(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 149 410**

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

(21) **N° d'enregistrement national :** **24 05517**

(51) Int Cl[8] : ***G 06 Q 20/40*** *(2024.01), G 06 F 21/32, G 06 Q 20/08, 20/16, 20/22, 20/30, 20/38, G 06 F 21/31, G 06 V 40/12*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 29.05.24.

(30) **Priorité :** 30.05.23 EP 23315219.8.

(43) **Date de mise à la disposition du public de la demande :** 06.12.24 Bulletin 24/49.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

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

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *THALES DIS FRANCE SAS SAS, société par actions simplifiée* — FR.

(72) **Inventeur(s) :** FAVREAU Valentin, OUNG Richard et CHUA Jun Ping Bryan.

(73) **Titulaire(s) :** THALES DIS FRANCE SAS SAS, société par actions simplifiée.

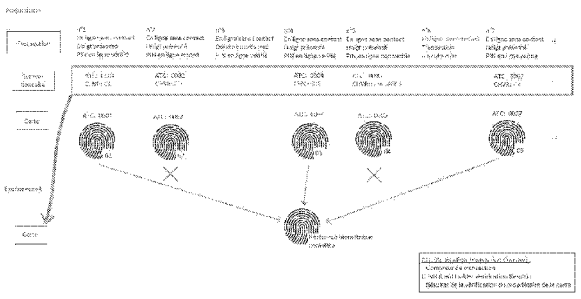
(74) **Mandataire(s) :**

(54) **Procédé pour l'inscription d'une référence biométrique dans un dispositif portable.**

(57) L'invention concerne un procédé pour l'inscription d'une référence (51) dans un dispositif portable (10) intégrant un capteur biométrique (14) dans lequel une première phase comporte l'étape suivante exécutée pour une pluralité de transactions avec un ou plusieurs terminaux (20) :

- pendant chaque transaction en cours de ladite pluralité de transactions, la capture d'une donnée biométrique candidate (60) à partir d'un identificateur de sujet d'un utilisateur (50), l'attribution d'un indicateur (58) à la donnée biométrique candidate (60), ledit indicateur permettant de déterminer si l'utilisateur a été authentifié avec succès pendant ladite transaction en cours et le stockage de la donnée biométrique candidate et dudit indicateur attribué dans le dispositif portable ;

et en ce que le procédé comprend une deuxième phase, dans laquelle, lors d'une détection d'un événement, le dispositif portable identifie une liste de données biométriques candidates dont l'indicateur attribué reflète une authentification couronnée de succès de l'utilisateur, et construit la référence uniquement à l'aide de ladite liste.



FR 3 149 410 - A1

Description

Titre de l'invention : Procédé pour l'inscription d'une référence biométrique dans un dispositif portable

[0001] (DOMAINE DE L'INVENTION)

[0002] La présente invention concerne des procédés permettant d'inscrire une référence biométrique dans un appareil portable. Elle se rapporte en particulier à des procédés pour l'inscription d'une référence biométrique d'un utilisateur à l'aide d'un capteur biométrique intégré dans un dispositif portable.

[0003] (ARRIERE-PLAN DE L'INVENTION)

[0004] Un dispositif portable peut être une carte à puce comprenant une mémoire, un microprocesseur et un système d'exploitation pour des traitements informatiques. Il peut comprendre des applications de services de type applications de paiement ou de télécommunication. Des cartes à puce peuvent être considérées comme des éléments sécurisés. Elles comprennent une pluralité de mémoires de différents types, comme une mémoire non volatile et une mémoire volatile. Elles sont considérées comme inviolables (ou « sécurisées ») parce qu'elles sont capables de commander un accès aux données qu'elles contiennent et d'autoriser ou non l'utilisation de leurs données par d'autres machines. Une carte à puce peut également fournir des services de calcul en fonction de composants cryptographiques. En général, des cartes à puce ont des ressources informatiques limitées et des ressources de mémoire limitées et elles sont prévues pour connecter une machine hôte qui peut leur fournir de la puissance électrique soit en mode de contact soit en mode sans contact.

[0005] Un dispositif portable peut connecter un dispositif terminal pour participer à une transaction. Par exemple, lorsque le dispositif portable est un instrument de paiement, il peut participer à une transaction de paiement avec un terminal de point de vente (POS).

[0006] Des dispositifs portables intégrant un capteur biométrique peuvent devoir inscrire une référence biométrique d'un utilisateur authentique de sorte qu'ils peuvent compter sur la référence biométrique inscrite pour authentifier l'utilisateur dans une phase ultérieure.

[0007] Habituellement, le dispositif portable doit capturer entre 5 et 12 échantillons biométriques pour construire une référence biométrique fiable.

[0008] De nombreux dispositifs portables sont dépourvus de batterie ou ont une ressource de puissance très limitée. L'inscription d'une référence biométrique fiable par le capteur biométrique intégré dans le dispositif portable exige que le dispositif portable soit alimenté en puissance pendant plusieurs minutes.

[0009] Le dispositif portable peut obtenir de l'énergie en provenance d'un équipement terminal couplé pendant une transaction impliquant à la fois le dispositif portable et l'équipement terminal.

[0010] Le document US2019/0318361 A1 décrit un système pour l'inscription d'une référence biométrique d'un utilisateur utilisant une référence anonyme d'un client associée à un attribut de l'utilisateur.

[0011] (RESUME DE L'INVENTION)

[0012] Pendant l'opération d'inscription, le dispositif portable capture et stocke plusieurs échantillons biométriques. Typiquement, un ensemble d'empreintes digitales de la personne manipulant le dispositif portable est capté et enregistré en tant qu'échantillons biométriques dans le dispositif portable. Lorsque le dispositif portable est une carte de paiement sans contact, le dispositif portable peut capturer des échantillons biométriques pendant une transaction de paiement sans contact. Il convient de noter que les échantillons biométriques sont capturés et stockés sans vérification de leur validité. En fonction de règles de sécurité, la transaction de paiement sans contact peut être achevée avec succès sans authentification du titulaire de carte. Par exemple, lorsque le montant est inférieur à un seuil prédéfini, la carte peut accepter la transaction de paiement sans exiger d'authentification du titulaire de carte.

[0013] En supposant que la carte de paiement sans contact a été perdue ou volée et récupérée par la personne malveillante, la personne malveillante peut inscrire sa propre empreinte digitale dans la carte au lieu de l'utilisateur authentique.

[0014] Il y a un besoin pour empêcher une personne autre que l'utilisateur officiel de la carte d'inscrire son empreinte digitale dans la carte.

[0015] L'invention vise à résoudre le problème technique susmentionné.

[0016] Un objet de la présente invention est un procédé pour l'inscription d'une référence biométrique attribuée à un utilisateur dans un dispositif portable intégrant une mémoire non volatile et un capteur biométrique. Le procédé comprend une première phase comportant l'étape suivante exécutée pour une pluralité de transactions, dont la finalité première est différente d'une inscription biométrique, entre un ou plusieurs terminaux et ledit dispositif portable :

- pendant chaque transaction en cours de ladite pluralité de transactions, la capture d'une donnée biométrique candidate à partir d'un identificateur de sujet de l'utilisateur par le capteur biométrique, l'attribution d'un indicateur à la donnée biométrique candidate, ledit indicateur permettant de déterminer si l'utilisateur a été authentifié avec succès en utilisant un code secret entré par l'utilisateur pendant ladite transaction en cours et le stockage de la donnée biométrique candidate et dudit indicateur attribué, dans la mémoire non volatile.

[0017] Le procédé comprend une deuxième phase, postérieure à la première phase, dans laquelle, lors d'une détection d'un événement prédéterminé, le dispositif portable identifie une liste desdites données biométriques candidates dont l'indicateur attribué reflète le fait que l'utilisateur a été authentifié avec succès, et construit la référence biométrique uniquement à l'aide de données biométriques candidates appartenant à ladite liste.

