce service applicatif est activé.

L'activation d'un service applicatif consiste notamment à le rendre accessible de l'extérieur, exécuter un algorithme ou bien déverrouiller une application ou des données.

Avec le dispositif selon l'invention, on réalise une double vérification avant d'activer un service applicatif. La première vérification est environnementale puisqu'il s'agit de détecter un signal venant de l'environnement extérieur. La seconde vérification est biométrique. On dispose ainsi d'un système sécurisé,

intelligent et économe en énergie. Le dispositif selon l'invention est intelligent car il est auto-adaptatif. Il est capable de reconnaître l'environnement dans lequel il est utilisé et d'enclencher le mécanisme de reconnaissance biométrique qui autorisera ou non le service applicatif correspondant. Le dispositif selon l'invention est multi-applications et peut choisir de façon automatique le service applicatif adéquat.

Le dispositif selon l'invention détermine l'action ou le canal de communication adapté face à un stimulus et fait valider l'activation par le porteur du dispositif grâce à sa signature biométrique.

Selon une caractéristique avantageuse de l'invention, les circuits applicatifs comprennent un émetteur-récepteur de signaux radiofréquences. Il peut s'agir d'une antenne radiofréquence.

Le service applicatif qui est activé peut être tout type d'application utilisant l'antenne radiofréquence. On peut utiliser un signal radiofréquence pour ouvrir une porte dans des hôtels ou autre, ou activer une machine à sous par exemple. L'unité de commande peut comprendre une puce de type puce RFID.

Selon l'invention, ces circuits applicatifs peuvent comprendre au moins un connecteur métallique pour communication avec un lecteur par exemple.

Avantageusement, les circuits applicatifs comprennent au moins un détecteur environnemental. Ce détecteur environnemental peut être l'un des éléments suivants :

- un détecteur acoustique,
- un détecteur thermique,
- un détecteur olfactif,
- un photo-détecteur,
- un détecteur de pression, et
- un accéléromètre.

Ces détecteurs peuvent notamment être réalisés en utilisant des capteurs MEMS.

On peut prévoir que l'unité de commande n'identifie un circuit applicatif excité que lorsque l'excitation atteint un seuil prédéterminé. On peut aussi envisager le fait que le signal externe d'excitation est codé de sorte que l'unité de commande ne considère l'excitation qu'après analyse du code. Ce code peut également servir à identifier un service applicatif parmi plusieurs services applicatifs possibles. Ce code peut se manifester notamment sous la forme d'une

mélodie particulière dans le cadre d'un détecteur acoustique, d'une onde ou fréquence de signal lumineux particulière dans le cas du photodétecteur, d'un signal RFID codé, et ainsi de suite.

De préférence, le circuit biométrique comprend un capteur biométrique associé à une unité de calcul pour traiter des données biométriques. Les données d'identification d'un ou plusieurs utilisateurs peuvent être stockées dans l'unité de calcul ou dans une mémoire associée au cours d'une étape d'enrôlement. En fonctionnement, à chaque sollicitation du circuit biométrique, l'utilisateur interagit avec le capteur biométrique qui transmet des données détectées vers l'unité de calcul pour une comparaison et une authentification.

Le circuit biométrique peut ainsi générer directement l'autorisation d'activation. Mais, lorsque le circuit biométrique ne comporte pas une unité de calcul, la comparaison peut se faire au sein de l'unité de commande.

Avantageusement, le dispositif selon l'invention comprend une interface homme-machine pour indiquer un état de fonctionnement. Il peut s'agir d'indicateurs sonores pour émettre un son particulier, une voix ou de la musique à partir d'un élément piézoélectrique. Il peut s'agir d'indicateurs visuels comprenant des DELS pour Diodes électroluminescentes. L'interface homme-machine peut également proposer un écran d'affichage, un clavier, un micro et des enceintes par exemple, pour accéder à l'unité de commande.

Le dispositif selon l'invention peut être alimenté par une batterie intégrée ou de préférence une pile qui est flexible ou non, rechargeable ou non. On peut par exemple envisager un capteur solaire pour recharger une pile photovoltaïque intégrée dans le dispositif. Autrement, on peut utiliser une alimentation par une source externe, notamment lorsqu'on utilise des dispositifs peu mobiles.

