

①⑨ RÉPUBLIQUE FRANÇAISE
—
**INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE**
—
COURBEVOIE
—

①① N° de publication : **3 131 645**

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

②① N° d'enregistrement national : **21 14722**

⑤① Int Cl⁸ : **G 06 F 21/32** (2022.01), G 06 Q 30/06, G 06 K 19/
067, H 04 L 9/32

⑫

BREVET D'INVENTION

B1

⑤④ Dispositif biométrique de transaction par carte à puce.

②② Date de dépôt : 31.12.21.

③③ Priorité :

④③ Date de mise à la disposition du public
de la demande : 07.07.23 Bulletin 23/27.

④⑤ Date de la mise à disposition du public du
brevet d'invention : 20.12.24 Bulletin 24/51.

⑤⑥ Liste des documents cités dans le rapport de
recherche :

Se reporter à la fin du présent fascicule

⑥⑥ Références à d'autres documents nationaux
apparentés :

○ Demande(s) d'extension :

⑦① Demandeur(s) : *SMART PACKAGING SOLUTIONS
SAS — FR.*

⑦② Inventeur(s) : *BERTRAND Bertrand, SEMORI
Stéphane et TONIN Jérôme.*

⑦③ Titulaire(s) : *SMART PACKAGING SOLUTIONS
SAS.*

⑦④ Mandataire(s) : *BRANDON IP.*

FR 3 131 645 - B1



Description

Titre de l'invention : Dispositif biométrique de transaction par carte à puce

[0001] L'invention concerne les systèmes pour la réalisation de transactions électroniques par carte à puce sécurisées par des informations biométriques du porteur de la carte à puce. Les transactions électroniques visées peuvent être de toute nature, comme les transactions de paiement, de transfert d'argent ou de valeurs, d'accès physique ou d'identification numérique, mais à titre d'exemple non limitatif, l'invention sera décrite plus particulièrement en liaison avec des transactions électroniques de paiement par carte à puce, qu'il s'agisse d'une carte à puce à fonctionnement par contact avec un lecteur de carte à puce, d'une carte à puce à fonctionnement sans contact, ou d'une carte à puce duale à fonctionnement mixte à contact et sans contact.

État de la technique

[0002] La plupart des cartes à puce sans contact ou des cartes à puce duales à fonctionnement mixte à contact et sans contact connues comportent un corps de carte, un module électronique inséré dans une cavité du corps de carte et pourvu d'une puce microélectronique, et une antenne disposée dans le corps de carte. Celle-ci est soit galvaniquement connectée à des plots de sortie de la puce microélectronique, soit couplée inductivement à une antenne plus petite directement intégrée au module électronique de la carte à puce. Dans les deux configurations, l'antenne du corps de carte permet une communication par voie radiofréquence avec l'antenne d'un lecteur de carte à puce.

[0003] Alternativement, il existe des cartes à puce à fonctionnement purement à contact, et dont le corps de carte ou le module électronique ne comporte pas d'antenne.

[0004] Dans un certain nombre d'applications, il est devenu nécessaire d'intégrer à la carte à puce un ou plusieurs modules électroniques complémentaires par rapport au module principal, par exemple pour l'intégration de capteurs biométriques susceptibles de collecter des informations biométriques et de les transmettre au module principal à des fins d'identification biométrique de l'utilisateur de la carte à puce.

[0005] Cela est particulièrement vrai dans le domaine des paiements par carte bancaire, qui nécessitent une sécurisation poussée par une authentification forte à deux facteurs afin de minimiser les paiements frauduleux.

[0006] Dans le cas du paiement par contact avec détection d'une « Carte Présente » (CP) dans le lecteur, on utilise un code PIN stocké dans la carte et qui permet de sécuriser les transactions par contact. En ce qui concerne les transactions sans contact, le moyen de sécurisation utilisé actuellement est la demande d'introduction d'un code PIN

uniquement à partir d'un certain nombre de transactions ou à partir d'un plafond de montant de la transaction (fixé à 50€ en France), ce qui limite l'impact financier d'une fraude éventuelle. Le taux de fraude constaté en paiement par contact est de l'ordre de 0.01% des transactions, alors que celui constaté pour les transactions sans contact est supérieur, de l'ordre de 0.02%.

- [0007] Afin de limiter les cas de fraude dans des transactions de paiement sans contact utilisant des cartes à puce traditionnelles, on a introduit de nouvelles cartes bancaires, à savoir des cartes bancaires biométriques possédant un capteur biométrique. Ces cartes biométriques répondent au besoin d'authentification forte à deux facteurs et peuvent permettre de supprimer le plafond limitant le montant des transactions.
- [0008] Toutefois, l'ajout de cette fonction biométrique dans les cartes à puce entraîne une complexité accrue de la structure de ces cartes et de leur utilisation, bien supérieure à celles des cartes à puce traditionnelles.
- [0009] Ainsi, l'introduction de la fonction biométrique a nécessité jusqu'à présent l'intégration dans le corps de carte d'un module biométrique distinct du module principal, notamment un capteur d'empreintes digitales, ainsi que d'une interface de signalisation par exemple sous la forme de LEDs permettant de guider l'utilisateur de la carte dans le cadre de l'exécution d'une transaction sécurisée par la fonction biométrique. Cette intégration d'un module biométrique entraîne un surcout et peut restreindre la fiabilité de la carte à puce dans le temps.
- [0010] Par ailleurs, il a été prouvé que la performance et la sécurité du système dépendent de la surface du capteur d'empreintes digitales. Plus cette surface est importante et plus fiable est la reconnaissance des minuties. Cette performance est exprimée à l'aide de deux taux d'erreur, à savoir FAR et FRR, acronymes pour « False Acceptance Rate » et « False Rejection Rate » en terminologie anglo-saxonne.
- [0011] Le taux FAR est le pourcentage d'identification dans lequel des personnes non autorisées sont incorrectement acceptées pour l'exécution d'une transaction avec la carte à puce biométrique.
- [0012] Le taux FRR est le pourcentage d'identification dans lequel des personnes normalement autorisées sont incorrectement rejetées pour l'exécution d'une transaction. Ces deux taux varient de manière opposée, quand FAR diminue, FRR augmente.
- [0013] Selon la norme ISO 17839, le capteur biométrique doit avoir une surface minimale de 169 mm² (13x13 mm²) pour assurer une précision correcte de l'empreinte biométrique, mais elle ne peut pas non plus avoir une surface trop importante pour des questions d'assemblage du capteur biométrique sur la carte et de respect des normes de résistance de la carte à puce à la flexion, qui en pratique limitent la surface du capteur biométrique.

- [0014] L'utilisation d'une telle carte biométrique à capteur d'empreinte digitale conforme à l'état de la technique est alors la suivante.
- [0015] La première opération que l'utilisateur doit réaliser quand il reçoit sa carte biométrique est l'opération dite d'enrôlement biométrique, à savoir la capture et le stockage sécurisés de son empreinte digitale qui devra servir d'empreinte de référence dans les transactions avec la carte biométrique.
- [0016] Pour cela, quatre options sont actuellement proposées, à savoir un enrôlement au sein d'une agence bancaire, ou sur un terminal de paiement chez un commerçant, ou encore chez soi avec un équipement électronique d'enrôlement spécifique tel qu'un lecteur fourni avec la carte à puce, ou encore l'enrôlement à l'aide d'une application sur un smartphone compatible avec le protocole NFC. Le code PIN de la carte à puce est alors nécessaire lors du premier paiement pour activer la biométrie.
- [0017] Toutes ces options d'enrôlement avec les cartes biométriques connues présentent des inconvénients, donc certains sont exposés ci-dessous.
- [0018] Ainsi, l'enrôlement en agence bancaire impose au titulaire de la carte de se déplacer en agence pendant les heures d'ouverture de celle-ci. Ceci est chronophage, et en outre n'est pas possible pour les banques en ligne qui sont dépourvues d'agences.
- [0019] L'enrôlement sur un terminal de paiement nécessite de positionner un doigt plusieurs fois sur le capteur biométrique de la carte à puce insérée dans le terminal de paiement. Cela peut donc prendre plusieurs minutes, qu'il s'agisse d'un enrôlement chez soi sur un terminal personnel, ou d'un enrôlement sur le terminal d'un commerçant. Dans ce dernier cas, cette opération d'enrôlement peut notamment générer une file d'attente en caisse en cas d'affluence.
- [0020] L'enrôlement chez soi avec utilisation d'un équipement électronique dédié qui ne sert qu'une fois pose des problèmes écologiques, cet équipement à usage unique étant ensuite perdu. Dans le cas où l'utilisateur possède plusieurs cartes de paiement, il recevra autant d'équipements d'enrôlement que de cartes de paiement, ce qui augmentera l'impact environnemental du problème.
- [0021] Enfin, l'enrôlement à l'aide d'une application pour smartphone en liaison NFC avec la carte biométrique nécessite d'une part d'installer une application spécifique, avec laquelle tous les smartphones ne sont pas compatibles, et d'autre part demande des manipulations répétées du smartphone et de la carte biométrique afin de lire plusieurs fois les minuties de l'empreinte digitale.

But de l'invention

- [0022] Un but général de l'invention est par conséquent de proposer un nouveau dispositif biométrique pour la réalisation de transactions à l'aide d'une carte à puce, notamment des transactions de paiement, qui soit apte à éliminer les inconvénients liés aux cartes à puce biométriques connues.

- [0023] Un autre but de l'invention est de proposer un dispositif biométrique utilisant des cartes à puce aussi fiables et peu coûteuses que les cartes à puce à contact, sans contact ou duales connues.
- [0024] Un autre but de l'invention est de proposer un dispositif biométrique avec lequel l'opération d'enrôlement de l'empreinte biométrique de l'utilisateur soit beaucoup plus simple qu'avec les cartes à puce biométriques connues.
- [0025] Un autre but de l'invention est de proposer un dispositif de transaction à sécurisation biométrique qui soit évolutif et aisé à adapter à une grande variété de cas d'usage.

