(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2011-90686
(P2011-90686A)
(43)公開日　平成23年5月6日(2011.5.6)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330F	5B035
H04L 9/32	(2006.01)	H04L	9/00	673D	5B043
G06K 19/10	(2006.01)	G06F	15/00	330G	5B285
G06K 19/07	(2006.01)	G06K	19/00	S	5J104
G06K 19/073	(2006.01)	G06K	19/00	H	

審査請求 有　請求項の数 25　ＯＬ　外国語出願　（全 29 頁）　最終頁に続く

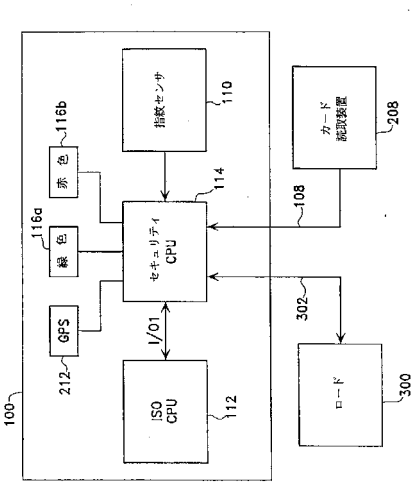
(21)出願番号　特願2010-243762 (P2010-243762)
(22)出願日　平成22年10月29日 (2010.10.29)
(62)分割の表示　特願2004-571994 (P2004-571994)の分割
原出願日　平成15年9月10日 (2003.9.10)
(31)優先権主張番号　60/409,716
(32)優先日　平成14年9月10日 (2002.9.10)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/409,715
(32)優先日　平成14年9月10日 (2002.9.10)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/429,919
(32)優先日　平成14年11月27日 (2002.11.27)
(33)優先権主張国　米国 (US)

(71)出願人　505090344
アイブイアイ・スマート・テクノロジーズ、インコーポレイテッド
アメリカ合衆国、カリフォルニア州　９５１３１、サン・ホセ、ナンバーエフ、オールド・オークランド・ロード　１８１０
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】アイデンティティの秘密保護された生物測定学的検査

(57)【要約】　（修正有）
【課題】高いセキュリティの識別カードを提供する。
【解決手段】高いセキュリティの識別カード１００は、記憶された生物測定学的データのためのオンボードメモリと、生体の生物測定学的データを捕捉するオンボードセンサ１１０とを備えている。カード上のオンボードプロセッサ１１４は整合動作を行って、捕捉された生物測定学的データが局所的に記憶されている生物測定学的データに一致することを確認する。整合が肯定的であった場合にのみ、追加の検査を行いおよび、またはさらに処理するためにカードからデータが送信される。
【選択図】図５



【特許請求の範囲】
【請求項１】
基準データを記憶するオンボードメモリと、
生の生物測定学的データを捕捉するオンボードセンサと、
捕捉された生物測定学的データを対応した記憶されている基準データと予め定められたしきい値の範囲内で比較し、この予め定められたしきい値範囲内に一致が存在する場合にのみ確認メッセージを発生するオンボードマイクロプロセッサと、
確認メッセージを外部ネットワークに伝送する手段とを備えているインテリジェント識別カード。
【請求項２】
確認メッセージは少なくとも、記憶されている基準データからの抜粋を含んでいる請求項１記載の識別カード。
【請求項３】
確認メッセージは少なくとも、捕捉された生物測定学的データからの抜粋を含んでいる請求項２記載の識別カード。
【請求項４】
確認メッセージは、追加の確認検査のために遠隔認証システムに送られる請求項３記載の識別カード。
【請求項５】
遠隔認証システムは、局所的に記憶された基準データとは異なった遠隔的に記憶された基準データを含んでいる請求項４記載の識別カード。
【請求項６】
オンボードマイクロプロセッサは、遠隔認証システムにおいて使用されるものとは異なった整合アルゴリズムを使用する請求項４記載の識別カード。
【請求項７】
全体的な整合プロセスはオンボードプロセッサによって行われ、捕捉された生物測定学的データはネットワークに送られない請求項２記載の識別カード。
【請求項８】
オンボードメモリ中に記憶されているオリジナルに捕捉された生物測定学的データおよび任意の他の“秘密”情報は共に、如何なる外部処理に対しても利用可能にされない請求項２記載の識別カード。
【請求項９】
カードはＩＳＯスマートカードコンパチブルである請求項２記載の識別カード。
【請求項１０】
さらに、ＩＳＯスマートカードプロセッサを備えている請求項９記載の識別カード。
【請求項１１】
秘密保護された生物測定学的データを記憶し、処理するために使用されるセキュリティプロセッサは、ファイヤウォールによってＩＳＯスマートカードプロセッサから機能的に分離されている請求項１０記載の識別カード。
【請求項１２】
セキュリティプロセッサとの間でやり取りされる外部データは全て、ＩＳＯスマートカードプロセッサを通過する請求項１０記載の識別カード。
【請求項１３】
ＩＳＯスマートカードプロセッサとの間でやり取りされる外部データは全て、セキュリティプロセッサを通過する請求項１０記載の識別カード。
【請求項１４】
セキュリティプロセッサはロードプロセス中にデータをロードするために使用される第１の接続と、外部ネットワークに接続された第２の接続とを有している請求項１０記載の識別カード。
【請求項１５】

ロードプロセスが終了した後、第１の接続は永久にディスエーブルされる請求項１０記載の識別カード。
【請求項１６】
秘密保護された生物測定学的データを記憶し、処理するために使用されるセキュリティプロセッサは、ファイヤウォールによってＩＳＯスマートカードプロセッサから機能的に分離されている請求項１０記載の識別カード。
【請求項１７】
カードは上方磁気ストライプ領域と下方浮き彫り領域とを備え、
生物測定学的センサは指紋センサであり、
セキュリティプロセッサと、ＩＳＯスマートカードプロセッサと、指紋センサとは全て、前記上方領域と前記下方領域との間の中間領域内に配置されている請求項１０記載の識別カード。
【請求項１８】
生物測定学的データは指紋データを含み、センサは、そのセンサ上に置かれたユーザの指からデータを捕捉する指紋センサである請求項２記載の識別カード。
【請求項１９】
ユーザが指紋センサ上の彼の指を操作しているときに実時間フィードバックが行われてセンサ上の指を最適に位置させるようにする請求項１８記載の識別カード。
【請求項２０】
整合プロセスは、捕捉された生物測定学的データ中の細部および全体的な空間的関係の両方を考慮するハイブリッド整合アルゴリズムを使用する請求項１８記載の識別カード。
【請求項２１】
指紋センサは、バッキングプレートによって支持された結晶シリコンのシートを含んでいる請求項１８記載の識別カード。
【請求項２２】
バッキングプレートは、２つの金属層に挟まれたガラスエポキシ層を含んでいる請求項２１記載の識別カード。
【請求項２３】
バッキングプレートは、シリコンのシートを取囲む支持体フレームによって補強されている請求項１８記載の識別カード。
【請求項２４】
カードはさらに、カードの使用を予め定められた位置に制限する手段を備えている請求項１記載の識別カード。
【請求項２５】
ユーザが関与している秘密保護された安全な金融取引の処理を行うアプリケーションサーバへのオンラインアクセスの許可の前に、そのユーザのアイデンティティの秘密保護されて安全な確認検査のために、捕捉された生物測定学的データおよび基準データの少なくともいくつかが分離した認証サーバに送られる請求項１記載の識別カード。
【請求項２６】
認証サーバにおいて肯定的な一致が生じる特定のアプリケーションサーバにおける特定のログオンの試みに関する整合リクエストに応答して、秘密保護された安全な３ウェイ認証プロトコルが実行され、このプロトコルにおいてチャレンジ文字シーケンスが認証サーバから識別カードに送られ、その後この識別カードがチャレンジ文字シーケンスと整合リクエストとを使用してチャレンジ応答を発生し、それはその後このチャレンジ応答をアプリケーションサーバに転送し、その後このアプリケーションサーバはチャレンジ応答を認証サーバに転送し、その後この認証サーバは、このチャレンジ応答が有効であるか否かを検査する請求項２５記載の識別カード。
【請求項２７】
カードからの出力は、秘密保護された安全な区域に物理的にアクセスするために使用される請求項１記載の識別カード。

【請求項２８】
アクセスの試みの成功および不成功の記録は、カード上に保持される請求項２７記載の識別カード。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アイデンティティの秘密が保護された生物測定学的検査に関する。
【背景技術】
【０００２】
本出願は、この明細書においてその全体が参考文献とされている暫定的な米国特許出願第60/409,716号（2002年9月10日出願）、米国特許出願第60/409,715号（2002年9月10日出願）、米国特許出願第60/429,919号（2002年11月27日出願）、米国特許出願第60/433,254号（2002年12月13日出願）および米国特許出願第60/484,692号（2003年7月3日出願）に基づいており、また、これらについて優先権を主張している。
【０００３】
コンピュータ化、とくにインターネットテクノロジーは金融データ、医療データ、個人データを含むデータへの非常に高いアクセス性を、秘密データが更新され、あるいは交換される金融およびその他の取引を迅速に処理する手段により提供している。
【０００４】
パスワードは一般に、このようなデータの機密性を保持するために使用されている。しかしながら、パスワードは、簡単に推測され、秘密保護について全く安全ではない誕生日または電話番号に基づいていることが多い。さらに、ランダムに発生された複雑なパスワードでさえ容易に盗まれることがしばしば可能である。したがって、パスワードベースのデータアクセスシステムは犯罪性のアタックを受け易く、その結果産業や経済、さらには人命にさえ危険およびダメージが及ぶことになる。したがって、データをその秘密について保護し、そのデータを許可されていないアクセスから保護する改良された方法が必要とされている。
【０００５】
生物測定学的データは、捕捉は困難であるが、解析が容易な正確な詳細（一連の指紋の詳細のような）または捕捉は容易であるが解析が困難な全体的なパターン（隣接した指紋の渦巻きの空間的特性のような）を含むことができる。
【０００６】
許可されたユーザだけが利用可能な１つのデジタル鍵を必要とする暗号化アルゴリズムが存在する。適切な鍵がなければ、かなりの量の時間と処理リソースを費やさない限り、その暗号化されたデータは使用可能なフォーマットに解読されることができず、それは暗号化されていないデータのある特性が知られている（あるいは少なくとも予測可能である）場合であってすら同様である。
【０００７】
サイトウ氏による公開された日本国特開昭60-029868号（1985年2月15日）には、カード保持者から得られた暗号化された生物測定学的データを登録するために集積メモリを備えたアイデンティティカードを使用する個人識別システムが教示されている。生物測定学的データには、声紋、指紋、身体的外観および、または生物学的分析評価が含まれる。使用において、カード上のデータは読取られ、そのカードを提示した人物から捕捉された対応したデータとの比較のために解読される。このようなシステムは、登録された個人が高度の正確さで明確に識別されることを可能にする。しかしながら、生物測定学的データは外部装置によって獲得されて処理されるため、カード上に記憶されている情報を変更不可能にし、および、またはアイデンティティを窃盗から保護することが困難である。
【０００８】
カード上に記憶されている生物測定学的データを暗号化すると共に隔離するハードウェアファイヤウォールを提供し、それによってその記憶されているデータを許可されていな

い変更から実質的にさらに高いセキュリティで保護するためにデータ駆動マルチプロセッサチップをカード上に含んでいる改良された識別カードが提案されている。しかしながら、実際の整合プロセスは、生体の生物測定学的データを捕捉した同じ外部読取端末上で行われ、したがって依然として潜在的に外部からの不正操作を受ける可能性を有している。

