(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4922288号
(P4922288)

(45)発行日　平成24年4月25日(2012.4.25)　(24)登録日　平成24年2月10日(2012.2.10)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	21/20	132
G06K 17/00	(2006.01)	G06K	17/00	T
H04L 9/32	(2006.01)	H04L	9/00	673E
		H04L	9/00	673D

請求項の数 10　(全 11 頁)

(21)出願番号	特願2008-503250 (P2008-503250)
(86)(22)出願日	平成18年3月24日 (2006.3.24)
(65)公表番号	特表2008-535061 (P2008-535061A)
(43)公表日	平成20年8月28日 (2008.8.28)
(86)国際出願番号	PCT/US2006/010910
(87)国際公開番号	WO2006/102625
(87)国際公開日	平成18年9月28日 (2006.9.28)
審査請求日	平成21年2月25日 (2009.2.25)
(31)優先権主張番号	60/665,043
(32)優先日	平成17年3月24日 (2005.3.24)
(33)優先権主張国	米国(US)

(73)特許権者　507419965
プリバリス，インコーポレイテッド
アメリカ合衆国　バージニア州　２２９１１　シャーロッツビル　ピーター　ジェファーソン　パークウェイ　６５０　スイート　３３０
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100093861
弁理士　大賀　眞司
(74)代理人　100109346
弁理士　大貫　敏史

最終頁に続く

(54)【発明の名称】スマートカード機能を備えた生体認証デバイス

(57)【特許請求の範囲】

【請求項１】

電子ユーザ証明を識別および認証する自律的な可搬型装置であって、

生体認証入力を受信するよう構成された生体認証センサと、

開口部を備えた物理的筐体であって、前記開口部を通してスマートカードを収容するよう構成された物理的筐体と、

前記物理的筐体に接続されるスマートカード・リーダであって、スマートカードが前記開口部を通して前記物理的筐体に収容された際に、前記スマートカード・リーダはスマートカードに接続され；前記スマートカードが前記スマートカード・リーダに接続された際に、前記スマートカードに対して情報を読み書きするよう構成される、スマートカード・リーダと、

前記物理的筐体の内部に配置されるプロセッサであって、前記プロセッサは前記生体認証センサと前記スマートカード・リーダに動作可能に接続され；前記プロセッサは、前記スマートカードが前記スマートカード・リーダに接続される前に、前記プロセッサのメモリ内に格納された生体認証テンプレートに基づいて、前記生体認証入力を認証するように構成され；前記生体認証入力が認証された後、識別番号が前記スマートカードによって認証されるよう、前記プロセッサは、前記スマートカード・リーダを介して前記スマートカードに前記認証番号を送るように構成される、プロセッサと、

を含む装置。

【請求項２】

前記物理的筐体が不正行為検出可能又は不正行為防止可能である、請求項１に記載の装置。

【請求項３】

スマートカードが前記開口部に挿入された際に、前記スマートカードの外面が視認できるよう前記物理的筐体の前記開口部が向けられている、請求項１に記載の装置。

【請求項４】

前記スマートカード・リーダと前記プロセッサとの間の通信を確実にして不正行為を防止すべく、前記スマートカード・リーダ及び前記プロセッサの少なくとも一部が特定用途向け集積回路に実装されている、請求項１に記載の装置。

【請求項５】

前記スマートカード・リーダ及び前記プロセッサが、シリアル通信を用いて通信するように構成されている、請求項１に記載の装置。

【請求項６】

前記スマートカード・リーダ及び前記プロセッサが、ユニバーサル・シリアルバスを用いて通信するように構成されている、請求項１に記載の装置。

【請求項７】

電子ユーザ証明を識別および認証する自律的な可搬型装置にユーザを関連付ける方法であって、

前記装置のプロセッサにおいて、スマートカードが前記装置の開口部の内部に配置される際に、スマートカードに割り当てられたシリアル番号を受信するステップであって、前記装置はスマートカード・リーダと前記装置のユーザから生体認証入力を取得するよう構成される生体認証センサとを備え；前記プロセッサは、前記装置の内部に配置され、前記生体認証センサと前記スマートカード・リーダに接続され；前記スマートカードが前記装置の開口部の内部に配置された際に、前記スマートカード・リーダはスマートカードに接続され；前記スマートカードが前記スマートカード・リーダに接続された際に、前記スマートカード・リーダは、前記スマートカードに対して情報を読み書きするよう構成される、ステップと、

