

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2007-524151

(P2007-524151A)

(43) 公表日 平成19年8月23日(2007.8.23)

(51) Int. Cl.	F I	テーマコード (参考)
G07G 1/12 (2006.01)	G07G 1/12 321Z	3E142
G06Q 40/00 (2006.01)	G07G 1/12 321P	5B285
G06Q 20/00 (2006.01)	G06F 17/60 222	5J104
H04L 9/32 (2006.01)	G06F 17/60 414	
G06F 21/20 (2006.01)	H04L 9/00 673D	
審査請求 未請求 予備審査請求 未請求 (全 12 頁) 最終頁に続く		

(21) 出願番号 特願2006-528296 (P2006-528296)
 (86) (22) 出願日 平成16年9月27日 (2004.9.27)
 (85) 翻訳文提出日 平成18年4月25日 (2006.4.25)
 (86) 国際出願番号 PCT/US2004/031691
 (87) 国際公開番号 W02005/031663
 (87) 国際公開日 平成17年4月7日 (2005.4.7)
 (31) 優先権主張番号 60/506,533
 (32) 優先日 平成15年9月26日 (2003.9.26)
 (33) 優先権主張国 米国 (US)

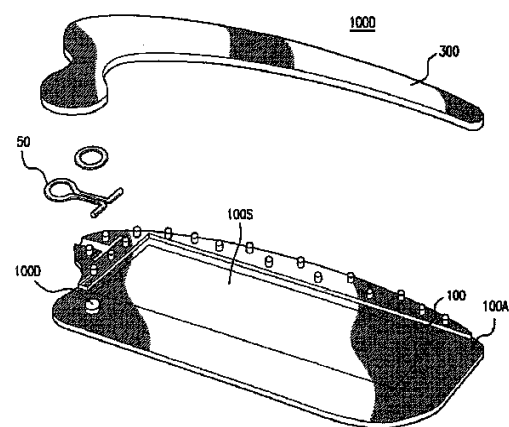
(71) 出願人 500557864
 マスターカード インターナショナル イン
 コーポレーテッド
 アメリカ合衆国 ニューヨーク州 105
 77-2509 パーチェス パーチェス
 ストリート 2000
 (74) 代理人 100072051
 弁理士 杉村 興作
 (74) 代理人 100107227
 弁理士 藤谷 史朗
 (74) 代理人 100114292
 弁理士 来間 清志
 (74) 代理人 100113745
 弁理士 藤原 英治

最終頁に続く

(54) 【発明の名称】 近接装置をバイオメトリクスで有効化する方法およびシステム

(57) 【要約】

POS装置を通る近接決済トランザクションをするための自己で有効であることを検証する決済装置が提供される。決済装置は、POS装置に格納された、または処理された支払人情報の無線通信用電子機器を含む。バイオメトリクスリーダを決済装置に一体化する。実地での決済装置のユーザのバイオメトリクス測定情報は、決済装置が当該ユーザに対応するバイオメトリクス測定情報を登録してある基準と内部で比較される。決済装置は、比較の結果によって、使用のためにそれ自体を自分で有効化する。



【特許請求の範囲】

【請求項 1】

P O S 装置を通じて試行される近接決済トランザクションでの支払いカードの使用を有効にするために支払人が本人であることを検証する方法であって、

実地での近接決済の使用のため登録された支払人に、電子的に結合されたバイオメトリクスリーダと、前記支払いカードとを組み合わせたものを提供するステップであって、前記組み合わせたものは共通の筐体内に物理的に配置され、前記組み合わせたものが前記登録された支払人に対応する基準バイオメトリクスパラメータを含むステップと、

実地で支払人のバイオメトリクスパラメータを測定するためにバイオメトリクスリーダを使用するステップと、

前記測定されたバイオメトリクスパラメータを、前記登録された支払人に対応する基準バイオメトリクスパラメータと比較し、この比較の結果が肯定的なものである場合には、前記近接決済トランザクションのための支払いカードの使用を有効にするステップと、を含む方法。

10

【請求項 2】

請求項 1 に記載の方法において、

前記測定されたバイオメトリクスパラメータを、前記登録された支払人に対応する基準バイオメトリクスパラメータと比較した後、この比較の結果が否定的なものである場合には、前記近接トランザクションのための前記支払いカードの使用が無効にされる、ことを特徴とする方法。