De préférence, le dispositif est un élément portatif sous un format de carte à puce, de clé USB, ou d'étiquette électronique.

Selon un autre aspect de l'invention, il est proposé un procédé mis en œuvre dans une carte de communication sans fil comprenant une pluralité de circuits applicatifs, une unité de commande et un circuit biométrique ; ce procédé comprenant les étapes suivantes :

on détecte un signal externe d'excitation au moyen d'un des circuits applicatifs, chaque circuit applicatif étant associé à au moins un service applicatif contenu de façon sécurisée au sein de la carte,

au sein de l'unité de commande, on identifie le circuit applicatif excité et le service applicatif associé à ce circuit applicatif excité, et on démarre un processus d'authentification par comparaison biométrique au sein du circuit biométrique, puis on active ledit service applicatif excité en réponse à une autorisation d'activation provenant du circuit biométrique.

Bien entendu, les différentes caractéristiques, formes et variantes de réalisation de l'invention peuvent être associées les unes avec les autres selon diverses combinaisons dans la mesure où elles ne sont pas incompatibles ou exclusives les unes des autres.

Par ailleurs, diverses autres caractéristiques de l'invention ressortent de la description ci-dessous effectuée en référence aux dessins annexés qui illustrent des formes non limitatives de réalisation d'une carte à puce RFID auto-adaptative intégrant un circuit biométrique.

Les figures 1 à 4 sont des schémas simplifiés illustrant le principe général de mise en œuvre d'un dispositif selon l'invention,

Les figures 5 à 8 sont des schémas simplifiés illustrant un mode de mise en œuvre du dispositif selon l'invention appliqué à un circuit RFID,

La figure 9 est une vue générale d'une carte à puce selon l'invention.

Sur les figures 1-9, les différents éléments communs aux diverses variantes ou formes de réalisation portent les mêmes références.

Le principe d'une carte auto-adaptative selon l'invention est schématiquement illustré sur les figures 1 à 4 sur lesquelles on distingue une carte à puce 1 comprenant d'une part un ensemble de circuits applicatifs 2 à 4 et, d'autre part, un circuit biométrique 5.

La carte à puce 1 peut comporter de nombreux circuits applicatifs, seuls trois d'entre eux sont représentés ici. Les références 2 à 4 représentent respectivement les circuits applicatifs n-1, n et n+1. Un circuit applicatif peut être constitué d'un émetteur-récepteur associé à un service applicatif. Chaque circuit applicatif est sensible à un phénomène physique donné caractérisant l'environnement dans lequel se trouve la carte. Ces phénomènes physiques peuvent comprendre le thermique, le toucher (contact), la lumière, l'olfactif, l'acoustique, la pression, le champ électromagnétique,... Lorsque la carte est plongée dans un environnement « n », le circuit applicatif n détecte la présence de cet environnement qui lui est

directement associé, mais n'active pas le service applicatif n correspondant. Ce service applicatif peut être un protocole d'échange avec cet environnement « n » ou l'exécution d'un programme particulier.

Les autres circuits applicatifs n-1 et n+1 restent insensibles : l'environnement « n » n'est pas reconnu par ces circuits applicatifs.

Ensuite, une demande d'autorisation est transmise vers le circuit biométrique 5 comme on le voit sur la figure 2. Dès réception de cette demande d'autorisation, le circuit biométrique démarre un processus d'authentification de façon à reconnaître et identifier l'utilisateur de la carte. Pour ce faire, le circuit biométrique comporte un capteur biométrique qui peut être de différents types : par analyse de caractéristiques physiques (empreinte digitale, imagerie de l'iris, imagerie de la rétine, ...), par analyse comportementale (analyse vocale, signature,...).

L'utilisateur doit alors se soumettre à la détection biométrique de façon à ce que le circuit biométrique récupère des données qui sont ensuite comparées à des données contenues dans la carte. Lorsque la comparaison est satisfaisante, la reconnaissance biométrique est alors positive et un signal d'accord est envoyé pour activer le servie applicatif n comme on le voit sur la figure 3. Une fois le service applicatif activé, le circuit applicatif n peut interagir avec l'environnement comme on le voit sur la figure 4.