前記装置の前記プロセッサにおいて、前記受信されたシリアル番号が前記装置に登録されていないとき、前記装置の前記ユーザから前記生体認証入力を受信するステップであって、前記生体認証入力が受信されたとき、前記装置が外部登録ステーションに接続する、ステップと、

前記受信した生体認証入力を、生体認証テンプレートとして、前記プロセッサのメモリに格納するステップであって、前記生体認証テンプレートは、前記スマートカードの前記シリアル番号に関連付けられる、ステップと、

前記シリアル番号が前記装置に登録された後、前記生体認証テンプレートが前記プロセッサの前記メモリと前記スマートカードのメモリに格納されるよう、前記生体認証テンプレートを前記スマートカードへ送信するステップと、

を含む方法。

【請求項８】

電子ユーザ証明を識別および認証する自律的な可搬型装置を使用して、デバイスに対してユーザを認証する方法であって、

前記装置のプロセッサにおいて、前記装置の前記ユーザから前記生体認証入力を受信するステップであって、前記装置はスマートカード・リーダを備え；前記装置は前記生体認証入力を取得するよう構成される生体認証センサを備え；前記プロセッサは、前記装置の内部に配置され、前記生体認証センサと前記スマートカード・リーダに接続され；前記スマートカードが前記装置の開口部の内部に配置された際に、前記スマートカード・リーダはスマートカードに接続され；前記スマートカードが前記スマートカード・リーダに接続された際に、前記スマートカード・リーダは、前記スマートカードに対して情報を読み書きするよう構成される、ステップと、

前記装置のユーザから個人認証番号を受信するステップと、

前記受信した生体認証入力を、前記スマートカードが前記スマートカード・リーダに接続される前に前記プロセッサに保存された生体認証テンプレートと比較するステップと、
前記受信した生体認証入力が、前記保存されている生体認証テンプレートに合致した場合、前記ユーザを認証するステップと、
前記認証後、前記受信した個人認証番号が前記スマートカードによって認証されるよう、前記受信した個人認証番号を前記プロセッサから前記スマートカードに送信するステップと、
を含む方法。
【請求項９】
前記スマートカードから生体認証テンプレートを受信するステップと、
保存された生体認証テンプレートに基づいて、前記受信した生体認証テンプレートを認証するステップと、
をさらに含む、請求項８に記載の方法。
【請求項１０】
前記比較ステップが、前記プロセッサで実行される、請求項８に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
関連米国出願データ
本出願は、合衆国法典第３５巻第１１９条（ｅ）に基づき、２００５年3月２４日出願の米国仮特許出願第６０／６６５，０４３号「スマートカード機能を備えた生体認証デバイス」を優先権主張するものであり、その全体が参照により本明細書に組み入れられるものとする。
【０００２】
発明の背景
発明の分野
本発明は、可搬型の電子個人識別・認証デバイスの分野に関する。本発明は、より具体的には、生体および／またはスマートカード認証技術を用いる電子装置に関する。
【背景技術】
【０００３】
関連技術
ズイリ（Ｚｕｉｌｉ）による米国特許第６，９９１，１７４号は、出荷処理を認証する方法および装置を開示している。開示された装置は本特許の特許請求の範囲ではないが、多くの異なる認証メカニズムを組み込んだ可搬型スマートカード・リーダであって、個人識別番号（ＰＩＮ）、非対称暗号鍵および／または生体認証技術を含んでいる。本装置は独立して、あるいは携帯情報端末（ＰＤＡ）、携帯電話、または遠隔制御等、他の電子装置と合わせて用いることができる。本装置は、コンピュータ・ネットワーク、テレビやケーブル・アクセス、および支払い処理を含む各種の用途に設計されている。特許登録された発明は特に、スマートカードおよびスマートカード・リーダを用いる出荷処理の認証、顧客からの生体認証情報および出荷情報の取得、並びに本生体認証情報を用いる出荷情報の暗号化、暗号化された出荷情報のスマートカードおよびデータベースへの保存、出荷情報を変更すべく顧客によるデータベースへのアクセス許可、並びに出荷処理を認証すべく顧客に対する生体認証情報の再提出要求を行なう方法である。
【０００４】
メイズ（Ｍａｅｓ）他による米国特許第６，０１６，４７６号は、生体認証を備えた可搬型ＰＤＡを開示している。本ＰＤＡは更に、スマートカード、磁気ストライプ・カード、光カードおよび／または電子的に変更可能な読出し専用メモリ（ＥＡＲＯＭ）カードと間で情報の読み書きが可能である。本ＰＤＡは、支払い処理での使用を意図されていて、有線か無線トランシーバのいずれかを介してＰＯＳ端末等、他の電子装置と通信することができる。