20

【請求項 3】

請求項 2 に記載の方法において、

前記比較の結果が、前記近接決済トランザクションが試行される P O S 装置に無線で伝えられる、ことを特徴とする方法。

【請求項 4】

請求項 1 に記載の方法において、

前記バイオメトリクスリーダおよび前記支払いカードが、無線通信をしている2つの別の電子ユニットを含み、

前記方法が、さらに、

前記測定されたバイオメトリクスパラメータを暗号化するステップと、

前記基準バイオメトリクスパラメータと比較するため、前記暗号化されたバイオメトリクスパラメータを、前記バイオメトリクスリーダの電子ユニットから前記支払いカードの電子ユニットへ伝えるステップとを含む、ことを特徴とする方法。

30

【請求項 5】

請求項 1 に記載の方法において、

前記バイオメトリクスリーダの提供が、指紋リーダを提供することを含む、ことを特徴とする方法。

【請求項 6】

請求項 1 に記載の方法において、

前記バイオメトリクスリーダの提供が、声紋リーダを提供することを含む、ことを特徴とする方法。

40

【請求項 7】

請求項 1 に記載の方法において、

前記バイオメトリクスリーダと、前記支払いカードとを組み合わせたものを提供するステップが、この組み合わせ自体に電力を供給するドライセルバッテリーを提供することを含む、

ことを特徴とする方法。

【請求項 8】

50

請求項 7 に記載の方法において、

前記支払いカードが、前記近接決済トランザクションのため P O S 装置と無線通信するための無線周波数トランシーバを含み、前記無線周波数トランシーバのデフォルト状態が、オフ状態である、
ことを特徴とする方法。

【請求項 9】

請求項 8 に記載の方法において、

前記支払いカードが有効にされた後のみ、前記近接決済トランザクションで使用するため前記無線周波数トランシーバがオンにされる、
ことを特徴とする方法。

10

【請求項 10】

請求項 8 に記載の方法において、

前記支払いカードが無効にされた後、前記比較の否定的な結果を P O S 装置に伝えるために、前記無線周波数トランシーバがオンにされる、
ことを特徴とする方法。

【請求項 11】

P O S 装置を通じて近接決済トランザクションをするための決済装置であって、

前記決済装置が、

P O S 装置と無線で支払人情報をやりとりするために電子機器を持っている支払いカードと、

20

前記決済装置のユーザーのバイオメトリクスパラメータの測定のため、および、前記支払いカードの電子機器と通信するため電子機器を持つバイオメトリクスリーダであって、前記支払いカードおよびバイオメトリクスリーダが共通の筐体に共に配置されるようなバイオメトリクスリーダと、
を含む決済装置。

【請求項 12】

請求項 11 に記載の決済装置において、

前記バイオメトリクスリーダが、前記支払いカードに物理的に装着され、

前記支払いカードの電子機器および前記バイオメトリクスリーダの電子機器が、相互に無線或いは有線の通信をしている別個の電子ユニットである、
ことを特徴とする決済装置。

30

【請求項 13】

請求項 11 に記載の決済装置において、

前記バイオメトリクスリーダの電子機器が、前記支払いカードに埋め込まれている、
ことを特徴とする決済装置。

【請求項 14】

請求項 13 に記載の決済装置において、

前記支払いカードの電子機器および前記バイオメトリクスリーダの電子機器が、共に配線で接続されている、
ことを特徴とする決済装置。

40

【請求項 15】

請求項 11 に記載の決済装置において、

前記バイオメトリクスリーダが、指紋リーダである、
ことを特徴とする決済装置。

【請求項 16】

請求項 11 に記載の決済装置において、

前記バイオメトリクスリーダが、声紋リーダである、
ことを特徴とする決済装置。

【請求項 17】

請求項 11 に記載の決済装置において、

50

前記決済装置に登録されている支払人に対応する基準バイオメトリクスパラメータ、をさらに含むことを特徴とする決済装置。

【請求項 18】

請求項 17 に記載の決済装置において、

測定されたバイオメトリクスパラメータを前期基準バイオメトリクスパラメータと比較し、これに応じて前記決済装置の使用を自己で有効にするように、或いは、無効にするように前記支払いカードおよび前記バイオメトリクスリーダの電子機器が構成されている、ことを特徴とする決済装置。