Sur les figures 5 à 8, on voit un exemple de réalisation d'un dispositif selon l'invention. La carte est toujours désignée par la référence 1. Les circuits applicatifs 2 à 4 sont respectivement un circuit acoustique, un circuit thermique et un circuit RFID.

Dans cet exemple de réalisation, l'environnement est représenté par un lecteur RFID 6 qui génère un champ électromagnétique ou champ RF vers la carte à puce 1. Le circuit RFID détecte ce champ RF et transmet sur la figure 6 une demande d'autorisation vers le circuit biométrique 5. Cette demande d'autorisation a pour but d'activer un service de communication RFID entre le circuit RFID 4 et le lecteur RFID 6. Le circuit biométrique 5 authentifie l'utilisateur puis transmet un signal d'accord ou de désaccord vers le circuit RFID. En cas d'accord tel que représenté sur la figure 7, le circuit RFID active le service de communication qui permet notamment le transfert de données ou de consigne vers le lecteur RFID 6 comme illustré sur la figure 8. Le lecteur RFID 6 peut être associé à une porte, à une machine à sous ou à tout autre système de sorte que la réception d'une

consigne provenant de la carte à puce peut entraîner l'ouverture de la porte, l'activation de la machine à sous, la mise sous tension ou en veille d'un système, ...

La consigne peut comporter des données personnelles de l'utilisateur ainsi que des instructions codées ou non destinées au lecteur RFID 6.

Le signal de l'environnement détecté par un circuit applicatif peut être un signal codé ou non permettant notamment de distinguer quel service applicatif nécessite d'être activé lorsque par exemple plusieurs services applicatifs sont susceptibles d'être activés via ce circuit applicatif.

On peut envisager que le service applicatif activé lance une communication avec une machine à sous par champ RF pour par exemple créditer un compte de l'utilisateur dans la machine à sous ou récupérer des gains réalisés par l'utilisateur, notamment en temps réel.

La figure 9 est un schéma bloc simplifié d'un exemple de réalisation d'une carte à puce selon l'invention. On distingue un émetteur-récepteur acoustique 7 associé à un seul service applicatif A1. L'émetteur-récepteur thermique 8 est associé à un seul service applicatif A2. L'émetteur-récepteur RFID 9 est associé à un seul service applicatif A3. On peut imaginer un système plus complexe dans lequel un émetteur-récepteur est associé à plusieurs services applicatifs. On peut même prévoir d'utiliser plusieurs signaux d'excitation détectés simultanément par plusieurs émetteur-récepteurs pour déterminer un service applicatif adéquat pour l'environnement en cours.

Tel qu'illustré sur la figure 9, dans chaque liaison entre l'émetteur-récepteur et son service applicatif associé, on introduit respectivement un interrupteur commandé 11, 12 et 13, de sorte qu'un service applicatif n'est activé que lorsque l'interrupteur commandé associé est fermé.

Sur la figure 9 chaque émetteur-récepteur 7, 8 et 9 est relié à une unité de commande 10 qui gère l'ensemble des composants et programmes logiciels de la carte à puce 1. L'unité de commande 10 est un microcontrôleur équipé :

- d'une mémoire flash renfermant les applications logicielles pour son propre fonctionnement et destinées à commander le circuit biométrique 5,
- d'une mémoire RAM,
- d'une horloge, et
- de plusieurs entrées/sorties.

Elle est sous la forme d'une puce intégrée dans la carte et présente une consommation réduite. L'unité de commande 10 est configurée pour fermer un des

interrupteurs 11, 12 et 13 en réponse à un accord d'activation émis par le circuit biométrique 5.

Une interface homme-machine IHM 17 comporte des moyens d'affichage, de saisie, de diffusion sonore et visuelle. La diffusion visuelle peut se faire via des diodes électroluminescentes DELs. Une batterie intégrée 16 alimente l'ensemble des composants de la carte 1.

Le circuit biométrique 5 comporte un capteur biométrique 14 qui se charge de la saisie des données biométriques brutes. On utilise un capteur d'empreinte digitale. Le circuit biométrique 5 comporte également une unité de calcul 15 capable de traiter des données biométriques de façon à réaliser l'enrôlement et des comparaisons d'empreintes.