[0018] Avantageusement, chaque indicateur peut contenir une référence de la transaction en cours pendant laquelle il a été attribué,
pendant chaque transaction en cours, un serveur distant peut essayer d'authentifier l'utilisateur et stocke une paire comprenant la référence de la transaction en cours et une balise reflétant si l'utilisateur a été authentifié avec succès pendant ladite transaction en cours, et
pendant la deuxième phase, le dispositif portable peut récupérer lesdites paires auprès du serveur distant et peut identifier la liste de données biométriques candidates en trouvant la correspondance entre des indicateurs stockés et des balises appartenant aux paires récupérées.

[0019] Avantageusement, le serveur distant peut détecter l'événement prédéterminé en comparant le nombre de paires stockées à un premier seuil et le serveur distant peut initier l'envoi desdites paires au dispositif portable.

[0020] Avantageusement, le dispositif portable peut récupérer lesdites paires auprès du serveur distant par l'intermédiaire d'une application logicielle hébergée sur un téléphone, lesdites paires étant acheminées entre le dispositif portable et le téléphone par le biais d'un canal NFC© ou BLE©.

[0021] Avantageusement, le dispositif portable peut détecter l'événement prédéterminé en comparant le nombre de données biométriques candidates stockées à un second seuil, le dispositif portable peut être une carte combi qui rejette volontairement une transaction sans contact en cours de réalisation avec un terminal couplé pour forcer le terminal couplé à établir une connexion filaire entre le serveur distant et le dispositif portable, et le dispositif portable peut récupérer lesdites paires auprès du serveur distant par l'intermédiaire de la connexion filaire.

[0022] Avantageusement, pendant chaque transaction en cours, le dispositif portable peut essayer d'authentifier l'utilisateur et peut stocker dans l'indicateur généré pendant la transaction en cours une valeur reflétant si l'utilisateur a été authentifié avec succès pendant la transaction en cours.

[0023] Avantageusement, le procédé peut comprendre une troisième phase, postérieure à la deuxième phase, dans laquelle, une nouvelle liste de données biométriques candidates supplémentaires dont l'indicateur attribué indique que l'utilisateur a été authentifié avec succès est identifiée et le dispositif portable peut affiner la référence biométrique à

l'aide de données biométriques candidates supplémentaires appartenant à la nouvelle liste.

[0024] Un autre objet de la présente invention est un dispositif portable intégrant une mémoire non volatile et un capteur biométrique et apte à inscrire une référence biométrique attribuée à un utilisateur. Le dispositif portable est configuré pour mettre en œuvre une première phase comportant l'étape suivante exécutée pour une pluralité de transactions entre un ou plusieurs terminaux et ledit dispositif portable :
- pendant chaque transaction en cours de ladite pluralité de transactions, le dispositif portable est configuré pour capturer une donnée biométrique candidate à partir d'un identificateur de sujet de l'utilisateur par le capteur biométrique, pour attribuer un indicateur à la donnée biométrique candidate, ledit indicateur permettant de déterminer si l'utilisateur a été authentifié avec succès pendant ladite transaction en cours et pour stocker la donnée biométrique candidate et ledit indicateur attribué dans la mémoire non volatile.

[0025] Le dispositif portable est configuré pour mettre en œuvre une deuxième phase, postérieure à la première phase, dans laquelle, lors d'une détection d'un événement prédéterminé, le dispositif portable est configuré pour identifier une liste desdites données biométriques candidates dont l'indicateur attribué reflète le fait que l'utilisateur a été authentifié avec succès, et pour construire la référence biométrique uniquement à l'aide de données biométriques candidates appartenant à ladite liste.

[0026] Un autre objet de la présente invention est un système comprenant un dispositif portable selon l'invention, un terminal de transaction et un serveur distant. Chaque indicateur contient une référence de la transaction en cours pendant laquelle il a été attribué. Pendant chaque transaction en cours, le serveur distant est configuré pour essayer d'authentifier l'utilisateur et pour stocker une paire comprenant la référence de la transaction en cours et une balise reflétant si l'utilisateur a été authentifié avec succès pendant ladite transaction en cours. Pendant la deuxième phase, le dispositif portable est configuré pour récupérer lesdites paires auprès du serveur distant et pour identifier la liste de données biométriques candidates en trouvant la correspondance entre des indicateurs stockés et des balises appartenant aux paires récupérées.

[0027] Avantageusement, le serveur distant peut être configuré pour détecter l'événement prédéterminé en comparant le nombre de paires stockées à un premier seuil et le serveur distant peut être configuré pour initier l'envoi desdites paires au dispositif portable.

[0028] Avantageusement, le dispositif portable peut être configuré pour récupérer lesdites paires auprès du serveur distant par l'intermédiaire d'une application logicielle hébergée sur un téléphone, lesdites paires étant acheminées entre le dispositif portable et le téléphone par le biais d'un canal NFC© ou BLE©.

[0029] Avantageusement, le dispositif portable peut être configuré pour détecter l'événement prédéterminé en comparant le nombre de données biométriques candidates stockées à un second seuil, le dispositif portable peut être une carte double configurée pour rejeter volontairement une transaction sans contact en cours de réalisation avec un terminal couplé pour forcer le terminal couplé à établir une connexion filaire entre le serveur distant et le dispositif portable, et le dispositif portable peut être configuré pour récupérer lesdites paires auprès du serveur distant par l'intermédiaire de la connexion filaire.

[0030] Avantageusement, pendant chaque transaction en cours, le dispositif portable peut être configuré pour essayer d'authentifier l'utilisateur et de stocker dans l'indicateur généré pendant la transaction en cours une valeur reflétant si l'utilisateur a été authentifié avec succès pendant la transaction en cours.

[0031] Avantageusement, pendant une troisième phase, postérieure à la deuxième phase, le dispositif portable peut être configuré pour affiner la référence biométrique à l'aide d'une nouvelle liste de données biométriques candidates supplémentaires dont l'indicateur attribué indique que l'utilisateur a été authentifié avec succès.

[0032] Avantageusement, le dispositif portable peut être un instrument de paiement, le terminal de transaction peut être un terminal de paiement et le serveur distant peut être un serveur de banque.

[0033] (BREVE DESCRIPTION DES DESSINS)

[0034] D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante d'un certain nombre de modes de réalisation préférés de l'invention, en référence aux dessins joints correspondants sur lesquels :

- la [Fig.1] montre un premier diagramme de flux donné à titre d'exemple permettant d'inscrire une référence biométrique dans un dispositif portable selon un exemple de l'invention ;
- la [Fig.2] montre une première architecture donnée à titre d'exemple d'un dispositif portable selon un exemple de l'invention ;
- la [Fig.3] montre un diagramme d'architecture d'un système comprenant un dispositif portable, un terminal et un serveur distant selon un exemple de l'invention, et
- la [Fig.4] montre un second diagramme de flux permettant d'inscrire une référence biométrique dans un dispositif portable selon un exemple de l'invention.

[0035] (DESCRIPTION DETAILLEE DES MODES DE REALISATION PREFERES)

[0036] Des cartes à puce comprennent au moins une interface de communication pour échanger des données avec l'extérieur. Certaines cartes à puce ont une interface de contact apte à communiquer en mode de contact telle que définie par les normes ISO/IEC7816. Certaines cartes à puce ont une interface sans contact apte à communiquer

en mode sans contact lesquelles peuvent être conformes aux normes ISO14443, ISO/IEC21481 ou ISO18092.

[0037] Certaines cartes à puce ont à la fois une interface de contact et une interface sans contact. Elles sont appelées cartes combi (ou de type combi ou à double interface).

[0038] L'invention peut s'appliquer à n'importe quel type de dispositif portable intégrant un ou plusieurs capteurs biométriques. L'invention peut s'appliquer à n'importe quel type de cartes à puce biométriques. L'invention peut s'appliquer à des transactions dont le but premier est différent d'une inscription de données biométriques. Par exemple, les transactions peuvent être des transactions de paiement avec une carte à puce bancaire, des transactions de contrôle d'accès impliquant une carte de transport, un badge d'accès ou une carte de fidélité ou encore des transactions de contrôle d'identité avec un document d'identité.

[0039] L'invention est bien adaptée pour n'importe quel dispositif portable de type bracelet, bague ou porte-clés.

