



(86) Date de dépôt PCT/PCT Filing Date: 2010/12/16
(87) Date publication PCT/PCT Publication Date: 2011/07/14
(45) Date de délivrance/Issue Date: 2023/03/21
(85) Entrée phase nationale/National Entry: 2012/06/14
(86) N° demande PCT/PCT Application No.: FR 2010/052767
(87) N° publication PCT/PCT Publication No.: 2011/083241
(30) Priorité/Priority: 2009/12/22 (FR0959414)

(51) Cl.Int./Int.Cl. G06F 21/32 (2013.01),
G06F 21/34 (2013.01), G06Q 20/32 (2012.01),
G06Q 20/40 (2012.01)

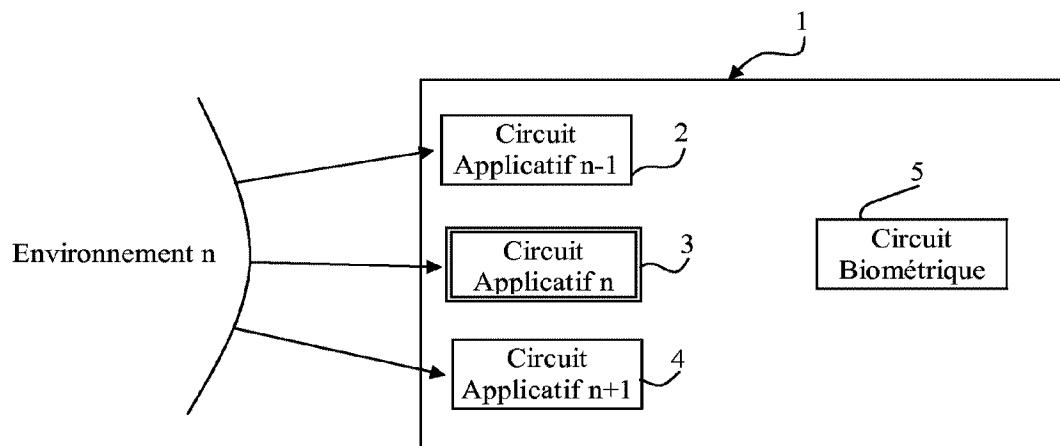
(72) Inventeurs/Inventors:
PARTOUCHÉ, PATRICK, FR;
BLOT, PHILIPPE, FR;
MOBETIE, DIDIER, FR

(73) Propriétaire/Owner:
MEREAL BIOMETRICS, FR

(74) Agent: SMART & BIGGAR LP

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

(54) Title: MULTIPLE APPLICATION CHIP CARD HAVING BIOMETRIC VALIDATION



(57) Abrégé/Abstract:

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.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international



(43) Date de la publication internationale
14 juillet 2011 (14.07.2011)

PCT

(10) Numéro de publication internationale

WO 2011/083241 A1

(51) Classification internationale des brevets :
G06F 21/00 (2006.01)

(74) Mandataires : PONTET ALLANO et al.; PONTET, Bernard, 25 rue Jean Rostand, Parc Orsay-université, F-91893 Orsay Cedex (FR).

(21) Numéro de la demande internationale : PCT/FR2010/052767

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) Date de dépôt international : 16 décembre 2010 (16.12.2010)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité : 0959414 22 décembre 2009 (22.12.2009) FR

(71) Déposant (pour tous les États désignés sauf US) : MEREAL BIOMETRICS [FR/FR]; 141 bis rue de Saussure, F-75017 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : PARTOUCHÉ, Patrick [FR/FR]; Villa Pouiksan, 13 Boulevard Cointet, F-06400 Cannes (FR). BLOT, Philippe [FR/FR]; 25 rue Victor Hugo, F-78370 Plaisir (FR). MOBETIE, Didier [FR/FR]; 70 rue de Montrouil, F-78000 Versailles (FR).