L'enrôlement se déroule de la manière suivante :

- l'utilisateur active la carte via le circuit de commande,
- le circuit de commande active le circuit biométrique en le mettant en mode « enrôlement »,
- l'utilisateur pose son doigt sur le capteur d'empreinte qui envoie des informations correspondantes vers l'unité de calcul, et
- lorsque ces informations sont transférées puis stockées dans l'unité de calcul, l'unité de commande informe l'utilisateur que l'enrôlement s'est bien passé par le biais de l'interface IHM 17.

Le fonctionnement de la carte peut être le suivant. Lorsqu'un signal d'excitation est détecté par l'un des émetteurs-récepteurs 7, 8 ou 9, par exemple l'émetteur-récepteur 7, l'unité de commande 10 est activée et démarre un processus d'authentification :

- le circuit de commande active le circuit biométrique en le mettant en mode « authentification »,
- l'utilisateur pose son doigt sur le capteur d'empreinte qui envoie des informations correspondantes vers l'unité de calcul,
- l'unité de calcul compare ces informations avec des informations préalablement stockées lors de la phase d'enrôlement, et
- après authentification, l'unité de commande informe l'utilisateur du résultat et désactive le circuit biométrique.

En cas de réponse positive (authentification réussie), l'unité de commande ferme alors l'interrupteur 11 de façon à permettre la communication du service applicatif A1 avec l'environnement extérieur via l'émetteur-récepteur 7. Bien

entendu, les interrupteurs commandés 11, 12 et 13 peuvent être réalisés sous forme logicielle, l'accès aux services applicatifs étant obtenus après réception d'un accord d'authentification.

Bien sûr, l'invention n'est pas limitée aux exemples qui viennent d'être décrits et de nombreux aménagements peuvent être apportés à ces exemples sans sortir du cadre de l'invention. Le dispositif peut s'appliquer à différents domaines tels que :

Le domaine bancaire,

L'identification d'individu,

Le domaine du Jeux,

La clef numérique pour ouverture de porte,

Le domaine de l'enregistrement/lecture de message,

La restitution de data,

Le domaine médical par exemple pour l'analyse de sang ou de l'ADN.

REVENDICATIONS

1. Dispositif de communication sécurisée, comprenant :

- une pluralité de circuits applicatifs qui sont associés chacun à au moins un service applicatif contenu de façon sécurisée au sein du dispositif, chaque circuit applicatif étant apte à être excité par un signal externe,

- une unité de commande permettant d'identifier le circuit applicatif excité, le service associé et d'activer ledit service en réponse à une autorisation d'activation, et

- un circuit biométrique pour authentifier l'utilisateur de façon à générer ladite autorisation d'activation.

2. Dispositif selon la revendication 1, caractérisé en ce que les circuits applicatifs comprennent un émetteur-récepteur de signaux radiofréquences.

3. Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce que les circuits applicatifs comprennent au moins un connecteur métallique.

4. Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce que les circuits applicatifs comprennent au moins un détecteur environnemental.

5. Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce que les circuits applicatifs comprennent au moins l'un des éléments suivants :

- un détecteur acoustique ;
- un détecteur thermique ;
- un détecteur olfactif ;
- un photo-détecteur ;
- un détecteur de pression ;
- un accéléromètre.

6. Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce que le circuit biométrique comprend un capteur biométrique associé à une unité de calcul pour traiter des données biométriques.

7. Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend une interface homme-machine pour indiquer un état de fonctionnement du dispositif.

8. Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est alimenté par une pile flexible ou non, rechargeable ou non.

9. Dispositif selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il est alimenté par une source externe.

10. Dispositif selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est sous un format de carte à puce, de clé USB, ou d'étiquette électronique.

11. Procédé mis en œuvre dans une carte de communication sécurisée comprenant une pluralité de circuits applicatifs, une unité de commande et un circuit biométrique ; ce procédé comprenant les étapes suivantes :

on détecte un signal externe d'excitation au moyen d'un des circuits applicatifs, chaque circuit applicatif étant associé à au moins un service applicatif contenu de façon sécurisée au sein de le la carte,

au sein de l'unité de commande, on identifie le circuit applicatif excité et le service applicatif associé à ce circuit applicatif excité, et on démarre un processus d'authentification par comparaison biométrique au sein du circuit biométrique, puis on active ledit service applicatif excité en réponse à une autorisation d'activation provenant du circuit biométrique.