[0040] La [Fig.1] représente un diagramme de flux donné à titre d'exemple pour l'inscription d'une référence biométrique dans un dispositif portable selon un exemple de l'invention.

[0041] Dans cet exemple, le dispositif portable 10 est une carte de paiement intégrant un capteur d'empreinte digitale 14.

[0042] Pendant une première phase d'inscription, le dispositif portable 10 capture une série de données biométriques candidates auprès d'un utilisateur pendant une ou plusieurs transactions avec un ou plusieurs terminaux.

[0043] À ce stade, le dispositif portable ne contient pas encore la référence biométrique.

[0044] Ensuite pendant une deuxième phase survenant après la première phase, le dispositif portable construit la référence biométrique à partir des données biométriques candidates capturées.

[0045] Une fois que le dispositif portable contient la référence biométrique, le dispositif portable peut l'utiliser pour authentifier l'utilisateur par le biais d'une nouvelle capture réalisée par le capteur biométrique et d'un algorithme de concordance. La référence biométrique est parfois appelée schéma biométrique ou un modèle biométrique.

[0046] À une première étape S10, la première phase d'inscription d'une référence biométrique à attribuer à un utilisateur du dispositif portable démarre. Dans certains modes de réalisation, la première phase démarre la première fois que le dispositif portable est impliqué dans une transaction avec un terminal.

[0047] Dans certains modes de réalisation, la première phase démarre dès que l'utilisateur donne son consentement pour inscrire sa référence biométrique dans le dispositif portable.

[0048] À l'étape S11, une transaction démarre entre le dispositif portable 10 et un terminal 20 couplé au dispositif portable. Pendant la transaction en cours (par exemple, active), le capteur 14 capture une nouvelle donnée biométrique candidate à partir d'un identificateur de sujet de l'utilisateur. L'identificateur de sujet peut être un doigt, le visage, un iris ou n'importe quelle source biométrique pertinente.

[0049] Ensuite le dispositif portable attribue un indicateur à la nouvelle donnée biométrique candidate. Le contenu de l'indicateur permet de déterminer (dans une étape future) si l'utilisateur a été authentifié avec succès pendant la transaction en cours. (Étape S12).

[0050] Le dispositif portable stocke à la fois la nouvelle donnée biométrique candidate et son indicateur attribué dans une mémoire non volatile du dispositif portable. (Étape S13)

[0051] Le dispositif portable répète la séquence d'étapes S11 à S13 permettant de stocker une pluralité de données biométriques candidates et leurs indicateurs attribués jusqu'à ce qu'un événement prédéfini survienne.

[0052] Il convient de noter que le dispositif portable peut mettre en œuvre une série de transactions avec un ou plusieurs terminaux.

[0053] Dans certains modes de réalisation, le dispositif portable peut capturer et stocker plus d'une nouvelle donnée biométrique candidate pendant une seule transaction. Dans un tel cas, le dispositif portable peut attribuer l'identificateur à toutes les données biométriques candidates capturées pendant la même transaction ou attribuer autant d'indicateurs individuels.

[0054] À ce stade, la référence biométrique n'est pas encore générée. Par conséquent, le dispositif portable ne peut pas utiliser l'une quelconque donnée biométrique candidate capturée pendant la première phase pour essayer d'authentifier l'utilisateur.

[0055] Une fois que l'événement prédéfini survient à l'étape S14, le dispositif portable entre dans une deuxième phase qui est postérieure à la première phase. La deuxième phase vise à construire la référence biométrique à partir des données biométriques candidates stockées pendant la première phase.

[0056] À l'étape S15, le dispositif portable identifie une liste comprenant les données biométriques candidates stockées dont l'indicateur attribué reflète le fait que l'utilisateur a été authentifié avec succès pendant la transaction conduisant à la capture des données biométriques candidates.

[0057] Le dispositif portable construit la référence biométrique uniquement à l'aide de données biométriques candidates appartenant à la liste. (Étape S16). Le dispositif portable peut construire la référence biométrique en générant une unique donnée récapitulative ou en gardant individuellement toutes les données biométriques candidates sélectionnées qui forment la référence biométrique.

[0058] Le dispositif portable écarte des données biométriques candidates dont l'indicateur attribué reflète le fait que l'utilisateur n'a pas été authentifié avec succès et peut les effacer pour libérer de l'espace dans sa mémoire.

[0059] À ce stade, la référence biométrique existe maintenant dans le dispositif portable et son inscription est achevée. Par conséquent, le dispositif portable peut maintenant utiliser la référence biométrique pour essayer d'authentifier l'utilisateur à l'aide d'une donnée supplémentaire capturée par le capteur 14.

[0060] Dans certains modes de réalisation, chaque indicateur contient une référence de la transaction de la première phase (c'est-à-dire la transaction en cours) pendant laquelle il a été attribué. Par exemple, chaque indicateur peut contenir le Compteur de transaction d'application (ATC) tel que défini par «EMV Integrated Circuit Card Specifications for Payment Systems – Book 3 : Application Specification» (version 4.4 – Octobre 2022).

[0061] Pendant chaque transaction de la première phase (également désignée «transaction en cours»), un serveur distant 30 peut essayer d'authentifier l'utilisateur (grâce à des données récupérées auprès de l'utilisateur et envoyées par le terminal couplé au dispositif portable) et stocker une paire comprenant la référence 31 de la transaction en cours et une balise 32 reflétant si l'utilisateur a été authentifié avec succès pendant la transaction en cours. La référence de la transaction en cours peut contenir le Compteur de transaction d'application (ATC).

[0062] Pendant la deuxième phase, le dispositif portable peut récupérer les paires auprès du serveur distant et identifier la liste de données biométriques candidates en trouvant la correspondance entre des indicateurs stockés dans le dispositif portable et des balises appartenant aux paires récupérées. En d'autres termes, le dispositif portable peut compter sur le serveur distant pour savoir quels échantillons biométriques capturés sont fiables parce qu'ils ont été captés auprès d'un utilisateur authentifié par le serveur distant.

[0063] À titre d'illustration, la [Fig.4] représente un diagramme de flux permettant d'inscrire une référence biométrique dans un dispositif portable en fonction de paires générées par un serveur distant selon un exemple de l'invention.

[0064] La [Fig.4] montre une série de sept transactions qui sont survenues pendant la première phase. La première transaction est un paiement sans contact dans lequel l'utilisateur présente un doigt sur le capteur de carte 14 et dans lequel le PIN (par exemple code secret ou mot de passe) entré par l'utilisateur sur le terminal de paiement 20 est vérifié avec succès par le serveur bancaire 30. À la fin de la transaction numéro 1, le serveur bancaire stocke une première paire comprenant une première référence contenant «0001» (c'est-à-dire la valeurATC) et une première balise (qui pourrait être nommée CHVR) contenant «OK» (ou une valeur correspondant à «utilisateur

authentifié avec succès»). De façon similaire, la carte de paiement stocke un premier ensemble comprenant un premier indicateur contenant «0001» (c'est-à-dire la valeur ATC) et une première donnée biométrique candidate (par exemple une empreinte digitale capturée ou un extrait d'une empreinte digitale capturée).

[0065] La deuxième transaction est un paiement sans contact dans lequel l'utilisateur présente un doigt sur le capteur de carte 14 et dans lequel la vérification du PIN entré par l'utilisateur sur le terminal de paiement 20 échoue au niveau du serveur bancaire 30. À la fin de la transaction numéro 2, le serveur bancaire stocke une deuxième paire comprenant une deuxième référence contenant «0002» (c'est-à-dire la valeurATC) et une deuxième balise contenant «KO». De façon similaire, la carte de paiement stocke un second ensemble comprenant un deuxième indicateur contenant «0002» et une seconde donnée biométrique candidate.

[0066] La troisième transaction est un paiement sans contact dans lequel l'utilisateur ne présente pas un doigt sur le capteur de carte 14 et dans lequel la vérification du PIN entré par l'utilisateur sur le terminal de paiement 20 réussit au niveau du serveur bancaire 30. À la fin de la transaction numéro 3, le serveur bancaire n'enregistre pas de nouvelle paire étant donné qu'aucun doigt n'a été présenté sur le capteur.