【発明の概要】

【０００９】

高いセキュリティの識別カードの第１の実施形態は、記憶された生物測定学的データのためのオンボードメモリだけでなく、生の生物測定学的データを捕捉するオンボードセンサもまた備えている。遠隔認証システムは、生物測定学的データを含んでいる秘密保護された安全なデータベースを維持する。カード上のオンボードプロセッサは予備的な整合動作を行って、捕捉された生物測定学的データが局所的に記憶されている生物測定学的データに一致することを検査する。局所的な整合検査の結果が肯定的であった場合にのみ、追加の確認の検査を行い、さらに処理するために、捕捉されたデータまたは取り扱いに注意を要する記憶されているデータが遠隔認証システムに送信される。悪意のあるアタックからさらに保護するものとして、局所的に記憶されたデータは遠隔的に記憶されたデータと異なっていることが好ましく、異なった整合アルゴリズムを使用して局所的な整合および遠隔的な整合が行われることが好ましい。したがって、カード、局所的に記憶されたデータおよび、またはそのカードが接続されているローカル端末が危険にさらされた場合でさえ、遠隔認証システムが依然として侵害行為の試みを検出することが可能である確率は高い。

【００１０】

第２の実施形態もまた、記憶された生物測定学的データのためのオンボードメモリと、生の生物測定学的データを捕捉するオンボードセンサと、およびオンボードプロセッサとを備えている。しかしながら、この実施形態においては、整合プロセス全体がオンボードプロセッサによって行われ、オンボードメモリ中に記憶されているオリジナルに捕捉されている生物測定学的データおよび任意の他の“秘密”情報は共に、如何なる外部処理に対しても利用可能にされていない。その代わり、新しく捕捉された生物測定学的データと前に捕捉された生物測定学的データとの間における整合の成功に応答して確認メッセージが発生されるだけである。確認メッセージにより、カードは通常の個人識別番号（ＰＩＮ）の入力の成功／不成功時に通常のＩＳＯスマートカードに類似した方式で、しかし秘密保護に関してさらに安全な検査プロセスによって付加的なセキュリティを与えられて機能する。これらの両実施形態において、記憶されている生物測定学的データおよび任意の関連した局所的に記憶されている暗号化アルゴリズムまたは暗号化鍵は、カード所有者に最初に発行したときに任意の後続する外部アクセスを阻止する方式でカードにロードされ、それによって記憶されている生物測定学的データの完全性および検査プロセス全体の完全性をさらに強化することが好ましい。

【００１１】

１実施形態において、ＩＳＯスマートカードは、保護された生物測定学的データの記憶および処理を行うために使用されるセキュリティプロセッサを悪意のある外部アタックからＩＳＯスマートカードインターフェースによって保護するファイヤウォールとして機能する。別の実施形態においては、セキュリティプロセッサはＩＳＯスマートカードインターフェースと変更されていないＩＳＯスマートカードプロセッサとの間に挿入され、ユーザの指紋が前に登録された指紋と一致するまで何等の外部通信も阻止する。

【００１２】

オンボード指紋整合能力を備えた高いセキュリティの識別カードの好ましい１実施形態においては、ユーザが彼の指を指紋センサ上で操作している期間中に実時間フィードバックが行われ、それによってそのセンサ上に指を最適に位置させることを容易にする。このフィードバックは、計算上の複雑さを減少させるだけでなく、未経験のユーザと不正なユーザとを弁別する付加的な手段もまた提供し、それによって誤った否定および、または誤った肯定の確率をさらに減少させる。別の好ましい実施形態においては、付加的なスチフ

ネスを提供する支持体内に指紋センサが保持される。
【００１３】
１つの例示的な適用において、捕捉された生物測定学的データおよび、またはカード所有者のアイデンティティの表示は暗号化され、機密データへのオンラインアクセスの任意の許可または秘密保護された安全な取引を終了する任意の自動プロセスの前に、金融機関および分離した認証サーバを含む取引ネットワークに入力される。別の例示的な適用においては、カードからの出力は、秘密保護された安全な区域に物理的にアクセスするために使用される。いずれの適用においても、アクセスの試みの成功または不成功の記録は、カードまたは外部セキュリティサーバのいずれか、あるいは両方において保持されることができる。
【図面の簡単な説明】
【００１４】
【図１】スマートカードを提示した人物のアイデンティティのオンボード生物測定学的検査が行われるそのスマートカードの１実施形態を示す概略図。
【図２】ユーザが指を指紋センサ上に最適に位置させるのを助ける例示的なプロセスを示すフローチャート。
【図３】秘密保護された安全な識別カードを提示した人物のアイデンティティの局所的検査および遠隔的な検査の両方を行うことのできる生物測定学的検査システムの機能ブロック図。
【図４】カード保持者の生物測定学的データの最初のロード期間中および遠隔地アプリケーションに対するカード保持者のアイデンティティの検査期間中に使用される異なった物理的データ路を備えた例示的な生物測定学的検査カードの機能ブロック図。
【図５】変更されていないＩＳＯスマートカードＣＰＵによる使用を意図された図４の例示的な生物測定学的検査カードの別の実施形態を示す概略図。
【図６】カード保持者のアイデンティティのローカル的な検査だけが行われる、例示的なアプリケーションと例示的な検査カードとの間における通信を示すフローチャート。
【図７】図６のフローチャートに類似しているが、しかし図５の例示的な生物測定学的検査カードによる使用のために修正されたフローチャート。
【図８】ローカル端末に対して無線または電気コネクタのいずれかによって接続されることのできる、オンボード生物測定学的検査を行われているスマートカードの第２の実施形態を示す概略図。
【図９】図８のカードの断面図。
【図１０】例示的な指紋センサの回路図。
【図１１】図１０のセンサのための支持装置の１実施形態を示す斜視図。
【詳細な説明】
【００１５】
スマートカード
“スマートカード”または“インテリジェントカード”という用語は、ここでは、手で把持され、首の回りに装着され、あるいは、そうでなければ、その人物により携帯されるように十分に小さく、また、ある個人のカード保持者に関する、あるいは、そうでなければ、その人物に関連したデジタル的に符号化された情報の記憶、処理および通信を行うことのできるマイクロプロセッサを含む任意の物理的な対象物を示すために一般的な意味で使用されている。このようなスマートカードの１つのよく知られている例はＩＳＯ（国際標準化機構）スマートカードであり、これは通常のクレジットカードと同じ物理的寸法および形状を有しているが、しかし特定ユーザ向けデータを記憶するためのフラッシュメモリと、パワフルな暗号化アルゴリズムによりプログラムされることのできるマイクロプロセッサとを含んでおり、このマイクロプロセッサは、ユーザ端末から受信されたＰＩＮ（個人識別番号）がこのカード上に記憶されている暗号化されたＰＩＮに一致したか否かを示し、それによってこのカードを提示した人物が本当のカード所有者であることに関する信頼度は、署名および、または物理的な類似の視覚的な比較だけに依存する検査システム

で可能であるよりも高いものとなる。

【００１６】

以下、オンボード生物測定学的検査が行われるそのスマートカードの１実施形態を示している図１を参照とする。カード100は一般にプラスチック材料から形成され、ほぼ５３．９８×８５．６ｍｍのＩＳＯ７８１６において指定されている近似的な大きさおよびほぼ０．７６ｍｍ以上の厚さの通常のクレジットカードと同様の全体的外観を有している。

【００１７】

通常のクレジットカードと同様に、カード100は磁気ストライプ（ＩＳＯ７８１１－２＆７８１１－６により指定されている）をカードの後面上に支持するためにカードの横幅全体に沿って延在するフリーの上方領域102を含んでおり、この磁気ストライプ上には、カード保持者および任意の関連した口座に関する通常符号化された英数字情報が記憶されることができ、それによってカード100が通常の磁気ストライプ読取装置において使用されることを可能にする。しかしながら、磁気ストライプに埋込まれた任意のデータは容易に変更されることができるため、このような磁気ストライプは、古い磁気ストライプベースの端末との逆適合の必要性が、磁気ストライプがシステムにもたらす潜在的なセキュリティの低下より重要なある適用での使用だけを意図されたものである。

【００１８】

この上方領域102はまた、カード保持者の不正変更防止のカラー写真および、またはカード発行者のホログラフロゴのような種々の詐欺行為予防手段をサポートするために使用されてもよい。カード100の下方領域104は、カード保持者の氏名、数字による口座（またはカード）識別名および有効期限のような浮き彫りにされた情報（ＩＳＯ７８１１－１により指定されている）のために慣例的なやり方で使用されることが可能であり、それによってカード100が通常のカード刻印機において使用されることが可能になる。

【００１９】

上方領域102および下方領域104は、８個の可視ＩＳＯスマートカードコンタクトパッド108のセットが埋込まれた中間領域106によって分離され、これらコンタクトパッド108はカードとカード読取装置上の対応したコンタクトとの間に便利な電気接続を提供する。この手段により、読取装置とＩＳＯ７８１６－３において指定されているカードとの間においてデータだけでなく、電力、タイミングおよび制御信号もまた交換されることができる。

【００２０】

領域106の右側には、指紋データをカード保持者の指から捕捉するために使用されるセンサパッド110が認められる。カードは、たとえば、通常のＩＰおよび、またはＭＡＣアドレスのフォーマットでのコード等の、センサ110またはそのカードに埋込まれている他の電子コンポーネントに特有であるＩＤコードを備えていることが好ましい。

【００２１】

図１には、コンタクトパッド108およびセンサ110と協同して、その他の方法で可能なもの優れた機能、とくに、良好なセキュリティを提供する複数の付加的な電子コンポーネントもまた概略的に示されている。

【００２２】

１実施形態において、ＩＳＯスマートカード適合プロセッサ112は、ＩＳＯコンタクトパッド108に直接接続されて外部ＩＳＯ適合カード読取装置（示されていない）との電気接続を提供し、それによって電力をオンボード電子装置に供給するだけでなく、カード読取装置上でまたはこのカード読取装置とネットワークされた任意の関連した計算装置上で実行中の任意の外部通信ソフトウェア、セキュリティソフトウェアおよび、またはその他のアプリケーションソフトウェアとカードとの間でデータのやり取りをする手段を提供する。

【００２３】

示されている実施形態においては、カード100と外部カード読取装置との間のデータ路はＩＳＯ指定スマートカードコンタクト装置を使用する配線式接続の形態であるが、別の

実施形態では、ＵＳＢまたはＲＳ２３２ＣまたはＳＰＩ（直列）接続のような別の伝送技術もまた、おそらく無線ＲＦ（無線周波数）、マイクロ波および、またはＩＲ（赤外線）通信リンクによって使用可能であることを理解すべきである。

【００２４】

また、記載されている実施形態はカード読取装置から電力を受取るが、別の実施形態は太陽電池または電池のようなオンボード電源を有することができる。このようなオンボード電源は、たとえば、カード100と特定のタイプのカード読取装置との間の機械的インターフェースは、コンタクト108がカード読取装置内の対応した接続部に接続されたときにユーザが指紋センサ110にアクセスできず、したがってカード100がカード読取装置に直接接続されていないときはそのユーザの指紋データが捕捉されなければならないようなものである場合等に有効である。

【００２５】

セキュリティプロセッサ

示されているように、セキュリティプロセッサはＩＳＯプロセッサ112とセンサ110との間に接続され、捕捉されたデータの秘密保護された安全な処理および記憶を行うと共に、以下に説明するように、秘密保護された安全な“ファイヤウォール”を提供して、その専用メモリ中に記憶されているデータおよびプログラムをＩＳＯプロセッサ112を介した不正アクセスの試みから保護する。このようなファイヤウォールは、前に記憶された指紋パターンから抽出されたデータあるいはＣＰＵ番号または指紋センサ番号のような特有に割当てられた装置番号のような、特有に割当てられたネットワークアドレスに基づいているか、あるいはそうでなければ特定のカードに特有である暗号化鍵を使用して暗号化されたデータだけを通過させるように設計されてもよい。別の実施形態において、ファイヤウォールは、前の伝送またはデータからの特有の識別データを含むデータだけを通過させる。さらに別の実施形態においては、ファイヤウォールは異なったアプリケーションに対して異なった鍵を保持し、これらの鍵を使用してデータを異なった各プロセッサまたはメモリ区分に送る。

【００２６】

別の実施形態（示されていない）において、セキュリティプロセッサ114はＩＳＯコンタクト108に直接接続され、ＩＳＯプロセッサ112とＩＳＯコンタクト108との間の秘密保護された安全なゲートキーパーとして動作する。このような別の構成には、ＩＳＯプロセッサ112中にすでに組込まれている可能性のある如何なるセキュリティ特徴とも妥協することなしに、セキュリティプロセッサ114およびセンサ110により付加的なセキュリティが提供されるという利点がある。