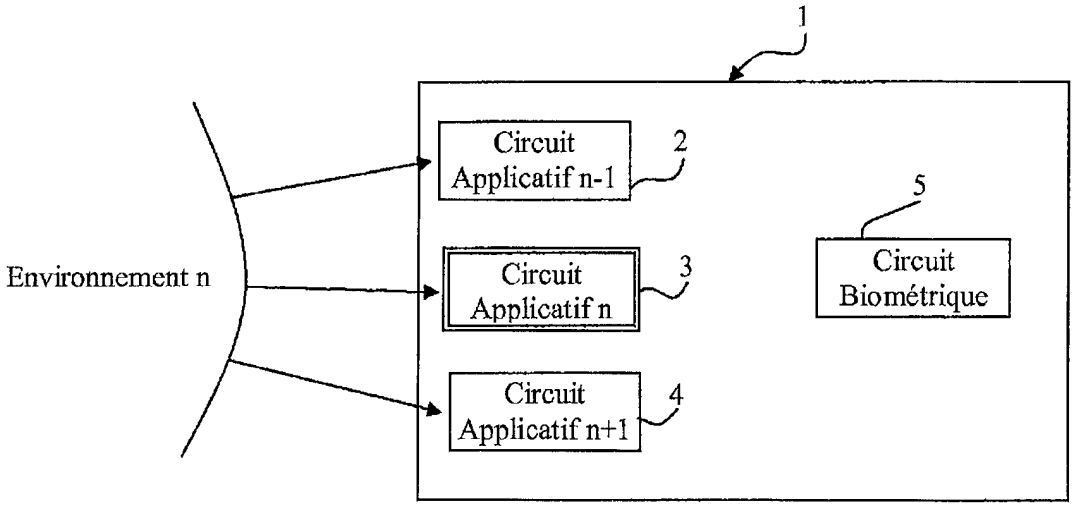

FIGURE 1

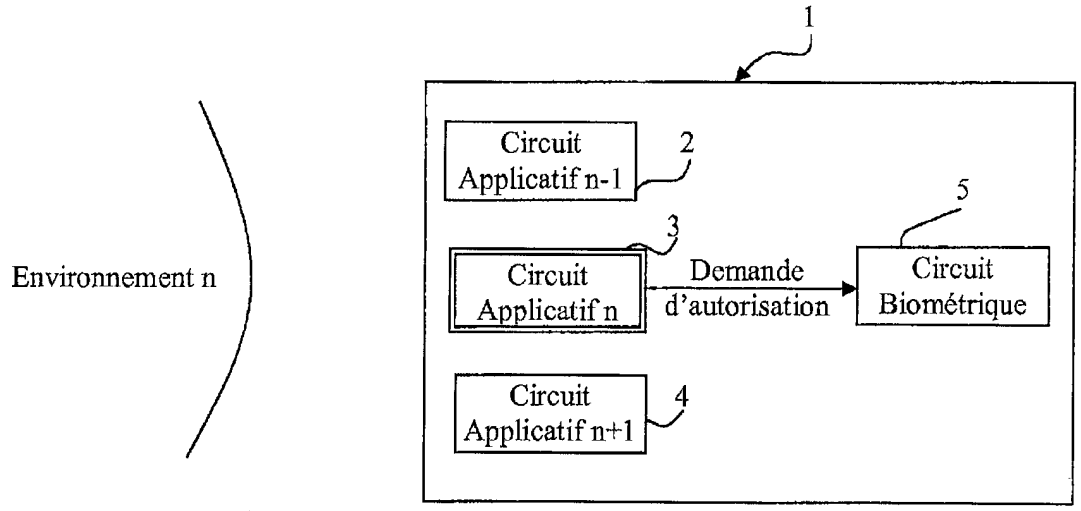

FIGURE 2