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

[Suite sur la page suivante]

(54) Title : MULTIPLE APPLICATION CHIP CARD HAVING BIOMETRIC VALIDATION

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

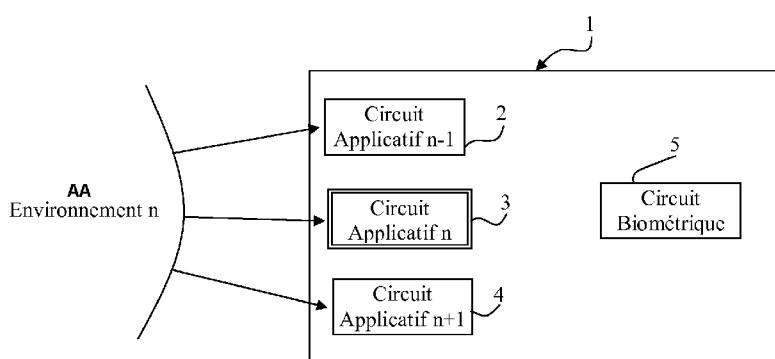


FIGURE 1

AA... Environment n
2... Application Circuit n-1
3... Application Circuit n
4... Application Circuit n+1
5... Biometric Circuit

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

(57) Abstract : The invention relates to a smart card including: a plurality of application circuits that are each related to at least one application service securely contained within the card, each application circuit that is energizable by an outside signal; a control unit making it possible to identify the energized application circuit and the related service and moreover to activate said service in response to activation authorization; and a biometric circuit for authenticating the user so as to generate said activation authorization.

(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,

WO 2011/083241 A1

WO 2011/083241 A1

Publiée :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

— *avec rapport de recherche internationale (Art. 21(3))*

" 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 5 données contenues dans la carte; un circuit RFID permettant la communication avec l'extérieur.

Selon un premier aspect, une solution alternative aux solutions existantes de sécurisation de données contenues dans une carte est proposée.

En outre, une nouvelle carte intelligente capable d'intégrer de nombreuses 10 fonctionnalités est décrite.

Selon un autre aspect, un dispositif enrichi est présenté capable de prendre en compte l'environnement dans lequel il se trouve.

Selon un autre aspect, un dispositif de communication sécurisée est présenté, comprenant une pluralité de circuits applicatifs disposés dans le dispositif qui sont 15 associés chacun à au moins un service applicatif contenu de façon sécurisée au sein du dispositif, chaque circuit applicatif comprenant au moins un détecteur environnemental apte à être excité par un signal externe venant d'un environnement extérieur au dispositif, sensible à un phénomène physique donné caractérisant l'environnement dans lequel se trouve le dispositif, et un émetteur-récepteur de signaux radiofréquences pour la 20 communication avec l'environnement extérieur. Le dispositif comprend également : une unité de commande permettant d'identifier le circuit applicatif excité, le service applicatif associé et d'activer ledit service applicatif en réponse à une autorisation d'activation. Le dispositif comprend également : un circuit biométrique pour authentifier l'utilisateur de façon à générer ladite autorisation d'activation, au moins l'une de la pluralité de circuits 25 applicatifs, associé à l'unité de commande et au circuit biométrique dans le dispositif, est configuré pour détecter le signal externe sur la base du phénomène physique dû au signal externe.

Le dispositif est configuré pour qu'une demande d'autorisation soit transmise dudit circuit applicatif correspondant audit circuit biométrique, et lors de la réception de la demande d'autorisation, ledit circuit biométrique démarre un processus d'authentification pour identifier l'utilisateur, dans lequel ledit circuit biométrique effectue une comparaison

- 5 biométrique avec des données contenues dans le dispositif, et après une comparaison indiquant une reconnaissance biométrique positive, un signal d'accord est envoyé dudit circuit biométrique audit circuit applicatif correspondant pour accorder ladite autorisation d'activation, et dans lequel ledit service applicatif est activé sur la base de ladite autorisation d'activation de telle sorte que ledit circuit applicatif correspondant interagit
- 10 avec l'environnement extérieur.

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.

- 15 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 économique 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.

10 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.

15 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.

20 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.