Résumé de l'invention

- [0026] Dans son principe, l'invention consiste à délocaliser le capteur biométrique de la carte à puce, notamment de la carte bancaire, vers un objet annexe, à savoir un porte-carte pourvu d'un moyen de communication à contact ou sans contact avec la carte à puce. Ce porte-carte biométrique permet donc l'enrôlement et la sécurisation des transactions de paiement par carte sans contact tout en conservant une carte à puce traditionnelle dépourvue de tout capteur biométrique, soit une carte à puce à contact, sans contact, ou à fonctionnement dual à contact et sans contact.
- [0027] Le dispositif porte-carte a donc deux fonctions en relation avec une transaction, à savoir l'enrôlement de la biométrie du porteur dans la carte à puce, et l'authentification forte du porteur par biométrie lors de la transaction, notamment une transaction de paiement.
- [0028] L'invention porte par conséquent sur un dispositif biométrique pour la réalisation de transactions électroniques, comportant d'une part une carte à puce pourvue d'un corps de carte intégrant un module microélectronique comportant un microprocesseur et une mémoire pour stocker des informations d'identification du titulaire de la carte à puce, caractérisé en ce qu'il comporte d'autre part un porte-carte configuré pour recevoir ladite carte à puce, et ledit porte-carte comportant un capteur biométrique apte à capter une information biométrique d'un utilisateur du dispositif, et une interface de communication configurée pour transmettre ladite information biométrique au module microélectronique de la carte à puce. La fonction de capture d'empreinte biométrique est donc déportée sur le porte-carte, ce qui permet notamment d'en augmenter la taille, la performance et la fiabilité dans le temps.
- [0029] Selon un mode de réalisation de base, ledit porte-carte comporte un microcontrôleur recevant l'information biométrique du capteur biométrique, une interface utilisateur apte à indiquer à l'utilisateur le statut des échanges d'information entre ladite carte à puce et ledit porte-carte, et une source d'énergie alimentant électriquement le capteur biométrique, le microcontrôleur, et l'interface utilisateur.

- [0030] Selon un mode de réalisation, la carte à puce est une carte à contact pourvue d'une interface à contacts selon la norme ISO 7816-1 et le porte-carte comporte une interface à contacts apte à engager de façon galvanique les contacts de l'interface à contacts de la carte à puce.
- [0031] Selon une variante de réalisation, la carte à puce est une carte à fonctionnement sans contact ou à fonctionnement dual à contact et sans contact, comportant une antenne connectée à une interface de communication sans contact du module microélectronique, et le porte-carte comporte une antenne connectée au microcontrôleur du porte-carte et qui est apte à être positionnée en couplage inductif avec l'antenne de la carte à puce.
- [0032] Selon des options de réalisation, la source d'énergie du porte-carte est prise parmi une batterie ou un super condensateur susceptible d'être connecté de manière filaire à un dispositif d'alimentation externe, ou une cellule photovoltaïque, ou une antenne susceptible d'être couplée inductivement à un dispositif d'alimentation sans contact externe.
- [0033] De préférence, afin de positionner facilement la carte à puce sur le porte-carte, celui-ci possède sur sa face avant un moyen de guidage ou de rétention de la carte à puce.
- [0034] Selon un mode de réalisation, ledit moyen de guidage ou de rétention de la carte à puce est constitué par un couvercle délimitant une fente dans laquelle s'insère la carte à puce, et le capteur biométrique est situé sur la face externe dudit couvercle.
- [0035] Selon une variante de réalisation, ledit moyen de guidage ou de rétention de la carte à puce est constitué par une glissière périphérique aménagée sur au moins deux côtés du porte-carte et dans laquelle s'insère la carte à puce, et le capteur biométrique du porte-carte est dans ce cas situé sur la face arrière du porte-carte.
- [0036] De préférence, la surface utile du capteur biométrique du porte-carte est supérieure à 169 mm².
- [0037] Selon un mode de réalisation, le porte-carte est fixé à plusieurs cartes à puce articulées entre elles en éventail et articulées par rapport au porte-carte.
- [0038] Selon un mode de réalisation, le porte-carte est configuré en forme de portefeuille, ou est intégré à un accessoire tel qu'une coque de téléphone portable.
- [0039] Selon un mode de réalisation, au moins l'une des faces du porte-carte comporte un marquage publicitaire ou décoratif.
- [0040] Selon une variante plus évoluée du dispositif biométrique, le porte-carte comporte en outre un module de communication radiofréquence apte à établir une liaison de type BLE entre le porte-carte et un ordinateur ou un smartphone distant, ou avec un autre dispositif biométrique du même type.
- [0041] Selon un autre mode de réalisation, le porte-carte comporte en outre une mémoire sécurisée apte à stocker un portefeuille de monnaies ou valeurs électroniques.

- [0042] L'invention a également pour objet l'utilisation d'un système constitué d'un dispositif biométrique tel que décrit plus haut et d'un lecteur sans contact de carte à puce, dans laquelle ledit lecteur sans contact est utilisé pour alimenter électriquement une carte à puce sans contact par couplage inductif entre le lecteur sans contact et ladite carte à puce, et pour alimenter électriquement le porte-carte par contact galvanique entre la carte à puce et le porte-carte.
- [0043] L'invention a également pour objet l'utilisation d'un système constitué d'un dispositif biométrique tel que décrit plus haut et d'un lecteur sans contact de carte à puce, dans laquelle ledit lecteur sans contact est utilisé pour alimenter électriquement une carte à puce sans contact et le porte-carte par couplage inductif entre le lecteur sans contact, le porte-carte et la carte à puce.
- [0044] L'invention a enfin pour objet un procédé de réalisation par un utilisateur d'une transaction électronique entre un lecteur NFC d'un système de transaction par cartes à puce et un dispositif biométrique tel que décrit plus haut, caractérisé en ce qu'il comporte des étapes consistant à :
- dans une phase préliminaire d'enrôlement de l'utilisateur, positionner une carte à puce de l'utilisateur sur le porte-carte, apposer un doigt de l'utilisateur sur le capteur biométrique du porte-carte de façon à capter par le porte-carte une empreinte biométrique de référence de l'utilisateur, puis transmettre cette empreinte biométrique de référence du porte-carte à la carte à puce et la stocker dans une mémoire de la carte à puce;
 - dans une phase d'exécution d'une transaction électronique, positionner sur le porte-carte la carte à puce contenant l'empreinte biométrique de référence et un microprogramme d'exécution de transactions électroniques, puis apposer le doigt de l'utilisateur sur le capteur biométrique du porte-carte de façon à capter et transmettre à la carte à puce une empreinte biométrique de transaction ;
 - comparer par le microprogramme de la carte à puce l'empreinte biométrique de référence et l'empreinte biométrique de transaction, et en cas de correspondance des deux empreintes biométriques, autoriser l'exécution par le microprogramme de la carte à puce de la transaction électronique entre la carte à puce et le lecteur NFC.
- [0045] D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée effectuée dans le cadre de l'application de l'invention à une carte à puce, et des dessins annexés dans lesquels :
- La [Fig.1] représente de façon schématique une carte à puce biométrique conforme à l'état de la technique.

- Les figures 2A à 2E représentent plusieurs vues des composants d'un premier mode de réalisation du dispositif selon l'invention.
- Les figures 3A, 3B, 3C représentent respectivement des vues en plan, en coupe et en perspective d'un dispositif selon l'invention, formé par une carte à puce insérée dans le porte-carte.
- La [Fig.4A] représente en vue de dessus d'un premier mode de réalisation du porte-carte du dispositif selon l'invention.
- La [Fig.4B] représente en vue de dessous d'un second mode de réalisation du porte-carte du dispositif selon l'invention.
- Les figures 5A et 5B représentent en vue en perspective deux modes de réalisation du dispositif selon l'invention.
- La [Fig.6] représente un comparatif des opérations à mener dans le cadre d'une transaction de paiement avec une carte à puce biométrique conforme à l'état de la technique, et avec un dispositif de paiement conforme à l'invention.
- La [Fig.7A] représente de façon schématique une version de base du dispositif selon l'invention, en phase d'enrôlement, avant insertion d'une carte à puce à contact dans le lecteur porte-carte.
- La [Fig.7B] représente le dispositif de la [Fig.7A], après insertion partielle de la carte à puce dans le porte-carte.
- La [Fig.7C] représente une variante du dispositif de la [Fig.7B].
- La [Fig.8A] représente un premier mode de réalisation du dispositif selon l'invention, en phase d'utilisation pour la réalisation d'une transaction de paiement entre une carte bancaire et un lecteur externe.
- La [Fig.8B] représente un second mode de réalisation du dispositif selon l'invention, en phase d'utilisation pour la réalisation d'une transaction de paiement entre une carte bancaire et un lecteur externe.
- La [Fig.9A] représente un troisième mode de réalisation du dispositif selon l'invention, en phase d'utilisation pour la réalisation d'une transaction de paiement entre une carte bancaire et un lecteur externe.
- La [Fig.9B] représente un quatrième mode de réalisation du dispositif selon l'invention, en phase d'utilisation pour la réalisation d'une transaction de paiement entre une carte bancaire et un lecteur externe.
- La [Fig.10] représente un mode de réalisation du dispositif selon l'invention, adapté à la réalisation de transactions de paiement en mode CNP (« Card Not Present ») à l'aide d'une liaison de type « Bluetooth » ou équivalent entre le dispositif biométrique selon l'invention et un ordinateur ou smartphone distant.

- La [Fig.11] représente de façon schématique l'utilisation de deux dispositifs selon l'invention, pour réaliser une transaction de transfert d'argent ou de valeurs entre deux cartes à puce.
- La [Fig.12] représente un mode de réalisation du dispositif selon l'invention, adapté à la réalisation de transactions entre un portefeuille électronique sécurisé et un ordinateur ou smartphone.

Description détaillée

- [0046] Les mêmes éléments sont désignés par les mêmes références dans les différentes figures.
- [0047] On se réfère à la [Fig.1], qui représente une vue schématique d'une carte à puce connue 1 à fonctionnement mixte à contact et sans contact. Cette carte à puce 1 comporte un corps de carte 2, un premier module électronique 3 pourvu de contacts normalisés selon la norme ISO 7816-1 et d'une antenne, et un second module électronique 4, qui comporte notamment un capteur biométrique, tel qu'un capteur d'empreintes digitales. Le premier module électronique 3 comporte une puce microélectronique (non représentée) qui stocke de façon sécurisée des informations d'identification du porteur de carte, en particulier des empreintes biométriques de référence du porteur de carte. La carte à puce 1 comporte en outre un circuit imprimé PCB portant un ensemble de composants discrets 5 tels que des résistances ou condensateurs permettant de mettre en forme le signal analogique issu du capteur biométrique 4, et des pistes conductrices 6 pour interconnecter les différents composants électroniques de la carte à puce biométrique 1.
- [0048] Afin d'autoriser une transaction avec la carte à puce 1, l'utilisateur doit soumettre son empreinte biométrique au second module électronique 4, et cette empreinte est sécurisée et transmise au module électronique 3 où elle est comparée à une empreinte biométrique de référence stockée lors de l'enrôlement de la carte à puce par son titulaire, par exemple les minuties d'une empreinte digitale.
- [0049] Comme on le voit, cette carte à puce 1 comportant deux modules électroniques 3, 4, et d'autres composants électroniques 5 et pistes 6 forme une structure complexe, difficile à fabriquer, présentant un coût élevé, et susceptible de présenter des problèmes de fiabilité dans le temps, notamment raison des flexions répétées auxquelles elle est soumise pendant son cycle de vie. Dans cette configuration connue, la surface du capteur biométrique 4 est limitée afin de ne pas pénaliser la fiabilité de la carte, ce qui ne permet pas d'optimiser les taux d'erreur FAR et FRR mentionnés plus haut.
- [0050] Le dispositif biométrique 10 selon l'invention, schématisé en figure 2, prend le contrepied de l'approche connue. Au lieu d'intégrer à la fois un module de sécurité 3 et un module biométrique 4 dans une même carte à puce, le dispositif 10 selon

l'invention associe d'une part une carte à puce classique 12 schématisée en [Fig.2B], et d'autre part un porte-carte 11 schématisé en figures 2A, 2C, 2D, 2E.

