(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 967 801**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **10 59564**

(51) Int Cl[8] : ***G 06 F 21/00*** *(2012.01), G 07 F 7/08, G 06 K 9/00*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 19.11.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 25.05.12 Bulletin 12/21.

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

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

(71) **Demandeur(s) :** *OBERTHUR TECHNOLOGIES Société anonyme* — FR.

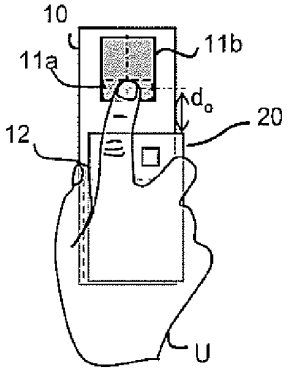
(72) **Inventeur(s) :** AUBIN YANN LOIC.

(73) **Titulaire(s) :** OBERTHUR TECHNOLOGIES Société anonyme.

(74) **Mandataire(s) :** MARKS & CLERK FRANCE.

(54) SYSTEME BIOMETRIQUE D'ACCES SECURISE UTILISANT UNE CARTE A MICROCIRCUIT(S) ET ANTENNE.

(57) Un système de contrôle d'accès biométrique, pour autoriser l'accès à des fonctions ou services, comporte un terminal de contrôle 10 muni d'un capteur de données biométriques et d'un système de communication radiofréquence incluant une antenne AT pour la communication radiofréquence entre le terminal de contrôle et une carte à microcircuit(s) 20 comportant elle-même une antenne. La carte contient un gabarit biométrique d'un doigt au moins d'un utilisateur autorisé. Le terminal comporte une surface supérieure incluant une surface de capture 1 a de données biométriques relatives à un doigt et le capteur de données biométriques dans cette surface. La configuration de l'antenne du terminal et la surface de capture est telle que lorsque la carte 20 est tenue dans la main d'un utilisateur U avec un doigt s'étendant vers l'avant, et qu'elle est présentée à la surface supérieure du terminal, l'antenne de la carte est apte à communiquer avec l'antenne du terminal à la fin d'un mouvement de la main permettant la capture des données biométriques du doigt étendu vers l'avant au-dessus de la surface de capture.



FR 2 967 801 - A1

SYSTEME BIOMETRIQUE D'ACCES SECURISE UTILISANT UNE CARTE A MICROCIRCUIT(S) ET ANTENNE

DOMAINE DE L'INVENTION

Le domaine de l'invention est celui de l'accès sécurisé ou réglementé à des lieux, des biens ou des services, par identification biométrique.

ETAT DE L'ART

Les techniques d'identification biométrique sont basées sur des mesures de caractéristiques physiques ou biologiques propres à chaque individu, et stables tout le long de la vie. Ces techniques sont notamment utilisées dans des applications de contrôle d'accès automatique à des locaux. La sécurité de ces systèmes de reconnaissance biométriques repose sur la nature de l'information qui est contrôlée, considérée comme sûre en elle-même, parce qu'elle est par nature unique pour chaque personne. Elle suppose cependant de détecter des éventuelles fraudes. Certains capteurs biométriques intègrent ainsi une fonction de détection de mouvement, permettant de vérifier que l'échantillon biométrique présenté est bien vivant. Par exemple des capteurs d'empreinte digitale peuvent effectuer des mesures de pression sanguine, battements de cœur, conductivité ...Un capteur du motif d'un iris peut intégrer un dispositif destiné à déclencher une réaction oculaire, par exemple un faible éclairage, ou un bref jet d'air. La détection de la réaction valide l'échantillon saisi.

Ces systèmes d'identification biométrique utilisent généralement une base de données, sur un serveur informatique, dans laquelle sont stockés les gabarits biométriques de toutes les personnes autorisées et des terminaux de contrôle associés à des capteurs biométriques pour vérifier qu'une personne qui se présente, est bien une personne autorisée. On trouve essentiellement deux modes de vérification : comparaison de l'échantillon biométrique capturé par le terminal, aux gabarits enregistrés dans la base ; lecture d'un identifiant contenu dans un badge d'accès et comparaison de l'échantillon biométrique capturé par le terminal, au gabarit enregistré dans la base pour cet identifiant.

Ces systèmes à base de données se révèlent assez lents, notamment à cause du temps d'interrogation de la base, ainsi que complexes à gérer. En outre la gestion de ces bases de données

biométriques peut poser des problèmes sur le plan légal, selon les pays quant à l'utilisation de données personnelles.

Pour éviter l'utilisation d'une telle base de données, la demande US2006/0274920 propose un enregistrement du gabarit de l'empreinte digitale d'une personne autorisée, dans une bague ou un bracelet muni d'un circuit électronique avec mémoire et équipé de moyens de communication radiofréquence. Mais la communication radiofréquence avec la bague est difficile, tant pour des aspects de surface d'antenne que de position et orientation par rapport à un lecteur. En outre elle ne permet pas une authentification et de la bague et de son porteur.

Par ailleurs, on connaît bien les systèmes d'accès sécurisés par cartes sans contact, dans lesquels une carte est personnalisée avec des données d'identification qui sont vérifiées à chaque utilisation de la carte, par un protocole d'authentification initié à l'ouverture de chaque session de communication sans contact entre la carte et un terminal de lecture. Ces protocoles d'authentification bien connus, basés sur l'utilisation d'algorithme de cryptographie symétriques, à clefs privées (par exemple 3DES ou AES) ou asymétriques, à clés publiques et privées (par exemple RSA, ECC ou autres), permettent d'authentifier la carte.

Il est cependant souhaitable d'authentifier non seulement la carte, mais aussi son porteur. Cette double authentification permet la double assurance que la carte n'est pas fausse, et que son utilisateur est légitime. C'est cette capacité à sécuriser l'accès à un niveau suffisamment élevé, qui conditionne le développement de ces modes d'accès sécurisé, facile et rapide à des biens ou des services de la vie courante : transactions financières de faibles montants, accès à un local sécurisé, accès à des données confidentielles contenues dans un ordinateur ou dans une clef USB, passage de barrières, par exemple dans les transports, ...

Une technique bien connue d'authentification des porteurs de carte est l'authentification par mot de passe, ou code PIN. Mais si cette technique est parfaitement intégrée dans le contexte des cartes dites à contact, où la carte est insérée dans un lecteur qui comporte un clavier (carte bancaire et terminal de paiement, carte intelligente et ordinateur, carte sim et téléphone portable), cette technique convient mal dans un contexte

d'authentification du type sans contact, où l'on cherche une authentification rapide, au vol.