[0067] Le serveur bancaire peut savoir si une concordance biométrique a été tentée ou non sur le côté carte, car son résultat peut faire partie de données de transaction envoyées au serveur bancaire. Des données de transaction contiennent habituellement des détails de transaction (montant, date, code devise, résultats de vérification de titulaire de carte, ATC) en même temps qu'une signature (cryptogramme de transaction) en guise de preuve que la carte a participé à la transaction.

[0068] De façon similaire, la carte de paiement n'enregistre pas de nouvel ensemble car le capteur n'a pas capturé une nouvelle donnée biométrique candidate.

[0069] Selon une autre possibilité, à la fin de la transaction numéro 3, le serveur bancaire peut enregistrer une nouvelle paire comme il l'a fait pour des transactions précédentes.

[0070] La quatrième transaction est un paiement sans contact dans lequel l'utilisateur présente un doigt sur le capteur de carte 14 et dans lequel le PIN entré par l'utilisateur sur le terminal de paiement 20 est vérifié avec succès par le serveur bancaire 30. À la fin de la transaction numéro 4, le serveur bancaire stocke une troisième paire comprenant une troisième référence contenant «0004» et une troisième balise contenant «OK».

[0071] De façon similaire, la carte de paiement stocke un troisième ensemble comprenant un troisième indicateur contenant «0004» et une troisième donnée biométrique candidate.

[0072] La cinquième transaction est un paiement sans contact dans lequel l'utilisateur présente un doigt sur le capteur de carte 14 et dans lequel aucun PIN n'a été vérifié par le serveur bancaire 30. À la fin de la transaction numéro 5, le serveur bancaire

stocke une quatrième paire comprenant une quatrième référence contenant «0005» et une quatrième balise contenant une valeur signifiant «PIN non vérifié». De façon similaire, la carte de paiement stocke un quatrième ensemble comprenant un quatrième indicateur contenant «0005» et une quatrième donnée biométrique candidate.

[0073] La sixième transaction est un paiement sans contact qui a avorté. À la fin de la transaction numéro 6, le serveur bancaire n'enregistre pas de nouvelle paire et la carte n'enregistre pas de nouvel ensemble.

[0074] La septième transaction est un paiement sans contact dans lequel l'utilisateur présente un doigt sur le capteur de carte 14 et dans lequel le PIN entré par l'utilisateur sur le terminal de paiement 20 est vérifié avec succès par le serveur bancaire 30. À la fin de la transaction numéro 7, le serveur bancaire stocke une cinquième paire comprenant une cinquième référence contenant «0007» et une cinquième balise contenant «OK». De façon similaire, la carte de paiement stocke un cinquième ensemble comprenant un cinquième indicateur contenant «0007» et une cinquième donnée biométrique candidate.

[0075] Pendant la deuxième phase, la carte récupère les cinq paires existantes stockées dans le serveur bancaire puis compare le contenu des références correspondantes au contenu de ses propres indicateurs pour reconstituer les données provenant d'une même transaction. Par exemple, étant donné que la première référence et le premier indicateur contiennent la même valeur (c'est-à-dire «0001»), la carte déduit que la première balise est jointe à la première donnée biométrique candidate. Étant donné que la première balise contient «OK», la carte déduit que la première donnée biométrique candidate doit être utilisée pour construire la référence biométrique.

[0076] En analysant toutes les paires récupérées, la carte sait que les première, troisième et cinquième données biométriques candidates doivent être utilisées pour générer la référence biométrique (également nommés «modèle complet»). Inversement, la carte sait que les deuxième et quatrième données biométriques candidates doivent être écartées.

[0077] Pour des raisons de simplicité et de clarté, les numérotations de paire et d'ensemble sont synchronisées dans l'exemple montré ci-dessus. Cependant, il peut arriver qu'une divergence existe dans leur numérotation. En d'autres termes, la n-ième paire peut ne pas correspondre au n-ième ensemble.

[0078] Dans certains modes de réalisation, plusieurs données biométriques candidates peuvent correspondre à une même paire si elles ont été capturées pendant une transaction unique.

[0079] Dans certains modes de réalisation, le serveur distant peut détecter la survenue de l'événement prédéterminé en comparant le nombre de paires stockées à un premier seuil. Par exemple, le premier seuil peut être défini sur 5 ou 9. Ensuite le serveur

distant initie l'envoi de ses paires au dispositif portable. Le serveur distant peut être préparé à envoyer les paires pendant la transaction suivante impliquant le dispositif portable.

[0080] De préférence, le serveur distant conserve une trace de l'identité du dispositif portable auquel les paires sont associées de façon unique. Par exemple, le serveur peut allouer un identificateur de dispositif à toutes les paires créées pendant une transaction impliquant le dispositif portable.

[0081] Dans certains modes de réalisation, le serveur distant peut détecter la survenue de l'événement prédéterminé en comparant le nombre de paires stockées ayant une balise contenant « OK » à un seuil prédéfini. Par exemple, le seuil prédéfini peut être défini sur 2 ou 7.

[0082] Dans certains modes de réalisation, l'événement prédéterminé peut être une date, une durée, ou une décision prise par le serveur distant ou par le dispositif portable.

[0083] La [Fig.3] montre un diagramme d'architecture d'un système 90 comprenant un dispositif portable 10, un terminal 20 et un serveur distant 30 selon un exemple de l'invention.

[0084] Dans l' exemple de la [Fig.3], le dispositif portable 10 est une carte de paiement, le terminal 20 est un terminal de point de vente (POS) et le serveur distant 30 est un serveur bancaire.

[0085] La carte de paiement 10 comprend une mémoire non volatile 11, une puce sécurisée 12 et un capteur biométrique 14. La carte de paiement 10 peut établir un canal de communication 71 avec le terminal 20 en mode de contact ou sans contact. Le terminal 20 peut établir un canal de communication 72 avec le serveur distant 30 par le biais d'un ou plusieurs réseaux câblés.

[0086] L'utilisateur de la carte de paiement peut posséder un téléphone 40 hébergeant une application logicielle 41 conçue pour un objectif bancaire. Dans certains modes de réalisation, le téléphone 40 est apparié à la carte à puce 10 pour stocker une valeur secrète ou une clé permettant d'échanger de manière sécurisée des messages ayant un contenu au moins partiellement chiffré/signé.

[0087] Dans certains modes de réalisation, le téléphone 40 peut établir un canal de communication 73 avec le serveur bancaire 30 par l'intermédiaire d'une combinaison de réseau(x) de télécommunication (ou Wi-Fi® ou Bluetooth®) et d'Internet.
Le téléphone 40 peut être apte à communiquer avec la carte de paiement par l'intermédiaire d'un canal de communication NFC© ou Bluetooth basse énergie© (BLE) 74.

[0088] Dans certains modes de réalisation, une fois que le serveur distant a détecté la survenue de l'événement prédéterminé, il peut envoyer un message à l'application logicielle 41 pour avertir l'utilisateur qu'une masse de données est prête à être

téléchargée du serveur bancaire vers la carte de paiement. Le message peut contenir les paires créées par le serveur bancaire pendant la première phase. Ensuite l'application logicielle peut envoyer les paires à la carte de paiement par l'intermédiaire d'un canal NFC©, d'un canal BLE© ou de n'importe quel canal disponible.

[0089] La carte de paiement peut obtenir suffisamment d'énergie du téléphone couplé (par le biais d'une collecte de puissance dans le champ électromagnétique généré) pour achever la deuxième phase.

[0090] Selon une autre possibilité, la carte de paiement peut attendre la connexion suivante à un terminal de paiement ou à un guichet automatique bancaire (ATM) pour achever la deuxième phase en obtenant les paires et en construisant la référence biométrique.