- [0051] La carte à puce classique 12 peut être à contact, sans contact, ou à fonctionnement dual à contact et sans contact. Elle contient de façon connue un microprogramme configuré pour piloter l'exécution d'une transaction avec un lecteur de carte à puce, par exemple une transaction de paiement.
- [0052] Le porte-carte 11 peut dans certains cas d'usage aussi faire office de lecteur de carte. Selon l'invention, il comporte dans tous les cas de figure un capteur biométrique 13, de sorte que la fonction biométrique du dispositif biométrique 10 est déporté dans le porte-carte 11. Le capteur biométrique 13 est disposé sur l'une des faces du porte-carte 11. Il peut être plus grand et plus efficace que le capteur biométrique 4 des cartes à puce biométriques 1 connues dans l'état de la technique. En particulier il n'est pas soumis aux drastiques normes de taille et de résistance aux flexions qui s'imposent aux cartes à puce normalisées.
- [0053] De façon optionnelle, la face du porte-carte 11 qui présente le capteur biométrique 13, notamment un capteur d'empreintes digitales, comporte en outre une zone 14 pourvue d'un texte imprimé ou d'une image, par exemple pour expliquer le mode d'utilisation du dispositif biométrique 10.
- [0054] De façon avantageuse, les autres portions visibles du porte-carte 11 peuvent comporter des motifs décoratifs ou publicitaires, des logos d'entreprise, par exemple le logo d'une banque émettrice de la carte à puce bancaire, ou tout autre marquage utile.
- [0055] De façon avantageuse, le porte-carte 11 du dispositif biométrique 10 selon l'invention comporte des moyens de guidage ou de rétention de la carte à puce 12, de façon à faciliter la présentation de l'ensemble du dispositif 10 en face d'un lecteur de carte à puce d'un commerçant pour l'exécution d'une transaction.
- [0056] Selon un mode de réalisation représenté en figures 2 et 3, ce moyen de guidage est constitué par exemple par un couvercle 15 solidaire du corps du porte-carte 11 et délimitant avec celui-ci une fente 16 située sur la face avant du porte-carte 11 (c'est-à-dire celle sur laquelle on vient poser la carte à puce 12) et dans laquelle on insère la carte à puce 12. En figure 3, le dispositif biométrique 10 selon l'invention est représenté en position d'utilisation, lorsque la carte à puce 12 est positionnée dans le porte-carte 11.
- [0057] Selon une variante non représentée, le moyen de guidage de la carte à puce 12 peut être constitué par une glissière s'étendant sur plusieurs côtés du porte-carte, à l'exception d'un côté dépourvu de glissière et laissé libre pour permettre l'introduction de la carte à puce dans le porte-carte 11. Dans ce cas de figure, le capteur biométrique 13 sera positionné sur la face arrière du porte-carte 11.

- [0058] Pour permettre l'utilisation de cartes à puce 12 à contact, dont le module d'identification 3 présente des contacts galvaniques tels que les contacts normalisés selon la norme ISO 7816, le porte-carte 11 comporte des contacts 3' ([Fig.3B]) homologues des contacts du module 3 de la carte à puce 12 et disposés de manière à être en face des contacts de la carte à puce lorsque celle-ci est insérée dans le porte-carte. Les contacts 3' du porte-carte 11 pourront donc notamment être utilement situés sur la face interne du couvercle 15, ou sur la face avant du porte-carte, faisant face au couvercle 15 du porte-carte 11.
- [0059] Comme représenté en figure 4, le capteur biométrique 13 du porte-carte 11 peut être disposé sur la face externe du couvercle 15 ([Fig.4A]), ou sur la face arrière du porte-carte 11 ([Fig.4B]), à savoir la face opposée à celle destinée à recevoir la carte à puce 12.
- [0060] En fonction notamment de l'épaisseur admissible pour le porte-carte 11, d'autres modes de réalisation sont possibles dans le cadre de l'invention.
- [0061] Dans une version très pratique, le porte-carte 11 a sensiblement la longueur et la largeur d'une carte à puce, et une épaisseur légèrement supérieure à celle de la carte à puce, par exemple inférieure au triple de l'épaisseur d'une carte à puce standardisée, de façon que l'ensemble du dispositif 10 de transaction biométrique puisse encore être inséré dans un portefeuille. Un tel porte-carte 11 peut aisément être réalisé sous la forme d'un boîtier en matière plastique injectée autour d'un circuit imprimé PCB portant les composants électroniques du porte-carte.
- [0062] En [Fig.5A], le porte-carte 11 se présente sous la forme d'un boîtier parallélépipédique pourvu sur une face d'un capteur biométrique 13, et sur un côté d'une fente pour l'insertion de la carte à puce 12.
- [0063] En [Fig.5B], le porte-carte 11 possède un couvercle 15 pourvu d'un capteur biométrique 13, et de glissières latérales de guidage 17 facilitant le guidage de la carte à puce 12 vers la fente 16 du porte-carte pour une introduction facilitée de la carte à puce 12 dans le porte-carte.
- [0064] Dans une autre variante envisageable (non représentée), le porte-carte peut comporter un corps pourvu d'une liaison par charnière configurée pour recevoir plusieurs cartes à puce 12 disposées en éventail et articulées par rapport au porte-carte. Il suffira alors de choisir une carte 12 donnée et de la mettre en position en face du lecteur porte-carte pour réaliser une transaction entre une carte à puce 12 et un lecteur de carte externe.
- [0065] En variante, le porte-carte 11 pourra être directement intégré dans un portefeuille ou dans un accessoire tel qu'une coque de protection pour téléphone portable, permettant ainsi d'effectuer une transaction entre une carte à puce 12 et un lecteur externe (non représenté) sans avoir à sortir la carte bancaire de son portefeuille ou de l'accessoire.

- [0066] Dans l'ensemble de ces configurations, la surface du capteur biométrique 13 du porte-carte 11 peut être sensiblement supérieure à la surface de 169 mm² typiquement utilisée pour les capteurs des cartes biométriques selon l'état de la technique. Cela permet d'augmenter la fiabilité et la vitesse de la lecture de l'empreinte biométrique de l'utilisateur du dispositif 10 selon l'invention.
- [0067] La [Fig.6] représente un comparatif des étapes pour la mise en œuvre des cartes biométriques selon l'état de la technique (partie gauche de la figure), et selon l'invention (partie droite de la figure). Comme on le voit, les étapes d'utilisation sont comparables, à ceci près que dans le cas des cartes biométriques connues, elles utilisent un dispositif d'enrôlement (enrôleur) souvent jetable et à usage unique, tandis que dans le cas de l'invention, l'enrôlement biométrique est effectué à l'aide du porte-carte 11, qui n'est pas jeté mais réutilisé dans le cadre de l'exécution des transactions de paiement. En outre, ce porte-carte 11 est évolutif en fonction des applications, comme cela va apparaître dans les cas d'usage décrits en relation avec les figures 7 à 12.
- [0068] En figures 7A à 7C on a représenté de façon schématique une version de base du dispositif biométrique 10 selon l'invention. Dans ce cas, le porte-carte 11 comporte plusieurs composants intégrés, à savoir un capteur biométrique 13, notamment un capteur d'empreintes digitales, une source d'alimentation 18 qui alimente chacun des autres composants via une ligne d'alimentation 20 qui est représentée par un trait continu, un microcontrôleur 19, et une interface utilisateur 22. Le trait interrompu 21 représente le canal de communication de données entre les différents composants.
- [0069] La source d'alimentation électrique 18 des composants du lecteur porte-carte 11 peut également être réalisée de différentes manières, soit par une batterie ou un super-condensateur intégré au porte-carte (figures 7A, 7B), soit par l'intermédiaire d'une prise USB intégrée au porte-carte ([Fig.7C]) dans les cas où celui-ci peut avoir une épaisseur compatible avec l'intégration d'une telle prise, soit encore par l'intermédiaire d'une antenne 23 apte à capter par induction l'énergie à partir d'un lecteur de carte à puce sans contact 30 ou d'une carte sans contact lors d'une transaction de paiement (figures 8A, 9).
- [0070] Afin de guider l'utilisateur pendant la réalisation des étapes d'une transaction avec un lecteur 30 externe, le porte-carte 11 sera de préférence pourvu d'une interface utilisateur 22 à des fins de signalisation ou de commande. L'interface utilisateur 22 peut être réalisée de différentes manières, allant de simples LEDs de signalisation visuelle, à un écran d'affichage intégré dans le porte-carte 11, et éventuellement pourvu de boutons de commande pour saisir par exemple le montant d'une transaction à exécuter.