【０００５】
リサーチインモーション社（Ｒｅｓｅａｒｃｈ　Ｉｎ　Ｍｏｔｉｏｎ，Ｌｔｄ．）（ＲＩＭ）は、「ブラックベリー（ＢｌａｃｋＢｅｒｒｙ（登録商標））スマートカード・リーダ」と呼ばれる装置を製造および販売しており、これはブラックベリー装置へのアクセスまたは使用を試みているユーザに２要素認証、対称暗号鍵およびスマートカードを提供する可搬型スマートカード・リーダである。スマートカードと暗号鍵が装置で処理されたならば、本装置はブルートゥース（Ｂｌｕｅｔｏｏｔｈ）無線技術を介してブラックベリー装置と通信して、ユーザが安全な電子メールを送信できるようにする。本装置は生体認証を含んでいない。
【０００６】
キーオベイション（Ｋｅｙ　Ｏｖａｔｉｏｎ）社は「ゴールドタッチ（Ｇｏｌｄｔｏｕｃｈ）エルゴセキュア（ＥｒｇｏＳｅｃｕｒｅ）スマートカードおよび生体認証キーボードＳＦ２．４」を製造している。本装置は標準型人間工学的コンピュータ・キーボードであり、スマートカード・リーダとオーセンテック（Ａｕｔｈｅｎｔｅｃ）社製の指紋センサの両方を組み込んでいる。これは可搬型ではなく、且つ無線技術を備えているようには見えない。
【発明の開示】
【発明が解決しようとする課題】
【０００７】
発明の必要性
企業、政府その他の組織は、各種の物理的およびデジタル・リソースを保有しており、これらは貴重で保護が必要な場合が多い。これらのリソースのいくつかは、特定の建物、事務所または土地のように物理的である一方、他のものはデータベース、コンピュータ・ファイルその他のデジタルデータのように無形である。リソースを保護したいという当然の帰結として、リソースへのアクセスに対する規則を指定すべく関連付けられたセキュリティ・ポリシーまたは構造を組織は暗黙的または明示的に開発する。個人が被保護リソースへのアクセスを望む場合、組織のセキュリティ・ポリシーは、再び暗黙的または明示的に、本個人に対し受理可能な仕方で身分証明することを求め、次いで身分証明された個人をセキュリティ・ポリシーに対して認証する。身分証明および認証された個人がリソースに対する特権が有している場合、当人によるアクセスが許可される。
【０００８】
政府機関および民間業界は共に、これらのセキュリティ・ポリシーを実装すべく多くの異なる技術を開発してきた。このような技術に一つに、商業ビルおよび事務所への物理的アクセスを確実に行うべく一般的に用いられる「近接型カード」がある。近接型カードは通常、クレジットカードの大きさであって、一意な識別子の保存およびアクセス・ポイントに設置された受信器への無線送信を行なうのに充分な電子機器を含んでいる。近接型カードは、その無線送信の特徴的種類から自身の名称を取得することにより、ユーザは、カードをリーダに挿入しなくても単にカードをアクセス・ポイントの近く（通常は数インチ以内に）かざすだけで済む。近接型カードを個人に支給する際に、中央データベースが、本個人に本カードの一意な識別子を関連付け、当人がリソースにアクセスすべく近接型カードを提示した場合、識別子がアクセス・ポイントへ送信されて関連付けが検証される。一意な識別子が近接型カード上へ一度プログラムされたならば、変更不可能であり、且つ追加的なデータをカードに加えることもできない。
【０００９】
開発者は一様に、コンピュータ、ネットワークその他のデジタル・リソースへアクセスするための多くの認証技術を開発してきた。最も簡単な例として、個人がリソースへのアクセスを許可される前に提示する必要があるパスフレーズまたは個人識別番号（ＰＩＮ）がある。実質的に、全ての電子メール・システムはこの方式で保護されている。別の一般的な例としてＷｉｎｄｏｗｓ（登録商標）ログイン・プロセスがあり、ユーザ名およびパスワードをユーザに入力させる。より高度なシステムでは、個人に公開鍵／秘密鍵の対の