[0091] Dans certains modes de réalisation, le dispositif portable peut être une carte de paiement ayant à la fois des caractéristiques de contact et sans contact (c'est-à-dire une carte combi). Le dispositif portable peut être apte à détecter la survenue de l'événement prédéterminé en comparant le nombre de données biométriques candidates stockées à un second seuil qui peut être défini sur 4 ou 14 par exemple. Ensuite, la carte de paiement peut rejeter volontairement une transaction de paiement sans contact en cours de réalisation avec un terminal couplé pour forcer le terminal couplé à établir une connexion filaire entre le serveur bancaire et la carte de paiement. Ainsi, la carte de paiement peut demander au serveur bancaire d'envoyer ses paires par l'intermédiaire de la connexion filaire.

[0092] Dans certains modes de réalisation, pendant chaque transaction de la première phase, le dispositif portable peut essayer d'authentifier l'utilisateur en vérifiant le PIN entré par l'intermédiaire de l'interface utilisateur du terminal couplé et de stocker dans l'indicateur généré pendant la transaction une valeur reflétant si l'utilisateur a été authentifié avec succès pendant la transaction. Dans un tel cas, le dispositif portable reste indépendant du serveur distant pour l'authentification d'utilisateur.

[0093] De cette façon, le dispositif portable peut détecter la survenue de l'événement prédéterminé en comparant le nombre de données biométriques candidates stockées (ou le nombre d'indicateurs reflétant une authentification d'utilisateur couronnée de succès) à un seuil prédéfini pour démarrer la deuxième phase et en construisant la référence biométrique sans exiger que des données soient téléchargées d'un serveur distant vers le dispositif portable.

[0094] Dans certains modes de réalisation, un premier lot de données biométriques candidates capturées pendant des transactions où un utilisateur est authentifié par le serveur distant et un second lot de données biométriques candidates capturées pendant des transactions où un utilisateur est authentifié par le dispositif portable peuvent être utilisés pour construire la référence biométrique pendant la deuxième phase.

[0095] Dans certains modes de réalisation, le procédé peut comprendre une troisième phase qui est postérieure à la deuxième phase. Pendant la troisième phase, le dispositif portable peut capturer une ou plusieurs données biométriques candidates supplémentaires et les stocker avec des indicateurs associés. Ensuite le dispositif portable peut identifier qu'une nouvelle liste de données biométriques candidates supplémentaires dont l'indicateur attribué indique que l'utilisateur a été authentifié avec succès est identifiée et affiner (par exemple mettre à jour) la référence biométrique 51 existante à l'aide de données biométriques candidates supplémentaires appartenant à la nouvelle liste. Ainsi, le dispositif portable peut améliorer la référence biométrique en tenant compte de données biométriques candidates supplémentaires capturées pendant un processus d'authentification de l'utilisateur par le biais de données capturées par le capteur 14.

[0096] La [Fig.2] montre une architecture donnée à titre d'exemple d'un dispositif portable 10 selon un exemple de l'invention.

[0097] Dans cet exemple, le dispositif portable 10 est une carte à puce de paiement prévue pour être couplée à un terminal de paiement pour mettre en œuvre des transactions de paiement.

[0098] La carte de paiement 10 comprend à la fois une interface de communication physique 15 destinée à communiquer en mode de contact avec des terminaux de paiement et une interface de communication physique 16 destinée à communiquer en mode sans contact avec un appareil sans contact comme un téléphone.

[0099] La carte de paiement 10 comprend un capteur biométrique 14 qui peut être un lecteur d'empreinte digitale.

[0100] La carte de paiement 10 comprend une unité de surveillance matérielle 13 destinée à surveiller le capteur et une puce sécurisée matérielle 12 comportant un système d'exploitation 52. L'unité de surveillance 13 comprend un processeur matériel 61 apte à exécuter un algorithme anti-usurpation 62 pour détecter de fausses données biométriques capturées. L'élément sécurisé 12 comprend un processeur matériel 53 apte à exécuter un algorithme de concordance 54 pour de vérifier si une donnée biométrique capturée est suffisamment proche de la référence biométrique. La puce sécurisée 12 et l'unité de surveillance matérielle 13 sont reliées par un bus et aptes à échanger des données.

[0101] La puce sécurisée 12 est reliée aux deux interfaces de communication 15 et 16 et apte à échanger des données avec l'extérieur.

[0102] Dans certains modes de réalisation, la puce sécurisée 12 et l'unité de surveillance 13 peuvent être fusionnées en un composant matériel unique.

[0103] Le système d'exploitation 52 est configuré pour mettre en œuvre une première phase pendant laquelle une pluralité de transactions entre un ou plusieurs terminaux et le

dispositif portable sont effectuées. Pendant chaque transaction de cette pluralité de transactions, le dispositif portable est configuré pour capturer une donnée biométrique candidate 60 à partir d'un identificateur de sujet de l'utilisateur 50 par le biais du capteur biométrique 14. La donnée biométrique candidate 60 peut être traitée et envoyée à la puce sécurisée 12. Ensuite le système d'exploitation 52 attribue un indicateur 58 à la donnée biométrique candidate capturée. L'indicateur permet de déterminer si l'utilisateur a été authentifié avec succès pendant ladite transaction. Le système d'exploitation 52 stocke la donnée biométrique candidate 60 et son indicateur attribué dans la mémoire non volatile 11 du dispositif portable.

[0104] Le système d'exploitation 52 est configuré pour mettre en œuvre une deuxième phase qui est postérieure à la première phase. Pendant la deuxième phase, lors d'une détection d'un événement prédéterminé, le système d'exploitation 52 est configuré pour identifier une liste de données biométriques candidates (parmi les données biométriques candidates stockées pendant la première phase) dont l'indicateur attribué reflète le fait que l'utilisateur a été authentifié avec succès et pour construire la référence biométrique uniquement à l'aide de données biométriques candidates appartenant à la liste identifiée.

[0105] Dans certains modes de réalisation, chaque indicateur stocké dans le dispositif portable 10 contient une référence de la transaction de la première phase (c'est-à-dire la transaction en cours) pendant laquelle il a été attribué. La référence de la transaction en cours peut être un compteur de transaction ou n'importe quelle valeur permettant d'identifier de manière unique une transaction parmi une série de transactions. Par exemple, la référence de la transaction en cours peut être un horodatage.

[0106] Pendant chaque transaction de la première phase, le serveur distant 30 (voir [Fig.3]) peut être configuré pour essayer d'authentifier l'utilisateur par le biais d'un code PIN tapé par l'utilisateur sur le terminal de transaction 20 et pour stocker une paire comprenant une référence de la transaction en cours et une balise reflétant si l'utilisateur a été authentifié avec succès pendant la transaction en cours.

[0107] Pendant la deuxième phase, le serveur distant peut être configuré pour envoyer les paires qu'il a générées au dispositif portable (par le biais d'un terminal de transaction ou d'un téléphone). Le dispositif portable peut être configuré pour identifier une liste de données biométriques candidates en trouvant la correspondance entre des indicateurs précédemment stockés dans la mémoire du dispositif portable et des balises appartenant aux paires reçues.

[0108] Dans certains modes de réalisation, le serveur distant peut être configuré pour n'envoyer au dispositif portable que des paires ayant une balise reflétant le fait que l'utilisateur a été authentifié avec succès pendant la transaction correspondante.

[0109] Dans certains modes de réalisation, le serveur distant peut être configuré pour détecter l'événement prédéterminé en comparant le nombre de paires stockées à un premier seuil et pour initier l'envoi des paires au dispositif portable.

[0110] Dans certains modes de réalisation, le dispositif portable est configuré pour récupérer les paires auprès du serveur distant par l'intermédiaire d'une application logicielle 41 hébergée sur un téléphone 40.

[0111] Dans certains modes de réalisation, le dispositif portable peut être une carte combi configurée pour détecter l'événement prédéterminé en comparant le nombre de données biométriques candidates stockées à un second seuil. Le dispositif portable peut être configuré pour rejeter volontairement une transaction sans contact en cours de réalisation avec le terminal de transaction couplé pour forcer le terminal couplé à établir une connexion filaire entre le serveur distant et le dispositif portable. De plus, le dispositif portable peut être configuré pour récupérer les paires auprès du serveur distant par l'intermédiaire de la connexion filaire établie.