- [0071] Le dispositif biométrique 10 selon l'invention permet une grande flexibilité de réalisation et une grande richesse de cas d'usage, en fonction notamment du type de carte à puce 12 utilisé. On décrira par la suite quelques exemples non exhaustifs de réalisation et de mise en œuvre, sans aucun caractère limitatif.
- [0072] Ainsi, dans le mode de réalisation représenté en figures 7A à 7C, l'enrôlement biométrique nécessite le positionnement de la carte à puce 12 dans le porte-carte 11 (figures 7B, 7C). L'alimentation électrique du porte-carte 11 se fait par sa batterie 18 ([Fig.7B]) ou par une prise USB alimentée par un câble USB externe ([Fig.7C]). L'alimentation électrique de la carte à puce 12 et la communication entre la carte à puce 12 et le porte-carte 11 se font alors directement par le porte-carte 11 par l'intermédiaire des contacts galvaniques du module 3 s'il s'agit d'une carte à puce à contacts.
- [0073] En figures 8A, 8B on a représenté des cas d'usage correspondant à une opération de paiement en mode CP (acronyme pour « Carte Présente ») entre une carte à puce 12 sans contact et un lecteur sans contact 30.
- [0074] En [Fig.8A], le porte-carte 11 comporte une antenne 23 pour la captation d'énergie par couplage inductif, et pour l'alimentation du porte-carte 11. Le lecteur 30 alimente électriquement la carte à puce 12 par couplage inductif. La carte à puce 12 est une carte à puce à fonctionnement dual à contact et sans contact. Elle alimente à son tour le porte-carte 11 par couplage inductif entre l'antenne 23 du porte-carte et l'antenne (non représentée) de la carte à puce 12. La communication entre la carte à puce 12 et le porte-carte 11 passe également par les contacts du module 3.
- [0075] Alternativement, comme représenté en [Fig.8B], la carte à puce duale 12 est alimentée par le lecteur 30 par couplage inductif, et la carte à puce 12 charge alors la batterie 18 du porte-carte 11 via les contacts de son module électronique 3.
- [0076] Dans le mode de réalisation de la [Fig.9A], le porte-carte 11 est pourvu d'une antenne 23 et la carte à puce 12 est une carte à fonctionnement dual. Le lecteur 30 alimente électriquement le porte-carte 11 directement via un couplage inductif entre son antenne et l'antenne 23 du porte-carte. Il alimente aussi la carte à puce 12 via une antenne (non représentée) connectée au module électronique 3. La communication de données entre la carte à puce 12 et le porte-carte 11 se fait via les contacts du module 3.
- [0077] La variante de la [Fig.9B] diffère de celle de la [Fig.9A] en ce que la communication de données entre la carte à puce duale 12 et le porte-carte 11 se fait en mode sans contact.
- [0078] Dans le mode de réalisation de la [Fig.10], le dispositif biométrique 10 selon l'invention est adapté à la réalisation d'une transaction de paiement en mode CNP (acronyme pour « Carte Non Présente ») avec un dispositif distant tel qu'un ordinateur

portable 26 ou un smartphone 27. A cet effet, on a intégré en plus dans le porte-carte 11 un composant de communication 24 par exemple de type BLE (acronyme pour « Bluetooth Low Energy »). Dans l'exemple représenté, l'alimentation électrique du porte-carte 11 est une batterie 18, mais on pourrait (version non représentée) utiliser une alimentation et la communication des données par un autre moyen, par exemple au moyen d'une interface USB. La communication des données biométriques entre le porte-carte 11 et la carte à puce 12 se fait en mode contact via les contacts ISO du module électronique 3 de la carte à puce et des contacts homologues (non représentés) du porte-carte 11.

- [0079] Dans le mode de réalisation de la [Fig.11], on a représenté l'utilisation simultanée de deux dispositifs biométriques 10a, 10b semblables au dispositif biométrique 10 de la [Fig.10], pour effectuer une transaction de paiement ou de transfert de valeur (crédits, jetons, ...) directement entre les deux dispositifs biométriques 10a, 10b. Dans le cas de figure schématisé, chacun des dispositifs biométriques 10a, 10b est alimenté par une batterie 18, mais l'un ou l'autre pourrait être alimenté différemment, notamment depuis l'extérieur par exemple via un câble USB. La communication de chaque carte à puce 12a, 12b avec son porte-carte respectif 11a, 11b se fait via les contacts des modules électroniques 3 des cartes à puce, mais l'un ou l'autre des dispositifs 10a, 10b pourrait utiliser une communication par couplage inductif entre sa carte à puce et son porte-carte.
- [0080] Dans ce mode d'utilisation, il suffira pour chaque utilisateur de positionner sa carte à puce 12 dans son lecteur porte-carte 11, de positionner un doigt sur son capteur d'empreintes 13 pour s'identifier de façon forte vis-à-vis de sa propre carte à puce 12, puis de rapprocher les deux dispositifs biométriques 10 à une distance inférieure à la portée d'une liaison NFC ou Bluetooth, et le transfert de valeur ou le paiement se fera de carte à carte via les lecteurs porte-carte 11 respectifs.
- [0081] Dans le mode de réalisation de la [Fig.12], on a représenté encore une autre évolution du dispositif biométrique 10 selon l'invention, adaptée à la réalisation d'une fonction de portefeuille électronique sécurisé (encore appelé « Cold Wallet » en terminologie anglo-saxonne.) Dans ce cas, le porte-carte 11 comporte en outre une mémoire sécurisée 27, encore appelée « Secure Element » en terminologie anglo-saxonne, et connue en soi. Cette mémoire sécurisée 27 permet par exemple de stocker un portefeuille de crypto monnaies à bord du porte-carte 11, que l'on peut alors utiliser pour des transactions avec un ordinateur 26 ou un smartphone 27 distant qui communiquent en mode sans-contact avec le porte-carte 11 via le module BLE 24.
- [0082] En définitive, le lecteur porte-carte 11 du dispositif biométrique 10 selon l'invention a deux fonctions de base, à savoir l'enrôlement de la biométrie de l'utilisateur dans

la carte bancaire 12, et l'authentification forte par biométrie de l'utilisateur lors de l'exécution d'une transaction, notamment une transaction bancaire.

[0083] A ces deux fonctions de base peuvent en être ajoutées d'autres à condition d'enrichir le lecteur porte-carte 11 et de le faire évoluer vers un objet multifonction démultipliant les usages de la carte bancaire, comme décrit en relation avec les exemples des figures 9 à 12.

Avantages de l'invention

[0084] En définitive, l'invention répond aux buts fixés.

[0085] Le capteur biométrique 13 déporté dans le lecteur porte-carte 11 permet d'augmenter la taille du capteur biométrique et par conséquent la facilité de l'enrôlement et la fiabilité de la reconnaissance biométrique. L'enrôlement est effectué via le porte-carte 11 qui contient un capteur biométrique. L'information biométrique captée par le porte-carte 11 est ensuite stockée dans la mémoire sécurisée de la carte à puce 12, comme connu en soi.

[0086] Le fait de pouvoir utiliser une surface du capteur biométrique 13 plus importante que celui d'une carte bancaire biométrique permet aussi d'améliorer la résolution et les taux d'erreur FAR et FRR et donc la sécurité du système tout en préservant l'expérience utilisateur.

[0087] En outre, le dispositif 10 selon l'invention permet d'utiliser des cartes bancaires standard, qu'elles soient à contact, sans contact, ou duales. Cela préserve la fiabilité et la durée de vie de la carte bancaire. De plus, aucune re-certification de la carte à puce ne sera nécessaire, au contraire d'une carte bancaire biométrique.

[0088] De plus, l'invention n'interfère pas avec les usages habituels de la carte bancaire standard, tels que les paiements à un point de vente, les retraits d'espèces aux distributeurs de billets, ou l'utilisation de la piste magnétique.

[0089] Enfin, le fait de conserver le porte-carte 11 aussi bien pour l'enrôlement biométrique que pour les opérations de transactions ultérieures est meilleur d'un point de vue écologique que les dispositifs d'enrôlement jetables connus.

Revendications

[Revendication 1]

Dispositif biométrique (10) pour la réalisation de transactions électroniques, comportant d'une part une carte à puce (12) pourvue d'un corps de carte intégrant un module microélectronique (3) comportant un microprocesseur et une mémoire pour stocker des informations d'identification du titulaire de la carte à puce, et comportant d'autre part un porte-carte (11) assurant l'enrôlement de la biométrie du porteur dans la carte à puce et l'authentification forte du porteur par biométrie lors d'une transaction, ledit porte-carte (11) étant configuré pour recevoir ladite carte à puce (12), et comportant un capteur biométrique (13) apte à capter une information biométrique d'un utilisateur du dispositif (10) et une interface de communication configurée pour transmettre ladite information biométrique au module microélectronique (3) de la carte à puce, et ledit porte-carte (11) comportant en outre un microcontrôleur (19) recevant l'information biométrique du capteur biométrique (13), une interface utilisateur (22) apte à indiquer à l'utilisateur le statut des échanges d'information entre ladite carte à puce (12) et ledit porte-carte (11), caractérisé en ce que la surface utile du capteur biométrique (13) du porte-carte (11) est supérieure à 169 mm^2 , et en ce que ledit porte-carte (11) comporte une source d'énergie (18) alimentant électriquement le capteur biométrique (13), le microcontrôleur (19), et l'interface utilisateur (22), ladite source d'énergie (18) du porte-carte (11) étant prise parmi une batterie ou un super condensateur susceptible d'être connecté de manière filaire à un dispositif d'alimentation externe, une cellule photovoltaïque, ou une antenne (23) susceptible d'être couplée inductivement à un dispositif d'alimentation sans contact externe.

[Revendication 2]

Dispositif biométrique (10) selon la revendication 1, caractérisé en ce que la carte à puce (12) est une carte à contact pourvue d'une interface à contacts selon la norme ISO 7816-1 et en ce que le porte-carte (11) comporte une interface à contacts apte à engager de façon galvanique les contacts de l'interface à contacts de la carte à puce (12).

[Revendication 3]

Dispositif biométrique (10) selon la revendication 1, caractérisé en ce que la carte à puce (12) est une carte à fonctionnement sans contact ou à fonctionnement dual à contact et sans contact, comportant

une antenne connectée à une interface de communication sans contact du module microélectronique (3), et en ce que le porte-carte (11) comporte une antenne connectée au microcontrôleur (19) du porte-carte (11) et apte à être positionnée en couplage inductif avec l'antenne de la carte à puce (12).