【００２７】

セキュリティプロセッサ114は、前に登録された指紋パターンおよび、またはその他の個人の生物測定学的情報を記憶するＦＲＡＭ、ＯＴＰ、E^2ＰＲＯＭ、ＭＲＡＭ、ＭＲＯＭのような不揮発性の半導体または非半導体メモリを含んでいることが好ましい。別の実施形態においては、セキュリティプロセッサ114の機能のいくつかまたは全てがＩＳＯプロセッサ112において実施されることが可能であり、および、またはＩＳＯプロセッサ112の機能のいくつかまたは全てがセキュリティプロセッサ114において実施されることが可能である。このような１つの組合せ構成は依然として種々の機能間のソフトウェアファイヤウォールを維持し、これは、とくに、記憶されているソフトウェアプログラムへの後続的な変更を許さないプロセスによりその装置が構成されていた場合に有効である。その代わりに、プロセッサ112および114の両者は、各プロセスを異なるプロセッサにおいて実行中の別のプロセスからの干渉から保護するように設計された単一のマルチプロセッサ装置内の別々のプロセッサであることができる。このようなマルチプロセッサ装置の一例は、日本のシャープ社製のＤＤＭＰ（データ駆動マルチプルプロセッサ）である。

【００２８】

これらの種々のセンサ、コンタクトおよびその他の電子コンポーネント、ならびにそれらが相互接続されている印刷回路その他の電気配線は全て、それらが侵蝕および外部汚染

から保護されるようにカード100の本体内に完全に組込まれていることが好ましいが、それらは上方領域102と下方領域104との間の中間領域106内の好ましい位置によりそれらの別の領域と機械的にインターフェースする通常の磁気ストライプ読取装置、浮き彫り装置および刻印機から受ける可能性のある損傷からさらに保護される。

【００２９】

ＬＥＤフィードバック

ＬＥＤ116aおよび116bはセキュリティプロセッサ114により制御され、ユーザに可視フィードバックを提供する。示されている実施形態においては、それらは下方領域104内の好ましくはカードの、コンタクトパッド108と反対側の、サイドエッジの位置に配置されている。いずれにしても、ＬＥＤ116a、116bは、それらが浮き彫りプロセス期間中に損傷を受けない場所であって、かつ、カードが通常のＩＳＯスマートカード読取装置中に挿入されたときおよび、またはユーザの指が指紋センサ上110に置かれているあいだ、それらが見える場所に配置されていることが好ましい。たとえば：

検査確認モードにおいて：

・赤色明滅：指を待っている
・明滅の停止：指がセンサ上に置かれた
・一度の赤色明滅：整合不可能、指を動かしてもよい
・一度の長い緑色明滅：整合された、指をどけてもよい

登録モードにおいて：

・緑色明滅：指を待っている
・明滅の停止：指がセンサ上に置かれた
・一度の赤色明滅：登録不可能、指を動かしてもよい
・一度の緑色明滅：登録された、指をどけてもよい

消去モードにおいて：

・緑色および赤色明滅：消去準備完了
・一度の緑色明滅：消去された

ユーザは、否定的な報告が送信される前に、整合または登録の成功のために彼の指を位置する多くの機会を与えられることが好ましい。１実施形態においては、緑色のオーケー表示を受取る前にユーザが彼の指をどけた場合あるいは予め定められた時間限界を超えた場合にのみ、否定的な報告が認証サーバに送信される。このようなプロセスにより、ユーザはセンサ上で彼の指を最適に位置するように訓練され、それによって計算の複雑さが減少するだけでなく、もっと多くの弁別しきい値を使用することが可能になる。この可視フィードバックはまた、未経験のユーザ（典型的に彼が適切に位置させることができるまで試行し続ける）と不正ユーザ（典型的に注意を引くことを望まず、彼の悪意のある意図に気づかれないうちにその場を離れる）とを弁別するための心理的ベースを提供する。最終的な結果として、誤った否定および、または誤った肯定の確率は著しく減少する。

【００３０】

図２は、ユーザが彼の指をセンサ110上に置くのを助ける例示的なプロセスを示している。ブロック150において、赤色ＬＥＤ116bは明滅している。指が検出される（ブロック152）と、ＬＥＤは明滅するのを止めて、イメージ品質（指の皮膚の先と付け根とに対応する規定された細長い領域）のテストが行われる（ブロック154）。その品質が不十分である場合（ノーの分枝156）、赤色ＬＥＤ116bは一度明滅することによりユーザに彼の指を別の位置に移動するように命令する（ブロック158）；そうでない場合（イエス分枝160）、そのユーザを登録するために使用されたのと同じ指が同じ位置に置かれたか否かを決定するために第２のテストが行われ（ブロック162）、その結果、比較的簡単な整合アルゴリズムにより、生体のデータが記憶されているデータに予め定められたしきい値範囲内において一致することが確認され、それによって生体の指が初めに登録された指と同じである（イエス分枝164）ことを確認することができ（イエス分枝164）、緑色ＬＥＤが起動され（ブロック166）、それは整合が成功したのでユーザは彼の指をどけてもよいことを確認するのに十分な時間のあいだ行われる（ブロック168）。その代わり、整合しきい値は

満足されない場合（ノー分枝170）、赤色ＬＥＤ116bは一度明滅することよりユーザに彼の指を別の位置に移動するように命令し（ブロック158）、このプロセスが繰返される。

【００３１】

例示的なネットワークアーキテクチャ

次に、秘密保護された安全な識別カードを提示した人物のアイデンティティの局所的および遠隔的な両方の確認検査を行うことのできる生物測定学的検査システムの可能な１実施形態が示されている図３を参照する。それは、クライアント端末200、アプリケーションサーバ202および認証サーバ204の３つの主要なコンポーネントを含んでいる。クライアント端末200は、ユーザの指紋のライブ捕捉および局所的処理を行い、局所的に処理されたデータの暗号化を行い、アプリケーションサーバおよび認証サーバとの秘密保護された安全な通信を、好ましくはＩＰ／ＴＣＰアドレス指定方式および伝送プロトコルを使用してインターネットによって行い、通常のＩＰファイヤウォール206により不正アクセスから保護される機能を備えている。別の実施形態において、ファイヤウォール206は、送信されたデータが許可されたデータであることを確認された後にそれを符号化し、受信されたデータが本当に許可されたデータであるか否かを、たとえば、ＤＥＳ128のような暗号化アルゴリズム使用して決定する前にそれを復号するフィルタおよび暗号化エンコーダ／デコーダを備えることができる。これによって、ファイヤウォール206は、メッセージヘッダだけでなくメッセージ内容にも基づいてデータを許可されたものまたは潜在的に悪意のあるものとして分類することができる。

【００３２】

クライアント端末200は専用ウェブアプライアンスとして構成されてもよいし、あるいはＷｉｎｄｏｗｓ（登録商標）（Ｒ）ＸＸＸ、ＯＳ　Ｘ、ＳｏｌａｒｉｓＸＸ、Ｌｉｎｕｘ（登録商標）またはＦｒｅｅＢＳＤのような汎用オペレーティングシステムによって制御されるプログラム可能なデスクトップ、ノートブックまたは他のワークステーションあるいはパーソナルコンピュータ上にインストールされたソフトウェアで構成されることができる。クライアント端末200は、セキュリティの付加的な手段を提供する最新“否定”データベース（たとえば、紛失した、あるいは盗まれたカードのアイデンティティ、または特定のカードまたはカードのグループに対する制限等）を含んでいることが好ましい。

【００３３】

アプリケーションサーバ202は、認証サーバ204によってユーザのアイデンティティが確認された後に、取引を行うか、あるいは、そうでなければクライアント端末200における遠隔ユーザからの命令に応答する機能を備えている。認証サーバ204は、クライアント端末200およびアプリケーションサーバ202の両者と秘密保護された安全な通信を行い、認証指紋データおよび前に登録されたユーザに関する他の情報を記憶し、その記憶されたデータを、クライアント端末200から受信された暗号化された生のデータと比較して、特定された生のデータが特定された記憶された指紋データと一致するか否かをアプリケーションサーバ202に知らせる機能を備えている。

【００３４】

とくに、クライアント端末200はさらに、インターネットブラウザ端末210とカード読取装置インターフェース108a（それはＩＳＯスマートカードコンタクトパッド108との各電気接続を形成する１組の電気コンタクトにおいて終端している簡単なＵＳＢケーブルであってもよい）を含むコンポーネントである固定されたカード読取装置208と、ポータブルスマートカードコンポーネント100’の２つの主要なコンポーネントを備えている。１実施形態において、ポータブルコンポーネント100’は、指紋センサ110、セキュリティプロセッサ114およびＩＳＯスマートカードプロセッサ112を含んでいる上述したスマートカード100であってもよい。

【００３５】

アプリケーションサーバ202はさらに、ファイヤウォール206およびインターネットブラウザ214ならびに取引アプリケーションモジュール216および妥当性検査モジュール218を含むインターネットサーバインターフェースを含んでいる。アプリケーションサーバおよ

びアプリケーションモジュール216がＩＰ／ＴＣＰプロトコルにより外部と通信するようには設計されなかった継承（ｌｅｇａｃｙ）装置である場合、ファイヤウォール206は、妥当性検査モジュール218の組込みを行うと共に固定されたＩＰアドレスを有している適切なプロトコル変換装置で置換されてもよい。アプリケーションサービスサーバは、たとえば、サービスをインターネットによって許可されたユーザに自ら進んで提供する第３パーティによって動作されてもよい。

【００３６】

認証サーバ204はさらに、インターネットサーバインターフェース220と、指紋整合アルゴリズム224を含む処理モジュール222と、個人がそのシステムに登録され、彼等のアイデンティティがそのシステムのオペレータを満足させるものであると保証されたときにそれら個人から収集された指紋およびその他の認識情報を記憶するデータベース226とを備えている。セキュリティをさらに強化するものとして、任意の特定の個人に対する記憶されたデータは情報の単一のシーケンスとしてアプリケーションサーバ上に記憶されるのではなく、むしろ各項目が分離して記憶されることが好ましく、これらの項目を結びつける任意の必要とされる索引または関係は、その個人の秘密データの一部として認証サーバ中に保持されている対応した鍵によってのみアクセス可能である。

【００３７】

位置

ある実施形態においては、固定された読取装置208および、またはポータブルカード100’’はまた、ある特定の取引が行われた時の読取装置およびカードの現在の位置に関する有用な情報を提供することのできる集積ポジショニング衛星（ＧＳＰ）受信機212を備えていてもよい。とくに、ＧＰＳ受信機212からの位置データは、読取装置および、またはカードがその使用の許可されていない位置に移動された場合にその読取装置および、またはカードを動作不能にする（永久的にまたは一時的に）ために使用されてもよい。位置はまた、ＧＰＳ以外の手段によって、たとえば、ＰＨＳ（日本国のセルラー電話）発信元位置決定技術、または地球の電磁界のローカル変化に応答するロケーションセンサを使用して自動的に決定されることができる。ＧＰＳを備えたカードの特定の場合においては、アンテナ、信号増幅、ＡＤ変換器およびサンプリングおよび保持回路、ならびに位置を計算するためのデジタルプロセッサを含む種々のＧＰＳコンポーネントは、カードの本体と統合され、そこに埋込まれ、あるいはその上に積層にされた単一の集積回路の、または単一の回路板上に取付けられたディスクリートな装置の全ての部分であることが好ましい。

【００３８】

オンボード整合ＩＳＯプロセッサインターフェースを備えたＩＳＯカードに対するカードアーキテクチャ

図４は、カード保持者の生物測定学的データの最初のロード期間中および遠隔地アプリケーションへのカード保持者のアイデンティティの検査期間中に使用される異なった物理的データ路を備えた例示的なＩＳＯスマートカードコンパチブル生物測定学的検査カード100または100’の機能ブロック図である。