【請求項 19】

請求項 17 に記載の決済装置において、

前記支払いカードの電子機器が、前記 P O S 装置に前記比較の結果を伝えるように構成されている、ことを特徴とする決済装置。

【請求項 20】

請求項 1 に記載の決済装置において、

前記決済装置が電源内蔵のものであり、

前記決済装置が、前記 P O S 装置との無線通信が切られているようなデフォルト状態を持つ、ことを特徴とする決済装置。

【請求項 21】

請求項 20 に記載の決済装置において、

前記決済装置の使用を自己で有効にした後のみ、前記 P O S 装置との無線通信を再開するように、前記決済装置の電気機器が構成されている、ことを特徴とする決済装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、商取引、即ち商業トランザクションにおける支払いをするため、支払いカードやその他の決済装置を使う購買者を識別する、即ち、本人であることを識別するための方法および装置に関する。

【背景技術】

【0002】

本発明は、特に、いわゆる「近接決済」トランザクションに関与する支払人の同一性のバイオメトリクス（生体測定）の検証に関するものである。

関連出願への相互参照

本出願は、2003年9月26日に出願した米国仮特許出願60/506,533号の優先権の利益を要求する。

【0003】

購入者が存在する状況であって、ベンダー/受取人との物理的な接触を必要とせずに、支払をすることができるということが有用である、或いは、少なくともより便利であるという状況において近接決済（接近決済）が使用される。購入者は、例えば、手動でカードを従来の P O S 装置（即ち、磁気ストリップカードリーダ）に通す必要なしに、近接決済をする、無接触の「スマート・カード」を使用することができる。典型的な無接触スマート・カードは、マスターカード PayPass (TM) カードである。このカードは、隠して埋め込まれたマイクロプロセッサ・チップおよびアンテナ（即ち、小型の無線周波数(RF)トランシーバ・チップおよびアンテナ、或いは能動型の無線周波数識別(RFID)タグ）を特色とする機能向上した支払いカードである。マスターカード PayPass は、購入者により簡便な支払い方法を提供する。購入者は、特別な装備をした商人端末上で、彼または彼女のマスターカード PayPass 支払いカードを単に軽くタップするか、振ることができ、その端末は、その後、リーダを通してカードを読取り機に通す必要を除去して、無線で無線周波数

10

20

30

40

50

信号を使用して支払明細を送信することができる。アカウント（即ち口座）の詳細は、特別な装備を施した商人端末へ直接伝えられ、次に、マスターカードの高度な信頼性を持つ受理ネットワークを通して処理される。購入者は、彼または彼女のマスターカードPayPassカードで前記端末を軽くタップした後、彼または彼女は、支払い確認（即ち決済承認）を受け取り、すぐに帰れる。

【0004】

スマート・カード（マスターカードのPayPassなどのような）に基づいた近接決済手段は、速さが不可欠の従来の現金のみの環境（例えば、迅速なサービスでカジュアルなレストラン、ガソリン・スタンド、および、映画館）で有利に実施することができる。スマート・カード上のマイクロチップに格納され得る購入者情報は、マイクロチップからPOSシステムのPOS（販売時点管理）装置、或いは、他の無線リーダ・デバイス（読み取り装置）へ直接送られるが、これら読取装置は、最大約10cmまで離すことができる。接近決済は、必要なときに、処理された、或いは、格納されたアカウント（口座）情報を格納したり、再送信したりするマイクロチップを持つように適切に構成されている、他の決済装置（例えば、携帯電話、PDA或いはハンドヘルド・コンピュータ）を使用して実施することもできる。共通の産業上の赤外線或いは無線のプロトコル（例えば、Bluetooth）は、決済装置とベンダー/受取人無線リーダ（或いはPOS装置）との間の通信を規定することができる。

10

【0005】

インターネットおよび他の電子商取引の取引上で行なわれる電子支払いトランザクションと同様に、近接決済トランザクションの両方の当事者はセキュリティ上の問題を持つであろう。支払人は、ベンダー/受取人が支払人情報を悪用する無法な犯罪者でないことの再保証、即ち、安心感を必要とし、ベンダー/受取人は、支払人が正当であることを知る必要がある、双方の当事者は、無許可の第3の当事者がトランザクション情報を傍受（インターセプト）するができないことを知る必要がある。これらのセキュリティ上の問題のうちのいくつかを少なくとも解決する多数の技法が利用可能である。例えば、データ暗号化技術を使用して、送信の間のトランザクション情報を安全にすることができる。従来の近接決済のスキーム（枠組み）では、遠隔（リモート）のバイオメトリクスリーダを使用することができる。バイオメトリクスリーダから、或いはそこへの個人データの無線の伝送も関連する。この無線による送信は、無許可の第3の当事者によるインターセプト或いは漏洩の機会を与えることになる。