- [Revendication 4] Dispositif biométrique (10) selon l'une des revendications 1 à 3, caractérisé en ce que le porte-carte (11) possède sur sa face avant un moyen (15) de guidage ou de rétention de la carte à puce (12).
- [Revendication 5] Dispositif biométrique (10) selon la revendication 4, caractérisé en ce que ledit moyen (15) de guidage ou de rétention de la carte à puce (12) est constitué par un couvercle (15) délimitant une fente (16) dans laquelle s'insère la carte à puce (12), et en ce que le capteur biométrique (13) est situé sur la face externe du couvercle (15).
- [Revendication 6] Dispositif biométrique (10) selon la revendication 4, caractérisé en ce que ledit moyen (15) de guidage ou de rétention de la carte à puce (12) est constitué par une glissière périphérique aménagée sur au moins deux côtés du porte-carte et dans laquelle s'insère la carte à puce (12), et en ce que le capteur biométrique (13) du porte-carte (11) est situé sur la face arrière du porte-carte (11).
- [Revendication 7] Dispositif biométrique (10) selon l'une des revendications précédentes, caractérisé en ce que le porte-carte (11) est fixé à plusieurs cartes à puce (12) articulées entre elles en éventail.
- [Revendication 8] Dispositif biométrique (10) selon l'une des revendications 1 à 6, caractérisé en ce que le porte-carte (11) est configuré en forme de portefeuille ou est intégré à un accessoire tel qu'une coque de téléphone portable.
- [Revendication 9] Dispositif biométrique (10) selon l'une quelconque des revendications précédentes, caractérisé en ce que le porte-carte (11) comporte en outre un module de communication radiofréquence (24), apte à établir une liaison de type BLE entre le porte-carte (11) et un ordinateur (26) ou un smartphone (27) distant, ou avec un autre dispositif biométrique (10).
- [Revendication 10] Dispositif biométrique (10) selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte en outre une mémoire sécurisée (27) apte à stocker un portefeuille de monnaies ou valeurs électroniques.
- [Revendication 11] Utilisation d'un système constitué d'un dispositif biométrique (10) selon l'une quelconque des revendications précédentes et d'un

lecteur sans contact (30) de carte à puce, dans laquelle ledit lecteur sans contact (30) est utilisé pour alimenter électriquement une carte à puce (12) sans contact par couplage inductif entre le lecteur sans contact (30) et ladite carte à puce, et pour alimenter électriquement le porte-carte (11) par contact galvanique entre la carte à puce (12) et le porte-carte (11).

[Revendication 12]

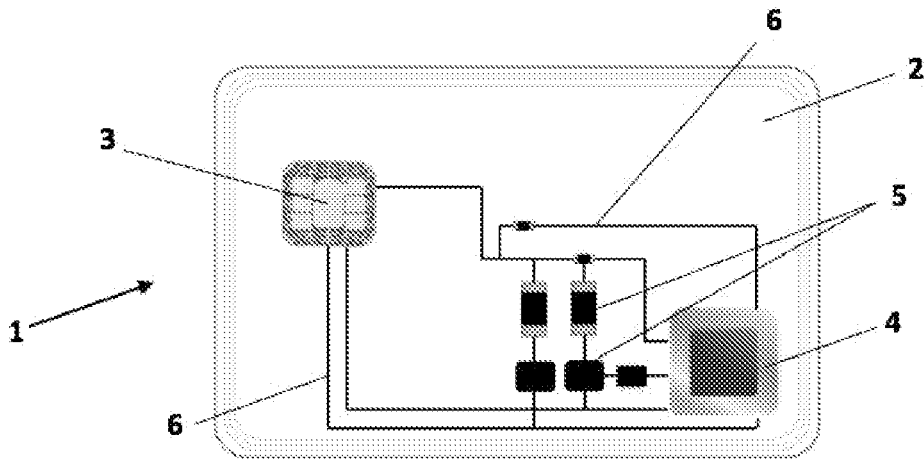
Utilisation d'un système constitué d'un dispositif biométrique (10) selon l'une quelconque des revendications 1 à 10 et d'un lecteur sans contact (30) de carte à puce, dans laquelle ledit lecteur sans contact (30) est utilisé pour alimenter électriquement une carte à puce sans contact (12) et le porte-carte (11) par couplage inductif entre le lecteur sans contact (30), le porte-carte (11) et la carte à puce (12).

[Revendication 13]

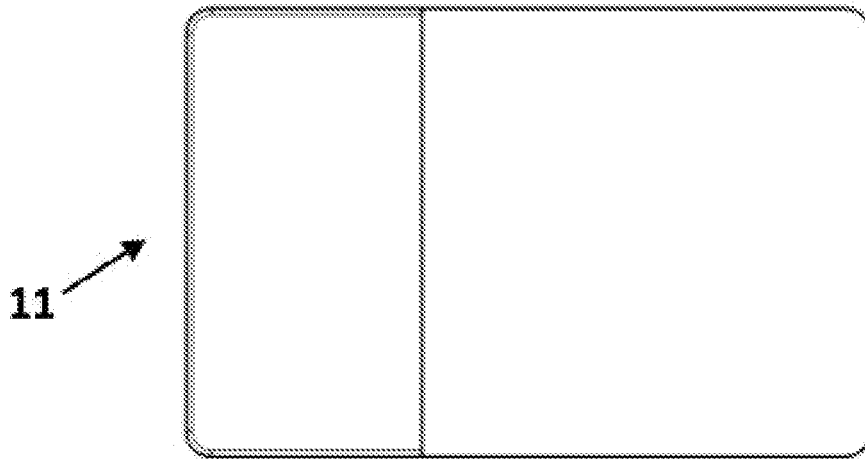
Procédé de réalisation par un utilisateur d'une transaction électronique entre un lecteur NFC (30) d'un système de transaction par cartes à puce et un dispositif biométrique (10) selon l'une quelconque des revendications 1 à 10, caractérisé en ce qu'il comporte des étapes consistant à :

- dans une phase préliminaire d'enrôlement de l'utilisateur, positionner une carte à puce (12) de l'utilisateur sur le porte-carte (11), apposer un doigt de l'utilisateur sur le capteur biométrique (13) du porte-carte (11) de façon à capter par le porte-carte (11) une empreinte biométrique de référence de l'utilisateur, puis transmettre cette empreinte biométrique de référence du porte-carte (11) à la carte à puce (12) et la stocker dans une mémoire de la carte à puce (12) ;
- dans une phase d'exécution d'une transaction électronique, positionner sur le porte-carte (11) la carte à puce (12) contenant l'empreinte biométrique de référence et un microprogramme d'exécution de transactions électroniques, puis apposer le doigt de l'utilisateur sur le capteur biométrique (13) du porte-carte (11) de façon à capter et transmettre à la carte à puce (12) une empreinte biométrique de transaction ;
- comparer par le microprogramme de la carte à puce (12) l'empreinte biométrique de référence et l'empreinte biométrique de transaction, et en cas de correspondance des deux empreintes biométriques, autoriser l'exécution par le microprogramme de la carte à puce (12) de la transaction électronique entre la carte à puce (12) et le lecteur NFC (30).

[Fig. 1]



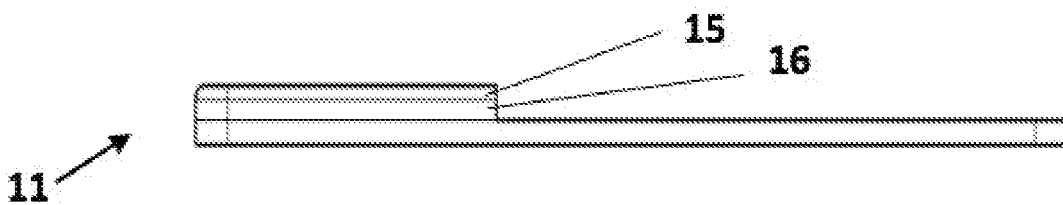
[Fig. 2A]



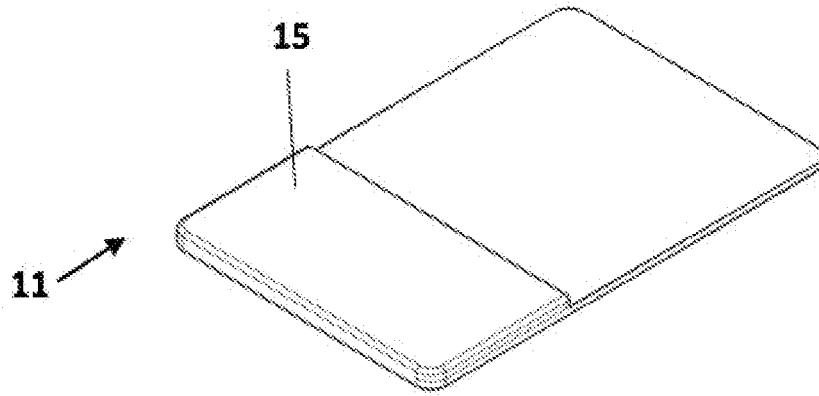
[Fig. 2B]



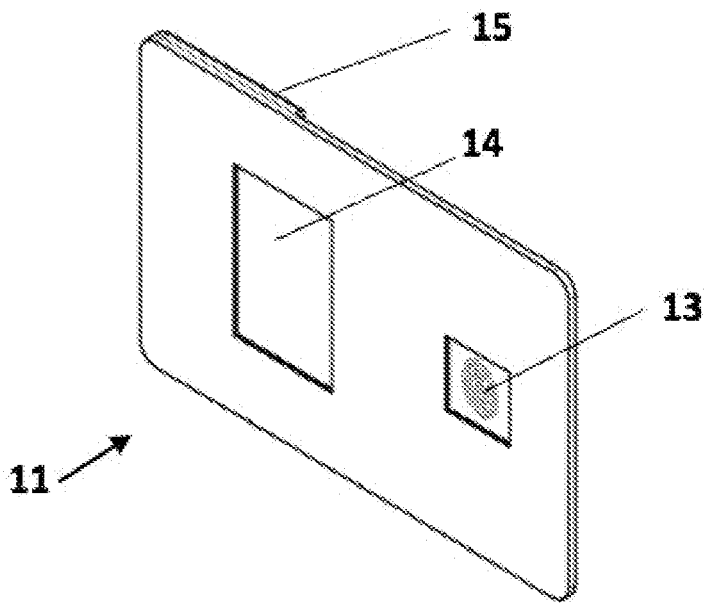
[Fig. 2C]



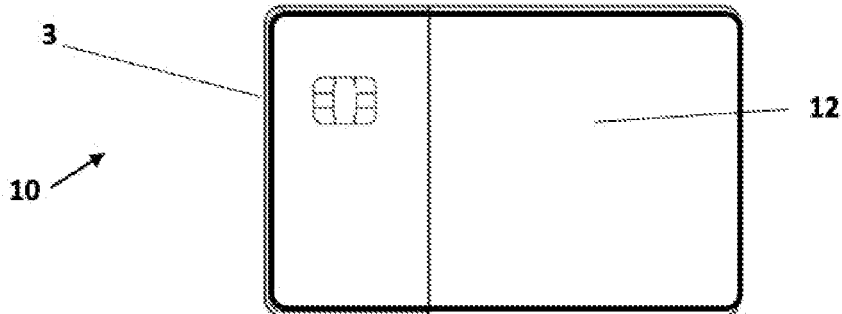
[Fig. 2D]