【００３９】

とくに、上述したＩＳＯプロセッサ112、セキュリティプロセッサ114、指紋センサ110、ＬＥＤ116a、116bおよびオプションのＧＰＳ受信機212に加えて、ＩＳＯプロセッサ112だけがＩＳＯスマートカードコンタクトパッド108を介してカード読取装置208に直接接続された状態で、分離したロードモジュール300および関連した一時的接続302が示されており、この一時的接続302は最初のユーザ登録期間中にセキュリティプロセッサ114との直接的な通信を提供する。ＩＳＯプロセッサ112はＩ／Ｏポート304、306によってセキュリティプロセッサ114と通信し、一方一時的なロード接続302は分離したＩ／Ｏポート308に接続されていることが認められる。セキュリティプロセッサは、取り扱いに注意を要する任意のセキュリティ関連データまたはソフトウェアがポート304および306からではなくポート308からのみアクセス可能であり、それによって接続302がディスエーブルされた後、これらの取り扱いに注意を要するデータへの悪意のあるアクセスの可能性を回避するように

プログラムされることが好ましい。

【００４０】

入手可能な大部分のＩＳＯプロセッサは少なくとも２つのＩ／Ｏポートを有しており、いくつかは少なくとも３つのＩ／Ｏポートを備えている。外部ＩＳＯコンパチブルカード読取装置208への通常のＩＳＯスマートカード直列データ接続108に対して、これらのポートの１つ（Ｉ／Ｏ１）だけが示されている。余分な１または２つのＩ／Ｏポートは、ＩＳＯプロセッサ112とセキュリティプロセッサ114との間に専用ハードワイヤード通信を提供することが好ましく、それは、セキュリティプロセッサ114を再プログラムしようとする、あるいはセンサ110によって前に捕捉された、あるいはそうでなければセキュリティプロセッサ114内に記憶されている取り扱いに注意を要する情報にアクセスしようとする悪意のある試みを阻止するハードウェアファイヤウォールとして働く。３つ以上のＩ／Ｏラインを備えたＩＳＯプロセッサの特定の場合においては、セキュリティプロセッサが完全にパワーダウンされているときでさえ、ＩＳＯプロセッサとセキュリティプロセッサとの間の専用通信路上における静的状態情報の、（１）準備完了、（２）ビジー、（３）失敗、および（４）合格のような３以上の状態を提供することが可能である。当然ながら、１つのＩ／Ｏポートしか利用できない場合でも、これら４つの状態は直列データとして動的に送信されることができる。

【００４１】

ＩＳＯ　ＣＰＵとセキュリティＣＰＵとの間においてＩＳＯインターフェースＩ／Ｏ２およびＩ／Ｏ３を介して送信されることのできる可能なコマンドおよびデータには、以下のものが含まれる：

・ユーザを登録し、あるいは認証するためのコマンドであって、これに対してセキュリティＣＰＵは局所記憶および、または遠隔アプリケーションへの送信のために登録の結果または認証の結果を送る。

・テンプレート（基準）としての指紋情報は、遠隔アプリケーションへの送信のためにＩＳＯスマートカードメモリ中に記憶されるためにセキュリティＣＰＵからＩＳＯ　ＣＰＵに送られることができる。取り扱いに注意を要する個人情報のセキュリティを高めるために、基準データはそれがＩＳＯ　ＣＰＵに送られる前にセキュリティＣＰＵによって暗号化されることができる。

【００４２】

ロード接続302は、セキュリティＣＰＵ114にもまたパワーを利用できるようにＩＳＯ　ＣＰＵ112とＩＳＯ読取装置208との間の通信をおそらく保持しながら、ファイヤウォール保護を与えられたＩＳＯ接続および関連した専用Ｉ／Ｏ304および306をバイパスしてセキュリティＣＰＵ114への直接接続を提供する。それは主として特定のユーザへのカードの最初の登録期間中に使用され、許可されていないアクセスから保護されなければならない。

【００４３】

図５は、変更されていないＩＳＯスマートカードＣＰＵによる使用を意図された図４の例示的な生物測定学的検査カードの別の実施形態を示している。とくに、ＩＳＯ　ＣＰＵ112’は、通常の使用中またはロード中のいずれの期間中も、もはやカード読取装置208とセキュリティＣＰＵ114’との間の如何なるゲートウェイ機能も行ってはならず、したがって、それは、何の変更もなされず、カード読取装置208および任意の外部アプリケーションの両者に対して絶対的に透明である方法でのみ使用される任意のＩＳＯ認可チップであることができる。このような別の実施形態においては、セキュリティＣＰＵ114’は、捕捉された指紋が記憶されている指紋に一致した場合にはＩＳＯ　ＣＰＵ112’と任意の外部アプリケーションとの間の透明なファイヤウォールとして動作し、また、捕捉された指紋が記憶されている指紋に一致しなかった場合にはこのような通信を全て阻止する。

【００４４】

カード初期化および記憶されているデータの保護

ギロチン

１実施形態において、オリジナルな製造されたカードは、セキュリティＣＰＵおよびＩＳＯインターフェースの少なくとも一部分および、またはディスクリートなオンボードメモリへの直接接続を提供する突出した印刷回路拡張部を有している。この直接接続インターフェースはカードのテストおよび指紋データの登録のためだけに使用され、登録プロセスをエネーブルする信号を含んでいる。この回路拡張部は、登録が完了した後、これ以上登録することが不可能であり、セキュリティＣＰＵメモリがＩＳＯ　ＣＰＵおよびこのＩＳＯ　ＣＰＵとセキュリティＣＰＵとの間の上述したファイヤウォールを介してのみアクセスできるように機械的に切断される。

【００４５】

ヒューズ

別の実施形態において、セキュリティＣＰＵは、登録された指紋パターンが一度書込まれるとアクセス不可能になる１つのタイプのメモリを有している。このようなメモリの一例は、構成がＥＥＰＲＯＭに類似しているがＵＶには不透明であるため消去されることのできないワンタイムＰＲＯＭ（“ＯＴＰ”）である。別の例は、登録が完了した後に、たとえば、エネーブルまたはアドレスあるいはデータ信号路の一部に物理的な破断（“ヒューズ”）を形成するように十分な電流をその信号路の一部分に与えることによって読取専用にされるフラッシュＲＯＭである。

【００４６】

例示的な認証プロセス

１実施形態において、例示的な認証プロセスは、物理的な指紋データを、たとえば、アプリケーションサービスサーバに接続するためにアクセスする人物により使用されるクライアント端末において光学、圧力、導電性、容量性、音響的、弾性または写真技術等を使用して捕捉することを含んでおり、この物理的な指紋データはその後分離した指紋認証サーバに送られる（好ましくは、暗号化された形態で）。指紋認証サーバは捕捉された指紋データを認証ソフトウェアを使用して、登録されたユーザの指紋データを含む指紋ファイルと比較し、データが一致した場合は認証サーバはエネーブル命令をアプリケーションサービスサーバに送る。

【００４７】

別の実施形態において、ユーザは、氏名、住所および誕生日のような個人データと共に全ての指紋がそこに予め登録される指紋のファイルを含んでいる指紋認証サーバの秘密保護された安全なウェブブラウザにアクセスする。ＨＴＴＰＳフォーマットのような秘密保護された安全なプロトコルによってユーザがアクセスしている秘密保護された安全な指紋認証サーバは、その後ユーザの指紋をクライアント端末で捕捉せよという命令をクライアント端末に送る。クライアント端末のブラウザにより表示された命令に応答して、ユーザは彼の選択した指を指紋センサ上に置き、クライアント端末内に存在する指紋捕捉ソフトウェアが、たとえば、２５ミクロン乃至70ミクロンピッチ解像度および１２．５mm^2乃至２５mm^2の面積を有すると共にさらに８ビットグレースケールを有している画素ベースのイメージ等のデジタル指紋を捕捉する。

【００４８】

秘密保護された安全な指紋認証サーバは、ユーザＩＤおよびインターネットＩＰアドレスおよび、または指紋センサ個人コード（ＭＡＣアドレス）および、またはクッキーおよび、または任意の固有コードあるいは特定の個人または端末を識別する他の情報（たとえば、クライアント端末と秘密保護された安全な指紋認証サーバとの間の前の会話からの詳細）と共に指紋データを受取り、その後それはその受取られた指紋データを、認証ソフトウェアを使用して、ユーザＩＤを、氏名、住所、誕生日、犯罪暦、運転免許証、社会保証番号のような個人情報と共に予め登録された指紋データである指紋ファイルと比較し、これは詳細（ｍｉｎｕｔｉａｅ）比較であることが可能であり、および、または高速フーリエ変換比較であることができる。

【００４９】

認証プロセスの始まりにおいて、関連したアプリケーションに対してウェブサーバ214

は視覚的または聴覚的にユーザに彼の指を指紋捕捉センサ110上に置いて彼のマウスボタンをクリックするか、あるいはキーボードキーを押し、それによってセキュリティプロセッサ114中の指紋捕捉ソフトウェアに知らせるように命令する。そのあと、ユーザの捕捉された指紋データは暗号化されたフォーマット（たとえば、秘密保護された安全なＲＡＳ暗号化伝送プロトコルＨＴＴＰＳを使用して）でクライアント端末200のＩＳＯプロセッサ112およびウェブブラウザ210を介して指紋認証サーバ204のウェブサーバ220に送られる。捕捉されたデータがデータベース226中の対応したデータと成功的に一致した場合、指紋認証サーバ204はそのユーザのアイデンティティをクライアント端末200およびアプリケーションサーバ202の両者に対して有効なものにする。

【００５０】

以下、図３を参照として３ウェイ認証プロトコルおよびワンタイムパスワードをハッシュ文字符号化シーケンスとして使用する例示的な好ましい実施形態を説明する。

・クライアント端末200のウェブブラウザ210は、アプリケーションプロセス216にアクセスするリクエストによりアプリケーションサーバ202の対応したウェブインターフェース214にアクセスする。

・アプリケーションサーバ202のウェブインターフェース214は、アプリケーションプロセス216にアクセスするためのログインスクリーン情報および関連した命令で応答する。

・クライアント端末200はＩＳＯプロセッサ112にセキュリティプロセッサ114を起動するように命令する。

・ＩＳＯプロセッサ112はセキュリティプロセッサ114をトリガーする。

・セキュリティプロセッサ114は指紋センサ110からの指紋データを待機し、有効なデータが受信されたとき、ＩＳＯプロセッサ112を介してウェブブラウザ210に転送されたデジタル指紋パターンを抽出する。

・ウェブブラウザ210は、ユーザＩＤ、クライアント端末200のＩＰアドレス、および、またはセンサ110のハードワイヤードＩＤコード（ＭＡＣアドレス）のような関与するカード100’およびカード読取装置208に関する関連情報を伴って（あるいは、それにより暗号化されて）、抽出された指紋パターンの暗号化されたバージョンを認証サーバ204に送信する。

・認証サーバ204のウェブインターフェース220は、抽出された指紋パターンをクライアント端末200からその他の情報と共に受取るとき、その情報を指紋整合プロセッサ222に転送する。

・整合ソフトウェア224の制御の下で、指紋整合プロセッサ222は受信されたユーザＩＤまたはその他のユーザに特定の関連情報を使用して対応した基準指紋パターンをデータベース226から検索し、捕捉された指紋パターンをその基準指紋パターンと比較する。

・その結果（一致した、あるいは一致しなかった）は端末200、ユーザＩＤカード100’およびリクエストしたアプリケーション216を識別する関連情報と共にアクセス履歴ログ中に記憶され、制御が認証サーバウェブインターフェース220に戻される。

・結果が一致であった場合、認証サーバウェブインターフェース220は、クライアント端末200に送信されるワンタイムパスワードをチャレンジ文字シーケンスの形態で発生し、また、そのチャレンジ文字シーケンスをハッシュコードとして使用して、それが将来可能性のある参照基準に備えて対応したチャレンジ応答として保存する関連情報を暗号化する。