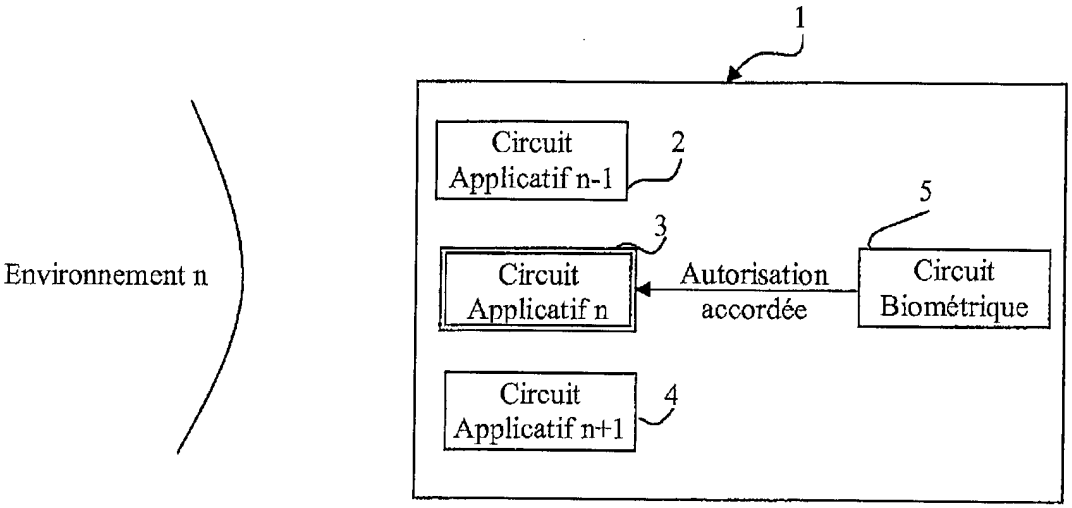

FIGURE 3

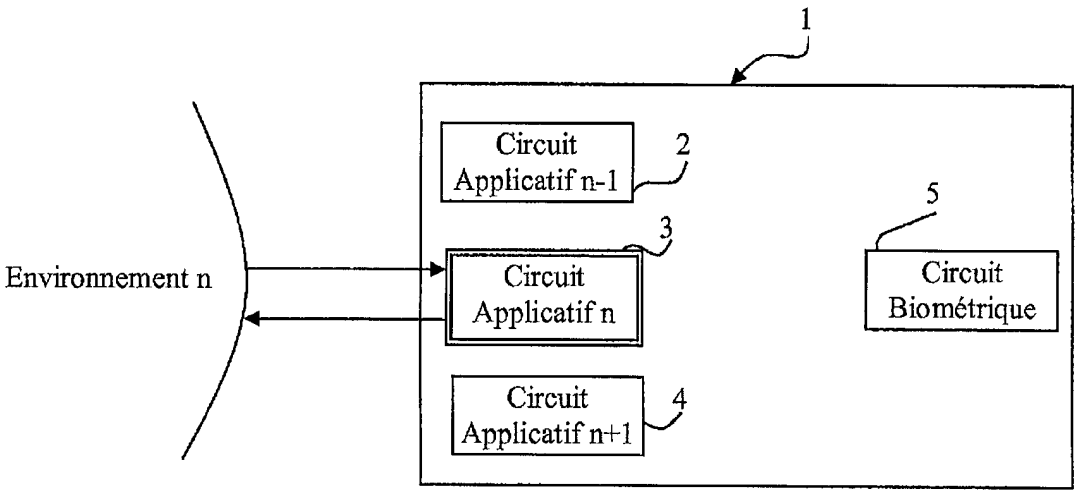

FIGURE 4

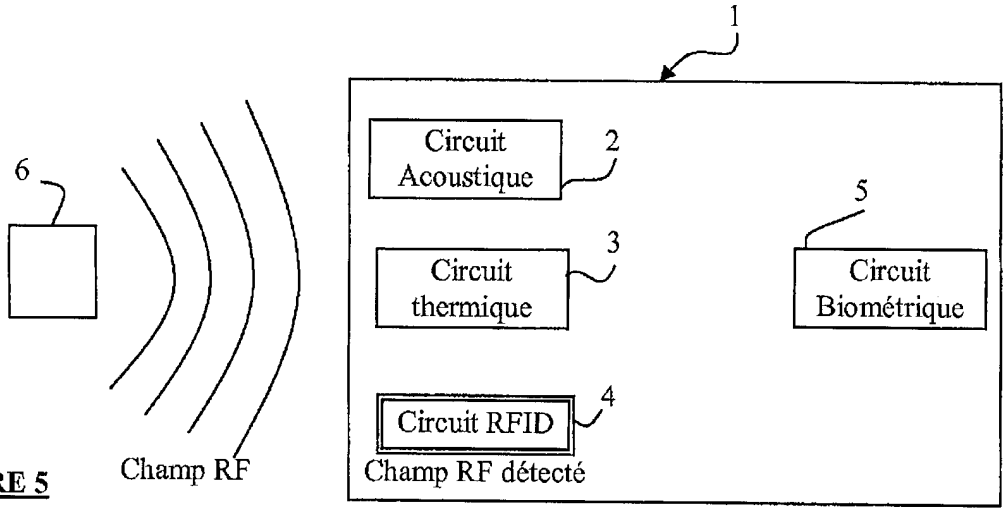