RESUME DE L'INVENTION

Pour permettre une telle authentification, l'invention se propose de combiner identification biométrique et authentification dans un système de contrôle d'accès basé sur un protocole de communication sans contact, pour authentifier la carte et le porteur légitime de la carte. L'invention propose ainsi un système de contrôle d'accès pour autoriser l'accès à des fonctions ou services à un utilisateur, le système comportant un terminal de contrôle muni d'un capteur biométrique et d'un système de communication radiofréquence incluant une antenne pour la communication radiofréquence entre le terminal de contrôle et une carte à microcircuit(s) comportant elle-même une antenne, le terminal comportant une surface supérieure incluant une surface de capture de données biométriques relatives à un doigt, caractérisé en ce que les positions relatives de l'antenne du terminal et de la surface de capture sont telles que lorsque la carte est tenue dans la main d'un utilisateur avec un doigt s'étendant vers l'avant, et présentée à la surface supérieure du terminal, l'antenne de la carte est apte à communiquer avec l'antenne du terminal à la fin d'un mouvement de la main permettant la capture des données biométriques du doigt étendu vers l'avant au-dessus de la surface de capture. L'invention concerne aussi un protocole d'authentification qui authentifie la carte et le porteur sur la base de données biométriques enregistrées dans la carte. L'invention concerne encore un procédé de contrôle d'accès biométrique, pour autoriser l'accès à des fonctions ou services, comprenant

-une étape d'enregistrement d'un gabarit biométrique au moins d'un utilisateur autorisé dans une carte à microcircuit(s) comportant une antenne,

-une étape d'ouverture d'une session de communication radiofréquence entre la carte et un terminal de contrôle muni d'un capteur biométrique avec une surface de capture de données biométriques relatives à un doigt sur une surface supérieure du terminal et d'un système de communication radiofréquence incluant une antenne,

-une étape de capture de données biométriques relatives à un doigt d'un porteur de la carte, par le capteur biométrique du terminal, caractérisé en ce que lesdites étapes d'ouverture de session et de capture sont obtenues par une présentation de la carte tenue en main avec un doigt étendu vers l'avant, à la surface supérieure du terminal telle que l'antenne de la carte est apte à communiquer avec l'antenne du terminal à la fin d'un mouvement de la main permettant la capture des données biométriques d'un doigt étendu vers l'avant au-dessus de la surface de capture.

D'autres avantages et caractéristiques sont décrits dans la description détaillée suivante d'un mode de réalisation de l'invention, en référence aux dessins annexés dans lesquels :

-la figure 1 illustre schématiquement une carte à microcircuit(s) et antenne pour la communication radiofréquence, utilisé dans un système de contrôle d'accès selon l'invention;

-la figure 2 est un schéma simplifié d'un système de contrôle d'accès selon l'invention utilisant une carte à microcircuit(s) et antenne,

-les figures 3 et 4 illustrent un mode de présentation d'une carte pour authentification, dans un mode de capture d'une empreinte ou d'une image du réseau veineux d'un doigt, par glissement du doigt sur une surface de capture biométrique;

-la figure 5 illustre un autre mode de présentation, dans lequel le doigt est simplement posé sur la surface de capture;

-la figure 6 représente une carte munie de moyens facilitant le positionnement d'un doigt aux fins de la capture des données biométriques de ce doigt,

-les figures 7a à 7d illustrent l'utilisation d'un système de contrôle d'accès selon l'invention pour différentes inclinaisons de la surface supérieure du terminal et

-la figure 8 est un synoptique illustrant les différentes étapes d'un protocole d'authentification initié à chaque ouverture de session de communication sans contact, entre une carte à microcircuit(s) et antenne et le terminal, dans un exemple de mise en œuvre de l'invention.

DESCRIPTION DETAILLEE

L'invention utilise les techniques d'identification biométrique. A ce titre, il est utile de préciser quelques notions ou termes associés avant de décrire plus particulièrement le système de contrôle d'accès selon l'invention qui utilise une telle identification.

Un gabarit biométrique, aussi bien qu'un échantillon biométrique, est un ensemble de données binaires obtenues après acquisition d'image(s) par un capteur et traitement numérique des données correspondantes. Le gabarit et l'échantillon biométrique à comparer sont obtenus par les mêmes techniques de capture de données biométriques et de traitement numérique de ces données. Plus précisément, on ne prend pas toutes les données biométriques acquises par le capteur, car cela représente des fichiers de taille déraisonnable. Aussi les données acquises par le capteur sont exploitées par des algorithmes de traitement numérique, pour former un gabarit ou un échantillon biométrique, représentatif de la personne et de taille raisonnable. Les traitements appliqués dépendent de la nature des données biométriques saisies, et du mode d'acquisition. Si on prend l'exemple d'un capteur optique d'une empreinte digitale, le traitement consiste en un traitement d'image pour extraire un certains nombre de données caractéristiques. Ces données caractéristiques peuvent être des minuties, qui sont des creux locaux qui apparaissent en tant que terminaison ou bifurcation, ou des caractéristiques plus macroscopiques telles que des cambrures, des boucles, des spirales. Au final on obtient un gabarit biométrique représentatif, permettant une identification fiable par comparaison à un échantillon biométrique obtenu par les mêmes traitements, et de taille raisonnable, comprise entre 100 et 1500 octets typiquement. On entend par identification fiable, une identification qui assure un taux de faux rejets (pourcentage de personnes rejetées par erreur), un taux de fausses acceptations (pourcentage d'acceptation de personnes par erreur), et un taux d'égale erreur (pourcentage de cas où l'on ne peut pas décider) acceptables.

Le gabarit biométrique correspond à ce qui est enregistré en mémoire comme modèle de référence. Dans l'invention, il est enregistré dans la carte.

L'échantillon biométrique correspond à ce qui est enregistré temporairement, en "live", aux fins d'une comparaison immédiate avec un

gabarit. Dans l'invention, il est obtenu et mémorisé temporairement dans le terminal de contrôle.

Dans l'invention, les données biométriques considérées sont celles d'une empreinte digitale et/ou du dessin du réseau veineux d'un doigt. C'est ce qui permet, comme expliqué en détail ci-après, de permettre l'authentification selon l'invention, d'un seul geste et d'une seule main d'un porteur tenant en main la carte dans laquelle est enregistré le gabarit.

Les capteurs biométriques correspondants peuvent être de technologies variées. D'une manière générale, ces capteurs se composent d'une surface de présentation d'un doigt, avec un élément de capture de données biométriques dans cette surface et d'éléments de traitement numérique (microprocesseur, mémoire, interface de données). La surface de présentation peut être une surface transparente telle qu'un verre ou une surface métallique, en fonction de la technologie de capture employée.

La littérature technique et commerciale abonde d'exemples de tels capteurs. En matière de capteurs d'empreinte digitale on peut par exemple citer des capteurs optiques CCD (capteur "CMOS sensor" de la société DELSY), des capteurs capacitifs (Finger TIP™ de Infinéon), des capteurs électro-thermiques (FingerCHIP™ de Atmel) ou encore des capteurs de champ électrique ou de pression. En matière d'image de réseau veineux, ce sont des capteurs d'image infra-rouge qui sont utilisés (Palmscure™ de Fujitsu).

Dans l'invention, on utilise un tel capteur biométrique pour permettre un contrôle d'accès sécurisé, avec reconnaissance biométrique, au moyen d'une carte 20 à microcircuit(s), à antenne A_C, comme illustré sur la figure 1. La carte 20 comprend de manière bien connue, une puce 21 à microprocesseur avec mémoire, qui contient le gabarit biométrique B_T et l'antenne radiofréquence A_C, intégrée dans l'épaisseur de la carte et connectée à la puce 21.

