【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成18年10月26日(2006.10.26)

【公表番号】特表2006-501583(P2006-501583A)
【公表日】平成18年1月12日(2006.1.12)
【年通号数】公開・登録公報2006-002
【出願番号】特願2004-571994(P2004-571994)
【国際特許分類】
Ｇ０６Ｆ　21/20　(2006.01)
Ｂ４２Ｄ　15/10　(2006.01)
Ｇ０６Ｔ　 1/00　(2006.01)
Ｇ０６Ｔ　 7/00　(2006.01)
Ｇ０６Ｋ　19/10　(2006.01)
Ｇ０６Ｋ　19/073　(2006.01)
Ｇ０６Ｋ　19/077　(2006.01)
Ｈ０４Ｌ　 9/32　(2006.01)
Ａ６１Ｂ　 5/117　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　15/00　３３０Ｆ
Ｂ４２Ｄ　15/10　５２１
Ｇ０６Ｔ　 1/00　４００Ｇ
Ｇ０６Ｔ　 7/00　５３０
Ｇ０６Ｋ　19/00　Ｓ
Ｇ０６Ｋ　19/00　Ｐ
Ｇ０６Ｋ　19/00　Ｋ
Ｇ０６Ｋ　19/00　Ｒ
Ｈ０４Ｌ　 9/00　６７３Ｄ
Ｈ０４Ｌ　 9/00　６７３Ｅ
Ａ６１Ｂ　 5/10　３２２

【手続補正書】
【提出日】平成18年9月8日(2006.9.8)
【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】
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インターフェースとを備えており、
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おり、確認メッセージは、前記オンボードメモリに記憶されている基準データとは異なる基準データを使用する追加の確認検査のために遠隔認証システムに送られるインテリジェントな識別カード。

【請求項２】
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１記載の識別カード。
【請求項３】
カードはＩＳＯスマートカードコンパチブルである請求項１記載の識別カード。
【請求項４】
前記オンボードプロセッサは、秘密保護された生物測定学的データを記憶し、処理するためのセキュリティプロセッサであり、前記識別カードはさらにＩＳＯスマートカードプロセッサを備えている請求項３記載の識別カード。
【請求項５】
前記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４記載の識別カード。
【請求項６】
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４記載の識別カード。
【請求項７】
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４記載の識別カード。
【請求項８】
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４記載の識別カード。
【請求項９】
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８記載の識別カード。
【請求項１０】
カードは上方の磁気ストライプ領域と下方の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の領域と前記下方の領域との間の中間領域内に配置されている請求項４記載の識別カード。
【請求項１１】
生物測定学的データは指紋データを含み、前記センサは、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１記載の識別カード。
【請求項１２】
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１１記載の識別カード。
【請求項１３】
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１１記載の識別カード。
【請求項１４】
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１１記載の識別カード。
【請求項１５】
前記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１４記載の識別カード。
【請求項１６】
前記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１４記載の識別カード。

【請求項１７】
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１８】
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１９】
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１記載の識別カード。
【請求項２０】
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２１】
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２０記載の識別カード。
【請求項２２】
前記インターフェースは、
電気コンタクトインターフェースと、
無線通信インターフェースの少なくとも１つを含んでいる請求項１記載の識別カード。
【請求項２３】
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、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２４】
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２３記載の識別カード。
【請求項２５】
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２４記載の識別カード。
【請求項２６】
第１のオンボ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、ＩＳＯスマートカードプロセッサを通過する請求項２４記載の識別カード。
【請求項２７】
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、愛１のオンボードプロセッサを通過する請求項２４記載の識別カード。

【請求項２８】
第１のオンボード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２７記載の識別カード。
【請求項２９】
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２３記載の識別カード。
【請求項３０】
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２９記載の識別カード。
【請求項３１】
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１２３記載の識別カード。
【請求項３２】
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２３記載の識別カード。
【請求項３３】
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３２記載の識別カード。
【請求項３４】
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３２記載の識別カード。
【請求項３５】
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３４記載の識別カード。
【請求項３６】
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、
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、
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し、
確認メッセージを外部ネットワークに伝送し、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おり、
前記オンボードメモリに記憶されている基準データとは異なる基準データを使用して遠隔認証システムのユーザを追加的に確認検査するステップを含んでいる方法。
【請求項３７】
識別カードで使用される整合アルゴリズムは遠隔認証システムにおいて使用される整合アルゴリズムとは異なっている請求項３６記載の方法。
【請求項３８】
さらに、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を分離された別の認証サーバに送信するステップを含んでいる請求項３６記載の方法。
【請求項３９】
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を受信し、
その整合リクエストに応答して、認証サーバにおいて肯定的な一致が生じるならば、秘密保護された安全な３ウェイ認証プロトコルを実行するステップを含み、この認証プロトコルは、
チャレンジ文字シーケンスを認証サーバから識別カードへ送信し、
チャレンジ文字シーケンスと整合リクエストに基づいて、識別カードでチャレンジ応答を発生し、
そのチャレンジ応答をアプリケーションサーバに転送し、
そのチャレンジ応答をアプリケーションサーバから認証サーバに転送し、
認証サーバにおいて、このチャレンジ応答が有効であるか否かを検査するステップを含んでいる請求項３６記載の方法。
【請求項４０】
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、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、
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４１】
ロードプロセス中に、第１の接続を介して、データをセキュリティプロセッサへロードし、
ロードプロセスが終了した後、第１の接続を永久にディスエーブルにするステップをさらに含んでいる請求項４０記載の方法。
【請求項４２】
ＩＳＯ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の第２の接続を通過する請求項４０記載の方法。
【請求項４３】
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カードプロセッサを通過する請求項４０記載の方法。
【請求項４４】
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４０記載の方法。
【請求項４５】
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４４記載の方法。
【請求項４６】
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４０記載の方法。
【請求項４７】
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４０記載の方法。

【請求項４８】
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４０記載の方法。
【請求項４９】
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４８記載の方法。
【請求項５０】
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４８記載の方法。
【請求項５１】
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５０記載の方法。
【請求項５２】
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、
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、
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手段と、
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具備し、
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おり、確認メッセージは遠隔認証システムに送信されて、前記オンボードメモリに記憶されている基準データとは異なる遠隔位置に記憶されている基準データを使用して追加の確認検査が行われるユーザ識別装置。
【請求項５３】
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、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５４】
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５３記載の装置。