片方のような暗号鍵、またはデジタル証明を提供することができる。これらの技術は一様に、パスフレーズや暗号鍵等の特定の証明と個人との以前の関連付けに基づいている。

【００１０】

物理的およびデジタル的アクセスの一方または両方の目的を達成すべく多用される一つ技術が「スマートカード」である。近接型カードと同様に、スマートカードはクレジットカードの形状を有している。しかし、スマートカードは一般に、暗号および双方向送信を含む多くの異なるタスクを実行するのに充分な処理能力を有する小型の集積回路を含んでいる。スマートカードは、暗号鍵、パスフレーズその他のユーザ・データ等の一意な識別子を保存できると共に、物理的リソースへアクセスすべく搬送および使用することができる。１枚のスマートカードで、各々が異なる識別子を有する多くの異なるリソースを保存および認証することができる。スマートカードは、近接型カード等の証明を無線で送信するのではなく、接触型送信を使用し、スマートカードをアクセス・ポイントに設置されたリーダに挿入するようユーザに求める。スマートカード・リーダはコンピュータやネットワーク端末等の電子リソース、またはドアやゲート等の物理的リソースに取り付けられていてよい。双方向送信機能により、スマートカードに保存されたデータはスマートカード・リーダを介して変更または更新可能である。スマートカードは、非常に普及しており、例えば、国防総省（ＤｏＤ）は現在、スマートカードを利用した共通アクセスカード（ＣＡＣ）を用いて自身の組織およびリソースへのアクセスを許可している。ＣＡＣは、従来のスマートカードの機能および特徴の全てを保持していて、視覚的且つ電子的識別および認証を可能にすべく、カードの外側に所有者の写真を組み込んでいる。

【００１１】

これらのセキュリティ技術は、極めて有用であるが、詐称者により利用されやすい。個人が自分の近接型カードまたはスマートカードを紛失した場合、それを拾った人物は誰でもそれを使ってリソースにアクセスすることができる。指紋等の身体的特徴を用いて個人を認証する生体認証技術によりこのリスクを大幅に減らすことができる。指紋認識の場合、個人の指紋が電子的にスキャナ入力され、数値テンプレートとして保存される。個人がリソースにアクセスしたい場合、指を再スキャンし、保存されている指紋とデジタル的に比較して合致するか否かを判定する。生体認証は、従来技術に対して明確な優位性を提供する。すなわち、スマートカードは盗難に遭いやすく無未許可の個人に使われる恐れがあるが、指紋の電子偽造の実現ははるかに困難である。

【００１２】

Ｐｒｉｖａｒｉｓ（登録商標）ＢＰＩＤ（商標）セキュリティ・デバイスは、生体認証技術に基づく認証デバイスの一種であり、スマートカードよりはるかに新しい技術である。ＢＰＩＤセキュリティ・デバイスは手持ちの可搬型電子装置であり、指紋スキャナ、双方向無線通信、メモリ、および暗号機能およびオンデバイス指紋認証アルゴリズムを実行するため充分な処理能力を含んでいる。スマートカードと同様に、ＢＰＩＤセキュリティ・デバイスは、暗号鍵およびパスフレーズを含む一意な識別子を保存することができ、多くの異なるリソースに対し個人を認証するために用いることができる。しかし、ＢＰＩＤセキュリティ・デバイスは、従来のスマートカードより高い処理能力およびメモリを有しているが、その理由の一つは指紋テンプレートの記憶および比較が装置オンボードで行なわれるためである。更に、ＢＰＩＤセキュリティ・デバイスは無線技術に基づいているため、近接型カードで用いられているものと同一プロトコル、Ｂｌｕｅｔｏｏｔｈ（登録商標）プロトコル等のより新しい標準、あるいはその両方を使用することができる。ＢＰＩＤセキュリティ・デバイスに関するデータは、デバイスをリーダに挿入しなくても送信または受信することができるため、スマートカードを使用するよりも、物理的アクセス・ポイントにおける個人認証がより高速に行なえる。