20

30

【発明の開示】

【発明が解決しようとする課題】

【0006】

本発明は、例えば、盗んだ支払いカード、或いは、紛失した支払いカードの詐欺的使用を防止するために、支払人の身元（本人であること、即ち本人性）の検証のためのスキームの改善を目的とする。特に、近接決済トランザクションに関与する支払人の同一性の迅速で安全なバイオメトリクス（生体測定情報）の検証（認証）を目的とすることに注意されたい。

【課題を解決するための手段】

40

【0007】

<発明の要約>

本発明によれば、近接決済トランザクションに関与する支払人のバイオメトリクス（生体測定情報）の識別のためのシステムおよび方法が提供される。

【0008】

POSシステムのPOS装置を通して近接決済トランザクションをするため、自己で有効にする、即ち、自ら認証を行う決済装置が提供される。この決済装置は、データを格納し処理するため、および、POS装置と無線通信を行うための従来の電子回路を含むものである。電子バイオメトリクスリーダは、決済装置に物理的に統合、即ち、一体化されている。バイオメトリクスリーダは、例えば、指紋リーダ或いは声紋リーダとすることがで

50

きる。バイオメトリクスリーダは、近接決済をすることを試みている人のバイオメトリクス（生体測定情報）を獲得、即ち、読み取るために使用される。獲得したバイオメトリクス測定情報は、電子的に内部で処理される、即ち、決済装置のなかで処理され、試みる人が、許可された者、即ち、決済装置の登録されたユーザであるかどうかを確認する。この目的のために、獲得したバイオメトリクス測定情報は、許可された、即ち、登録されたユーザについての格納されたバイオメトリクス測定情報のレコードと比較することができる。したがって、決済装置は、内部比較の結果によって試行する人による使用のために決済装置自体を自己で有効にすることができる。

【0009】

近接決済トランザクションを行う好適な方法では、個々人に設定された決済装置がユーザに発行される。決済装置は、その中に通常の利用者アカウント（口座）情報を記録することによって、および、許可された個人の生物測定（バイオメトリクス）のプロフィールかテンプレートをその中にさらに記録することによって個人用に設定される。実地の使用では、決済装置に一体化されたバイオメトリクスリーダを使用して、近接決済をするために決済装置を使用することを試みている人のバイオメトリクス測定情報を得る。これらの実地でのバイオメトリクス測定情報が、許可された当該個人の以前に記録されているバイオメトリクスプロフィールと内部で比較される。この比較の肯定的な結果に基づいて、決済装置が、接近トランザクションをすることを試みる人による使用のために有効にすることができる。反対に、否定的な結果の場合は、決済装置の使用を無効にすることができる。

10

20

【0010】

好適には、決済装置の電子機器回路は、例えば、ドライセルバッテリーなどを装備することによって自己で電力（動力）を供給する。そのような決済装置は、電子回路のような従来の受動型RFIDタグと異なり、回路の活動化、即ち、機能させるために外部のRFパワー信号を受け取る必要はない。ユーザ識別のプロセスは、外部デバイス（例えば、RFIDタグリーダ、POS装置、或いは、その他の無線ネットワークアクセスポイント）との相互作用、即ち、通信をすることがないような決済装置レベルで隔絶した状態で局所的に達成することができる。この隔絶は、決済装置が外部デバイスと継続的に無線通信をしている場合に発生し得るアカウント情報の「電子的なスリ」の危険を低減する。

【0011】

本発明のさらなる特徴、その性質、および、様々な利点は、添付図面および以降の詳細な説明によってさらに明らかになるであろう。

30

【発明を実施するための最良の形態】

【0012】

<発明の詳細な記述>

本発明は、本発明の進歩性のある原理が近接決済トランザクションで使用されるかもしれない他のタイプの決済器具或いは装置に適用可能であるという理解のもと、支払いカードを使用して為される近接決済トランザクションの文脈で説明する。近接決済をする支払人の迅速で安全なバイオメトリクス識別のためのシステムおよび方法を開示する。