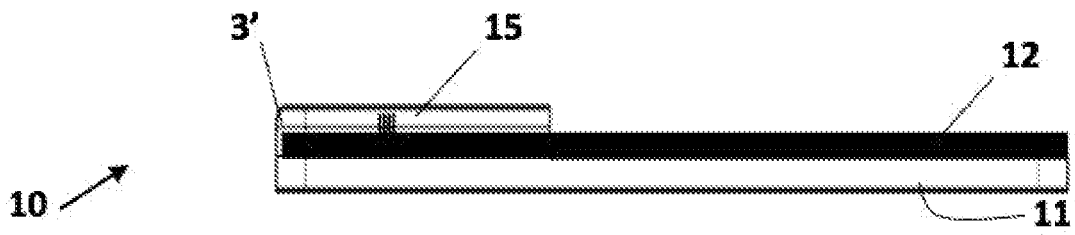
[Fig. 2E]



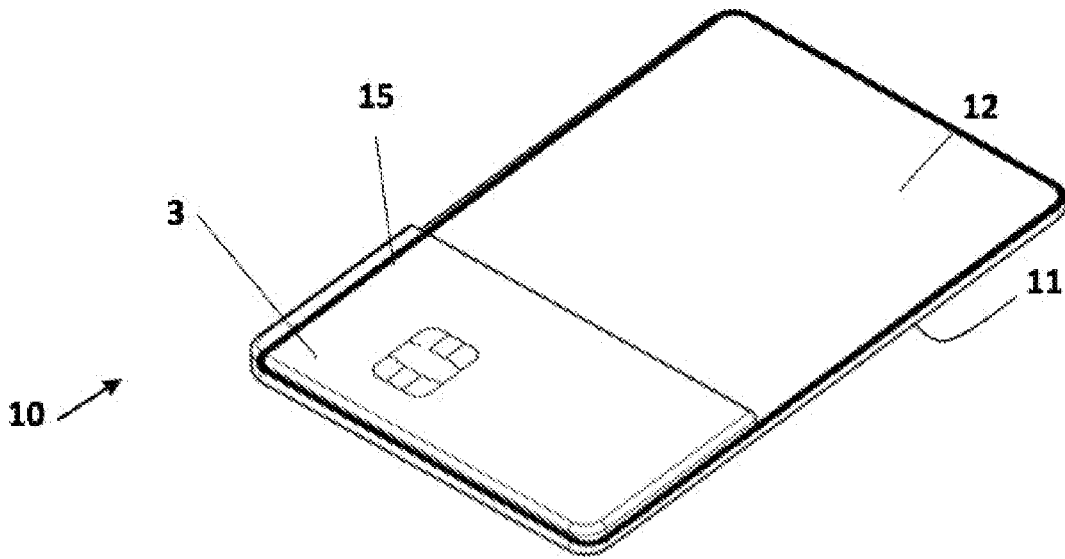
[Fig. 3A]



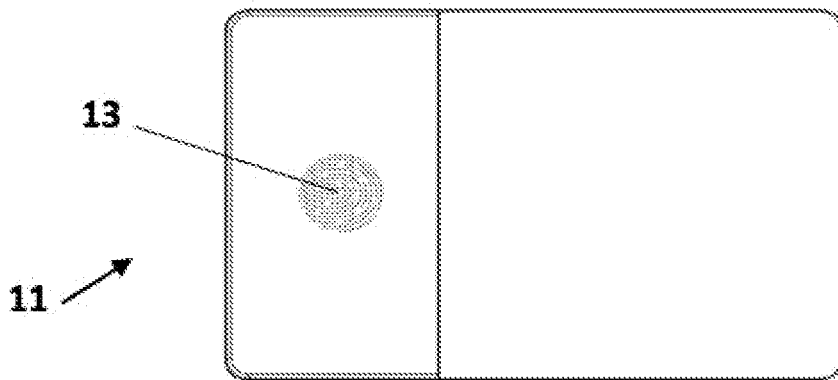
[Fig. 3B]



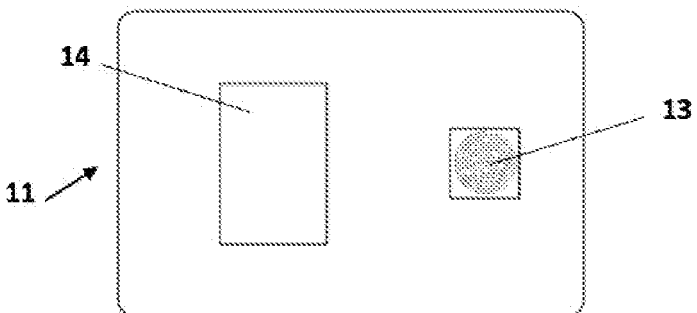
[Fig. 3C]



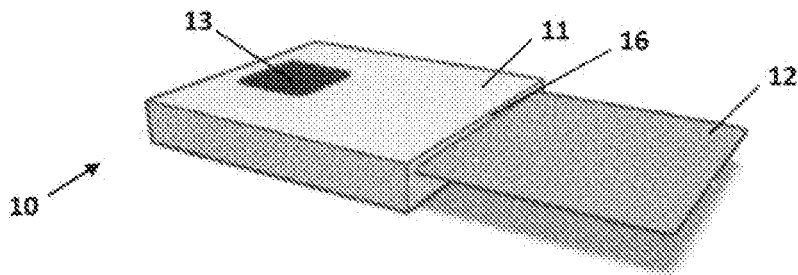
[Fig. 4A]



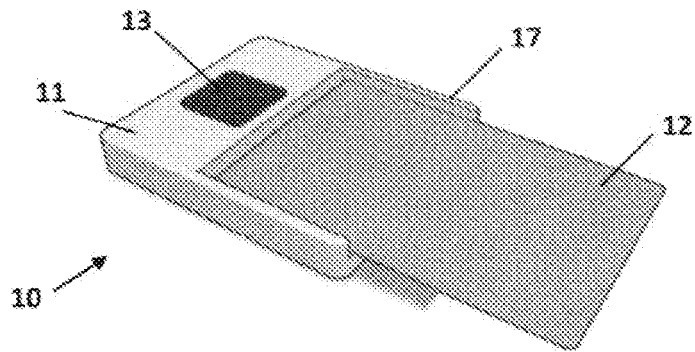
[Fig. 4B]



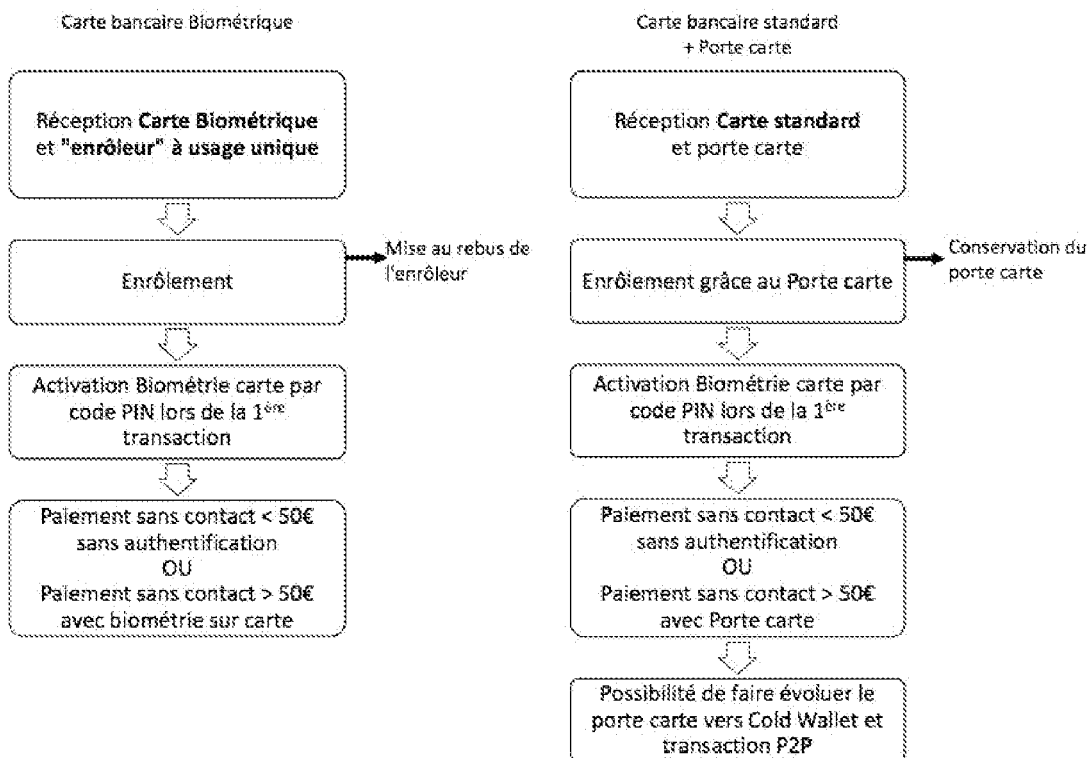
[Fig. 5A]



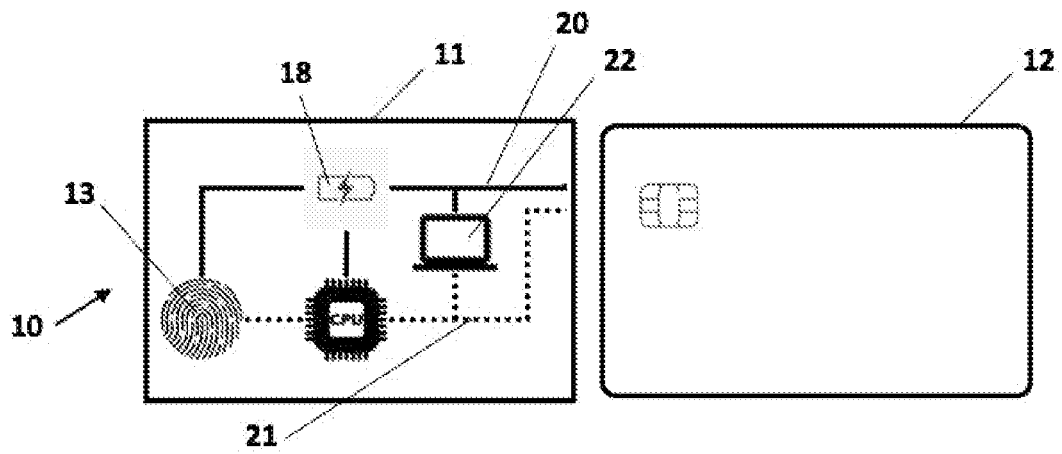
[Fig. 5B]