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

30 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 5 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 10 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 20 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 25 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 un dispositif de communication sécurisée comprenant une pluralité de circuits applicatifs, 30 une unité de commande et un circuit biométrique. L'édit procédé comprend les étapes

suivantes : on détecte un signal externe d'excitation venant d'un environnement extérieur au dispositif au moyen d'un des circuits applicatifs, chaque circuit applicatif, disposé dans le dispositif et comprenant au moins un détecteur environnemental sensible à un phénomène physique donné caractérisant l'environnement dans lequel se trouve le dispositif, et étant associé à au moins un service applicatif contenu de façon sécurisée au sein du dispositif. 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 disposé dans le dispositif, puis on active ledit service applicatif excité en réponse à une autorisation d'activation provenant du circuit biométrique et dans lequel au moins l'une de ladite pluralité de circuits applicatifs, couplé à ladite unité de commande et audit circuit biométrique à l'intérieur du dispositif, détecte ledit signal externe sur la base du phénomène physique donné dû au signal externe, dans lequel une demande d'autorisation est transmise dudit circuit applicatif correspondant audit circuit biométrique, et lors de la réception de la demande d'autorisation, ledit circuit biométrique démarre un processus d'authentification pour identifier un utilisateur, dans lequel ledit circuit biométrique effectue une comparaison biométrique avec des données contenues dans le dispositif, et après une comparaison indiquant une reconnaissance biométrique positive, un signal d'accord est envoyé dudit circuit biométrique audit circuit applicatif correspondant pour accorder ladite autorisation d'activation, et dans lequel le service applicatif est activé sur la base de ladite autorisation d'activation de telle sorte que ledit circuit applicatif correspondant interagit avec l'environnement extérieur.

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 appliquée à un circuit RFID,

5 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 10 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 15 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 20 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 :
5 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 :
10 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
15 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 service 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
20 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.

25 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
30 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
35 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.

5 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.

10 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.

15 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 20 plusieurs émetteur-récepteurs pour déterminer un service applicatif adéquat pour l'environnement en cours.

25 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 :

- 30
- 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.

35 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

interruuteurs 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 5 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 10 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 15 « 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 20 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 :

- 25 - 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 30 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 35 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.

5 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 :

- 10 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,
- 15 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 disposés dans le dispositif qui sont associés chacun à au moins un service applicatif contenu de façon sécurisée au sein du dispositif,
- 5 chaque circuit applicatif comprenant au moins un détecteur environnemental apte à être excité par un signal externe venant d'un environnement extérieur au dispositif, sensible à un phénomène physique donné caractérisant l'environnement dans lequel se trouve le dispositif, et un émetteur-récepteur de signaux radiofréquences pour la communication avec l'environnement extérieur,
- 10 – une unité de commande permettant d'identifier le circuit applicatif excité, le service applicatif associé et d'activer ledit service applicatif en réponse à une autorisation d'activation, et
- 15 – un circuit biométrique pour authentifier l'utilisateur de façon à générer ladite autorisation d'activation
- au moins l'une de la pluralité de circuits applicatifs, associé à l'unité de commande et au circuit biométrique dans le dispositif, est configuré pour détecter le signal externe sur la base du phénomène physique dû au signal externe,
- 20 – le dispositif est configuré pour qu'une demande d'autorisation soit transmise dudit circuit applicatif correspondant audit circuit biométrique, et lors de la réception de la demande d'autorisation, ledit circuit biométrique démarre un processus d'authentification pour identifier l'utilisateur, dans lequel ledit circuit biométrique effectue une comparaison biométrique avec des données contenues dans le dispositif, et après une comparaison indiquant une reconnaissance biométrique positive, un signal d'accord est envoyé dudit circuit biométrique audit circuit applicatif correspondant pour accorder ladite autorisation d'activation, et dans lequel ledit service applicatif est activé sur la base de ladite autorisation d'activation de telle sorte que ledit circuit applicatif correspondant interagit avec l'environnement extérieur.

2. Dispositif selon la revendication 1, selon lequel, les circuits applicatifs comprennent au moins un connecteur métallique.

3. Dispositif selon l'une quelconque des revendications 1 et 2, selon lequel les

5 circuits applicatifs comprennent au moins l'un des éléments suivants :

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

4. Dispositif selon l'une quelconque des revendications 1 à 3, selon lequel le circuit biométrique comprend un capteur biométrique associé à une unité de calcul pour traiter 15 des données biométriques.

5. Dispositif selon l'une quelconque des revendications 1 à 4, comprenant une interface homme-machine pour indiquer un état de fonctionnement du dispositif.

20 6. Dispositif selon l'une quelconque des revendications 1 à 5, ledit dispositif étant alimenté par une pile flexible ou non, rechargeable ou non.