【0013】

本発明によれば、バイオメトリクスリーダが、支払人に発行された、或いは支払人によって登録された支払い（決済）カードと共に提供される。バイオメトリクスリーダを使用して、選択対象（例えば、指紋或いは声紋テンプレート）のバイオメトリクスパラメータ識別パラメータの実地で測定したものと、支払いカードに格納されている登録された識別パラメータを比較することによって、支払人が本人であること（本人性または同一性）を検証する。バイオメトリクスリーダは、選ばれた識別パラメータによって、指紋リーダ或いは声紋リーダとすることができる。バイオメトリクスリーダは、簡便な幾何学的構成で支払いカードに物理的に装着される。

40

【0014】

図1-3に、バイオメトリクスリーダが支払いカード200に物理的に装着されているよ

50

うな例示の幾何学的構成(例えば、共通の筐体1000)のコンポーネント(構成要素)を示す。支払いカード200(例えば、マスターカードPayPassカード)は、POS装置(図示せず)に支払人アカウント情報を伝える(通信する)ためのアンテナ、マイクロプロセッサまたはRFIDチップなどの通常の電子機器構成を持つことができる。

【0015】

筐体1000においては、バイオメトリクスリーダが、プラスチックベース、即ち、カバー100Aに埋め込まれている。バイオメトリクスリーダは、例えば、表面のキャパシタンス測定に依存して指紋を記録する、電子指紋測定装置100とすることができる。指紋測定装置100は、測定面100Sを伴うプラスチックベース、或いは、カバー100Aに埋め込むことができる。指紋リーダ100は、ベース100Aに配置されるような、さらに適切な測定/処理の電子機器(例えば、マイクロプロセッサまたはASICチップ)、および、無線通信のための電子機器(例えば、RFトランシーバ)を含むことができる。ベース100Aに埋め込んだドライセルバッテリー(図示せず)によって電力(動力)を電子機器に供給することができる。或いは、RFIDタグリーダによって一般に用いられている受動型RFIDタグに電力を供給するのと同じ方法で、POS装置によって生成された適切な無線周波数信号によって電力を例えば電磁誘導で電子機器に供給することもできる。指ガイド(テンプレート)300が、プラスチックスリーブ100Aに装着される。支払いカード200を自由に収容できるようなスリーブを形成するように、指ガイド300は、ベース100A上の適切な高さで配置することができる。筐体1000は、キーホルダーまたはチェーンで支払いカード/スリーブ構成を持ち運ぶのに支払人が便利のように、小穴50、悪い歯、他の機械的な特徴をさらに含むことができる。

10

20

【0016】

筐体1000においては、それ(カード)がスリーブの中で、およびそのスリーブから自由に回転する、或いはスライドすることができるように、支払いカード200は、従来の機械構成(例えば、ピン(即ちダボ)100D)を使ってスリーブに物理的に装着される。支払いカード200がスリーブから外側に回転する場合、測定面100Sが露出され、その面が指紋測定に利用可能になる。支払いカード200および指紋リーダ100の物理的な接近(近接)は、2つのコンポーネント中の電子回路のRFカップリング(RF-coupling)には有利である。電子回路のRFカップリング(結合)は、電子回路および安全な通信プロトコルの適切な設計によって、2つのコンポーネント間の直接のデータ伝送のために使うことができる。

30

【0017】

筐体1000の一部の設計では、支払いカード200の電子回路は、物理的な装着点(例えば、伝導性ピン(或いはダボ)100dの使用によって)を通り抜ける、導電性のワイヤー(要素)によって、指紋リーダ100の電子機器に電氣的に接続することができる。このような筐体1000の設計では、支払いカード・チップはデュアル(2つの)インターフェイスを持つ。1つは、指紋リーダ機能のための接触(有線)インターフェイスであり、もう1つは、近接決済機能のための非接触インターフェイスである。適切なデータ通信プロトコルが、データ・セキュリティを保証する2つのインターフェイス間の通信のために実装することができる。

【0018】

さらに、そのような設計においては、処理電子機器(例えば、従来の支払いカードで使用するマイクロプロセッサ、或いはRFIDチップ)のうちの一部、或いは全てを、支払いカード200から移動することが好適であり、指紋リーダ100用の電子機器にそれを統合することができる場合には、移動したものをベース100aに配置することができる。したがって、ベース100aの単一のマイクロプロセッサ(即ちチップ)は、近接決済カードおよび指紋リーダの両方の機能をサポートするために使用することもできる。再び、安全な通信プロトコルを、指紋リーダ機能インターフェイスと近接決済機能インターフェイスの間のデータ通信のために実装することができる。