・クライアント端末200は受信されたチャレンジ文字シーケンスをハッシュコードとして使用して、前に記憶された暗号化されていない実行依頼された関連情報のコピーを暗号化し、その後これをアプリケーションサーバ202のウェブインターフェース214にアプリケーションログインプロセスへのその応答の一部として転送する。

・アプリケーションサーバ202のウェブインターフェース214は、ハッシュ変換された関連情報を受信すると、それをアプリケーションサービス216に転送し、このアプリケーションサービス216がこれをクライアントサーバからの進行中のログオンの試みと関連付け

、また、その一致した結果を確認するために、認証サーバによりチャレンジ応答として提供されたチャレンジシーケンスを使用してクライアント端末によりハッシュされたその受信された関連情報を転送する。

・認証サーバ204のウェブインターフェース220は、チャレンジ応答をアプリケーションサーバから受信すると、その応答を認証プロセス222に転送し、この認証プロセス222がこれを、予測されたチャレンジ応答の前に保存されたその基準コピーと比較し、そのユーザアイデンティティが実際に認証されているか否かを決定する。

・この比較から結果的に得られた認証されたユーザアイデンティティ情報はその後、アプリケーションサーバ202のアプリケーションサーバウェブインターフェース220および有効化インターフェース218を介してアプリケーションプロセス216に戻される。

・有効化インターフェース218はその認証を使用して、オリジナルなログオンの試みで設定されるそのユーザのアイデンティティが有効なものにされていることを確認する。

・ユーザのアイデンティティが確認されると、認証プロセス216はその後アプリケーションサーバ202のウェブインターフェース214を介してクライアント端末200のウェブブラウザ210と直接通信し始める。

【００５１】

図６は、全ての整合がセキュリティＣＰＵ114によって図４のＩＳＯコンパチブルカードに関して行われ、外部認証サーバ204は使用されない別の認証プロセスを示している。

【００５２】

図６の左側には認証サーバ202により行われる機能が示されており、一方右側にはＩＳＯスマートカード100によって行われる機能が示されている。

【００５３】

スマートカード100がカード読取装置208中に挿入されたとき、リセット信号ＲＳＴがカード読取装置からＩＳＯ　ＣＰＵ（スタートブロック502）および指紋ＣＰＵ114（指紋検査ブロック504）の両者に送られ、両者はカード読取装置208からパワーＶＣＣを受取る。その後、ＩＳＯ　ＣＰＵはＡＴＲ（リセットに対する応え）メッセージで応答し、必要とされたときＰＰＳ（プロトコルおよびパラメータ選択）を送る（ブロック506）。同時に、指紋ＣＰＵは指紋データを受信するために待機状態になり、データがセンサ110から受取られたときに認証プロセスを行う（ブロック504）。

【００５４】

アプリケーション216によって最初のリクエストコマンドがＩＳＯ　ＣＰＵ112に送られたとき（ブロック508）、ＩＳＯ　ＣＰＵは認証状態をセキュリティＣＰＵに問合せる（ブロック510）。応答が肯定的であった場合、ＩＳＯ　ＣＰＵはリクエストされたコマンドを実行することによりそのアプリケーションに応答する（ブロック512）。そうでない場合（セキュリティＣＰＵ114からエラーメッセージまたは応答なしのいずれか）、それはリクエストされたコマンドに応答せず、むしろ新しい第１のリクエストを待機する（ブロック508b）。

【００５５】

指紋は検査されて確認され、第１の応答がアプリケーション216によってタイムリーに受信され、応答していると決定された（ブロック514）と仮定すると、アプリケーションから１つのリクエストも受信されなかった予め定められた検査タイムアウトを超えるか（ブロック522）、あるいはアプリケーションが予測された応答の受信に失敗する（ブロック524）まで、リクエスト／応答プロセスは続行する（ブロック516、518、520）。

【００５６】

図７は図６のフローチャートに類似しているが、しかし図５の例示的な生物測定学的検査カードによる使用のために修正されたフローチャートである。図７の左端にはアプリケーションサーバ202によって行われる機能が示され、次の列は読取装置208に対応し、その次の列はＩＳＯコンタクト108を表し、次の列はセキュリティＣＰＵ114によって行われる機能を示し、右端には変更されていないＩＳＯスマートカードＣＰＵ112によって行われる機能が示されている：

・スマートカードがカード読取装置中に挿入されたとき、あるいはアプリケーションソフトウェアがカード読取装置の動作を開始させたいずれかのときに、リセット信号550がカード読取装置208からセキュリティＣＰＵ114に送られる。

・セキュリティＣＰＵがリセット信号550を受信した後すぐに対応したリセット信号552をＩＳＯ　ＣＰＵ112に送る。同時に、セキュリティＣＰＵは指紋センサからの指紋データを待機する。

・ＩＳＯ　ＣＰＵはリセット信号552を受信すると、ＡＴＲ（リセットに対する応え）応答554を行って、その後必要とされたときにＰＰＳ（プロトコルおよびパラメータ選択）を送る。

・セキュリティＣＰＵ114はＩＳＯ　ＣＰＵからＡＴＲ（リセットに対する応え）を受信するとすぐに、これをカード読取装置に転送し（ブロック556）、これには任意の関連したＰＰＳコマンドが含まれている。

・その期間中に、セキュリティＣＰＵが指紋データを受信した場合、それは上述した認証プロセスを実行する。認証テストの結果が合格であった場合、その合格状態が特定の時間期間中保持される。結果が失敗であった場合、セキュリティＣＰＵ114は新しい指紋データを待機する。

・アプリケーションの実行時に、コマンドリクエスト558はセキュリティＣＰＵに送られ、このセキュリティＣＰＵはコマンドリクエスト560をＩＳＯ　ＣＰＵに転送すると共に、セキュリティＣＰＵが依然として上述の合格状態であるか、あるいは最後の正しい応答がもっと多くのデータビットセットを有している（テストブロック564）場合にのみ、その正しい応答562をカード読取装置に転送する。

・そうでない場合（ノー分枝566）、指紋ＣＰＵはダミーリクエスト568を発生し、それをＩＳＯ　ＣＰＵに転送すると共に結果的に得られたＥＲＲ応答570をカード読取装置216に転送し、それによってリクエストと応答におけるシーケンス番号の間の適切な同期を維持する。

【００５７】

暗号化およびセキュリティ

任意の外部ネットワークによる送信の前に、取り扱いに注意を要する任意のデータおよび、または認証結果は、おそらくＤＥＳまたはツーフィッシュ暗号化を使用して暗号化されることが好ましい。暗号化鍵は、捕捉されたまたは記憶されている指紋データ、ユーザＩＤコード、センサの特有に割当てられたコード、メモリアドレス、メモリ中の隣接したデータ、別の機能的に関連したデータ、前の会話（取引）、ＩＰアドレス、端末コードまたは割当てられたパスワードに基づくことができる。その代わり、取り扱いに注意を要するデータは、秘密保護された安全なＨＴＴＰＳプロトコルを使用してインターネットによって送信されることができる。

【００５８】

さらに高いセキュリティを提供するために、ハードウェアＤＥＳ暗号化および解読のような仮想秘密ゲートウェイが秘密保護された安全な指紋認証サーバとネットワーク接続との間に挿入されると共に、対応的にアプリケーションサービスサーバとネットワーク接続との間にも挿入されることができる。このような仮想ゲートウェイまたは仮想秘密ネットワーク（“ＶＰＮ”）を使用してそのようにすることにより、取り扱いに注意を要するデータは暗号化の付加的な層、たとえば、ＤＥＳ128（典型的にＶＰＮにおいて使用される）およびＲＳＡ（ＨＴＴＰＳにより使用される）の両者等、によってさらに保護される。

【００５９】

とくに、秘密保護されて安全なアプリケーションについて、全ての通信はセキュリティの付加的な層によりラップされてもよい。とくに、下位層中のメッセージヘッダは上位層において暗号化されることができる。

【００６０】

無線通信

別の実施形態は、コンタクト（ＩＳＯ７８１６）および無線（ＩＳＯ１４４３Ａまたは

Ｂ）の両動作に対する二重インターフェースを含んでおり、全てが１枚のカード上にある（とくに）ＩＳＯ７８１６コンタクト、ＩＳＯ１４４３Ａ、ＩＳＯ１４４３Ｂ、ＩＳＯ１５６９３およびＨＩＤ継承無線システム間における共同利用を可能にするマルチインターフェースパワーユニットを組込んでいることが好ましい。その代わり、カードは、ブルートゥース（短距離）またはセルラー（中距離）あるいはマイクロ波（長距離）のような別の無線通信テクノロジーに備えた構成を含んでいてもよい。

【００６１】

次に図８を参照すると、無線または電気コネクタのいずれかによってローカル端末に接続されることのできる、オンボード生物測定学的検査を行われているスマートカードが示されている。主要な部分について、その構成およびアーキテクチャは上述された図１の実施形態のものに類似しており、同じ参照符号（おそらくシングルクォーテーションマークによって区別される）は類似した素子を示している。とくに、ＩＳＯ　ＣＰＵ112は異なった位置（コンタクト108の片側ではなくその下方）に示されているが、しかし上述したものと同じ機能を有している。

【００６２】

ＩＳＯアンテナ132は、ほぼカード100の周囲に沿うように配置された２つのループを備え、配線式の電気インターフェース108により提供されるものに類似したデータおよびパワーの両方のためのＩＳＯ　ＣＰＵ112へのＩＳＯコンパチブル無線インターフェースを提供する。さらに、セキュリティアンテナ134（示されている例では、内側アンテナ132であり、ただ１つのループから構成されている）は、ＤＣ－ＤＣ電力調整装置120を介したセキュリティＣＰＵ114への分離した電源を提供する。ＩＳＯ　ＣＰＵ112による以外に無線データへの直接的な接続は存在しないため、セキュリティＣＰＵ114内に記憶されている取り扱いに注意を要するデータは、このような無線インターフェースにより危険にさらされない。その代わり、外部読取装置および外部ネットワークへの配線接続だけを有する実施形態に関して上述したように、２個のプロセッサの機能は結合されることが可能であり、あるいは外部インターフェースがＩＳＯ　ＣＰＵ112ではなくセキュリティＣＰＵ114を介するものであることが可能であり、このとき、適切な無線セキュリティ手段がこのように変更されたアーキテクチャに組込まれなければならない。

【００６３】

図９は図８のカードの断面図である。示されているコンポーネントの大部分は中心コア126内に含まれており、コンタクトパッド108だけが上部保護層122を貫通していることに注意しなければならない。センサ110の動作領域は、上部層122中の上部ウインドウおよび上部層122と中心コア126との間に配置されたＰＣＢ134中の下部ウインドウを通ってアクセス可能であり、このＰＣＢ134は、種々の電気コンポーネントの間において必要とされる電気接続およびセンサ110の活動領域を取囲む包囲静電放電接地コンタクトを提供する。

【００６４】

下部層124および磁気ストライプ128もまた示されている。

【００６５】

指紋センサ

図１０はセンサ110の例示的な概略回路図であり、センサセル402のアレイ400が行404および列406に配列されている。示されているように、各セル402は起動ゲート410およびトランスデューサ412を備えている。指紋は指の皮膚リッジとバレーから形成されている。各センサセルトランスデューサ412は、これらのリッジの1つがアレイ400内のセル402のすぐ近くに触れたときに機械的および、または電気的な変化を経験し、実際に、指先上のリッジおよびバレーによって発生されたセンサ表面を横切るマイクロ圧力変化に基づいてデジタル指紋イメージを提供する。各トランスデューサ412は単一の可変キャパシタとして示されているが、種々のタイプのトランスデューサが人間の皮膚のこれらのリッジの１つの存在に応答することができることに注意すべきである。圧力感応性の圧電薄膜トランスデューサの特定の例においては、その薄膜がセルの付近で変形されて変化を生じさせ、そ