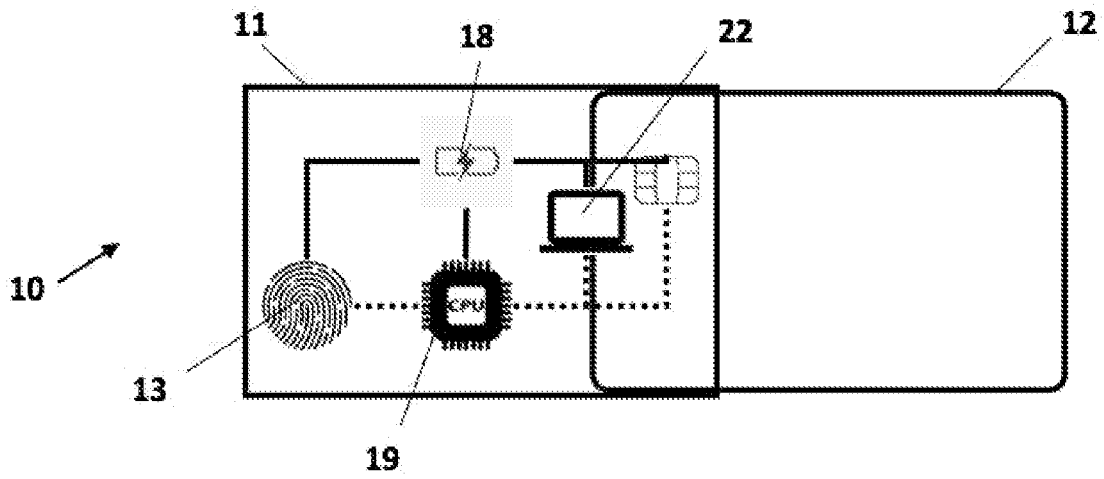
[Fig. 6]



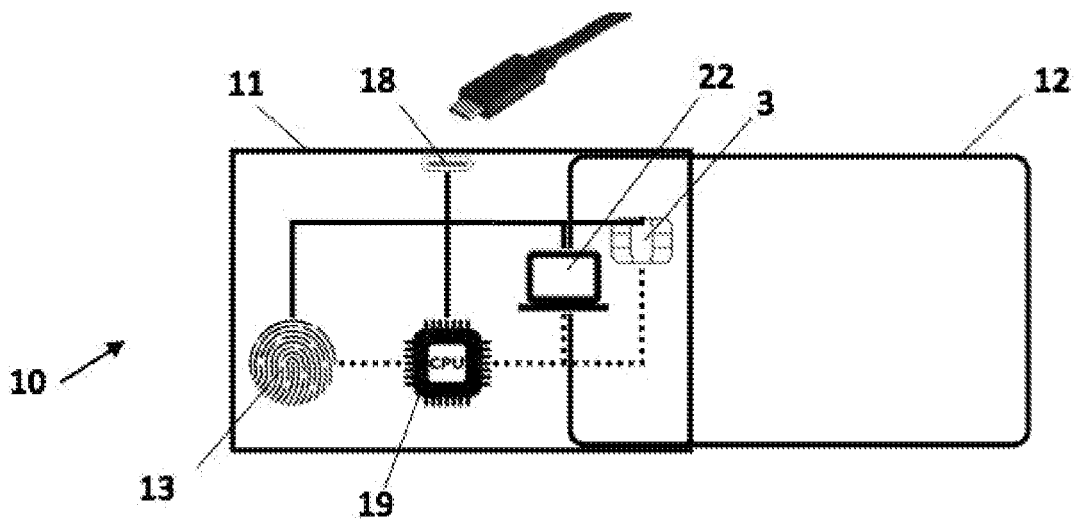
[Fig. 7A]



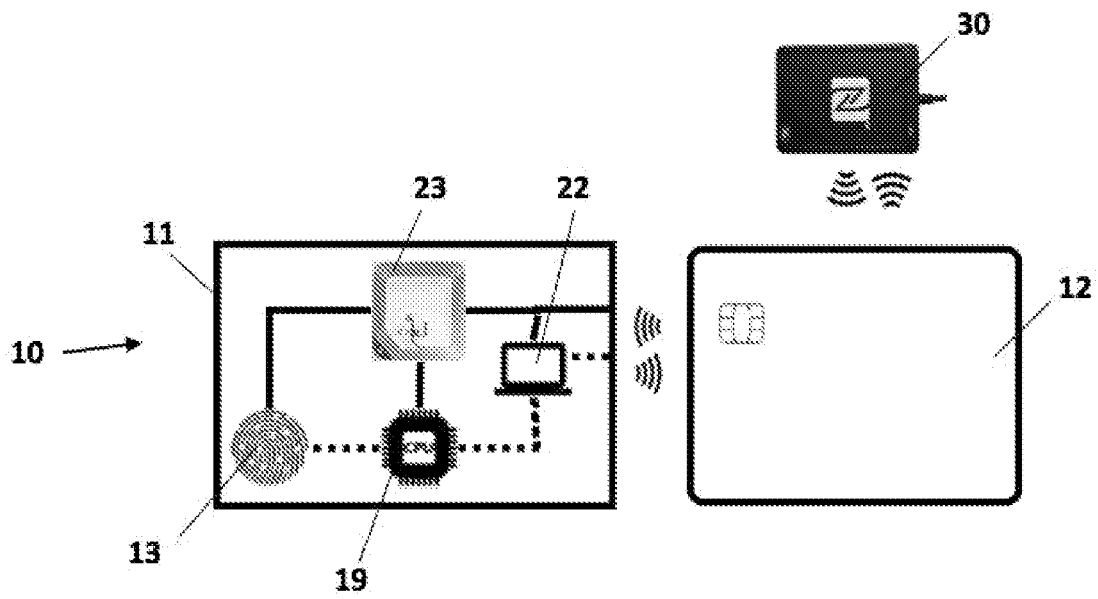
[Fig. 7B]



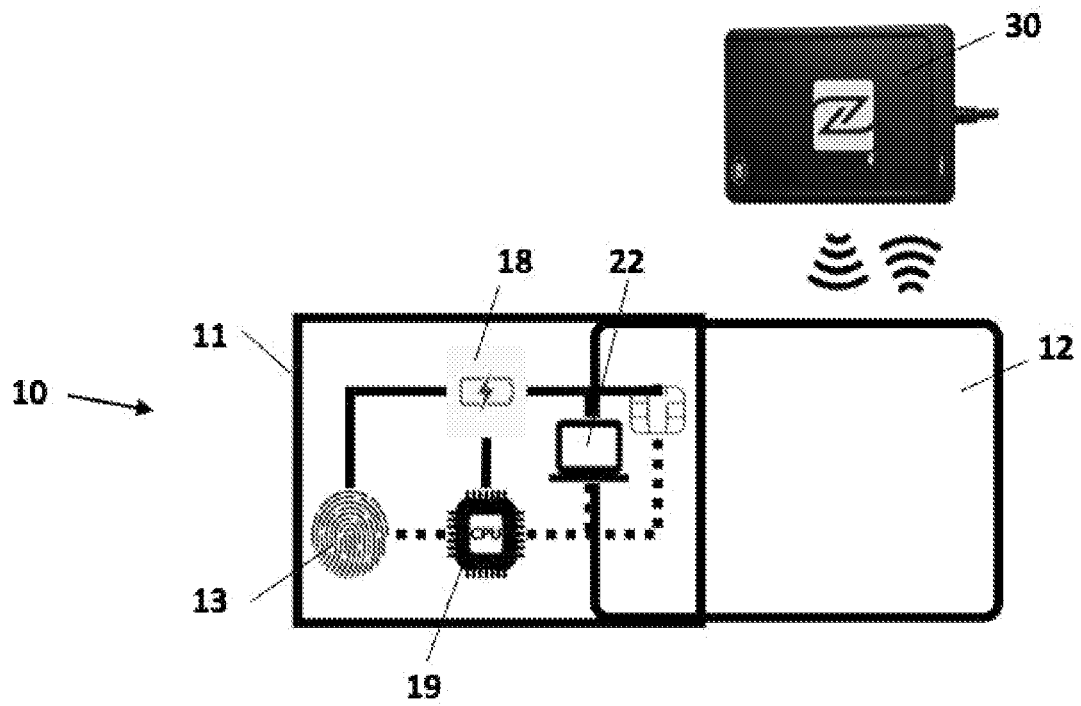
[Fig. 7C]



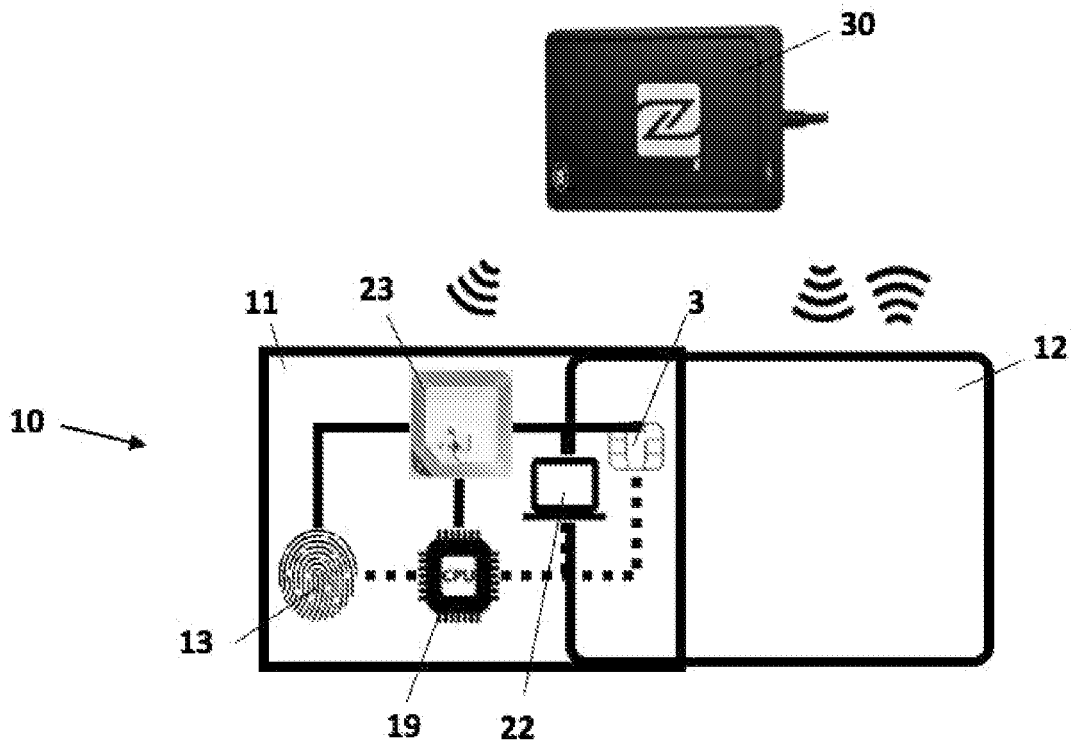
[Fig. 8A]