Un système de contrôle d'accès selon l'invention est schématiquement illustré sur la figure 2. Il comprend un terminal de contrôle 10 intégrant un capteur biométrique 11 avec une surface de capture 11a à la surface 10a du terminal, et un lecteur 12, relié à une antenne A_T pour la communication radiofréquence entre le terminal de contrôle et la carte 20 illustrée à la figure 1.

Le capteur biométrique du terminal permet de saisir un échantillon biométrique BS d'un doigt aux fins de comparaison avec un gabarit correspondant contenu dans la carte, qui aura été obtenu par la même technique de capture.

La capture des données biométriques est obtenue en présentant un doigt au dessus de la surface de capture 11a, en considérant la surface de capture dans un plan horizontal. Le terme "au-dessus" signifie aussi bien "sur" que "à faible distance".

En pratique, une surface de présentation de doigt(s) 11b est matérialisée à la surface 10a du terminal, et la surface de capture est dans la surface de présentation.

Dans l'exemple illustré sur les figures 2 à 4, la surface de capture 11a est plus petite que la surface de présentation 11b. Cette configuration correspond un mode de capture dynamique dit "*swipe*", avec glissement du doigt au-dessus de la surface de capture, dans lequel le capteur relève une série d'images correspondant au défilement des différentes parties du doigt sur l'élément de capture et l'échantillon biométrique est formé à partir de cette série d'images. Ce mode de capture correspond notamment à des capteurs du type électrothermique, qui relèvent des différences de chaleur, tel le capteur électrothermique FingerCHIP™ de la société Atmel. Ces capteurs ont l'avantage d'être petits, se présentant sous forme d'une barrette multilinéaire.

Dans l'exemple illustré sur la figure 5, la surface de capture 11a correspond sensiblement à celle de la surface de présentation 11b. Le capteur relève une image du doigt présenté à l'arrêt au-dessus de la surface de capture, et fournit un échantillon biométrique correspondant. On trouve ce mode de capture par exemple dans les capteurs CCD.

Les positions relatives de la surface de capture et de l'antenne AT du terminal sont telles que lorsque la carte est tenue dans la main d'un utilisateur avec un doigt s'étendant vers l'avant (cf flèche sur la figure 1), et qu'elle est présentée à la surface supérieure du terminal, l'antenne de la carte est apte à communiquer avec l'antenne du terminal à la fin d'un mouvement de la main permettant la capture des données biométriques du doigt étendu vers l'avant au-dessus de la surface de capture.

Par l'expression "doigt étendu vers l'avant", on entend le fait que le doigt s'étend sensiblement dans un plan parallèle à la direction de l'avant-bras de l'utilisateur, et dans le sens allant du coude vers la main, l'extrémité du doigt débordant dans ce sens au-delà du bord de la carte. Les figures 7a à 7c illustrent bien cette définition, pour différentes orientations du plan de surface supérieure du terminal de contrôle par rapport à un utilisateur qui présente sa carte comme indiqué.

En tenant compte de cette définition de "l'avant", le mouvement de déplacement de la main tenant la carte avec un doigt étendu vers la main, peut être un mouvement de l'avant vers l'arrière ou de l'arrière vers l'avant ou même un mouvement de côté.

A la fin de ce mouvement de la main, le doigt est au-dessus de la surface de capture et l'antenne de la carte est dans une position optimale, ou proche de cette position optimale, pour la communication radiofréquence avec l'antenne du terminal. Idéalement, l'antenne de la carte arrive dans la position optimale pour la communication avec l'antenne du terminal, c'est-à-dire dans la position où l'échange d'énergie radioélectrique entre les deux antennes est maximisé. Mais, compte-tenu de la variété possible de la longueur de doigt ou de la manière d'étendre le doigt vers l'avant, la carte peut se trouver un peu décalée par rapport à la position optimale mais dans une position permettant une bonne communication permettant l'échange de données entre la carte et le terminal.

La communication radiofréquence entre le terminal et la carte est un protocole de communication sans contact standard, tel que décrits par exemple dans les normes ISO 14443-3 et -4, types A ou B, Mifare, FeliCa, ou encore NFC.

Les antennes utilisées dans ces communications radiofréquence en champ proche, sont typiquement des antennes cadre, c'est-à-dire formées de plusieurs spires réalisées dans un plan de surface (antenne 2D) ou en volume (antenne 3D). Ces spires sont généralement de forme sensiblement circulaire ou rectangulaire : le centre d'antenne est alors le centre des spires. Typiquement, l'antenne A_C de la carte est une antenne réalisée dans le plan de surface. Pour une carte à microcircuit(s) standard, conforme à la norme ISO 7816 (dimensions de la carte) et à la norme ISO 14443 (communication radiofréquence), c'est une antenne qui comporte

généralement 2 à 5 spires, réalisées sur la périphérie, avec une distance entre spires avoisinantes de l'ordre de 1,5 mm, la spire la plus externe étant à environ 2,5 mm du bord de carte. Elle est habituellement réalisée sur tout le périmètre de la carte comme illustrée sur la figure 1, ou seulement la moitié (carte à demi-antenne, dite carte ID1), plus précisément sur toute la longueur l mais seulement une demi-largeur w de la carte. Dans le terminal, ce peut être une antenne 2D également. Ce sera plus souvent une antenne 3D, c'est-à-dire réalisée en volume dans l'épaisseur du terminal, comme schématiquement illustré sur la figure 2. Dans les deux cas les spires de l'antenne sont dans un plan parallèle à la surface externe (de la carte, du terminal). Elles ont un axe de symétrie orthogonal au plan de surface supérieure du terminal, et qui coupe la surface supérieure du terminal au point o comme illustré sur la figure 2. Sa surface ou son volume peut être important, et occuper plus ou moins d'espace dans le terminal, en fonction de la technologie d'antenne retenue et la puissance recherchée.

Dans l'exemple illustré sur les figures 2 à 5, l'antenne du terminal est disposée à côté de la surface de capture. Dans cet exemple, on peut définir les positions relatives de l'antenne du terminal et de la surface de capture par la distance d entre l'antenne du terminal et la surface de capture.

Cette distance d entre la surface de capture et l'antenne du terminal peut se définir de manière simple, comme la distance entre le centre de la surface de capture et le point o défini ci-dessus, et illustré sur la figure 2.

Mais l'invention ne se limite pas à cette configuration. D'autres configurations sont possibles. Notamment l'antenne du terminal peut occuper une surface plus grande, avec la surface de capture qui se retrouve en tout ou partie à "l'intérieur" de l'antenne. Elles sont alors disposées l'une par rapport à l'autre de manière appropriée, pour produire l'effet technique recherché, à savoir que l'antenne de la carte est apte à communiquer avec l'antenne du terminal à la fin d'un mouvement de la main permettant la capture des données biométriques du doigt étendu vers l'avant au-dessus de la surface de capture.