れがそのセルに接続されているキャパシタ中に記憶される。したがって、キャパシタ上の電圧は圧電材料の変形により生じた機械的応力の関数であり、それ故、これは、山または谷がセルより上方にあるか否かの関数である。関連した列ドライバ414からの１つの信号がそのセルのゲート410をオンに切替え、関連した行ドライバ416が接地されたとき、その電圧が行の出力ライン418上に出現し、出力ドライバ420において８ビットデジタル信号に変換される。圧電材料の変形の検出を最大化するために、圧電材料がポリイミドのような弾性材料上に形成されてもよいし、あるいはそれがポリイミド圧電材料であってもよい。類似したアレイ組織により構成されることできる別の例示的なアナログトランスデューサ技術は、可変抵抗および可変キャパシタンスを含んでいる。その代わり、各セルは、情報の単一のビットだけを提供する簡単なデジタルスイッチから構成されることができる。その場合、情報の付加的なビットは、同じ領域内にもっと多くのセルを設けることにより、あるいはもっと高い周波数で各セルをサンプリングすることにより発生されることができる。このような別の実施形態により、Ａ／Ｄ変換器は必要なくなる。

【００６６】

例示的な実施形態において、センサはわずか０．３３ｍｍの薄さであり、スマートカード中に埋込まれるように十分な耐性を有しており、静電気、素子またはユーザの皮膚の状態（湿っている、乾燥している、暖かい、冷たい）により影響を与えられない。センサ110の典型的な単位セルのサイズは２５ミクロン乃至７０ミクロンであり、典型的なピッチは２５ミクロン乃至７０ミクロンである。例示的なセンサは、１２．５ｍｍ^{2}乃至２５ｍｍ^{2}の感知領域と８ビットのマルチレベルの感度を有している。このようなセンサは、ＴＦＴ（薄膜トランジスタ）のアレイと、チタンバリウム酸化物またはストロンチウムバリウム酸化物のような薄膜圧電材料により形成されたもののような圧力感応キャパシタとによって製造されることが可能であり、感知領域全体をカバーして保護する上部電極を含んでいる。機械的な応力が与えられた場合、対応した電荷が発生され、薄膜圧電キャパシタ中に記憶される。その代わり、圧力ベースのセンサは、薄膜キャパシタと、炭素繊維が分散されたゴムシートのような圧力伝導性材料のシート、金属（銅または錫あるいは銀のような）めっきされた炭素繊維またはガラス繊維ベースの紙、あるいは金属が分散された弾性材料（シリコーンのような）により形成されるもののような圧力感応キャパシタと、および感知領域全体をカバーする上部電極シートと共にＴＦＴ（薄膜トランジスタ）のアレイとして製造されることができる。

【００６７】

行および列ドライバ416および414は、特定の指定された指紋センサ素子402が電気データを出力回路420に出力し、それによってユーザの指紋を表す物理的な入力をアナログ電気データに変換するためのものである。その後、出力回路420内のＡ／Ｄ変換器はアナログ電気信号をデジタル電気信号に変換する。各薄膜トランジスタは、共用される行相互接続をその関連したキャパシタ上の電圧に選択的に切替え、したがって各キャパシタ上の電圧が読取られることができ、また、それによって各セルの変形が測定されることができる。薄膜トランジスタの１つの全体的な列が同時に切替えられることが好ましく、したがって１つの選択された列中の複数（たとえば、８個）のセルが異なって行相互接続上において並列に読取られることができる。行および列のような多数のゲートの相互接続により、相互接続の数は減少し、一方同じ列の異なった行からの多数のセルの並列読取りにより全体的なアレイの読取り時間が減少する。センサからの出力電圧は、差動増幅器によって増幅されることができる。このような増幅器の出力はサンプリングされ、アナログデジタル変換（Ａ／Ｄ変換器）のために保持されることができる。

【００６８】

基板はガラス（非アルカリ族ガラスのような）、ステンレス鋼、アルミニウム、セラミックス（アルミニウム酸化物のような）、紙、ガラス樹脂であることができるが、しかし結晶シリコンの薄いシートであることが好ましい。薄膜半導体材料は、アモルファスシリコン、ポリシリコン、ダイヤモンド、または任意の別の半導体薄膜であることができる。圧電材料は、厚さの範囲が０．１乃至５０．０ミクロンであることが好ましいジルコン酸

チタン酸鉛（ＰＺＴ）薄膜のような圧電セラミックスであるか、あるいは圧電ポリマーポリイミド薄膜材料であることができる。相互接続材料は、Ｔｉ／Ｎｉ／Ｃｕ、Ａｌ、Ｃｒ／Ｎｉ／Ａｕ、Ｔｉ／Ｎｉ／Ａｕ、Ａｌ／Ａｕ、Ｗ／Ｃｕ、Ｗ／Ａｕであってもよい。

【００６９】

図１１は、結晶シリコンの薄い基板上に形成されたセンサのための支持装置を示している。結晶シリコンは優れた電気特性を有しており、また、必要とされるドライバおよび出力回路とのセンサアレイの集積を容易にするが、しかしながら、シリコーンの比較的広くて薄いシートは、局所化された表面圧力にさらされたときに曲がって折れる。示されている支持体は、同じ全体的な厚さを有するシリコンのシートにより提供されるものよりはるかに堅牢な構造を提供する。

【００７０】

示されているように、シリコンのモノリシックシート430はその厚さが約０．１ｍｍであり、バッキングプレート434上に取付けられたガラスエポキシの同じ厚さのフレーム432によって取囲まれており、このバッキングプレート434もまたガラスエポキシ構造であり、その厚さは約０．０５ｍｍである。フレーム432およびバッキングプレート434は、通常の印刷回路板（ＰＣＢ）技術を使用して容易に構成されることができる。とくに、バッキングプレート434の上面および下面は、ガラスエポキシコアにより分離された薄い銅の層436によってカバーされている。フレーム432は、セキュリティプロセッサ114に接続するための多数のはんだパッド440をその外周に沿って備えている。薄いシリコンチップ430は、フレーム432およびプレート434にエポキシで接着され、そのアクチブな領域は、上部保護電極446を取囲むシリコン430の露出された外端部444における通常のワイヤボンディング442によってフレーム432内の各電気トレースに電気的に結合されている。

【００７１】

整合アルゴリズム

処理電力が制限され、単一の基準サンプルとの簡単な１：１の整合だけが試みられる局所オンボード処理のために、指紋整合ソフトウェアは、２つのパターンから得られた詳細の比較的簡単な比較に基づくことができる。たとえば、１つの指紋のグレースケールのイメージは白および黒の２つの値に減少されることができ、３次元リッジは２次元の細いライン（ベクトル）に変換される。したがって、この方法の正確さは、数ある問題の中でもとくに、ぼやけ、膠着、歪、ラインセグメントの部分的欠如およびその他の効果の影響を受け易い。詳細方法は、原則的にその正確さは低いが、それに必要とされる計算リソースは少なく、また、多数の既存のデータベースに適合する可能性が生じる。

【００７２】

多くの処理パワーが利用可能であり、さらに精確な弁別が要求される可能性のある遠隔認証サーバにおける処理に対して、たとえば、“ＰＯＣ”（フェーズオンリー相関）整合アルゴリズムが使用される。ＰＯＣは、イメージ全体のマクロスコピックな整合に基づいた識別アルゴリズムである。逆に言えば、ＰＯＣは広範囲にわたる、すなわち、細部から全体的なイメージまでの構造的情報を整合する。したがって、ＰＯＣは膠着および部分的隙間のような雑音に強い正確さを提供することができる。原理的に、ＰＯＣ方法は、位置シフトおよび輝度の差の悪影響を受けず、高速であり（オフライン整合に対して約０．１秒）、非常に正確である。たとえば、ＰＯＣソフトウェアは、２次元高速フーリエ変換（“２ＤＦＦＴ”）を使用して２つの指紋パターンの空間周波数比較を行うことができる。２ＤＦＦＴは、指紋の物理的な２次元分布を表すデジタル化されたデータのアレイを周波数空間に変換し、換言すると、逆空間分布に変換し、ここでは高い密度のパターンが高い空間周波数を有する。回転変換は、周波数空間パターン整合を整合するために使用されることができる。ＰＯＣパターン整合は詳細ベクトル整合を有しており、それは、ＰＯＣは雑音として認識するが詳細解析は意味のあるデータとして解釈する記録された指紋パターン中の共通の欠陥によって誤って導かれないため、さらに有効である。

【００７３】

とくに要求の厳しいアプリケーションに対して、ハイブリッド方法は、いずれか１つの

方法だけよりも高い正確さおよびセキュリティを提供することができる。たとえば、捕捉する時に詳細方法を使用することができ、一方ＰＯＣ方法は遠隔サーバにおいて使用されることができる。別の例として、整合プロセスは、詳細および空間的関係の両者を解析し、両者の結果を考慮して１つの組合せられたスコアを生成することができる。

【００７４】

アプリケーション

上述した技術は、民間および政府用の両方において多くのアプリケーションに対して高レベルのセキュリティを提供する。各アプリケーションの要求に応じて、多数の秘密保護された安全なアプリケーションが同じカードおよび、または同じ認証サーバ上に共存して動作することが可能である。１実施形態において、ある単一のカードは２４個までの無関係の秘密保護された安全なアプリケーションを含むことができる。たとえば、この技術は、アクセス（物理的および、または論理的）の許可／拒否を行い、個人および、またはウォッチリストパーティの正確な位置および、または動きを識別すると同時に一方において別の秘密保護された安全なアプリケーションを動作させており、それらはそれぞれ互いから完全に、かつ秘密保護されて安全に隔離されている。

【００７５】

ここで考慮されているアプリケーションには以下のものがある：

・空港ＩＤ／アクセス
・建物のセキュリティ
・ホテルの客室のアクセス／料金請求
・病院
・オンラインゲーム
・ダウンロードされたエンターテイメント
・出生証明書
・コンピュータアクセス
・運転免許証－ＴＷＩＣ
・電子財布
・緊急医学情報
・爆発物取扱い免許証
・政府および軍用ファシリティアクセス
・ＨＡＺＭＡＴ免許証
・メディケアおよび給付金カード
・駐車場アクセス
・パスポート
・パイロットの免許証
・港ＩＤ／アクセス
・保険の証明
・社会保障カード
・信頼できる旅行者カード
・ビザまたは入国／出国許可証
・投票者登録カード
・福祉および食糧スタンプカード

これらのアプリケーションの多くに対して、カードのオンボードメモリはまた、登録されたカード保持者が彼のアイデンティティを証明してアクセスを許可したときにのみこのようなアクセスが可能である種々の種類の個人秘密情報の秘密保護された安全な記憶を行うことが好ましい。このような秘密情報の例を以下に示す：

・氏名、住所、生年月日、出生地、国籍、宗教、組織における地位、社会保障番号、運転免許証の番号、パスポート番号のような管理用情報、およびビザのタイプ、ビザの期限、市民権等のような入国管理情報
・電子財布のような金融情報、ビザ、マスターカード、アメリカンエクスプレス等のク

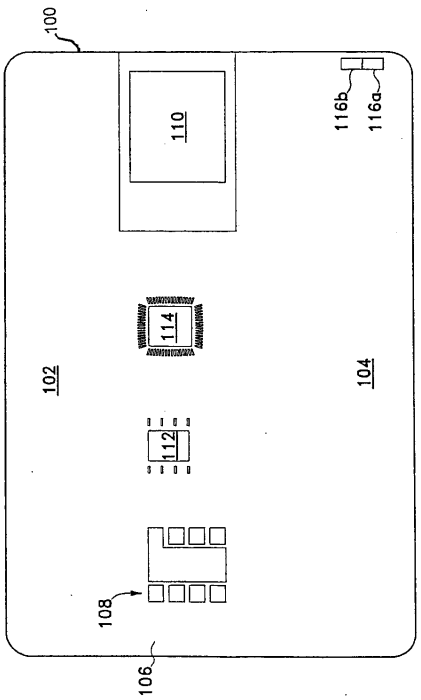
レジットカード情報、銀行の名称、銀行のバランス、マネートランスファー情報、ＩＲＳ番号、倒産記録等のような銀行情報
・身長、体重、指紋、虹彩、網膜、手の大きさ、骨格、声、ＤＮＡのような個人を識別するための生物測定学的情報、血液型、医学的診断テスト結果、病歴、薬物、保険情報、ある刺激に対する心理的および生理学的反応等のような生理学的または健康情報
・犯罪暦、重罪、軽犯罪、違反のような事件情報
・共同墓地、親類およびその他の連絡情報、弁護士情報、宗教情報のような緊急情報
・通学した学校、学位、ＦＤＤに関連する勤務していた会社を含む学歴や職歴
・データアクセス履歴（アクセス履歴のデータをカードに記憶すると共にカードから記憶する）
・指紋パターン、処理された指紋パターン、指紋パターンの結果のようなＩＤ関連情報
・永久パスワード、一時的パスワードおよび、またはワンタイムパスワードのようなパスワード
・公開キー、パーソネル（ｐｅｒｓｏｎｎｅｌ）キーおよび、またはワンタイムキーのような暗号化キー
以下、例示的なカード登録システムを説明する。