7. Dispositif selon l'une quelconque des revendications 1 à 5, ledit dispositif étant alimenté par une source externe.

25 8. Dispositif selon l'une quelconque des revendications 1 à 7, ledit dispositif étant sous un format de carte à puce, de clé USB, ou d'étiquette électronique.

9. Procédé mis en œuvre dans un dispositif de communication sécurisée comprenant une pluralité de circuits applicatifs, une unité de commande et un circuit 30 biométrique ; ce procédé comprenant les étapes suivantes :

on détecte un signal externe d'excitation venant d'un environnement extérieur au dispositif au moyen d'un des circuits applicatifs, chaque circuit applicatif, disposé dans le dispositif et comprenant au moins un détecteur environnemental sensible à un phénomène physique donné caractérisant l'environnement dans lequel

5 se trouve le dispositif, et étant associé à au moins un service applicatif contenu de façon sécurisée au sein du dispositif,

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

10 biométrique disposé dans le dispositif, puis on active ledit service applicatif excité en réponse à une autorisation d'activation provenant du circuit biométrique, et

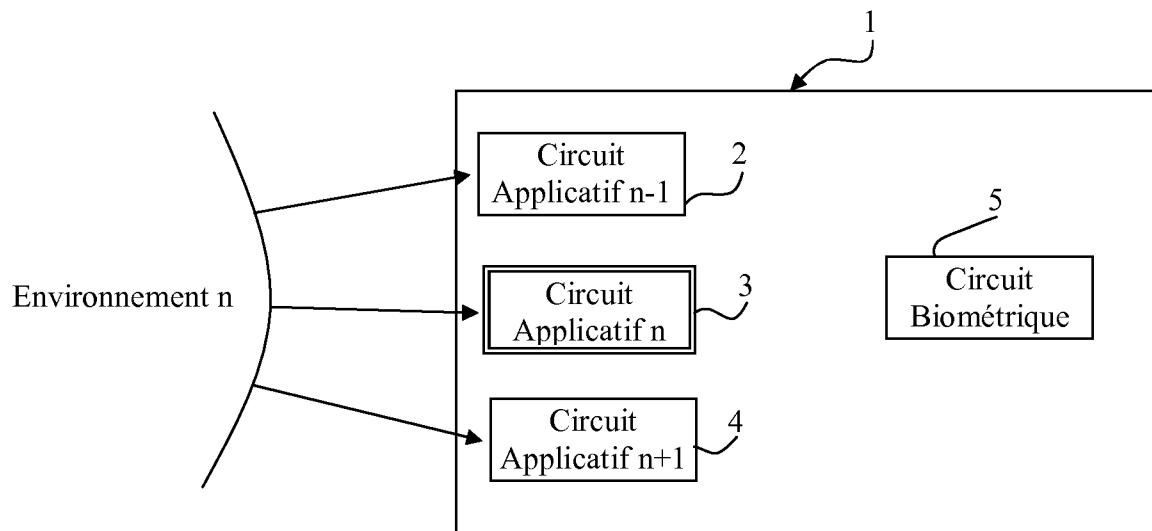
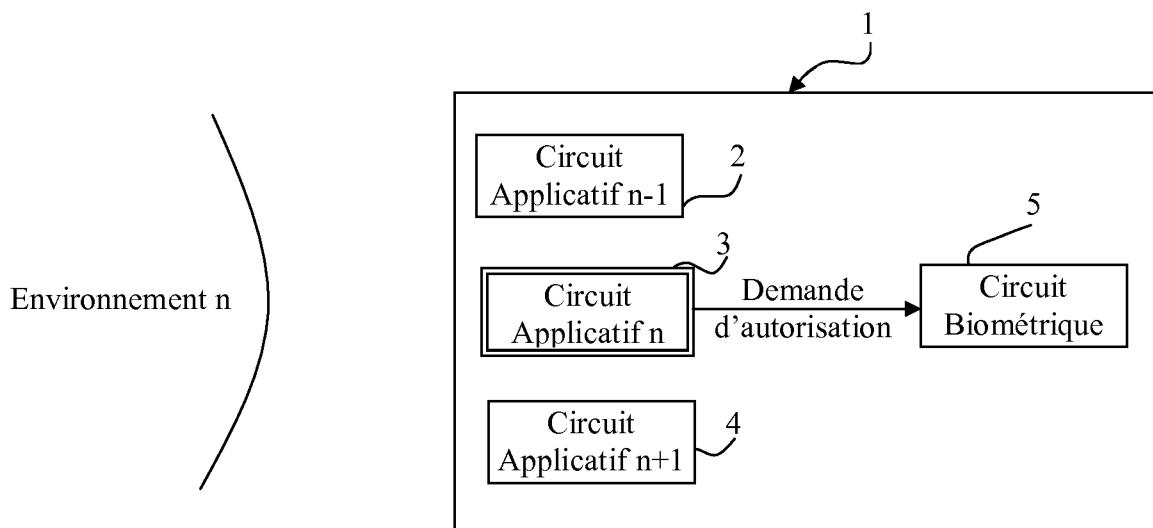
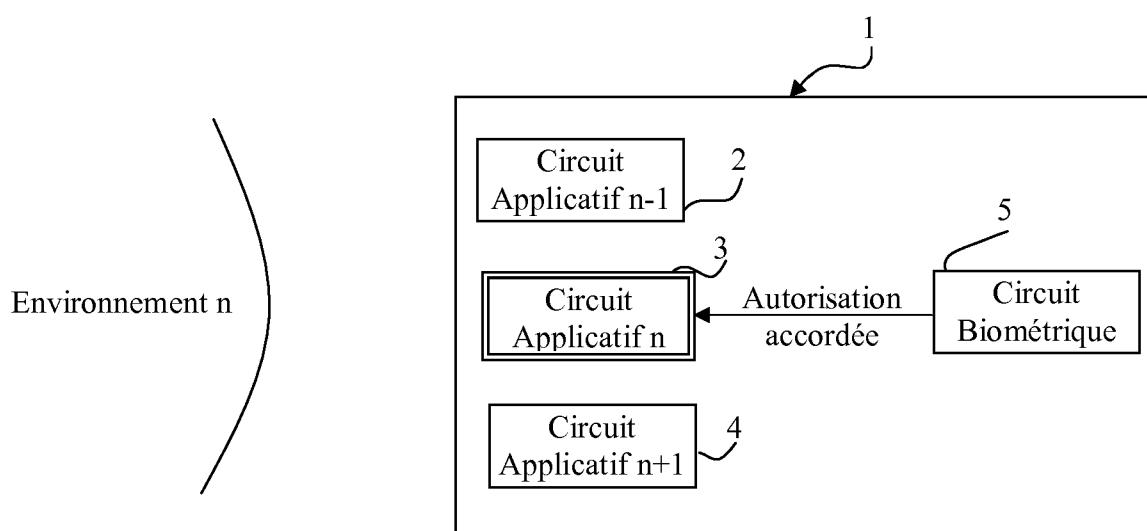
dans lequel au moins l'une de ladite pluralité de circuits applicatifs, couplé à ladite unité de commande et audit circuit biométrique à l'intérieur du dispositif, détecte ledit signal externe sur la base du phénomène physique donné