De manière bien connue, les dimensions de l'antenne de la carte, et la position de cette antenne par rapport à l'antenne du terminal sont

déterminantes pour une communication radiofréquence performante avec l'antenne du terminal de contrôle. En effet, dans ces systèmes, la carte est télé-alimentée par le terminal, et la transmission radiofréquence par la carte se fait par rétro-modulation de courant. C'est ainsi que l'antenne de la carte doit avoir une surface suffisamment grande, car c'est ce qui conditionne sa capacité à moduler le champ électrique qu'elle reçoit, et doit être positionnée correctement dans le champ magnétique rayonné par l'antenne du terminal. Il existe une position optimale où l'échange d'énergie est maximisé. Cette position varie d'un lecteur et/ou d'une carte à l'autre en fonction des caractéristiques des antennes. Elle peut se définir par un positionnement en x et y de la carte par rapport au plan de surface du terminal, la carte étant présentée sensiblement parallèle, ou légèrement inclinée, par rapport au plan de surface du terminal, et typiquement à une distance inférieure à dix centimètres environ de ce plan. Le système de contrôle d'accès selon l'invention permet un placement de la carte dans une position optimale ou proche de la position optimale relativement à l'antenne du terminal pour la communication radiofréquence, et ce de manière naturelle, automatique pour tout un chacun, en un geste unique.

En pratique, le terminal de contrôle se présente sous forme d'une borne d'accès, présentant à sa surface supérieure 10a la surface de capture 11a du capteur biométrique intégrée au terminal, et un lecteur 12 avec un système de communication radiofréquence comprenant l'antenne radiofréquence AT.

Compte tenu de la définition de "l'avant", et en se plaçant dans les conditions d'un utilisateur qui se trouve face à la borne, et en considérant une surface du terminal en vue de dessus, la surface de capture 11a est placée sur la partie la plus en avant de la borne du terminal et l'antenne AT du terminal est placée à côté de la surface de capture, et en arrière. L'utilisateur U, c'est-à-dire le porteur de la carte, tient la carte dans la main avec un doigt étendu vers l'avant, typiquement l'index ou le majeur, et les autres repliés autour de la carte, c'est-à-dire au moins le pouce et deux doigts (l'annulaire et l'auriculaire) et présente l'extrémité de ce doigt dans la surface de capture 11a du terminal. Ce geste du porteur est facile, car quasi-naturel. Dans une variante non illustrée, la surface de capture comprend deux surfaces de capture, une pour chacun des deux doigts, index et majeur.

Le système peut alors être configuré pour recueillir les deux empreintes, et utiliser une des empreintes ou les deux, dans le processus d'authentification, la carte contenant alors deux gabarits correspondants.

La présentation du ou des doigts au-dessus de la surface de capture sur le terminal peut-être facilitée comme représenté sur la figure 6 par des moyens de positionnement du ou des doigts, prévus sur la carte. Ces moyens prévus sur la carte peuvent comprendre une encoche 22, et/ou un repère graphique 23. De tels éléments s'obtiennent facilement par des contours ou formes moulées ou découpées, et par des étapes de personnalisation graphique. Il est facile d'intégrer leur réalisation dans le processus standard de fabrication des cartes : l'encoche est réalisée avec la découpe de la carte, typiquement par estampage ; le repère est ajouté aux motifs et/ou inscriptions figurant sur la carte, dans l'étape de personnalisation graphique de la carte.

L'encoche est avantageuse, car elle facilite la prise en main de la carte. Le dessin des spires de l'antenne de la carte est alors adapté pour tenir compte de cette découpe.

On pourra encore noter que la borne du terminal peut se présenter à l'utilisateur avec une surface supérieure dans un plan de surface horizontal, incliné vers l'utilisateur, ou dans l'autre sens, voire sensiblement vertical, comme respectivement illustré sur les figures 7a à 7d. Le geste à reproduire avec la carte en main pour effectuer la capture et déclencher le contrôle d'accès est sensiblement aussi aisé dans toutes ces configurations.

Les figures 2, 3 et 4 illustrent la configuration d'un système intégrant un capteur à mode de capture dynamique, avec glissement du doigt (ou des doigts) au-dessus de la surface de capture. Ce mode de capture dit "*swipe*" correspond notamment à des capteurs du type thermique, qui relèvent des différences de chaleur, par exemple le capteur électro-thermique FingerCHIP™ de la société Atmel. Ces capteurs ont l'avantage d'être petits.

Dans l'exemple illustré (figures 2 à 4), la surface de présentation et la surface de capture sont agencées dans une configuration qui s'accorde avec un mouvement de l'avant vers l'arrière. D'autres configurations sont possibles. Par exemple, la surface de présentation et la surface de capture dans cette surface de présentation peuvent être agencées pour une capture

correspondant à un glissement correspondant à un mouvement de la main de gauche à droite (ou de droite à gauche).

La surface de présentation 11b plus grande que la surface de capture 11a, s'accorde au mouvement de la main amenant le doigt en amont de la surface de capture, avant de le faire glisser, assurant le défilement de toutes les parties utiles du doigt sur la surface de capture. A la fin du mouvement de la main, l'extrémité du doigt est sensiblement dans la surface de capture. A la fin de ce mouvement de la main et comme illustré sur la figure 4, la carte est dans la position optimale, ou proche de cette position optimale, pour la communication radiofréquence avec l'antenne du terminal. Typiquement, dans cette position optimale, en projetant la carte sur la surface du terminal, le centre de la surface de capture est à une distance d_o de l'ordre de 2 à 4 centimètres du bord de la carte.

La figure 5 illustre un autre mode de capture, statique, des données biométriques d'un doigt présenté à l'arrêt, au-dessus de la surface de capture. Le capteur relève une seule image, à partir de laquelle il forme l'échantillon biométrique. A la fin du mouvement de la main, le doigt est en arrêt au-dessus de la surface de capture, et la carte est dans la position optimale ou proche de cette position optimale pour la communication radiofréquence avec l'antenne du terminal, c'est-à-dire distante de 2 à 4 cm du centre de surface de capture.

Le système de contrôle d'accès sécurisé dont deux mises en œuvre viennent d'être décrites, permet de comparer un échantillon biométrique du porteur U, saisi par le terminal au moyen du capteur biométrique, à un gabarit biométrique B_T enregistré dans la carte, à l'intérieur d'un protocole d'authentification. Ce protocole est du type à deux facteurs (la présence de la carte et l'échantillon biométrique : empreinte digitale ou image du réseau veineux), permettant une authentification de la carte auprès du porteur et également une authentification mutuelle entre la carte et le lecteur (basée de façon classique sur un échange d'aléas encryptés) dans un processus d'échanges de données par transmission radiofréquence entre le terminal et la carte.

Ce processus d'authentification est initié par la capture de l'échantillon et l'initialisation d'une session de communication radiofréquence

entre la carte et le terminal. Il comprend la comparaison biométrique entre l'échantillon saisi par le terminal et le gabarit mémorisé dans la carte. Cette comparaison peut être réalisée dans la carte ou le terminal.