【００７６】
希望者は、申込書に記入してそれを提出し、写真および指紋がそれに含まれていることが好ましい。大部分の希望者について、彼等の養育者の書類の検査および１以上の入手可能な政府および民間データベースに対する提出された情報の簡単なクロスチェックは、その個人の本当のアイデンティティを確定するのに十分なものでなければならない。

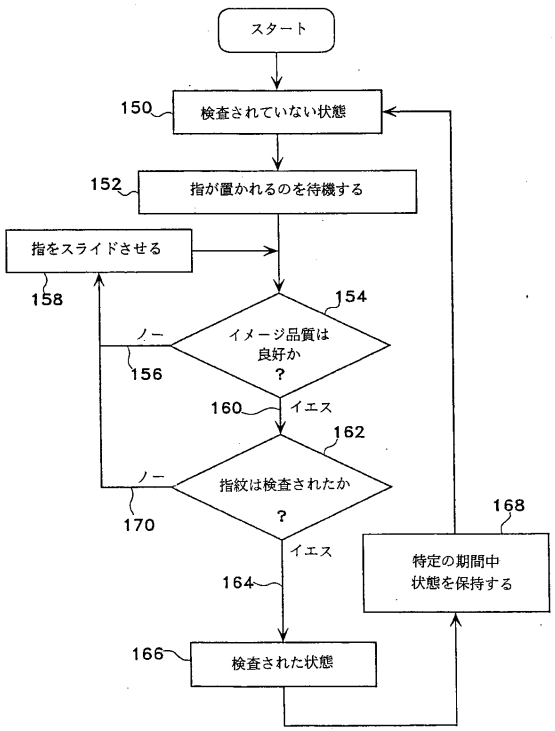
【００７７】
彼のアイデンティティがそのようにして検査され確認された後、希望者は発行局に進み、ここでカード発行者により必要だと考えられた任意の情報がカードにロードされる。希望者は、カード上のセンサの上に彼の指紋を置く。指紋がセンサ上に満足できるように置かれてカードにロードされると、カード上のタブは、誰かがカードのある定まった領域に二度と書込まないようにするそのある定まったヒューズの機能を果たさなくする電気衝撃が与えられる。その後、小さいタブは切断／ギロチンをオフにする（臍の緒のように）。その時点で、カードはＩＳＯコンタクト読取装置またはＩＳＯ無線システムによって読取りまたは書込みのいずれかだけを行うことができる。

【００７８】
ネットワークされた認証サーバの場合、カードにロードされた同じデータの一部または全てはまた暗号化された形態で遠隔サーバに送信される。このデータは、おそらく、通常カード上に記憶されておらず、ある定まった高度のセキュリティのアプリケーションに対して必要とされる可能性のある付加的なデータで補われる。

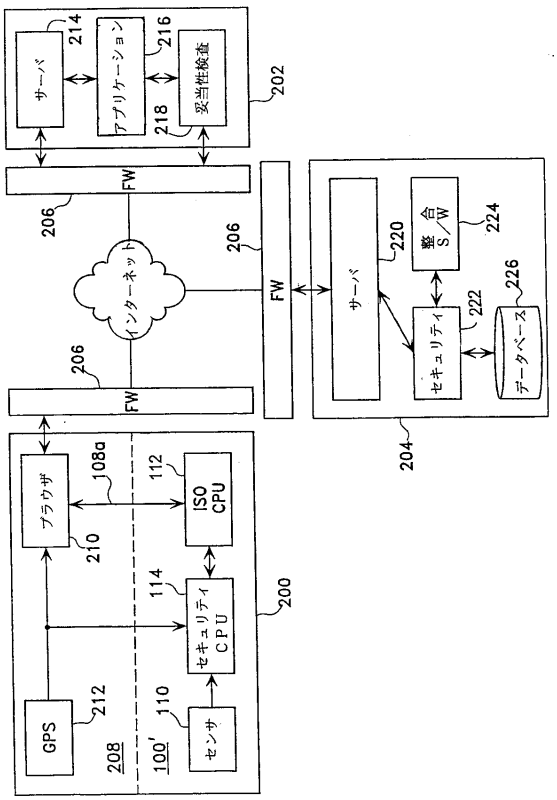
【図１】


100
110
116b
116a
114
102
104
112
108
106

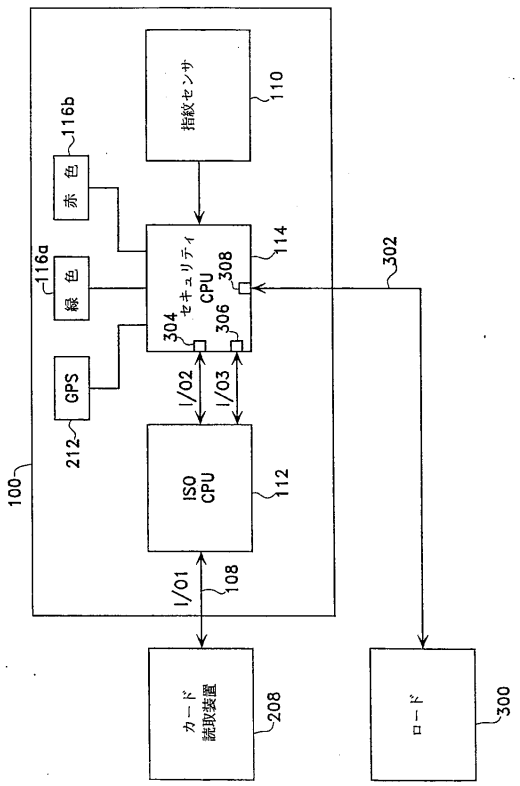
【図２】


スタート
150
検査されていない状態
152
指が置かれるのを待機する
指をスライドさせる
158
154
イメージ品質は良好か？
ノー
156
160
イエス
162
指紋は検査されたか？
ノー
170
イエス
168
特定の期間中状態を保持する
164
166
検査された状態

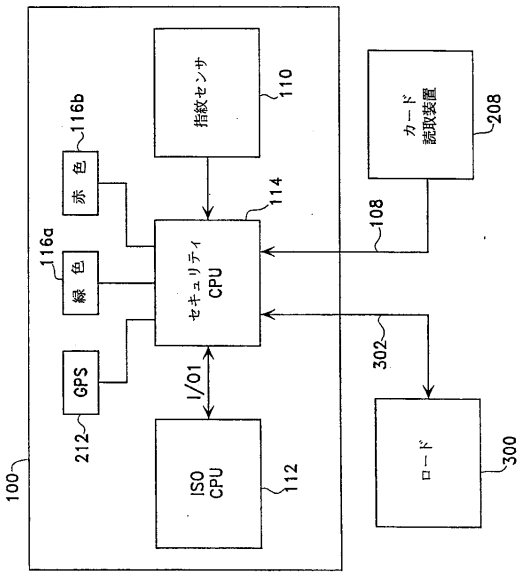
【図３】


サーバ
214
アプリケーション
216
妥当性検査
218
202
FW
206
インターネット
FW
206
FW
206
サーバ
220
整合S/W
224
セキュリティ
222
データベース
226
204
ブラウザ
108a
210
ISO CPU
112
セキュリティ CPU
114
200
GPS
212
センサ
110
208
100'

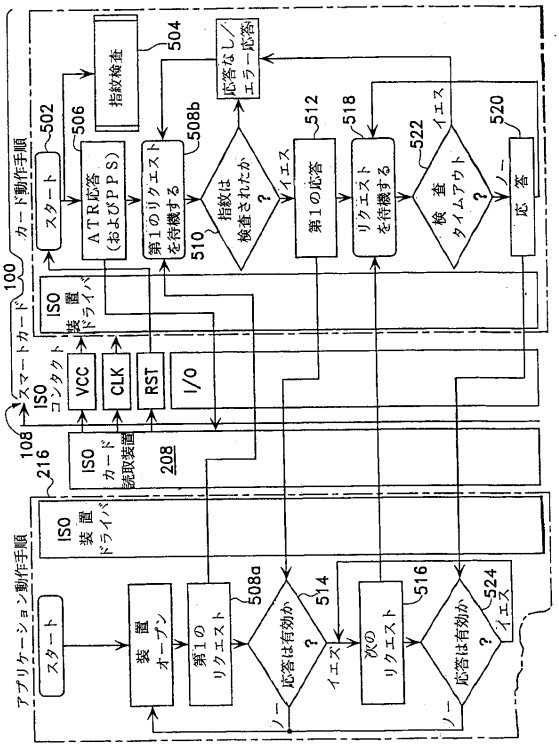
【図４】


指紋センサ
110
赤色
116b
緑色
116a
GPS
212
セキュリティ CPU
308
304
306
114
302
I/02
I/03
ISO CPU
112
I/01
108
100
カード読取装置
208
ロード
300

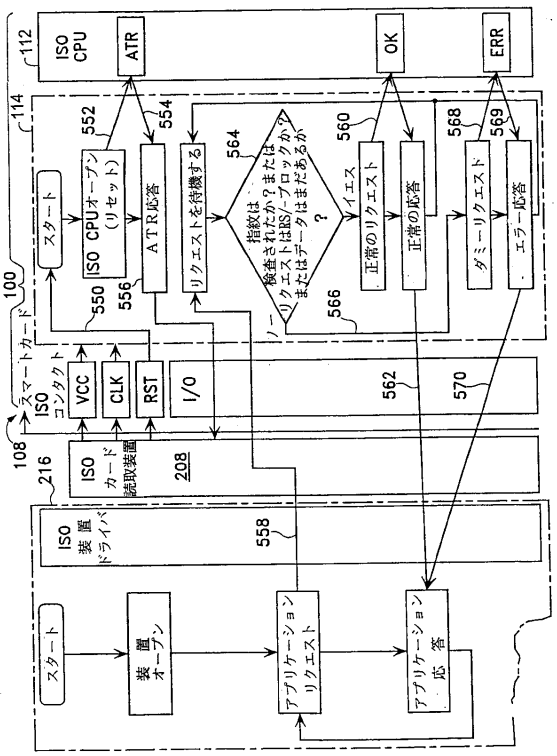
【図５】


100
ISO CPU
112
I/O1
212
GPS
116a
緑色
116b
赤色
セキュリティ CPU
114
指紋センサ
110
108
302
ロード
300
カード読取装置
208

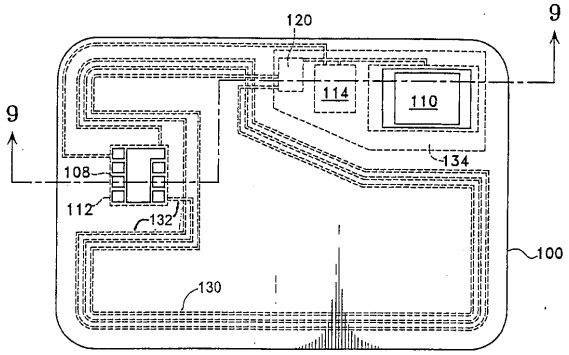
【図６】


カード動作手順
スタート
ATR応答 (およびPPS)
指紋検査
第1のリクエストを待機する
指紋は検査されたか?
イエス
第1の応答
リクエストを待機する
検査タイムアウト?
ノー
応答
応答なし/エラー応答
スマートカード 100
ISO コンタクト
VCC
CLK
RST
I/O
ISO 装置ドライバ
ISO カード読取装置 208
アプリケーション動作手順
装置オープン
第1のリクエスト
応答は有効か?
次のリクエスト