15 dû au signal externe, dans lequel une demande d'autorisation est transmise dudit circuit applicatif correspondant audit circuit biométrique, et lors de la réception de la demande d'autorisation, ledit circuit biométrique démarre un processus d'authentification pour identifier un utilisateur, dans lequel ledit circuit biométrique effectue une comparaison biométrique avec des données contenues dans le

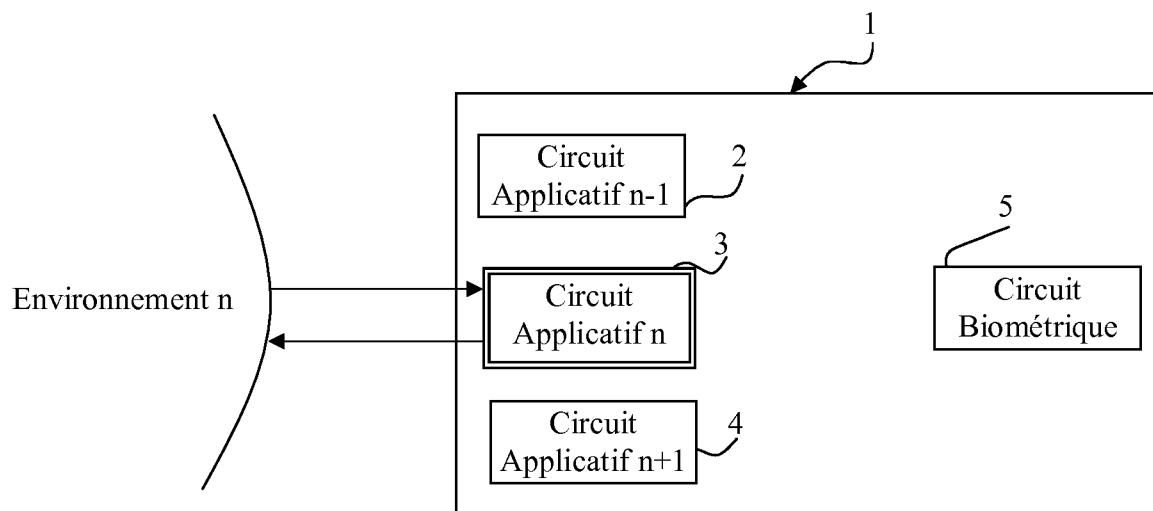
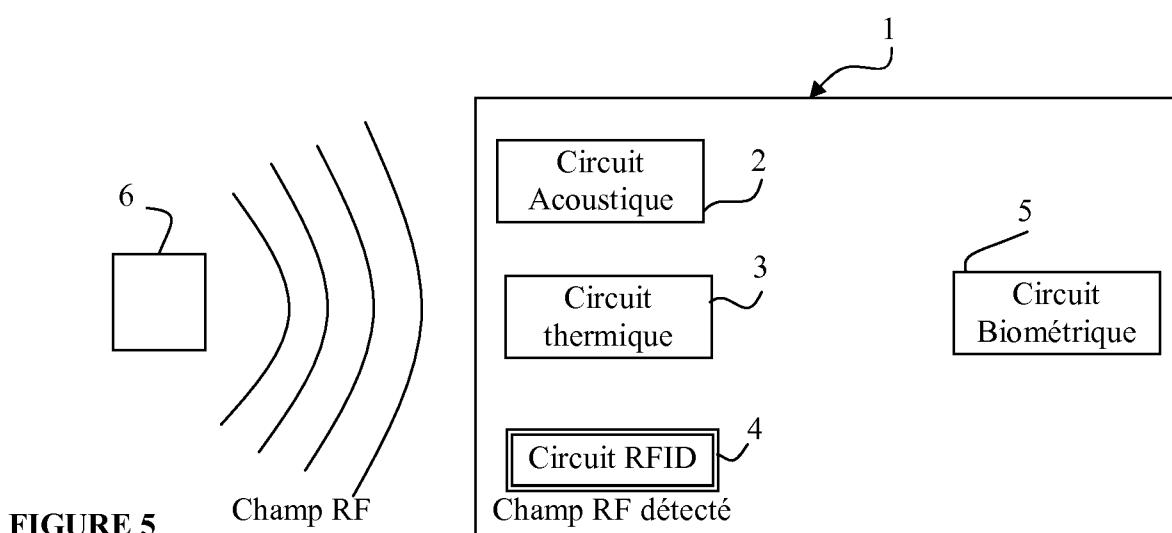
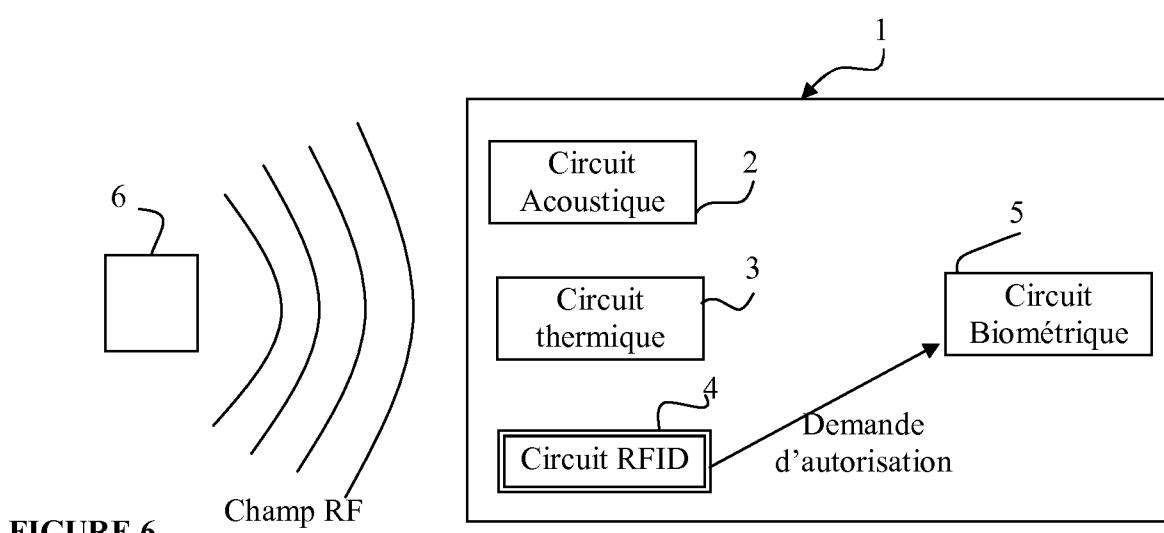
20 dispositif, et après une comparaison indiquant une reconnaissance biométrique positive, un signal d'accord est envoyé dudit circuit biométrique audit circuit applicatif correspondant pour accorder ladite autorisation d'activation, et dans lequel le service applicatif est activé sur la base de ladite autorisation d'activation de telle sorte que ledit circuit applicatif correspondant interagit avec