【００１３】

スマートカードの出現以来、多くの組織で、スマートカードに含まれる共通情報を利用しながら、同時に本情報のセキュリティを高めて、承認されたリソースへのアクセスを許可する前に、スマートカードを用いて個人の身分証明を保証する、複数の組織に共通の識

別システムの開発を試みてきた。メモリの不足、非接触用途の限定された範囲、既存の建物アクセスシステムに対応すべく多数のカードが必要な点、信頼性が高い生体認証が必要な点、およびカードのデータ更新に付随する困難さ等が全て問題になった。ＢＰＩＤセキュリティ・デバイスはこれらの懸念を大幅に解消できるものの、スマートカードの形状をなしておらず、従ってＣＡＣの視覚的識別要素に適していない。また、ＢＰＩＤセキュリティ・デバイスは、現在スマートカード・リーダを使用しているシステムと対話できる接触型の送信機構を含んでいない。必要とされているのは、視覚的識別が可能なスマートカードの特徴と、ＢＰＩＤセキュリティ・デバイスの生体認証および無線機能を組み合わせることにより、必要に応じて接触型スマートカードシステムへの転換が可能な装置および方法である。

【課題を解決するための手段】

【００１４】

発明の概要

本発明は、スマートカードとＢＰＩＤセキュリティ・デバイス技術を一体化する装置および方法を開示する。以下で「スマートカード対応ＢＰＩＤセキュリティ・デバイス」と称する本発明の主要装置は、スマートカード・リーダをＢＰＩＤセキュリティ・デバイスと一体化することにより個人がスマートカードをＢＰＩＤセキュリティ・デバイスの物理的筐体の開口部に挿入して、スマートカードとＢＰＩＤセキュリティ・デバイスが互いに電子的に通信できるようにする。本発明の一つの主要な実施形態において、スマートカード対応ＢＰＩＤセキュリティ・デバイスは、ＢＰＩＤセキュリティ・デバイスが挿入されたスマートカードと直接通信することができるようにスマートカード端子を組み込んだカスタム特定用途向け集積回路（ＡＳＩＣ）に基づいている。本発明の別の実施形態において、スマートカード対応ＢＰＩＤセキュリティ・デバイスは、民生（ＣＯＴＳ）マイクロプロセッサに基づいており、シリアル、ＵＳＢ、または他の種類の通信プロトコルを用いてＣＯＴＳスマートカード受信器と通信することができる。本発明の第１の方法は、スマートカード対応ＢＰＩＤセキュリティ・デバイスへ、ユーザ証明を登録する方法である。本発明の第２の方法は、スマートカード対応ＢＰＩＤセキュリティ・デバイスを用いて個人を認証する方法である。

【発明を実施するための最良の形態】

【００１５】

発明の詳細な説明

以下の詳細記述は、本発明を実施するための現在考え得る最良のモードである。以下の記述は、本発明を限定することを意図しておらず、あくまでも本発明の実施形態の一般的原理を例示すべくなされたものである。

【００１６】

本発明の主要な装置を「スマートカード対応ＢＰＩＤセキュリティ・デバイス」と称する。図１に示すように、ＢＰＩＤスマートカード・セキュリティ・デバイス１００は、ストラップ１１０に取り付け可能であるため、個人の首周りに装着したり、または他の何らかの便利な携帯方法で使用することができる。ＢＰＩＤスマートカード・セキュリティ・デバイス１００は、スマートカードを収容する開口部１０２を有する物理的筐体１０１、生体認証コンポーネント３００（図４参照）、およびスマートカード・リーダ２１０（図４参照）を含んでいる。ＢＰＩＤセキュリティ・デバイスの指紋センサ３１０は、物理的筐体１０１を介して外部から使用可能となっている。図２、３に示すように、開口部１０２は、ＣＡＣ等スマートカード２００の外側にある画像または写真が、物理的筐体１０１内で、個人に接近している全員に容易に見えるように向けられている。