[0112] Dans certains modes de réalisation, pendant chaque transaction de la première phase, le dispositif portable peut être configuré pour essayer d'authentifier l'utilisateur (en vérifiant un PIN entré sur le terminal couplé 20) et pour stocker dans l'indicateur généré pendant la transaction en cours une valeur reflétant si l'utilisateur a été authentifié avec succès pendant la transaction en cours. Ainsi, le dispositif portable peut stocker tous les éléments permettant la construction de la référence biométrique au niveau de la deuxième phase sans devoir télécharger des paires auprès du serveur distant.

[0113] Grâce à certains modes de réalisation de l'invention, un utilisateur authentique peut profiter de transactions habituelles pour capturer une série de sous-modèles biométriques qui sont utilisés dans une deuxième phase pour construire automatiquement une référence biométrique qui est inscrite dans le dispositif portable.

[0114] L'invention n'est pas limitée aux modes de réalisation ou aux exemples décrits. En particulier, les exemples et modes de réalisation décrits peuvent être combinés.

[0115] L'invention n'est pas limitée à des cartes à puce de paiement et s'applique à n'importe quel dispositif portable comprenant au moins un capteur biométrique.

[0116] Le dispositif portable peut comprendre plusieurs capteurs biométriques de différents types et peut capturer des données biométriques candidates par l'intermédiaire de différents capteurs.

[0117] Bien que des exemples de l'invention aient été principalement fournis dans le domaine bancaire, l'invention s'applique également à d'autres domaines. Par exemple, le dispositif portable peut être un document d'identité ou un appareil d'accès fournissant un accès à une zone virtuelle, à une zone physique comme un bâtiment ou à un réseau de transport.

Revendications

[Revendication 1] Procédé pour l'inscription d'une référence biométrique (51) attribuée à un utilisateur (50) dans un dispositif portable (10) intégrant une mémoire non volatile (11) et un capteur biométrique (14), caractérisé en ce que le procédé comprend une première phase comportant l'étape suivante exécutée pour une pluralité de transactions dont la finalité première est différente d'une inscription biométrique entre un ou plusieurs terminaux (20) et ledit dispositif portable :
- pendant chaque transaction en cours de ladite pluralité de transactions, la capture d'une donnée biométrique candidate (60) à partir d'un identificateur de sujet de l'utilisateur par le capteur biométrique, l'attribution d'un indicateur (58) à la donnée biométrique candidate (60), ledit indicateur permettant de déterminer si l'utilisateur a été authentifié avec succès en utilisant un code secret entré par l'utilisateur pendant ladite transaction en cours et le stockage de la donnée biométrique candidate et dudit indicateur attribué, dans la mémoire non volatile ;
et en ce que le procédé comprend une deuxième phase, postérieure à la première phase, dans laquelle, lors d'une détection d'un événement prédéterminé, le dispositif portable identifie une liste desdites données biométriques candidates dont l'indicateur attribué reflète le fait que l'utilisateur a été authentifié avec succès, et construit la référence biométrique uniquement à l'aide de données biométriques candidates appartenant à ladite liste.

[Revendication 2] Procédé selon la revendication 1, dans lequel chaque indicateur contient une référence de la transaction en cours pendant laquelle il a été attribué,
dans lequel, pendant chaque transaction en cours, un serveur distant (30) essaie d'authentifier l'utilisateur et stocke une paire comprenant la référence (31) de la transaction en cours et une balise (32) reflétant si l'utilisateur a été authentifié avec succès pendant ladite transaction en cours, et
dans lequel, pendant la deuxième phase, le dispositif portable récupère lesdites paires auprès du serveur distant et identifie la liste de données biométriques candidates en trouvant la correspondance

entre des indicateurs stockés et des balises appartenant aux paires récupérées.

[Revendication 3] Procédé selon la revendication 2, dans lequel le serveur distant détecte l'événement prédéterminé en comparant le nombre de paires stockées à un premier seuil et dans lequel le serveur distant initie l'envoi desdites paires au dispositif portable.

[Revendication 4] Procédé selon la revendication 3, dans lequel le dispositif portable récupère lesdites paires auprès du serveur distant par l'intermédiaire d'une application logicielle (41) hébergée sur un téléphone (40), lesdites paires étant acheminées entre le dispositif portable et le téléphone par le biais d'un canal NFC© ou BLE©.

[Revendication 5] Procédé selon la revendication 2, dans lequel le dispositif portable détecte l'événement prédéterminé en comparant le nombre de données biométriques candidates stockées à un second seuil, dans lequel le dispositif portable est une carte combi qui rejette volontairement une transaction sans contact en cours de réalisation avec un terminal couplé pour forcer le terminal couplé à établir une connexion filaire entre le serveur distant et le dispositif portable, et dans lequel le dispositif portable récupère lesdites paires auprès du serveur distant par l'intermédiaire de la connexion filaire.

[Revendication 6] Procédé selon la revendication 1, dans lequel, pendant chaque transaction en cours, le dispositif portable essaie d'authentifier l'utilisateur et stocke dans l'indicateur généré pendant la transaction en cours une valeur reflétant si l'utilisateur a été authentifié avec succès pendant la transaction en cours.

[Revendication 7] Procédé selon la revendication 1, dans lequel le procédé comprend une troisième phase, postérieure à la deuxième phase, dans laquelle, une nouvelle liste de données biométriques candidates supplémentaires dont l'indicateur attribué indique que l'utilisateur a été authentifié avec succès est identifiée et le dispositif portable affine la référence biométrique (51) à l'aide de données biométriques candidates supplémentaires appartenant à la nouvelle liste.

[Revendication 8] Dispositif portable (10) intégrant une mémoire non volatile (11) et un capteur biométrique (14) et apte à inscrire une référence biométrique (51) attribuée à un utilisateur (50),
caractérisé en ce que le dispositif portable est configuré pour mettre en œuvre une première phase comportant l'étape suivante exécutée pour une pluralité de transactions dont la finalité première

est différente d'une inscription biométrique entre un ou plusieurs terminaux (20) et ledit dispositif portable :
- pendant chaque transaction en cours de ladite pluralité de transactions, le dispositif portable est configuré pour capturer une donnée biométrique candidate (60) à partir d'un identificateur de sujet de l'utilisateur par le capteur biométrique, pour attribuer un indicateur (58) à la donnée biométrique candidate (60), ledit indicateur permettant de déterminer si l'utilisateur a été authentifié avec succès en utilisant un code secret entré par l'utilisateur pendant ladite transaction en cours et pour stocker la donnée biométrique candidate et ledit indicateur attribué dans la mémoire non volatile ; et en ce que le dispositif portable est configuré pour mettre en œuvre une deuxième phase, postérieure à la première phase, dans laquelle, lors d'une détection d'un événement prédéterminé, le dispositif portable est configuré pour identifier une liste desdites données biométriques candidates dont l'indicateur attribué reflète le fait que l'utilisateur a été authentifié avec succès, et pour construire la référence biométrique uniquement à l'aide de données biométriques candidates appartenant à ladite liste.

[Revendication 9] Système (90) comprenant un dispositif portable selon la revendication 8, un terminal de transaction et un serveur distant (30), dans lequel chaque indicateur contient une référence de la transaction en cours pendant laquelle il a été attribué,
dans lequel, pendant chaque transaction en cours, le serveur distant (30) est configuré pour essayer d'authentifier l'utilisateur et pour stocker une paire comprenant la référence de la transaction en cours et une balise reflétant si l'utilisateur a été authentifié avec succès pendant ladite transaction en cours, et
dans lequel, pendant la deuxième phase, le dispositif portable est configuré pour récupérer lesdites paires auprès du serveur distant et pour identifier la liste de données biométriques candidates en trouvant la correspondance entre des indicateurs stockés et des balises appartenant aux paires récupérées.

[Revendication 10] Système selon la revendication 9, dans lequel le serveur distant est configuré pour détecter l'événement prédéterminé en comparant le nombre de paires stockées à un premier seuil et dans lequel le serveur distant est configuré pour initier l'envoi desdites paires au dispositif portable.