40

【0019】

筐体1000のあるバージョンでは、支払いカード200が、POS装置とのRF通信用の近接

50

アンテナだけを保持するために作製される。他の電子機器の全ては、近接決済機能をサポートする必要があり、指紋リーダ機能はベース100Aに配置される。さらに、この配置は、ベース100A(例えば、長さ、幅、或いは厚さ)の寸法が、産業標準(例えば、支払いカードの寸法のための国際標準機構(ISO)の標準)に準拠する必要があるような支払いカードの寸法と同じようには制約されないため、筐体1000の幾何学的(形状的)設計に柔軟性を与え得る。

【0020】

他の例示の幾何学的配置では、バイオメトリクスリーダ(例えば、指紋リーダ100、或いは声紋リーダ)は、決済装置(例えば、キーフォブ(即ちキーホルダー))に固定状態で組み込むことができる。そのような幾何学的配置では、指紋リーダの電子機器410および支払いカードの電子機器420は、共に一体化する、或いはハードワイヤード、即ち配線で接続し、共通の電源を共用することが好適である。図4、例えば、ビルトイン、即ち、内臓の指紋リーダ500を持つ支払いカード400を示す。この幾何学的配置の利点は、バイオメトリクスリーダと接近チップの間に通信するための直接の物理的なリンクを確立することである。本構成中で設けたバイオメトリクスリーダは、銀行業界(例えば、マスターカードまたはビザによって発行された支払いカードのような国際標準機構(ISO)の寸法に準拠する支払いカード)で使用される従来の支払いカードの標準化された寸法に物理的なサイズを制限さない。支払いカード400は、従来の近接支払いカード(例えば、マスターカードPayPassカード)と同じ方法でプラスチックシート材料から作製することができる。支払いカード400を作製するために使用されるプラスチックシート材料の厚さは、利用可能な指紋リーダ電子機器を完全に埋め込めるように適切に設計することができる。カードの表の面、或いは、裏面の指定の部分は、指紋測定表面として機能するように構成することができる。

【0021】

図1を再び参照するが、指紋リーダ100は、当該分野で既知の指紋分析で確立している方法のうちのいずれか1つを使用して、指紋テンプレートを抽出するように構成させることができる。指紋リーダ100は、送信されるデータをエンコードするための何らかの適切なデータ暗号化アルゴリズムを使用して、支払いカード200(即ち、支払いカード中のマイクロプロセッサ、或いはRFIDチップ)への安全な通信チャンネルを確立するように構成させることができる。設けられるデータ暗号化アルゴリズムは、例えば、政府および銀行業界でデータ暗号化に広く使用される、対称トリプルデータ暗号規格(DES)アルゴリズムとすることができる。指紋リーダ100は、カード200に安全を確保されたセキュア通信チャンネルを通してそれを送信する前に、抽出された指紋テンプレートを暗号化するように構成させることもできる。これに応じて、支払いカード200中のマイクロプロセッサかRFIDチップは、受信指紋テンプレートを復号し、かつ復号された指紋をそのメモリに格納された基準(参照)指紋テンプレートと比較するように構成させることができる。基準指紋テンプレートは、認可された支払人が支払いカード200を登録する時に記録された指紋テンプレートとすることができる。

【0022】

近接決済トランザクションを行う好適な方法では、支払人の識別(本人であること)のバイオメトリクスの検証は、近接決済カード(例えばカード200または400)に埋め込まれたバイオメトリクスリーダを使用して迅速に得ることができる。例えば、支払いカード200を使用したい支払人は、彼または彼女の本人性(身元)を確認する認証プロセスに、最初に従うことを要求することができる。この認証については、そのスリーブから外側に支払いカード200をはじめにスライドして指紋測定面100Sを露出するように支払人に指示することができる。その後、支払人に対して、測定面100S上に、測定する指紋に彼または彼女の人差し指か親指を置くように指示することができる。これに応じて、指紋リーダ100は、指紋分析およびデータ暗号化の装備されている方法を使用して、指紋テンプレートを抽出し暗号化する。指紋リーダ100は、支払いカード200中のマイクロプロセッサ或いはRFIDチップに暗号化された指板テンプレートが送信されるような、支払いカード200への安全