【００１７】

図４は、物理的筐体および開口部を省いた状態でのスマートカード対応ＢＰＩＤセキュリティ・デバイスの模式的表現である。スマートカード・リーダ２１０は、電子データスマートカードを受送信する接触型端子２１１（以下「スマートカード端子」という）および外部デバイスにデータを送受信する少なくとも１つの追加的な端子２１２（以下「外部

デバイス端子」という）を組み込む任意の既存技術でもあってよい。生体認証コンポーネント３００およびスマートカード・リーダ２１０は、物理的筐体１０１内に配置されているため、開口部１０２に挿入されたスマートカード２００はスマートカード端子２１１と物理的に接触して、既存のスマートカードプロトコルを用いてスマートカード・リーダ２１０との間で情報を転送することができる。スマートカード・リーダ２１０は、生体認証コンポーネント３００と物理的に連結されているため、外部デバイス端子２１２によりスマートカード・リーダ２１０は生体認証コンポーネント３００と通信することができる。

【００１８】

本装置の第１実施形態において、生体認証コンポーネント３００は、ＲＳ２３２（現在はＥＩＡ２３２として知られる）またはユニバーサル・シリアルバス（ＵＳＢ）等の、しかしこれに限定されない標準通信プロトコルを介して、外部デバイス端子２１２と通信することができる。本装置の代替的な実施形態において、生体認証コンポーネント３００およびスマートカード・リーダ２１０は、セキュリティ保証されたマイクロプロセッサ（以下「ＢＰＩＤセキュリティ・デバイス／リーダ）に共存することにより、外部デバイス端子２１２と生体認証コンポーネント３００との間の通信は物理的且つ電子的に同一ＡＳＩＣに置かれる。本発明のこの実施形態において、ＢＰＩＤセキュリティ・デバイス／リーダは物理的筐体１０１内に配置されることにより、物理的筐体１０１の開口部１０２に挿入されたスマートカード２００はＢＰＩＤセキュリティ・デバイス／リーダのスマートカード端子２１１と直接接触する。これによりＡＳＩＣが物理的且つ電子的に保護されため、ＢＰＩＤスマートカード・セキュリティ・デバイス１００のセキュリティが向上する。

【００１９】

本発明の第１の方法により、スマートカードを携帯する個人がＢＰＩＤスマートカード・セキュリティ・デバイス１００に自身を登録することができる。最初に、個人がスマートカード２００を物理的筐体１０１の開口部１０２に挿入して、スマートカード２００をリーダ２１０のスマートカード端子２１１に接触させる。個人は次いで、スマートカード対応ＢＰＩＤセキュリティ・デバイス１０１への電源投入を行ない、スマートカード・リーダ２１０がスマートカードのシリアル番号を読む。スマートカード・リーダ２１０は、外部デバイス端子２１２を用いて、シリアル番号を生体認証コンポーネント３００へ送信する。生体認証コンポーネント３００は、これが特定のスマートカード２００に既に登録されていない旨を検証する。生体認証コンポーネント３００は次いで、ＢＰＩＤセキュリティ・デバイス登録ステーションに接続して、正規の手順に従って個人を登録する。登録手順の間、生体認証コンポーネント３００は個人の生体データおよびＰＩＮを保存し、これらは次いで生体認証コンポーネント３００メモリ内でスマートカード２００のシリアル番号に関連付けられる。生体認証コンポーネント３００はまた、外部デバイス端子２１２を介して個人の生体データおよびＰＩＮをスマートカード・リーダ２１０へ送信し、スマートカード・リーダ２１０は、スマートカード端子２１１を介して生体データおよびＰＩＮをスマートカード２００に書き込む。この時点でＢＰＩＤスマートカード・セキュリティ・デバイス１００が登録されており、ユーザは物理的筐体１０１の開口部１０２から、スマートカードを取り出すことができる。