[Revendication 11] Système selon la revendication 10, dans lequel le dispositif portable est configuré pour récupérer lesdites paires auprès du serveur distant par l'intermédiaire d'une application logicielle (41) hébergée sur un téléphone (40), lesdites paires étant acheminées entre le dispositif portable et le téléphone par le biais d'un canal NFC© ou BLE©.

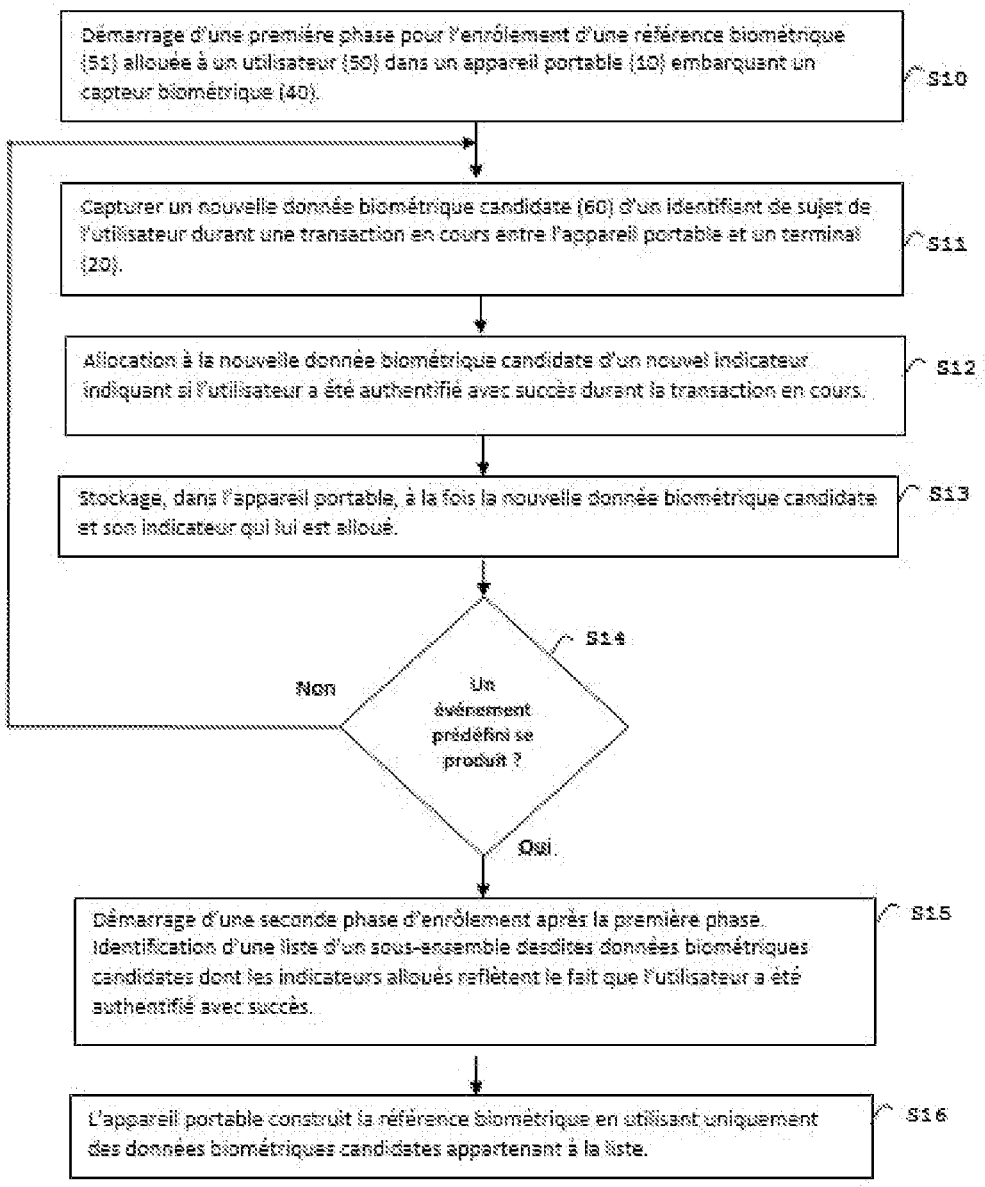
[Revendication 12] Système selon la revendication 9, dans lequel le dispositif portable est configuré pour détecter l'événement prédéterminé en comparant le nombre de données biométriques candidates stockées à un second seuil, dans lequel le dispositif portable est une carte combi configurée pour rejeter volontairement une transaction sans contact en cours de réalisation avec un terminal couplé pour forcer le terminal couplé à établir une connexion filaire entre le serveur distant et le dispositif portable, et dans lequel le dispositif portable est configuré pour récupérer lesdites paires auprès du serveur distant par l'intermédiaire de la connexion filaire.

[Revendication 13] Système selon la revendication 9, dans lequel, pendant chaque transaction en cours, le dispositif portable est configuré pour essayer d'authentifier l'utilisateur et pour stocker dans l'indicateur généré pendant la transaction en cours une valeur reflétant si l'utilisateur a été authentifié avec succès pendant la transaction en cours.

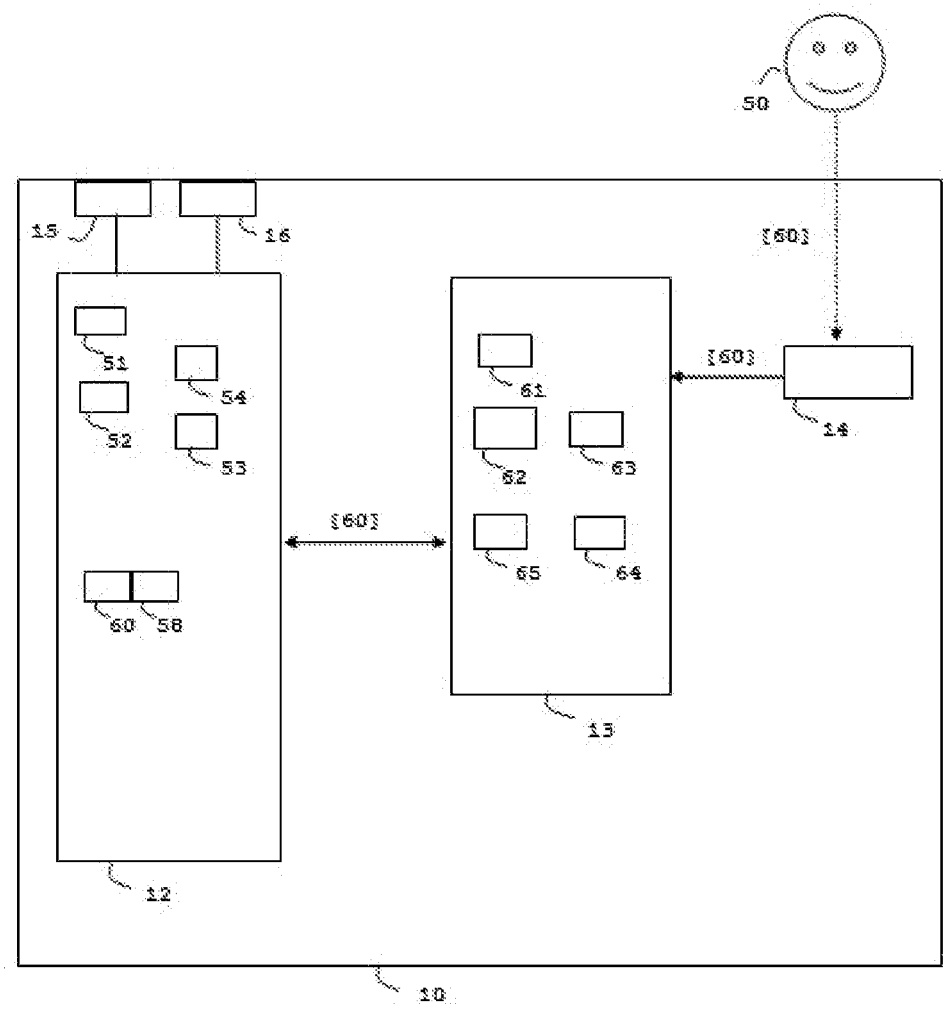
[Revendication 14] Système selon la revendication 9, dans lequel pendant une troisième phase, postérieure à la deuxième phase, le dispositif portable est configuré pour affiner la référence biométrique (51) à l'aide d'une nouvelle liste de données biométriques candidates supplémentaires dont l'indicateur attribué indique que l'utilisateur a été authentifié avec succès.