25 l'environnement extérieur.

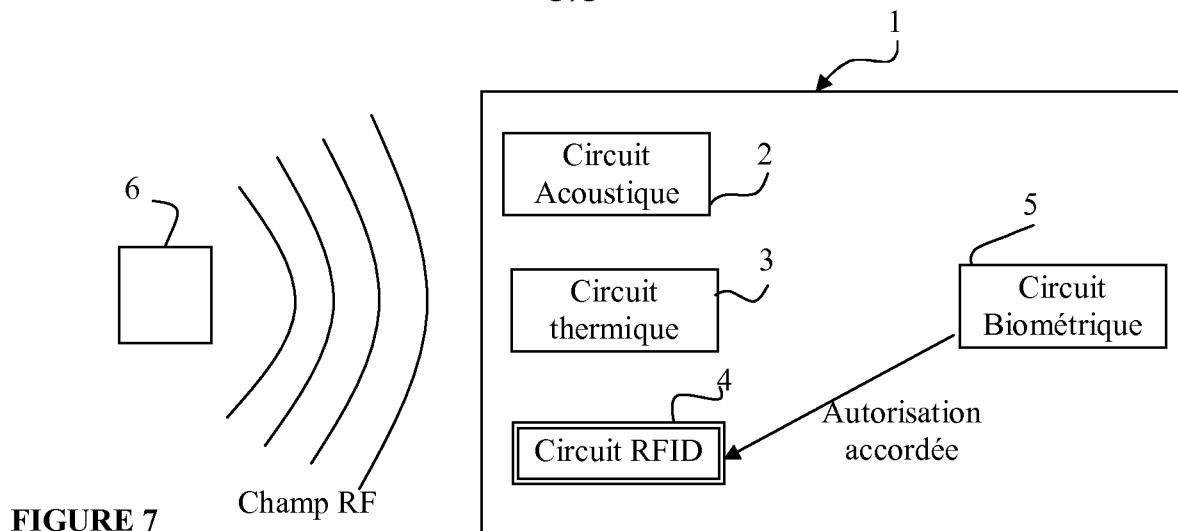
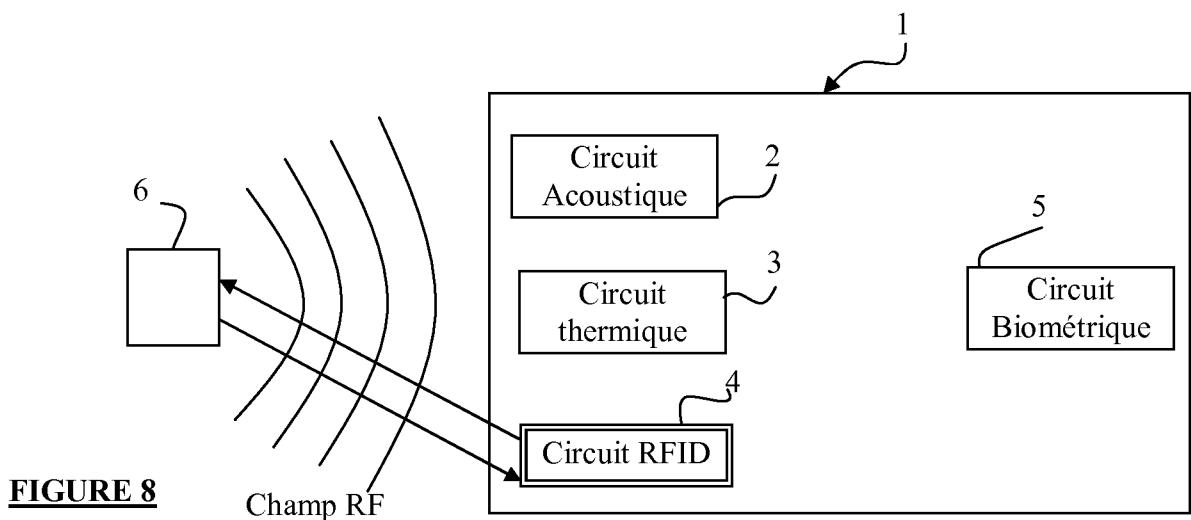
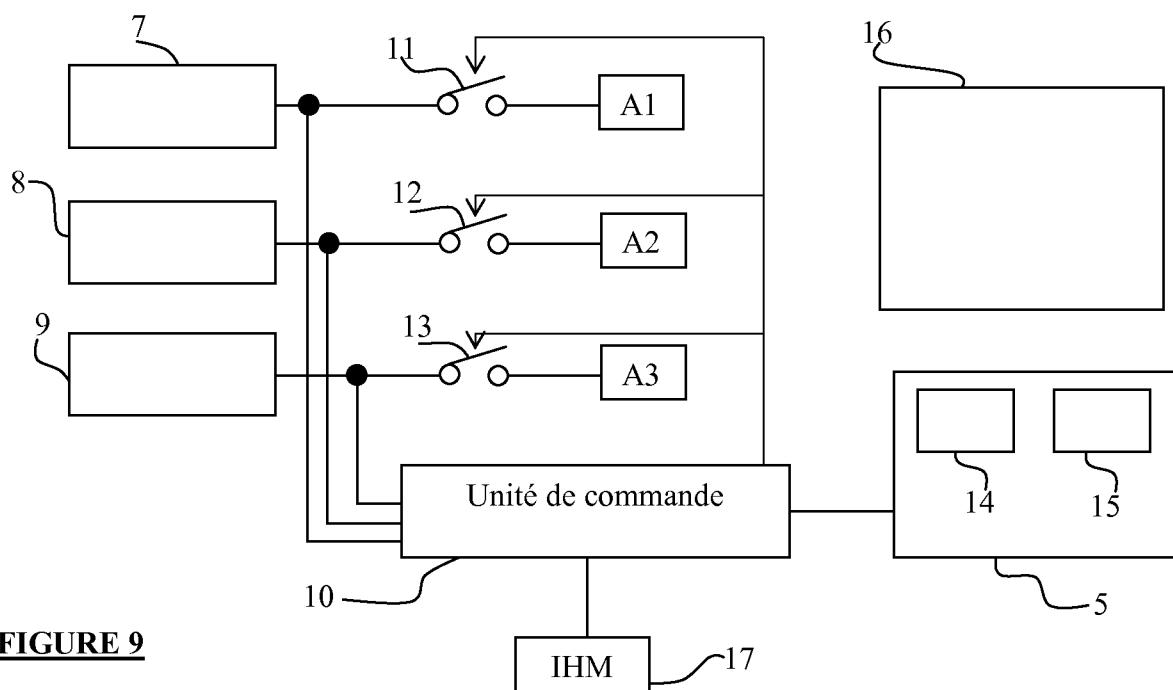
1/3

**FIGURE 1****FIGURE 2****FIGURE 3**

2/3

**FIGURE 4****FIGURE 5****FIGURE 6**

3/3

**FIGURE 7****FIGURE 8****FIGURE 9**