FIGURE 5

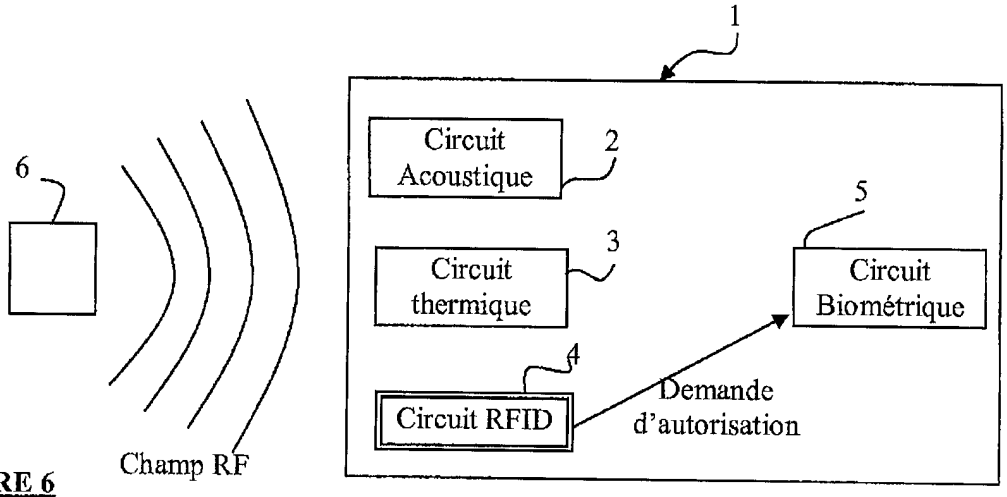

FIGURE 6

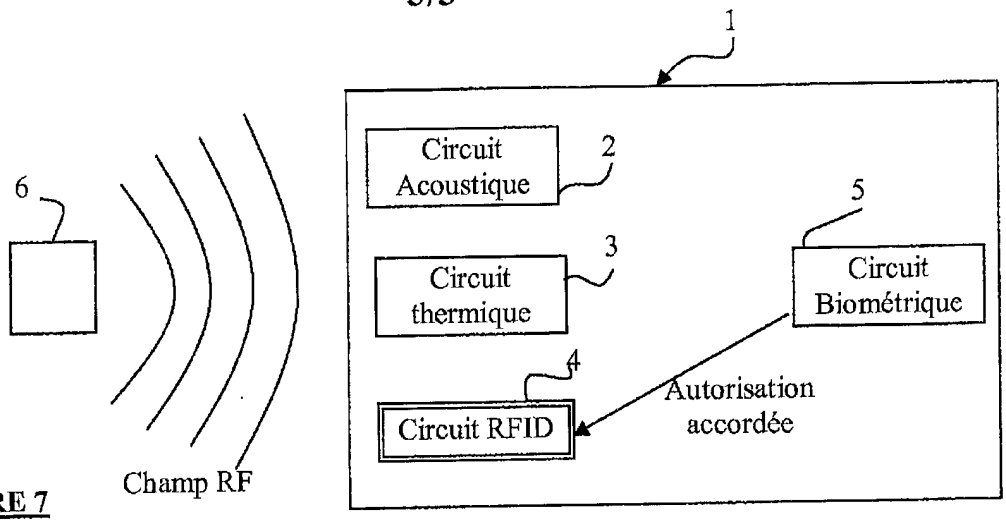