【００２０】

本発明の第２の方法は、個人が、以前に登録したＢＰＩＤスマートカード・セキュリティ・デバイス１００に、自身を認証できるようにさせる。最初に、個人が物理的筐体１０１の開口部１０２にスマートカード２００を挿入して、スマートカード２００をリーダ２１０のスマートカード端子２１１を接触させる。個人は次いで、スマートカード対応ＢＰＩＤセキュリティ・デバイス１０１への電源投入を行ない、スマートカード・リーダ２１０はスマートカードのシリアル番号を読む。スマートカード・リーダ２１０は、外部デバイス端子２１２を用いてシリアル番号を生体認証コンポーネント３００へ送信する。生体認証コンポーネント３００は、これが特定のスマートカード２００により既に登録されていることを検証し、個人に対し標準的な手順に従って生体認証コンポーネント３００に自身を認証させることを要求する。生体認証コンポーネント３００が首尾よく個人を認証し

たならば、生体認証コンポーネント３００はスマートカードの２００シリアル番号に関連付けられたＰＩＮを特定して、外部デバイス２１２を介してＰＩＮをスマートカード・リーダ２１０へ送信する。スマートカード・リーダ２１０は次いで、スマートカード端子２１１を介してＰＩＮをスマートカード２００へ送信する。

【００２１】

スマートカード２００が「カード上マッチング」機能、すなわち、スマートカードが指紋テンプレートをカードに保存されているものをマッチングする機能を備えている場合、生体認証コンポーネント３００は、スマートカードの２００シリアル番号に関連付けられている指紋テンプレートを特定して、外部デバイス２１２を介してテンプレートをスマートカード・リーダ２１０へ送信する。スマートカード・リーダ２１０は次いで、スマートカード端子２１１を介してテンプレートをスマートカード２００へ送信する。スマートカード２００が、送信されたＰＩＮおよび指紋テンプレートの両方を、自身に保存されているＰＩＮおよびテンプレートとマッチングさせる場合、自身に保存されている電子データをスマートカード端子２１１を介してスマートカード・リーダ２１０へ送信し、続いてスマートカード・リーダ２１０は保存されている電子データを外部デバイス端子２１２を介して生体認証コンポーネント３００へ送信する。生体認証コンポーネント３００はこの時点で、必要に応じてスマートカード２００に保存されている電子データを使用することができる。

【００２２】

スマートカード２００が「カード上マッチング」機能を備えていない場合、スマートカード２００は送信されたＰＩＮだけを保存されている自身のＰＩＮとマッチングさせる。スマートカード２００は次いで、保存されている指紋テンプレートをスマートカード端子２１１を介してスマートカード・リーダ２１０へ送信し、次いでスマートカード・リーダ２１０は外部デバイス端子２１２を介して指紋テンプレートを生体認証コンポーネント３００へ送信する。生体認証コンポーネント３００は、スマートカード２００のシリアル番号に関連付けられた指紋テンプレートを特定して、保存されているテンプレートをスマートカード２００から送信されたテンプレートと比較する。両者が合致した場合、生体認証コンポーネント３００は、スマートカード・リーダ２１０に対し、保存されている自身の電子データをスマートカード端子２１１を介してスマートカード・リーダ２１０へ送信するようプロンプトを発する。スマートカード・リーダ２１０は次いで、保存されている電子データを外部デバイス端子２１２を介して生体認証コンポーネント３００へ送信する。上述のように、生体認証コンポーネント３００はこの時点で、必要に応じてスマートカード２００に保存されている電子データを使用することができる。

【００２３】

当業者には、ステップの厳密な順序を変更しても結果的に同一機能が得られることが理解されるであろう。当業者には明らかであるように、本明細書に記載し、添付の請求項に規定する本発明の趣旨および範囲から逸脱することなく、各種の改良、変更、および追加が可能である。