De manière plus détaillée, le terminal transmet à la carte l'échantillon biométrique crypté et signé par lui ; la carte transmet au terminal des données d'identification biométrique, qui sont soit le gabarit biométrique (quand la comparaison biométrique est réalisée par le terminal), soit le résultat de la comparaison biométrique (quand la comparaison biométrique est réalisée par la carte), cryptées et signées par lui.

Les données cryptées et signées reçues par la carte, lui permettent d'authentifier le terminal. La carte peut ensuite lui transmettre les données d'identification biométrique.

Les données d'identification cryptées et signées reçues en retour par le terminal, lui permettent d'authentifier la carte par vérification de la signature des données d'identification biométrique, puis d'authentifier le porteur en fonction du résultat de la comparaison de l'échantillon et du gabarit biométriques.

L'authentification est bien à deux facteurs, car elle utilise deux moyens de contrôle d'identification, la carte et l'échantillon biométrique.

En pratique, le protocole d'authentification utilise deux aléas de session, un aléa T généré par le terminal et transmis à la carte, et un aléa C généré par la carte et transmis au terminal. La carte et le terminal utilisent chacun ces deux aléas de session pour dériver les clés de chiffrement, signature et déchiffrement des données biométriques qu'ils s'échangent.

Un exemple de mise en œuvre d'un tel protocole d'authentification va maintenant être expliqué en relation avec la figure 8, dans le cas où la comparaison biométrique est réalisée dans la carte. Cette mise en œuvre est avantageuse, car la donnée d'identification transmise par la carte est alors le résultat de la comparaison biométrique, qui est une donnée binaire sur un seul bit, voire deux bits, alors que le gabarit est une donnée de 100 octets au moins, comme on l'a vu supra.

Le processus d'authentification pour permettre un accès à des fonctions/services contrôlés par le système, est activé par la capture (100) de données biométriques, et l'ouverture (101) d'une session de

communication radiofréquence avec une carte, qui comprend une séquence d'initialisation consistant en des échanges d'initialisation tel que spécifié par exemple dans la norme ISO14443-3 (type A ou B). Si la séquence d'initialisation de la session de communication avec la carte aboutit, le protocole d'authentification démarre. Ce protocole comprend une séquence d'étapes comprenant :

Dans le terminal :

-une étape 102 de formation dans le terminal d'un échantillon biométrique B_S, à partir des données capturées sur la surface de capture, suivant toute technique connue adaptée à la nature des données biométriques saisies, à savoir empreinte digitale ou réseau veineux, et au capteur utilisé. L'étape de formation peut être réalisée par des moyens de traitement numérique du lecteur 12 ou, réalisée par le capteur qui fournit alors l'échantillon biométrique au lecteur.

-une étape 103 de génération d'un aléa T de session par le terminal et une étape de requête 103.1 d'un aléa C de session généré par la carte. Ces aléas sont typiquement obtenus au moyen d'une boucle logicielle de génération d'un aléa (nombre pseudo-aléatoire de taille finie).

-une étape 104 d'encryptage et signature de l'échantillon biométrique B_S en fonction des deux aléas T et C et de transmission vers la carte. A l'issue de cette étape, le terminal se met en mode d'attente de réception de données (étape 105).

Dans la carte, après l'ouverture 200 de session de communication radiofréquence, la carte fournit dans une étape 201, un aléa C de session, en réponse à la requête du terminal. Cette étape est suivie :

-d'une étape 202 de réception des données transmises par le terminal, typiquement de l'échantillon biométrique B_S crypté et signé et de l'aléa T.

-d'une étape 203 de décryptage de l'échantillon biométrique B_S reçu, suivie d'une étape 204 de vérification de la signature de cet échantillon B_S. Ces étapes utilisent les aléas de session C et T et permettent à la carte d'authentifier le terminal.

-d'une étape 205 de comparaison de cet échantillon B_S au gabarit biométrique B_T enregistré dans la carte.

-une étape 206 de cryptage et signature de données, dans laquelle le résultat de la comparaison, typiquement une donnée sur 1 ou 2 bits, qui est obtenu à la fin de l'étape 205, est alors encrypté, puis signé, par la carte en fonction des deux aléas de session T et C, et transmis au terminal (étape 207). D'autres données personnelles contenues dans la carte peuvent être encryptées et signées avec le résultat et transmises au terminal.

La procédure d'authentification se poursuit dans le terminal avec les étapes suivantes, qui est en attente de données de la carte (étape 105) :

-une étape 106 de décryptage des données transmises par la carte, comprenant au moins le résultat R de la comparaison biométrique, et de vérification de la signature, permettant au terminal d'authentifier (ou non) la carte, utilisant les deux aléas de session C et T.

-une étape 107 d'authentification du porteur, en fonction du résultat R de la comparaison. Le terminal autorise (étape 108) ou non (étape 109) l'accès aux fonctions applicatives en fonction de ce résultat R

On peut prévoir qu'un message correspondant s'affiche sur un écran intégré au terminal.

Si l'accès est autorisé, les données supplémentaires éventuellement transmises avec le résultat de la comparaison, servent alors à la réalisation des fonctions applicatives dont l'accès est autorisé. S'il s'agit d'une transaction financière, les données supplémentaires sont des données personnelles permettant de réaliser la transaction.

Dans ce protocole d'authentification mis en œuvre, toutes les étapes d'encryptage et signature de données, et de décryptage et authentification par la signature, côté terminal et coté carte, font usage des deux aléas C et T générés pour la session, pour la génération des clefs correspondantes d'encryptage, décryptage et signature.

Il est connu d'utiliser un aléa pour dériver les clefs utilisés pour le cryptage/décryptage et les clefs utilisées pour la signature/vérification de signature, que ce soit dans les algorithmes à architecture symétrique (à clés privées) ou asymétrique (à clefs publique et privée).

L'utilisation de deux aléas de session, l'un généré par le terminal et l'autre par la carte, permet de protéger le système contre l'utilisation de copies frauduleuses de données d'autres cartes authentiques. L'utilisation de ces aléas varie en pratique selon les algorithmes d'encryptage et signature

implémentés. Elle ne pose pas de problème particulier de mise en œuvre à l'homme de l'art.

Dans l'exemple plus particulièrement illustré, après ouverture et initialisation d'une session de communication (étape 101), le terminal initialise une étape 103 d'obtention d'aléas de session, avec une étape 103-1 de génération en interne d'un aléa T, et une étape 103-2 de requête d'un aléa C de session auprès de la carte, qui renvoie l'aléa C en réponse. Le terminal transmet son propre aléa de session T généré en interne, vers la carte. Dans l'exemple, l'aléa T est transmis en même temps que l'échantillon biométrique crypté et signé, à l'étape 104. Il peut être transmis indifféremment en clair ou sous forme cryptée et signée.