FIGURE 7

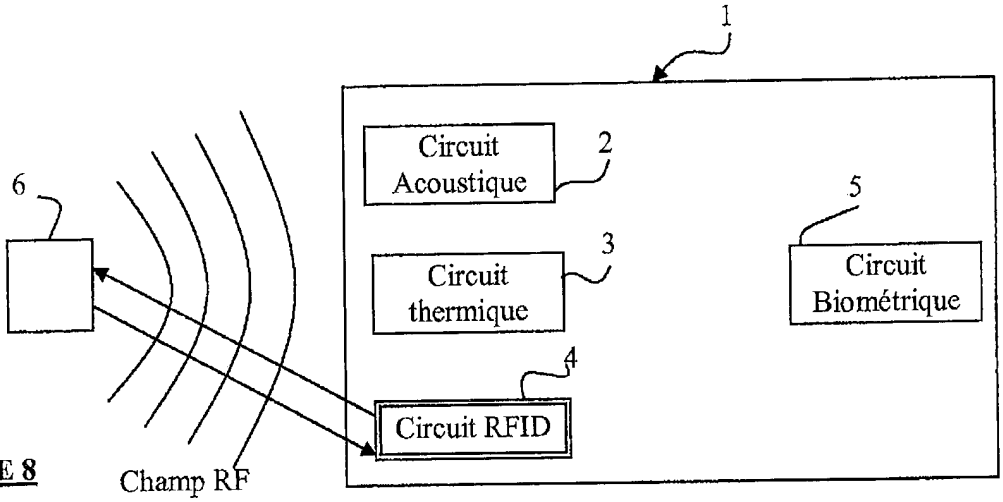

FIGURE 8

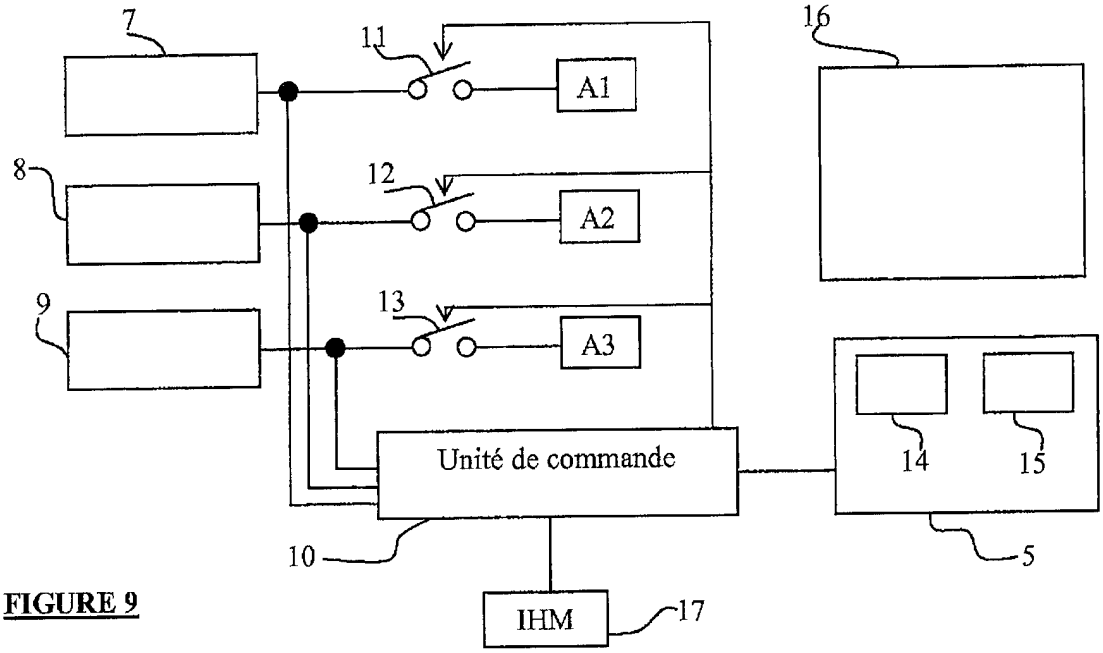

FIGURE 9