【図面の簡単な説明】

【００２４】

【図１】スマートカード対応ＢＰＩＤセキュリティ・デバイスを示す。

【図２】スマートカード対応ＢＰＩＤセキュリティ・デバイスに挿入されつつあるスマートカードを示す。

【図３】スマートカード対応ＢＰＩＤセキュリティ・デバイスに挿入されたスマートカードを示す。

【図４】スマートカード対応ＢＰＩＤセキュリティ・デバイスの模式的表現である。

【符号の説明】

【００２５】

１００　ＢＰＩＤスマートカード・セキュリティ・デバイス

１０１　物理的筐体

１０２　スマートカードを収容する開口部
１１０　ストラップ
２００　スマートカード
２１０　スマートカード・リーダ
２１１　スマートカード端子
２１２　外部デバイス端子
３００　生体認証コンポーネント
３１０　ＢＰＩＤセキュリティ・デバイスの指紋センサ

【図１】

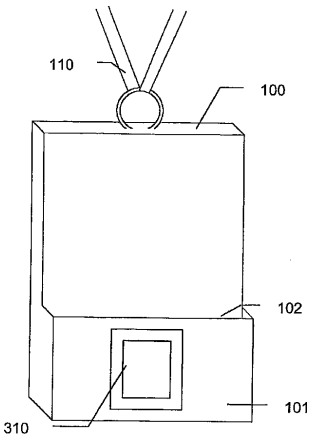

FIG. 1

【図２】

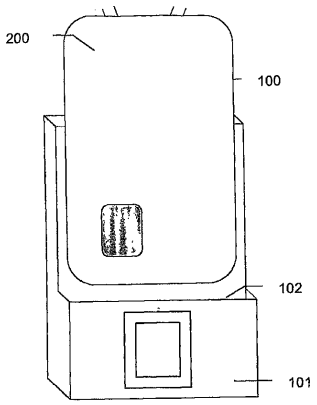

FIG. 2

【図３】

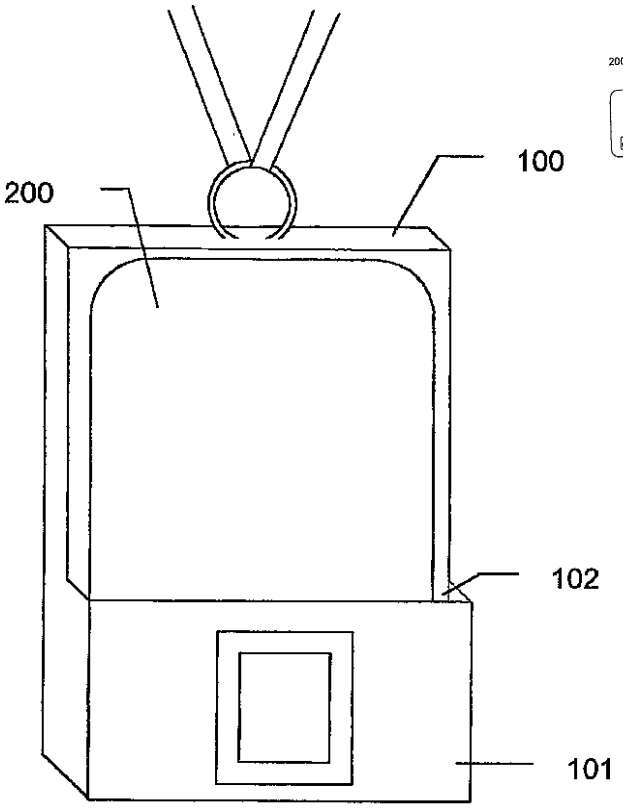

FIG. 3

【図４】

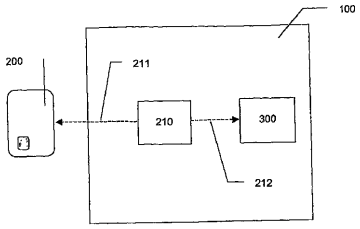

FIG. 4

フロントページの続き

(72)発明者　キャノン，チャールズ
アメリカ合衆国，バージニア州　２０１０６，アミスビル，バトル　マウンテン　ロード　７１０
(72)発明者　レイグル，トーマス
アメリカ合衆国，バージニア州　２２１９２，ウッドブリッジ，コルゲート　コート　１２５７３

審査官　深沢　正志

(56)参考文献　米国特許出願公開第２００５／０００１０２８（ＵＳ，Ａ１）
特表平１１－５１１２７８（ＪＰ，Ａ）
特開２００２－０６３１４１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/00 - 21/24