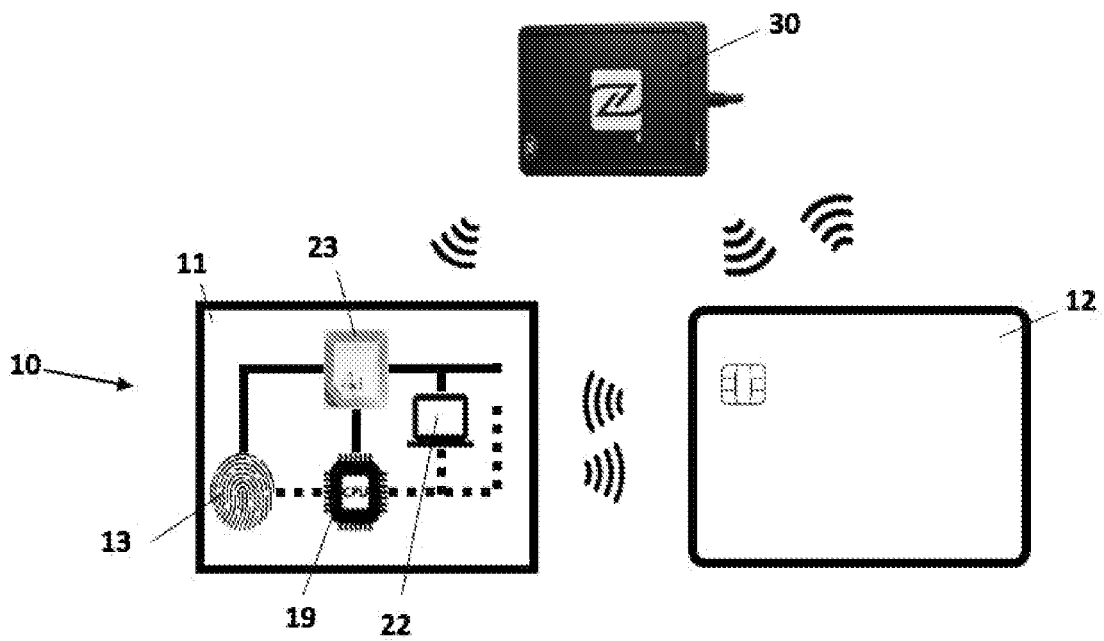
[Fig. 8B]



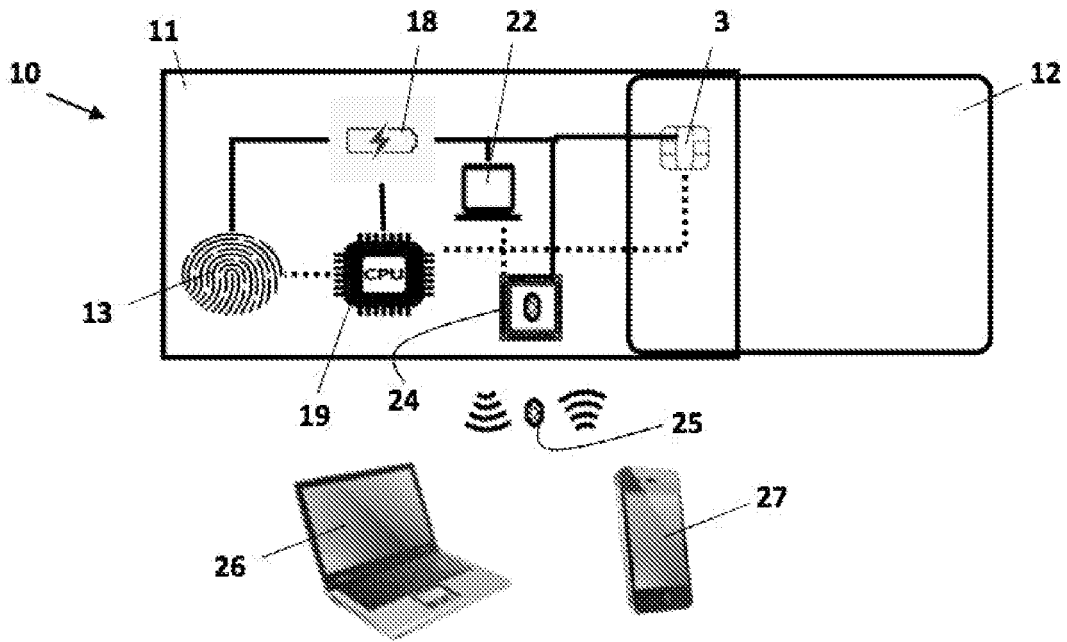
[Fig. 9A]



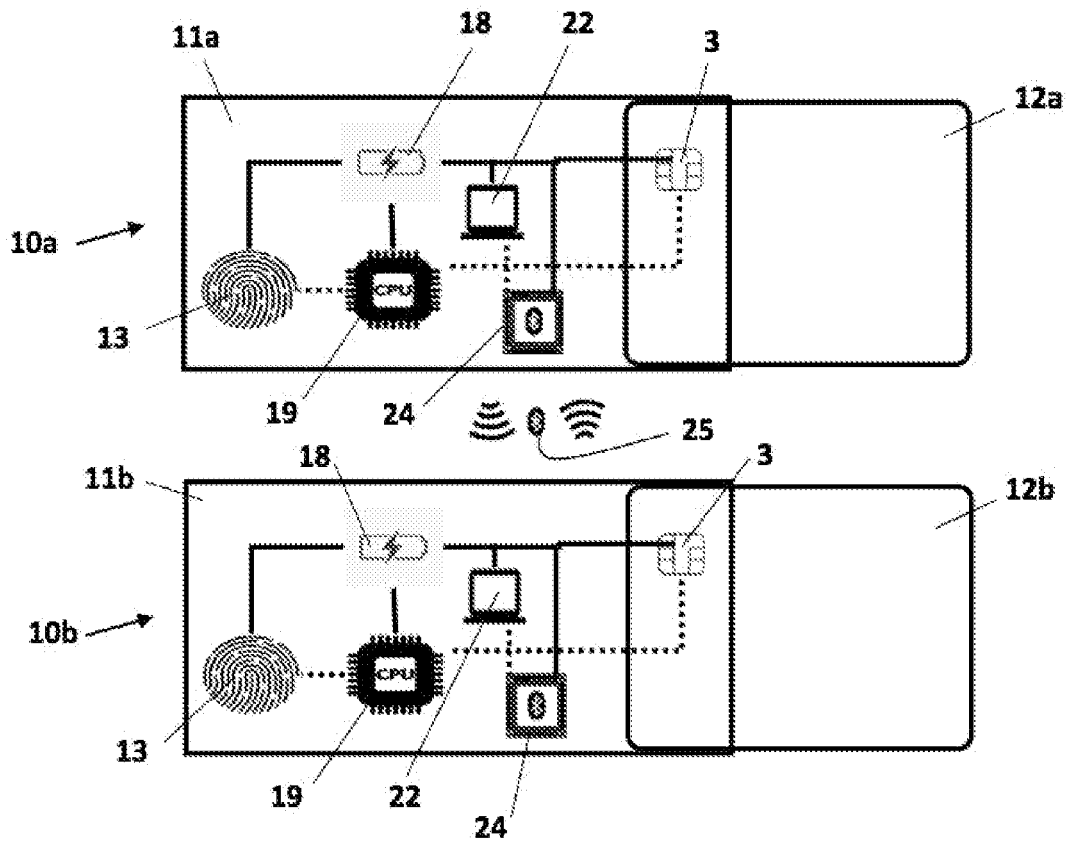
[Fig. 9B]



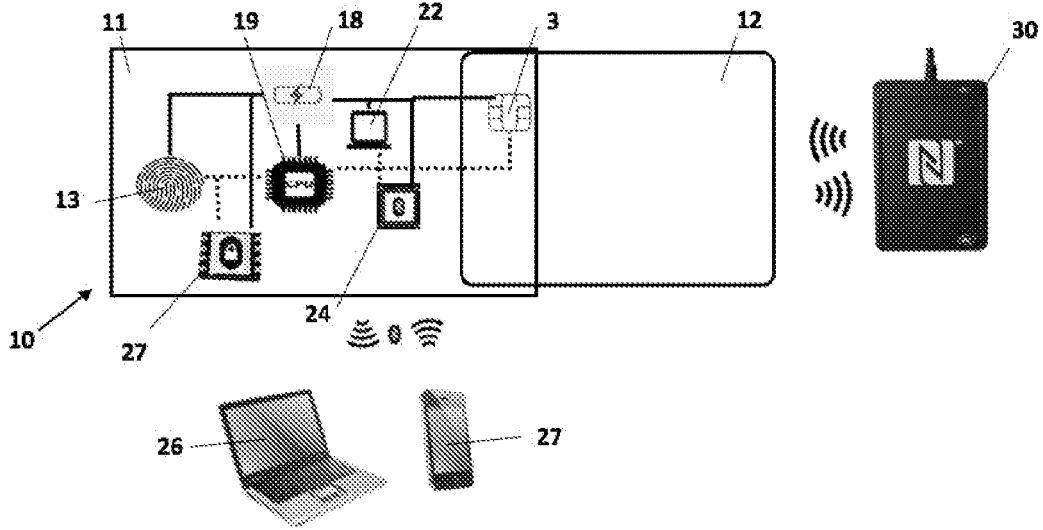
[Fig. 10]



[Fig. 11]



[Fig. 12]



RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveau) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.

Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

Le demandeur a maintenu les revendications.

Le demandeur a modifié les revendications.

Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

Aucun document n'a été cité en cours de procédure.

**1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN
CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION**

JP 2004 220175 A (SEIKO EPSON CORP)
5 août 2004 (2004-08-05)

US 2021/192529 A1 (SOUCHON PIERRE [FR] ET
AL) 24 juin 2021 (2021-06-24)

US 2007/040017 A1 (KOZLAY DOUGLAS [US])
22 février 2007 (2007-02-22)

**2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN
TECHNOLOGIQUE GENERAL**

MARIANO FONS ET AL: "Hardware-Software
Co-design of a Fingerprint Matcher on
Card",
ELECTRO/INFORMATION TECHNOLOGY, 2006 IEEE
INTERNATIONAL CONFERENCE ON, IEEE, PI,
1 mai 2006 (2006-05-01), pages 113-118,
XP031019887,
ISBN: 978-0-7803-9592-3

EP 1 120 755 A1 (PEDERSEN SOREN DEGNBOL
[DK]) 1 août 2001 (2001-08-01)

**3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND
DE LA VALIDITE DES PRIORITES**

NEANT