L'invention qui vient d'être décrite fait usage des algorithmes de cryptage et signature de données bien connu dans le domaine de l'authentification des cartes à puce notamment. Elle utilise des clés de cryptage et signature publiques et/ou privées, comme enseigné dans l'état de l'art. L'invention ne porte pas sur ces algorithmes, mais sur l'intégration d'une comparaison biométrique dans un protocole d'authentification, avec utilisation de deux aléas de session, un aléa "carte" et un aléa "terminal", permettant une authentification dynamique de la carte et du porteur.

Dans l'exemple illustré, l'authentification du porteur est basée sur la collecte et la comparaison d'un échantillon biométrique correspondant à un doigt du porteur. L'invention ne se limite pas à cet exemple. Il peut être envisagé de saisir et comparer, différents échantillons, correspondant par exemple, à deux doigts par exemple, l'index et le majeur. Le terminal peut aussi intégrer un écran permettant d'afficher des invites à l'attention de l'utilisateur, par exemple une invite à poser ou glisser un doigt.

L'invention est applicable au contrôle d'accès sécurisé de toutes fonctions applicatives, avec l'utilisation d'une carte à microcircuit(s) à antenne. Elle ne se limite pas à la carte à microcircuit(s) définie par le standard ISO 7816. La carte peut être de toute forme dès lors qu'elle correspond à un objet portable qui peut être tenu en main comme indiqué, et avec une antenne intégrée correspondant aux normes de communication radiofréquence en champ proche. C'est par exemple, une clef électronique USB, un téléphone mobile, un passeport électronique….

Un système de contrôle d'accès sécurisé selon l'invention trouve une utilité dans tous les domaines où l'on souhaite assurer un accès sécurisé à des fonctions applicatives par une personne légitime. Ces fonctions peuvent être des accès à des données personnelles l'utilisation de programmes confidentiels, l'accès à des locaux, l'usage d'un ordinateur, la réalisation de transactions financières, …. Cette liste n'est pas exhaustive.

Le geste unique, simple et rapide réalisé par l'utilisateur, permet l'acquisition des données biométriques, et leur authentification ainsi que l'authentification de la carte, en un temps très court, par exemple entre 200 et 500 millisecondes. Ce temps d'acquisition/authentification dépend en pratique des performances du capteur, de la taille des données biométriques à comparer, du nombre de gabarits à comparer et des algorithmes d'encryptage et signature utilisés.

REVENDICATIONS

1. Système de contrôle d'accès biométrique, pour autoriser l'accès à des fonctions ou services, le système comportant un terminal de contrôle (10) muni d'un capteur biométrique (11) et d'un système de communication radiofréquence incluant une antenne (AT) pour la communication radiofréquence entre le terminal de contrôle et une carte à microcircuit(s) (20) comportant elle-même une antenne (AC), et contenant un gabarit biométrique (BT) d'un doigt au moins d'un utilisateur autorisé, le terminal comportant une surface supérieure incluant une surface de capture (11a) de données biométriques relatives à un doigt, caractérisé en ce que les positions relatives de l'antenne du terminal et de la surface de capture sont telles que lorsque la carte est tenue dans la main d'un utilisateur avec un doigt au moins s'étendant vers l'avant, et qu'elle est présentée à la surface supérieure du terminal, l'antenne de la carte est apte à communiquer avec l'antenne du terminal à la fin d'un mouvement de la main permettant la capture des données biométriques d'un doigt étendu vers l'avant au-dessus de la surface de capture.

2. Système de contrôle d'accès biométrique selon la revendication 1, caractérisé en ce que les positions relatives de l'antenne du terminal et de la surface de capture sont telles que, à la fin du mouvement de la main, la carte est dans une position optimale ou proche de la position optimale pour la communication avec l'antenne du terminal.

3. Système de contrôle d'accès biométrique selon l'une quelconque des revendications précédentes, dans lequel le capteur biométrique est un capteur d'empreinte digitale ou d'une image de réseau veineux.

4. Système de contrôle d'accès biométrique selon l'une quelconque des revendications précédentes, caractérisé en ce que, à la fin du mouvement de la main, l'antenne de la carte est apte à communiquer avec l'antenne du terminal lorsque la carte est tenue entre le pouce et au moins deux doigts.

5. Système de contrôle d'accès biométrique selon l'une quelconque des revendications précédentes, dans lequel la carte à microcircuit(s) comprend une encoche (22) ménagée dans la carte et/ou un repère graphique (23).

6. Système de contrôle d'accès biométrique selon l'une quelconque des revendications précédentes, dans lequel lorsque des données biométriques ont été capturées par le capteur et une session de communication radiofréquence ouverte entre le terminal et une carte, le terminal active un protocole d'authentification du porteur de la carte qui comprend la comparaison d'un échantillon biométrique (BS) correspondant aux données biométriques acquises par le capteur à un gabarit biométrique pré-enregistré (BT) dans la carte correspondant à des caractéristiques biologiques d'un doigt d'un utilisateur autorisé.

7. Système de contrôle d'accès selon la revendication 6, dans lequel l'activation d'un protocole d'authentification entre le terminal et la carte comprend
   - -. un échange d'aléas de session entre le terminal et la carte, un aléa (T) généré par le terminal, et un aléa (C) généré par la carte,
   - -. un échange entre le terminal et la carte de données cryptées et signées à partir desdits aléas de session (C et T) comprenant l'échantillon biométrique (BS) transmis à la carte par le terminal, et une donnée d'identification biométrique transmise par la carte au terminal, ladite donnée d'identification biométrique correspondant au gabarit biométrique (BT) ou au résultat (R) d'une comparaison entre le gabarit biométrique (BT) et l'échantillon biométrique (BS).

8. Système selon la revendication 7, dans lequel la carte transmet au terminal la donnée d'identification avec d'autres données sensibles contenues dans la carte.

9. Système de contrôle d'accès selon la revendication 7 ou 8, dans lequel :
   - la carte authentifie le terminal par vérification sur la base desdits aléas de session, de la signature de l'échantillon biométrique reçu;
   - le terminal authentifie la carte par vérification de signature, sur la base desdits aléas de session, de la donnée d'identification biométrique reçue, et authentifie le porteur de la carte sur la base du résultat (R) de la comparaison, pour autoriser ou non l'accès à une fonction applicative.

10. Système de contrôle d'accès selon l'une des revendications 6 à 9, dans lequel la comparaison (C) entre le gabarit biométrique (B_T) et l'échantillon biométrique (B_S) est réalisée par la carte.

11. Système selon l'une quelconque des revendications précédentes dans lequel la carte à microcircuit(s) est une carte à microcircuit(s) dont les dimensions sont conformes aux dimensions définies dans la norme ISO 7816.

12. Terminal de contrôle (10) d'accès sécurisé muni d'un capteur biométrique (11) et d'un système de communication radiofréquence incluant une antenne (A_T) pour la communication radiofréquence avec une carte à microcircuit(s) (20) à antenne (A_C), et comportant une surface supérieure (10a) incluant une surface de capture (11a) de données biométriques (B_S) relatives à un doigt humain, caractérisé en ce que les positions relatives de l'antenne du terminal et de la surface de capture sont telles que lorsque une carte est tenue dans la main d'un utilisateur avec un doigt au moins s'étendant vers l'avant, et qu'elle est présentée à la surface supérieure du terminal, l'antenne de la carte est apte à communiquer avec l'antenne du terminal à la fin d'un mouvement de la main permettant la capture des données biométriques d'un doigt étendu vers l'avant au-dessus de la surface de capture.