な通信チャンネルを、次に或いは同時に、確立することができる。支払いカード200は、受信した指紋テンプレートを復号し、この復号された指紋テンプレートをそのメモリに格納された基準テンプレートと電子的に比較する。この比較の結果に応じて、支払いカード200は、支払人が登録された支払人であることを確認すること、或いは、支払人が無許可のユーザであることを決めることができる。従って、支払いカード200は、接近トランザクションで使用するために自己を有効化したり、或いは、無効にしたりすることができる。支払人が無許可のユーザである場合には、支払いカード200は、例えば、所望であれば無許可の支払人の身柄を拘束することができるように、POS装置を通じて店員に即座に警告を発することもできる。

【0023】

バイオメトリクスリーダおよび電子の支払いカードの物理的な近接によって、個人のバイオメトリクスデータの空中での伝送を回避するような、2つの間の短距離通信リンクが与えられる。したがって、遠隔のバイオメトリクスリーダからの従来のデータ伝送では存在していたような、個人のバイオメトリクスデータのインターセプト（傍受）の危険が低減される。さらに、バイオメトリクスリーダおよび支払いカード電子回路の親密な構成は、支払人（即ち、登録されたカード所有者）認証をサポートする何らかの機能や特徴を提供するための、受取人/買い手のPOS装置におけるどんな必要性も除去する。

【0024】

さらに、自己で動力を供給する（例えば、埋め込まれたドライセルバッテリーを利用する）ような、支払いカード/バイオメトリクスカードリーダの組み合わせは、支払いカードのコンポーネント中に受動型RFIDタグ状の電子回路を設けることが好適である。従来の受動型RFIDタグ回路と異なり、これらの受動型RFIDタグ状の電子回路は、回路の操作或いは活動化させるため支払いカードに誘導で動力（電力）を供給するRFID無線ビーコン信号を生成するPOS装置を必要としない。したがって、支払いカードは、無線状態を通常はオフ、即ち、「常時オフ」にしておき、局所的な認証処理によって支払人が有効化（承認）されたときだけオンにさせるようにすることができる、支払いカードの「常時オフ」の無線状態は、近接決済RFIDチップが範囲内にある全てのRFIDリーダ、或いは、POS装置に電子的に結合されるような従来の近接決済スキームで存在する、支払い口座（アカウント）データの電子的なスリの可能性を低減させる。

【0025】

本発明を具体的な例示の態様で説明してきたが、本発明の原理に従って、開示した実施態様に対して当業者によって様々な変更、置換、変更を行うことができるもの理解すべきである。例えば、本発明の原理は、2つのアイテム間の物理的な通信チャンネルを作成するために2つのどんな異なるコンポーネント（それらは異なる形およびサイズでもよい）も物理的に装着するために適用することができる。物理的な通信チャンネルを、コンポーネントのうちの1つに配置された近接RFIDチップ中で認証プロセスをサポートするために使用してもよい。本発明を使って、多様なバイオメトリクスリーダのタイプ、および、技法（例えば、指紋または声紋のテンプレート）を、POS装置およびカードリーダの多種多様な設置・設備を使用して近接決済スキームで展開することもできる。支払人認証プロセスが決済装置/バイオメトリクスリーダの組み合わせに局地化されるので、POS装置およびカードリーダの多種多様な設備における共通、或いはグローバルなバイオメトリクスリーダ標準の義務は必要ない。