[Revendication 15] Système selon la revendication 9, dans lequel le dispositif portable est un instrument de paiement, le terminal de transaction est un terminal de paiement et le serveur distant est un serveur bancaire.

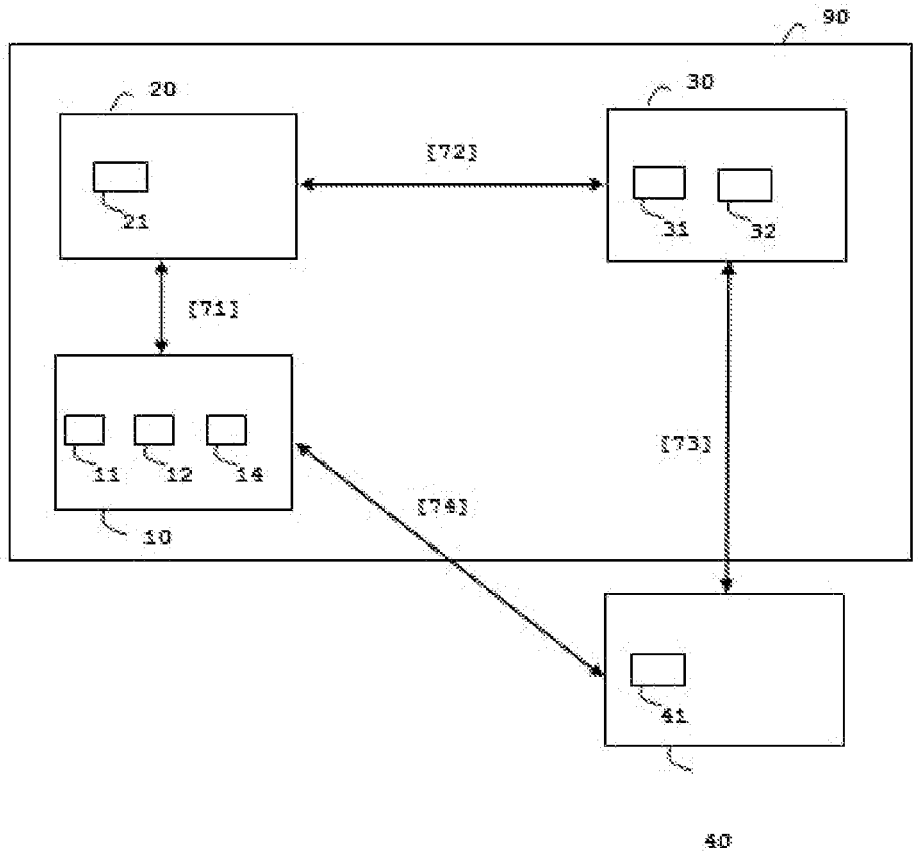
[Fig. 1]


Démarrage d'une première phase pour l'enrôlement d'une référence biométrique (51) allouée à un utilisateur (50) dans un appareil portable (10) embarquant un capteur biométrique (40).
S10
Capturer un nouvelle donnée biométrique candidate (60) d'un identifiant de sujet de l'utilisateur durant une transaction en cours entre l'appareil portable et un terminal (20).
S11
Allocation à la nouvelle donnée biométrique candidate d'un nouvel indicateur indiquant si l'utilisateur a été authentifié avec succès durant la transaction en cours.
S12
Stockage, dans l'appareil portable, à la fois la nouvelle donnée biométrique candidate et son indicateur qui lui est alloué.
S13
S14
Un événement prédéfini se produit ?
Non
Oui
Démarrage d'une seconde phase d'enrôlement après la première phase. Identification d'une liste d'un sous-ensemble desdites données biométriques candidates dont les indicateurs alloués reflètent le fait que l'utilisateur a été authentifié avec succès.
S15
L'appareil portable construit la référence biométrique en utilisant uniquement des données biométriques candidates appartenant à la liste.
S16

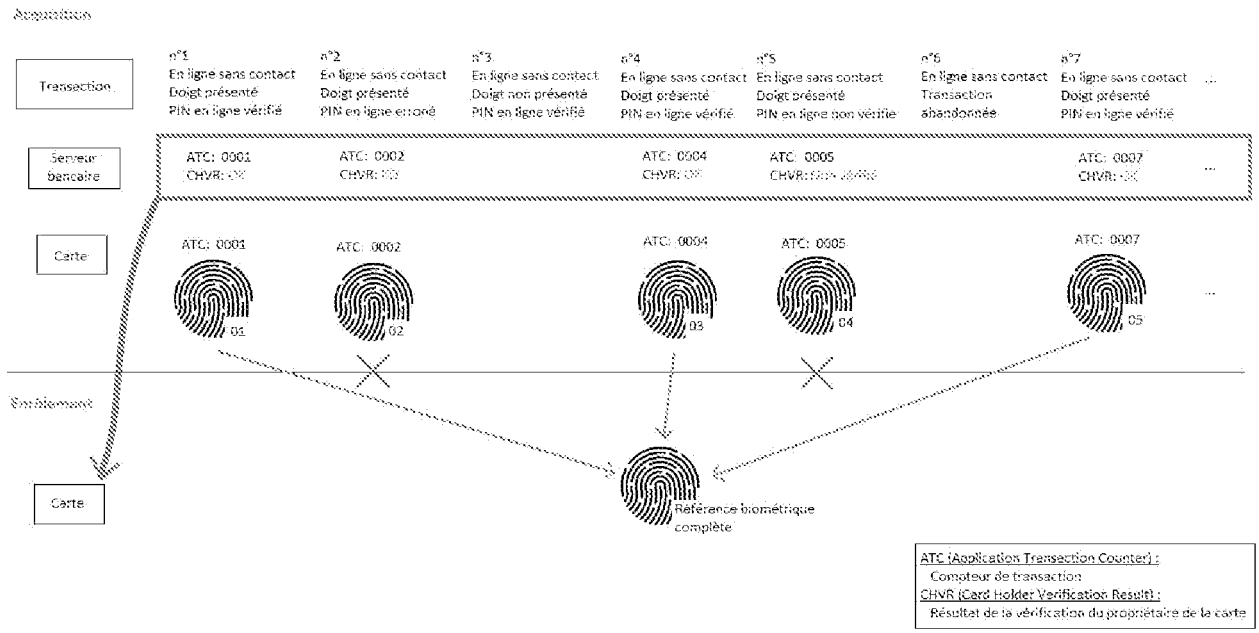
[Fig. 2]



[Fig. 3]


90
20
30
[72]
21
31
32
[71]
[73]
11
12
14
[74]
10
41
40

[Fig. 4]


Acquisition
Transaction
Serveur bancaire
Carte
Environnement
Carte
n°1 En ligne sans contact Doigt présenté PIN en ligne vérifié
n°2 En ligne sans contact Doigt présenté PIN en ligne erroné
n°3 En ligne sans contact Doigt non présenté PIN en ligne vérifié
n°4 En ligne sans contact Doigt présenté PIN en ligne vérifié
n°5 En ligne sans contact Doigt présenté PIN en ligne non vérifié
n°6 En ligne sans contact Transaction abandonnée
n°7 En ligne sans contact Doigt présenté PIN en ligne vérifié
ATC: 0001
ATC: 0002
ATC: 0004
ATC: 0005
ATC: 0007
01
02
03
04
05
Référence biométrique complète
ATC (Application Transaction Counter) :
Compteur de transaction
CHVR (Card Holder Verification Result) :
Résultat de la vérification du propriétaire de la carte