13. Procédé de contrôle d'accès biométrique, pour autoriser l'accès à des fonctions ou services, comprenant

-une étape d'enregistrement d'un gabarit biométrique (B_T) au moins d'un utilisateur autorisé dans une carte à microcircuit(s) (20) comportant une antenne (A_C)

-une étape d'ouverture d'une session de communication radiofréquence entre la carte et un terminal de contrôle (10) muni d'un capteur biométrique (11) avec une surface de capture (11a) de données biométriques relatives à un doigt sur une surface supérieure du terminal et d'un système de communication radiofréquence incluant une antenne (A_T),

-une étape de capture de données biométriques relatives à un doigt d'un porteur de la carte, par le capteur biométrique du terminal,

caractérisé en ce que lesdites étapes d'ouverture de session et de capture sont obtenues par une présentation de la carte tenue en main avec un doigt étendu vers l'avant, à la surface supérieure du terminal telle que l'antenne de la carte est apte à communiquer avec l'antenne du terminal à la fin d'un mouvement de la main permettant la capture des données biométriques d'un doigt étendu vers l'avant au-dessus de la surface de capture.

14. Procédé de contrôle d'accès biométrique selon la revendication 13, dans lequel l'ouverture d'une session de communication entre le terminal et la carte et la capture de données biométriques dans l'étape de capture active une étape d'authentification comprenant une comparaison d'un échantillon biométrique (B_S) correspondant aux données biométriques acquises par le terminal dans l'étape de capture, à un gabarit biométrique pré-enregistré (B_T) dans la carte.