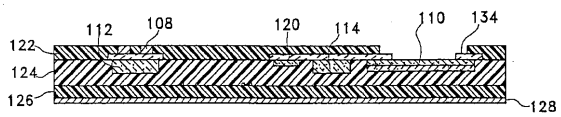
【図７】


ISO CPU 112
ATR
OK
ERR
スマートカード 100
スタート
ISO CPUオープン (リセット)
ATR応答
リクエストを待機する
指紋は検査されたか?またはリクエストはBIO/ブロックか?またはデータはまだあるか?
正常のリクエスト
正常の応答
ダミーリクエスト
エラー応答
ISO コンタクト
VCC
CLK
RST
I/O
ISO カード読取装置 208
ISO 装置ドライバ
装置オープン
アプリケーションリクエスト
アプリケーション応答

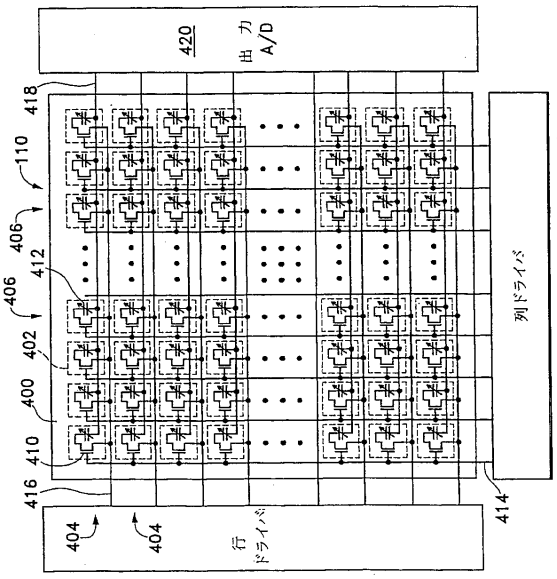
【図８】


120
9
9
114
110
134
108
112
132
100
130

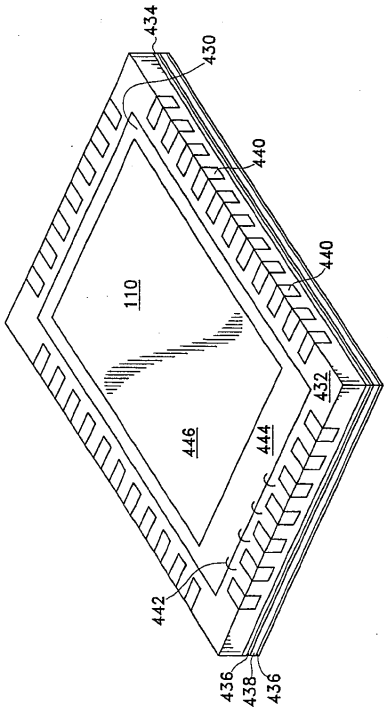
【図９】


112
108
120
114
110
134
122
124
126
128

【図１０】



【図１１】



【手続補正書】
【提出日】平成22年11月25日(2010.11.25)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
インテリジェントな識別カードにおいて、
生の生物測定学的データを捕捉するオンボードセンサと、
前記オンボードセンサに結合され、基準データを記憶するメモリを含み、捕捉された生物測定学的データを、対応した記憶された基準データと予め定められたしきい値内で比較し、前記予め定められたしきい値内に一致が存在する場合のみ、確認メッセージを発生し、前記予め定められたしきい値範囲内に一致が存在しない場合に前記識別カードの外部から入力されるデータへの接続をディスエーブルする第１のオンボードプロセッサと、
前記第１のオンボードプロセッサに結合され、インテリジェントカード機能を実行し、確認メッセージによってエネーブルされる第２のオンボードプロセッサと、
前記第１のオンボードプロセッサと前記第２のオンボードプロセッサのいずれか一方に結合され、外部ネットワークと通信するためのインターフェースとを具備しているインテリジェントな識別カード。
【請求項２】
前記第２のオンボードプロセッサはＩＳＯスマートカードプロセッサである請求項１記載の識別カード。
【請求項３】

前記第１のオンボードプロセッサはファイヤウォールによってＩＳＯスマートカードプロセッサから機能的に分離されている請求項２記載の識別カード。
【請求項４】
第１のオンボードプロセッサとの間でやり取りされる、前記識別カードの外部から入力されるデータは全て、ＩＳＯスマートカードプロセッサを通過する請求項２記載の識別カード。
【請求項５】
ＩＳＯスマートカードプロセッサとの間でやり取りされる、前記識別カードの外部から入力されるデータは全て、第１のオンボードプロセッサを通過する請求項２記載の識別カード。
【請求項６】
識別カードの現在の位置を決定するためのオンボード位置検出器と、
検出された位置に基づいて、カードの使用を制限する手段とをさらに具備している請求項１記載の識別カード。
【請求項７】
前記オンボード位置検出器は全地球測位衛星システム（ＧＰＳ）信号受信機を含んでいる請求項６記載の識別カード。
【請求項８】
ユーザが指紋センサ上でその指を操作しているときに実時間フィードバックが行われてセンサ上の指を最適に位置させるようにするインジケータをさらに具備している請求項１記載の識別カード。
【請求項９】
前記インターフェースは、
前記第２のオンボードプロセッサに結合されている無線インターフェースと、
前記第２のオンボードプロセッサに結合されている配線式の電気インターフェースとの少なくとも１つを含んでいる請求項１記載の識別カード。
【請求項１０】
前記無線インターフェースは、データおよびパワー送信の両方を行うＩＳＯコンパチブルアンテナである請求項９記載の識別カード。
【請求項１１】
前記インターフェースは、
パワー回路を介して前記第１のオンボードプロセッサに結合され、パワーを前記第１のオンボードプロセッサにのみ提供するセキュリティアンテナをさらに含んでいる請求項９記載の識別カード。
【請求項１２】
前記セキュリティアンテナはまたパワー回路を介して、前記オンボードセンサにもパワーを提供する請求項１１記載の識別カード。
【請求項１３】
基準データを記憶するオンボードメモリと、オンボード生物測定学的センサと、セキュリティプロセッサと、ＩＳＯカードプロセッサとを含んでいるインテリジェントな識別カードのユーザを識別する方法において、
オンボードセンサを使用して、生の生物測定学的データを捕捉し、
セキュリティプロセッサを使用して、捕捉された生物測定学的データを、オンボードメモリに記憶されている対応した基準データと予め定められたしきい値の範囲内で比較し、
セキュリティプロセッサを使用して、前記予め定められたしきい値範囲内に一致が存在する場合にのみ確認メッセージを発生し、その確認メッセージはＩＳＯカードプロセッサをエネーブルし、前記予め定められたしきい値範囲内に一致が存在しない場合に前記識別カードの外部から入力されるデータへの接続をディスエーブルし、
ユーザのアイデンティティが確認されたならば、ＩＳＯカードプロセッサの動作を可能にするステップを含んでいる方法。

【請求項１４】
ＩＳＯカードプロセッサとの間でやり取りされる、前記識別カードの外部から入力されるデータは全て、セキュリティプロセッサの第２の接続を通過する請求項１３記載の方法。
【請求項１５】
セキュリティプロセッサとの間でやり取りされる、前記識別カードの外部から入力されるデータは全て、ＩＳＯカードプロセッサを通過する請求項１３記載の方法。
【請求項１６】
生物測定学的データは指紋データを含み、センサは、そのセンサ上に置かれたユーザの指からデータを捕捉する指紋センサである請求項１３記載の方法。
【請求項１７】
ユーザが指紋センサ上のその指を操作しているときに実時間フィードバックを行い、センサ上の指を最適に位置させるようにする請求項１６記載の方法。
【請求項１８】
整合プロセスは、捕捉された生物測定学的データ中の細部および全体的な空間的関係の両方を考慮したハイブリッド整合アルゴリズムを使用する請求項１３記載の方法。
【請求項１９】
ユーザが指紋センサ上でその指を操作しているときに実時間フィードバックを行い、センサ上の指を最適に位置させるようにする請求項１３記載の方法。
【請求項２０】
前記確認メッセージの通信は、
ＩＳＯカードプロセッサに結合されている無線インターフェースを介する通信と、
ＩＳＯカードプロセッサに結合されている配線式の電気インターフェースを介する通信の少なくとも１つを含んでいる請求項１３記載の方法。
【請求項２１】
前記無線インターフェースは、データおよびパワー送信の両方を行うＩＳＯコンパチブルアンテナである請求項２０記載の方法。
【請求項２２】
さらに、セキュリティプロセッサに結合されているセキュリティアンテナおよびパワー回路を介して、パワーをセキュリティプロセッサに提供し、セキュリティアンテナとパワー回路とはカード上に設けられている請求項２０記載の方法。
【請求項２３】
さらに、セキュリティアンテナおよびパワー回路を介して、パワーをオンボード生物測定学的センサに供給する請求項２２記載の方法。
【請求項２４】
基準データを記憶するオンボードメモリと、オンボード生物測定学的センサと、セキュリティプロセッサと、ＩＳＯカードプロセッサとを含んでいるインテリジェントな識別カードのユーザを識別する装置において、
オンボードセンサを使用して、生の生物測定学的データを捕捉する手段と、
セキュリティプロセッサを使用して、捕捉された生物測定学的データを、オンボードメモリに記憶されている対応した基準データと予め定められたしきい値の範囲内で比較する手段と、
セキュリティプロセッサを使用して、前記予め定められたしきい値範囲内に一致が存在する場合にのみ確認メッセージを発生し、前記予め定められたしきい値範囲内に一致が存在しない場合に前記識別カードの外部から入力されるデータへの接続をディスエーブルする手段とを具備し、その確認メッセージはＩＳＯカードプロセッサをエネーブルし、
さらに、ユーザのアイデンティティが確認された場合に、ＩＳＯカードプロセッサの動作を可能にする手段を具備しているユーザ識別装置。
【請求項２５】
さらに、ユーザが指紋センサ上でその指を操作しているときに実時間フィードバックを

行い、センサ上の指を最適に位置させるようにする請求項２４記載の装置。

フロントページの続き

(51)Int.Cl.		F I			テーマコード（参考）
Ｇ０６Ｔ　7/00	*(2006.01)*	Ｇ０６Ｋ	19/00	Ｐ	
		Ｇ０６Ｔ	7/00	５３０	

(31)優先権主張番号　60/433,254
(32)優先日　平成14年12月13日(2002.12.13)
(33)優先権主張国　米国(US)
(31)優先権主張番号　60/484,692
(32)優先日　平成15年7月3日(2003.7.3)
(33)優先権主張国　米国(US)

（特許庁注：以下のものは登録商標）
１．ＦＲＡＭ

(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100095441
弁理士　白根　俊郎
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100103034
弁理士　野河　信久
(72)発明者　タミオ・サイトウ
アメリカ合衆国、カリフォルニア州　９４１０５、サン・フランシスコ、ビール・ストリート・ナンバー１５０７　３８８
(72)発明者　タカシ・アイダ
アメリカ合衆国、カリフォルニア州　９５１１７、サン・ホセ、デザート・アイル・ドライブ　９２８
(72)発明者　ウェイン・ドリズィン
アメリカ合衆国、カリフォルニア州　９５１３１、サン・ホセ、スイート・エフ、オールド・オークランド・ロード　１８１０

Ｆターム(参考)　5B035 AA14 BA03 BB09 BC01 CA01 CA23 CA25 CA38
5B043 AA04 AA09 BA02 DA05 DA07 FA04 GA02
5B285 AA01 AA04 BA03 BA06 BA07 BA08 CA32 CA42 CA43 CB07
CB08 CB12 CB15 CB52 CB55 CB62 CB64 CB73 CB75 CB85
CB92 CB94 DA04 DA05 DA09 DA10
5J104 AA07 KA01 KA04 KA16 KA17 NA05 NA35 NA38

【外国語明細書】
2011090686000001.pdf