【図面の簡単な説明】

【0026】

【図1】本発明の原理による支払いカードに物理的に装着されている、バイオメトリクスリーダの典型的なアセンブリ（組み立て品）のコンポーネントを示す図である。

【図2】本発明の原理による支払いカードに物理的に装着されている、バイオメトリクスリーダの典型的なアセンブリ（組み立て品）のコンポーネントを示す図である。

【図3】本発明の原理による支払いカードに物理的に装着されている、バイオメトリクスリーダの典型的なアセンブリ（組み立て品）のコンポーネントを示す図である。

10

20

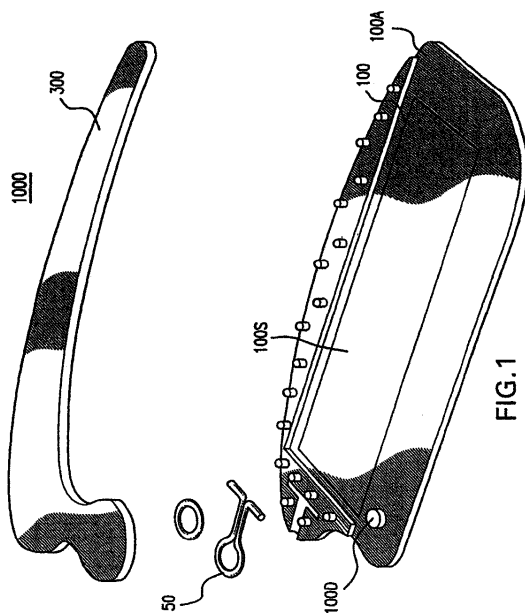
30

40

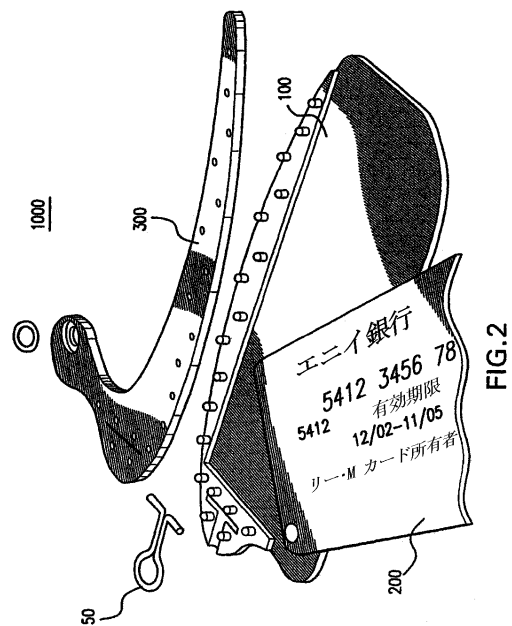
50

【図 4】 本発明の原理による近接決済カードに埋め込まれているバイオメトリクスリーダーを示す図である。

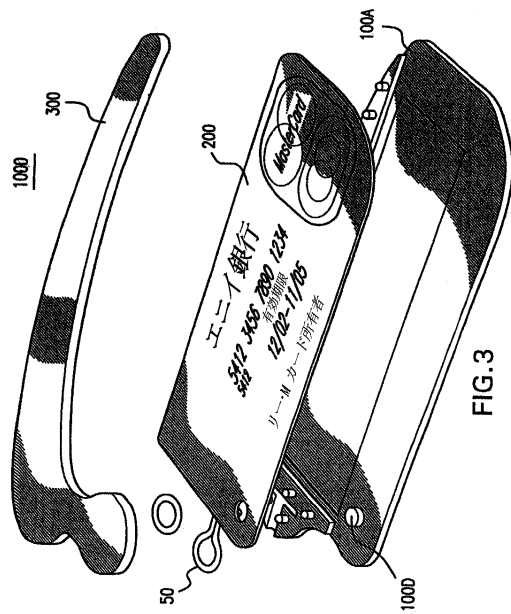
【図 1】



【図 2】



【図 3】



【図 4】

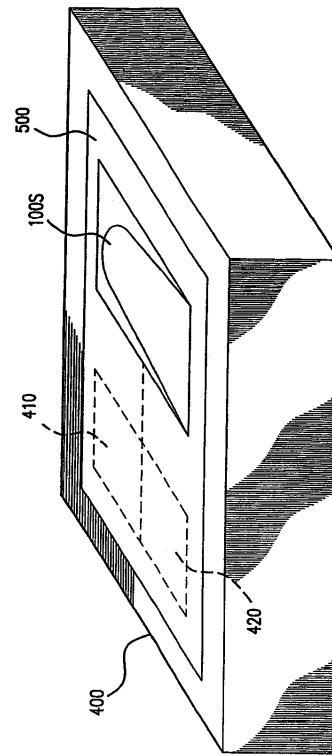


FIG. 4

フロントページの続き

(51)Int.Cl.	F I	テーマコード (参考)
	G 0 6 F 15/00	3 3 0 F
	G 0 6 F 15/00	3 3 0 G

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(特許庁注：以下のものは登録商標)

1. Bluetooth

(72)発明者 ジョン ヴァンクミューラー

アメリカ合衆国 ニューヨーク州 1 1 0 2 0 グレイト ネット タナーズ ロード 3 5

Fターム(参考) 3E142 FA02 FA28 GA07 GA36

5B285 CA02 CA41 CB08 CB15 CB23 CB64 CB75 DA10

5J104 AA07 KA01 KA04 KA16 NA05 NA27 NA38 PA15