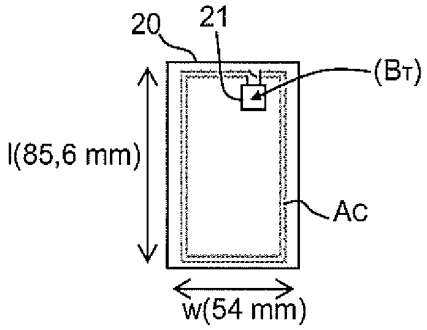


Fig. 1

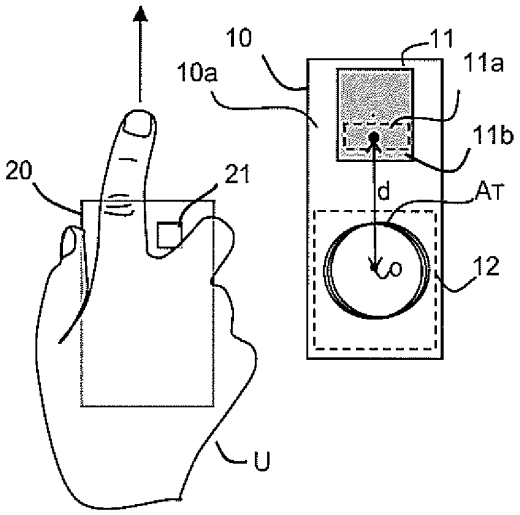


Fig. 2

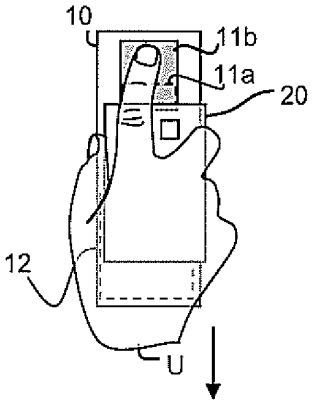


Fig. 3

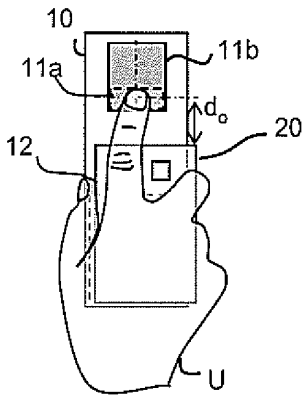


Fig. 4

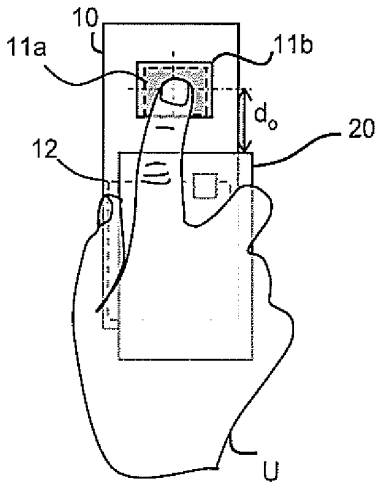


Fig. 5

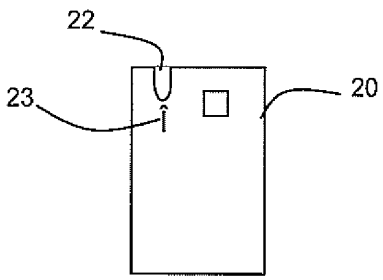


Fig. 6

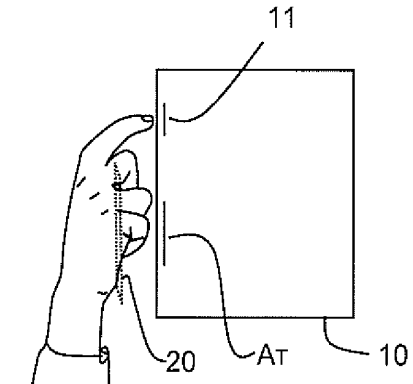


Fig. 7a

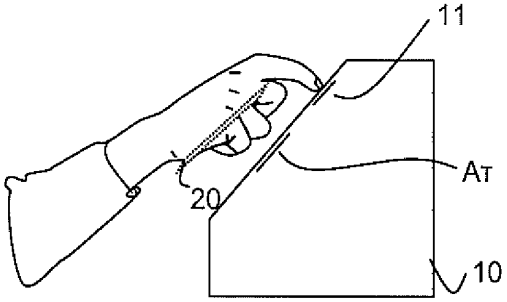


Fig. 7b

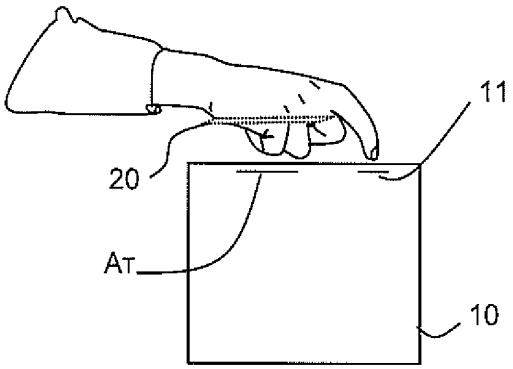


Fig. 7c

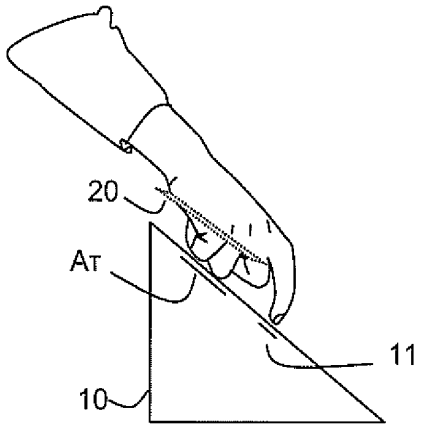
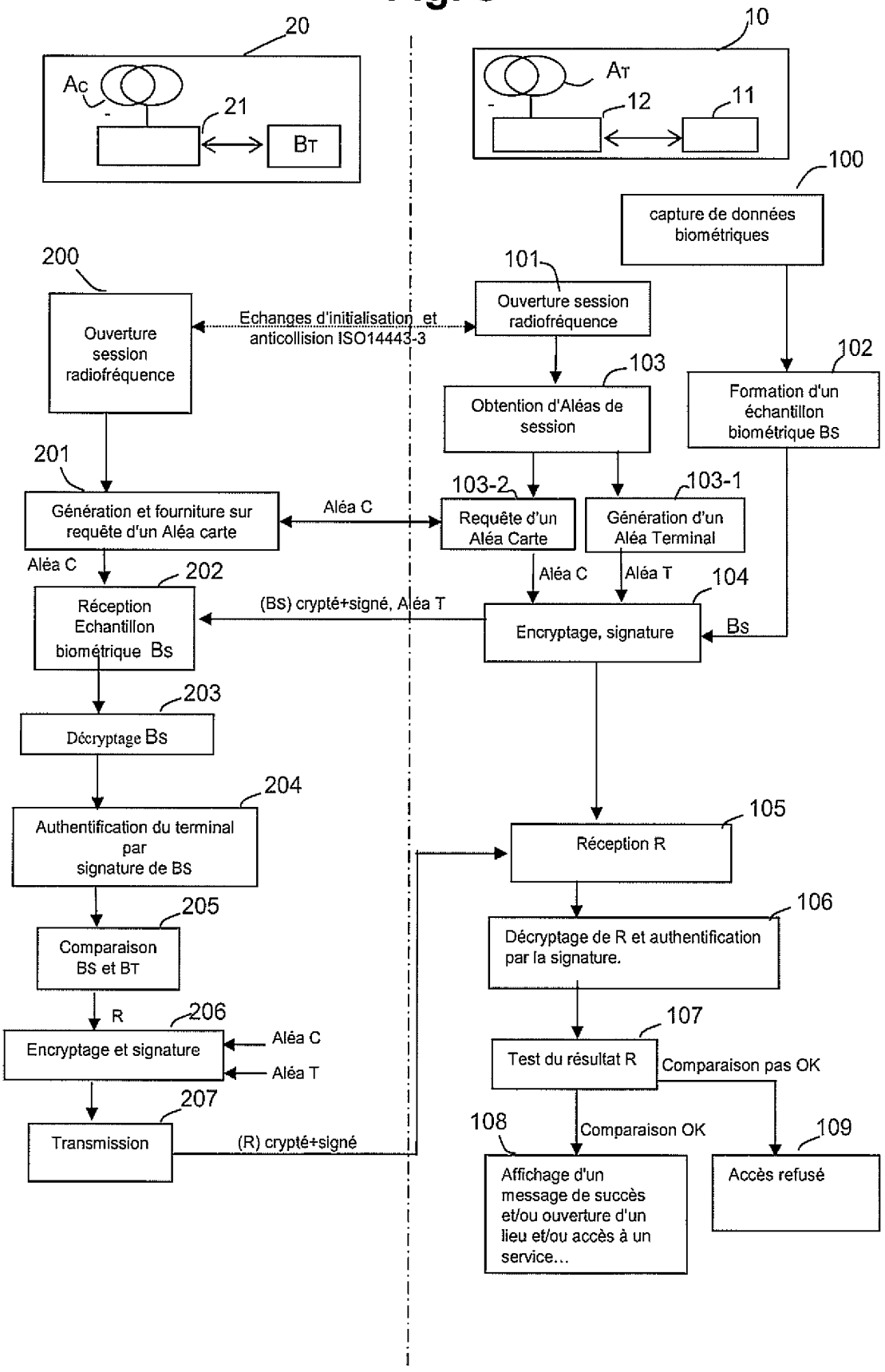


Fig. 7d

Fig. 8


20
AC
21
BT
10
AT
12
11
100
capture de données biométriques
200
Ouverture session radiofréquence
Echanges d'initialisation et anticollision ISO14443-3
101
Ouverture session radiofréquence
102
Formation d'un échantillon biométrique BS
103
Obtention d'Aléas de session
201
Génération et fourniture sur requête d'un Aléa carte
Aléa C
103-2
Requête d'un Aléa Carte
103-1
Génération d'un Aléa Terminal
Aléa C
Aléa T
202
Réception Echantillon biométrique Bs
(BS) crypté+signé, Aléa T
104
Encryptage, signature
Bs
203
Décryptage Bs
204
Authentification du terminal par signature de BS
105
Réception R
205
Comparaison BS et BT
106
Décryptage de R et authentification par la signature.
R
206
Encryptage et signature
Aléa C
Aléa T
107
Test du résultat R
Comparaison pas OK
207
Transmission
(R) crypté+signé
108
Comparaison OK
109
Affichage d'un message de succès et/ou ouverture d'un lieu et/ou accès à un service...
Accès refusé

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 750975
FR 1059564

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	CA 2 142 227 A1 (INFOTAG SYSTEMS INC [CA]) 11 août 1996 (1996-08-11) * abrégé * * page 7, ligne 20 - page 8, ligne 11 * * page 10, ligne 11 - page 11, ligne 7 * * page 14, ligne 10 - page 15, ligne 11 * * page 20, ligne 27 - page 21, ligne 32 * * page 26, ligne 35 - page 27, ligne 5 * * revendications 1,5,13 * * figures 1,2,6 * -----	1-14	G06F21/00 G07F7/08 G06K9/00
X,D	US 2006/274920 A1 (TOCHIKUBO OSAMU [JP] ET AL) 7 décembre 2006 (2006-12-07) * abrégé * * alinéa [0002] * * alinéa [0005] - alinéa [0012] * * alinéa [0018] * * alinéa [0108] - alinéa [0132] * * alinéa [0156] * * alinéa [0160] * * figures 1-8,22 * -----	1-14	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06K G07C

Date d'achèvement de la recherche	Examinateur
22 septembre 2011	Jacobs, Peter

CATÉGORIE DES DOCUMENTS CITÉS

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

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1059564 FA 750975

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 22-09-2011
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
CA 2142227 A1	11-08-1996	AUCUN	
US 2006274920 A1	07-12-2006	WO 2004111940 A1	23-12-2004

EPO FORM P0465